Estado de la

Ciberseguridad

en el Sistema Financiero Colombiano

ASOBANCARIA

OEA

Más derechos para más gente

Estado de la Ciberseguridad en el Sistema Financiero Colombiano

Preparado y publicado por el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (cybersecurity@oas.org)

Luis Almagro
Secretario General
Organización de los Estados Americanos

Farah Diva Urrutia
Secretaria de Seguridad Multidimensional
Organización de los Estados Americanos

Alison August Treppel
Secretaria Ejecutiva
Comité Interamericano conrta el Terrorismo
Organización de los Estados Americanos

Equipo Técnico de la OEA
Belisario Contreras
Orlando Garcés
Jorge Bejarano
Kerry-Ann Barrett
David Moreno
Diego Subero
Gabriela Montes de Oca
Valentina Namé
Mariana Cardona
Jaime Fuentes
Víctor Sánchez
Sofía Hunter
María Paula Lozano
Einar Lanfranco
Juan Sebastián Fonseca

Santiago Castro Gómez
Presidente
Asociación Bancaria y de Entidades Financieras de Colombia ASOBANCARIA

Mónica Gómez Villafañe
Vicepresidente
Asociación Bancaria y de Entidades Financieras de Colombia ASOBANCARIA

Alejandro Vera Sandoval
Vicepresidente Técnico
Asociación Bancaria y de Entidades Financieras de Colombia ASOBANCARIA

Equipo Técnico ASOBANCARIA
Ángela Vaca Bernal
Jaime Rincón Arteaga
Santiago Castiblanco Hernández

Agradecimientos
Consejería Presidencial para Asuntos Económicos y Transformación Digital.

Superintendencia Financiera de Colombia.

Asociación de Compañías de Financiamiento – AFIC.

Asociación de Comisionistas de Bolsa – ASOBOLSA.

Asociación de Fiduciarias de Colombia – ASOFIDUCIARIAS.

Asociación Colombiana de Administradoras de Fondos de Pensiones y de Cesantía – ASOFONDOS.

Federación de Aseguradores Colombianos – FASECOLDA.

TABLA DE CONTENIDO

Estado de la

Ciberseguridad

en el Sistema Financiero Colombiano

1.

Resumen Ejecutivo

Este estudio es un aporte de la Secretaría General de la Organización de Estados Americanos (OEA), que tiene como propósito brindar información fidedigna sobre el Estado de la Ciberseguridad en el Sistema Financiero Colombiano. Este documento es un esfuerzo más de la OEA en su tarea de fortalecer las capacidades y nivel de conciencia sobre las crecientes amenazas a la seguridad digital que aborda la región América Latina y el Caribe.

La información analizada en el presente estudio proviene de una base de datos de 73 entidades financieras participantes del Sistema Financiero Colombiano[1]. Para llevar a cabo este análisis, la OEA diseñó, con el apoyo de expertos del sistema financiero, un instrumento específico de recolección e información. A partir del análisis efectuado con base en el instrumento empleado, se presentan a continuación los principales hallazgos.

Hallazgos significativos sobre la seguridad digital en las entidades financieras del Sistema Financiero Colombiano:

- En relación con la preparación y gobernanza de la seguridad digital, en el 40% de las entidades financieras del país existen dos (2) niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital. No obstante, el número de niveles jerárquicos que existen entre el CEO y el máximo responsable de la seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) depende también del tamaño de la organización. En referencia al número de áreas a cargo de estas temáticas, en el 23% de las entidades del sector bancario existe una única área responsable de la seguridad digital, valor inferior al registrado en los bancos de la región de América Latina y el Caribe, en el cual el 74% tiene esta misma condición (Organización de Estados Americanos, 2018).

- Respecto al apoyo a la gestión del riesgo de seguridad de la información (incluyendo ciberseguridad) por parte de la alta dirección de la entidad financiera, se destaca que un 71% del total de las entidades financieras del país lo demuestran aprobando mayor presupuesto, y un 63% fomentando la concientización, educación y capacitación. Particularmente, en el sector bancario de Colombia, se resalta que un 69% del total de los establecimientos bancarios del país lo demuestran aprobando mayor presupuesto y un 62% aprobando / reforzando una estructura organizacional especializada, mientras que en el sector bancario de América Latina y el Caribe, es más común que se haga exigiendo la adopción de buenas prácticas de seguridad (65%), fomentando la capacitación y sensibilización en seguridad digital (63%) e impulsando planes de seguridad digital (60%) (Organización de Estados Americanos, 2018).

- En el 97% de las entidades financieras de Colombia, la junta directiva recibe reportes periódicos acerca de riesgos de seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales, mientras el 55% de quienes atendieron la encuesta considera que lograr que la alta dirección de la organización invierta en soluciones de seguridad digital es medianamente o muy complejo, a pesar de la relevancia que tienen las inversiones especialmente en materia de prevención y desarrollo de capacidades. En este mismo sentido, al comparar el sector bancario de Colombia con el promedio de la región de América Latina y el Caribe, se observa que en dicho sector, en el 100% de los establecimientos bancarios la junta directiva recibe reportes periódicos acerca de riesgos de seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales, cifra superior a la reportada en la región (72%) (Organización de Estados Americanos, 2018).

- Dentro de los marcos de seguridad y/o estándares internacionales más implementados en las entidades financieras, se encuentran ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems e ISO/IEC 27032:2012 - Information technology -- Security techniques -- Guidelines for cybersecurity (en el 85% y 60% de las entidades financieras, respectivamente).

• En materia de conformación de equipos de profesionales de seguridad de la información (incluyendo ciberseguridad) por cada entidad financiera en Colombia, se observa que éstos se componen en promedio de trece (13) miembros. No obstante, este valor varía dependiendo del tamaño de la entidad.

• Se resalta que el 77% de entidades financieras encuestadas en el país considera adecuado que el equipo creciera en el corto plazo, lo cual es un reconocimiento a necesidades de gestión crecientes en los aspectos a su cargo. Estas necesidades crecientes llevan en muchos casos a requerir procesos de tercerización, siendo la actividad que más frecuentemente se contrata la relativa a la realización de pruebas de seguridad / análisis de vulnerabilidades con un 78% del total, seguida de correlación de eventos con un 67% del total.

• En cuanto a capacidades de detección y análisis de eventos de seguridad de la información (incluyendo ciberseguridad), que son vitales para la gestión sistemática de este tipo de riesgos para proteger los sistemas de información críticos entre el 93% y del 90% de entidades financieras del país se centran en la implementación de los cortafuegos (firewalls) y las actualizaciones automatizadas de virus y sistemas. Temas como la aplicación de computación cognitiva, internet de las cosas (Internet of Things –IoT–) o Registro distribuido (Blockchain) para la detección y análisis de eventos de seguridad se encuentran aún muy incipientes con niveles inferiores al 3% de entidades financieras.

• Los riesgos de seguridad de la información que las entidades financieras de Colombia consideran que merecen mayor atención, sin importar el tamaño de la organización, son i) pérdida / robo de activos de información clasificada (confidencial o sensible), ii) indisponibilidad de infraestructura crítica, y iii) compromiso de credenciales de usuarios privilegiados.

• El 100% de las entidades financieras de Colombia manifiestan que identificaron algún tipo de evento (ataques exitosos y ataques no exitosos) de seguridad digital en su contra. Los eventos de seguridad digital más comúnmente identificados son: i) el código malicioso o malware (75% del total de entidades), ii) el Phishing, Vishing o Smishing (75% del total de entidades) y iii) la violación de políticas de escritorio limpio (clear desk) (70% del total de entidades). Se destaca que un 19% de las entidades financieras identifican ocurrencia de eventos de malware diariamente.

• Según las entidades financieras en Colombia, el tipo de eventos (ataques exitosos y ataques no exitosos) de seguridad digital que usan los ciberdelincuentes con más frecuencia contra los clientes (socios, asociados o usuarios) de servicios financieros son: i) Phishing, ii) Software espía (Malware o troyanos), y iii) Ingeniería social. También resulta importante anotar que dentro de las principales motivaciones para la realización de estos ataques se encuentran las económicas (75%), y mencionan que no existieron razones como asuntos de reputación personal como hacker, asuntos geopolíticos o espionaje.

• Respecto a la gestión, respuesta y recuperación ante incidentes de seguridad digital, al menos un tercio de las entidades financieras del país contaron con estrategias de gestión, respuesta y recuperación ante incidentes de seguridad de la información (incluyendo ciberseguridad).

- Como parte de las estrategias de gestión de riesgos de seguridad digital, el 85% de las entidades financieras en el país realizan evaluación de madurez bajo alguna metodología de seguridad de la información. Aquellas entidades financieras que no logran hacer este tipo de evaluaciones señalan que las principales razones son: i) falta de asignación de presupuesto (30% de entidades sin evaluación), y ii) complejidad técnica de las soluciones requeridas (30% de entidades sin evaluación).

- En cuanto a la comunicación de incidentes de seguridad digital, casi la totalidad (96% de las entidades financieras) ofrece un mecanismo para que sus colaboradores (empleados y contratistas) reporten incidentes (ataques exitosos) de seguridad digital sufridos y el 82% cuenta con un plan de comunicaciones que permita informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida. El 99% de las entidades financieras reporta incidentes (ataques exitosos) sufridos ante una autoridad de regulación en Colombia.

- En materia de capacitación y concientización, el 94% de entidades financieras cuenta con planes de preparación, respuesta y capacitación en asuntos de seguridad de la información (incluyendo ciberseguridad) para sus colaboradores, los cuales se ejecutan en su mayoría de manera continua / permanente (41% de entidades). El mecanismo más efectivo a partir del cual se ha generado mayor conciencia en las entidades financieras respecto de los riesgos de seguridad digital es a través de capacitaciones internas y el uso de campañas por correo electrónico.

- En promedio, el retorno sobre la inversión en seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales equivale aproximadamente a 10%, lo que la mayoría considera que es un retorno de alta rentabilidad.

- El presupuesto destinado a la seguridad digital para una entidad financiera en Colombia equivale aprox. al 1,76% del EBITDA del año inmediato anterior.

- El costo total de respuesta y de recuperación ante incidentes de seguridad digital para una entidad financiera en Colombia equivale aprox. al 2,16% del EBITDA del último año fiscal.

- Con los valores obtenidos del estudio se estima que el costo total anual de respuesta y de recuperación ante incidentes de seguridad digital de las entidades financieras de la muestra[2] en Colombia en 2018 fue de COP $ 321 mil millones aproximadamente.

Cuadro 1.

Principales resultados por tamaño de entidad financiera del Sistema Financiero Colombiano

Entidades Financieras Grandes	Entidades Financieras Medianas	Entidades Financieras Pequeñas
En el 33% existe una única área responsable de la seguridad digital	En el 85% existe una única área responsable de la seguridad digital	En el 82% existe una única área responsable de la seguridad digital
En el 75% existen dos (2) niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital	En el 80% existen dos (2) niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital	En el 83% existen dos (2) niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital
La mayoría de las entidades grandes (50%) cuenta con un equipo conformado por 16-30 miembros	La mayoría de las entidades medianas (48%) cuenta con un equipo conformado por 1-5 miembros	La mayoría de las entidades pequeñas (85%) cuenta con un equipo conformado por 1-5 miembros
Son objeto de ataques de todo tipo de eventos de seguridad digital, resaltando identificación de todos por la mayoría de dichas entidades en el país	Son objeto de ataques de todo tipo de eventos de seguridad digital, resaltando identificación de todos por la mayoría de dichas entidades en el país	Son objeto de ataques de todo tipo de eventos de seguridad digital, resaltando identificación de todos por la mayoría de dichas entidades en el país
El 80% identifican ocurrencia de eventos de malware diariamente	El 25% identifican ocurrencia de eventos de malware diariamente	El 13% identifican ocurrencia de eventos de malware diariamente
La mayoría (50%) detecta entre un 61% y un 80% de eventos con sistemas propios	La mayoría (31%) detecta entre un 80% y un 100% de eventos con sistemas propios	La mayoría (47%) detecta entre un 80% y un 100% de eventos con sistemas propios
El 67% manifiestan que han sido víctimas de ataques exitosos	El 19% manifiestan que han sido víctimas de ataques exitosos	El 7% manifiestan que han sido víctimas de ataques exitosos
El 83% realiza evaluación de madurez y adelanta las acciones correspondientes	El 50% realiza evaluación de madurez y adelanta las acciones correspondientes	El 50% realiza una evaluación de madurez y adelanta las acciones correspondientes
El 100% ofrece un mecanismo para que sus clientes reporten a la entidad incidentes (ataques exitosos) sufridos	El 88% ofrece un mecanismo para que sus clientes reporten a la entidad incidentes (ataques exitosos) sufridos	El 73% ofrece un mecanismo para que sus clientes reporten a la entidad incidentes (ataques exitosos) sufridos
El 100% cuenta con un plan de comunicaciones para informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida	El 84% cuenta con un plan de comunicaciones para informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida	El 77% cuenta con un plan de comunicaciones para informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida
El 50% reporta entre el 0% y el 20% de los incidentes ocurridos ante la Fiscalía General de la Nación o la Policía Judicial en Colombia	El 42% reporta entre el 0% y el 20% de los incidentes ocurridos ante la Fiscalía General de la Nación o la Policía Judicial en Colombia	El 40% reporta entre el 0% y el 20% de los incidentes ocurridos ante la Fiscalía General de la Nación o la Policía Judicial en Colombia

Entidades Financieras Grandes	Entidades Financieras Medianas	Entidades Financieras Pequeñas
El 40% manifiesta que el presupuesto de seguridad digital equivale en promedio a menos del 1% del EBITDA del anterior año fiscal	El 40% manifiesta que el presupuesto de seguridad digital equivale en promedio a menos del 1% del EBITDA del anterior año fiscal	El 67% manifiesta que el presupuesto de seguridad digital equivale en promedio a menos del 1% del EBITDA del anterior año fiscal
El presupuesto destinado a la seguridad digital equivale aprox. al 2,63% del EBITDA del año inmediato anterior	El presupuesto destinado a la seguridad digital equivale aprox. al 2,03% del EBITDA del año inmediato anterior	El presupuesto destinado a la seguridad digital equivale aprox. al 1,77% del EBITDA del año inmediato anterior
En el 100% el presupuesto de seguridad digital aumentó en comparación al año fiscal inmediato anterior	En el 83% el presupuesto de seguridad digital aumentó en comparación al año fiscal inmediato anterior	En el 60% el presupuesto de seguridad digital aumentó en comparación al año fiscal inmediato anterior
Destinan el 50% del presupuesto en Plataformas y medios tecnológicos (ej.: hardware, software)	Destinan el 39% del presupuesto en Plataformas y medios tecnológicos (ej.: hardware, software)	Destinan el 29% del presupuesto en Plataformas y medios tecnológicos (ej.: hardware, software)
Destinan el 30% del presupuesto en Servicios tercerizados (ej.: gestión de seguridad, externalización, soporte)	Destinan el 32% del presupuesto en Servicios tercerizados (ej.: gestión de seguridad, externalización, soporte)	Destinan el 40% del presupuesto en Servicios tercerizados (ej.: gestión de seguridad, externalización, soporte)
El retorno sobre la inversión en seguridad digital equivale aproximadamente a un 15,00%	El retorno sobre la inversión en seguridad digital equivale aproximadamente a un 10,00%	El retorno sobre la inversión en seguridad digital equivale aproximadamente a un 3,75%
El 40% manifiesta que estimó el costo total de respuesta y de recuperación ante incidentes	El 33% manifiesta que estimó el costo total de respuesta y de recuperación ante incidentes	El 17% manifiesta que estimó el costo total de respuesta y de recuperación ante incidentes
El 100% manifiesta que el costo total de respuesta y de recuperación ante incidentes equivale en promedio a menos del 1% del EBITDA del anterior año fiscal	El 40% manifiesta que el costo total de respuesta y de recuperación ante incidentes equivale en promedio a menos del 1% del EBITDA del anterior año fiscals	El 60% manifiesta que el costo total de respuesta y de recuperación ante incidentes equivale en promedio a menos del 1% del EBITDA del anterior año fiscal
El costo total de respuesta y de recuperación ante incidentes de seguridad digital por entidad equivale aprox. al 1,00% del EBITDA del último año fiscal.	El costo total de respuesta y de recuperación ante incidentes de seguridad digital por entidad equivale aprox. al 2,18% del EBITDA del último año fiscal.	El costo total de respuesta y de recuperación ante incidentes de seguridad digital por entidad equivale aprox. al 2,83% del EBITDA del último año fiscal.

Hallazgos significativos sobre la ciberseguridad desde la perspectiva de los usuarios de las entidades del sector bancario en Colombia:

- Los usuarios de Bancos y otros establecimientos de crédito privilegian los medios virtuales sobre los presenciales, lo cual concuerda con el alto grado de digitalización de los servicios y el impulso a la utilización de estos, ya que el 80% de los encuestados consulta saldos disponibles y realiza movimientos (transacciones) usando internet, porcentaje muy superior a los que consultan directamente en la oficina con un 22%, o por línea telefónica 30%, e igualmente prefieren utilizar las aplicaciones móviles con un 69%, mientras que lo hacen por cajero automático un 38%.

- Para operaciones como depósito de cheques o efectivo en Bancos y otros establecimientos de crédito, se empieza a posicionar dentro de las opciones disponibles, medios con apoyo tecnológico como los cajeros automáticos multifuncionales, para realizar este tipo de operaciones, con un 17% de usuarios, que realizan estas transacciones en los cajeros automáticos de las entidades que ofrecen este servicio. Otro aspecto para destacar frente a este tipo de operaciones, es el importante rol que juegan los corresponsales bancarios, empleados por el 29% de los clientes de Bancos y otros establecimientos de crédito.

- Los cajeros automáticos continúan siendo los canales más utilizados para el manejo del efectivo, con un 82% de los usuarios de Bancos y otros establecimientos de crédito encuestados, sin embargo, este tipo de transacciones también ha tomado fuerza a través de opciones que ofrecen las entidades financieras como los corresponsales bancarios, que con un 39%, superan en preferencia de los usuarios a las transacciones realizadas directamente en las oficinas de las entidades bancarias (33%).

- Dentro del uso de medios para realizar compras por parte de usuarios de Bancos y otros establecimientos de crédito, se evidencia un incremento en la utilización de medios virtuales como internet con un 68%, el cual supera al uso del datáfono que alcanza un 55% y se posicionan de forma importante las aplicaciones móviles, que ya tienen un 48% de usuarios que las usan para este propósito.

- Servicios que fueron antes muy comunes, hoy se ven desplazados por nuevas opciones: Para el pago de obligaciones de los productos de Bancos y otros establecimientos de crédito se impone el uso de medios de pago virtuales, siendo internet el preferido con un 59% seguido de aplicaciones móviles un 46%, lo cual supera al 30% de usuarios que aun prefieren hacerlo en oficinas de la entidad, de igual manera, para otra operación muy común como lo es el pago de servicios públicos también se prefieren los medios virtuales como internet (59%) o por aplicaciones móviles (40%) , que a los medios físicos como corresponsales bancarios (31%), o en oficinas (29%).

- Respecto a los tipos de dispositivo empleados por usuarios de Bancos y otros establecimientos de crédito, se prefiere de interacción digital a través de teléfono inteligente (smartphone), con un 53%, que supera por más del doble la preferencia de uso de dispositivos como un computador de escritorio (22%) o portátil (20%), ya sea para realizar transacciones o consultas.

- El grado de utilización de medios digitales para realizar transacciones bancarias que reflejan los usuarios de banca encuestados es alto, alcanzando un 88%. Solo el 12% de los usuarios manifestó no usar medios digitales para realizar transacciones, siendo la desconfianza en el entorno digital (60%) la principal motivación de quienes no utilizan los medios digitales para realizar sus operaciones bancarias.

- Respecto a cultura de seguridad digital solo un 43% de los usuarios bancarios manifestaron conocer muchas de las definiciones ofrecidas en la encuesta y solo un 24% conocía todas las expresiones referidas a distintos tipos de incidentes cibernéticos. Los usuarios indicaron que se mantienen informados principalmente a través de prensa y medios de comunicación (67%), así como mediante las redes sociales (55%). Apenas un 47% de los usuarios se informan de las nuevas amenazas de ciberseguridad por campañas de seguridad adelantadas por sus entidades bancarias, lo cual puede evidenciar que aún las mismas no resultan suficientes para facilitar el desarrollo de conciencia sobre las amenazas con destino al eslabón más débil de la cadena, que es precisamente el usuario.

- En cuanto a las medidas de seguridad implementadas por los usuarios de Bancos y otros establecimientos de crédito para prevenir incidentes digitales, la más frecuente fue la de usar antivirus en sus computadores (78%), seguido por otras prácticas de seguridad relacionadas con el acceso exclusivo en computadoras confiables (76%), uso de contraseñas con condiciones seguras (66%) y evitando el acceso a través de redes Wi-Fi públicas (59%), la habilitación de notificaciones de transacciones vía SMS (57% o correo electrónico (55%), y el uso de tokens o medios complementarios de autenticación (37%).

- Respecto a la experiencia de usuarios frente a incidentes de seguridad digital que han visto comprometida la confidencialidad, integridad o disponibilidad de su información o sus recursos financieros en su Banco, el 61% afirmó no haber sufrido este tipo de incidentes, mientras que el 27%, indicó que sí había sido afectado y un 5% respondió no saber y/o conocer el asunto. Del total de usuarios afectados,Entre los tipos de incidentes digitales experimentados más frecuentes, un 20% del total de usuarios afectados señaló fraude por llamada telefónica, mientras el un 17% señalo que fue por fraude a través de correo electrónico, y el un 13% apuntó a la infección con software malintencionado (virus) como la causa, y al tiempo que un 7% indicó al fraude por medio de mensaje de texto. Es de anotar que un porcentaje alto indicó no saber la causa (58%).

Entre los tipos de incidentes digitales experimentados más frecuentes, un 20% del total de usuarios afectados señaló fraude por llamada telefónica, un 17% fraude a través de correo electrónico, un 13% infección con software malintencionado (virus), y un 7% indicó al fraude por medio de mensaje de texto. Es de anotar que un porcentaje alto indicó no saber la causa (58%).

- La frecuencia con la que los usuarios expresan haber sido víctimas dio como resultado que en su mayoría, esto es un 59%, sufrió incidentes de esta naturaleza una a dos veces, mientras que un 29% señaló ninguna, y solo el 7% indicó de tres a cinco veces.

- Con respecto al efecto negativo de los incidentes sufridos por los usuarios de Bancos y otros establecimientos de crédito, el de mayor impacto fue la exposición de datos personales, con un 50%. Un 49% manifiesta que a raíz del incidente tuvo

pérdida de recursos financieros, un 33% se vio afectado para tener acceso al servicio, mientras un 29% manifiesta un deterioro de la imagen que tenían sobre la entidad financiera y un 10% tuvo como efecto un daño a su reputación como cliente del sistema financiero, como por ejemplo en su perfil de crédito, y finalmente el mismo porcentaje obtuvo la afectación de robo de identidad.

- En cuanto al impacto económico para los usuarios de Bancos y otros establecimientos de crédito afectados participantes del estudio, un 40,66% manifiesta que no sufrió pérdida de dinero, un 13,69% perdió entre 100.001 y 500.000 pesos, un 12,86% perdió de 1.000.000 a 3.000.000 de pesos y un 11,62% de 500.001 a 1.000.000 de pesos. De la totalidad de los usuarios que efectivamente tuvieron pérdida económica, el 49% manifestó haber sido reparado o compensado totalmente, frente a un 14% que indicó haberlo sido parcialmente y un 37% que expresó no haber recibido ningún tipo de indemnización.

- Sobre los mecanismos de reporte, los usuarios de Bancos y otros establecimientos de crédito entrevistados indicaron, en su mayoría, que la institución bancaria sí ofrece un mecanismo para reportar incidentes (67%) y que en efecto han reportado el incidente ante su banco (81%). Por su parte, se resalta la manifestación de que, conforme a las respuestas, un 56% no sabe de su existencia, solo el 24% afirma que en su país existe un mecanismo para reportar incidentes ante un ente gubernamental, mientras que un 20% indica que no existe y el escenario es aún menos positivo si se tiene en cuenta el bajo nivel de reporte ante autoridades policiales o judiciales, dado que, de las respuestas obtenidas, solo el 26% han elevado a estas instancias los incidentes que les han afectado.

- Respecto a la percepción de los usuarios sobre la evolución de los riegos de que ocurran incidentes cibernéticos, un 64% indica que han empeorado en el último año, frente a un 26% y 10% que indicó desconocerlo o no percibir ese aumento, respectivamente.

El detalle del estudio puede apreciarse en los numerales 4 y 5 de este documento, los cuales desarrollan en profundidad los hallazgos enunciados y muchos otros aspectos que pueden resultar de interés.

Estado de la Ciberseguridad en el Sistema Financiero Colombiano

2.

Prólogo

Luis Almagro

Secretario General

Organización de los Estados Americanos (OEA)

La pandemia de COVID-19 durante el año 2020 está teniendo un impacto dramático en la sociedad y en la economía global. Según un reporte del Foro Económico Mundial (FEM)[3], se pronostica que en 2020: la economía mundial se contraerá un 3%, 500 millones de personas correrán el riesgo de caer en la pobreza y el comercio mundial colapsará entre 13% y 32%. El panorama para la región de América Latina y el Caribe -solo en las actividades de este año- se proyecta tendrá una contracción del 5.3%, conforme a un estudio efectuado por la Comisión Económica para América Latina y el Caribe de Naciones Unidas (CEPAL)[4].

El citado reporte del FEM también analizó las consecuencias económicas de COVID-19 que dominan las percepciones de riesgos de las organizaciones alrededor del mundo encontrando que la tercera consecuencia más preocupante para las empresas es un aumento en los ataques cibernéticos y el fraude de datos.

Otro reporte del FEM[5] encuentra que esta pandemia ha obligado a todos a depender en gran medida de Internet y su economía digital, por lo que es imperativo que los líderes gestionen estratégicamente los riesgos de seguridad digital y adopten un enfoque estratégico para la resiliencia cibernética. Es decir, la ciberseguridad es tema central en la agenda global para generar confianza digital y adaptación para el futuro digital tanto de las organizaciones como de los individuos.

Bajo la actual coyuntura, la Secretaría General de la Organización de los Estados Americanos (OEA) a través del Programa de Ciberseguridad adscrito al Comité Interamericano contra el Terrorismo (CICTE) continúa trabajando en el desarrollo de una agenda sobre seguridad digital en las Américas, en cooperación con una amplia gama de entidades nacionales y regionales de los sectores público y privado en la región.

El objetivo del Programa de Ciberseguridad es ser el principal punto de referencia en el hemisferio occidental para desarrollar la cooperación y la creación de capacidades en los Estados Miembros, desarrollando actividades para fortalecer la capacidad para detectar amenazas cibernéticas y prevenir, responder y recuperarse de incidentes cibernéticos, operando en tres (3) pilares: (i) el desarrollo normativo, especialmente Políticas Nacionales de Ciberseguridad; (ii) el fortalecimiento de capacidades para disfrutar de las oportunidades que aportan el desarrollo de las TIC pero también para hacer frente a los riesgos asociados; y (iii) actividades de investigación y gestión del conocimiento en Ciberseguridad.

Con apoyo de actores claves, la producción de estudios relevantes sobre el estado de la ciberseguridad en sectores estratégicos de la economía por parte de la OEA se ha logrado obtener y compartir importantes resultados, conclusiones y recomendaciones con los Estados Miembros.

Uno de los sectores estratégicos con mayor relevancia, incluso bajo la actual coyuntura generada por la pandemia de COVID-19, ha sido el sector financiero. Este sector ha logrado adoptar y aprovechar efectivamente tecnologías de la información y las comunicaciones con soluciones que van desde acceso remoto a gran escala, para cumplir condiciones de distanciamiento social y órdenes de "quedarse en casa", hasta el uso de soluciones de inteligencia artificial para facilitar el análisis de otorgamientos de créditos y alivios a sus clientes, atendiendo medidas y facilidades implementadas por varios gobiernos en la región; lo cual no solo les ha permitido continuar sus operaciones, sino incluso generar beneficios y reducir costos.

Después de elaborar y socializar estudios regionales como el "Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe" en el año 2018 y estudios nacionales como el "Estado de la Ciberseguridad en el Sistema Financiero Mexicano" en el año 2019, el Programa de Ciberseguridad de la OEA publica el presente estudio sobre el "Estado de la Ciberseguridad en el Sistema Financiero Colombiano", elaborado con la colaboración de la Asociación Bancaria y de Entidades Financieras de Colombia (ASOBANCARIA) y con participación de otros importantes gremios del sistema financiero.

El estudio presenta los resultados y análisis sobre los eventos y/o incidentes de seguridad de la información (incluyendo de ciberseguridad) y fraudes ocurridos a través de medios digitales, a partir de información provista por entidades financieras y por usuarios del Sistema Financiero Colombiano, en el marco de un protocolo de confidencialidad de la información.

Los principales insumos del presente estudio fueron las encuestas aplicadas a entidades financieras, las cuales brindaron información que permitió conocer de mejor manera la forma en que gestionan los riesgos de seguridad digital y su impacto. Igualmente, se tuvo como fuente las encuestas aplicadas a usuarios, para obtener datos sobre el tipo de operaciones y el uso de los medios digitales, su cultura en seguridad digital, así como el grado de impacto sufrido como consecuencia de incidentes de seguridad digital.

El estudio se divide en dos partes de la siguiente manera:

- Parte 1) Ciberseguridad en las Entidades del Sistema Financiero Colombiano: Los instrumentos aplicados ofrecen información en tres secciones. La primera ofrece información sobre los perfiles de las características de las entidades financieras; la segunda se ocupa de aspectos asociados a la gestión de riesgos de seguridad digital y la tercera aborda aspectos relacionados con el impacto de los incidentes en las mismas.

- Parte 2) Ciberseguridad de los Usuarios de Servicios Prestados por las Entidades del Sistema Financiero Colombiano: Los instrumentos aplicados ofrecen información en tres secciones. La primera ofrece información sobre las características de los usuarios; la segunda se ocupa de aspectos asociados a la cultura de seguridad digital y la tercera aborda aspectos relacionados con el impacto de los incidentes.

La OEA agradece a ASOBANCARIA por la gestión de apoyo para convocar a sus entidades financieras agremiadas que participaron del estudio y también por coordinar con otros gremios del sector financiero colombiano, para facilitar la participación del resto de entidades financieros objeto de análisis. La valiosa colaboración de todas las entidades financieras, y de todas las autoridades participantes relacionadas con el Sistema Financiero Colombiano, permitieron al equipo técnico de la OEA preparar el reporte que está en sus manos.

A partir de lo anterior, así como de las investigaciones realizadas con soporte en diferentes referentes abordados en el estudio, el estudio genera hallazgos relevantes desde la perspectiva de entidades financieras y sus usuarios, así como recomendaciones pertinentes al Sistema Financiero Colombiano, contemplando las entidades financieras de Colombia, las autoridades y organismos reguladores del sistema financiero y las autoridades justicia del Gobierno de Colombia, y por supuesto, los usuarios de estas entidades, con miras a contar con un entorno digital más confiable y seguro para los servicios ofrecidos por este vital sector estratégico, el cual el país reconoce como infraestructura crítica.

Con este estudio, se reitera una vez más nuestro inquebrantable compromiso con la generación de conocimiento en materia de ciberseguridad en sectores estratégicos. En el sector financiero en particular, estamos consolidando unos insumos que, partiendo del estudio regional sobre el sector bancario, ahora exploran la realidad particular de países como México, y ahora Colombia, que seguramente permitirá a todos los actores del ecosistema digital relacionados con el sistema financiero, emprender acciones pertinentes para fortalecer su ciberseguridad.

Invito a los Estados Miembros, a que sigamos avanzando en este tipo de actividades de investigación y gestión del conocimiento en materia de ciberseguridad, como herramienta fundamental para mejorar las condiciones y capacidades de ciberseguridad de la región, y más aún bajo las actuales condiciones que surgen en ambientes de reactivación y recuperación posterior a la pandemia, de construcción de redes de seguridad socioeconómica y de fortalecimiento de cooperación global. Desde la OEA estaremos atentos al apoyo que podamos brindar.

Estado de la Ciberseguridad en el Sistema Financiero Colombiano

Santiago Castro

Presidente

Asociación Bancaria y de Entidades Financieras de Colombia ASOBANCARIA

El estudio Estado de la Ciberseguridad en el Sistema Financiero Colombiano, realizado por el Programa de Ciberseguridad adscrito a la Secretaría del Comité Interamericano contra el Terrorismo (CICTE), brinda un enfoque al desarrollo de políticas públicas, a la concientización del usuario financiero y una mirada del estado actual de ciberseguridad de las entidades financieras colombianas, temáticas sobre las cuales la Asociación Bancaria y de Entidades Financieras de Colombia, ASOBANCARIA, busca de manera permanente compartir y difundir conocimientos para la promoción de reflexiones y acciones.

Actualmente, la industria financiera es uno de los sectores con mayores índices de digitalización. De acuerdo con cifras de la Superintendencia Financiera de Colombia, al cierre de 2019, el 56,84% del monto total de las operaciones se realizaron a través de canales no presenciales. Cada día un mayor número de clientes del sector financiero son usuarios de la banca electrónica y realizan transacciones por internet o pagos a través de dispositivos móviles. El uso de estos canales digitales trae consigo nuevos retos, los cuales deben ser manejados de manera adecuada con el fin de mitigar los posibles ataques a los que están expuestos actualmente el sector y por supuesto, sus usuarios. Esto cobra particular relevancia en la pandemia actual del COVID-19 debido a que los diferentes gobiernos han pedido practicar distanciamiento social, lo cual ha llevado a los clientes a usar aún más canales no presenciales para realizar sus trámites financieros.

Teniendo en cuenta el rol que desempeña el sector financiero para el desarrollo y crecimiento de un país, no sorprende que cada vez haya un mayor nivel de concientización sobre las consecuencias e implicaciones de ataques cibernéticos, siendo claro que la ciberseguridad ya no puede considerarse como un tema exclusivo del departamento de sistemas sino un tema a tratarse desde una visión estratégica que abarque a toda la organización. Del mismo modo, cabe resaltar que, de acuerdo con cálculos de ASOBANCARIA, el fraude en ambiente no presente para 2018 representó el 58,5% del fraude total, concentrado principalmente en las categorías de tarjetas de crédito y cuentas de ahorro y corriente, demostrando así la relevancia de la ciberseguridad que debe tener la banca colombiana.

Asimismo, en los últimos años se han desarrollado estudios, por ejemplo, Advancing Cyber Resilence: Principles and Tools for Boards, del Foro Económico Mundial, el cual brinda

herramientas y principios para poder integrar el ciber riesgo y la ciber resiliencia en las estrategias de negocios. Por su parte en Colombia, los documentos CONPES 3701 de 2001, CONPES 3854 de 2016 y CONPES 3995 de 2020 han brindado el marco normativo y de política pública en ámbitos de ciberseguridad, ciberdefensa y mitigación de los diversos riesgos cibernéticos, involucrando no solamente al gobierno sino a su vez al sector privado.

No siendo ajenos a esta realidad, desde ASOBANCARIA hemos implementado diversas estrategias gremiales. En Colombia, los comités de Ciberseguridad y Prevención del Fraude actúan como instancia de estudio y consulta del sector financiero en temas de prevención y mitigación del riesgo de fraude y de ciberseguridad, promoviendo las mejores prácticas de seguridad entre las entidades asociadas.

Además, a través del Centro de Respuesta de Incidentes de Ciberseguridad – CSIRT, en ASOBANCARIA lideramos los esfuerzos de colaboración en el sector para compartir los incidentes de ataques cibernéticos. El CSIRT sectorial se fundamenta en estrechos lazos de cooperación local e internacional con agencias de investigación y una continua articulación con autoridades; a través de una plataforma en línea las entidades financieras y centros de investigación a nivel global, regional y local comparten información de amenazas cibernéticas bajo estándares internacionales.

Sabemos que es a través de la colaboración que podremos enfrentar este tipo de retos que afronta el sector financiero, por lo que en el futuro se espera que estos esfuerzos se den a nivel regional, gracias a las características y riesgos similares que comparte la banca en América Latina.

Es importante resaltar que, entre más rápido se comparte una amenaza o vulnerabilidad, más posibilidades tendrán las otras entidades para poner en marcha las defensas adecuadas para mitigarla. Así mismo, cuantos más datos confiables tengamos mejores serán las decisiones.

La voluntad de cooperación y el contar con información oportuna juegan un papel relevante en la pandemia actual dadas sus consecuencias en materia de ciberseguridad para los países, tomando en cuenta que las medidas de aislamiento social han implicado que la mayoría de las transacciones financieras se realicen en canales digitales. De acuerdo con Microsoft, cada país en el mundo ha tenido al menos un ciberataque con temática del coronavirus, es decir, malware o phishing, que utilizan palabras relacionadas con COVID-19 para engañar a los usuarios. Esto es más preocupante si se tiene en cuenta que las consecuencias económicas causadas por la emergencia sanitaria han llevado a los estados a brindar ayudas y asistencias a los grupos más necesitados, por lo que éstos corren el riesgo de perder estos alivios en tiempos apremiantes.

Para hacer frente a estas amenazas, que se han multiplicado en esta pandemia, es necesario un trabajo conjunto permanente entre los miembros del sector privado del ecosistema financiero, entes regulatorios y agencias del Estado.

Si bien esta información fue recolectada en 2019 y no recoge los efectos de la pandemia del COVID-19, confiamos en que los resultados de este estudio permitirán identificar de manera integral las oportunidades y fortalezas del sistema financiero colombiano en materia de ciberseguridad, siendo así de interés no solo de las entidades que conforman este sector sino de los supervisores y del Gobierno nacional, en busca de articular una agenda de política en ciberseguridad para nuestro país. De igual manera, la data recolectada de los usuarios financieros proporcionará información de cómo se ven afectados éstos y cómo generar campañas de concientización más asertivas.

Estado de la **Ciberseguridad** en el Sistema Financiero Colombiano

3.

Aportes

Victor Manuel Muñoz

Consejero Presidencial
para Asuntos Económicos y
Transformación Digital
Presidencia de la República de
Colombia

En varios países los sectores críticos y prioritarios en materia de seguridad cibernética son el sector de Defensa, Telecomunicaciones, Utilities, y claramente el sector financiero. Esto se debe a que son los sectores más digitalizados y líderes en automatización de procesos. Así mismo, uno de sus principales enfoques es innovar con el uso de tecnologías emergentes y adoptar nuevos modelos de negocios alrededor de la tecnología. Esta capacidad de innovación puede mejorar la relación con los ciudadanos en estos sectores, pero también les genera una mayor exposición a los riesgos cibernéticos.

En el caso específico del sector financiero, el Informe de Operaciones de la Superintendencia Financiera de Colombia del primer semestre de 2020, se evidenció que las operaciones financieras realizadas a través telefonía móvil (2.469.655.860) fueron el principal canal seguido del internet (966.211.885), superando a las efectuadas en oficinas (181.062.441). .. El sistema financiero reportó 966.211.885 operaciones realizadas en el canal Internet, de las cuales 313.056.268 fueron monetarias por $1.646,3 billones y 653.155.617 no monetarias. Las operaciones realizadas en 2020 en el canal Internet presentaron un aumento del 24.4% frente al segundo periodo de 2019

Este crecimiento apunta a una tendencia que se mantendrá por mucho más tiempo, por lo que debemos garantizar el ambiente propicio para que la adopción tecnológica sea acelerada y progresiva en este sector. En este sentido, además de la digitalización mediante el uso de tecnologías de vanguardia, se deben redoblar los esfuerzos para aumentar la confianza de los usuarios en este tipo de canales. Más aún cuando más del 50% de la población se encuentra en línea ahora y se cuenta con más de 21 mil millones de dispositivos IoT en todo el mundo, con una proyección de duplicar su número para 2025.[6]

Unido a la percepción de seguridad de los usuarios, es evidente que a medida que avanzamos en el objetivo de la digitalización, las amenazas de seguridad también incrementan. Según The Global Risks Report 2020, elaborado por el Foro Económico Mundial, el 75% de los encuestados manifestaron que esperaban riesgos asociados a ataques cibernéticos robo de dinero y de información

Esta situación no es ajena al caso colombiano, donde según información del Centro Cibernético Policial, en el periodo comprendido entre el 1° de enero de 2019 al 21 de septiembre de 2019 se produjeron 16.043 denuncias por delios cibernéticos, mientras que en el mismo periodo del 2020 se reportaron 28.207 denuncias.

En este punto toma relevancia el concepto de ciberseguridad y confianza digital, que ya es protagonista en varias discusiones de seguridad nacional. En este contexto, se busca que los países tomen medidas específicas para hacer un análisis detallado de los riesgos cibernéticos e implementen medidas efectivas que protejan infraestructuras críticas.

La respuesta a este nuevo escenario ha sido conjunta, no solo se ha fortalecido el marco normativo para combatir los delitos informáticos, sino que se trazó todo un marco de acción para orientar los esfuerzos del Gobierno con documentos de política pública tales como el CONPES 3701 del 14 de julio de 2011[7] y el 3854 del 11 de abril de 2016[8], desde los cuales se han abordado importante acciones para fortalecer la gestión de seguridad digital en Colombia. Recientemente, se expidió el documento CONPES 3995 de 2020[9] "Política Nacional de Confianza y Seguridad Digital" con el cual se actualiza el marco de política pública en esta materia y que tiene como objetivo *"Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías"*.

Ante esta nueva realidad cibernética, la pregunta obligada que debemos hacernos es: ¿Colombia está preparada? La respuesta es sí y con un plan de mejora permanente.

Como parte de la actualización de los lineamientos vigentes en el país en materia de seguridad digital estamos adoptando un "modelo de madurez de desarrollo de capacidades de seguridad cibernética". Este modelo atiende especialmente a las recomendaciones del Centro de Capacidad de Seguridad Cibernética Global de la Universidad de Oxford. Este enfoque incorporado en el nuevo CONPES fija acciones a favor de garantizar una mejora real y efectiva de las capacidades del país en Seguridad Digital e incorpora el concepto "confianza digital" como aspecto relevante para la política, entendiendo que, sin confianza digital, las personas no proporcionarán información, no se intercambiarán bienes o servicios en línea y no se darían interacciones tal como han resaltado instancias tan importante como el Foro Económico Mundial - FEM . Todo esto, alineado al proceso de transformación digital que se está adelantando para el país que incluye un mayor fomento para acciones de investigación y orientado a tecnologías propias de la Cuarta Revolución Industrial como Internet de las cosas, Big data, computación en la nube e Inteligencia Artificial y que hemos incluido tanto en el plan de desarrollo del país, como en la política pública a lo largo de estos años.

A su vez, los esfuerzos conjuntos entre el Gobierno Nacional y sectores como el financiero son fundamentales para el establecimiento de lazos de confianza en el entorno digital. Sólo así, se podrá avanzar en Colombia hacia un verdadero marco de Gobernanza para la Seguridad Digital que parta de una visión compartida de la ciberseguridad. Por lo tanto, se debe involucrar de manera efectiva a las múltiples partes interesadas y promover un trabajo coordinado y permanente, garantizando así que Colombia reafirme la alta competitividad de su sector financiero a nivel global. El año pasado, la Asociación Bancaria y de Entidades Financieras de Colombia ASOBANCARIA, constituyó un Equipo de Respuesta a Incidentes Cibernéticos (CSIRT- sus siglas en inglés) para intercambiar información sobre amenazas cibernéticas en el sector. El objetivo del CSIRT es reaccionar de manera oportuna y proactiva a amenazas que se presentan en el entorno digital como phishing, malware, ataques de denegación de servicios y ransomware

(secuestro de datos), entre otros. Para este fin, el equipo tiene disponibles más de 15 fuentes de información local e internacional que le permiten conocer las últimas amenazas que se vienen presentando y articulándose con los demás CSIRTs a partir del ColCERT.

No obstante, a lo anteriormente mencionado, con la pandemia originada por el SARS CoV2 (COVID-19) el mundo y Colombia se han tenido que replantear en la adopción y estructuración de las transacciones financieras y la ciberseguridad.

Es así como, según datos del Centro Cibernético Policial, al comparar tan solo en el periodo de la pandemia, la violación a datos personales presentó un aumento del 163%, con 4.115 denuncias, las suplantaciones de sitios web con un aumento del 435%, para un total de 2.612 denuncias y el acceso abusivo a sistemas informáticos con un aumento del 88% para un total de 3.382 denuncias.

A la fecha, se manejan diferentes iniciativas para poder concientizar a la ciudanía de la importancia de tener ciertos protocolos de seguridad con el fin de evitar ser un objetivo de crímenes digitales, para esto el gobierno ha implementado campañas a nivel nacional de seguridad junto con la policía nacional[10]. A la vez, el gobierno a trabajo en la articulación interinstitucional a partir del Comité de Seguridad Digital y canales de comunicación directos. Una buena estrategia que ha facilitado el proceso de identificación y denuncia ha sido el impulso del CAI Virtual[11] y el portal "A Denunciar Virtual"[12]

Por último, Colombia ha venido trabajando con diferentes organizaciones tanto nacionales como internacionales para reforzar e implementar mejores tácticas de defensa ante estos crímenes. Así mismo, el Grupo de Respuesta a Emergencias Cibernética de Colombia – colCERT ha participado de manera activa compartiendo información de indicadores de compromiso y dominios maliciosos asociados a COVID-19 a través de la plataforma csirtamericas.org de la Organización de Estados Americanos que ha permitido a 19 países y 27 equipos de respuesta a incidentes de los países miembros recibir información técnica para que permita generar acciones de mitigación, investigación de posibles amenazas que afectan la región.

Estado de la

Ciberseguridad

en el Sistema Financiero Colombiano

Jorge Castaño Gutiérrez

Superintendente Financiero de Colombia
Superintendencia Financiera de Colombia

La globalización y las aceleradas innovaciones tecnológicas están influyendo en el estilo de vida de las personas, las actividades económicas y el desarrollo de las naciones, exigiendo a los miembros de la sociedad una actitud proactiva frente a un entorno en permanente evolución, tal como lo plantea Eric Hoffer, escritor y filósofo estadounidense, cuando afirma *"En tiempos de cambio, quienes estén abiertos al aprendizaje se adueñarán del futuro, mientras que aquellos que creen saberlo todo estarán bien equipados para un mundo que ya no existe"*.

Innovación y sus riesgos

La innovación en la prestación de servicios financieros se está extendiendo rápidamente por todo el mundo y afecta a una gran cantidad de procesos en el sector, relacionados, entre otros, con el servicio al cliente, asesoría, pagos y transacciones, préstamos, seguros y gestión de cuentas.

Las entidades del sector financiero, que se ven enfrentadas a un entorno cambiante y a una dinámica transformación digital, encuentran en el uso de tecnologías emergentes la oportunidad de ofrecer al consumidor financiero servicios disruptivos, ajustados cada vez más a sus necesidades. En armonía con esta tendencia, Colombia es uno de los tres países que lideran la actividad FINTECH en América Latina de acuerdo con un estudio realizado por el Banco Interamericano de Desarrollo (BID), identificándolo como el más dinámico en la creación de startups.

Tecnologías como blockchain, inteligencia artificial, data analytics, biometría e internet de las cosas, se han consolidado, están al alcance de personas y entidades de todo tipo y tamaño y su aplicación en diferentes sectores y actividades solo está limitada por la creatividad.

Sin embargo, la interconectividad y la adopción de estas tecnologías traen consigo un incremento en la exposición a los riesgos cibernéticos que están demandando esfuerzos importantes para identificarlos y gestionarlos por parte de entidades y autoridades. Uno de los grandes retos de las organizaciones lo constituye la seguridad de la información, en particular, la que reside o se procesa en medios electrónicos, la cual, ahora más que nunca, se encuentra expuesta a las amenazas cibernéticas dado el entorno global de Internet y de los sistemas de información, que no tienen una limitación fronteriza.

Así lo confirman ataques como los perpetrados en 2016 con transferencias no autorizadas por más de $81 millones de dólares, o del ransomware WannaCry que infectó más de 250.000 sistemas informáticos en 150 países, al igual que las diferentes fugas que han comprometido información de cientos de millones de individuos. Los países de Centro y Suramérica también han comenzado a experimentar un creciente número de ataques en los últimos meses, afectando diferentes sectores de la economía, en particular, al sistema financiero con incidentes que han impactado a establecimientos bancarios y sistemas de pagos electrónicos.

Situaciones como las descritas son muestra de una realidad preocupante que ratifican la importancia de la seguridad de la información y reflejan un panorama de grandes retos tanto a nivel técnico como procedimental y legal.

Para hacerle frente a este panorama tan complejo, los ministros y gobernadores del G20 ya se pronunciaban en marzo de 2017, en Baden-Baden, Alemania, recordando la importancia de los servicios financieros nacionales e internacionales para el desarrollo de la sociedad y señalaban que el uso malicioso de las tecnologías de la información y las comunicaciones podrían alterarlos, comprometiendo la seguridad, la confianza y poniendo en peligro la estabilidad financiera. Mencionaron, además, que promoverían la capacidad de recuperación de los servicios en instituciones financieras que se vieran afectadas, incluso en países fuera del G20.

Sobre el riesgo cibernético

El uso malicioso de las tecnologías de la información y las comunicaciones, junto con la globalización e interconexión de las mismas, enfrentan a la sociedad a una nueva tipología de riesgo a gestionar, conocida como “riesgo cibernético”. Sus fuentes pueden encontrarse en la organización o fuera de ella. Un evento de riesgo cibernético a menudo es intencional, deliberado o malicioso, pero podría ser involuntario: vinculado a una falla de software, mal funcionamiento del hardware o configuración incorrecta de un componente de TI.

Los eventos de riesgo cibernético también conllevan un riesgo de reputación significativo, especialmente para las instituciones financieras, lo que puede conducir a la pérdida de la confianza del cliente en la entidad afectada y, en general, en el sistema. El impacto de un incidente de riesgo cibernético converge con otros dominios de riesgo, no está aislado o confinado, a menudo desencadena un conjunto de eventos que impacta y se superpone con otros riesgos y, aun así, generalmente se analiza de forma independiente por la importancia que ha adquirido en los últimos años. La evaluación del impacto del posible riesgo cibernético, dentro del marco más amplio de gestión de riesgos es, por lo tanto, todo un desafío.

En el contexto del sector de servicios financieros, el riesgo cibernético se refiere a los riesgos operativos en el entorno cibernético o virtual que comprende Internet, comunicaciones inalámbricas o computación en la nube, en otras palabras, la exposición de acciones u operaciones en el ambiente conocido como el “ciberespacio”, que pueden resultar en la pérdida de confidencialidad, integridad y disponibilidad de datos o información, afectando las operaciones de la entidad y su infraestructura tecnológica.

El riesgo cibernético tiene, además, una naturaleza cambiante impulsada por varios factores: la evolución de la tecnología, que puede generar nuevas vulnerabilidades; las interconexiones

entre instituciones financieras y con otras organizaciones; los esfuerzos de los ciberdelincuentes para encontrar nuevos métodos de ataque y comprometer los sistemas de TI; así como acciones delictivas que antes se hacían únicamente en el mundo físico y ahora emplean medios informáticos como la extorsión y la suplantación de identidad.

A medida que los servicios financieros crecen exponencialmente en el entorno digital, la naturaleza y la escala de los riesgos cibernéticos subyacentes están evolucionando. El aumento en el despliegue de la tecnología financiera, los tiempos de entrega para el lanzamiento de servicios financieros electrónicos, la integración de soluciones de múltiples proveedores, los prestadores de servicios de TI que a menudo operan fuera del ámbito regulatorio, el entorno global y generalizado de los servicios financieros y los flujos de transacciones de gran valor, hacen que los servicios financieros sean particularmente propensos a los ciberataques. Cada vez más, los grupos delictivos organizados, que son transnacionales o presuntamente respaldados por gobiernos, encuentran formas ingeniosas y perniciosas de llevar a cabo ataques cibernéticos para obtener ganancias ilícitas, realizar acciones terroristas o generar interrupciones de los sistemas financieros.

Acerca de la regulación

Cómo regular las tecnologías emergentes es una pregunta compleja, la imposición excesiva de estrictas restricciones al desarrollo de una tecnología puede retrasar o prevenir beneficios potenciales; pero también, de continuar la incertidumbre regulatoria, los inversores serán reacios a respaldar el desarrollo de tecnologías por temor a que puedan ser prohibidas más tarde o rechazadas si la ausencia de la regulación efectiva lleva a usos irresponsables y a una pérdida de la confianza pública. Las nuevas tendencias tecnológicas, que en su concepción suelen caracterizarse por ser disruptivas, exigen de parte de cada entidad una evaluación objetiva y técnica que permitan gestionar los diversos riesgos emergentes de cada proceso y producto financiero, contando necesariamente con el acompañamiento de los reguladores y supervisores.

Reconociendo la amenaza de los riesgos cibernéticos y la importancia de mejorar la resiliencia de las instituciones financieras, las autoridades de todo el mundo están tomando medidas regulatorias y de supervisión diseñadas para facilitar tanto la mitigación del riesgo cibernético por parte de las instituciones financieras como su respuesta efectiva y recuperación a los ciberataques.

En Colombia, las entidades financieras han avanzado en la gestión de los riesgos asociados a la seguridad de la información y la ciberseguridad; sin embargo, la creciente sofisticación de los delitos informáticos y el incremento en el número de ataques, exigió fortalecer los instrumentos para la gestión de los riesgos cibernéticos, como un complemento a los requerimientos realizados por la Superintendencia Financiera de Colombia para administrar el riesgo operativo, a las normas de control interno para la gestión de la tecnología y a las medidas para preservar la integridad, confidencialidad y disponibilidad de la información en la realización de operaciones financieras.

Es por ello que el 5 de junio de 2018, la Superintendencia expidió la circular externa 007, que establece los requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad, cuya implementación finalizó en diciembre de 2019. Esta circular ayuda a consolidar el modelo nacional de Ciberseguridad y Ciberdefensa liderado por el Gobierno nacional desde 2011, contemplado en el Documento CONPES 3701, en el cual se fijaron los lineamientos de la política en ciberseguridad para desarrollar una estrategia nacional que contrarreste el incremento

de amenazas informáticas que pudieran afectar significativamente al país. Adicionalmente, también apoya el Documento CONPES 3854 de 2016 que definió la Política Nacional de Seguridad Digital fijando lineamientos en materia de gobernanza, gestión de riesgos, educación, regulación, cooperación internacional y nacional, investigación y desarrollo, e innovación.

La Superintendencia es consciente que la regulación debería ser lo más estable posible, predecible, transparente, así como ágil y lo suficientemente adaptable para permanecer relevante frente a los cambios vertiginosos en las tecnologías y en la manera cómo ellas se utilizan, con el objetivo de construir confianza entre inversores, entidades y consumidores financieros. Considerando estos principios se expidió la circular.

Conclusión

Lo plasmado en este artículo nos invita a reflexionar acerca de un nuevo enfoque en la gestión de los riesgos en materia de seguridad de la información y ciberseguridad que podría tener un alcance regional y global en la medida en que los sistemas financieros están altamente interconectados.

Por lo tanto, una prevención efectiva debe abordar el problema de manera transversal, permitiendo a las entidades de regulación y supervisión, organismos de seguridad nacional y organizaciones internacionales, nutrirse de la experiencia de sus pares en otras latitudes, intercambiando conocimiento y formación de personal, compartiendo experiencias, legislación, estrategias y políticas cibernéticas, así como procedimientos de gestión de incidentes, fortaleciendo al sistema financiero global ante un riesgo de carácter sistémico.

La gestión de la ciberseguridad es una actividad compleja, continua, dinámica, exigente en recursos y que requiere de la cooperación nacional e internacional de las autoridades, el sector financiero, la ciudadanía, la academia y los organismos multilaterales que facilitan la articulación de estos esfuerzos.

Es por esto que estamos convencidos que el estudio realizado por la Organización de Estados Americanos (OEA) y la Asociación Bancaria y de Entidades Financieras de Colombia ASOBANCARIA contribuirá al desarrollo y madurez de la gestión de la ciberseguridad en el país y la región. Finalmente, extendemos un agradecimiento a todos aquellos quienes hicieron posible la realización de este documento.

Mauricio Botero Wolff

Presidente del Comité de Ciberseguridad y Prevención del Fraude de ASOBANCARIA

El mundo de los negocios ha tenido una evolución bastante acelerada en los últimos años generada a su vez por múltiples factores, dos de ellos transversales, la tecnología y la información. Una tecnología cada vez más económica, potente y abierta.

Hoy la tecnología es mucho más económica. Hasta hace unos pocos años las inversiones iniciales de los negocios se constituían en una barrera de entrada, pero ahora con la nube, dichas inversiones han disminuido y los conceptos de pago por uso en infraestructura y en software, hacen que se puedan probar sus nuevas ideas de negocio a costos muy razonables que no inhiben el emprendimiento. Por eso tiene mucho sentido que sin importar si las empresas son nuevas o no, se considere probar nuevos conceptos en la nube, lo que facilita el proceso de desarrollo, las salidas a producción, los cambios incrementales, entre otros, que nos muestran que cada vez más las entidades emprenden programas de migración a la nube. En el mundo hay ejemplos ya de entidades financieras corriendo 100% en la nube.

El incremento en potencia y capacidad de procesamiento de la tecnología es innegable y para esto hay múltiples ejemplos que comparan la capacidad de los dispositivos actuales frente a dispositivos similares de años atrás, hoy un disco duro externo o una memoria USB tiene mucha más capacidad que los computadores antiguos, un computador portátil tiene más capacidad que los servidores del pasado, y los servidores son mucho más potentes que los centros de datos de hace unas décadas. Es increíble cómo se ha avanzado tan rápido en tan poco tiempo, pero más increíble aun lo que viene, la computación cuántica. Con este tipo de computación podrá hacerse lo que aún no nos imaginamos. Será tal la potencia computacional disponible que la lógica y los algoritmos serán retados y replanteados.

El concepto de tecnología abierta ha sido clave en esta evolución y la forma como se empieza a repensar la arquitectura de infraestructura y aplicativa a partir de las posibilidades es impresionante en una dinámica en la que empiezan a tomar fuerza conceptos como servicios, APIs software de código abierto, Internet de las cosas, entre otros, que replantean la forma como se piensan y construyen las soluciones.

Y ¿por qué este replanteamiento?, porque ya las entidades no deben hacer todo solas y pueden usar servicios o APIs de terceros, siendo un ejemplo de esto el cómo muchos sitios web consumen API de autenticación de otras entidades que pueden cobrar o no para permitir dicho consumo. Una buena autenticación es costosa de implementar, toma tiempo y se le entrega al cliente la responsabilidad de administrar otro usuario y contraseña. Al consumir una API de autenticación se evita una inversión inicial, se paga por servicio y el cliente no tiene que memorizar nuevas credenciales. Otro ejemplo de cómo la tecnología abierta es clave en esta transición, es el Internet de las cosas, que nos genera un sinnúmero de beneficios al conectar diferentes dispositivos que hacen parte de la cotidianidad de las personas (auto, teléfono móvil, electrodomésticos, vivienda, etc).

En línea con la transformación digital de las empresas vale resaltar como la información se ha convertido en uno de los activos más importantes de las entidades. El aprovechamiento de esta con conceptos como big data, analítica, machine learning e inteligencia artificial se empiezan a convertir en elementos disruptivos de negocio. Las entidades han empezado a entender que en una dinámica donde la información es amplia, quien la aproveche de mejor manera podrá llegar con mejores propuestas de valor para sus clientes a través de, por ejemplo, iniciativas de microsegmentación que se ajusten a los gustos, hábitos de consumo, contexto laboral, entre otros.

Los riesgos

Sin embargo, todas estas oportunidades que nacen del buen uso de la tecnología y la información tienen implícito algunos riesgos de ciberseguridad para las compañías que empiezan a hacer uso frecuente de ellas. De hecho, el Foro Económico Mundial en su reporte anual de riesgos globales incluyó a los ciberataques y a los incidentes de pérdida o robo de información como uno de los principales riesgos para las empresas a nivel global. El mundo se ha empezado a familiarizar con titulares en los medios de comunicación sobre este tipo de ataques que se han materializado en entidades globales de mucha trayectoria y alta reputación, lo que reafirma que ninguna entidad, en ninguna industria, está exenta de ciberataques, como lo dice John Chambers, CEO de Cisco: “Existen dos tipos de empresas: las que han sido hackeadas y las que aún no saben que fueron hackeadas”.

Con este panorama y considerando el impacto que este tipo de eventos puede tener en la sostenibilidad y perdurabilidad de las entidades, se vuelve imperativo definir la ciberseguridad como una prioridad para las empresas y para los reguladores a nivel global. De hecho, la regulación local e internacional ha tenido un avance significativo en este sentido demandando de las entidades esfuerzos importantes para alcanzar los estándares esperados en modelos, políticas, herramientas, etc.

Desde el punto de vista empresarial se deberían tener en cuenta estas recomendaciones:

1. Conocer la situación actual

a. Suena básico pero la ciberseguridad y la seguridad de la información están inmersas en múltiples procesos de las entidades. Pasa por una revisión técnica y de procesos, no sólo a nivel general de red y conectividad, sino también a un nivel más granular de infraestructura (plataformas, bases de datos, etc.) y de aplicaciones.

b. Hay que revisar que los estándares de desarrollo y pruebas de aplicaciones tengan modelos de alta automatización que incluyan las pruebas de seguridad o prácticas de desarrollo seguro.

c. Cada vez las entidades se apoyan más en proveedores para el desarrollo de sus funciones, pero hay que hacerse las siguientes preguntas, cómo se conectan con cada uno, qué información comparten y cuál es el estándar de seguridad de estos proveedores.

d. Qué controles de ciberseguridad se tienen (Firewall, IPs, PGP, EPP, EDR, etc) y cómo están siendo gestionados, además si se tiene una visión integral y coordinada entre los mismos, y si pasa por la revisión de la arquitectura de seguridad.

e. Definir el inventario de activos de información con su respectiva valoración y seguridad asociada, de acuerdo con la valoración.

2. Definir una estrategia y apetito de riesgo

a. Todas las entidades son diferentes y cada una debe definir cuál es su aspiración, sus focos de trabajo y temas transversales.

b. No puede ser una estrategia que derive sólo planes de trabajo técnicos. Debe ser una estrategia incluyente que ponga a las personas en el centro de todo porque son precisamente las personas el eslabón más débil. Todo lo que se haga en cultura y pedagogía será insuficiente. No es un curso, es la sumatoria de acciones, teóricas, prácticas y vivenciales, que permita interiorizar los conceptos.

c. El trabajo coordinado con el resto de las áreas de las entidades y entre las líneas de defensa es fundamental. Se requiere del apoyo y el compromiso de todos.

d. Hay diferentes modelos o frameworks de ciberseguridad y se sugiere elegir alguno como referencia para guiar los esfuerzos de la entidad.

e. El apetito de riesgo debe retroalimentar la estrategia. Tener un modelo robusto permite darle foco a la gestión de ciberseguridad que tiene el reto de cerrar brechas a una velocidad superior a la que identifica vulnerabilidades. Por eso hay que tener el orden muy claro.

3. Plan de remediación y de transformación

a. Teniendo clara la estrategia y el apetito de riesgo debe definirse un plan de inversiones que reconozca los retos del entorno mencionados. Todos los días hay más amenazas y ataques cibernéticos, prepararse para enfrentarlos requiere inversiones significativas porque lo que está en riesgo para las entidades es mucho mayor.

b. Hay planes de acción que no dan espera y vulnerabilidades puntuales de las entidades que pueden ser aprovechadas muy fácilmente por un ciberdelincuente. Esto es lo que compone el plan de remediación, lo inmediato.

c. Se debe tener un plan de transformación de mediano y largo plazo que lleve a la entidad a donde quiere llegar. Este plan debe ser integral y con una visión muy fuerte de arquitectura que permita incrementar el nivel de protección al tiempo que ayude a optimizar la inversión.

4. Compromiso de todos

a. La ciberseguridad debe ser una prioridad de todos. Desde la Junta Directiva de las entidades hasta las diferentes áreas de la organización debe existir consciencia sobre el reto. Todos deben ayudar.

b. Es recomendable tener un foro o comité periódico con participación de diversas áreas relacionadas con el tema, donde no sólo se haga seguimiento a los planes de trabajo, sino que también sea un foro donde se tomen decisiones para apoyar la gestión de la ciberseguridad. Muchas de estas decisiones son difíciles de tomar, pero con una mirada interdisciplinaria se pueden considerar los riesgos que la entidad puede y que no puede aceptar.

c. Es importante mantener informados a los empleados en los diferentes niveles sobre estas nuevas amenazas con el propósito que entiendan cada vez mejor los incidentes de ciberseguridad. Muchas veces parecen cosas inverosímiles, pero es crítico que todos entiendan que es mucho más real de lo que muchos piensan.

d. Los proveedores y terceros con quienes interactúan las entidades hacen parte de sus ecosistemas de negocio. Para que una entidad pueda subir sus propios estándares de seguridad, requiere que sus proveedores también lo hagan.

5. Pruebe y reinicie el ciclo

a. La única forma de saber que se está haciendo bien la tarea en ciberseguridad es poner a prueba de manera continua a la entidad a través de equipos internos, con herramientas, con ayuda de terceros y de las diferentes líneas de defensa.

b. El universo a probar es muy amplio y por eso se debe priorizar, pero al mismo tiempo hay que diversificar las pruebas. Es muy común probar posibles vulnerabilidades en los procesos de autenticación, por ejemplo, pero no es tan común probar vulnerabilidades en los sistemas de tecnología operacional. En la evolución de la industria convergen los sistemas de tecnología de la información con los de tecnología operacional.

c. El resultado de un modelo de pruebas continuo es muy enriquecedor para que la entidad vuelva a recorrer el círculo virtuoso de conocimiento de la situación actual, definición de estrategia y apetito de riesgo, planes de remediación y transformación, y ejecutado con el compromiso de todos.

La ciberseguridad no puede ser un inhibidor de la transformación del negocio a través de la tecnología. Todo lo contrario, debe ser un habilitador. Pero esto requiere que se gestionen adecuadamente los riesgos y esto se da cuando se llevan a cabo cada uno de los puntos arriba mencionados. Es un nuevo normal y como tal debe ser interiorizado por todos.

Estado de la Ciberseguridad en el Sistema Financiero Colombiano

4.

Ciberseguridad en las Entidades del Sistema Financiero Colombiano

El Sistema Financiero Colombiano está integrado por: i) autoridades y organismos reguladores del sistema financiero, y ii) entidades financieras de diversos sectores que brindan atención a los diferentes segmentos de la población.

Por una parte, las autoridades y organismos reguladores del Sistema Financiero Colombiano son instituciones públicas que velan por la estabilidad y el desarrollo del sistema financiero y cumplen funciones de autorización, regulación, supervisión y sanción, entre otras, sobre los diversos sectores y entidades /instituciones que integran dicho sistema, así como sobre aquellas personas físicas y morales que realicen actividades previstas en las leyes relativas al mismo.

Gráfica 1.

Autoridades del Sistema Financiero Colombiano

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

A continuación, las autoridades y organismos que actualmente conforman dicho sistema en Colombia:

- Autoregulador del Mercado de Valores: es una organización de carácter privado, sin ánimo de lucro, que regula, monitorea, disciplina y profesionaliza el mercado de valores colombiano. Trabaja junto con los intermediarios del mercado de valores y divisas, y en coordinación con las autoridades estatales, para promover las buenas prácticas, proteger a los inversionistas y darle transparencia al mercado. (AMV, 2020)

- Banco de la República -BANREP-: es un órgano del Estado de naturaleza única, con autonomía administrativa, patrimonial y técnica, que ejerce las funciones de banca central. Según la Constitución, el principal objetivo de la política monetaria es preservar la capacidad adquisitiva de la moneda, en coordinación con la política económica general, entendida como aquella que propende por estabilizar el producto y el empleo en sus niveles sostenibles de largo plazo. En ejercicio de esta función adopta las medidas de política que considere necesarias para regular la liquidez de la economía y facilitar el normal funcionamiento del sistema de pagos, velando por la estabilidad del valor de la moneda. (Banco de la República, 2020)

- Ministerio de Hacienda y Crédito Público -MINHACIENDA-: coordina la política macroeconómica; define, formula y ejecuta la política fiscal del país; incide en los sectores económicos, gubernamentales y políticos; y gestiona los recursos públicos de la Nación, desde la perspectiva presupuestal y financiera, mediante actuaciones transparentes, personal competente y procesos eficientes, con el fin de propiciar: Las condiciones para el crecimiento económico sostenible, y la estabilidad y solidez de la economía y del sistema financiero; en pro del fortalecimiento de las instituciones, el apoyo a la descentralización y el bienestar social de los colombianos. (MINHACIENDA, 2020)

- Superintendencia Financiera de Colombia -SFC-: es un organismo técnico adscrito al Ministerio de Hacienda y Crédito Público, con personería jurídica, autonomía administrativa y financiera y patrimonio propio, que ejerce funciones de inspección, vigilancia y control sobre las personas que realicen actividades financiera, bursátil, aseguradora y cualquier otra relacionada con el manejo, aprovechamiento o inversión de recursos captados del público y tiene por objetivo supervisar el sistema financiero colombiano con el fin de preservar su estabilidad, seguridad y confianza, así como promover, organizar y desarrollar el mercado de valores colombiano y la protección de los inversionistas, ahorradores y asegurados. (SUPERFINANCIERA, 2020a)

- Unidad de Proyección Normativa y Estudios de Regulación Financiera -URF-: es un organismo técnico adscrito al Ministerio de Hacienda y Crédito Público, encargado de proponer normas con el fin de contar con un sistema financiero estable e inclusivo. Tiene como misión la preparación de la normativa para el ejercicio de la facultad de reglamentación en materia cambiaria, monetaria y crediticia y de las competencias de regulación e intervención en las actividades financiera, bursátil, aseguradora y cualquiera otra relacionada con el manejo, aprovechamiento e inversión de los recursos captados del público, para su posterior expedición por el Gobierno Nacional, dentro del marco de política fijado por el Ministerio de Hacienda y Crédito Público y sin perjuicio de las atribuciones de la Junta Directiva del Banco de la República. (URF, 2020)

Por otra parte, las entidades financieras captan, administran y canalizan los recursos financieros y dirigen el ahorro y la inversión de los ciudadanos en Colombia en diversos sectores. El sistema financiero colombiano se encuentra conformado por las siguientes entidades financieras (artículo 1 Estatuto Orgánico del Sistema Financiero -ESOF-) (SUPERFINANCIERA, 2020b)

- **Establecimientos de Crédito:** Instituciones financieras cuya función principal consiste en captar en moneda legal recursos del público, ya sea en depósitos a la vista (cuentas de ahorro, corriente) o a término (CDT y CDAT´S), para colocarlos nuevamente a través de préstamos, descuentos, anticipos u otras operaciones activas de crédito. Son establecimientos de crédito:

  - Establecimientos Bancarios: Tienen por función principal la captación de recursos en cuenta corriente bancaria, así como también la captación de otros depósitos a la vista o a término, con el objeto primordial de realizar operaciones activas de crédito.

  - Corporaciones Financieras: Tienen por objeto la movilización de recursos y la asignación de capital para promover la creación, reorganización, fusión, transformación y expansión de cualquier tipo de empresas, así como para participar en su capital, promover la participación de terceros, otorgarles financiación y ofrecer servicios financieros que contribuyan a su desarrollo.

  - Compañías de Financiamiento: Su función principal es la de captar recursos del público con el propósito de financiar la comercialización de bienes y servicios y realizar operaciones de arrendamiento financiero o leasing.

  - Cooperativas Financieras: Adelantan actividad financiera en los términos de la Ley que los regula.

• **Sociedades de Servicios Financieros:** Sociedades que tienen por función la realización de las operaciones previstas en el régimen legal que regula su actividad, si bien captan recursos del ahorro público, por la naturaleza de su actividad se consideran como instituciones que prestan servicios complementarios y conexos con la actividad financiera. Son sociedades de servicios financieros:

- Sociedades Fiduciarias: aunque no están definidas en la ley, este tipo de sociedades reciben uno o más de los bienes de una persona natural o jurídica (llamado fideicomitente) para cumplir con la finalidad determinada en el respectivo contrato; su régimen de operaciones está establecido en el artículo 29 del EOSF.

- Sociedades Administradoras de Pensiones y Cesantías: Sociedades que tienen como objeto exclusivo la administración de los fondos de cesantías y los de pensiones autorizados por la ley. Artículo 30 del EOSF.

- Almacenes Generales de Depósito: Su objeto es el depósito, la conservación y custodia, el manejo y la distribución, la compra y venta por cuenta de sus clientes, de acuerdo a lo dispuesto por el artículo 33 del EOSF.

- Sociedades de intermediación cambiaria y de servicios financieros especiales, abreviatura: SICA Y SFE: Son sociedades de intermediación cambiaria y de servicios financieros especiales, las personas jurídicas organizadas con arreglo a las disposiciones del Decreto 2555 de 2010, cuyo objeto social sea realizar las operaciones de pagos, recaudos, giros y transferencias nacionales en moneda nacional, así como actuar como corresponsales no bancarios, de conformidad con lo señalado en el artículo 34 de la Ley 1328 de 2009. En su condición de intermediario del mercado cambiario, las citadas sociedades podrán realizar las operaciones autorizadas bajo el régimen cambiario que para el efecto determine la Junta Directiva del Banco de la República. Las sociedades a las que se hace alusión con anterioridad deberán anunciarse por su razón social acompañada de la denominación completa “sociedades de intermediación cambiaria y de servicios financieros especiales” o de la abreviatura SICA y SFE.

• **Sociedades de Capitalización:** Son instituciones financieras cuyo objeto consiste en estimular el ahorro mediante la constitución, en cualquier forma, de capitales determinados, a cambio de desembolsos únicos o periódicos, con posibilidad o sin ella de reembolsos anticipados por medio de sorteos.

• **Entidades Aseguradoras:** Su objeto es la realización de operaciones de seguro, bajo las modalidades y los ramos facultados expresamente. Son entidades aseguradoras:

- Compañías de Seguros

- Compañías de Reaseguros

- Cooperativas de Seguros: Estos organismos deben ser especializados en la prestación de este tipo de servicios y cumplen la actividad aseguradora principalmente en interés de sus propios asociados y de la comunidad vinculada a ellos. Numeral 5 del artículo 38 del EOSF.

- **Intermediarios de Seguros y Reaseguros:** Son intermediarios de seguros:

  - Corredores de Seguros: De acuerdo con lo dispuesto por el artículo 1348 del Código del Comercio son las empresas constituidas como sociedades comerciales cuyo objeto social sea exclusivamente ofrecer seguros, promover su celebración y obtener su renovación, a título de intermediarios entre el asegurado y el asegurador.

  - Agencias de Seguros: representan a una o varias compañías de seguros en un determinado territorio. Debe resaltarse que este tipo de intermediarios no están sujetos a la vigilancia de la Superintendencia Financiera de acuerdo a lo dispuesto en el parágrafo quinto del artículo 75 de la ley 964 de 2005.

  - Agentes de Seguros: son las personas naturales que promuevan la celebración de contratos de seguro y capitalización y la renovación de los mismos en relación con una o varias compañías de seguros o sociedades de capitalización. No están sujetos a la inspección, control y vigilancia de la Superintendencia Financiera.

  - Corredores de Reaseguros: Estas sociedades deberán constituirse bajo la forma de sociedades comerciales y tendrán como objeto exclusivo el ofrecimiento del contrato de reaseguro y la promoción para su celebración o renovación a título de intermediario entre las entidades aseguradoras y las reaseguradoras, de acuerdo con lo dispuesto en el artículo 44 del Estatuto Orgánico del Sistema Financiero. Estas sociedades se encuentran sujetas a la vigilancia, inspección y control de la Superintendencia Financiera.

Gráfica 2.
Sectores del Sistema Financiero Colombiano

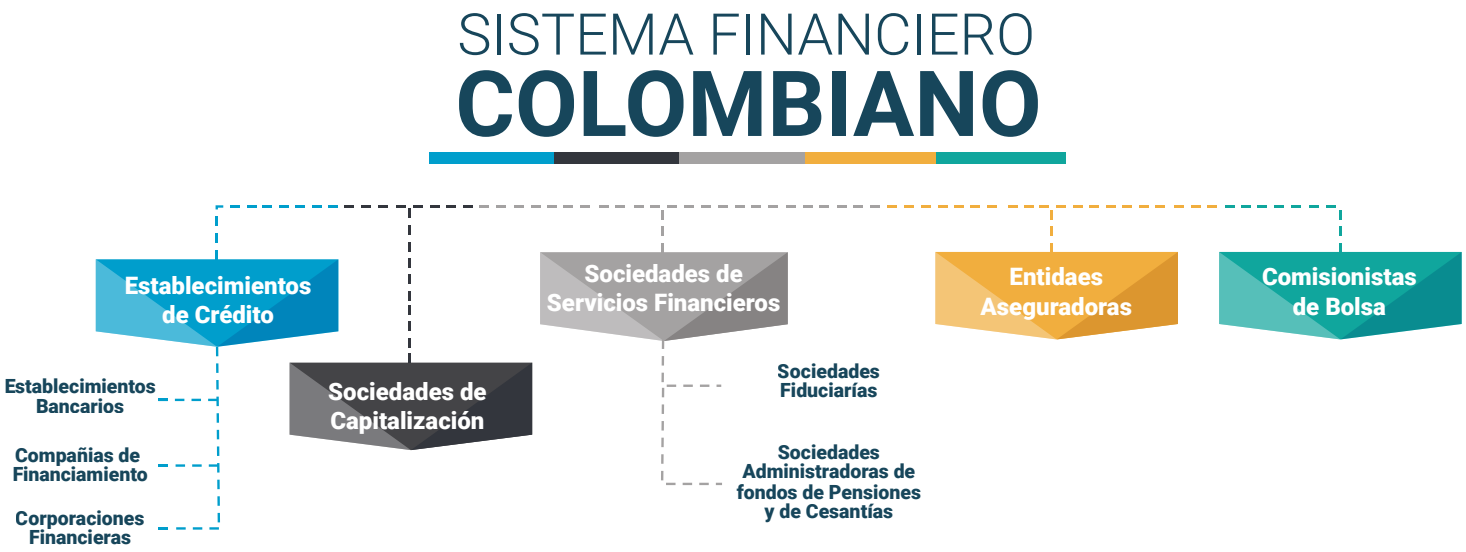
Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

A continuación, las entidades financieras del Sistema Financiero Colombiano consideradas para el presente reporte:

- Establecimientos Bancarios (sector Establecimiento de Crédito)
- Compañías de Financiamiento (sector Establecimiento de Crédito)
- Corporaciones Financieras (sector Establecimiento de Crédito)
- Sociedades Fiduciarias (sector Sociedades de Servicios Financieros)
- Sociedades Administradoras de Pensiones y Cesantías (sector Sociedades de Servicios Financieros)
- Sociedades de Capitalización (sector Sociedades de Capitalización)
- Compañías de Seguros de Vida y de Seguros Generales (sector Entidades Aseguradoras)
- Comisionistas de Bolsa (sector Intermediarios de Valores)

Gráfica 3.

Muestra de las entidades financieras del Sistema Financiero Colombiano para el desarrollo del reporte



Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

4.1. Caracterización de la entidad financiera

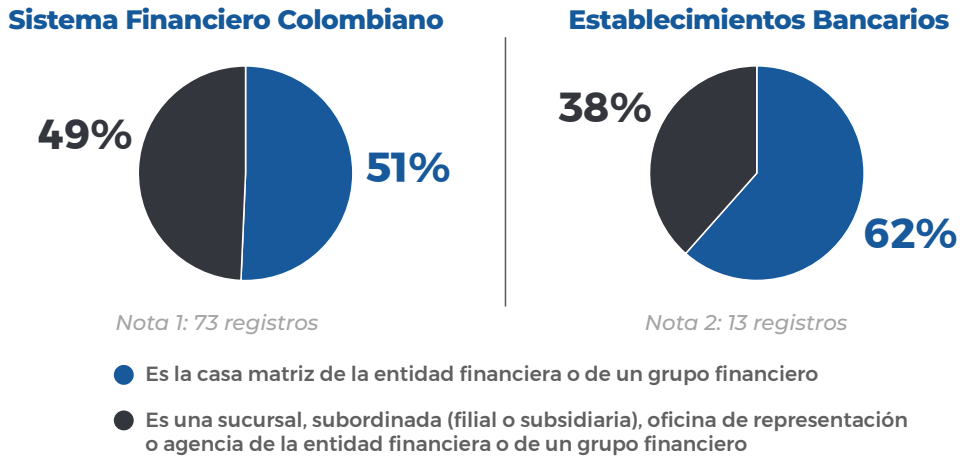
De un total de 92 respuestas obtenidas durante el periodo de publicación del instrumento de recolección de información (meses comprendidos durante el cuarto trimestre del año 2019), se estableció una base de datos con registros de 73 entidades financieras con cubrimiento en los treinta y dos (32) departamentos de Colombia y en el Distrito Capital. Se estima que la muestra de entidades financieras a partir de las cuales se presentan los resultados de este estudio alcanza activos a 31 de diciembre de 2018 cercanos a los COP $483,8 billones de pesos (aproximadamente un 65% del total de activos de los sectores analizados) y acumulan utilidades netas por COP $12,33 billones de pesos (aproximadamente un 83% del total de utilidades de los sectores analizados).

Las preguntas del instrumento estuvieron orientadas a ser respondidas por la entidad financiera a la cual el funcionario que respondió pertenecía a nivel local (es decir, en la entidad que operaba en el país), aun cuando las entidades financieras fueran: i) la casa matriz de la entidad financiera o de un grupo financiero o ii) una sucursal, subordinada (filial o subsidiaria), oficina de representación o agencia de la entidad financiera o de un grupo financiero. Para mayor claridad cada pregunta especificó de manera detallada el ámbito de aplicación de la misma.

De esta manera, el 51% de las entidades financieras del Sistema Financiero Colombiano entrevistadas corresponden a casa matriz de la entidad financiera o de un grupo financiero, mientras que el 49% corresponden a una Sucursal, subordinada (filial o subsidiaria), oficina de representación o agencia de la entidad financiera o de un grupo financiero. En particular, el 62% de los establecimientos bancarios entrevistadas corresponden a casa matriz de la entidad financiera o de un grupo financiero.

Gráfica 4.

Casa Matriz o Sucursal, subordinada (filial o subsidiaria), oficina de representación o agencia de la entidad financiera o de un grupo financiero



Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Con el fin de clasificar a las entidades financieras de Colombia por tamaño se tuvo en cuenta la metodología presentada en el estudio del Banco Interamericano de Desarrollo (BID) y la Federación Latinoamericana de Bancos (FELABAN) del año 2014 (BID & FELABAN, 2014), la cual fue utilizada también por la Organización de Estados Americanos (OEA) en el estudio "Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe" publicado en el año 2018 (Organización de Estados Americanos, 2018), en donde se considera una entidad pequeña como aquella que tiene menos de 300 empleados, o que contando con más de 300 empleados posee hasta 10 sucursales, una entidad mediana como aquella que tiene entre 301 y 5.000 empleados y entre 11 y 150 sucursales y una entidad grande como aquella que posee más de 150 sucursales.

A continuación, se presenta la clasificación de las 73 entidades financieras considerando la cantidad de empleados y de sucursales que tiene la entidad a la cual pertenecía el funcionario que diligenció el cuestionario (en el departamento en el que se encontraba). Por ejemplo, del total de la muestra se aprecia que 20 entidades financieras tienen menos de 300 empleados y poseen hasta 10 sucursales o que 6 entidades tienen más de 5.000 empleados y poseen más de 151 sucursales.

Cuadro 2.

Distribución de las entidades financieras por cantidad de empleados y de sucursales

Entidades Financieras Grandes	Cantidad de Sucursales					
	Sin sucursales	Hasta 10 sucursales	De 11 a 50 sucursales	De 51 a 150 sucursales	Más de 151 sucursales	**Total**
Hasta 300 empleados	7	20	3	1		31
Entre 301 y 999 empleados	3	11	9			23
Entre 1.000 y 4.999 empleados		2	6	3	1	12
Más de 5.000 empleados		1			6	7
Total	10	34	18	4	7	73

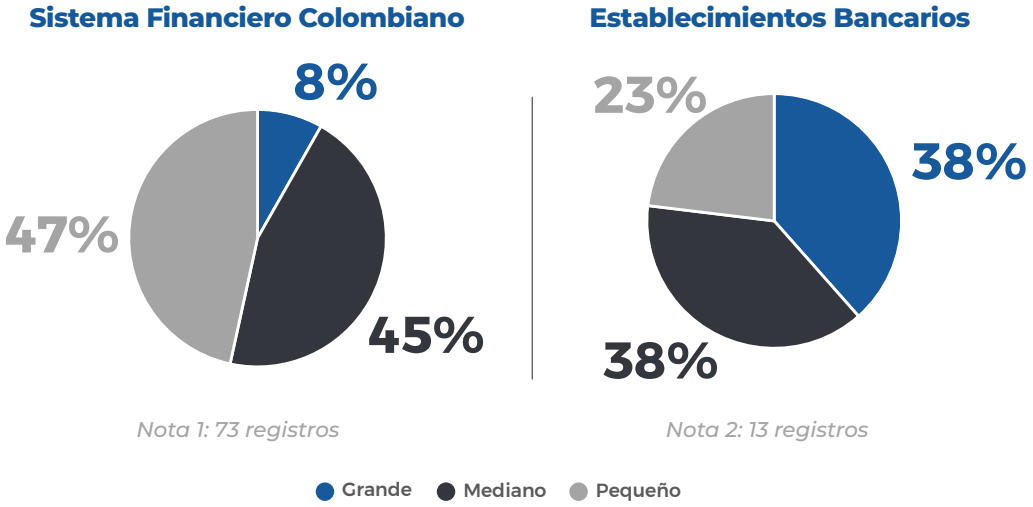
Nota: 73 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Con la información anterior, las entidades financieras del Sistema Financiero Colombiano entrevistadas se clasifican por tamaño así: el 47% de la muestra se consideran como entidades pequeñas, el 45% como entidades medianas y el 8% como entidades grandes. Esta clasificación es primordial ya que todo el análisis, las conclusiones y las recomendaciones respecto de la gestión de riesgos de seguridad digital y del impacto de los incidentes de seguridad digital en el presente capítulo tienen en cuenta el tamaño de la organización.

Gráfica 5.

Distribución de las entidades financieras por tamaño (grandes, medianas y pequeñas)



Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

De igual manera, el 27% de las entidades financieras entrevistadas son Establecimientos de Crédito (Establecimientos Bancarios, Compañías de Financiamiento y Corporaciones Financieras), el 25% son Sociedades de Servicios Financieros (Sociedades Fiduciarias y Sociedades Administradoras de Pensiones y Cesantías), el 37% son Entidades Aseguradoras y Sociedades de Capitalización y el 11% son Comisionistas de Bolsa.

Cuadro 3.

Distribución de las entidades financieras por tipo de actor

Sector	Tipo de entidad	Grande	Mediano	Pequeño	Total	%
Establecimiento de Crédito	Establecimientos Bancarios	5	5	3	13	18%
	Compañías de Financiamiento		3	2	5	7%
	Corporaciones Financieras			2	2	3%
Sociedades de Servicios Financieros	Sociedades Fiduciarias		5	9	14	19%
	Sociedades Administradoras de Pensiones y Cesantías		4		4	5%
Entidades Aseguradoras y Sociedades de Capitalización	Compañías de Seguros de Vida, de Seguros Generales y Sociedades de Capitalización	1	13	13	27	37%
Comisionistas de Bolsa	Comisionistas de Bolsa		3	5	8	11%
SISTEMA FINANCIERO COLOMBIANO		6	33	34	73	100%

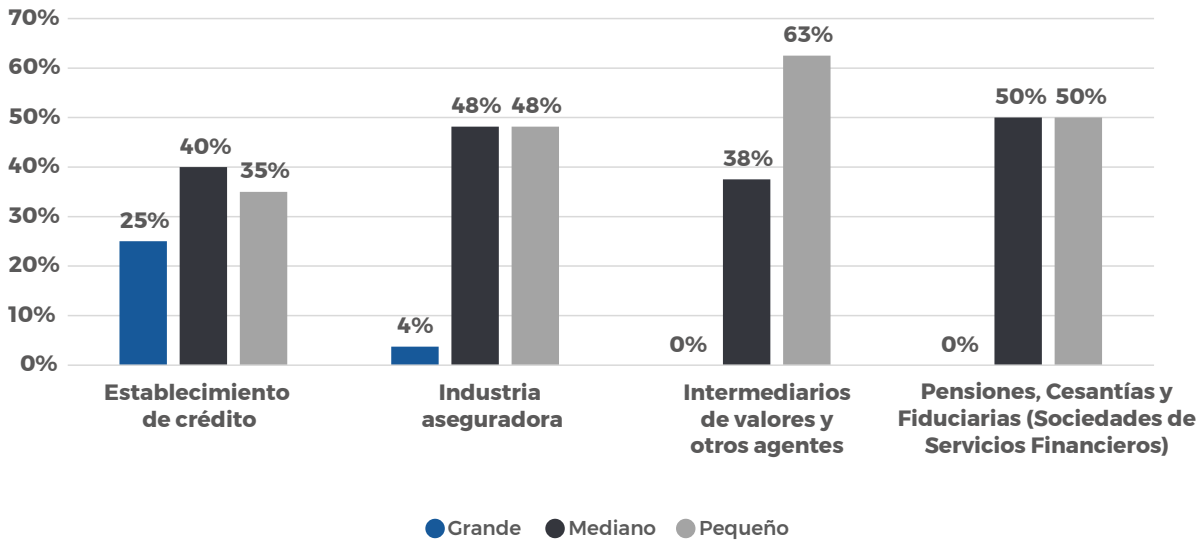
Nota: 73 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Al analizar por tamaño de entidad y por tipo de sector se aprecia que existe representatividad para las tres (3) categorías de tamaño (grande, mediana y pequeña) para los Establecimiento de Crédito y las Sociedades de Servicios Financieros. Por su parte, existe representatividad de entidad mediana y pequeña para las Entidades Aseguradoras y Sociedades de Capitalización, así como para las Comisionistas de Bolsa.

Gráfica 6.

Tipo de actor por sector en la muestra del Sistema Financiero Colombiano



Nota: 73 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Del total de la muestra, se aprecia que siete (7) entidades financieras encuestadas prestan sus servicios a más de 6 millones de clientes de servicios financieros en el país y otras siete (7) entidades financieras prestan sus servicios a entre 1 y 4 millones de clientes de servicios financieros.

Cuadro 4.

Clientes de servicios financieros en Colombia de la muestra

	Grande	Mediano	Pequeño	Total
Más de 6 millones clientes	3	4		7
Entre 5 millones y 6 millones clientes				0
Entre 4 millones y 5 millones clientes				0
Entre 3 millones y 4 millones clientes	1			1
Entre 2 millones y 3 millones clientes	1			1
Entre 1 millón y 2 millones clientes	1	3	1	5
Entre 800.001 y 1 millón de clientes		2		2
Entre 600.001 y 800.000 clientes				0
Entre 400.001 y 600.000 clientes		3		3
Entre 200.001 y 400.000 clientes		5	1	6
Entre 100.001 y 200.000 clientes		3		3
Entre 80.001 y 100.000 clientes		3		3
Entre 60.001 y 80.000 clientes		3		3
Entre 40.001 y 60.000 clientes			2	2
Entre 20.001 y 40.000 clientes		2	3	5
Entre 10.001 y 20.000 clientes		2	2	4
Entre 8.001 y 10.000 clientes			2	2
Entre 6.001 y 8.000 clientes			3	3
Entre 4.001 y 6.000 clientes		1	3	4
Entre 2.001 y 4.000 clientes		1	5	6
Entre 1.001 y 2.000 clientes			2	2
Hasta 1.000 clientes		1	10	11
SISTEMA FINANCIERO COLOMBIANO	**6**	**33**	**34**	**73**

Nota: 73 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Teniendo en cuenta el tipo de capital de la entidad financiera al cual pertenece el empleado que respondió la encuesta, se aprecia que el 81% del total de la muestra son entidades financieras privadas (100% de capital privado), el 3% son entidades financieras públicas (100% de capital público) y el 16% son entidades financieras mixtas (compuesto por capital tanto público como privado).

Al analizar por tamaño, el 83% de las entidades financieras grandes y el 88% de las entidades financieras medianas son entidades financieras privadas. De igual manera, mientras que el 12% de las entidades

financieras medianas tienen capital compuesto por capital tanto público como privado tan sólo el 3% de las entidades financieras pequeñas tienen dicha estructura de capital mixto.

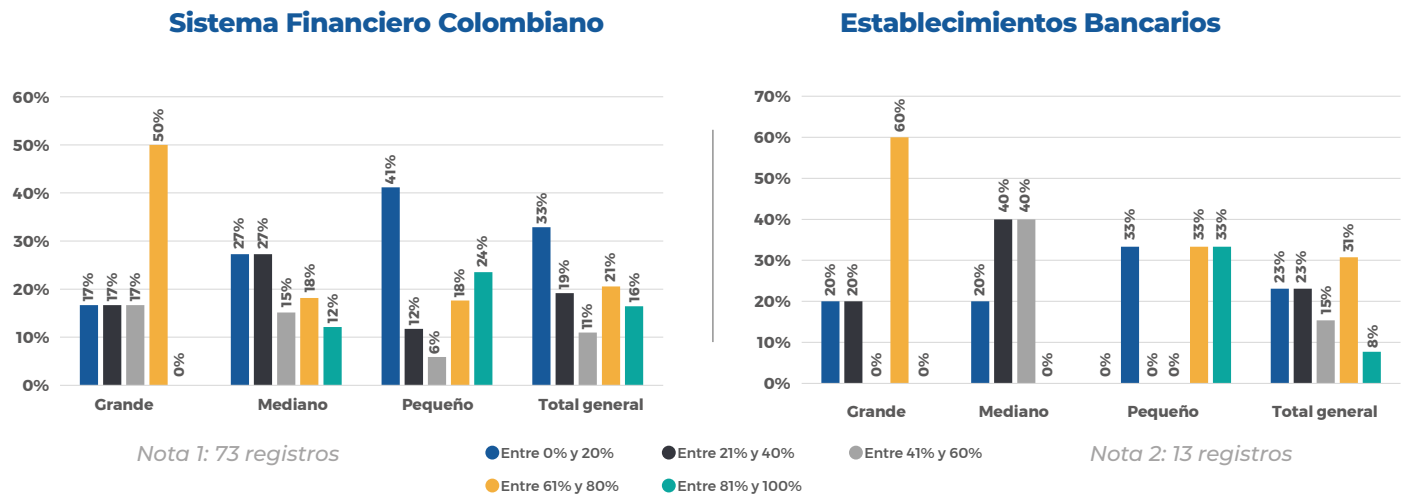
Ahora, el 60% de las entidades financieras entrevistadas tienen mayoría del capital social de origen nacional, mientras que el 25% tienen capital con mayoría de recursos de origen extranjero y el 15% tienen capital equitativo (50% nacional y 50% extranjero).

Al analizar el porcentaje de operaciones que se realizan en la entidad financiera por medio de canales transaccionales no presenciales (p.e. Internet, transacciones electrónicas, cajeros automáticos, pagos automáticos, E-trading, aplicaciones móviles y audio respuesta -IVR-) del total de operaciones de la entidad se aprecia que el 33% de las entidades financieras de la muestra tienen entre un 0% y un 20% de sus operaciones por medio de canales digitales.

Al analizar por tamaño de las entidades financieras, se aprecia por ejemplo que el 27% de las entidades medianas y el 41% de las pequeñas realizan entre un 0% y 20% de sus operaciones por medio de canales digitales mientras que el 17% de las entidades grandes realizan operaciones en dicho rango. Se destaca el hecho de que en las Sociedades Administradoras de Pensiones y Cesantías se alcanza un promedio de 76% de entidades financieras que realizan entre un 61% y un 80% de sus operaciones por medio de canales digitales. Asimismo, se observa que en ese mismo rango de operaciones el 31% de Establecimientos Bancarios realiza sus actividades por medio de canales digitales[14], lo cual duplica el promedio registrado por las entidades bancarias de América Latina y el Caribe que está en el 16% (Organización de Estados Americanos, 2018).

Gráfica 7.

Porcentaje de operaciones que se realizaron por medio de canales digitales



Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

4.2. Gestión de riesgos de seguridad digital

Como parte del estudio a las entidades financieras en Colombia, se realizaron una serie de preguntas con respecto a la gestión de riesgo de seguridad digital. Estas preguntas se formularon con el propósito de evaluar los principales aspectos y asuntos relacionados con los siguientes temas:

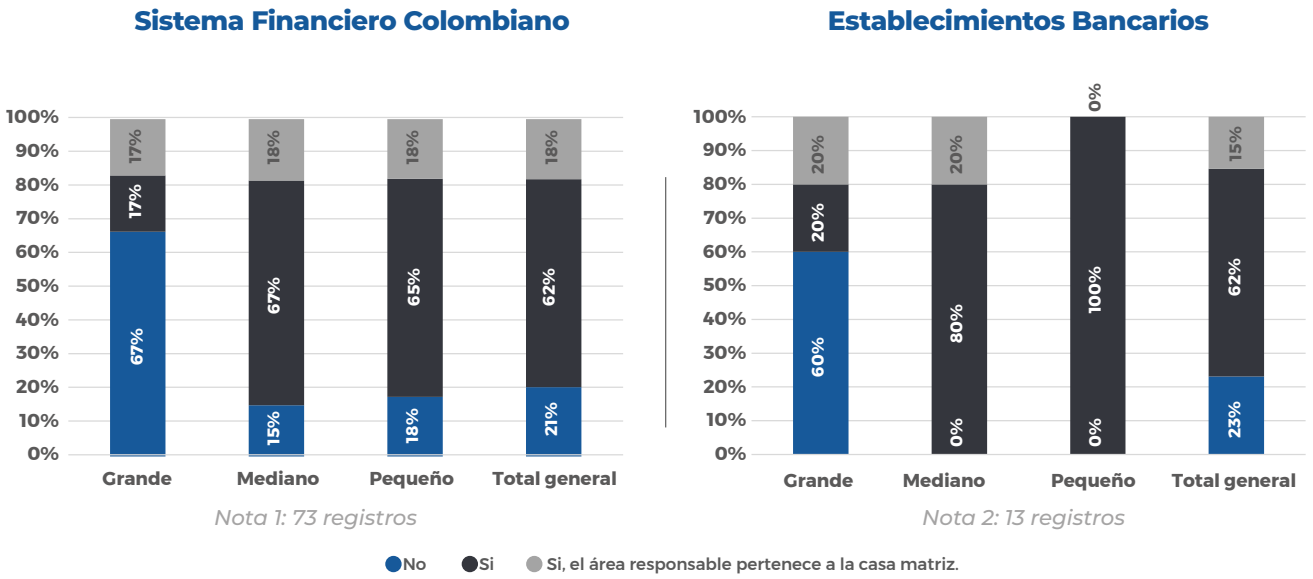
- Preparación y gobierno
- Detección y análisis de eventos de seguridad digital
- Gestión, respuesta y recuperación ante incidentes de seguridad digital
- Reportes de incidentes de seguridad digital
- Capacitación y concientización

4.2.1. Preparación y gobernanza

La mayoría de las entidades financieras entrevistadas (62%) mencionan que en su organización existe una única área responsable de la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude ocurridos a través de medios digitales. Vale la pena destacar que a medida que crece la entidad financiera aumentan las áreas responsables de la seguridad digital, ya que el 65% de las entidades pequeñas tienen una única área versus el 17% de las entidades grandes.

Gráfica 8.

Área única responsable de la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude ocurridos a través de medios digitales en la entidad financiera



Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Estas diferencias se acentúan aún más en las Corporaciones financieras, donde se evidencia que en el 100% de dichas entidades financieras existe una única área responsable por la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude ocurridos a través de medios digitales[15]. Por su parte, en el 62% de los Establecimientos Bancarios de Colombia existe una única área responsable mientras que en la región de América Latina y el Caribe las entidades bancarias registran un promedio del 74% (Organización de Estados Americanos, 2018).

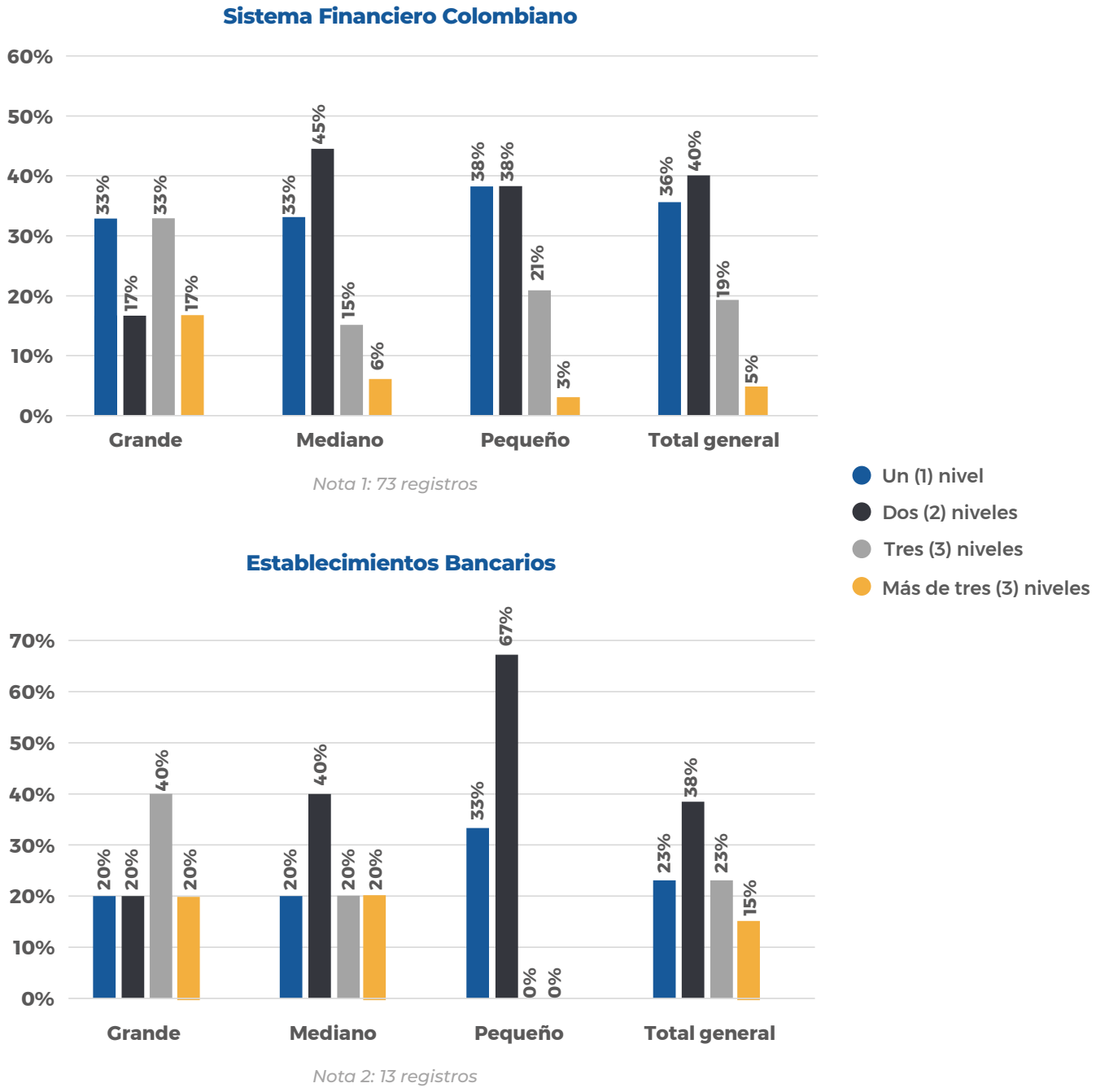
Entendiendo que el CEO (Chief Executive Officer) de la entidad financiera se consideraría la cabeza de la entidad y a partir de los resultados obtenidos, se concluye que los niveles jerárquicos que existen entre el CEO y el máximo responsable de la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude ocurridos a través de medios digitales dependen también del tamaño de la organización en el país. Por ejemplo, en el 38% de las entidades pequeñas el máximo responsable reporta directamente al CEO, es decir, está a un (1) nivel, mientras que en el 33% de las entidades grandes ocurre dicha situación. Asimismo, en otro33% de las entidades grandes existen tres (3) niveles entre el CEO y el máximo responsable de la seguridad digital.

Al analizar la muestra completa, se aprecia que en el 36% de las entidades financieras existe un (1) nivel jerárquico y en el 40% existen dos (2) niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital[16].

Al comparar los Establecimientos Bancarios de Colombia con el promedio de la región de América Latina y el Caribe, se observa que en dicho sector, en el 38% de bancos el máximo responsable está a dos (2) niveles del CEO, mientras que en la región se registra un promedio de 41% de bancos donde ocurre dicha situación (Organización de Estados Americanos, 2018).

Gráfica 9.

Número de niveles jerárquicos que hay entre el CEO y el máximo responsable de la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude ocurridos a través de medios digitales



Nota 1: 73 registros

Nota 2: 13 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

En el Sistema Financiero Colombiano, la denominación más común del cargo que tiene el máximo responsable de la seguridad de la información (incluyendo ciberseguridad) es Director/Gerente/Jefe de Seguridad de la Información (ISM). Por su parte, la denominación Oficial de Seguridad de la Información (ISO) también es común para las entidades medianas (24%) como para las pequeñas (21%). En el sector bancario de Colombia, así como en el sector bancario de la región América Latina y el Caribe, la denominación más común del cargo que tiene el máximo responsable de la seguridad de la información (incluyendo ciberseguridad) también es Oficial de Seguridad de la Información (ISO) (Organización de Estados Americanos, 2018).

Un aspecto importante sobre la preparación y gobernanza en torno a la seguridad digital es la tercerización de actividades relacionadas con la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude ocurridos a través de medios digitales por parte de la organización. En promedio y sin distinción por tamaño de entidad financiera, los servicios más contratados con un externo de la organización son: las Pruebas de seguridad / Análisis de vulnerabilidades (78% del total), la Correlación de eventos (67% del total), el Monitoreo de la Infraestructura de Seguridad (63% del total) y los Servicios de Seguridad en la Nube (53% del total).

Se destaca que, en el sector bancario de Colombia, la tercerización de actividades de Pruebas de seguridad / Análisis de vulnerabilidades llega a un 85%, coincidiendo con lo registrado en la región América Latina y Caribe, donde en promedio y sin distinción por tamaño de banco, los servicios más contratados por parte de las entidades bancarias de la región con un externo de la organización son: las Pruebas de Seguridad (65% del total).

Con respecto del tamaño del equipo que maneja procesos asociados a la seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales, se aprecia que en promedio una entidad financiera en Colombia cuenta con un equipo conformado por trece (13) personas. No obstante, este valor varía significativamente dependiendo del tamaño y sector de la entidad, pues mientras en los Establecimientos de Crédito (Establecimientos Bancarios, Compañías de financiamiento y Corporaciones financieras) el promedio es de treinta y uno (31) profesionales, en sectores como el de Pensiones, Cesantías y Fiduciarias es tan solo de ocho (8).

Cuadro 5.

Promedio de profesionales de seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales por sector y tamaño de entidad / institución financiera en Colombia

	Grande	Mediano	Pequeño	Promedio
Establecimiento de crédito	97	13	3	31
Pensiones, Cesantías y Fiduciarias (Sociedades de Servicios Financieros)		11	4	8
Industria aseguradora	23	6	5	6
Comisionistas de Bolsa		12	5	8
SISTEMA FINANCIERO COLOMBIANO	**84**	**10**	**4**	**13**

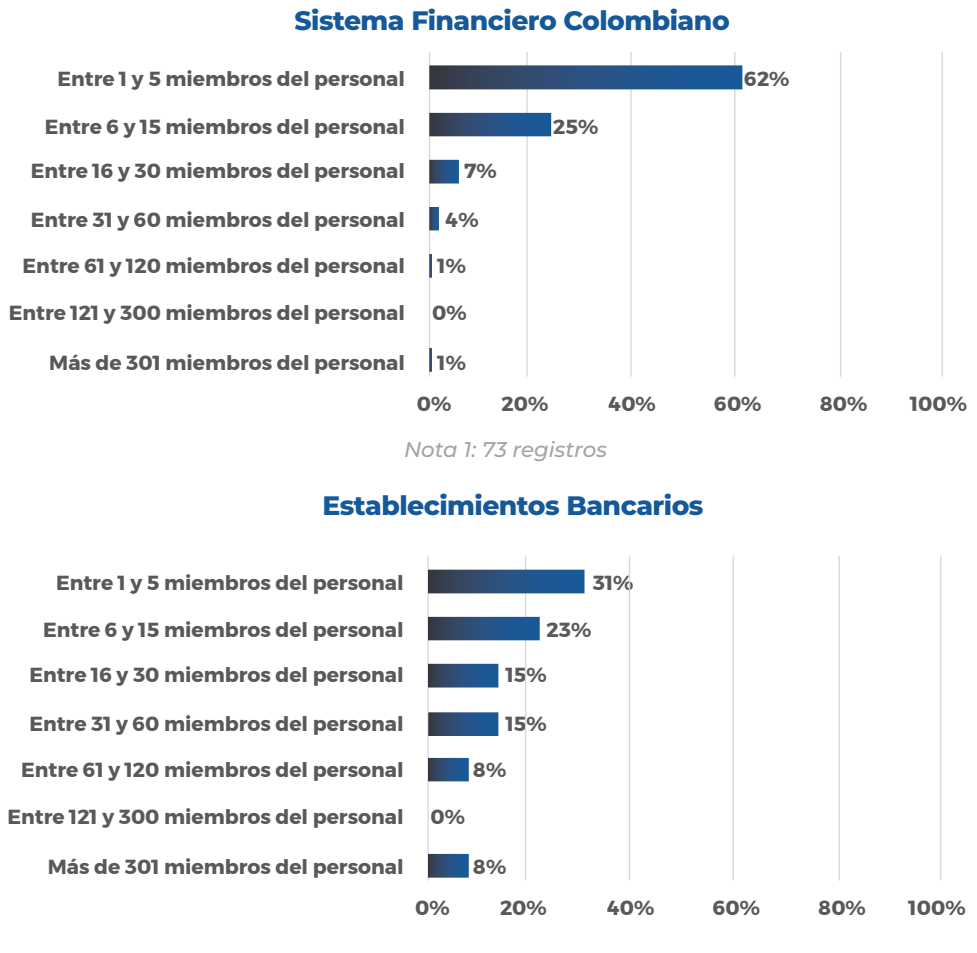
Nota: 73 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Al estimar dicho personal por tamaño de entidad financiera, se obtiene lo siguiente: un equipo de ochenta y cuatro (84) personas en promedio en una entidad grande, un equipo de diez (10) personas en promedio en una entidad mediana y un equipo de cuatro (4) personas en promedio en una entidad pequeña.

Gráfica 10.

Personas que conforman la totalidad de equipos que manejan procesos asociados a la seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales



Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Se resalta que, en el sector bancario de América Latina y el Caribe, el promedio es de cuarenta y nueve (49) personas en un banco grande, de dieciséis (16) personas en un banco mediano y de cuatro (4) personas en un banco pequeño (Organización de Estados Americanos, 2018).

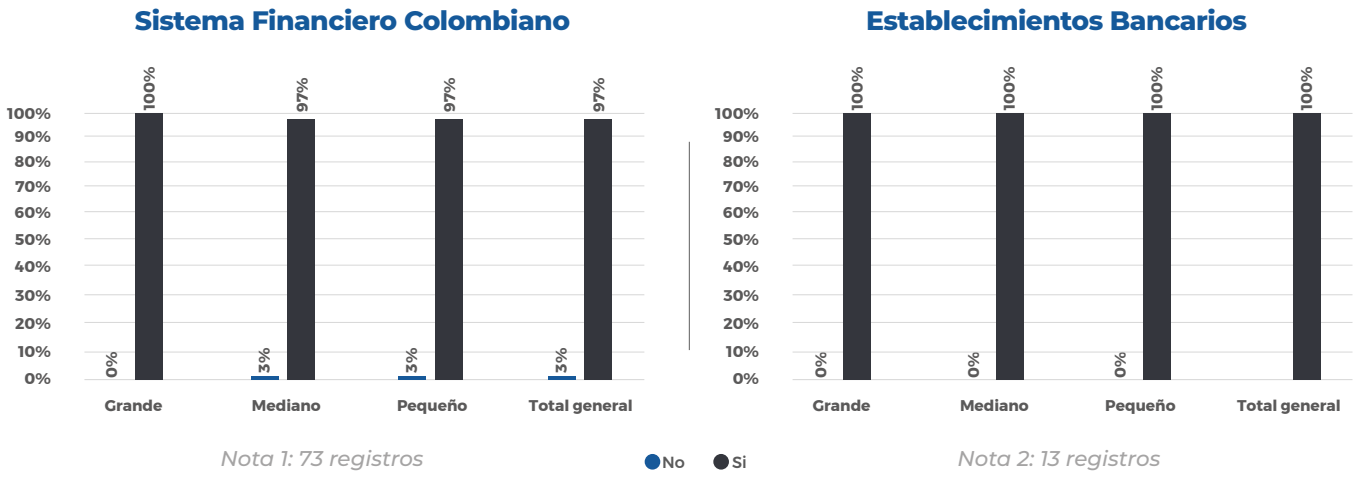
Pese a la presencia de equipos responsables de la seguridad digital en este tipo de organizaciones, el 77% de entidades financieras en Colombia considera adecuado que este equipo creciera en el corto plazo, esto teniendo en cuenta que el 82% de las entidades bancarias en la región de América Latina y el Caribe opina lo mismo (Organización de Estados Americanos, 2018). Al analizar por tamaño, se aprecia que el 50% de las entidades grandes, el 85% de las entidades medianas y el 74% de las entidades pequeñas consideran que el tamaño de los equipos debe aumentar. Así mismo se identifica que el único sector que equitativamente (50%) considera que no es adecuado que el equipo crezca en el corto plazo es el sector de Corporaciones financieras[17].

Como parte del modelo de gobierno de las entidades financieras, la Junta Directiva del 97% de las entidades financieras en el país recibe reportes periódicos acerca de indicadores, riesgos y gestión de riesgos de seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales. Se destaca que en el 100% de entidades grandes lo hace, mientras el 97% de las juntas directivas de las medianas y pequeñas reciben dicha información.

Se destaca que el 97% de Juntas Directivas de entidades financieras en Colombia reciben estos reportes de manera periódica[18] superando el promedio del sector bancario de la región América Latina y el Caribe, en el que el promedio de bancos que realizan dicha práctica es 72% (Organización de Estados Americanos, 2018).

Gráfica 11.

¿La Junta Directiva recibe reportes periódicos acerca de riesgos de seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales?



Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Según los resultados, el manejo de la gestión de la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude ocurridos a través de medios digitales en la mayoría de las entidades financieras en Colombia se prepara en el marco de un Comité de Seguridad. En las entidades financieras del país también existen otras instancias de manejo estratégico en relación con el tema como el Comité de Riesgos o el Comité Técnico o de Tecnología.

Se destaca que en el sector bancario de Colombia se utiliza mayormente el Comité de Seguridad o el Comité de Riesgos, situación similar a lo reportado por las entidades bancarias en la región América Latina y el Caribe, donde el 39% de la gestión de la seguridad de la información se prepara en el marco de dicho Comité (Organización de Estados Americanos, 2018).

Respecto al apoyo a la gestión de riesgos de seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales por parte de la alta dirección de la entidad financiera (Dirección General o Gerencia General o Presidencia), se destaca que un 71% del total de las entidades financieras lo demuestran aprobando mayor presupuesto mientras que el 63% lo hace fomentando la concientización, educación y capacitación.

Otro aspecto identificado es que, mientras en el sector bancario de la región América Latina y el Caribe el apoyo de la alta dirección a la gestión de riesgos de seguridad de la información se da principalmente (con un 65%) exigiendo la adopción de buenas prácticas de seguridad (Organización de Estados Americanos, 2018), el sector bancario de Colombia registra apenas un promedio de 38% para este ítem. Los establecimientos bancarios del país apoyan principalmente dicha gestión aprobando mayor presupuesto (69% de bancos) y aprobando / reforzando una estructura organizacional especializada (62% de bancos).

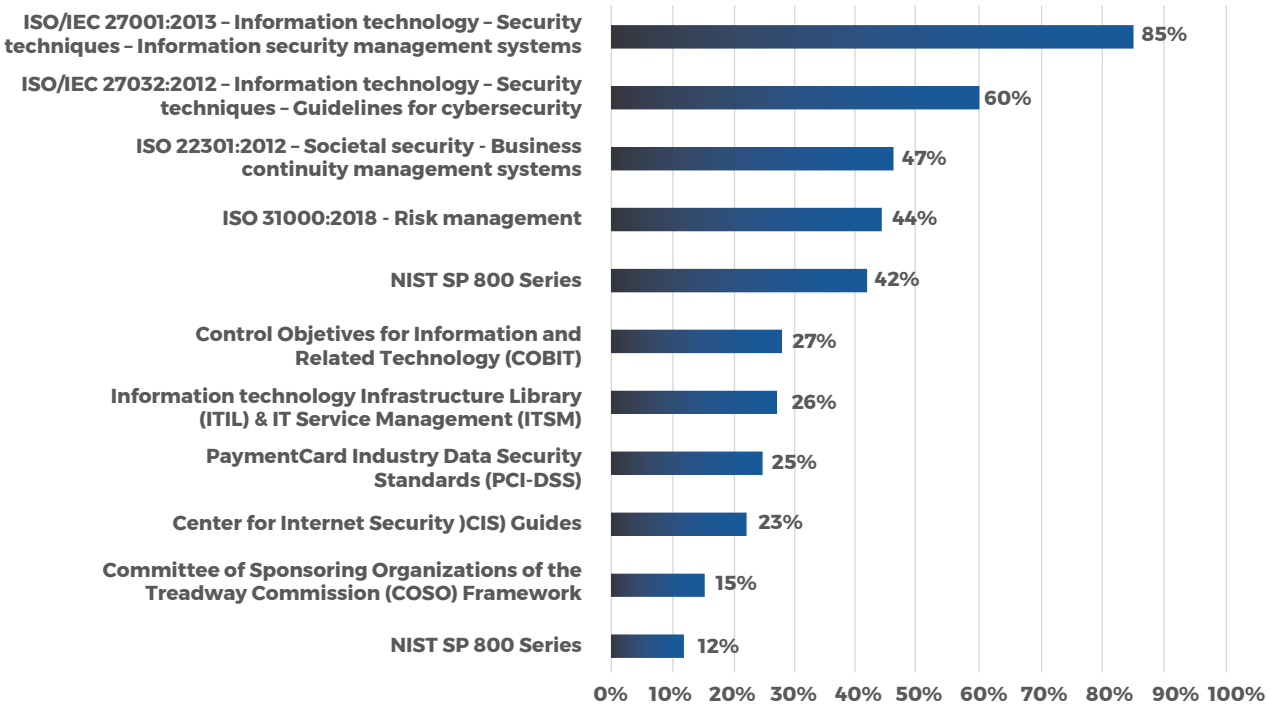
El rol que juega la alta dirección y la junta de las organizaciones respecto de la seguridad digital es fundamental. A nivel país, el presente estudio encuentra que para la mayoría de las entidades financieras (55% del total), es medianamente complejo lograr que la alta dirección de la organización tome decisiones de inversión en soluciones de seguridad digital, mientras que tan sólo el 15% de las organizaciones lo consideran altamente complejo. Se destaca el hecho de que sectores como las Comisionistas de Bolsa encuentran mayoritariamente (38%) que es poco complejo que la alta dirección tome decisiones de inversión en soluciones de seguridad digital.

Finalmente, en asuntos de preparación y gobernanza, vale la pena resaltar la adopción de marcos de gobierno, seguridad y/o estándares internacionales ISO en torno a la seguridad de la información (incluyendo la ciberseguridad) por parte de las entidades financieras del país. El 85% del total de entidades financieras menciona que ha adoptado las normas ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems, el 60% del total ha adoptado el ISO/IEC 27032:2012 - Information technology -- Security techniques -- Guidelines for cybersecurity, el 47% las ISO 22301:2012 - Societal security - Business continuity management systems y el 44% las ISO 31000:2018 - Risk management.

Gráfica 12.

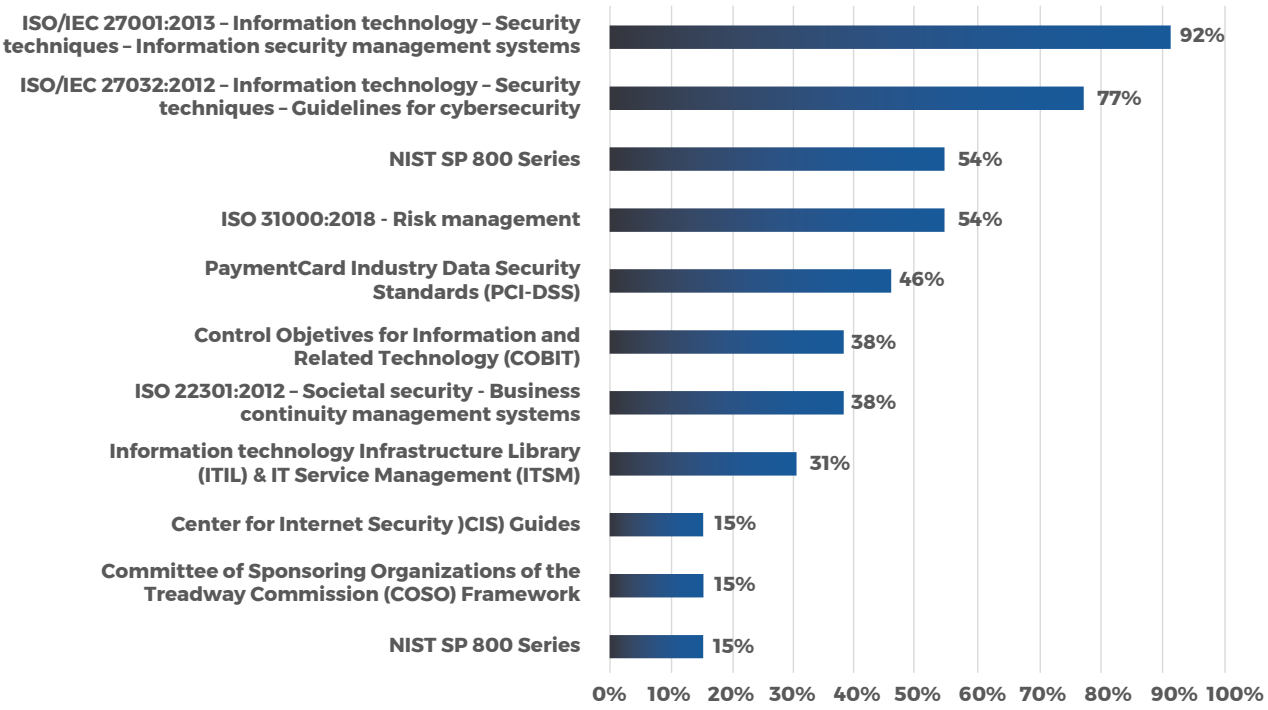
Marcos de gobierno, seguridad y/o estándares internacionales adoptados

Sistema Financiero Colombiano



Nota 1: 73 registros

Establecimientos Bancarios



Nota 2: 13 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

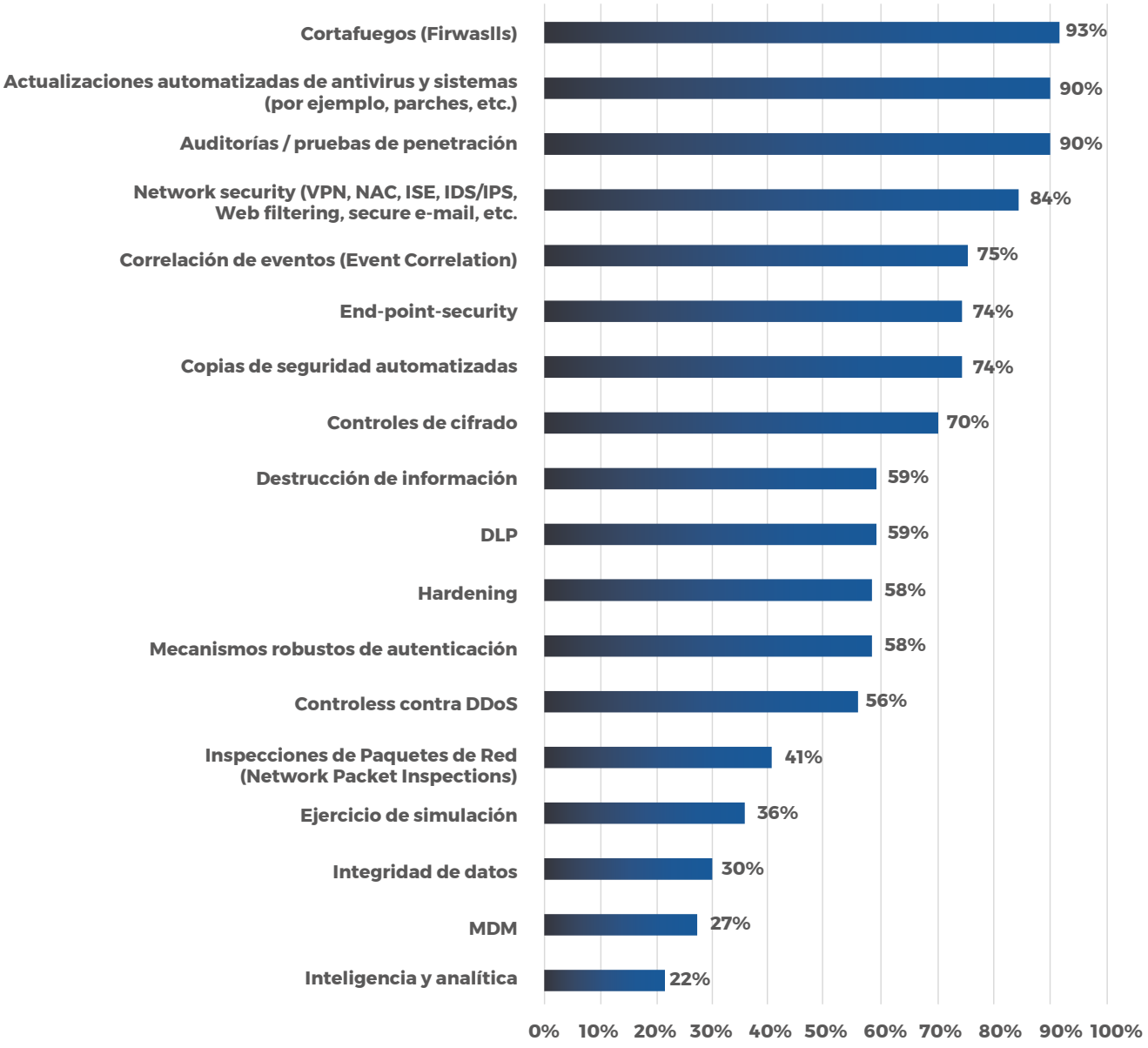
Se destaca que la aplicación de prácticas y adopción de normas en torno a ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems en el sector bancario de Colombia, registra un promedio del 92%, en concordancia a lo que ocurre en el sector bancario de la región de América Latica y el Caribe donde la mayoría (un 68% del total) de entidades bancarias menciona que ha adoptado dichas normas (Organización de Estados Americanos, 2018).

4.2.2. Detección y análisis de eventos de seguridad digital

Las acciones de detección y análisis de eventos de seguridad digital son fundamentales en el marco de gestión sistemática de este tipo de riesgos. Las principales acciones y medidas técnicas de la seguridad de la información (incluyendo ciberseguridad) que las entidades financieras de Colombia llevan a cabo son: i) los cortafuegos (93% del total), ii) las actualizaciones automatizadas de virus y sistemas (por ejemplo, parches, etc.) (90% del total), iii) las auditorías / pruebas de penetración (90% del total) y iv) el network security (VPN, NAC, ISE, IDS/IPS, Web filtering, secure e-mail, etc.) (84%). Se destaca que el 100% de las grandes entidades financieras implementan medidas como Cortafuegos, Actualizaciones automatizadas de virus y sistema, Network Security, Mecanismos robustos de autenticación, Auditorías / pruebas de penetración, Controles de cifrado y Controles contra DDoS, entre otras.

Gráfica 13.

Acciones y medidas técnicas de la seguridad de la información (incluyendo ciberseguridad) que tiene la entidad financiera (incluyendo los servicios provistos por la casa matriz) a la cual pertenece para proteger los sistemas de información críticos



Nota: 73 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Adicionalmente, los procesos / programas implementados en las entidades financieras del país más comunes asociados a la seguridad digital son: i) la educación y concientización (90%), ii) la gestión de Incidentes de seguridad (90%), iii) la protección de datos personales (90%), y iv) la evaluación de riesgos de seguridad de la información (88%). Se destaca que, en el sector bancario de Colombia, el 100% de los bancos grandes implementan todos los procesos / programas listados, con excepción de la Ciberinteligencia, con un 80% de los bancos grandes.

Gráfica 14.

Procesos / programas respecto a la seguridad digital implementados actualmente por las entidades financieras

Nota: 73 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

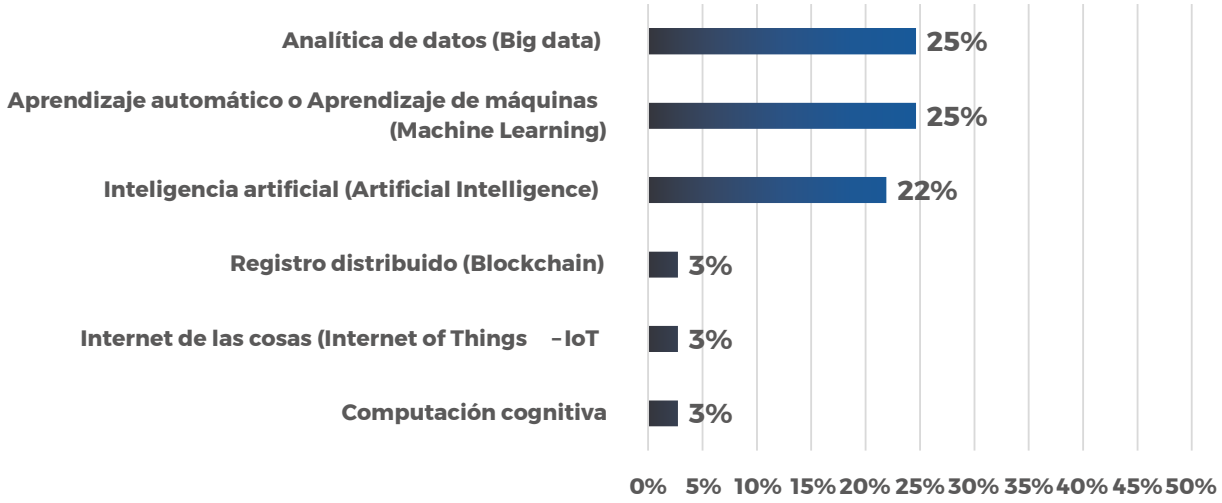
El uso de tecnologías digitales emergentes aplicadas a herramientas, controles o procesos de seguridad digital en entidades financieras en Colombia se encuentra aún rezagado. Tan sólo el 25% del total de entidades financieras implementan analítica de datos en herramientas, controles o procesos, el 25% del total de entidades financieras implementan el aprendizaje automático o Aprendizaje de máquinas (Machine Learning) y el 22% del total de entidades financieras implementan inteligencia artificial (Artificial Intelligence).

Se destaca el hecho de que, en el sector bancario de Colombia, el uso de Analítica de datos (Big Data) registra un promedio del 23%[19], muy similar al promedio del sector bancario de la región América Latina y el Caribe (29% del total) (Organización de Estados Americanos, 2018).

Gráfica 15.

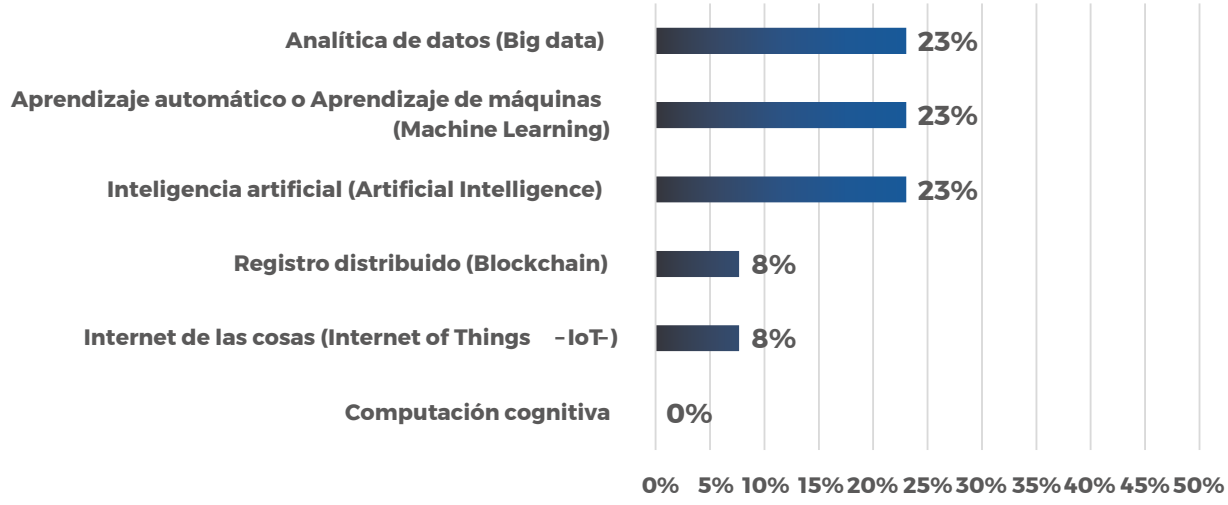
Tecnologías digitales emergentes aplicadas a herramientas, controles o procesos de seguridad digital en la entidad financiera

Sistema Financiero Colombiano



Nota 1: 68 registros

Establecimientos Bancarios



Nota 2: 12 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Por otra parte, los riesgos de seguridad de la información que consideran que merecen mayor atención por parte de las entidades financieras de Colombia, sin importar el tamaño de la organización, son: i) la pérdida / robo de activos de información clasificada (confidencial o sensible), ii) la indisponibilidad de infraestructura crítica, y iii) el compromiso de credenciales de usuarios privilegiados. Por parte de las entidades bancarias en la región América Latina y el Caribe, sin importar el tamaño de la organización, son: i) el robo de base de datos crítica, ii) el compromiso de credenciales de usuarios privilegiados, y iii) la pérdida de datos (Organización de Estados Americanos, 2018).

Cuadro 6.

Riesgos de seguridad de la información que merecen mayor atención por parte de la entidad financiera

	Grande	Mediano	Pequeño	Total
Pérdida / robo de activos de información clasificada (confidencial o sensible)	2,50	2,97	2,40	**2,68**
Indisponibilidad de infraestructura crítica	3,67	3,06	3,63	**3,37**
Compromiso de credenciales de usuarios privilegiados	2,83	3,78	3,53	**3,59**
Secuestro de información	3,83	3,72	4,00	**3,85**
Denegación del servicio	5,50	4,25	3,97	**4,24**
Sabotaje o fraude a través de un insider (personal interno)	3,50	4,31	4,50	**4,32**
Defacement – alteración en sitio web	6,17	5,91	5,97	**5,96**

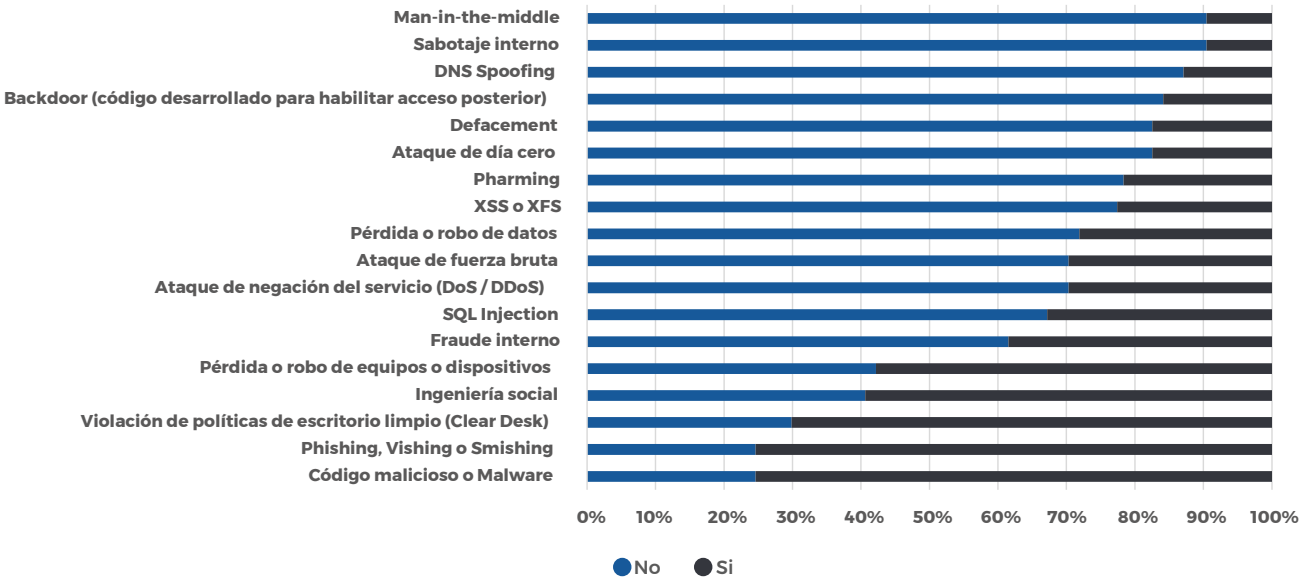
Nota: 68 registros y los entrevistados priorizaban los riesgos del 1 al 7, siendo el 1 el riesgo más alto y 7 el riesgo más bajo.

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Adicionalmente, los eventos de seguridad digital más comúnmente identificados por las entidades financieras de Colombia son: i) *el código malicioso o malware* (75% del total de entidades), ii) el *Phishing, Vishing o Smishing* (75% del total de entidades) y iii) *la violación de políticas de escritorio limpio* (*clear desk*) (70% del total de entidades). En contraste, las entidades financieras en el país mencionan que los eventos de seguridad menos comunes son: i) DNS *Spoofing* (tan sólo el 13% del total de entidades), ii) *Man-in-the-middle* (tan sólo el 10% del total de entidades), y iii) sabotaje interno (tan sólo el 10% del total de entidades). Es importante considerar la similitud con los eventos de seguridad digital más comúnmente identificados por las entidades bancarias de la región América Latina y el Caribe durante el año 2017, los cuales fueron: i) el código malicioso o malware (80% del total de Bancos), ii) *la violación de políticas de escritorio limpio* (*clear desk*) (63% del total de Bancos), y iii) *el phishing dirigido para tener acceso a sistemas del banco* (57% del total de Bancos) (Organización de Estados Americanos, 2018).

Gráfica 16.

Eventos (ataques exitosos y ataques no exitosos) de seguridad de la información (incluyendo ciberseguridad) contra entidades financieras identificados durante los últimos doce meses



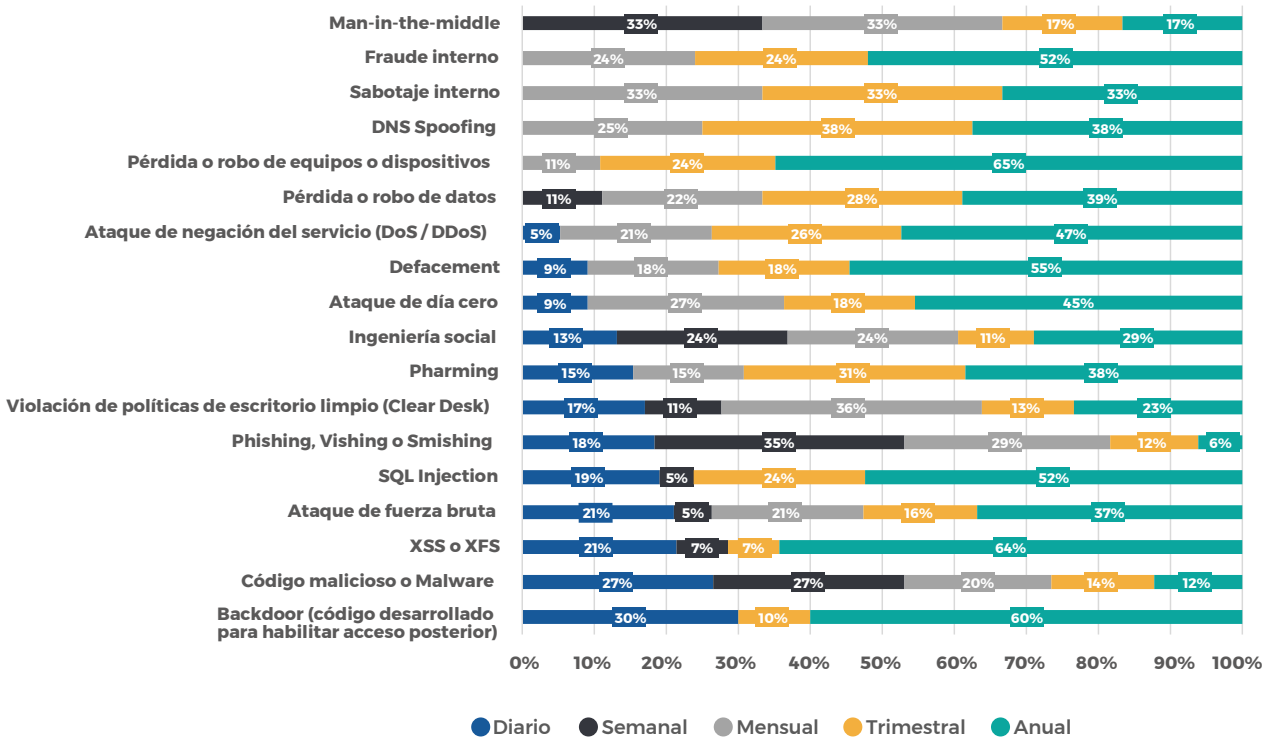
Nota: 68 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Al analizar los resultados respecto a la frecuencia aproximada de ocurrencia de eventos identificados por las entidades financieras en Colombia, se aprecia una dinámica particular por tipo de evento que depende también del tamaño de la organización. Por ejemplo, al revisar la frecuencia con la que ocurren eventos relacionados con código malicioso o malware para el total de entidades financieras en el país se aprecia lo siguiente: i) un 27% de las entidades identifican ocurrencia de eventos de malware diariamente, ii) un 27% del total lo identifican semanalmente, iii) un 20% del total lo identifican mensualmente, iv) un 14% del total lo identifican trimestralmente y v) un 12% del total lo identifican anualmente. Con respecto al Phishing, Vishing o Smishing se aprecia lo siguiente: i) un 18% de las entidades identifican ocurrencia de este tipo de eventos diariamente, ii) un 35% del total lo identifican semanalmente, iii) un 29% del total lo identifican mensualmente, iv) un 12% del total lo identifican trimestralmente y v) un 6% del total lo identifican anualmente.

Gráfica 17.

Frecuencia en la ocurrencia de eventos (ataques exitosos y ataques no exitosos) de seguridad de la información (incluyendo ciberseguridad)



Nota: 68 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

El análisis de la frecuencia con la que ocurren eventos (ataques exitosos y ataques no exitosos) de seguridad de la información (incluyendo ciberseguridad) en el Sistema Financiero Colombiano permite observar una realidad promedio de ocurrencia. No obstante, al revisar los resultados por tamaño de entidad financiera se presentan dinámicas particulares.

Por ejemplo, se observa que las entidades grandes del Sistema Financiero Colombiano son objeto de ataques de todo tipo de eventos de seguridad digital[20], resaltando identificación de todos por la mayoría de dichas entidades en el país. Los eventos (ataques exitosos y ataques no exitosos) de seguridad digital más comúnmente identificados por el 100% del total de entidades grandes son: i) ingeniería social, ii) Pishing, Vishing o Smishing, y iii) fraude inteno.

Al revisar la frecuencia con la que ocurren eventos relacionados con, por ejemplo, Pishing, Vishing o Smishing para el total de entidades grandes en Colombia se aprecia lo siguiente: i) un 33% de las entidades grandes lo identifican diariamente, ii) un 17% de las entidades grandes lo identifican semanalmente, iii) un 33% de las entidades grandes lo identifican mensualmente, y iv) un 17% de las entidades grandes lo identifican trimestralmente. Finalmente, se aprecia una dinámica de identificación de ocurrencia de una variedad de eventos de seguridad digital diaria, semanal, mensual, trimestral y anualmente por parte de las entidades grandes en el país.

Cuadro 7.

Eventos (ataques exitosos y ataques no exitosos) de seguridad de la información (incluyendo ciberseguridad) contra entidades financieras grandes identificados durante los últimos doce meses

	Si hay	No hay	Total
Ingeniería social	100%	0%	**100%**
Phishing, Vishing o Smishing	100%	0%	**100%**
Fraude interno	100%	0%	**100%**
Código malicioso o Malware	83%	17%	**100%**
Pérdida o robo de equipos o dispositivos	83%	17%	**100%**
Violación de políticas de escritorio limpio (Clear Desk)	67%	33%	**100%**
Pharming	50%	50%	**100%**
Ataque de día cero	50%	50%	**100%**
Ataque de negación del servicio (DoS / DDoS)	50%	50%	**100%**
SQL Injection	50%	50%	**100%**
Ataque de fuerza bruta	50%	50%	**100%**
Backdoor (código desarrollado para habilitar acceso posterior)	40%	60%	**100%**
XSS o XFS	40%	60%	**100%**
Man-in-the-middle	40%	60%	**100%**
Pérdida o robo de datos	33%	67%	**100%**
Defacement	33%	67%	**100%**
Sabotaje interno	17%	83%	**100%**
DNS Spoofing	0%	100%	**100%**

	Diario	Semanal	Mensual	Trimestral	Anual	Total
Ingeniería social	33%	0%	33%	17%	17%	**100%**
Phishing, Vishing o Smishing	33%	17%	33%	17%	0%	**100%**
Fraude interno	0%	0%	33%	33%	33%	**100%**
Código malicioso o Malware	80%	0%	0%	20%	0%	**100%**
Pérdida o robo de equipos o dispositivos	0%	0%	20%	20%	60%	**100%**
Violación de políticas de escritorio limpio (Clear Desk)	0%	0%	25%	0%	75%	**100%**
Pharming	33%	0%	33%	0%	33%	**100%**
Ataque de día cero	0%	0%	67%	0%	33%	**100%**
Ataque de negación del servicio (DoS / DDoS)	0%	0%	0%	67%	33%	**100%**
SQL Injection	100%	0%	0%	0%	0%	**100%**
Ataque de fuerza bruta	33%	0%	67%	0%	0%	**100%**
Backdoor (código desarrollado para habilitar acceso posterior)	50%	0%	0%	0%	50%	**100%**
XSS o XFS	100%	0%	0%	0%	0%	**100%**
Man-in-the-middle	0%	50%	50%	0%	0%	**100%**
Pérdida o robo de datos	0%	0%	0%	50%	50%	**100%**
Defacement	0%	0%	50%	50%	0%	**100%**
Sabotaje interno	0%	0%	100%	0%	0%	**100%**
DNS Spoofing	0%	0%	0%	0%	0%	**0%**

Nota: 6 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Las entidades medianas del Sistema Financiero Colombiano son objeto de ataques de todo tipo de eventos de seguridad digital, resaltando identificación de todos por la mayoría de dichas entidades en el país. Los eventos (ataques exitosos y ataques no exitosos) de seguridad digital más comúnmente identificados por entidades medianas son: i) Código malicioso o Malware (con el 88% de entidades medianas), ii) Phishing, Vishing o Smishing (con el 77% de entidades medianas), y iii) Violación de políticas de escritorio limpio (Clear Desk) (con el 75% de entidades medianas).

Al revisar la frecuencia con la que ocurren eventos relacionados con, por ejemplo, Código malicioso o Malware para el total de entidades medianas en Colombia se aprecia lo siguiente: i) un 25% de las entidades medianas lo identifican diariamente, ii) un 25% de las entidades medianas lo identifican semanalmente, iii) un 21% de las entidades medianas lo identifican mensualmente, iv) un 8% de las entidades medianas lo identifican trimestralmente, y v) un 4% de las entidades medianas lo identifican anualmente. Finalmente, se aprecia una dinámica de identificación de ocurrencia de una variedad de eventos de seguridad digital diaria, semanal, mensual, trimestral y anualmente por parte de las entidades medianas en el país.

Cuadro 8.

Eventos (ataques exitosos y ataques no exitosos) de seguridad de la información (incluyendo ciberseguridad) contra entidades financieras medianas identificados durante los últimos doce meses

	Si hay	No hay	Total
Código malicioso o Malware	88%	13%	**100%**
Phishing, Vishing o Smishing	77%	23%	**100%**
Violación de políticas de escritorio limpio (Clear Desk)	75%	25%	**100%**
Pérdida o robo de equipos o dispositivos	71%	29%	**100%**
Ingeniería social	55%	45%	**100%**
Fraude interno	50%	50%	**100%**
Ataque de negación del servicio (DoS / DDoS)	42%	58%	**100%**
Pérdida o robo de datos	39%	61%	**100%**
SQL Injection	39%	61%	**100%**
Ataque de fuerza bruta	39%	61%	**100%**
XSS o XFS	30%	70%	**100%**
Pharming	28%	72%	**100%**
Ataque de día cero	26%	74%	**100%**
Defacement	26%	74%	**100%**
DNS Spoofing	23%	77%	**100%**
Backdoor (código desarrollado para habilitar acceso posterior)	23%	77%	**100%**
Sabotaje interno	17%	83%	**100%**
Man-in-the-middle	13%	87%	**100%**

	Diario	Semanal	Mensual	Trimestral	Anual	Total
Código malicioso o Malware	25%	25%	21%	14%	14%	**100%**
Phishing, Vishing o Smishing	25%	38%	25%	8%	4%	**100%**
Violación de políticas de escritorio limpio (Clear Desk)	21%	13%	29%	17%	21%	**100%**
Pérdida o robo de equipos o dispositivos	0%	0%	9%	23%	68%	**100%**
Ingeniería social	12%	35%	12%	12%	29%	**100%**
Fraude interno	0%	0%	25%	19%	56%	**100%**
Ataque de negación del servicio (DoS / DDoS)	8%	0%	31%	15%	46%	**100%**
Pérdida o robo de datos	0%	0%	33%	25%	42%	**100%**
SQL Injection	8%	8%	0%	25%	58%	**100%**
Ataque de fuerza bruta	17%	8%	8%	25%	42%	**100%**
XSS o XFS	11%	11%	0%	11%	67%	**100%**
Pharming	13%	0%	0%	38%	50%	**100%**
Ataque de día cero	13%	0%	13%	25%	50%	**100%**
Defacement	13%	0%	13%	13%	63%	**100%**
DNS Spoofing	0%	0%	14%	43%	43%	**100%**
Backdoor (código desarrollado para habilitar acceso posterior)	29%	0%	0%	14%	57%	**100%**
Sabotaje interno	0%	0%	20%	40%	40%	**100%**
Man-in-the-middle	0%	25%	25%	25%	25%	**100%**

Nota: 32 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Por último, las entidades pequeñas del Sistema Financiero Colombiano son objeto de ataques de todo tipo de eventos de seguridad digital[21], resaltando identificación de todos por la mayoría de dichas entidades en el país. Los eventos (ataques exitosos y ataques no exitosos) de seguridad digital más comúnmente identificados por entidades pequeñas son: i) Phishing, Vishing o Smishing (con el 68% de entidades medianas), ii) Violación de políticas de escritorio limpio (Clear Desk) (con el 66% de entidades medianas), y iii) Código malicioso o Malware (con el 59% de entidades medianas).

Al revisar la frecuencia con la que ocurren eventos relacionados con, por ejemplo, Pishing, Vishing o Smishing para el total de entidades pequeñas en Colombia se aprecia lo siguiente: i) un 5% de las entidades pequeñas lo identifican diariamente, ii) un 37% de las entidades pequeñas lo identifican semanalmente, iii) un 32% de las entidades pequeñas lo identifican mensualmente, iv) un 16% de las entidades pequeñas lo identifican trimestralmente, y v) un 11% de las entidades pequeñas lo identifican anualmente. Finalmente, se aprecia una dinámica de identificación de ocurrencia de una variedad de eventos de seguridad trimestral y anualmente por parte de las entidades pequeñas en el país.

Cuadro 9.

Eventos (ataques exitosos y ataques no exitosos) de seguridad de la información (incluyendo ciberseguridad) contra entidades financieras pequeñas identificados durante los últimos doce meses

	Si hay	No hay	Total
Phishing, Vishing o Smishing	68%	32%	**100%**
Violación de políticas de escritorio limpio (Clear Desk)	66%	34%	**100%**
Código malicioso o Malware	59%	41%	**100%**
Ingeniería social	56%	44%	**100%**
Pérdida o robo de equipos o dispositivos	37%	63%	**100%**
SQL Injection	22%	78%	**100%**
Pérdida o robo de datos	15%	85%	**100%**
Ataque de fuerza bruta	15%	85%	**100%**
Ataque de negación del servicio (DoS / DDoS)	11%	89%	**100%**
Fraude interno	11%	89%	**100%**
XSS o XFS	11%	89%	**100%**
Pharming	8%	92%	**100%**
DNS Spoofing	4%	96%	**100%**
Defacement	4%	96%	**100%**
Backdoor (código desarrollado para habilitar acceso posterior)	4%	96%	**100%**
Ataque de día cero	0%	100%	**100%**
Sabotaje interno	0%	100%	**100%**
Man-in-the-middle	0%	100%	**100%**

	Diario	Semanal	Mensual	Trimestral	Anual	Total
Código malicioso o Malware	5%	37%	32%	16%	11%	**100%**
Phishing, Vishing o Smishing	16%	11%	47%	11%	16%	**100%**
Violación de políticas de escritorio limpio (Clear Desk)	13%	38%	25%	13%	13%	**100%**
Pérdida o robo de equipos o dispositivos	7%	20%	33%	7%	33%	**100%**
Ingeniería social	0%	0%	10%	30%	60%	**100%**
Fraude interno	0%	0%	0%	33%	67%	**100%**
Ataque de negación del servicio (DoS / DDoS)	0%	50%	0%	25%	25%	**100%**
Pérdida o robo de datos	25%	0%	25%	0%	50%	**100%**
SQL Injection	0%	0%	0%	33%	67%	**100%**
Ataque de fuerza bruta	0%	0%	0%	33%	67%	**100%**
XSS o XFS	0%	0%	0%	0%	100%	**100%**
Pharming	0%	0%	50%	50%	0%	**100%**
Ataque de día cero	0%	0%	100%	0%	0%	**100%**
Defacement	0%	0%	0%	0%	100%	**100%**
DNS Spoofing	0%	0%	0%	0%	100%	**100%**
Backdoor (código desarrollado para habilitar acceso posterior)	0%	0%	0%	0%	0%	**0%**
Sabotaje interno	0%	0%	0%	0%	0%	**0%**
Man-in-the-middle	0%	0%	0%	0%	0%	**0%**

Nota: 30 registros

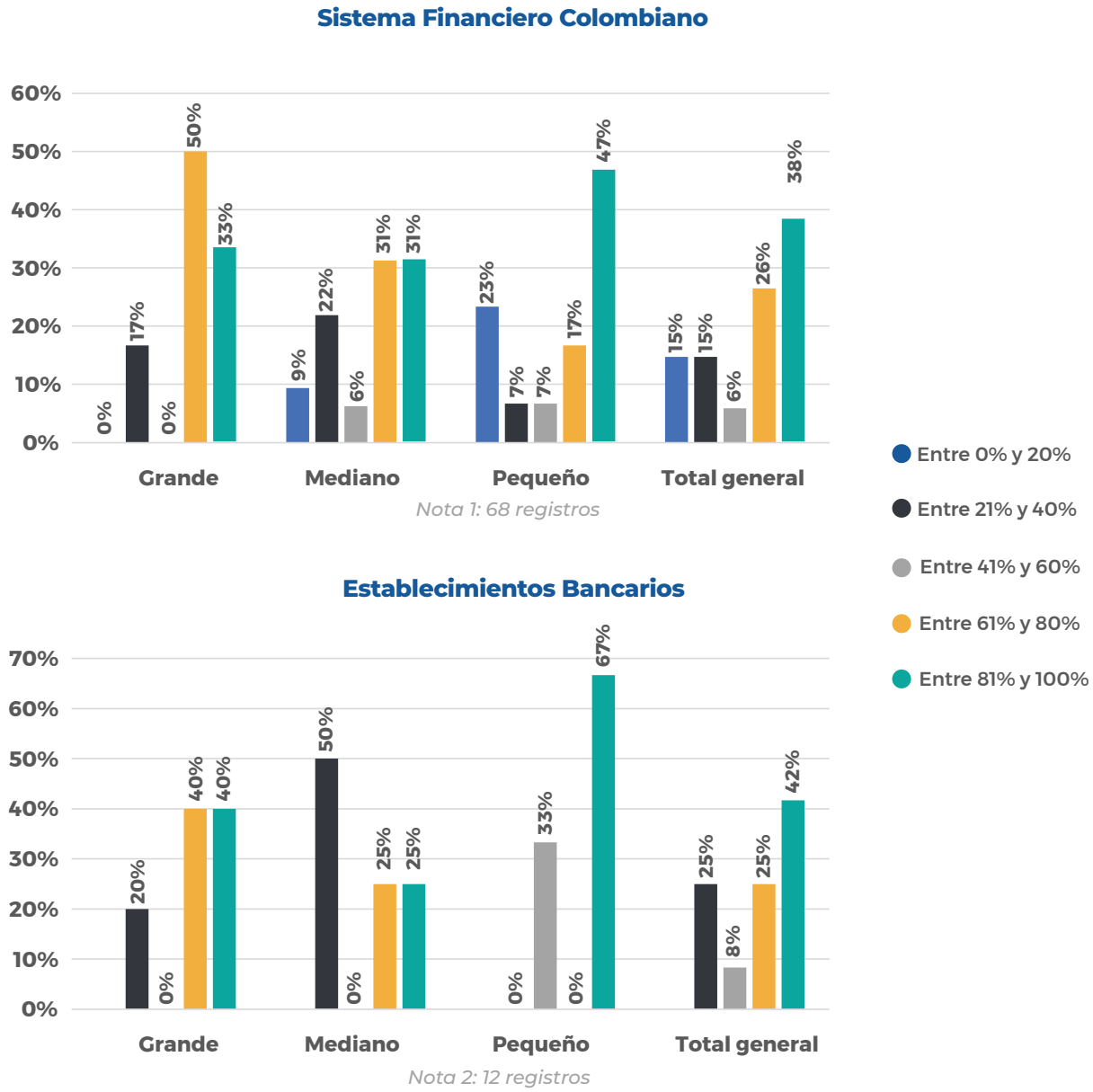
Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Al analizar el tipo de eventos (ataques exitosos y ataques no exitosos) de seguridad digital que usan los ciberdelincuentes contra los clientes de servicios financieros, las entidades financieras en Colombia mencionan que los eventos de i) Phishing, ii) Ingeniería social, y iii) Smishing son los más frecuentes en el país, similar a lo registrado por el sector bancario en la región América Latina y el Caribe en el año 2017 (Organización de Estados Americanos, 2018). Por otra parte, los eventos de seguridad digital contra clientes menos comunes son: i) Key logger, ii) Robo de identidad RFID (tarjetas de crédito / teléfonos móviles), y iii) Software falso que suplanta el software real de la entidad financiera.

Finalmente, en asuntos de detección y análisis de eventos de seguridad digital, se resalta que en promedio el 15% de las entidades financieras en el país detecta mediante sistemas propios (y no de terceros) entre un 0% y un 20% de eventos (ataques exitosos y ataques no exitosos) de seguridad de la información (incluyendo ciberseguridad), el 15% de las entidades detecta entre un 21% y un 40% de eventos con sistemas propios, el 6% de las entidades detecta entre un 41% y un 60% de eventos con sistemas propios, el 26% de las entidades detecta entre un 61% y un 80% de eventos con sistemas propios y el 38% de las entidades detecta entre un 81% y un 100% de eventos con sistemas propios. Se destaca que en sectores como el bancario, el 42% de los bancos detecta mediante sistemas propios (y no de terceros) entre un 81% y un 100% de eventos de seguridad de la información[22].

Gráfica 18.

Porcentaje de eventos (ataques exitosos y ataques no exitosos) detectados mediante sistemas operados por la entidad financiera (incluyendo los servicios provistos por la casa matriz)



Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Al analizar por tamaño de entidad, la mayoría de las entidades grandes (50%) detecta entre un 61% y un 80% de eventos con sistemas propios y la mayoría de las entidades medianas (31%) y la mayoría de las entidades pequeñas (47%) detecta entre un 81% y un 100% de eventos con sistemas propios. Se destaca el caso del sector bancario de Colombia donde el 40% de los bancos grandes detecta entre 81% y un 100% de eventos con sistemas propios, mientras que en promedio un 30% de los bancos grandes de la región América Latina y el Caribe detecta en dicho rango (Organización de Estados Americanos, 2018).

4.2.3. Gestión, respuesta y recuperación ante incidentes de seguridad digital

Es importante mencionar que en el instrumento de recolección de información enviado a las entidades financieras se resaltó la diferencia entre evento e incidente de seguridad de la información (incluyendo ciberseguridad) así:

- Evento de seguridad de la información (incluyendo ciberseguridad) es la suma de ataques exitosos y de ataques no exitosos que sufrió la entidad financiera durante un periodo de tiempo. Este concepto está en línea con lo establecido en el numeral 2.8 de la Circular Externa No. 007 de 2018 expedida por la Superintendencia Financiera de Colombia: "2.8. Evento de ciberseguridad. Ocurrencia de una situación que podría afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio."

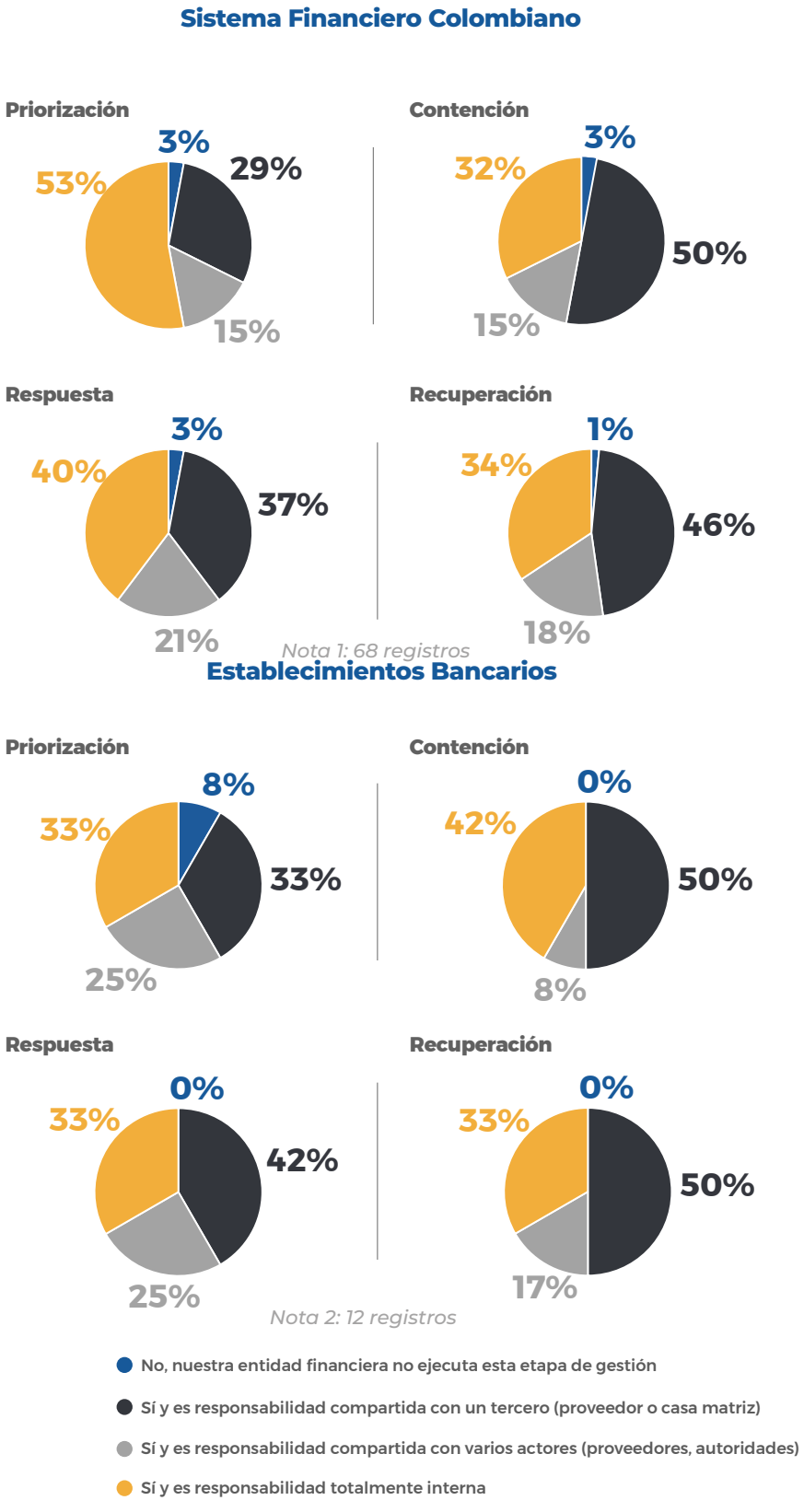
- Incidente de seguridad de la información (incluyendo ciberseguridad) es el total de ataques exitosos que sufrió la entidad financiera durante el mismo periodo de tiempo. Este concepto está en línea con lo establecido en el numeral 2.9 de la Circular Externa No. 007 de 2018 expedida por la Superintendencia Financiera de Colombia: "2.9. Ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio."

Teniendo en cuenta dichas definiciones a continuación se analizan los resultados haciendo énfasis a este último concepto: la gestión, respuesta y recuperación ante incidentes de seguridad digital.

Al analizar las etapas de gestión frente a incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad) se destaca que: i) el 53% de las entidades del país cuentan y ejecutan una estrategia de priorización de incidentes bajo la responsabilidad interna de la organización, ii) el 32% de las entidades del país cuentan y ejecutan una estrategia de contención de incidentes bajo la responsabilidad interna de la organización, iii) el 40% de las entidades del país cuentan y ejecutan una estrategia de respuesta de incidentes bajo la responsabilidad interna de la organización, y iv) el 34% de las entidades del país cuentan y ejecutan una estrategia de recuperación de incidentes bajo la responsabilidad interna de la organización. Es decir, al menos un tercio de las entidades del país cuentan con estrategias de gestión, respuesta y recuperación ante incidentes de seguridad digital.

Gráfica 19.

Estrategias frente a incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad)



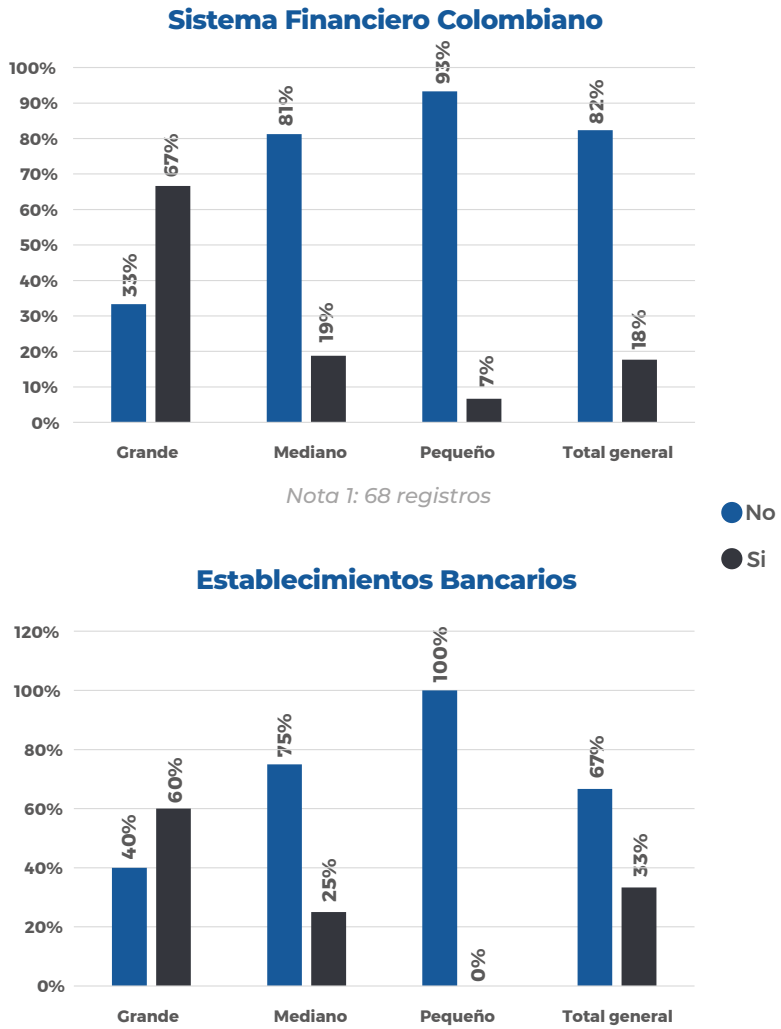
Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Al analizar el sector bancario en Colombia, el 100% de los bancos reportan que ejecutan las etapas de contención, respuesta y recuperación. Tan sólo un 8% de los establecimientos bancarios reportan que no ejecutan la etapa de priorización.

En relación con la materialización de incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad) en las entidades financieras en el país, se resalta que el 67% de las entidades grandes manifiestan que fueron víctimas de ataques exitosos, mientras que entre las entidades medianas el porcentaje es del 19% y entre las pequeñas, del 7%. Se resalta el hecho de que, en el sector bancario de Colombia, la materialización de incidentes (ataques exitosos) fue en un 60% en entidades grandes y en un 25% en entidades medianas[23]. No obstante, es inferior con respecto a lo evidenciado en el sector bancario de la región América Latina y el Caribe, donde un 65% de las entidades bancarias grandes, un 43% de las medianas y un 19% de las pequeñas admiten haber sido víctimas de ataques exitosos de seguridad de la información (incluyendo ciberseguridad).

Gráfica 20.

¿La entidad financiera a la cual usted pertenece (en el país en el que se encuentra), como organización, fue víctima de incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad) durante los últimos doce meses?



Nota 1: 68 registros

Nota 2: 12 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

En específico y tomando como base las entidades financieras que son víctimas de incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad) (12 entidades), se destaca que la la totalidad de entidades en los sectores bancario, compañías de financiamiento, sociedades de servicios financieros y entidades aseguradoras investigan la fuente[24].

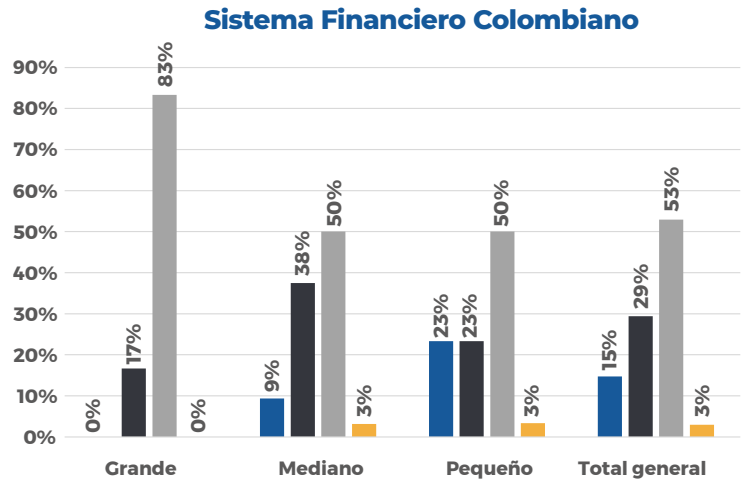
Además, y como resultado de las investigaciones, dichas entidades financieras en el país identifican y priorizan las principales motivaciones de dichos incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad), siendo éstas: i) motivos económicos (75% de las entidades víctimas), ii) robo de información personal (42% de las entidades víctimas), y iii) robo de información clasificada (confidencial o sensible) (33% de las entidades víctimas).

Con respecto al sector bancario de Colombia, las principales motivaciones son las mismas, pero con porcentajes superiores de ocurrencia en las dos primeras (75% de bancos víctimas por motivos económicos, 50% de los bancos víctimas por robo de información personal y 25% de los bancos víctimas por robo de información clasificada (confidencial o sensible). Vale la pena destacar que, en el sector bancario de la región de América Latina y el Caribe, el apartado Motivos políticos / hacktivismo no es considerado como una de las principales causas de motivación para generar ataques informáticos (Organización de Estados Americanos, 2018).

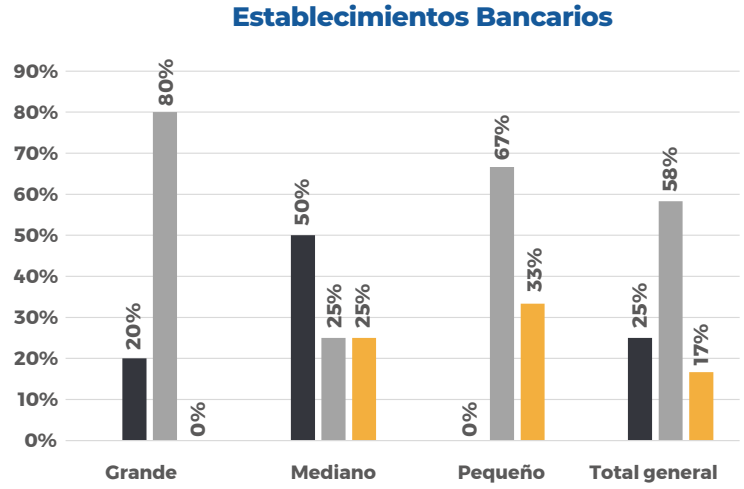
Al preguntar si las entidades financieras completan totalmente una evaluación de la madurez bajo una metodología de seguridad de la información (incluyendo ciberseguridad) o ejecutando todas sus acciones derivadas, se encuentran diferencias según el tamaño de la organización. Mientras que el 83% de las entidades grandes de Colombia realiza dicha evaluación y lleva a cabo las acciones correspondientes, tan sólo el 50% de las entidades medianas y el 50% de las entidades pequeñas reflejan dicha situación. En contraste, preocupa que el 9% de las entidades medianas y el 23% de las entidades pequeñas no evalúan la madurez de seguridad digital. A nivel sectorial, todos los establecimientos bancarios en Colombia realizan este tipo de evaluaciones[25].

Gráfica 21.

¿La entidad financiera a la cual usted pertenece ha sido evaluada externamente en los últimos dos (2) años bajo alguna metodología de seguridad de la información (incluyendo ciberseguridad) para determinar su nivel de madurez?



Nota 1: 68 registros



Nota 2: 12 registros

- No, nuestra entidad financiera no ha sido evaluada
- Sí se realizó la evaluación y se ejecutaron satisfactoriamente las acciones correspondientes
- Sí se realizó la evaluación y se están ejecutando actualmente las acciones correspondientes
- Sí se realizó la evaluación, pero no ha sido posible ejecutar las acciones correspondientes

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Las entidades financieras del Sistema Financiero Colombiano que manifestaron que no completan totalmente una evaluación de la madurez de la seguridad digital o no ejecutan las acciones derivadas atribuyen esta situación principalmente a: i) Falta de asignación de presupuesto (30% de entidades sin evaluación), ii) Complejidad técnica de las soluciones requeridas (30% de entidades sin evaluación), e iii) Insuficiente personal especializado (20% de entidades sin evaluación).

4.2.4. Reportes de incidentes de seguridad digital

Del análisis de resultados respecto al reporte de incidente de seguridad de la información (incluyendo ciberseguridad) (total de ataques exitosos que sufrió la entidad financiera durante el mismo periodo de tiempo) es importante revisar si las organizaciones cuentan con mecanismos o planes internos, así como la existencia de regulaciones específicas frente al tema.

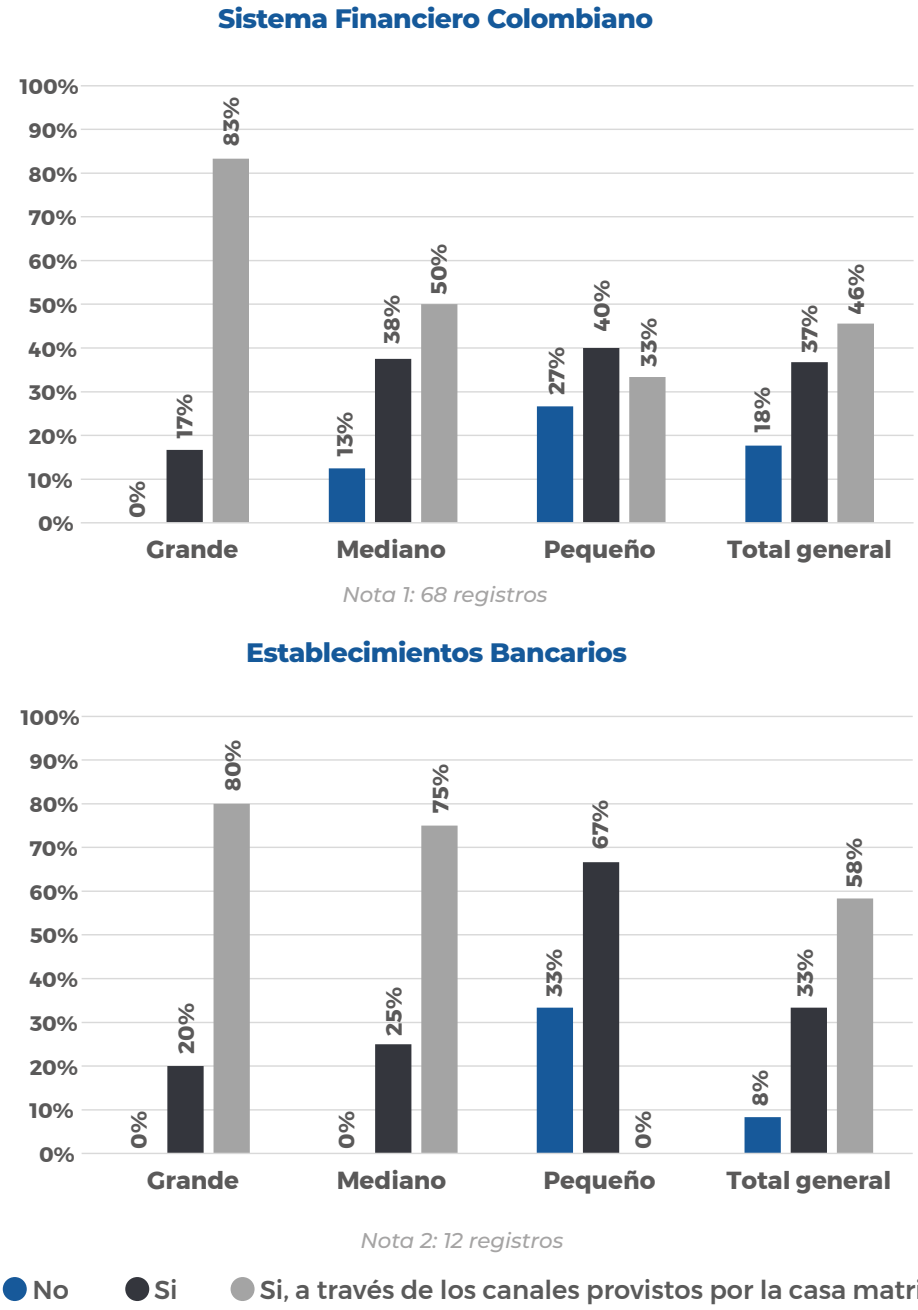
En términos generales, se aprecia que casi la totalidad de las entidades financieras de Colombia – grandes (100%), medianas (94%) y pequeñas (97%) – ofrece un mecanismo para que sus colaboradores (empleados y contratistas) reporten incidentes (ataques exitosos) de seguridad digital sufridos, y en sectores como el sector bancario de Colombia se alcanzan el 100%, superando incluso el promedio de la región de América Latina y el Caribe (68% de los bancos de la región) (Organización de Estados Americanos, 2018).

En contraste con lo anterior, la existencia de mecanismos para que sus clientes de servicios financieros reporten a la entidad incidentes (ataques exitosos) de seguridad digital sufridos varía según el tamaño de la entidad. Se aprecia que el 100% de las entidades grandes ofrece un mecanismo para que sus clientes de servicios financieros reporten a la entidad incidentes (ataques exitosos) de seguridad digital sufridos[26], en contraste con el 88% de las entidades medianas y el 73% de las entidades pequeñas del país.

En este caso, un 92% de los bancos del sector bancario de Colombia ofrece este tipo de mecanismos a sus clientes[27], superando el promedio de los bancos de la región de América Latina y el Caribe (68% del total) (Organización de Estados Americanos, 2018).

Gráfica 22.

¿La entidad financiera a la cual usted pertenece ofrece un mecanismo para que sus clientes de servicios financieros reporten incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales)?



Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

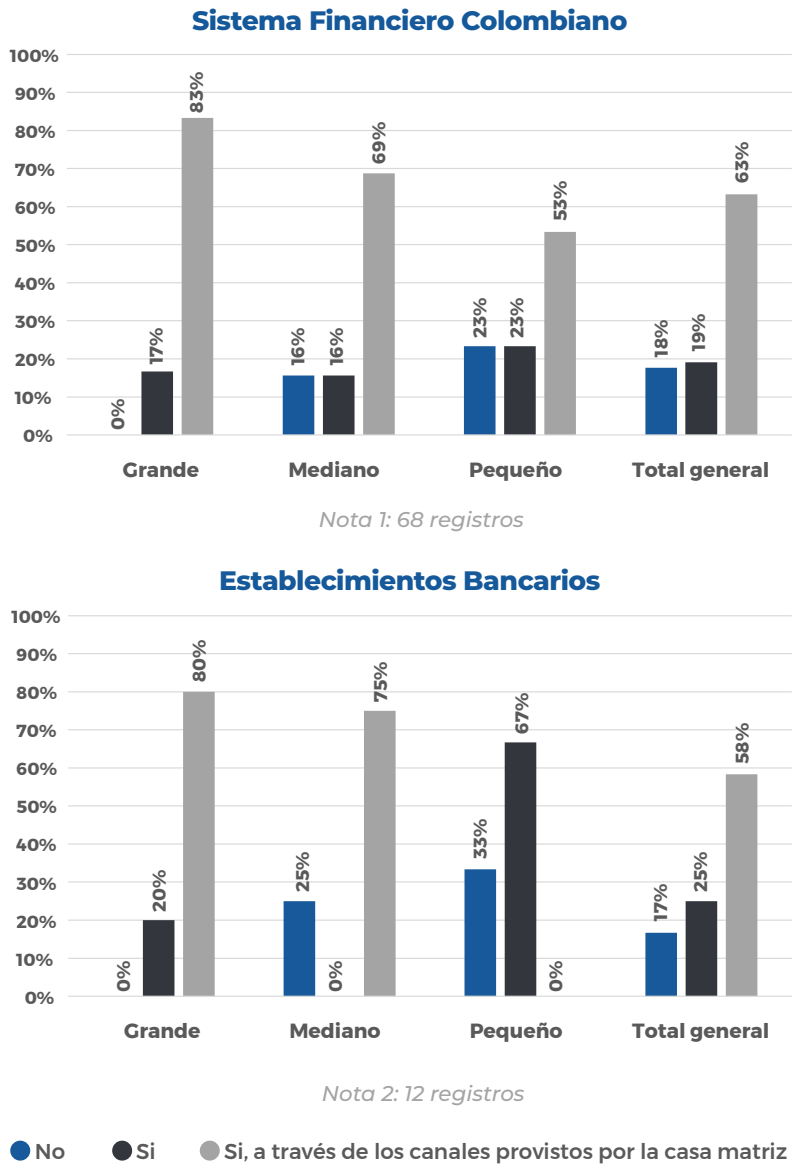
De igual manera, la existencia de un plan de comunicaciones que permita informar a los clientes de servicios financieros cuando su información personal se haya visto comprometida varía según el tamaño de la entidad. Se aprecia que en todas las entidades grandes existe un plan de comunicaciones para informar a sus clientes de servicios financieros cuando su información personal se haya visto

comprometida, en contraste con un 84% de las entidades medianas del país y con un 77% de las entidades pequeñas.

Al realizar un análisis sectorial dentro del Sistema Financiero Colombiano, se evidencia que la mayoría de las entidades financieras cuenta con el mencionado plan de comunicaciones, resaltando que el total de las entidades de los sectores de corporaciones financieras y sociedades administradoras de pensiones y cesantías tienen este plan. En cuanto al sector bancario, el 83% de los bancos reportan la existencia de este plan[28].

Gráfica 23.

Gráfica 23. ¿La entidad financiera a la cual usted pertenece cuenta con un plan de comunicaciones que permita informar a sus clientes cuando su información personal se haya visto comprometida?

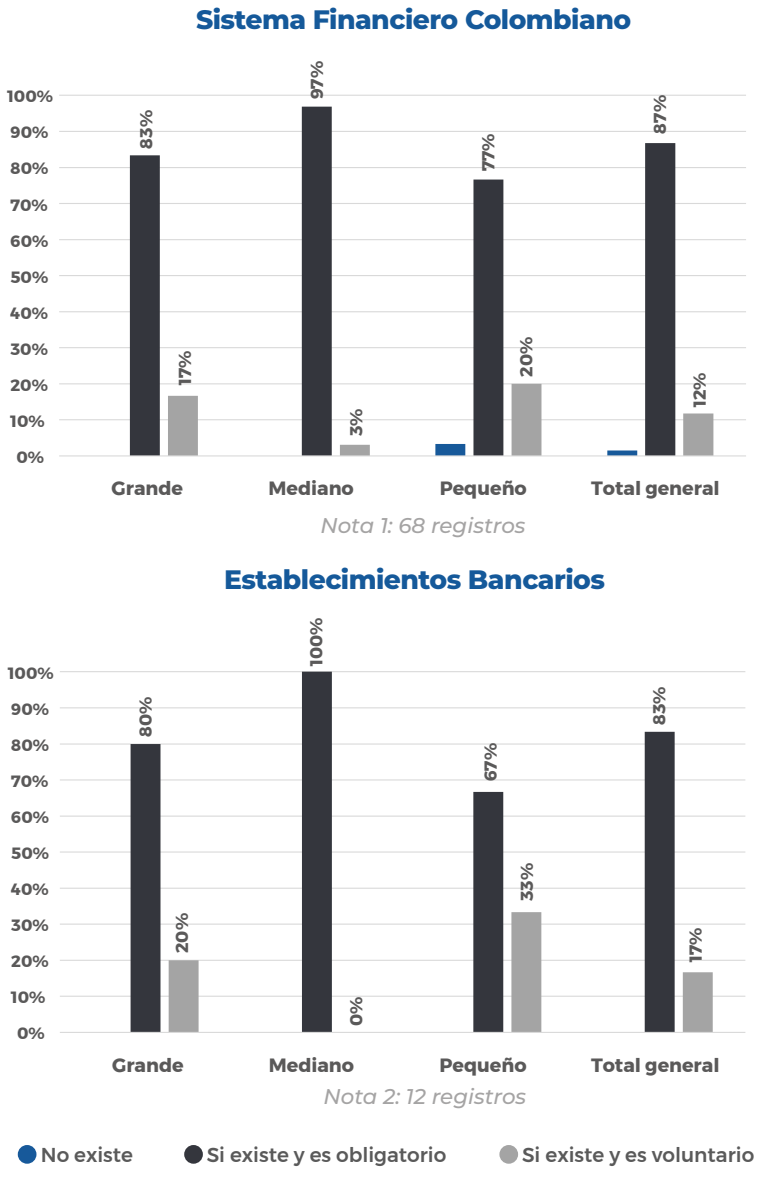


Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

En relación con el reporte de incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales) ante una autoridad de regulación en Colombia por parte de las entidades financieras, se aprecia que casi la totalidad de entidades tiene dicho mecanismo, existiendo leves diferencias entre entidades grandes frente a entidades medianas y pequeñas respecto de la obligatoriedad y la voluntariedad. El 83% de las entidades grandes versus el 97% de las entidades medianas y el 77% de las entidades pequeñas manifiestan que conocen algún mecanismo para reportar incidentes y es obligatorio debido a la existencia de disposiciones establecidas por alguna autoridad de regulación. Por otra parte, se resalta que en todos los establecimientos bancarios existe el mecanismo[29].

Gráfica 24.

¿Existe algún mecanismo para reportar incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales) sufridos por la entidad financiera a la cual usted pertenece ante una autoridad de regulación en Colombia?

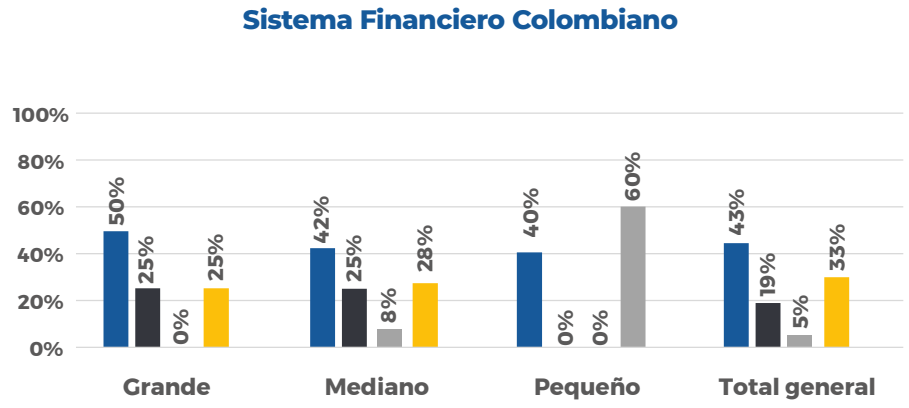


Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

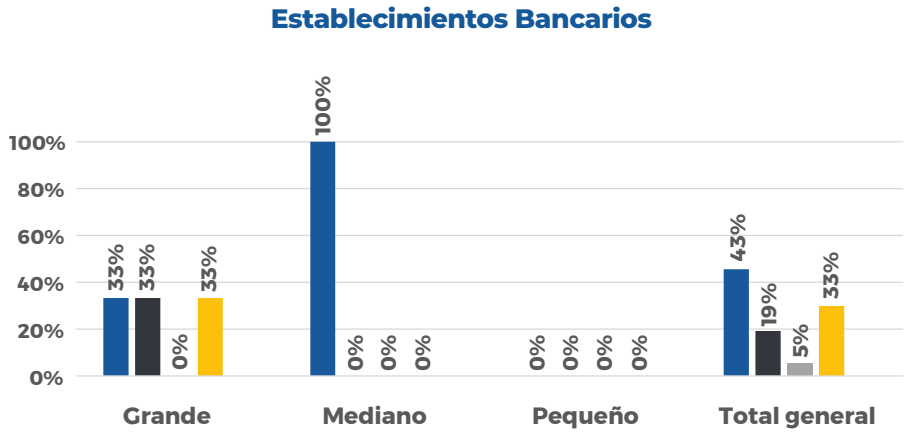
Adicionalmente, se aprecia que el reporte de incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales) ante la Fiscalía General de la Nación o Policía Judicial en Colombia por parte de las entidades financieras de Colombia es común. En particular, en el sector bancario, el 20% de los bancos reportan ente el 81% y el 100% de los incidentes ante dichas autoridades[30].

Gráfica 25.

¿La entidad financiera a la cual usted pertenece reporta los incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales) sufridos en los últimos doce meses ante la Fiscalía General de la Nación o Policía Judicial en Colombia?



Nota 1: 68 registros



Nota 2: 12 registros

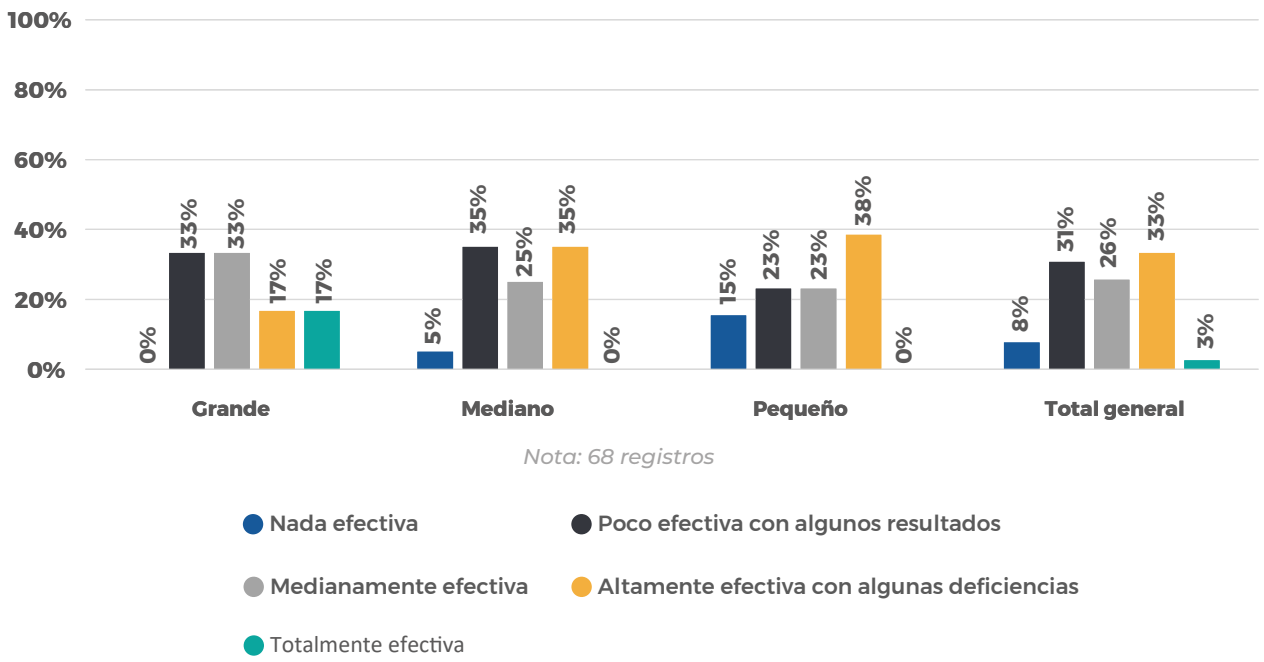
- Reporta entre el 0% y el 20% de los incidentes ocurridos
- Reporta entre el 21% y el 40% de los incidentes ocurridos
- Reporta entre el 61% y el 80% de los incidentes ocurridos
- Reporta entre el 81% y el 100% de los incidentes ocurridos

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Finalmente, e independientemente del tamaño de la entidad financiera, el 33% de entidades en Colombia considera como Altamente efectiva con algunas deficiencias el papel de la Fiscalía General de la Nación y la Policía Judicial en Colombia respecto a la investigación y judicialización de los ciberdelincuentes, mientras que tan sólo el 8% considera como nada efectiva el papel de las mencionadas autoridades.

Gráfica 26.

En general, ¿cómo considera la efectividad de las autoridades judiciales en Colombia respecto a la investigación y judicialización de los ciberdelincuentes en los últimos 12 meses?



Nota: 68 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Al analizar los resultados para el sector bancario de Colombia versus los resultados para el sector bancario de la región América Latina y el Caribe, se concluye que existen coincidencias respecto de la consideración de efectividad de las mencionadas autoridades: i) medianamente efectiva (29% de los bancos de Colombia versus 31% de los bancos de la región) y ii) poco efectiva con algunos resultados (57% de los bancos de Colombia versus 37% de los bancos de la región) (Organización de Estados Americanos, 2018).

4.2.5. Capacitación y concientización

Finalmente, la gestión sistemática de riesgos de seguridad digital debe contar con acciones de capacitación y concientización dentro de las organizaciones. En particular y sin distinguir por tamaño de la entidad financiera, casi la totalidad (94%) de las entidades financieras de Colombia cuenta con planes de concientización y formación en asuntos de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales para sus colaboradores. Se

destaca que el 100% de las entidades grandes del Sistema Financiero Colombiano cuentan con dichos planes en el país[31].

Considerada la base de entidades financieras de Colombia que cuentan con planes de preparación, respuesta y capacitación en asuntos de seguridad digital para sus colaboradores, se destaca que el 41% se ejecutan de manera continua / permanente, el 13% de los mismos se ejecutan mensual, trimestral y semestralmente, y el 22% anualmente[32].

Por otra parte, el 63% de las entidades financieras en el país evalúan la capacidad de los colaboradores de la entidad para responder adecuadamente a eventos (ataques exitosos y no exitosos) de seguridad de la información (incluyendo ciberseguridad) y amenazas tales como phishing e ingeniería social con periodicidad anual, el 18% con periodicidad semestral, el 6% con periodicidad trimestral, el 3% con periodicidad mensual y el 4% de manera continua / permanente[33].

Finalmente, en relación con asuntos de capacitación y concientización, las entidades financieras identifican que los mecanismos más efectivos a partir de los cuales se ha generado mayor conciencia en la entidad respecto de los riesgos de seguridad digital son: i) Capacitaciones, ii) Correos electrónicos, y iii) Boletines. Estos tres (3) mecanismos fueron también priorizados por el sector bancario de Colombia.

Cuadro 10.

Mecanismo más efectivo a partir del cual se ha generado mayor conciencia en la entidad financiera respecto de los riesgos de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales

	Grande	Mediano	Pequeño	Total
Capacitaciones	1,67	1,75	1,80	**1,76**
Correos electrónicos	3,83	3,00	2,50	**2,85**
Boletines	5,00	2,84	2,60	**2,93**
Requisitos legales y/o regulatorios	5,50	4,97	4,53	**4,82**
Presentaciones y debates en conferencias	6,50	6,34	6,07	**6,24**
Redes sociales	3,33	6,72	7,07	**6,57**
Publicaciones gratuitas en revistas, sitios web y listas de correo	6,67	7,09	6,83	**6,94**
Documentación de organismos especializados en la materia	7,33	7,47	7,63	**7,53**
Servicios especializados por suscripción	7,83	7,78	8,13	**7,94**
Asociaciones profesionales	8,67	7,66	8,23	**8,00**

Nota: 68 registros y se priorizan todos los mecanismos otorgándoles un número del 1 al 10, siendo el 1 el mecanismo más efectivo y 10 el mecanismo menos efectivo.

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

4.3.
Impacto de los incidentes de seguridad digital

Una vez caracterizadas las entidades financieras que participaron en el desarrollo del presente estudio y presentados los resultados encontrados sobre la gestión de riesgos de seguridad digital por parte del Sistema Financiero Colombiano, a continuación, se presenta el análisis del impacto de los incidentes de seguridad digital en entidades financieras en Colombia.

La muestra de entidades financieras a partir de las cuales se presentan los siguientes resultados alcanza unos activos a 31 de diciembre de 2018 cercanos a los COP $483,8 billones de pesos (aproximadamente un 65% del total de activos de los sectores analizados) y acumulan utilidades netas por COP $12,33 billones de pesos (aproximadamente un 83% del total de utilidades de los sectores analizados), lo que permite afirmar que dicha muestra contiene una representatividad de los distintos niveles de activos y patrimonio del país. Se destaca que los activos reportados por los Establecimientos Bancarios aportan COP $399,83 billones de los activos, correspondientes a casi un 83% del total de la muestra.

Cuadro 11.

Distribución del valor estimado de Activos por sector del Sistema Financiero Colombiano (billones de pesos)

	Grande	Mediano	Pequeño	Total
Establecimientos Bancarios	$361,91	$34,42	$3,51	**$399,83**
Compañías de Financiamiento		$4,25	$1,88	**$6,13**
Corporaciones Financieras			$12,23	**$12,23**
Sociedad Fiduciaria (incluye la actividad de custodia de valores)		$1,44	$0,79	**$2,24**
Pensiones, Cesantías y Fiduciarias (Sociedades de Servicios Financieros)		$5,95		**$5,95**
Compañías de Seguros de Vida, de Seguros Generales y Sociedades de Capitalización	$3,15	$18,54	$34,12	**$55,81**
Comisionistas de Bolsa		$0,23	$1,46	**$1,69**
SISTEMA FINANCIERO COLOMBIANO	$365,05	$64,83	$53,99	**$483,87**

Nota: 66 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Cuadro 12.

Distribución del valor estimado de EBITDA por sector del Sistema Financiero Colombiano (billones de pesos)

	Grande	Mediano	Pequeño	Total
Establecimientos Bancarios	$7,56	$0,34	$0,03	**$7,93**
Compañías de Financiamiento		$0,05	$0,03	**$0,08**
Corporaciones Financieras			$1,66	**$1,66**
Sociedad Fiduciaria (incluye la actividad de custodia de valores)		$0,20	$0,15	**$0,36**
Pensiones, Cesantías y Fiduciarias (Sociedades de Servicios Financieros)		$0,64		**$0,64**
Compañías de Seguros de Vida, de Seguros Generales y Sociedades de Capitalización	$0,06	$0,62	$0,92	**$1,60**
Comisionistas de Bolsa		$0,03	$0,04	**$0,07**
SISTEMA FINANCIERO COLOMBIANO	$7,62	$1,88	$2,83	**$12,33**

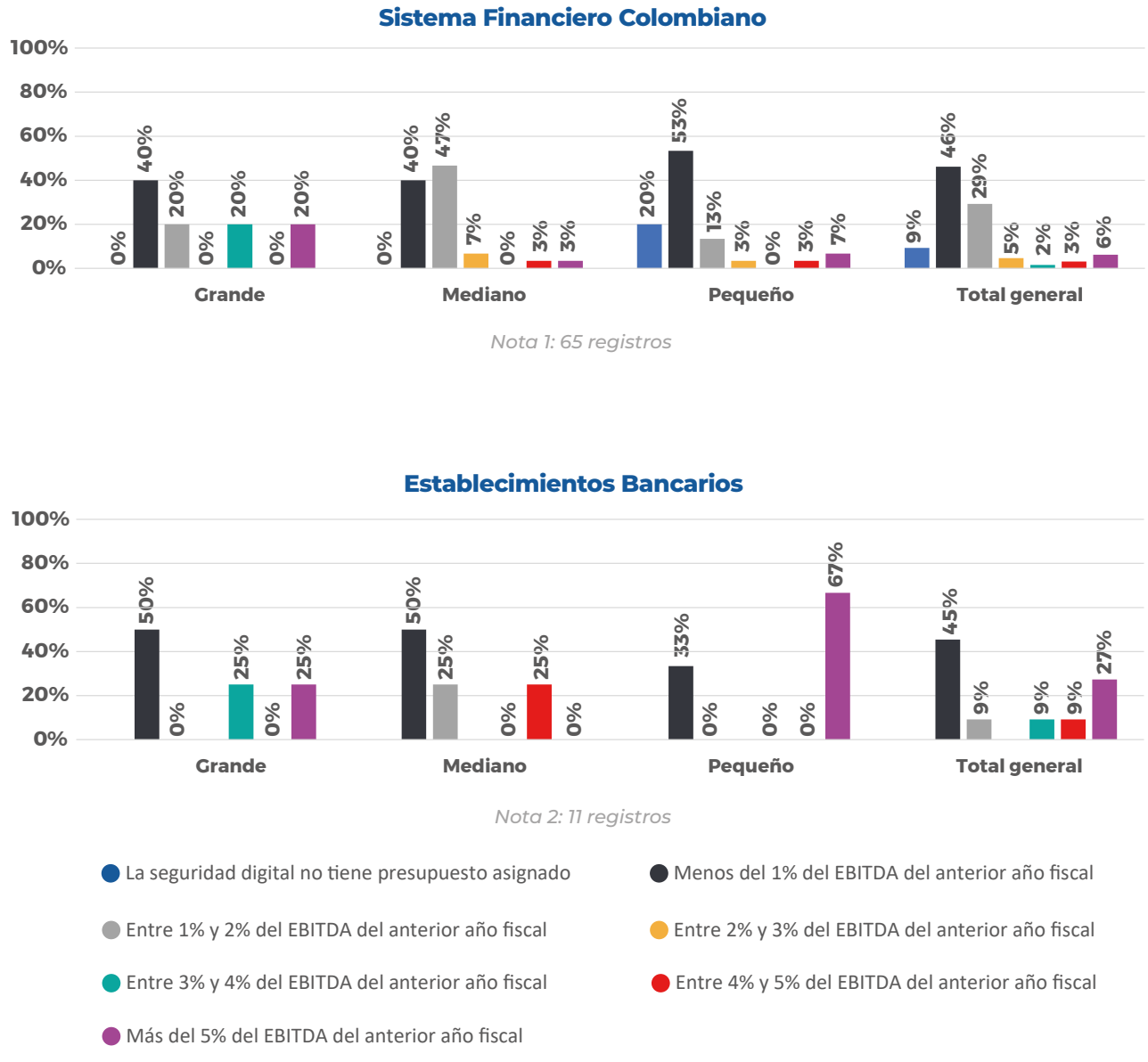
Nota: 66 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

A partir de las entidades financieras que presentaron información, se observa que el 46% de las entidades en la región manifiestan que el presupuesto de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) equivale en promedio a menos del 1% del EBITDA del anterior año fiscal, el 29% de las entidades afirman que el valor de dicho presupuesto está entre el 1% y el 2% del EBITDA del anterior año fiscal, el 5% de las entidades lo sitúan entre el 2% y el 3% del EBITDA del anterior año fiscal, el 2% de las entidades entre el 3% y el 4% del EBITDA del anterior año fiscal, el 3% de las entidades entre el 4% y el 5% del EBITDA del anterior año fiscal y el 6% de las entidades manifiestan que dicho presupuesto equivale a un valor mayor al 5% del EBITDA del anterior año fiscal.

Gráfica 27.

Presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales para el actual año fiscal como % del EBITDA



Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Se destacan las diferencias entre las estimaciones de dicho presupuesto entre el sector bancario de Colombia con el promedio del sector bancario de la región América Latina y el Caribe[34], en donde se aprecia que el 45% de bancos en Colombia versus el 61% de bancos en la región manifiestan que dicho presupuesto equivale en promedio a menos del 1% del EBITDA del anterior año fiscal, el 27% de bancos en Colombia versus el 34% de bancos en la región afirman que el valor de dicho presupuesto

está entre el 1% y el 5% del EBITDA del anterior año fiscal y el 27% de bancos en Colombia versus el 5% de bancos en la región sitúan el valor de dicha partida por encima del 5% del EBITDA del anterior año fiscal (Organización de Estados Americanos, 2018).

Del análisis de los resultados de la muestra se puede inferir que el valor del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales como porcentaje del EBITDA del actual año fiscal por parte de las entidades del sistema financiero colombiano equivale al 1,76%. También se estima que este presupuesto para entidades grandes equivale al 2,63% del EBITDA del actual año fiscal, para entidades medianas al 2,03% del EBITDA del actual año fiscal y para entidades pequeñas al 1,77% del EBITDA del actual año fiscal.

Cuadro 13.

Presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales para el actual año fiscal como % del EBITDA por sector del Sistema Financiero Colombiano

	Grande	Mediano	Pequeño	Total
Establecimientos Bancarios	3,25%	2,25%	5,00%	**3,50%**
Compañías de Financiamiento		1,67%	1,50%	**1,58%**
Corporaciones Financieras			0,50%	**0,50%**
Sociedad Fiduciaria (incluye la actividad de custodia de valores)		1,50%	1,00%	**1,25%**
Pensiones, Cesantías y Fiduciarias (Sociedades de Servicios Financieros)		1,25%		**1,25%**
Compañías de Seguros de Vida, de Seguros Generales y Sociedades de Capitalización	2,00%	1,83%	1,20%	**1,68%**
Comisionistas de Bolsa		3,67%	1,40%	**2,53%**
SISTEMA FINANCIERO COLOMBIANO	2,63%	2,03%	1,77%	**1,76%**

Nota: 65 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Al analizar por sector del Sistema Financiero Colombiano, se aprecia por ejemplo que el presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales para los Establecimientos Bancarios equivale al 3,50% del EBITDA del actual año fiscal, mientras que dicho presupuesto para la Sociedades de Servicios Financieros equivale al 1,25% del EBITDA del actual año fiscal.

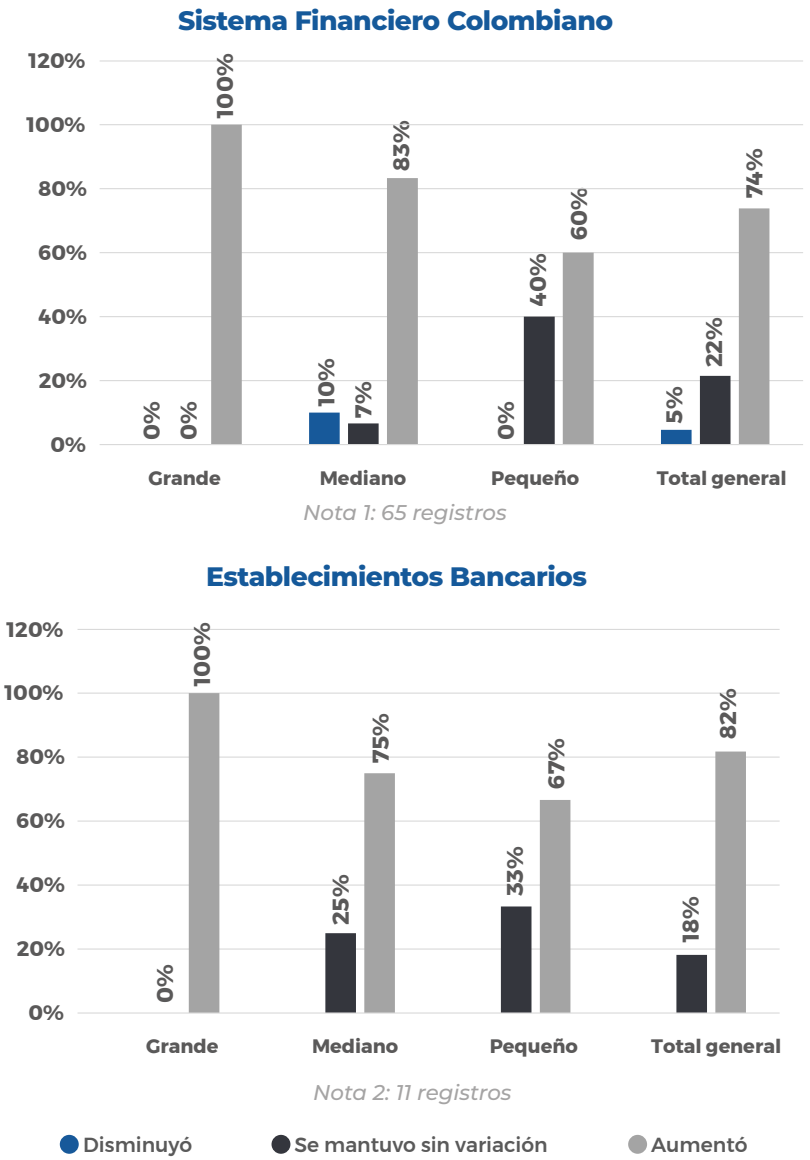
Además, en comparación al año fiscal inmediato anterior, el 74% de las entidades financieras en el país manifiestan que el presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales aumentó, el 21,5% manifiesta que se mantuvo sin variación y tan sólo el 4,6% manifiesta que se había disminuido. No obstante, los resultados

específicos para el sector bancario de Colombia son diferentes: el 83% de los bancos en el país señala que el presupuesto aumentó y el 17% que se mantiene sin variación.

Al analizar en detalle, se apreciaron diferencias en los resultados para cada tamaño de entidad financiera para el Sistema Financiero Colombiano. Se destaca que para el 100% de las entidades grandes, el 83% de las entidades medianas y el 60% de las entidades pequeñas, el presupuesto de seguridad digital aumenta en comparación al año fiscal inmediato anterior. Por otro lado, para el 7% de las entidades medianas y el 40% de las entidades pequeñas, el presupuesto de seguridad digital se mantiene igual a aquel del año fiscal inmediato anterior[35].

Gráfica 28.

Dinámica del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales para el actual año fiscal



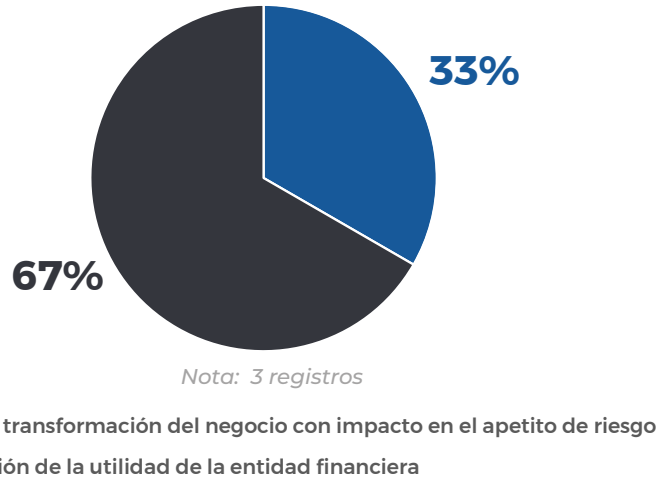
Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Del total de entidades financieras que manifiestan que el presupuesto de seguridad digital aumenta en comparación al año fiscal inmediato anterior, un 88% indicó que dicho aumento se debe a Cumplimiento Regulatorio, un 54% que es por Cumplimiento de nuevas políticas internas, y un 54% a Cambio / transformación digital del negocio. En relación con el sector bancario, se aprecia que en promedio los bancos de Colombia y los bancos de la región América Latina y el Caribe coinciden en que principalmente el aumento se debe a Cumplimiento Regulatorio (78% de bancos en Colombia versus 62% de bancos en la región) y Nuevas amenazas de ciberseguridad por el uso de NTIC (44% de bancos en Colombia versus 54% de bancos en la región), entre otros (Organización de Estados Americanos, 2018).

Por otro lado, del total de entidades financieras que manifiestan que el presupuesto de seguridad digital disminuye en comparación al año fiscal inmediato anterior, el 67% señala que se debe a una Disminución de la Utilidad de la entidad financiera, y el 33% a Cambio o transformación del negocio con impacto en el apetito de riesgo.

Gráfica 29.

Razones de la disminución del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales

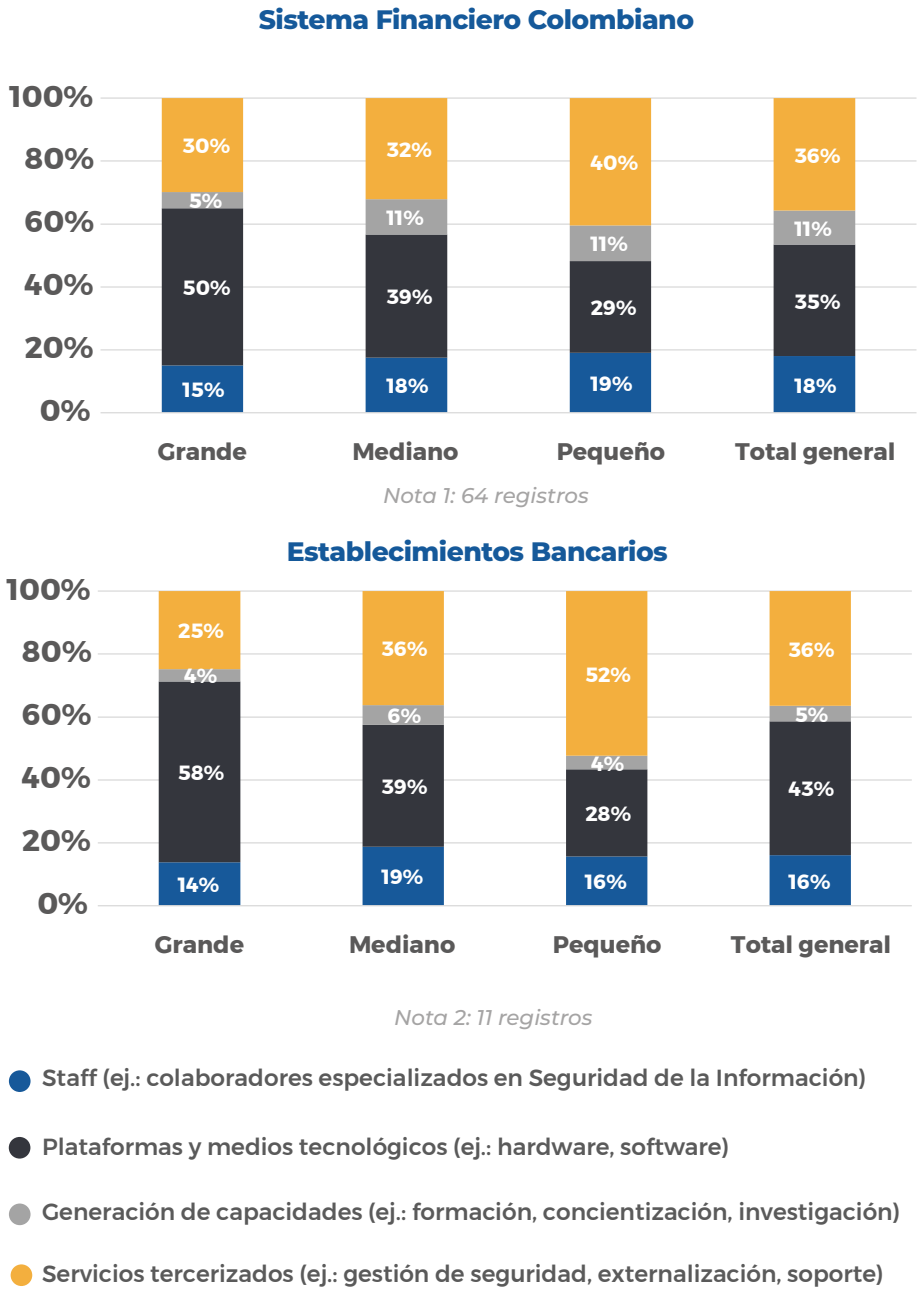


Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

El presupuesto destinado por parte de una entidad financiera promedio del Sistema Financiero Colombiano a seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales se distribuye del siguiente modo: el 35% en Plataformas y medios tecnológicos (ej.: hardware, software), el 36% en *Servicios tercerizados (ej.: gestión de seguridad, externalización, soporte) el 18% en Staff (ej.: colaboradores especializados en Seguridad de la Información), y el 11% en Generación de capacidades (ej.: formación, concientización, investigación).*

Gráfica 30.

Distribución del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales de la entidad financiera (en Colombia, sin incluir en el cálculo el presupuesto de su casa matriz)



Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Al comparar la distribución del mencionado presupuesto entre el sector bancario de Colombia con el promedio del sector bancario de la región América Latina y el Caribe[36] se aprecia lo siguiente: i) el 43% tanto en Colombia como en la región para Plataformas y medios tecnológicos (ej.: hardware, software), ii) el 16% en Colombia versus el 22% en la región para Staff (ej.: colaboradores especializados en Seguridad de la Información), iii) el 36% en Colombia versus el 22% en la región para Servicios tercerizados (ej.: gestión de seguridad, externalización, soporte) y iv) el 5% en Colombia versus el 13% en la región para Generación de capacidades (ej.: formación, concientización, investigación) (Organización de Estados Americanos, 2018).

Por otro lado, de la información recolectada de la muestra de entidades financieras se estima que el retorno de inversión (ROI) en seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales equivale aproximadamente a 10,00%. Al analizar por tamaño de entidad se obtiene: i) un 15% para una entidad grande en el país (representado por la Banca Comercial o Múltiple), ii) un 10,00% para una entidad mediana en el país, y iii) un 3,75% para una entidad pequeña del Sistema Financiero Colombiano.

Cuadro 14.

Retorno de inversión (ROI) en seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales para su entidad financiera en el año fiscal inmediatamente anterior

	Grande	Mediano	Pequeño	Total
Establecimientos Bancarios	15,00%	7,50%		**11,25%**
Compañías de Financiamiento		22,50%		**22,50%**
Corporaciones Financieras				
Sociedad Fiduciaria (incluye la actividad de custodia de valores)				
Pensiones, Cesantías y Fiduciarias (Sociedades de Servicios Financieros)		5,00%		**5,00%**
Compañías de Seguros de Vida, de Seguros Generales y Sociedades de Capitalización		12,50%	5,00%	**8,75%**
Comisionistas de Bolsa		2,50%	2,50%	**2,50%**
SISTEMA FINANCIERO COLOMBIANO	**15,00%**	**10,00%**	**3,75%**	**10,00%**

Nota: 11 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

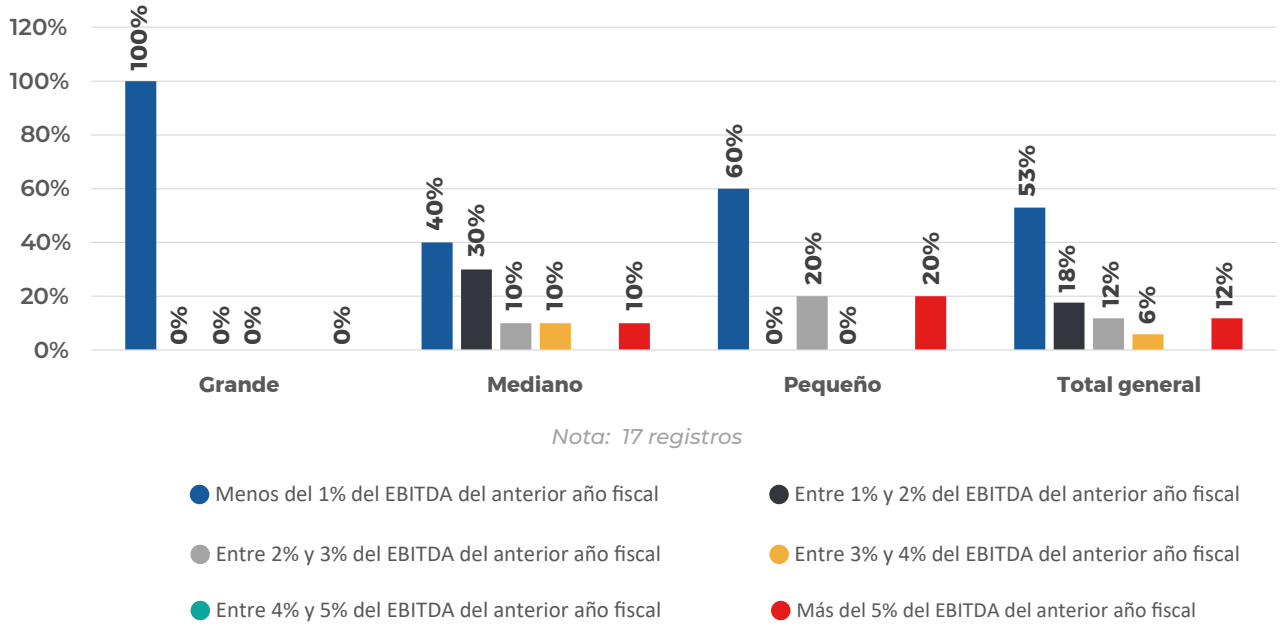
Respecto a las estimaciones del retorno sobre la inversión en seguridad digital, el 45% de las entidades financieras consideran que son retornos de alta rentabilidad, el 45% de las entidades financieras consideran que son retornos de media rentabilidad y tan solo el 9% lo considera de baja rentabilidad.

Ahora, a partir de las entidades financieras que presentaron información[37], se destaca que el 53% de las entidades en la región manifiestan que el costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) equivale en promedio a menos del 1% del EBITDA del anterior año fiscal, el 18% de las entidades calculan que el valor de dicho costo está entre el 1% y el 2% del EBITDA del anterior año fiscal, el 12% de las entidades ubican el valor de dicho costo entre el 2% y el 3% del EBITDA del anterior año fiscal, el 6% de las entidades sitúan esa partida entre el 3% y el 4% del EBITDA del anterior año fiscal y el 12% manifiestan que el valor de dicho costo está por encima del 5% del EBITDA del anterior año fiscal.

Del análisis también se puede inferir que a medida que aumenta el tamaño de la entidad financiera disminuye el costo total de respuesta y de recuperación ante incidentes de seguridad digital como % del EBITDA del año inmediato anterior. Por ejemplo, el 100% de las entidades grandes manifiestan que el valor de dicho costo es menor del 1% del EBITDA del anterior año fiscal, mientras que el 40% de las entidades medianas y el 60% de las entidades pequeñas manifiestan que dicho costo se encuentra en ese rango.

Gráfica 31.

Costo total de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) para el último año fiscal



Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Destaca la similitud entre las estimaciones de dicho costo en el sector bancario de Colombia y el promedio del sector bancario de la región América Latina y el Caribe: el 100% de bancos en Colombia versus el 73% de bancos en la región manifiestan que dicho costo equivale en promedio a menos del 1% del EBITDA del anterior año fiscal (Organización de Estados Americanos, 2018).

Del análisis de los resultados de la muestra se puede inferir que el valor del costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) como % del EBITDA del último año fiscal equivale al 2,16%. También se estima que este presupuesto para entidades grandes equivale al 1% del EBITDA del anterior año fiscal, para entidades medianas equivale al 2,18% del EBITDA del anterior año fiscal y para entidades pequeñas equivale al 2,83% del EBITDA del anterior año fiscal.

Cuadro 15.

Costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) para la entidad financiera (en Colombia) para el último año fiscal por sector del Sistema Financiero Colombiano

	Grande	Mediano	Pequeño	Total
Establecimientos Bancarios	1,00%	1,00%		**1,00%**
Compañías de Financiamiento		4,00%		**4,00%**
Corporaciones Financieras				
Sociedad Fiduciaria (incluye la actividad de custodia de valores)			1,67%	**1,67%**
Pensiones, Cesantías y Fiduciarias (Sociedades de Servicios Financieros)		1,67%		**1,67%**
Compañías de Seguros de Vida, de Seguros Generales y Sociedades de Capitalización		3,25%	4,00%	**3,63%**
Comisionistas de Bolsa		1,00%		**1,00%**
SISTEMA FINANCIERO COLOMBIANO	**1,00%**	**2,18%**	**2,83%**	**2,16%**

Nota: 17 registros

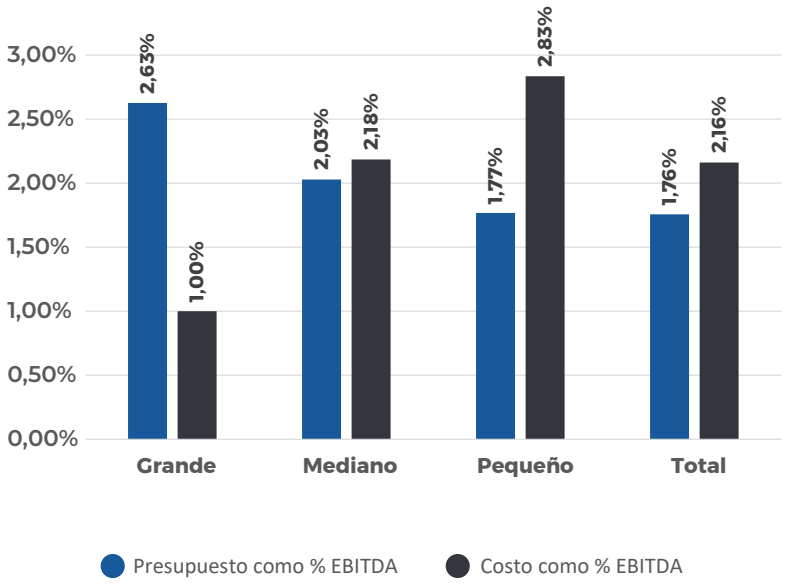
Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Al analizar por sector del Sistema Financiero Colombiano, se aprecia por ejemplo que el costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) para el sector de banca equivale al 1,00% del EBITDA del último año fiscal, mientras que para las Compañías de Financiamiento equivale al 4,00% del EBITDA del último año fiscal.

De lo analizado en el presente numeral del documento, a partir de la muestra de entidades financieras del Sistema Financiero Colombiano que reportaron información en promedio se concluye que: i) el presupuesto destinado a la seguridad digital por una entidad financiera promedio en la región equivale aproximadamente al 1,76% del EBITDA del año inmediato anterior (versus el 2,09% para el sector bancario de la región América Latina y el Caribe), y ii) el costo total de respuesta y de recuperación ante incidentes de seguridad digital para una entidad financiera promedio en la región equivale aproximadamente al 2,16% del EBITDA del año inmediato anterior (versus el 1,52% para el sector bancario de la región América Latina y el Caribe).

Gráfica 32.

Presupuesto y Costo total de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) como % del EBITDA del último año fiscal



Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

5.

Ciberseguridad de los Usuarios de Servicios Prestados por las Entidades del Sistema Financiero Colombiano

Con el fin de elaborar el presente Estudio sobre el estado de la Ciberseguridad en el Sistema Financiero Colombiano, la Secretaría General de la Organización de los Estados Americanos (SG/OEA), además del instrumento ya citado con destino a las entidades financieras, elaboró uno particular con el fin de obtener información sobre los aspectos relacionados con incidentes de seguridad digital (incluidos aspectos de tipos de operaciones financieras realizadas, medios empleados, medidas de seguridad, mecanismos de reporte e impacto) con destino a los clientes (usuarios finales) de servicios financieros de la entidad / institución financiera en Colombia.

En particular, el instrumento para clientes presentó un catálogo de preguntas clasificadas en tres (3) secciones:

- Caracterización de los clientes (usuarios finales)
- Cultura de seguridad digital
- Impacto de los incidentes de seguridad digital

Siguiendo la misma orientación en cuanto a la confidencialidad de la información, la SG/OEA no solicitó información alguna que pudiera ser identificada a nivel personal de ninguno de los clientes, ni se almacenó ningún atributo sobre su localización. Todas las respuestas fueron compiladas, analizadas y distribuidas a nivel agregado, es decir, por bloques temáticos, sin que las mismas se hagan disponibles a persona alguna en detalle.

Durante la aplicación del instrumento, además de las preguntas se ofrecieron conceptos en desarrollo de algunas de las mismas, especialmente para facilitar la verificación de aspectos asociados a cultura de seguridad digital.

Un total de 851 clientes del Sistema Financiero Colombiano hicieron la cumplimentación del cuestionario durante el periodo de publicación del instrumento de recolección de información (tres meses del último cuatrimestre del año 2019) y, a partir de la revisión detallada, se estableció una base de datos con igual número de registros. En este punto es necesario precisar que en la medida en la que el encuestado iba avanzando, podía encontrar preguntas que derivaran en proceder a responder preguntas posteriores o no. Un ejemplo de esto son las relativas a la afectación sobre incidentes cibernéticos, las cuales solo fueron respondidas por aquellos que en la respectiva pregunta habían indicado que habían sufrido un incidente, razón por la cual cada gráfica lleva asociado el número de respuestas obtenidas para la respectiva pregunta.

5.1. Impacto de los incidentes de seguridad digital

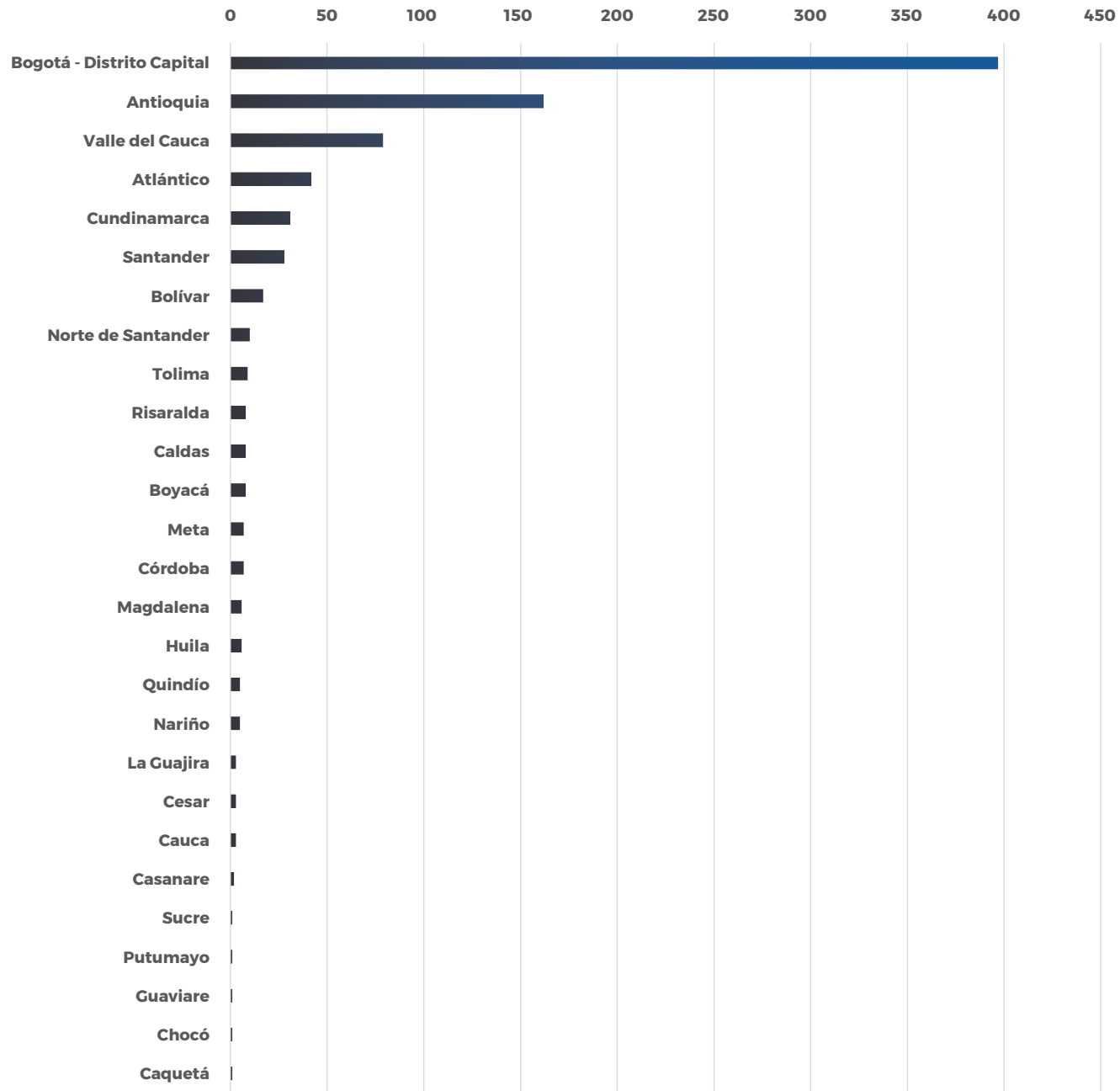
En este componente del estudio, el cuestionario estuvo orientado a establecer las características de los clientes del Sistema Financiero Colombiano que respondieron la encuesta, en aspectos asociados al individuo (tales como departamento y rango de edad), así como en la forma y características particulares de la forma en que los mismos realizan los distintos tipos de transacciones en las entidades / instituciones financieras, como por ejemplo, medios empleados (para revisar transacciones y saldos,

hacer depósitos, retiros, compras y transferencias) y la preferencia de distintos medios digitales, y en el caso de no usarlos, las motivaciones para no emplearlos en la realización de transacciones bancarias.

De un total de 851 respuestas obtenidas a través del instrumento de recolección de información, se establece que donde existe mayor número de usuarios del sistema financiero colombiano que atendieron la encuesta es en la ciudad de Bogotá, Distrito Capital, con un 46,7%, seguido por el departamento de Antioquia con 19%. No obstante, existen usuarios del sistema financiero colombiano que contestaron desde diferentes regiones del país, como se aprecia en la siguiente gráfica.

Gráfica 33.

Ciudad donde se encuentra el cliente



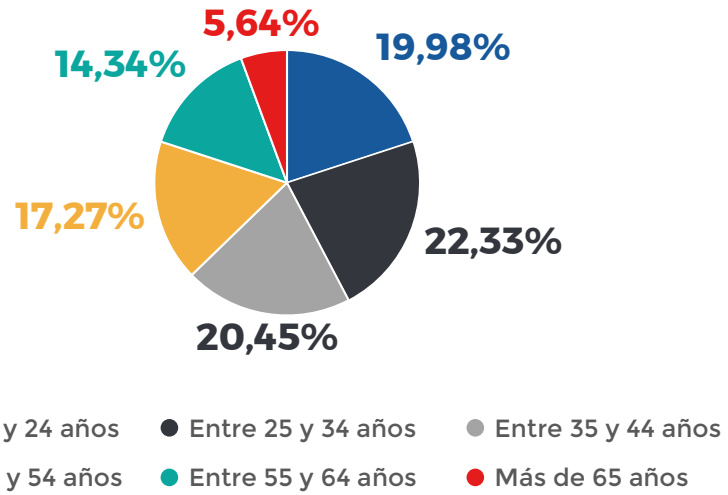
Nota: 851 registros

Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Respecto al rango de edad de los clientes que completaron el cuestionario, se tiene que la mayor representación, correspondiente al 22,33%, se encuentra entre los 25 y 34 años, el 20,45% entre los 35 y 44 años, el 19,98% entre los 18 y 24 años, el 17,27% entre los 45 y 54 años, el 14,34% entre los 55 y 64 años y solo el 5,64% tiene más de 65 años.

Gráfica 34.

Rango de edad del cliente



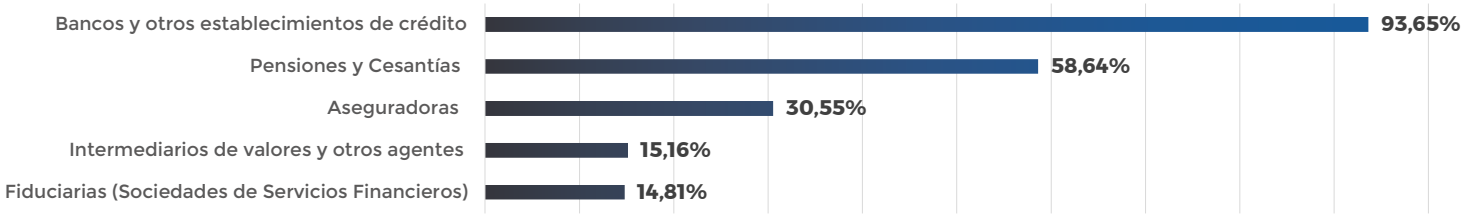
Nota: 851 registros

Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

De los clientes que participaron en el cuestionario se observa que el 93,65% son usuarios de bancos y otros establecimientos de crédito, mientras que son clientes de fondos de pensiones y cesantías un 58,64% y de aseguradoras un 30,55%. Con menor representación se encuentran con un 15,16% los clientes de intermediarios de valores y otros, así como un 14,81% que son usuarios de fiduciarias. Es de anotar que la forma en que se realizó esta pregunta permitía múltiples respuestas, por cuanto un cliente puede ser usuario de diferentes tipos de instituciones.

Gráfica 35.

Clientes de entidades / instituciones financieras



Nota: 851 registros

Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

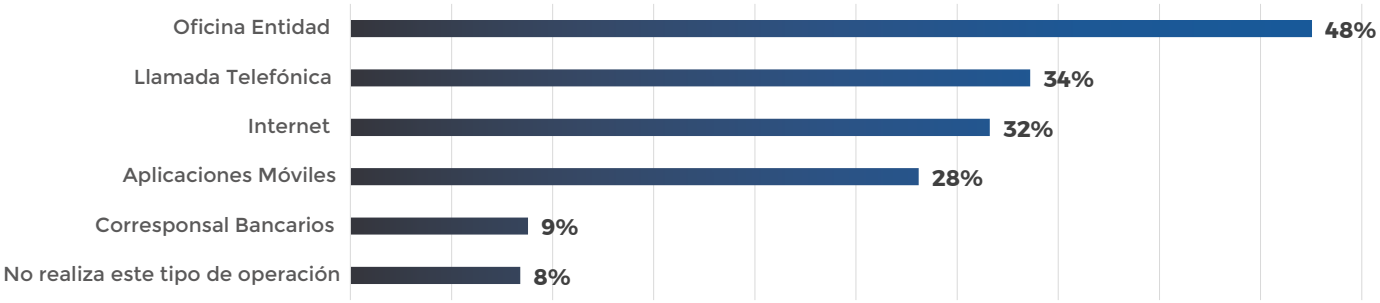
La inclusión financiera se ha incrementado en los últimos años en Colombia. El número de adultos que cuentan por lo menos con un producto financiero subió del 57% (16,7 millones) al 82,6% (28,6 millones), lo que indica que cerca de 12 millones de adultos accedieron a los productos financieros por primera vez. Adicional a lo anterior en cuanto a personas adultas con un producto financiero activo, se pasó del 61,2% al 69,8% entre el cierre de 2014 y junio de 2019. (Asobancaria, Estrategia de inclusión financiera en Colombia 2019-2022, 2019).

Para determinar el nivel de asimilación de los medios electrónicos en las operaciones en estas entidades/instituciones financieras, el estudio incluyó preguntas a efecto de determinar la preferencia respecto de diferentes opciones disponibles. Las preguntas incluyeron tanto canales presenciales como no presenciales.

Al analizar los resultados obtenidos, en cuanto a la preferencia de los medios que utilizan los colombianos para solicitar nuevos productos financieros, se observa que el principal canal para realizar esta actividad es directamente en las oficinas de las entidades con un 48%. El segundo canal más utilizado por los usuarios es las llamadas telefónicas con un 34%. Muy cercano a este porcentaje se ubica el de personas que usan como canal internet con un 32%. Adicional a lo anterior, resulta muy importante el porcentaje de clientes que hacen esta solicitud a través de aplicaciones móviles, alcanzando ya un 28% y que empieza a explotar el potencial de los teléfonos inteligentes como medio que facilita no solo diligenciar información, sino incluso, aportar imágenes o documentos. Es importante anotar que el sistema financiero colombiano cuenta con 6.278 oficinas en las cuales se realizaron más de 267 millones de operaciones; por más de $1.328 billones (Superintendencia Financiera de Colombia, 2019).

Gráfica 36.

Medios para solicitar productos en bancos y otros establecimientos de crédito



Nota: 797 registros

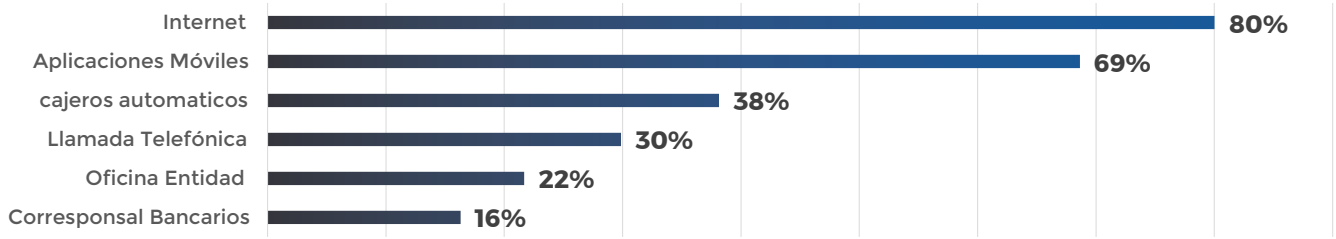
Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

En cuanto a la realización de consultas de saldos disponibles y movimientos (transacciones), resalta como medio preferido para los colombianos, el uso de Internet con un 80%, así como el importante segundo lugar que obtienen las aplicaciones móviles con un 69% de preferencia. Los otros canales, tales como cajeros automáticos, alcanzaron un 38%, el telefónico un 30% y los clientes que informaron realizar estas consultas directamente en la oficina fueron un 22%. Lo anterior demuestra la preferencia de medios virtuales a los presenciales, como puntos transaccionales para los clientes financieros, tal como sucede con los usuarios del sector bancario en América

latina y el Caribe, quienes también refieren su preferencia hacia internet como medio principal para realizar estas operaciones. No obstante, en Colombia se tiene mayor aceptación del uso de aplicaciones móviles para que los usuarios administren sus servicios financieros, diferente a lo reflejado en el estudio para los usuarios de América Latina y el Caribe, quienes ubican el uso de esta tecnología móvil, en un tercer lugar con un 53,88%. En segundo lugar se ubican los cajeros automáticos con un 61,17%, como medio para la realización de consultas de saldos disponibles y movimientos (Organización de Estados Americanos, 2018).

Gráfica 37.

Medios para realización de consultas de saldos disponibles y movimientos (transacciones) en bancos y otros establecimientos de crédito



Nota: 797 registros

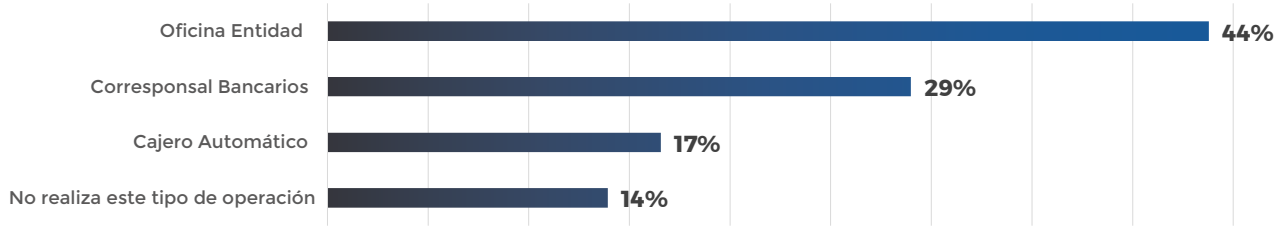
Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Sobre los medios preferidos para depositar cheques o efectivo, los usuarios participantes manifestaron en un porcentaje mayoritario de un 44% el uso de oficinas de las entidades financieras, como se ha desarrollado habitualmente esta actividad, seguido por corresponsales bancarios con un 29% y un 17% que prefiere los cajeros automáticos de su propia entidad / institución financiera. Situación similar se presenta para los usuarios del sector bancario en América Latina y el Caribe, quienes también reportan preferencia significativa para realizar este tipo de transacciones a través de las oficinas de las entidades, aunque en un porcentaje más elevado al que se presenta en Colombia, con un 64,18%. (Organización de Estados Americanos, 2018)

Llama la atención, tanto en el estudio colombiano como en el de América Latina y del Caribe, que se empiecen a posicionar dentro de las opciones medios con apoyo tecnológico como los cajeros automáticos multifuncionales, para realizar este tipo de operaciones. (Organización de Estados Americanos, 2018)

Gráfica 38.

Medios para depósitos en cheques / efectivo en bancos y otros establecimientos de crédito



Nota: 797 registros

Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

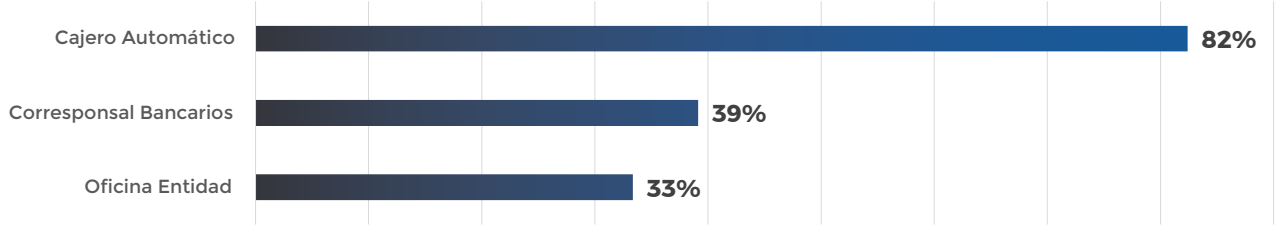
Respecto a los medios empleados por los clientes para hacer retiros en efectivo, se evidencia la utilización preferencial de los cajeros automáticos con un 82%, así como sucede en América Latina y el Caribe con un porcentaje correspondiente al 93,19%. (Organización de Estados Americanos, 2018)

Le siguen los corresponsales bancarios con un 39%, en tercer renglón las oficinas de las entidades bancarias, con un 33%, y tan solo el 2% manifiesta no utilizar ninguna operación para el retiro de su dinero. Llama la atención, en el caso de Colombia, el papel que juegan los corresponsales bancarios, superando incluso el uso de las propias oficinas de la entidad financiera, para realizar operaciones de retiro de dinero.

Según la Superintendencia Financiera de Colombia, los cajeros automáticos, son los canales más utilizados para realizar operaciones financieras. En el primer semestre de 2019, se efectuaron 452.028.751 operaciones: 406.267.383 monetarias por $141,2 billones y 45.761.368 no monetarias, a través de los 16.080 cajeros que operan, así mismo existen 106.344 corresponsales bancarios en los cuales se realizaron 185.499.176 operaciones monetarias por $68,2 billones. Los establecimientos bancarios realizaron 3.901.304.557 operaciones: 1.624.556.160 monetarias por $3.925,2 billones y 2.276.748.397 no monetarias. (Superintendencia Financiera de Colombia, 2019)

Gráfica 39.

Medio para retiros (obtención de dinero en efectivo) en bancos y otros establecimientos de crédito



Nota: 797 registros

Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

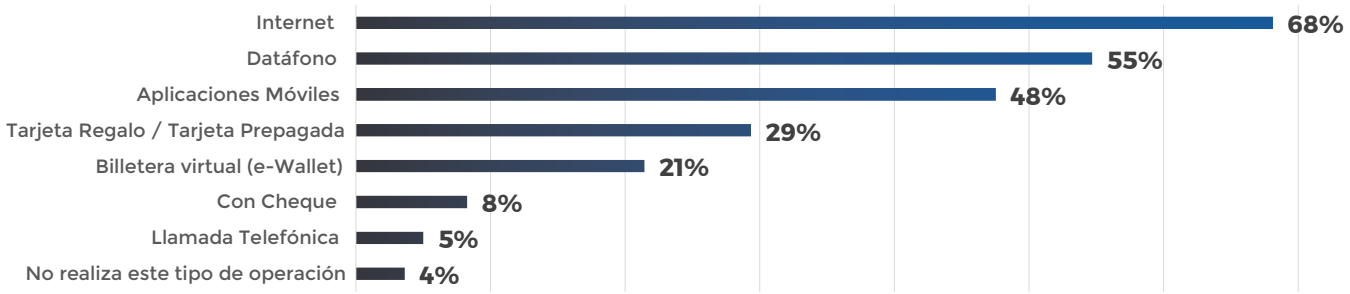
Respecto a los medios empleados para realizar compras, los usuarios participantes del estudio indicaron que mayoritariamente prefieren realizar estas operaciones por medio electrónico en Internet con un 68%, comercio que ha ido creciendo rápidamente, gracias a los beneficios obtenidos al comprar en línea, así como al impacto favorable en la calidad de vida de los usuarios que realizan estas operaciones, ya que se ahorra tiempo, se evitan desplazamientos, se dinamiza la competitividad entre comercios, ofertas y promociones, y se facilita la comparación en precios, y la variedad de productos. (MinTIC, Medición de Indicadores de consumo del Observatorio eCommerce., 2019)

En segundo lugar, el 55% de usuarios, prefieren realizar sus compras utilizando datafono, mientras que el 48% de los encuestados prefieren aplicaciones móviles, el 29% tarjetas de regalo y tarjetas prepagadas y un 21% utilizan la billetera virtual (e-wallet). Ya en un menor porcentaje de tan solo el 8% aparece el cheque como medio de pago de las compras. Así mismo el 5% manifestó que las realiza por medio de llamada telefónica y una minoría del 4% afirmó no realizar este tipo de operación.

A diferencia de Colombia, los usuarios financieros de América Latina y del Caribe, prefieren, el uso de las tarjetas débito y crédito a través de datafonos, para realizar compras, con porcentajes de 77,50% y 72,27%, respectivamente ya sea a través de canales presenciales o virtuales. (Organización de Estados Americanos, 2018).

Gráfica 40.

Medios para realizar compras



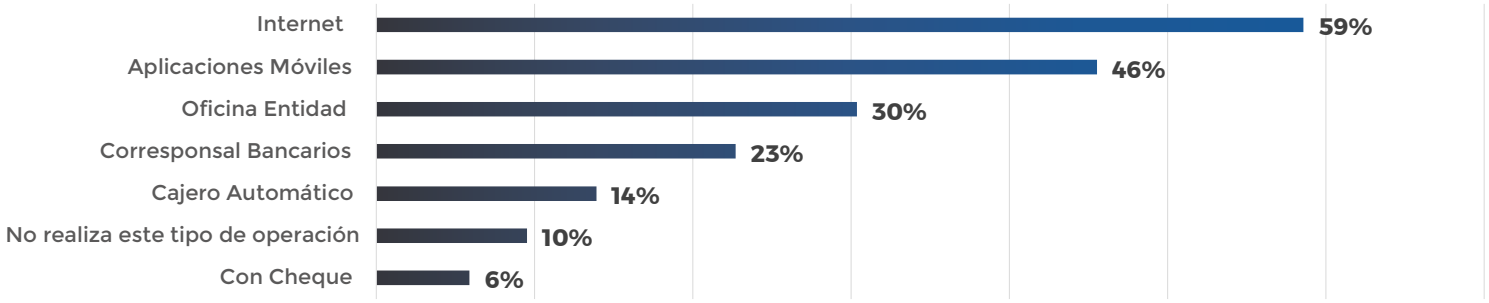
Nota: 797 registros

Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

De acuerdo con los resultados obtenidos, se confirma la preferencia en la utilización de medios no presenciales (digitales) sobre canales presenciales, en este caso para el pago de obligaciones de productos financieros de las entidades. El 59% de los clientes participantes del estudio, indicaron realizar sus pagos a través de una computadora (internet), el 46% mediante aplicaciones móviles, frente a un 30% que aun prefieren hacerlo en oficinas de la entidad / institución financiera, un 23% en corresponsales bancarios, el 14% por medio de cajeros automáticos y, un 6% con cheques.

Gráfica 41.

Medios para pago de productos



Nota: 797 registros

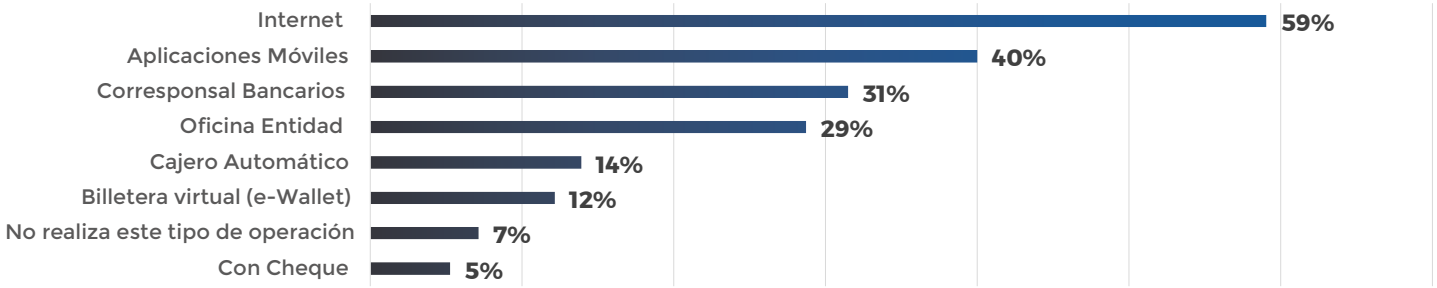
Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

También se aprecia una preferencia en la utilización de medios no presenciales (digitales) para el pago de servicios públicos. El uso de internet arroja un 59% seguido por las aplicaciones móviles con un 40%, corresponsales bancarios con un 31%, las oficinas de forma presencial con un 29%, los cajeros automáticos con un 14% y los cheques con un 5%.

Aquí se resalta como un 12% indica usar billeteras virtuales (e-Wallet) para este propósito, destacando los mecanismos que cada vez más las entidades financieras, empresas de servicios públicos y compañías de comercio generan para facilitar a sus usuarios el pago de sus obligaciones a través del uso de nuevas tecnologías. Actualmente, en Colombia se encuentran 11 billeteras electrónicas (e-Wallet) aproximadamente, entre aplicaciones bancarizadas e independientes (Fintech): Tpaga, Nequi (Bancolombia), Movii, Powwi, Davipay (Davivienda), Rappi Pay (Davivienda y Rappi), Tuya, Billetera Colpatria, Bbva Wallet y Billetera Móvil Bancolombia, por las cuales se pueden realizar diferentes clases de pagos, entre otros el pago de servicios públicos. (La República, 2019).

Gráfica 42.

Medios para pago de servicios públicos o privados en bancos y otros establecimientos de crédito



Nota: 797 registros

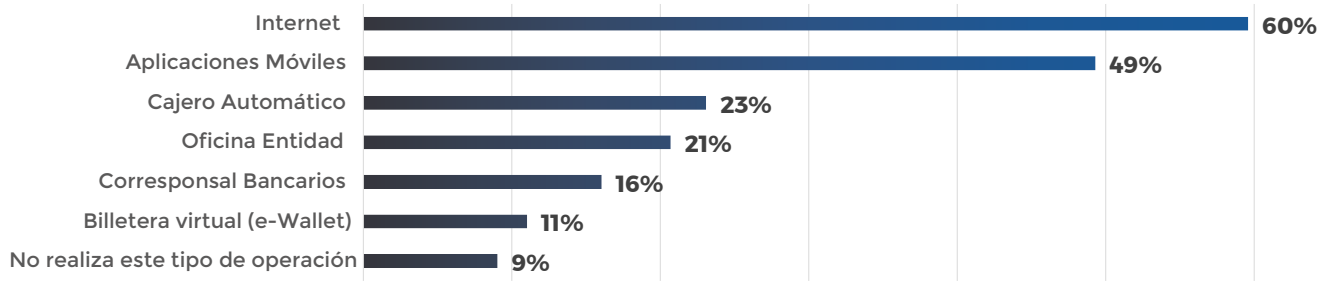
Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

En cuanto a los medios empleados para efectuar transferencias de fondos, los clientes que participaron en este estudio prefieren realizar estas operaciones en gran porcentaje utilizando internet, con un 60%, por delante de aplicaciones móviles con un 49%, cajeros automáticos con un 23%, las oficinas de la entidades bancarias con un 21%, los corresponsales bancarios con un 16% y la billetera virtual (e-wallet) con un 11% .

De acuerdo con el estudio de ciberseguridad desde la perspectiva de los usuarios de las entidades del sector bancario en América Latina y el Caribe, el comportamiento en cuanto a los resultados obtenidos es muy similar a los resultados colombianos, siendo internet el medio comúnmente utilizado para este tipo de transacciones con un 72,42%, frente a un 42,95% que realiza transferencias mediante aplicaciones móviles y un 36,93% que acude directamente al banco, entre otros, lo que evidencia nuevamente la preferencia por medios digitales. (Organización de Estados Americanos, 2018)

Gráfica 43.

Medios de transferencias de fondos en bancos y otros establecimientos de crédito



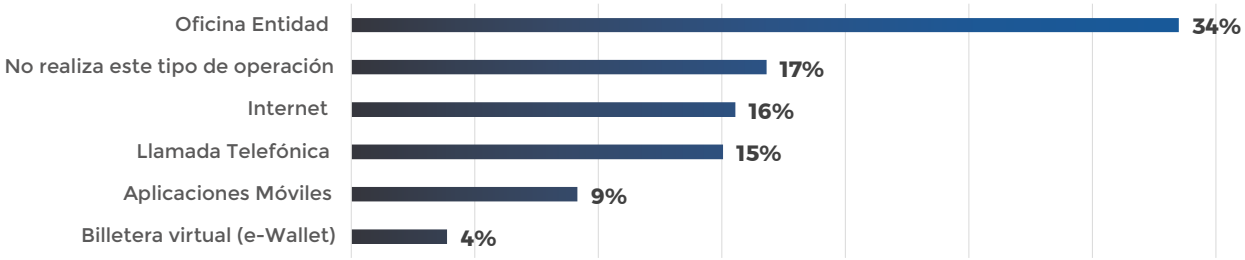
Nota: 797 registros

Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Respecto a los medios para solicitar alguna línea de crédito, los usuarios de este tipo de servicios financieros indican como el más utilizado el que es realizado por los clientes a través de las oficinas de las entidades con un 34%, frente a un 17% que manifiesta no realizar este tipo de operaciones, así como el 16% que prefiere solicitar crédito por internet. Un 15% accede a créditos por llamada telefónica, mientras que un 9% lo hace por aplicaciones móviles y solo un 4% lo realiza por billetera virtual (e-Wallet).

Gráfica 44.

Medios para solicitar créditos en bancos y otros establecimientos de crédito



Nota: 797 registros

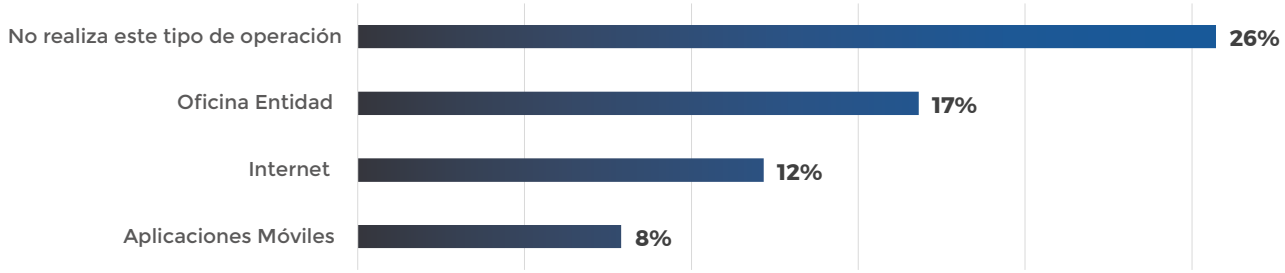
Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Para la realización de inversiones, los clientes prefieren recurrir a la oficina de la entidad con servicio personalizado, que representan un 17%, aunque el porcentaje no está lejos del de los que invierten a través de Internet (12%). La creciente utilización de medios de inversión basadas en medios digitales se debe al esfuerzo y disposición de las entidades financieras en la automatización y nuevas ofertas de tecnología financiera, conocida como fintech, la cual busca prestar los servicios financieros por medio de tecnologías avanzadas y canales de distribución digitales, para que sus usuarios realicen de manera cómoda y segura sus operaciones financieras (Colombiafintech, Transformacion digital , 2019)

Algunos de los usuarios consultados manifiestan haber realizado inversiones utilizando aplicaciones móviles, con un porcentaje de 8%. También cabe resaltar que un 26% manifestó no realizar este tipo de operación.

Gráfica 44.

Medios de transferencias de fondos en bancos y otros establecimientos de crédito



Nota: 797 registros

Fuente: *SG/OEA a partir de información recolectada dde clientes de servicios financieros en Colombia*

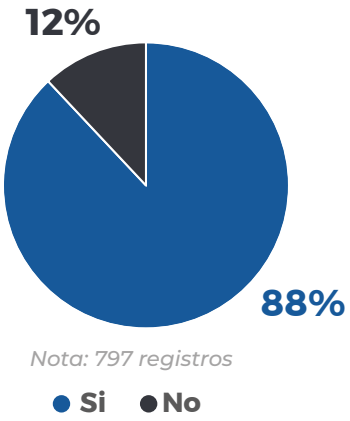
Por otra parte, a modo de pregunta general para valorar la apropiación de los medios digitales, se consultó si los clientes utilizaban éstos para realizar sus transacciones. Como resultado se obtuvo que el 88% sí los utiliza y el 12% no lo hace, igual resultado al obtenido en el estudio de Ciberseguridad: Estado del Sector Bancario en América Latina y el Caribe, con el cual se evidencia que los usuarios de los servicios financieros, continúan evolucionando hacia un consumidor de canales virtuales para sus transacciones. (Organización de Estados Americanos, 2018).

En este sentido, cabe resaltar que el año 2018 representó un hito respecto a la adopción de medios digitales por parte de los usuarios del sistema financiero en Colombia, dado que, por primera vez, el monto de operaciones realizadas por Internet superó al realizado por los clientes en las oficinas. Mientras que el valor de operaciones por Internet representó el 39% del total, el realizado en oficinas fue el 37%, el cual hasta el año 2017 era el canal que más recursos representaba (Superintendencia Financiera de Colombia, 2018).

Por otra parte en el año pasado, según el informe presentado por la Superintendencia Financiera de Colombia, en su reporte correspondiente al primer semestre 2019, el sistema financiero reportó 851.922.003 operaciones realizadas en canal nternet: 250.544.468 de ellas fueron monetarias por $1.687 billones y 601.377.535 no monetarias, lo que muestra como, a medida que transcurre el tiempo, las transacciones a través de medios virtuales se han venido fortaleciendo, ya que los hábitos de los usuarios del sistema financiero colombiano se han ido adaptando de acuerdo a los avances tecnológicos. (Superintendencia Financiera de Colombia, 2019)

Gráfica 46.

Porcentaje de utilización de medios digitales en transacciones en bancos y otros establecimientos de crédito

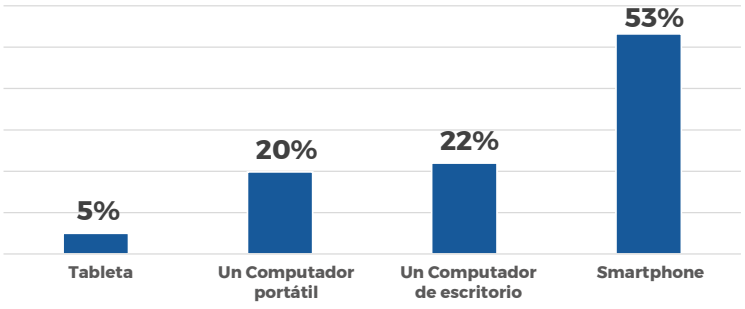


Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

En cuanto a los medios preferidos por los clientes para realizar transacciones digitales, según los resultados obtenidos, se encuentran en primer lugar el teléfono inteligente (smartphone) con un 53%, seguido por el computador de escritorio con un 22%, el computador portátil con un 20% y, por último, las tablets con un 5% de participación. Al comparar con América Latina y el Caribe, se observa que el medio más utilizado en esta región es el computador portátil con un 73,86%, por delante del smartphone con un 62,66% y el computador de escritorio con 45,13%. Cabe destacar que a pesar de que en Colombia el uso del smartphone ocupa el primer lugar de preferencia, el porcentaje es inferior al de toda la región. (Organización de Estados Americanos, 2018).

Gráfica 47.

Medio digital más preferido para realizar transacciones en bancos y otros establecimientos de crédito



Nota: 701 registros

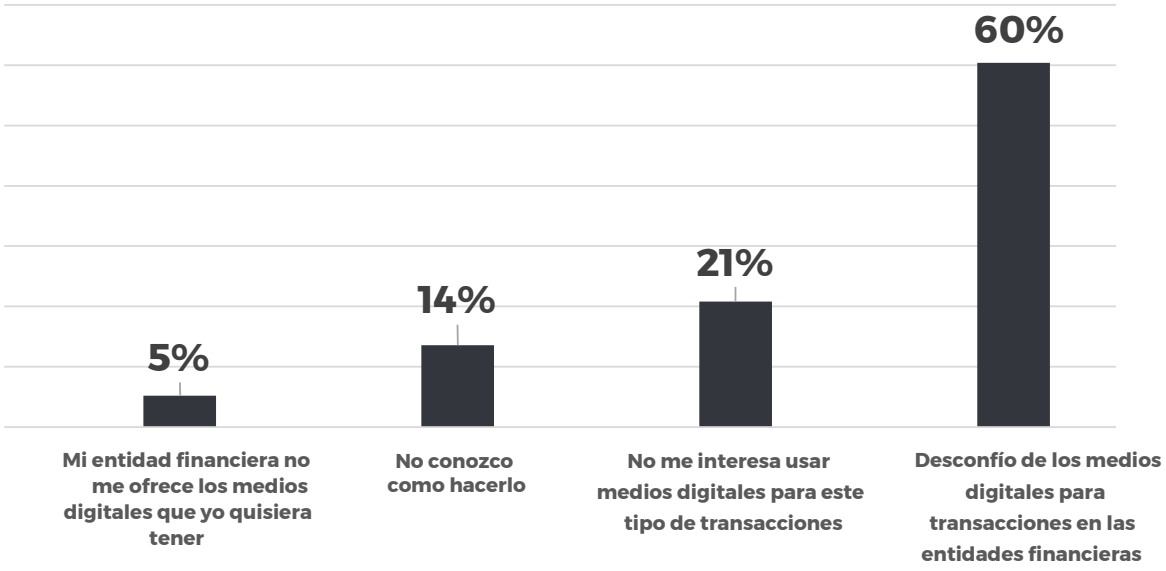
Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Ahora bien, en cuanto a los usuarios del Sistema Financiero Colombiano que indicaron no utilizar medios digitales, se indagó por los motivos por los cuales no los emplean, evidenciando que la razón principal es la falta de confianza por parte de los usuarios 60%, mientras el 21% indicó que no les interesa usar medios digitales para este tipo de transacciones, el 14% manifestó no saber cómo realizar las transacciones y finalmente un 5% de los que respondieron indicaron que la entidad financiera no les ofrece los medios digitales que quisieran tener. De acuerdo con el estudio realizado en América Latina y el Caribe, los motivos expuestos por los usuarios obedecen a las mismas motivaciones y la proporción frente a cada una es similar, ya que en la región el 59,26% desconfían de los medios digitales, seguida por la falta de interés en el uso de medios digitales (27,78%), el desconocimiento de estos (11,11%) y, finalmente, falta de oferta en esos servicios (9,26%). (Organización de Estados Americanos, 2018).

Lo anterior, denota la importancia de fortalecer acciones que incrementen la confianza de los usuarios en estos medios, así como aquellas que resalten los beneficios que trae a los usuarios el uso de servicios de base digital, para elevar su interés.

Gráfica 48.

Razones expuestas por aquellos que no utilizan medios digitales para realizar transacciones en bancos y otros establecimientos de crédito



Nota: 96 registros

Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

5.2. Cultura de Seguridad Digital

En este componente del estudio, se realizaron preguntas orientadas a establecer aspectos relacionados con la cultura en temáticas de seguridad digital de los usuarios de servicios financieros, en asuntos asociados con su conocimiento previo sobre definiciones relacionadas con tipos de incidentes cibernéticos, las medidas de seguridad más empleadas por ellos para prevenir tales incidentes, así como los medios a través de los cuales se mantienen informados de las nuevas formas de ataques y amenazas de seguridad.

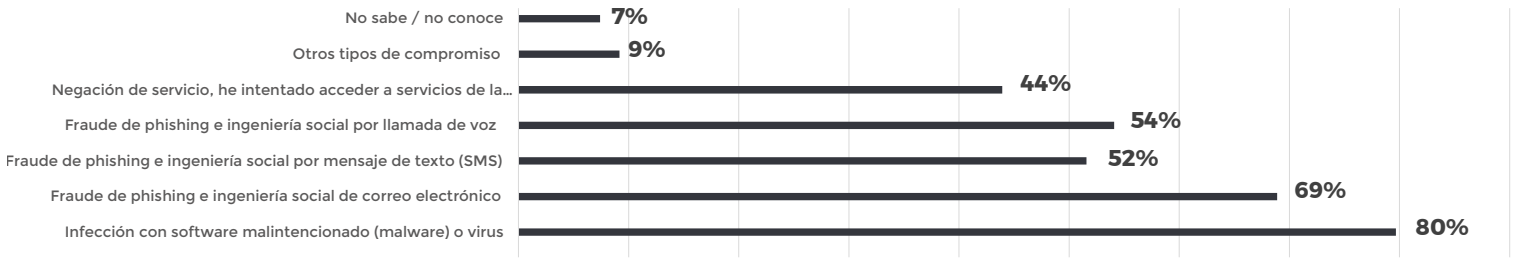
Es importante anotar que en el cuestionario que completaron los encuestados no se ofrecía para esta pregunta ningún tipo de definición, sino que se acudía a lo que los mismos clientes entendían sobre este tipo de conceptos.

Después de que los encuestados indicaron su respuesta sobre los incidentes cibernéticos que creían conocer y de que se les ofrecieran las definiciones reales de los mismos a efecto de validar su nivel de conocimiento, se encontró que un 80% de los encuestados indica conocer la infección con software (malware), un 69% indica conocer sobre fraude de phishing e ingeniería social por correo electrónico, mientras que un 54% y 52% conocen de fraudes de phishing e ingeniería social por voz y mensajes de texto, respectivamente. Un 44% indicó conocer la negación de servicio cuando ha intentado acceder a servicios de la entidad financiera y no funcionan, mientras que un 9% contestó saber del tema en cuanto a otros tipos de compromisos y solo un 7% manifestó no tener conocimiento sobre los tipos de incidentes.

Al comparar con el estudio realizado en América Latina y el Caribe, se obtuvieron resultados similares al estudio realizado en Colombia, en cuanto al conocimiento sobre los incidentes de seguridad en medios digitales. La infección con software malintencionado (malware) alcanzó referencias de un 85,7% de los participantes. Sin embargo, en el estudio regional el incidente cibernético más referenciado fue el fraude de phishing e ingeniería social de correo electrónico, indicado por un 86,2% de los participantes. (Organización de Estados Americanos, 2018).

Gráfica 49.

Incidentes de seguridad en medios digitales conocidos por parte de usuarios de bancos y otros establecimientos de crédito



Nota: 797 registros

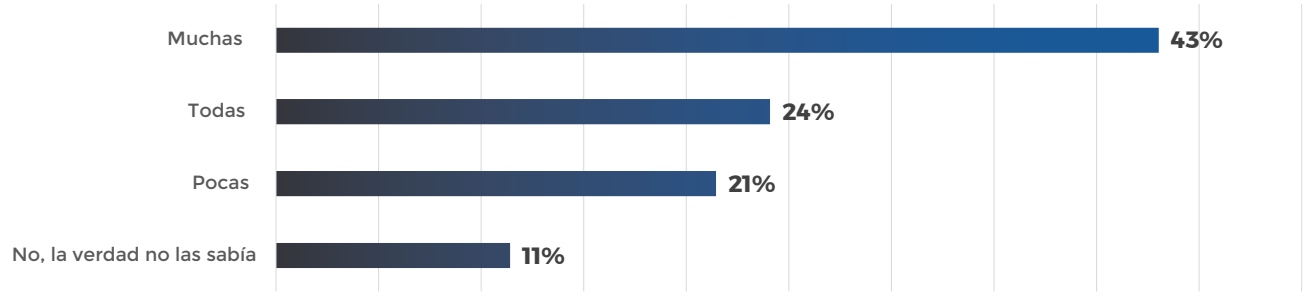
Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Una vez ofrecidas las definiciones reales a los usuarios financieros sobre los incidentes de seguridad en medios digitales, se evidenció que solo un 43% expresó conocer muchas de las definiciones, un 24% manifestó conocer cada una de las definiciones, así como un 21% reportó conocer pocas o algunas de las definiciones y un 11% indicó no conocer ninguna de las definiciones contempladas sobre los distintos tipos de incidentes cibernéticos. Así las cosas, según las respuestas obtenidas, un 67% de los usuarios contestaron que conocían muchas o todas las definiciones referidas a los diferentes incidentes que se pueden presentar, que al ser comparado con lo obtenido en América Latina y el Caribe, el nivel de conocimiento de este tipo de incidentes es superior al colombiano con un 85,3%. (Organización de Estados Americanos, 2018).

Lo anterior, supone la necesidad de generar más información y elevar conciencia sobre los tipos de incidentes cibernéticos a los que están expuestos los usuarios del Sistema Financiero en Colombia.

Gráfica 50.

Nivel de conocimiento frente a las definiciones reales de los distintos tipos de incidentes cibernéticos por parte de usuarios de bancos y otros establecimientos de crédito



Nota: 797 registros

Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Respecto a las medidas implementadas por parte de los usuarios de Bancos y otros establecimientos de crédito participantes en el estudio, para prevenir incidentes de seguridad en medios digitales, algunos usuarios realizan varias prácticas de las planteadas, como se referencia en la siguiente gráfica: el 78% protege sus computadores con antivirus, el 76% solo realiza transacciones desde computadores confiables, mientras el 66% hace uso de contraseñas con condiciones seguras, el 57% habilita notificaciones de transacciones vía mensaje de texto (SMS) y el 55% las recibe por mensaje de correo electrónico; complementan estas prácticas el no acceder a redes Wi-Fi públicas con un 59%, mientras que el 45% usa también antivirus en dispositivos móviles.

Llama la atención que solo el 34% de los clientes use una contraseña diferente para cada servicio, así como el bajo uso de tokens o medios complementarios de autenticación, que solo emplean el 31% de los clientes, mientras que, en la región, esta medida de seguridad alcanzó un 16%.

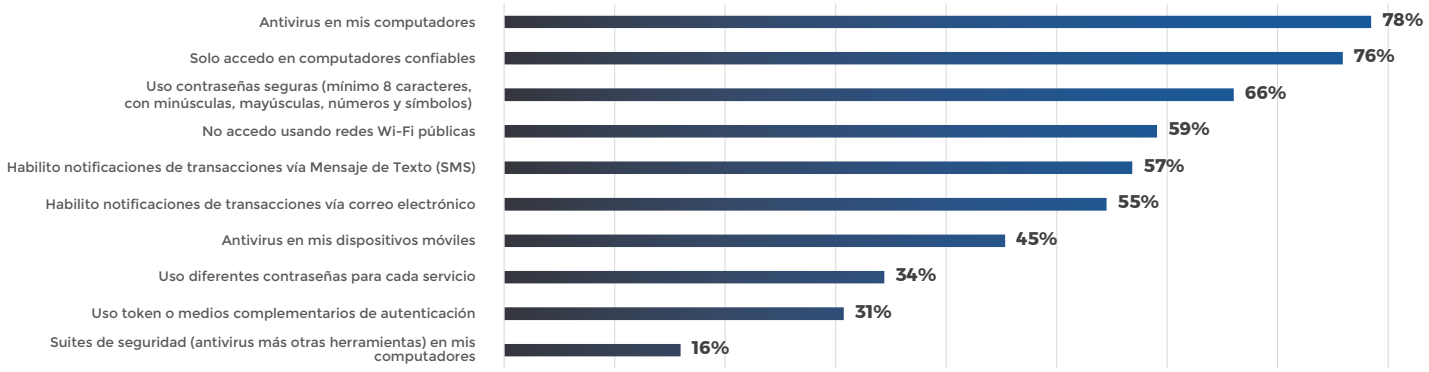
En lo relacionado a medidas, al comparar con el estudio para el sector bancario en América Latina y el Caribe, los usuarios también prefieren como principal medida de seguridad para prevenir incidentes digitales el uso de antivirus en las computadoras con un 84,02%, seguido por otras prácticas de seguridad relacionadas con el acceso exclusivo en computadoras confiables (75,95%),

la habilitación de notificaciones de transacciones vía correo electrónico (62,23%), el evitar el acceso usando redes Wi-Fi públicas (59,79%), el uso de tokens o medios complementarios de autenticación (53,09%) y, finalmente, el uso de antivirus en dispositivos móviles (46,91%) y suites de seguridad (39,69%) (Organización de Estados Americanos, 2018).

Es de anotar que en el estudio realizado en Colombia se ampliaron opciones para especificar medidas, incluyendo aquellas relacionadas con el uso de contraseñas seguras, así como diferentes contraseñas para cada servicio digital.

Gráfica 51.

Medidas de seguridad más usadas por clientes de bancos y otros establecimientos de crédito para prevenir incidentes digitales



Nota: 797 registros

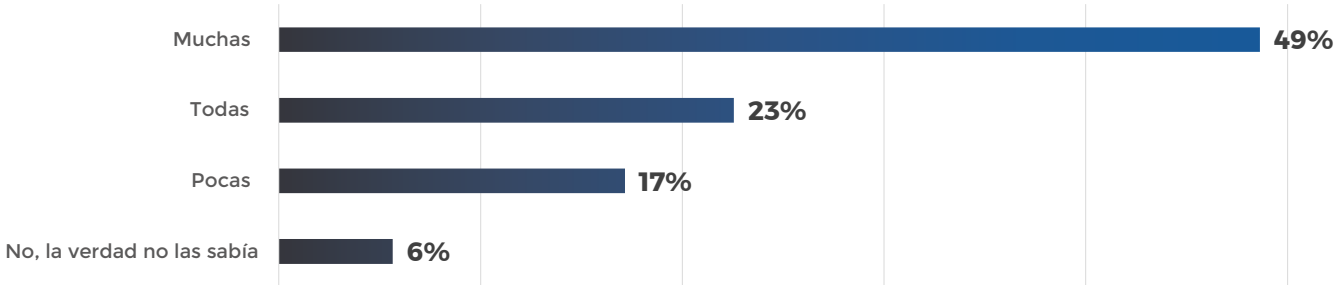
Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Al preguntar a los participantes si conocían las medidas de seguridad indicadas en el punto anterior, un 49% de ellos conocía muchas de las medidas y el 23% afirmó conocerlas todas, solamente un porcentaje mínimo de personas manifiestó no conocer ninguna de estas medidas de seguridad con un 6%.

Respecto al reporte regional, si bien el porcentaje obtenido de personas que manifestaron no conocer ninguna de estas medidas es muy similar (5,67%), contrasta el nivel de conocimiento expresado frente a todas las medidas, ya que este alcanzó un 54,12%, mientras en Colombia es prácticamente un poco menos de la mitad de este valor (Organización de Estados Americanos, 2018).

Gráfica 52.

Conocimiento de las medidas de seguridad para prevenir incidentes de seguridad en medios digitales (varias respuestas posibles) por parte de usuarios de bancos y otros establecimientos de crédito



Nota: 797 registros

Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

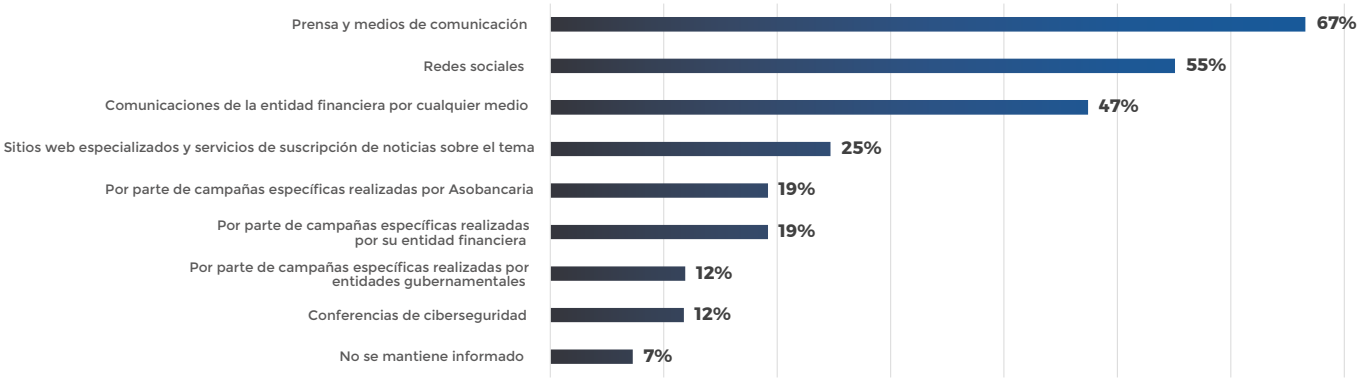
Ahora bien, como ya se ha indicado, debería resultar cada vez más relevante para los usuarios mantenerse informado sobre las nuevas formas de ataques y amenazas de seguridad, dada la dependencia cada vez mayor del entorno digital para la realización de sus transacciones. Al respecto, al consultar a los usuarios sobre las fuentes a las que más acuden para enterarse de estos aspectos, los entrevistados indican que el canal más empleado son la prensa y medios de comunicación con un 67%, seguido de las redes sociales con un 55%, las comunicaciones ofrecidas por las entidades financieras con un 47% y campañas específicas realizadas por las mismas con un 38,19%. Con menor frecuencia se indican sitios web, blogs y sitios especializados con un 25% y las campañas específicas realizadas por Asobancaria y las entidades financieras, ambas con 19%, mientras que los que se informan por campañas de las entidades gubernamentales y conferencias de ciberseguridad son un 12% y solo el 7% manifiestaron no mantenerse informados.

En cuanto a estas fuentes, los resultados difieren de los obtenidos en el informe regional en el que los entrevistados indicaron que los canales más empleados son las noticias en sitios web, blogs y sitios especializados (78,11%), así como mediante las redes sociales (66,73%). También resaltan otras fuentes como conferencias de ciberseguridad (60,14%), noticias de prensa tradicional escrita, noticieros y radio (58,90), listas de correo (44,48%) y campañas de las entidades bancarias (37,19%). (Organización de Estados Americanos, 2018).

Como se desprende de los resultados, aunque un mayor porcentaje de usuarios del sistema financiero en Colombia se informan de las nuevas amenazas de ciberseguridad por campañas de seguridad adelantadas por sus entidades bancarias que en el regional, se evidencia que se requieren aún más esfuerzos para facilitar el desarrollo de conciencia sobre las amenazas con destino al eslabón más débil de la cadena, que es precisamente el usuario. Resalta, en el caso colombiano, que los medios de comunicación tradicionales como los periódicos, la TV y radios locales, sean el principal medio que emplean los usuarios como fuente, lo que supone que este tipo de incidentes está teniendo visibilidad a través de estos canales, mientras que en la región este tipo de medios se ubicó en cuarto lugar. (Organización de Estados Americanos, 2018)

Gráfica 53.

Medios usados por los usuarios de bancos y otros establecimientos de crédito para informarse de las nuevas formas de ataques y amenazas de seguridad de la información



Nota: 797 registros

Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

5.3. Impacto de los incidentes de seguridad digital

Uno de los retos en la evaluación del impacto que tienen los incidentes cibernéticos es determinar el efecto financiero que puede tener la mencionada pérdida de reputación, la cual, en la práctica, se puede traducir en pérdida de clientes que deciden "migrar" a otra entidad / institución financiera por razones como la desconfianza.

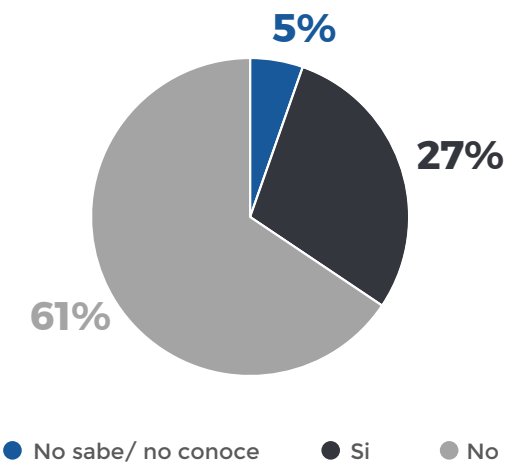
En este componente del estudio, se realizaron preguntas orientadas a establecer el impacto sufrido por los usuarios del Sistema Financiero Colombiano, en aspectos como el tipo de incidentes digitales experimentados, su frecuencia, mecanismos y acciones de reporte, así como impacto generado y su compensación o reparación y otros aspectos de percepción que se consideraron relevantes.

Al indagar a los encuestados sobre si se habían visto comprometidos respecto a la confidencialidad, integridad o disponibilidad de su información o de sus recursos financieros en su entidad / institución financiera, estos respondieron en su mayoría NO haber visto comprometida la confidencialidad, integridad o disponibilidad de su información o sus recursos financieros con un 61%, mientras que el 27% de participantes sí afirmó haber sufrido algún tipo de incidente, y solo el 5% desconoce si fue víctima de este tipo de incidentes.

Esta distribución porcentual es muy similar a la encontrada en el informe regional, en el cual el 62,45% indicó no haber sido afectado, mientras que el 27,30% de participantes sí afirmó haber sufrido algún tipo de incidente, y solo el 10,26% indicó desconocer si fue víctima de este tipo de incidentes (Organización de Estados Americanos, 2018).

Gráfica 54.

Incidente o situación que ha comprometido información personal o recursos financieros en bancos y otros establecimientos de crédito



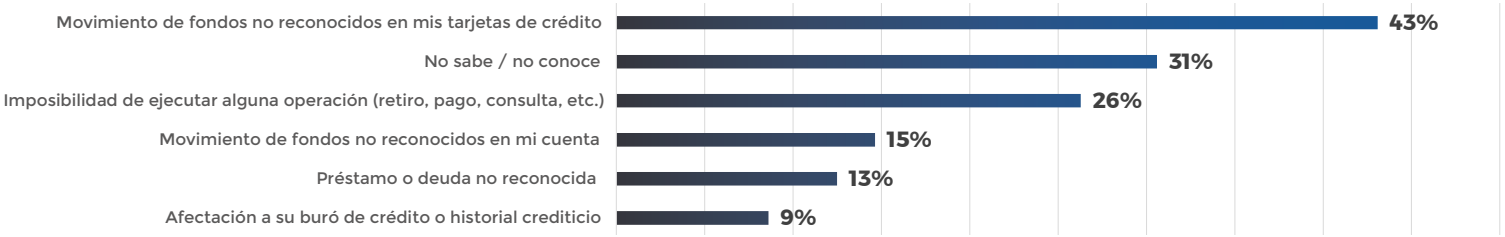
Nota: 797 registros

Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Frente a la pregunta relacionada con circunstancias sufridas, la mayor parte de usuarios de Bancos y otros establecimientos de crédito, esto es, un 43%, indicó la existencia de movimientos de fondos no reconocidos en las tarjetas de crédito. Mientras el 26% señaló la imposibilidad de ejecutar algunas operaciones, el 15% sufrió un movimiento de fondos no reconocidos en sus cuentas, el 13% indicó préstamos o deudas no reconocidas y el 9% afirmó haber sufrido una afectación a su buró de crédito o historial crediticio. Llama la atención que el 31% hayan indicado no saber o conocer si han tenido circunstancias de afectación como las expuestas.

Gráfica 55.

Incidencias cibernéticas ocurridas a usuarios de bancos y otros establecimientos de crédito



Nota: 232 registros

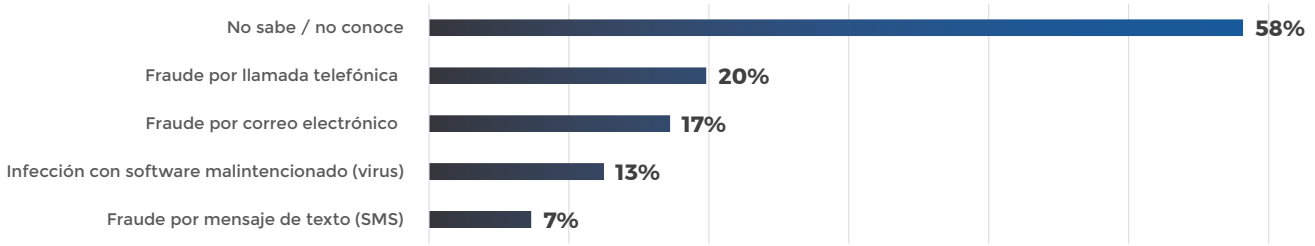
Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Al consultar a los participantes que habían experimentado algún incidente, si conocían sus causas, el 58% indicó no saber, mientras un 20% señaló fraude por llamada telefónica, un 17% afirmó que fue por fraude a través de correo electrónico y un 13% apuntó a la infección con software malintencionado (virus) como la causa, y un 7% indicó al fraude por medio de mensaje de texto.

Uno de los elementos más llamativos sobre las respuestas obtenidas, es que en el estudio regional solo el 2,55% indicó no saber o conocer el origen (Organización de Estados Americanos, 2018), lo que contrasta con el 58% indicado por los encuestados en Colombia. Es decir, no existe una conciencia sobre la causa del incidente cibernético, a pesar de haber sido víctima de éste.

Gráfica 56.

Niveles de conocimiento de las causas del incidente cibernético ocurridos a usuarios de bancos y otros establecimientos de crédito



Nota: 232 registros

Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

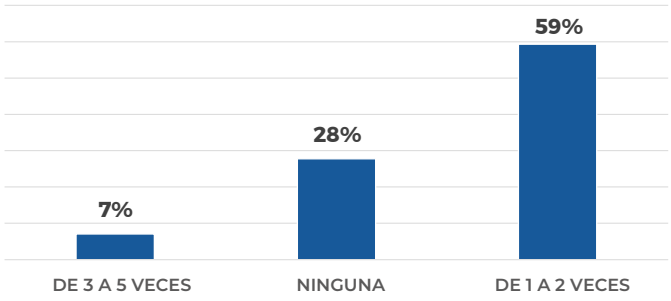
Con respecto a la pregunta sobre la cantidad de veces que los usuarios han sido víctima de incidentes de seguridad en los últimos doce (12) meses, la gran mayoría, esto es un 59% indicó que una a dos veces sufrieron incidentes de esta naturaleza, mientras que un 28% señaló ninguna, y solo un 7% indicó de tres a cinco veces.

En este punto, es importante resaltar que los usuarios del sistema financiero no necesariamente son conscientes de estar siendo afectados por incidentes de seguridad, porque no todos ellos han adoptado mecanismos o medidas de seguridad que entre otros aspectos les permitan ser advertidos de este tipo de situaciones, como por ejemplo las alertas que brindan las suites de seguridad como resultado de la protección en tiempo real, las notificaciones de acceso a plataformas virtuales o las notificaciones de transacciones u operaciones que pueden habilitarse con la entidad / institución financiera, a través de mensajes de texto (SMS) o correo electrónico.

Igualmente, resulta oportuno destacar que en el caso particular de Colombia, existe la Circular Externa 007 de 2018, expedida por la Superintendencia Financiera de Colombia, que exige -entre otros aspectos- que las entidades vigiladas por ese organismo deben informar a los consumidores financieros sobre los incidentes cibernéticos que se hayan presentado y en los que se vieran afectadas la confidencialidad o integridad de su información, al igual que las medidas adoptadas para solucionar la situación (Superintendencia Financiera de Colombia, 2018).

Gráfica 57.

Frecuencia de ocurrencia de incidentes cibernéticos sufridos por usuarios en bancos y otros establecimientos de crédito



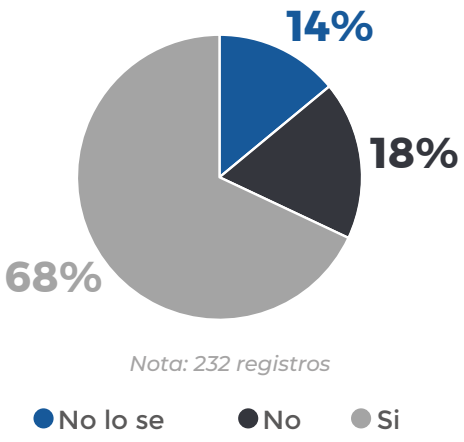
Nota: 232 registros

Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Con relación a los mecanismos y acciones de reporte cuando ocurren incidentes de seguridad, un 68% de los usuarios indicaron que conocen de mecanismos y acciones que las entidades financieras (bancos), ofrecen para reportar incidentes, un 18% de los encuestados consideran que no existen mecanismos para reportar incidentes y un 14% de las respuestas reflejan que no saben si la entidad financiera presta ese servicio.

Gráfica 58.

Conocimiento sobre mecanismos para reportar incidentes en usuarios de bancos y otros establecimientos de crédito



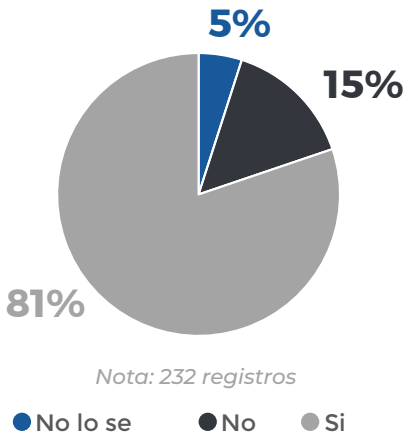
Nota: 232 registros

Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Frente a si los usuarios de Bancos y otros establecimientos de crédito reportaron a las entidades financieras (bancos) incidentes, se evidencia que un 81% sí realizó su respectivo reporte, un 15% no lo reportó y un 5% no sabía cómo realizar el reporte.

Gráfica 59.

Reporte a las entidades financieras del incidente por parte de usuarios de bancos y otros establecimientos de crédito

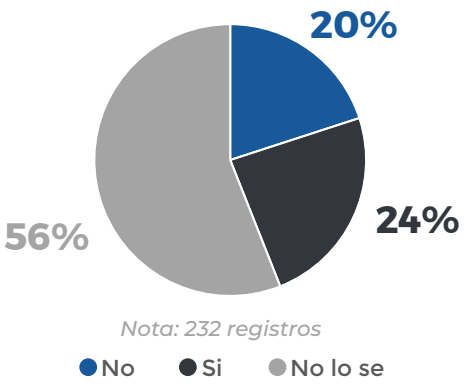


Fuente: *SG/OEA a partir de información recolectada dde clientes de servicios financieros en Colombia*

Una vez abordado el grado de incidentes se les preguntó a los usuarios de bancos y otros establecimientos de crédito, si conocían que en Colombia existiera un mecanismo para reportar incidentes ante un ente gubernamental, a lo cual un 56% manifestó que no sabe/no responde, un 24% dijo que sí y un 20% que no. Esto evidencia que la ciudadanía no conoce los canales de denuncias y tampoco los entes de control, inspección y vigilancia de las entidades financieras del país. En América Latina y el Caribe se evidencia un porcentaje menor conforme a las respuestas, ya que solo el 37,25% afirma tener conocimiento relacionado con un mecanismo para reportar incidentes ante un ente gubernamental, mientras que un 32,03% indica que no existe y un 30,72% no sabe de su existencia (Organización de Estados Americanos, 2018).

Gráfica 60.

Conocimiento sobre mecanismo disponible en el país para reportar incidentes ante un ente gubernamental por parte de usuarios de bancos y otros establecimientos de crédito



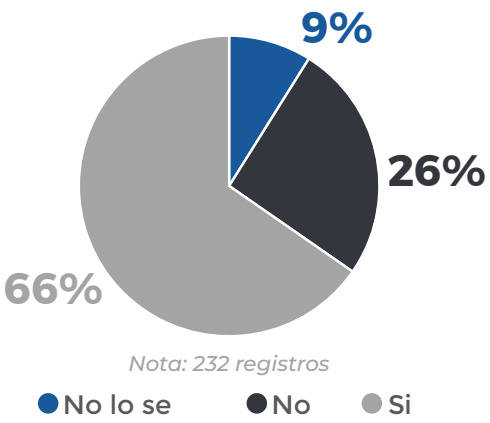
Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Se preguntó a los usuarios que habían indicado haber sido afectados por incidentes de seguridad, si reportaron o recibieron apoyo por parte de autoridades, a lo que el 66% de los clientes manifestó no haber reportado y el 26% sí haberlo hecho.

En la región el escenario es aún menos positivo si se tiene en cuenta el bajo nivel de reporte ante autoridades policiales o judiciales, dado que, de las respuestas obtenidas, solo el 23,53% ha elevado a estas instancias los incidentes que le han afectado. (Organización de Estados Americanos, 2018)

Gráfica 61.

Reporte ante una autoridad policial o judicial del incidente por parte de usuarios de bancos y otros establecimientos de crédito



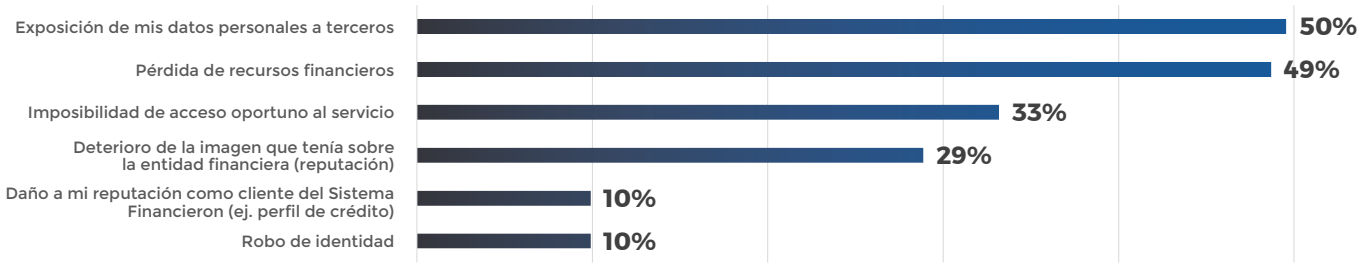
Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Los incidentes cibernéticos que le ocurren a los usuarios de bancos y otros establecimientos de crédito hacen que estos tengan consecuencias. El 50% manifiesta que la exposición de datos personales es la mayor consecuencia identificada, un 49% señala que a raíz del incidente tuvo pérdida de recursos financieros, un 33% se vio afectado para tener acceso oportuno al servicio, un 29% manifiesta un deterioro de la imagen que tenía sobre la entidad financiera, un 10% tuvo como efecto un daño a su reputación como cliente del sistema financiero, como por ejemplo en su perfil de crédito, y el mismo porcentaje obtuvo la afectación de robo de identidad.

La transformación en los servicios financieros hacia un esquema digital, tanto en la oferta de productos y servicios como en la operatividad interna de las entidades financieras, requiere asumir retos importantes en cuanto a la gestión de riesgos que se puedan presentar: protección de datos y el tratamiento de los riesgos cibernéticos, robustez y calidad de la infraestructura digital, fortalecimiento de la ciberseguridad, regulación vigente y asimetría regulatoria frente a las Fintech. (Asobancaria, Gestión de riesgos en el marco de la era digital, 2019)

Gráfica 62.

Consecuencia que produce en los usuarios de bancos y otros establecimientos de crédito ser víctima de incidentes cibernéticos



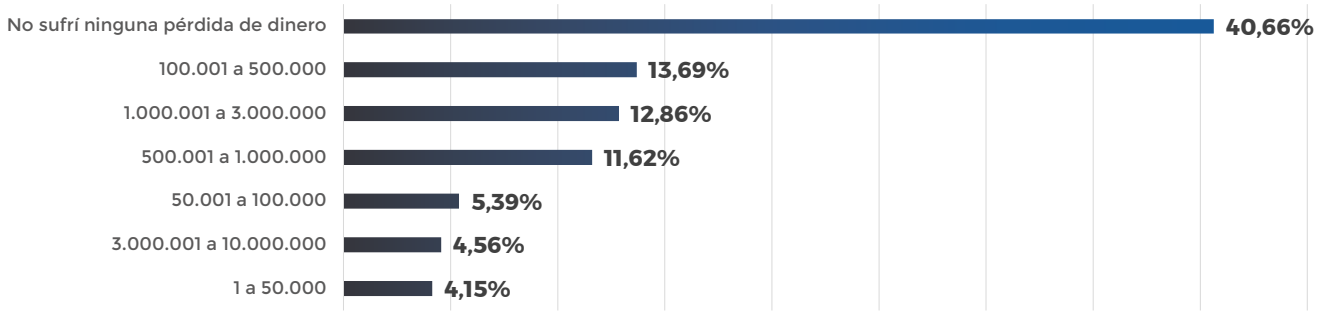
Nota: 232 registros

Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

De acuerdo con lo obtenido de usuarios de Bancos y otros establecimientos de crédito participantes del estudio, un 40,66% manifiesta que no sufrieron pérdida de dinero, un 13,69% perdió entre 100.001 y 500.000 pesos, un 12,86% perdió de 1.000.000 a 3.000.000 de pesos y un 11,62%, de 500.001 a 1.000.000 de pesos.

Gráfica 63.

Rangos de afectación respecto de incidentes cibernéticos que afectaron a usuarios de bancos y otros establecimientos de crédito



Nota: 232 registros

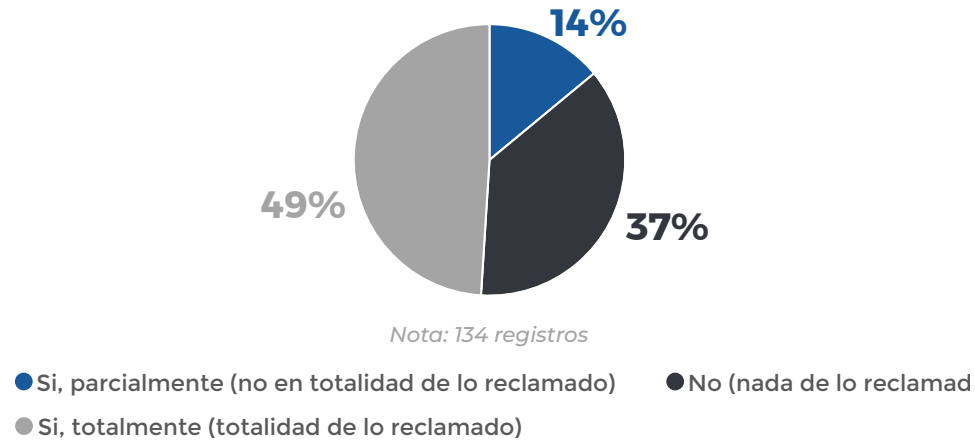
Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Tras la identificación de la afectación sufrida por el incidente, el 49% de los usuarios afectados indicaron que les fue reembolsada la totalidad del dinero que fue objeto del incidente, mientras que un 14% indicó que había sido reparado parcialmente y un 37% manifiesta no haber logrado reparación alguna por el monto reclamado.

En comparación con los usuarios del sector bancario de América Latina y del Caribe, que sufrieron afectación, el dato es muy similar respecto al número de personas que fueron compensadas totalmente por la entidad financiera, con un 44,87%. Un 25,64% indicó haber sido reparado parcialmente y un 29,49% expresó no haber recibido ningún tipo de indemnización (Organización de Estados Americanos, 2018).

Gráfica 64.

Rangos de afectación respecto de incidentes cibernéticos que afectaron a usuarios de bancos y otros establecimientos de crédito



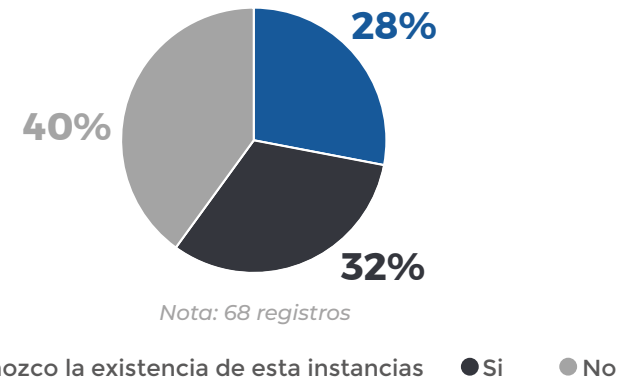
Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Al consultarle a los usuarios de bancos y otros establecimientos de crédito participantes del estudio, si acudieron a instancias diferentes a la entidad con el fin de reportar lo sucedido y obtener apoyo de éstas (como es el caso del Defensor del cliente financiero o la Superintendencia Financiera de Colombia), el 32% de los usuarios indican que sí acudieron a instancias de protección de usuarios, un 40% no acudió a ninguna entidad de protección al usuario y un 28% tiene total desconocimiento de las entidades que prestan ayuda a los usuarios en estos casos.

Estos resultados denotan la necesidad de posicionar aún más, las instancias existentes en Colombia para encontrar apoyo en procesos de reclamación o compensación cuando se es víctima de incidentes cibernéticos.

Gráfica 65.

Concurrencia a alguna instancia de protección al usuario de bancos y otros establecimientos de crédito para reportar incidentes

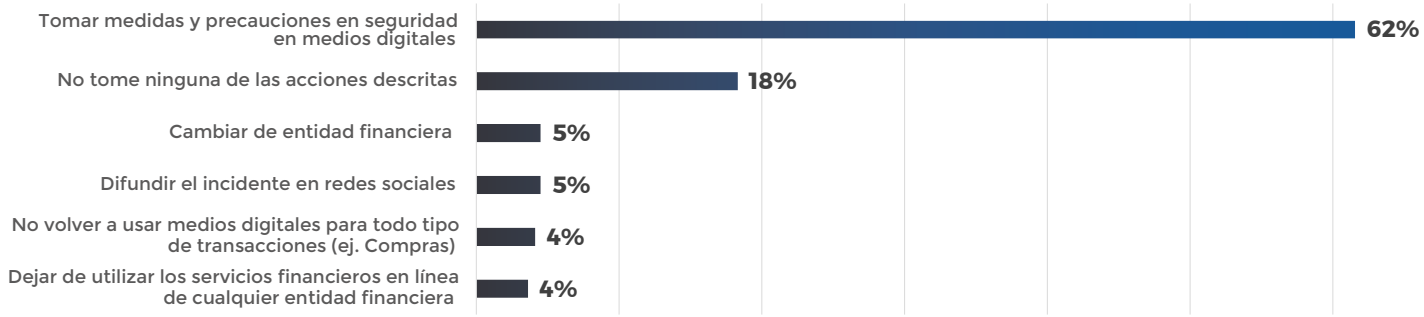


Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Teniendo en cuenta la ocurrencia de incidentes de seguridad en medios digitales, se consultó a los usuarios de bancos y otros establecimientos de crédito si esto los había motivado a tomar acciones concretas al respecto, obteniendo que un 68% de ellos han tomado medidas y más precauciones de seguridad en cuanto al uso de medios digitales, mientras que el 18% no hizo nada diferente. Aunque en porcentajes menores, llama la atención medidas extremas como, por ejemplo, el 5% que indicó que decidió no volver a usar medios digitales para todo tipo de transacciones, y el 4% que informó haber dejado de utilizar los servicios financieros en línea de cualquier entidad financiera, y un más del 5% que tomó la decisión de cambiar de entidad financiera.

Gráfica 66.

Decisiones motivadas en la ocurrencia de incidentes de seguridad en medios digitales en usuarios de bancos y otros establecimientos de crédito



Nota: 797registros

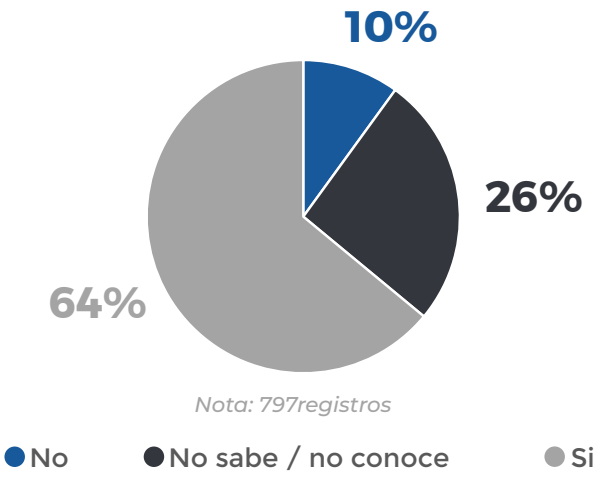
Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Por otra parte, el 64% de los usuarios de bancos y otros establecimientos de crédito, cree que en los últimos doce meses se han incrementado significativamente los incidentes de seguridad a través de los canales digitales, un 26% no sabe no responde, y solo un 10% cree que no se está incrementando.

La situación en Colombia, comparada con el estudio regional en este aspecto, denota una percepción más optimista que la que reflejan las respuestas dadas por los usuarios en la región, dado que un 79,54% indicó que efectivamente sí ha aumentado la presencia de este tipo de incidentes, frente a unos bajos 10,85% y 9,61% que indicaron no percibir ese aumento o desconocerlo, respectivamente (Organización de Estados Americanos, 2018).

Gráfica 67.

Porcentaje de usuarios de bancos y otros establecimientos de crédito que considera que los incidentes de seguridad en medios digitales se han incrementado en los últimos doce (12) meses



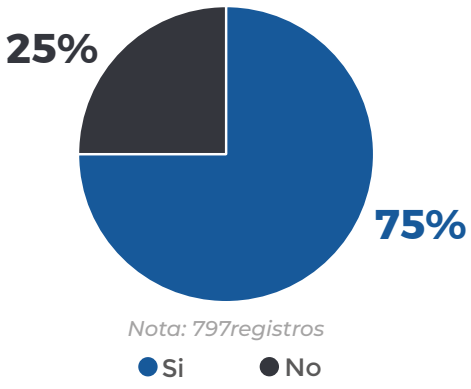
Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

En cuanto a si las entidades financieras están tomando medidas y acciones necesarias para proteger a sus clientes de incidentes de seguridad en los medios digitales, un 75% de los clientes de bancos y otros establecimientos de crédito manifiestan que sí han tomado tales medida y acciones, mientras que un 25% reporta que las entidades no lo han hecho.

La Superintendencia Financiera de Colombia, impartió instrucciones para fortalecer las medidas antifraude, como mecanismos de autenticación de los usuarios, así como estándares de seguridad en las transacciones dentro del ecosistema digital. También ha emitido importantes instrucciones como la generada a través de la Circular Externa 029 de 2019, entre otras varias medidas. (Superintendencia Financiera de Colombia, Circular Externa 029 de 2019 , 2019)

Gráfica 68.

Porcentaje de usuarios en bancos y otros establecimientos de crédito que considera que las entidades financieras están tomando las medidas y acciones necesarias para proteger a sus clientes de incidentes de seguridad en los medios digitales

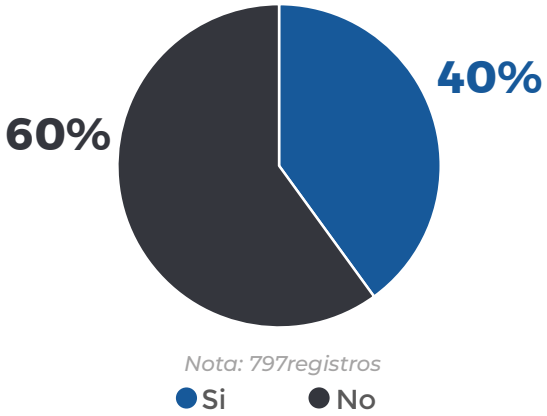


Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

Entre los usuarios de bancos y otros establecimientos de crédito que participaron en este estudio, el 60% considera que las entidades gubernamentales están tomando medidas para prevenir el incremento de incidentes de seguridad a través de canales digitales, no obstante, el 40% considera que no es suficiente lo que se está haciendo.

Gráfica 69.

Porcentaje de usuarios de bancos y otros establecimientos de crédito que considera que las entidades gubernamentales están tomando las medidas y acciones necesarias para proteger a los usuarios del sistema financiero colombiano de incidentes de seguridad en los medios digitales



Fuente: *SG/OEA a partir de información recolectada de clientes de servicios financieros en Colombia*

6.

Recomendaciones de Ciberseguridad para el Sistema Financiero Colombiano

Con base en los hallazgos encontrados, se establecieron un conjunto de recomendaciones de ciberseguridad para el Sistema Financiero Colombiano. Para el efecto se establecen tres (3) grupos objetivo como destinatarios de las recomendaciones: i) las entidades financieras de Colombia, ii) las autoridades y organismos reguladores del sistema financiero y las autoridades justicia del Gobierno de Colombia, y iii) los usuarios de las entidades financieras de Colombia.

6.1. Para las entidades financieras del Sistema Financiero Colombiano

Es importante anotar que estas sugerencias se formulan de manera general y puede que para ciertas organizaciones resulten ser en algunos casos obvias, pero se incluyen teniendo en cuenta la heterogeneidad de entidades financieras en el país y sus diferentes niveles de desarrollo y madurez en los aspectos de seguridad digital. Las recomendaciones se agrupan usando la misma estructura temática abordada por el instrumento de recolección de información usado.

6.1.1. En aspectos de preparación y gobernanza

- Fortalecer y posicionar el CSIRT Financiero actualmente liderado por ASOBANCARIA como instancia para liderar esfuerzos tendientes a fortalecer la gestión de incidentes de seguridad digital en las entidades financieras en Colombia. Esto requeriría de mayores acciones de coordinación entre los diferentes gremios del sector financiero, adicionales a ASOBANCARIA, tales como ASOFONDOS, FASECOLDA, ASOFIDUCIARIAS y AFIC, entre otros; esfuerzo que podría complementarse con la implementación de un modelo de Gobierno ampliado en este CSIRT, para lograr la participación activa de todos los actores que representan entidades e instituciones financieras en el país.

- Independientemente del tamaño de las organizaciones y los esfuerzos de especialización que motiva a parte de ellas a contar con diferentes áreas para gestionar aspectos de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude ocurridos a través de medios digitales, se debe garantizar que las mismas funcionen de manera coordinada y efectiva. En todo caso, es necesario considerar que, conforme al marco regulatorio vigente expedido por la Superintendencia Financiera de Colombia, se establece la necesidad de disponer de una unidad que gestione los riesgos de seguridad de la información y la ciberseguridad.

- Efectuar ejercicios de dimensionamiento de los equipos de trabajo dedicados a los aspectos de seguridad de la información, efectuar evaluaciones de seguridad de los colaboradores, segregar adecuadamente roles y funciones, garantizar procesos de gestión del conocimiento, y establecer mecanismos para elevar la lealtad y retención en los funcionarios apoyándose en el desarrollo del talento humano y considerando planes de incentivos.

- Fortalecer y disponer de mecanismos formales para la selección de proveedores de servicios tercerizados, considerando que podrían requerir el acceso a información sensible, con adecuados criterios de selección y con claras condiciones contractuales que garanticen la protección de datos personales, la confidencialidad, los acuerdos de nivel de servicio y demás requisitos que “blinden” las actividades tercerizadas (ej.: incluir en los contratos que se celebren con terceros críticos, las medidas y obligaciones pertinentes para la adopción y

el cumplimiento de políticas para la gestión de los riesgos de seguridad de la información y ciberseguridad). Esto es especialmente importante en el contexto particular colombiano, dada la regulación existente en cuanto a gestión de riesgos de seguridad de la información y ciberseguridad, y el uso de servicios de computación en la nube, así como las exigencias derivadas de la ley estatutaria en materia de protección de datos personales.

- Establecer mecanismos claros para asegurar el conocimiento de la gestión de riesgos de seguridad de la información (incluyendo ciberseguridad) por parte de las instancias de decisión en las organizaciones (alta dirección y junta directiva) y hacer procesos de sensibilización de manera periódica con la activa participación de sus miembros, a efecto de elevar la prioridad y apoyo a estas temáticas, principalmente en entidades medianas y pequeñas. De conformidad con el marco regulatorio expedido por la Superintendencia Financiera de Colombia, respecto de requerimientos mínimos para la gestión del riesgo de ciberseguridad, las instancias de decisión tienen un papel muy importante como receptores de reportes sobre los resultados de la gestión de riesgos de ciberseguridad, especialmente en la evaluación que haga de la confidencialidad, integridad y disponibilidad de la información, la identificación de ciberamenazas, los resultados de la evaluación de efectividad de los programas de ciberseguridad, así como las propuestas de mejora en materia de ciberseguridad y resumen de los incidentes de ciberseguridad que afectaron la respectiva entidad / institución financiera.

- Efectuar una revisión habitual de mejores prácticas en marcos de gobierno, seguridad y/o estándares internacionales, así como del marco regulatorio local e internacional aplicable a los diversos sectores y entidades financieras, haciendo un proceso de mapeo y priorización para su aplicación. Hacer énfasis especial en el cumplimiento de exigencias como las derivadas de los requerimientos mínimos para la gestión del riesgo de ciberseguridad aplicables a las instituciones financieras en el marco de la regulación colombiana.

- Es de la mayor relevancia llevar a cabo los procesos de adopción y aplicación de marcos regulatorios (local e internacional), mejores prácticas y/o estándares internacionales, con una orientación que vaya más allá de "listas de chequeo" de verificación y que realmente se constituyan en procesos de transformación positiva, orientados por la mejora continua y el fortalecimiento de la cultura de seguridad. El impulso en la adopción, si bien debe garantizar el cumplimiento en materia regulatoria, dadas las disposiciones y exigencias específicas existentes en Colombia, debe también apalancarse en los beneficios que brindaría a la entidad / institución financiera, contar con medidas que fortalezcan su "presencia segura" en el entorno digital.

6.1.2. En aspectos de detección y análisis de eventos de seguridad digital

- Garantizar que la priorización de acciones, procesos y programas de seguridad digital para proteger los sistemas de información críticos de la entidad / institución financiera, corresponden a un plan derivado de las necesidades de adopción y aplicación de marcos regulatorios (local e internacional), mejores prácticas y/o estándares internacionales. Resulta relevante que este plan tenga, como uno de sus focos objetivo, el elevar la resiliencia cibernética y garantizar la regulación vigente en cuanto a requisitos mínimos de ciberseguridad, así como la aplicación

de acciones derivadas de los planes y guías que en materia de protección de infraestructuras críticas se coordinan desde el Ministerio de Defensa Nacional, de manera específica para el sector financiero en Colombia.

- Se debe contar con mecanismos de contrastación de las capacidades propias de detección y análisis de eventos de seguridad en cada entidad / institución financiera, preferiblemente mediante colaboración con equipos de respuesta como el CSIRT Financiero, el ColCERT y otros equipos de respuesta a incidentes públicos o privados, principalmente en las entidades financieras pequeñas que ostentan menos capacidades de detección de este tipo de eventos. Este esfuerzo debe orientarse a validar si las capacidades desarrolladas están logrando predecir o detectar amenazas con el mismo grado de efectividad que lo están haciendo otros equipos de respuesta y transferir conocimiento que fortalezca tales capacidades.

- Elevar el desarrollo de capacidades usando tecnologías digitales emergentes, tales como Big Data, Inteligencia Artificial y sus relacionadas (tales como computación cognitiva y Machine Learning), que tienen un importante potencial en la optimización de recursos destinados a la detección y prevención.

- Extender la capa de detección y prevención a la esfera de la interacción realizada por los usuarios, por ejemplo, incorporando soluciones de detección o prevención que puedan instalar los usuarios en sus dispositivos, de forma voluntaria, lo cual además eleva la percepción de confianza en el servicio por parte de los usuarios.

6.1.3. En aspectos de gestión, respuesta, recuperación y reporte de incidentes de Seguridad Digital

- Garantizar el diseño e implementación de una estrategia de priorización, contención, respuesta y recuperación frente a eventos (ataques exitosos y ataques no exitosos) de seguridad de la información (incluyendo ciberseguridad) contra las entidades financieras, la cual debe articular la participación de terceros, según corresponda a las diferentes etapas, procesos o protocolos asociados, siendo de especial importancia la determinación de responsabilidades y momentos de intervención a cargo de proveedores, escalamiento o intervención de equipos de respuesta externos a la organización (por ejemplo, apoyo e intervención de equipos de respuesta a incidentes del sector y del país, reportes a la Superintendencia Financiero de Colombia y otras autoridades). Es de mucha relevancia que esta estrategia se soporte en el modelo nacional de gestión de riesgos de seguridad digital de Colombia, así como en otros procesos o protocolos nacionales que se dispongan.

- Fortalecer los esfuerzos para determinar la fuente que genera incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad). Se requiere generar una mayor dinámica de confianza entre entidades / instituciones financieras mediante mecanismos de articulación del sector, con entes como el equipo de respuesta a incidentes nacional – ColCERT, a efecto de que se reduzcan los temores por los efectos de los reportes de los incidentes y que se facilite la colaboración para profundizar en las investigaciones para determinar las fuentes de los mismos.

- Implementar mecanismos formales para apoyar las investigaciones de delitos cibernéticos y seguir los protocolos exigidos por las autoridades administrativas y judiciales, así como las mejores prácticas aplicables a la cadena de custodia de la evidencia digital (por ejemplo, que faciliten la cooperación nacional), que resulten relevantes para los procesos investigativos.

- Apoyar iniciativas, alianzas y estrategias que permitan compartir las conclusiones y lecciones aprendidas sobre la gestión de eventos (ataques exitosos y ataques no exitosos), que faciliten la identificación y prevención de delitos, así como el desarrollo de soluciones holísticas para gestionar el riesgo cibernético.

- Capacitar y especializar al personal destinando presupuestos adecuados para realizar procesos de evaluación de la madurez bajo una metodología de seguridad de la información (incluyendo ciberseguridad) de manera periódica por parte de agentes externos idóneos, que permitan establecer las oportunidades de mejora, la priorización y la actualización de los planes y estrategias relacionados. Estos esfuerzos deben soportar las instrucciones expedidas en la materia en cuanto a la promoción de una cultura de ciberseguridad.

- Tomar medidas tecnológicas razonables y apropiadas para proteger la información contra pérdida, mal uso y destrucción cumpliendo constantemente los principios fundamentales de seguridad (confidencialidad, integridad, disponibilidad y trazabilidad), con un alcance conforme con la regulación existente en cuanto a requisitos mínimos de gestión de seguridad de la información y ciberseguridad.

- Establecer, desde el punto de vista de Tecnología y sus procesos, el conjunto de acciones necesarias para garantizar que la información esté protegida durante todo su ciclo de vida, incluyendo como mínimo: i) evaluaciones periódicas de vulnerabilidad para aplicaciones e infraestructura, ii) remediación oportuna de los problemas encontrados en esas evaluaciones, iii) adopción de metodologías de desarrollo seguras para minimizar el riesgo de que se introduzcan nuevas vulnerabilidades en la producción de soluciones para el negocio, iv) adoptar controles para restringir el uso de soluciones sin soporte de fabricante (por condiciones de ciclo de vida de producto) y / o software ilegal, y v) adoptar procesos para realizar la instalación de actualizaciones de seguridad de forma sistemática, entre otros.

- Garantizar la adecuada comunicación hacia los clientes de los mecanismos de reporte de que disponga la entidad / institución financiera en el caso de que resulten víctimas de incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad). Adicionalmente, debe cumplirse lo exigido en la regulación vigente en cuanto a reportar a los consumidores financieros sobre incidentes cibernéticos que hubiesen afectado la confidencialidad o integridad de su información, así como las medidas adoptadas para remediarlo.

6.1.4.En aspectos de capacitación y concientización

- Infundir conceptos y buenas prácticas de ciberseguridad, especialmente con enfoque en aquellas áreas más relacionadas con procesos de innovación y transformación digital en las entidades financieras. Debe hacerse foco en aspectos como el ciclo de vida de desarrollo de software, incluyendo servicios web y apps, que procesan la información confidencial de la

entidad o de los consumidores financieros (desde las etapas iniciales tales como levantamiento de requerimientos hasta las pruebas de seguridad pertinentes y producción), aspectos relativos con la seguridad de la información que permitan mitigar dicho riesgo; aspectos considerados como parte de los requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad en la regulación colombiana.

- Asimilar criterios de diseño de productos y servicios de base digital bajo premisas de "seguridad desde el principio".

- Disponer planes de capacitación con públicos objetivos específicos (empleados internos, insourcing, proveedores, clientes, etc.) que se orienten a elevar la cultura de seguridad digital, el desarrollo de capacidades y la sensibilización (según sea el caso), garantizando su ejecución periódica y estableciendo evaluaciones a efecto de determinar su impacto. Esta capacitación debe incluir el desarrollo de capacidades tempranas en aspectos cibernéticos de forma que se cierre la brecha en cuanto a personal capacitado y se fomente una cultura de seguridad digital.

- Continuar los esfuerzos en campañas de prevención de eventos de i) phishing, ii) software espía (malware o troyanos), iii) ingeniería social y iv) robo de credenciales de clientes de los servicios financieros.

- Aumentar el porcentaje de inversión destinado en las entidades financieras para la generación de capacidades (ej.: formación, concientización, investigación) de la fuerza de trabajo, en especial en el desarrollo temprano de las mismas para cerrar la brecha en el personal ciber capacitado y para aumentar o mantener la fuerza laboral disponible en asuntos de seguridad digital con el fin de desarrollar y fortalecer una fuerza laboral ágil de resiliencia cibernética.

6.1.5. En aspectos relacionados con el impacto de los incidentes de seguridad digital

- Establecer responsabilidades al interior de la entidad / institución financiera para concentrar o centralizar el registro de los incidentes de seguridad digital y determinar los métodos de cuantificación de su impacto económico para la organización.

- Disponer de centros de costo u otros métodos para la determinación de la clasificación de inversiones y gastos recurrentes relacionados con seguridad digital, de forma que pueda evaluarse de manera precisa su peso dentro de los demás rubros a cargo de la organización y su comportamiento.

- Comunicar estratégicamente a la alta dirección y órganos de gobierno que los recursos destinados a seguridad digital no son un costo, sino realmente una inversión y que la protección contra incidentes digitales debe ser parte integral de la estrategia de negocio, dado el alto impacto y repercusión que se pueden derivar de su ocurrencia.

- Invertir en seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales como mecanismo para reducir el impacto negativo como resultado de la materialización de incidentes de seguridad digital. Esto a partir de del cálculo

de la tasa de retorno de las inversiones efectuadas en relación con seguridad digital, mediante una adecuada valoración de los activos de la organización, así como de la estimación de los costos asociados al impacto derivado de posibles incidentes de seguridad digital.

6.2. Para las autoridades y organismos reguladores del sistema financiero y las autoridades de justicia del Gobierno de Colombia

- Continuar con el esfuerzo liderado por el Ministerio de Defensa Nacional respecto a protección del Sistema Financiero, en su calidad de infraestructuras críticas y profundizar en los niveles de dependencia que tienen las entidades financieras del Sistema Financiero Colombiano, de forma que se valore su estado actual, la priorización de la gestión de sus riesgos asociados y en particular el impacto y la afectación que ataques a otras infraestructuras (por ejemplo, telecomunicaciones o energía) podrían tener sobre el mencionado sistema financiero. En este sentido, debe hacerse un seguimiento a los avances adelantados por las organizaciones de este sector, respecto de la implementación de planes y manuales de protección destinados al sector.

- Coordinar esfuerzos con gremios o asociaciones relacionadas con el Sistema Financiero Colombiano para el desarrollo de capacidades en materia de seguridad digital, a través de una agenda con resultados esperados, hitos, recursos y responsables.

- Desarrollar redes de gestión de conocimiento basadas en las capacidades de los diferentes equipos de respuesta de entidades del Sistema Financiero Colombiano, el CSIRT Financiero y del punto focal nacional (ColCERT), incorporando la participación voluntaria de otras instancias del gobierno, sector privado, academia, comunidades técnicas y de profesionales y organizaciones no gubernamentales, interesadas en aportar.

- Evaluar la pertinencia de desarrollar ciber-ejercicios que generen espacios retadores para promover el desarrollo de capacidades de seguridad digital en el Sistema Financiero Colombiano.

- Elevar las capacidades de las autoridades de justicia, respecto al apoyo a la respuesta, investigación y judicialización de cibercriminales cuyas actuaciones afecten el Sistema Financiero Colombiano.

- Establecer y socializar protocolos para la gestión de evidencia digital y garantizar su cadena de custodia, conforme lo exijan los parámetros de las autoridades competentes.

- Actualizar lineamientos, recomendaciones e instrucciones, según sea el caso, derivados de la revisión periódica de las mejores prácticas y/o estándares internacionales aplicables en torno a la seguridad digital, así como del marco regulatorio internacional aplicable al Sistema Financiero Colombiano, y de ser necesario liderar la generación de instrumentos legales complementarios que sean necesarios para su aplicación.

- Al momento de crear o actualizar regulación relacionada con ciberseguridad, adoptar reglamentaciones acordes a marcos ya establecidos por los emisores de estándares internacionales, reduciendo la fragmentación regulatoria, aprovechando las lecciones aprendidas y brindando estabilidad a través de todo el Sistema Financiero Colombiano, procurando la adecuada articulación con otros entes reguladores que puedan tener relación (ej. Superintendencia de Industria y Comercio en materia de datos personales).

- Verificar que las regulaciones estén basadas en principios y sean balanceadas frente a los riesgos que abordan, a fin de maximizar la efectividad, al tiempo que se evitan gastos y cargas innecesarias de control. Para el efecto es pertinente la generación de espacios para la retroalimentación respecto a los beneficios y retos derivados de la implementación de las condiciones exigidas en las circulares y demás instrumentos que constituyen el marco regulatorio del sector.

- Definición de indicadores de gestión de riesgos de seguridad digital, de forma tal que se pueda valorar la efectividad de las medidas adoptadas.

- Establecer una estrategia de aseguramiento de la cadena que conforma la estabilidad del Sistema Financiero Colombiano y desarrollar un marco legal para facilitar la persecución transnacional de los cibercriminales.

- Tener cuidado respecto de la estandarización de los detalles técnicos de los sistemas de control de seguridad y de los negocios, ya que esto podría aumentar la vulnerabilidad en lugar de disminuirla.

- Realizar evaluaciones periódicas a las recientes disposiciones que ha venido estableciendo la Superintendencia Financiera de Colombia, en materia de seguridad de la información y ciberseguridad, a efecto de medir su grado de implementación y la efectividad de las medidas adoptadas.

- Evaluar la efectividad de la obligación para las entidades financieras de reportar de los incidentes de seguridad digital que sufran. Se debe procurar que este reporte tenga como propósito ser base de las indagaciones, investigaciones y trabajo asociado requerido para la comprensión del incidente presentado y su alcance, así como la comprensión del contexto en el que se materializó a efecto de alertar y tomar medidas complementarias por parte de otras entidades financieras y actores del ecosistema.

- Establecer mecanismos de divulgación y socialización de resultados de los avances del CISRT Financiero Colombiano y disponer de ejercicios que pongan en práctica su integración con los demás actores involucrados en los protocolos nacionales de gestión de incidentes, para analizar su desempeño y orientar acciones para su mejora permanente.

- Verificar en las entidades financieras los mecanismos de reporte a través de los cuales sus clientes puedan reportar en el caso de ser víctimas de incidentes de seguridad digital. Evaluar los procesos de divulgación y socialización de éstos y su efectividad.

- Participar activamente en la implementación de una taxonomía común de incidentes cibernéticos, adaptada al modelo nacional de gestión de incidentes que se establezca en el país.

- Implementar mecanismos de intercambio de información entre el sector público y privado que facilite la detección temprana de patrones para permitir a las organizaciones protegerse mejor contra los ciberataques. Implementar mecanismos de intercambio de información tales como Traffic Light Protocol, el cual es ampliamente empleado por la comunidad internacional de Equipos de Respuesta a Incidentes para clasificar qué información se puede compartir. Esto, de la mano de legislación / regulación sólida para el intercambio de información, facilita que los sectores público y privado compartan información sobre amenazas cibernéticas de manera oportuna; permite que el gobierno desclasifique cierta información de amenazas para que pueda ser utilizada por el sector privado para su protección; y proporciona protección fuerte frente a las responsabilidades de las organizaciones que comparten información apropiada de amenazas cibernéticas.

- Promover procesos de transferencia de conocimiento y desarrollo de capacidades mediante colaboración, asistencia y cooperación en el orden local e internacional.

6.3.
Para los usuarios de entidades financieras del Sistema Financiero Colombiano

Los usuarios continúan y seguirán siendo el eslabón más débil de la cadena de la seguridad digital, de allí la relevancia de fortalecer sus capacidades frente a incidentes digitales dirigidos en su contra y promover prácticas que los hagan menos vulnerables. Aquí algunas recomendaciones:

- Evitar el uso de enlaces remitidos por correo electrónico o mensajes de texto, como supuesto canal de acceso a la entidad financiera. Tener en cuenta que dichas entidades nunca hacen solicitudes de información de datos de acceso (credenciales) por este medio, ni por teléfono o mensaje de texto.

- En todos los casos, digitar directamente la dirección del portal de la entidad financiera y determinar la autenticidad del sitio WEB de acceso a la entidad bancaria verificando que la conexión sea segura (debe aparecer una imagen de un candado al lado de la línea de dirección del sitio WEB).

- Establecer mecanismos robustos de autenticación o identificación ante su entidad bancaria, por ejemplo, de múltiples factores de autenticación, como es el caso de los token físicos, las contraseñas de utilización de un solo uso (One-Time-Password), y el uso de teclados virtuales durante el acceso, entre otros. Es importante indagar qué mecanismos de autenticación o identificación ofrece la entidad financiera para brindar más seguridad en la realización de transacciones.

- Utilizar contraseñas fuertes (secuencias de al menos ocho -8- caracteres que combinen letras en mayúsculas, minúsculas, así como números y caracteres especiales) y no usar la misma contraseña para los diferentes servicios en línea, incluidos los de banca electrónica y otros servicios financieros. El hecho de que una contraseña sea expuesta podría facilitar el acceso a operaciones fraudulentas, razón por la cual deben cambiarse periódicamente.

- Evitar almacenar las contraseñas de acceso a entidades financieras de manera automática por parte del navegador en los dispositivos personales. Aunque resulte una opción cómoda porque agiliza el acceso, debe tenerse en cuenta que se podría facilitar el acceso a un tercero en caso de hurto o pérdida del dispositivo.

- Activar notificaciones de transacciones y operaciones con la entidad financiera a través de correo electrónico o de mensajes de texto al teléfono móvil. Verificar qué opciones ofrece la entidad para el envío de estas notificaciones, incluidas las de reporte automático de acceso a través de los canales virtuales.

- Acceder periódicamente con la respectiva cuenta de banca electrónica para verificar las cuentas que se tienen registradas para hacer transferencias a cuentas de terceros de la misma entidad bancaria e interbancarias. Asegurarse de que no existan cuentas registradas diferentes a las que efectivamente se hayan dado de alta.

- Disponer de soluciones antivirus o suites de seguridad (antivirus más otras herramientas) en sus dispositivos, a efecto de poder ser alertado de posibles infecciones con malware o el acceso a vínculos potencialmente riesgosos. Asegurarse de que tanto estas soluciones como los sistemas operativos de los equipos y dispositivos están continuamente actualizados.

- Realizar transacciones financieras únicamente desde computadores confiables, es decir, cuyas condiciones de seguridad sean previamente conocidas. Evitar usar computadores de acceso público y en el caso de que no se tenga otra opción, asegurarse de borrar el historial de navegación, archivos temporales de Internet y apagar la computadora al terminar.

- No realizar transacciones financieras mediante dispositivos conectados a WiFi públicas, dado que no ofrecen las condiciones de seguridad adecuadas para este tipo de operaciones.

- Mantenerse informado de las nuevas formas de ataques y amenazas de seguridad digital. Particularmente, prestar especial atención a las comunicaciones o campañas relacionadas con aspectos de seguridad digital que realice la entidad financiera.

- Frente a cualquier tipo de incidente reportar a la entidad financiera a través del mecanismo establecido para el efecto. Indagar si además del reporte del incidente a la entidad es necesario realizar cualquier otro tipo de gestión o procedimiento, por ejemplo, ante la Policía Nacional de Colombia, como soporte de reclamaciones por fraude, y ofrecer toda la información pertinente sobre el incidente.

Estado de la Ciberseguridad en el Sistema Financiero Colombiano

7.

Bibliografía

Accenture Security. (2017). Building Confidence - Solving Banking's Cybersecurity Conundrum, High performance security report. Obtenido de www.bankdirector.com: https://www.bankdirector.com/files/4515/1982/3582/2018_Risk_Survey_Report.pdf

AMV. (2020). Autoregulador del Mercado de Valores de Colombia. Obtenido de Autoregulador del Mercado de Valores de Colombia: https://www.amvcolombia.org.co/acerca-de-amv/

Asobancaria, Estrategia de inclusión financiera en Colombia 2019-2022. (2019). Obtenido de https://www.asobancaria.com/wp-content/uploads/semana-economica-edicion-1206_min.pdf

Asobancaria, Gestión de riesgos en el marco de la era digital. (2019). Obtenido de https://www.asobancaria.com/wp-content/uploads/semana-economica-edicion-1204.pdf

BANCO DE LA REPÚBLICA. (2020). Banco de la República de Colombia. Obtenido de Banco de la República de Colombia: https://www.banrep.gov.co/es/funciones

Bankdirector. (2018). 2018 Risk Survey. Obtenido de www.accenture.com: https://www.accenture.com/t20170419T051104Z__w__/us-en/_acnmedia/PDF-49/Accenture-Building-Confidence-Solving-Bankings-Cybersecurity-Conundrum-Info.pdf#zoom=50

BDO. (2017). Cyber Security in Banking Industry. Our perspective. Obtenido de www.bdo.in: http://www.bdo.in/getmedia/b478e1ec-a9a3-4afe-997a-3aed7d190164/Cyber-Security-in-banking-industry.pdf.aspx?ext=.pdf&disposition=attachment

BID & FELABAN. (2014). PYME y Bancos en América Latina y el Caribe. El "Missing Middle" y los Bancos - Séptima Encuesta 2014. Obtenido de PYME y Bancos en América Latina y el Caribe. El "Missing Middle" y los Bancos - Séptima Encuesta 2014: https://www.felaban.net/archivos_publicaciones/archivo20150702202150PM.pdf

Capgemini. (2017). Top 10 Trends in Banking – 2017. Obtenido de www.capgemini.com: https://www.capgemini.com/wp-content/uploads/2017/07/banking_trends_2017_web_version.pdf

Cisco. (2018). Reporte Anual de Ciberseguridad CISCO 2018. Obtenido de www.cisco.com: https://www.cisco.com/c/es_co/products/security/security-reports.html#~stickynav=3

Colombiafintech, Transformacion digital . (2019). Obtenido de https://www.colombiafintech.co/novedades/transformacion-digital-del-sector-financiero-oportunidad-del-pais

Ernst and Young . (2018). Global banking outlook 2018 - Pivoting toward an innovation-led strategy. Obtenido de www.ey.com: http://www.ey.com/Publication/vwLUAssets/ey-global-banking-outlook-2018/$File/ey-global-banking-outlook-2018.pdf

Felaban. (2018). Informe Trimestral Económico Bancario Regional FELABAN, Edición No. 9 / 30 de abril de 2018 Cifras con corte a diciembre de 2017. Obtenido de www.felaban.net: https://www.felaban.net/archivos_publicaciones/archivo20180509104600AM.pdf

Global Knowledge. (2017). 2017 IT Skills and Salary Report. A comprehensive Study from Global Knowledge. Obtenido de mindhubpro.pearsonvue.com: https://mindhubpro.pearsonvue.com/v/vspfiles/documents/2017_Global_Knowledge_SalaryReport.pdf

ISACA. (2017). State of Cyber Security 2017 - Resources and Threats. Obtenido de cybersecurity.isaca.org: https://cybersecurity.isaca.org/static-assets/documents/State-of-Cybersecurity-part-2-infographic_res_eng_0517.pdf

ISACA. (2018). State of Cybersecurity 2018 - Contours of the Skills Gap. Obtenido de cybersecurity.isaca.or: https://cybersecurity.isaca.org/state-of-cybersecurity

Kaspersky Lab. (17 de Febrero de 2017). Informe de amenazas financieras: Cada segundo un ataque de phishing apunta al robo de su dinero. Obtenido de Kaspersky Lab: https://latam.kaspersky.com/about/press-releases/2017_informe-de-amenazas-financieras-cada-segundo-un-ataque-de-phishing-apunta-al-robo-de-su-dinero

La República. (2019). La República, internet-economy, billeteras virtuales. Obtenido de La República, internet-economy, billeteras virtuales: https://www.larepublica.co/internet-economy/hay-mas-de-10-billeteras-virtuales-en-el-mercado-2928189

MINHACIENDA. (2020). Ministerio de Hacienda y Crédito Público de Colombia. Obtenido de Ministerio de Hacienda y Crédito Público de Colombia: https://www.minhacienda.gov.co/webcenter/portal/AcercadelMinisterio/pages_misinyvisin

MinTIC, Medición de Indicadores de consumo del Observatorio eCommerce. (2019). Obtenido de https://www.mintic.gov.co/portal/604/articles-98220_Inf_eCommerce.pdf

Office of Financial Research. (2017). Cybersecurity and Financial Stability: Risks and Resilience. Obtenido de www.financialresearch.gov: https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf

Organización de Estados Americanos. (2018). Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. Washington, USA: OEA.

Ponemon Institute e IBM. (6 de Julio de 2018). Cost of a Data Breach Study. Obtenido de Cost of a Data Breach Study: https://www.ibm.com/security/data-breach

Price Waterhouse Cooper. (2017). Top financial services issues of 2018. Obtenido de www.pwc.se: https://www.pwc.se/sv/pdf-reports/finansiell-sektor/top-financial-services-issues-of-2018.pdf

PwC. (Junio de 2018). PwC's 2018 Digital Banking Consumer Survey: Mobile users set the agenda. Obtenido de PwC Financial Services : https://www.pwc.com/us/en/financial-services/publications/assets/pwc-fsi-whitepaper-digital-banking-consumer-survey.pdf

Secretaría de Comunicaciones y Transporte y OEA. (2019). Estudio Hábitos de los usuarios en ciberseguridad en México. México: SCT-OEA.

SUPERFINANCIERA. (2020a). Superintendencia Financiera de Colombia. Obtenido de

Superintendencia Financiera de Colombia: https://www.superfinanciera.gov.co/inicio/nuestra-entidad/acerca-de-la-sfc-60607

SUPERFINANCIERA. (2020b). Superintendencia Financiera de Colombia. Obtenido de Superintendencia Financiera de Colombia: https://www.superfinanciera.gov.co/publicacion/11268

Superintendencia Financiera de Colombia. (2018). Informe de operaciones y transacciones Junio-diciembre 2018. Obtenido de Informe de operaciones y transacciones Junio-diciembre 2018: https://www.superfinanciera.gov.co/descargas/institucional/pubFile1036463/informetransacciones1218.docx

Superintendencia Financiera de Colombia. (2018). Superintendencia Financiera de Colombia. Obtenido de https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/10097769/f/0/c/00

Superintendencia Financiera de Colombia. (2019). Informe de operaciones primer semestre 2019. Obtenido de https://www.superfinanciera.gov.co/descargas/institucional/pubFile1039567/informetransacciones0619.docx

Superintendencia Financiera de Colombia, Circular Externa 029 de 2019 . (2019). Obtenido de https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/10102439/dPrint/1/c/0

Symantec . (2017). Internet Security Threat Report - Financial Threats Review 2017, An ISTR Special Report. Obtenido de www.symantec.com: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pd

The Financial Brand. (6 de Agosto de 2018). Mobile banking features digital security. Obtenido de The Financial Brand: https://thefinancialbrand.com/74044/mobile-banking-features-digital-security/

URF. (2020). Unidad de Proyección Normativa y Estudios de Regulación Financiera de Colombia. Obtenido de Unidad de Proyección Normativa y Estudios de Regulación Financiera de Colombia: http://www.urf.gov.co/webcenter/portal/urf/pages_ai/quinessomos

v. (2018). Revitalizing privacy and trust in a data-driven world - Key findings from The Global State of Information Security® Survey 2018. Obtenido de www.pwc.com: https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf

World Bank Group. (2018). Financial Sector's Cybersecurity: Regulations and Supervision. Obtenido de documents.worldbank.org: http://documents.worldbank.org/curated/en/686891519282121021/pdf/123655-REVISED-PUBLIC-Financial-Sectors-Cybersecurity-Final-LowRes.pdf

World Economic Forum. (2018). The Global Risks Report 2018, 13th Edition. Obtenido de www3.weforum.org: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

ANEXO 1.
Información de la muestra de entidades financieras del Sistema Financiero Colombiano

Cuadro 16.

Información del Sistema Financiero Colombiano teniendo en cuenta reportes de la Superintendencia Financiera de Colombia

		MUESTRA				
		Grande	Mediano	Pequeño	Total	%
Establecimientos Bancarios	Establecimiento de Crédito	5	5	3	**13**	**18%**
Compañías de Financiamiento			3	2	**5**	**7%**
Corporaciones Financieras				2	**2**	**3%**
Sociedades Fiduciarias	Sociedades de Servicios Financieros		5	9	**14**	**19%**
Sociedades Administradoras de Pensiones y Cesantías			4		**4**	**5%**
Compañías de Seguros de Vida, de Seguros Generales y Sociedades de Capitalización	Entidades Aseguradoras y Sociedades de Capitalización	1	13	13	**27**	**37%**
Comisionistas de Bolsa	Comisionistas de Bolsa		3	5	**8**	**11%**
TOTAL GENERAL		6	33	34	**73**	**100%**

		ACIVOS DE LA MUESTRA A 31DIC2018				
		Grande	Mediano	Pequeño	Total	%
Establecimientos Bancarios	Establecimiento de Crédito	361,91	34,42	3,51	**399,83**	**82,6%**
Compañías de Financiamiento			4,25	1,88	**6,13**	**1,3%**
Corporaciones Financieras				12,23	**12,23**	**2,5%**
Sociedades Fiduciarias	Sociedades de Servicios Financieros		1,44	0,79	**2,24**	**0,5%**
Sociedades Administradoras de Pensiones y Cesantías			5,95		**5,95**	**1,2%**
Compañías de Seguros de Vida, de Seguros Generales y Sociedades de Capitalización	Entidades Aseguradoras y Sociedades de Capitalización	3,15	18,54	34,12	**55,81**	**11,5%**
Comisionistas de Bolsa	Comisionistas de Bolsa		0,23	1,46	**1,69**	**0,3%**
TOTAL GENERAL		365,05	64,83	53,99	**483,87**	**100%**

billones de $

		UTILIDAD DE LA MUESTRA A 31DIC2018				
		Grande	Mediano	Pequeño	Total	%
Establecimientos Bancarios	Establecimiento de Crédito	7,56	0,34	0,03	**7,93**	**64,3%**
Compañías de Financiamiento			0,05	0,03	**0,08**	**0,6%**
Corporaciones Financieras				1,66	**1,66**	**13,4%**
Sociedades Fiduciarias	Sociedades de Servicios Financieros		0,20	0,15	**0,36**	**2,9%**
Sociedades Administradoras de Pensiones y Cesantías			0,64		**0,64**	**5,2%**
Compañías de Seguros de Vida, de Seguros Generales y Sociedades de Capitalización	Entidades Aseguradoras y Sociedades de Capitalización	0,06	0,62	0,92	**1,60**	**13,0%**
Comisionistas de Bolsa	Comisionistas de Bolsa		0,03	0,04	**0,07**	**0,6%**
	TOTAL GENERAL	7,62	1,88	2,83	**12,33**	**100%**

billones de $

		UNIVERSO		
		Numero de Entidades	Activos a 31Dic2018 ($bill)	Utilidad a 31Dic2018 ($bill)
Establecimientos Bancarios	Establecimiento de Crédito	26	627,27	9,73
Compañías de Financiamiento		6	15,44	1,86
Corporaciones Financieras		14	13,25	0,11
Sociedades Fiduciarias	Sociedades de Servicios Financieros	28	3,16	0,55
Sociedades Administradoras de Pensiones y Cesantías		4	5,95	0,64
Compañías de Seguros de Vida, de Seguros Generales y Sociedades de Capitalización	Entidades Aseguradoras y Sociedades de Capitalización	45	76,37	1,84
Comisionistas de Bolsa	Comisionistas de Bolsa	20	3,87	0,12
	TOTAL GENERAL	**143**	**745,30**	**14,85**

billones de $ *billones de $*

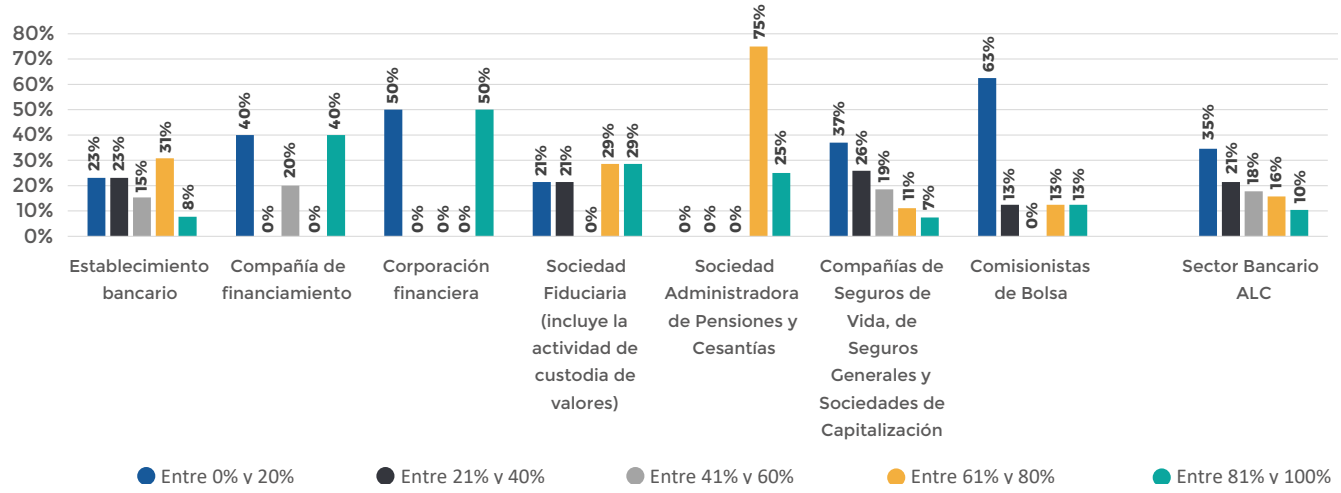
		REPRESENTATIVIDAD DE LA MUESTRA		
		Numero de Entidades	Activos a 31Dic2018 ($bill)	Utilidad a 31Dic2018 ($bill)
Establecimientos Bancarios	Establecimiento de Crédito	50%	64%	82%
Compañías de Financiamiento		83%	40%	4%
Corporaciones Financieras		14%	92%	1492%
Sociedades Fiduciarias	Sociedades de Servicios Financieros	50%	71%	65%
Sociedades Administradoras de Pensiones y Cesantías		100%	100%	100%
Compañías de Seguros de Vida, de Seguros Generales y Sociedades de Capitalización	Entidades Aseguradoras y Sociedades de Capitalización	60%	73%	87%
Comisionistas de Bolsa	Comisionistas de Bolsa	40%	44%	55%
	TOTAL GENERAL	**51%**	**65%**	**83%**

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

ANEXO 2.
Análisis comparativo entre sectores del Sistema Financiero Colombiano

Gráfica 70.

Porcentaje de operaciones que se realizaron por medio de canales digitales – Comparación entre sectores

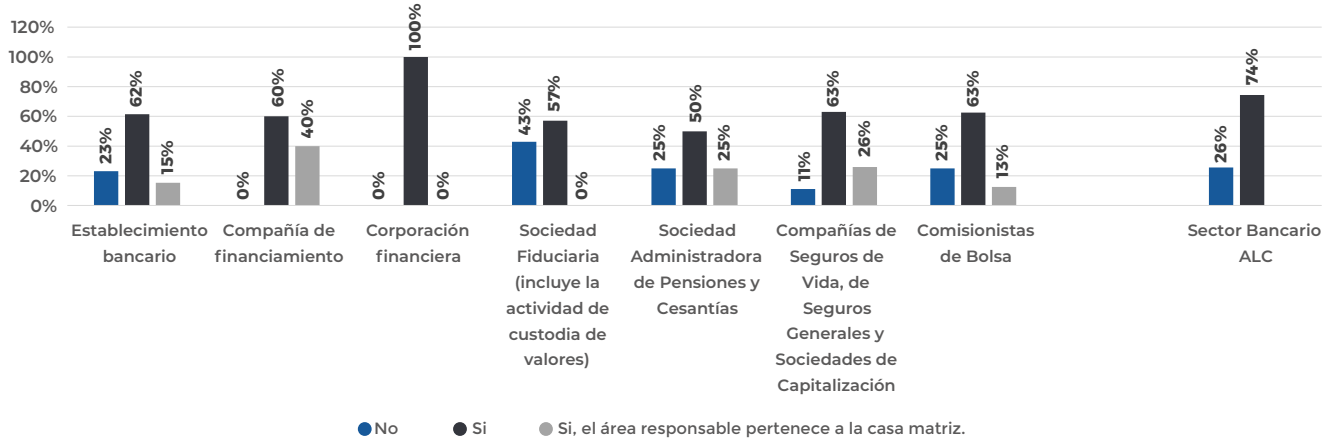


Nota: 73 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 71.

Área única responsable de la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude – Comparación entre sectores

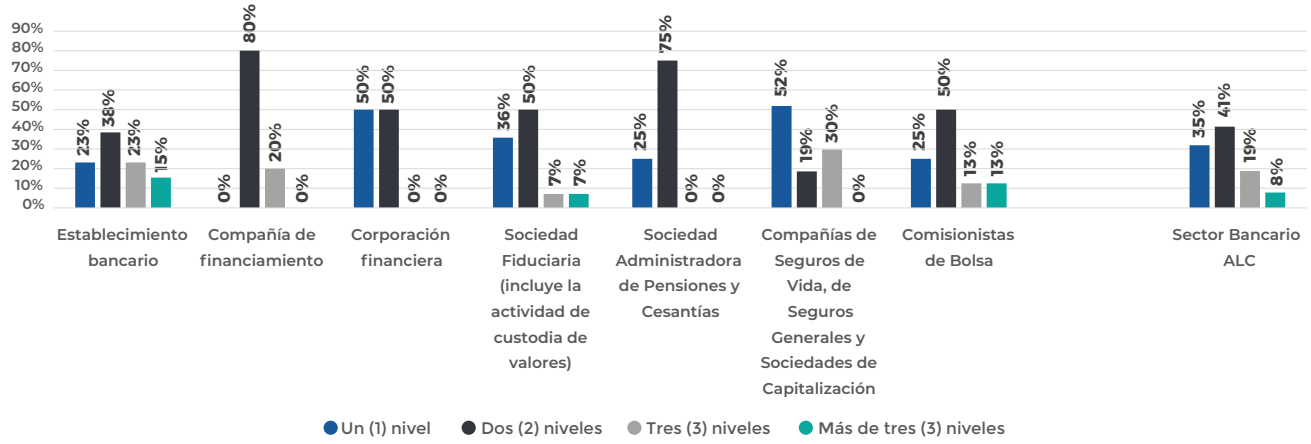


Nota: 73 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 72.

Número de niveles jerárquicos que hay entre el CEO y el máximo responsable de la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude – Comparación entre sectores

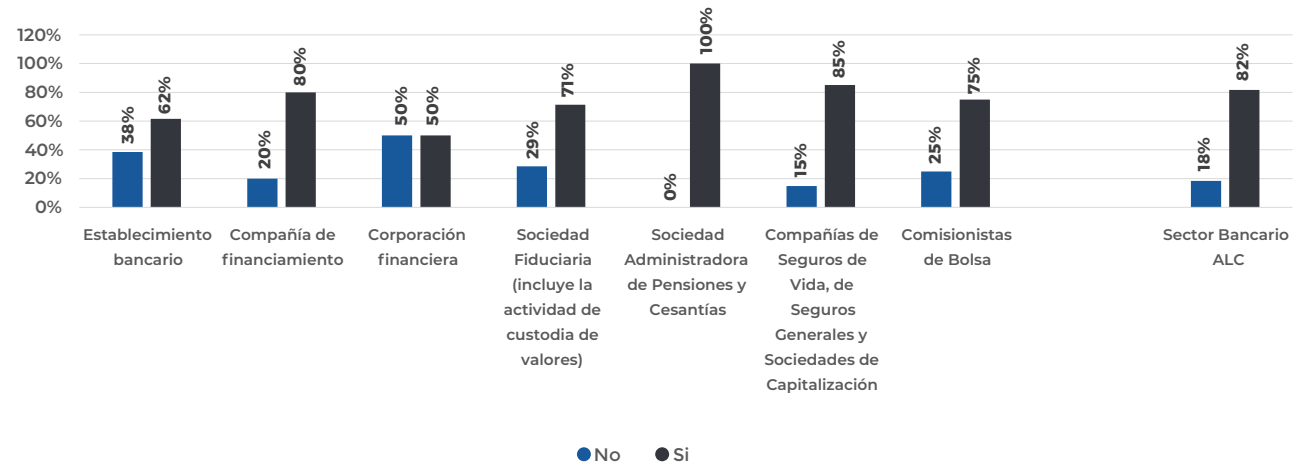


Nota: 73 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 73.

¿Se considera adecuado que el equipo que manejan procesos asociados a la seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales creciera en el corto plazo? – Comparación entre sectores

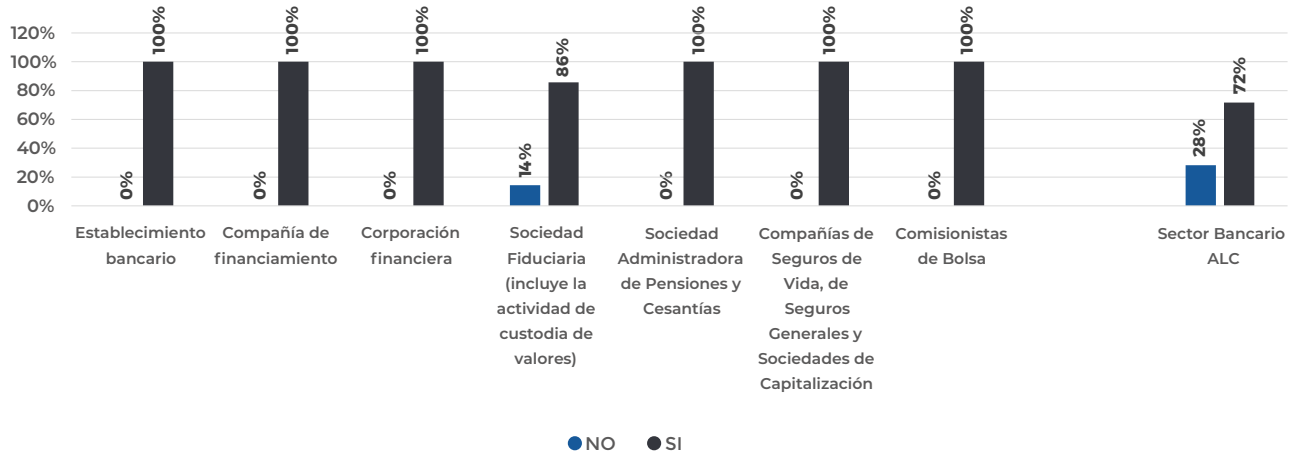


Nota: 73 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 74.

¿La Junta Directiva recibe reportes periódicos acerca de riesgos de seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales? – Comparación entre sectores

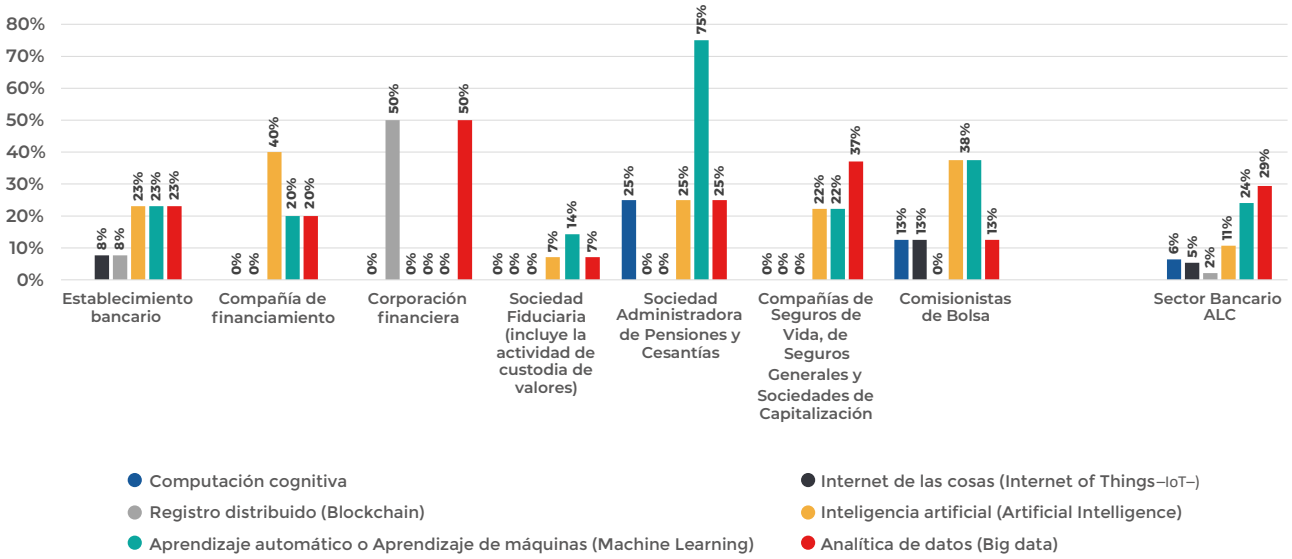


Nota: 73 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 75.

Tecnologías digitales emergentes aplicadas a herramientas, controles o procesos de seguridad digital en la entidad financiera – Comparación entre sectores

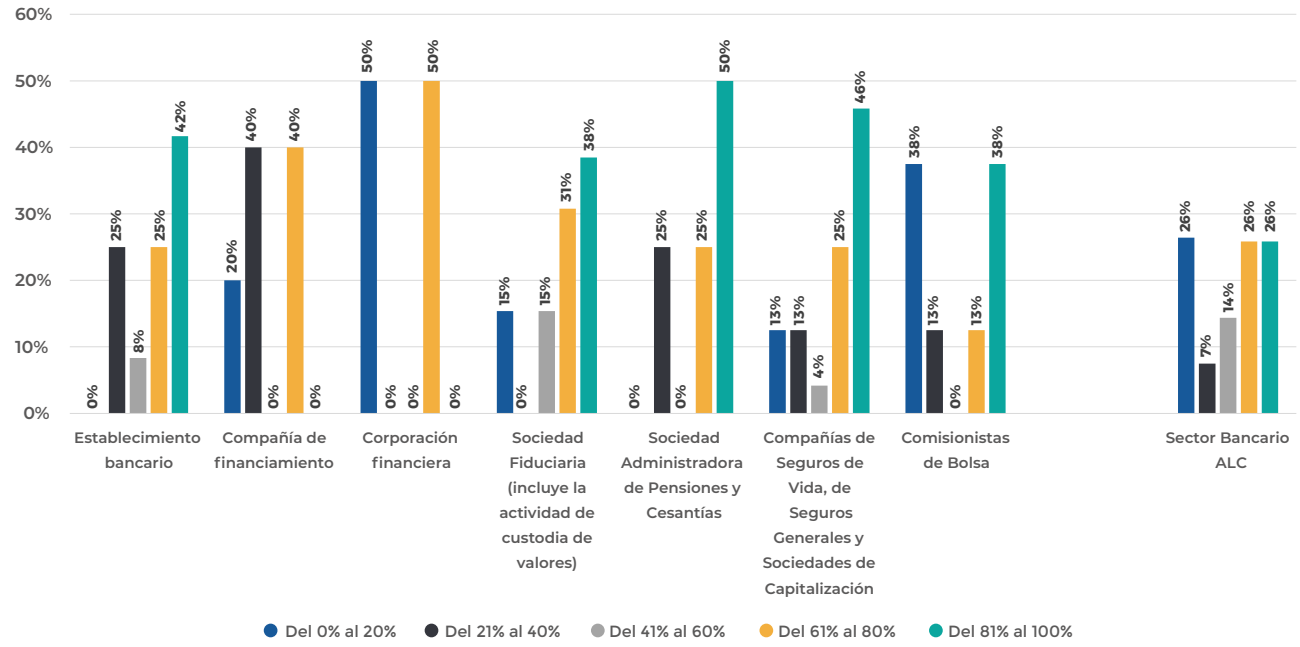


Nota: 68registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 76.

Porcentaje de eventos (ataques exitosos y ataques no exitosos) detectados mediante sistemas operados por la entidad financiera (incluyendo los servicios provistos por la casa matriz) – Comparación entre sectores

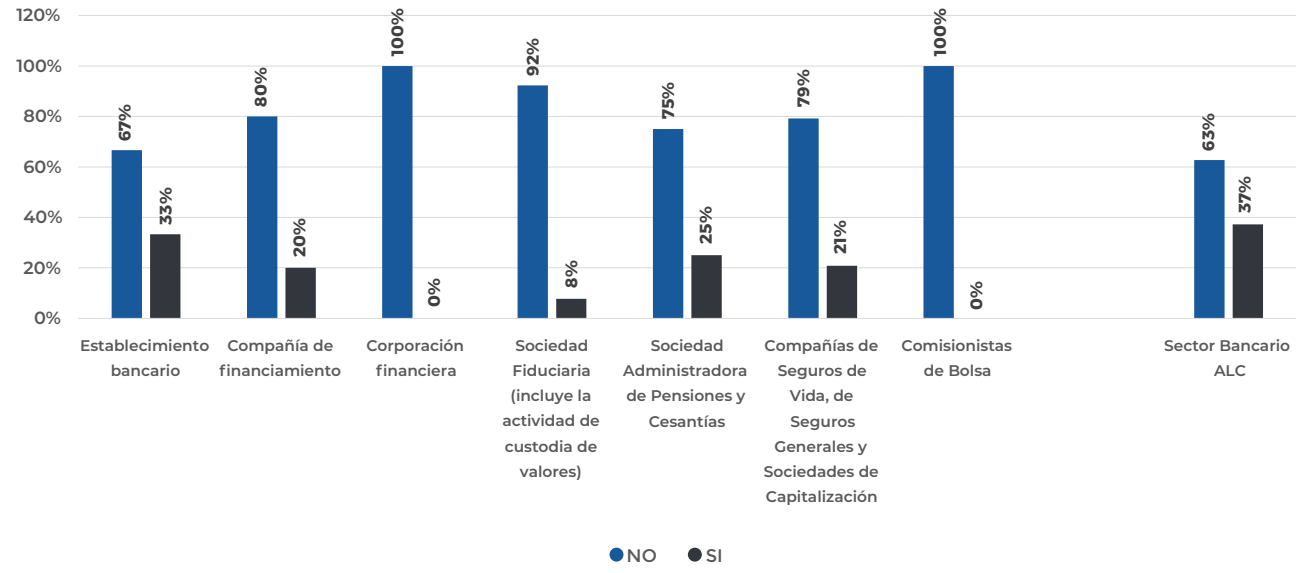


Nota: 68registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 77.

¿La entidad financiera fue víctima de incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad) durante los últimos doce meses? – Comparación entre sectores

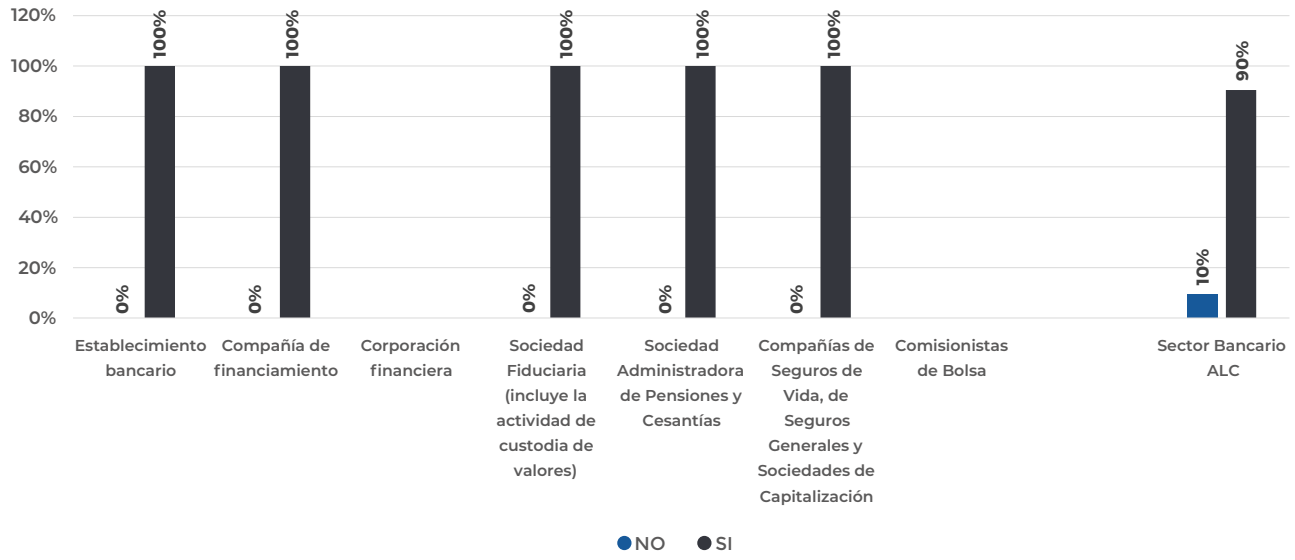


Nota: 68registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 78.

¿La entidad financiera a la cual usted pertenece investigó la fuente que generó dichos incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad)? – Comparación entre sectores

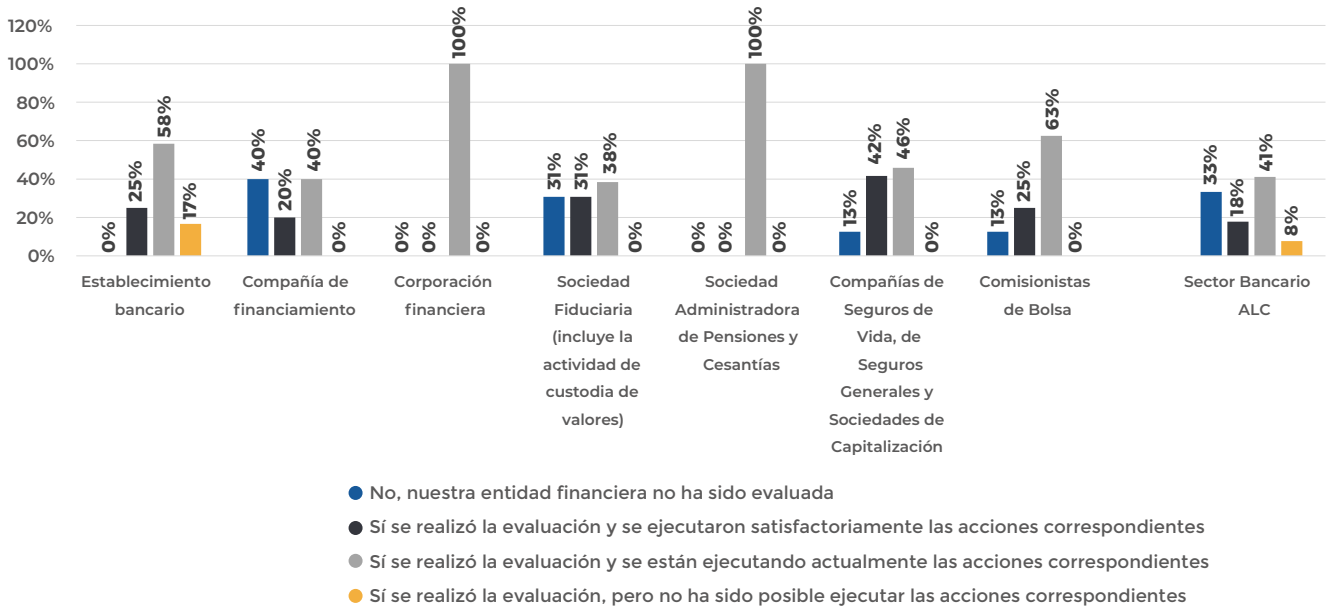


Nota: 12 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 79.

¿La entidad financiera a la cual usted pertenece ha sido evaluada externamente en los últimos dos (2) años bajo alguna metodología de seguridad de la información (incluyendo ciberseguridad) para determinar su nivel de madurez? – Comparación entre sectores

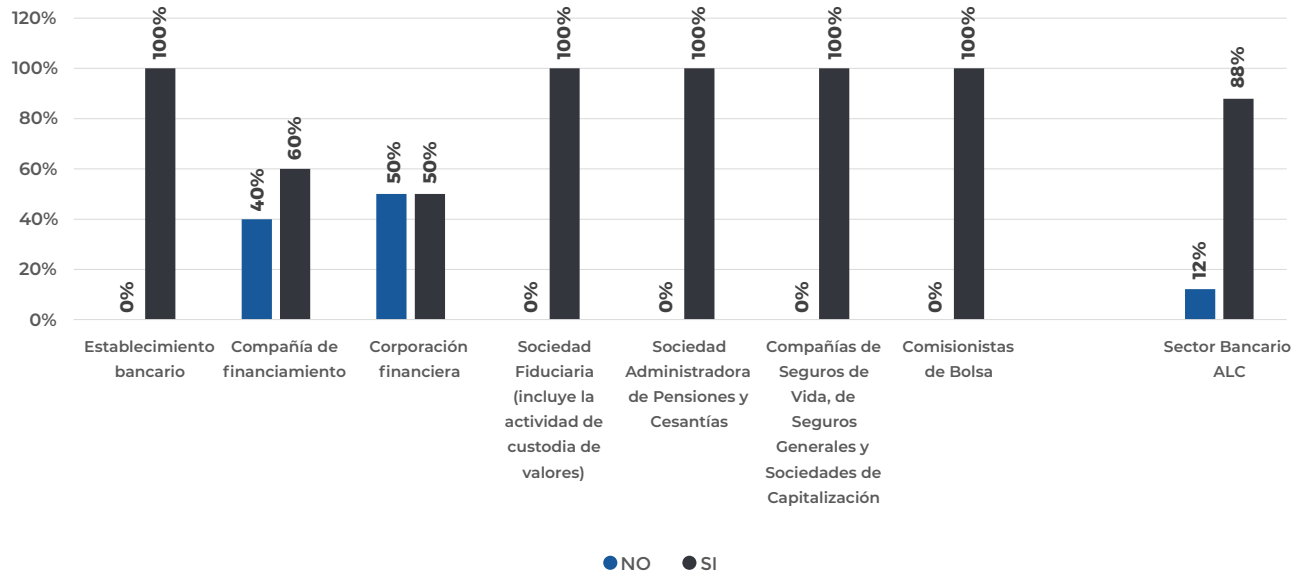


Nota: 68 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 80.

¿La entidad financiera ofrece un mecanismo para que sus colaboradores (empleados y contratistas) reporten incidentes (ataques exitosos)? – Comparación entre sectore

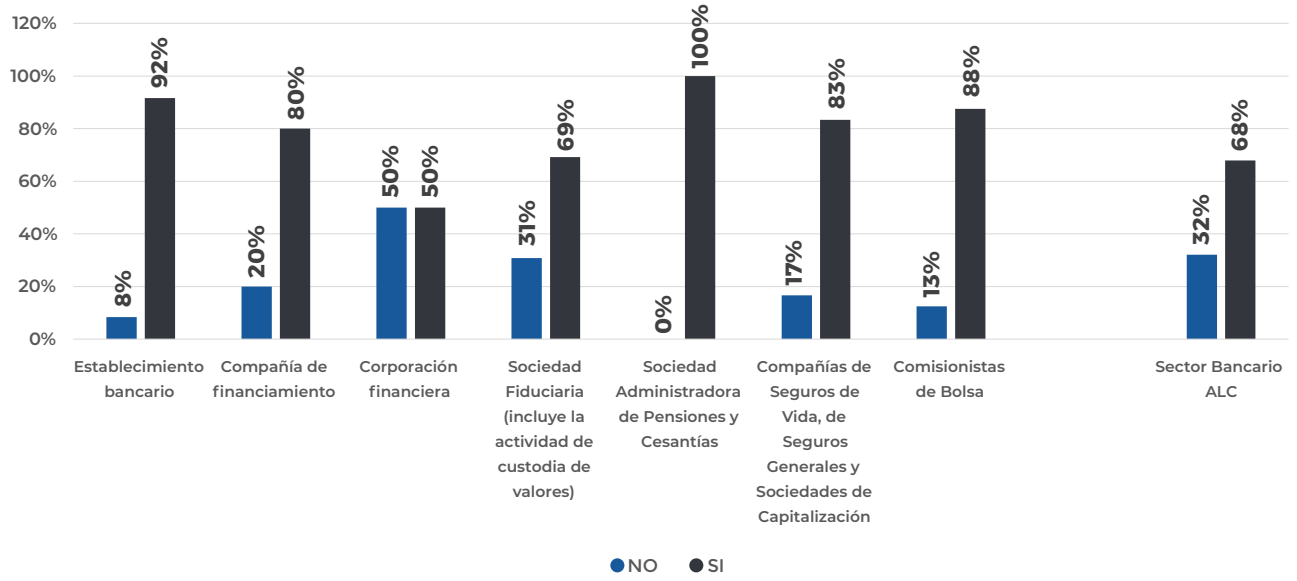


Nota: 68 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 81.

¿La entidad financiera ofrece un mecanismo para que sus clientes de servicios financieros reporten incidentes (ataques exitosos)? – Comparación entre sectores

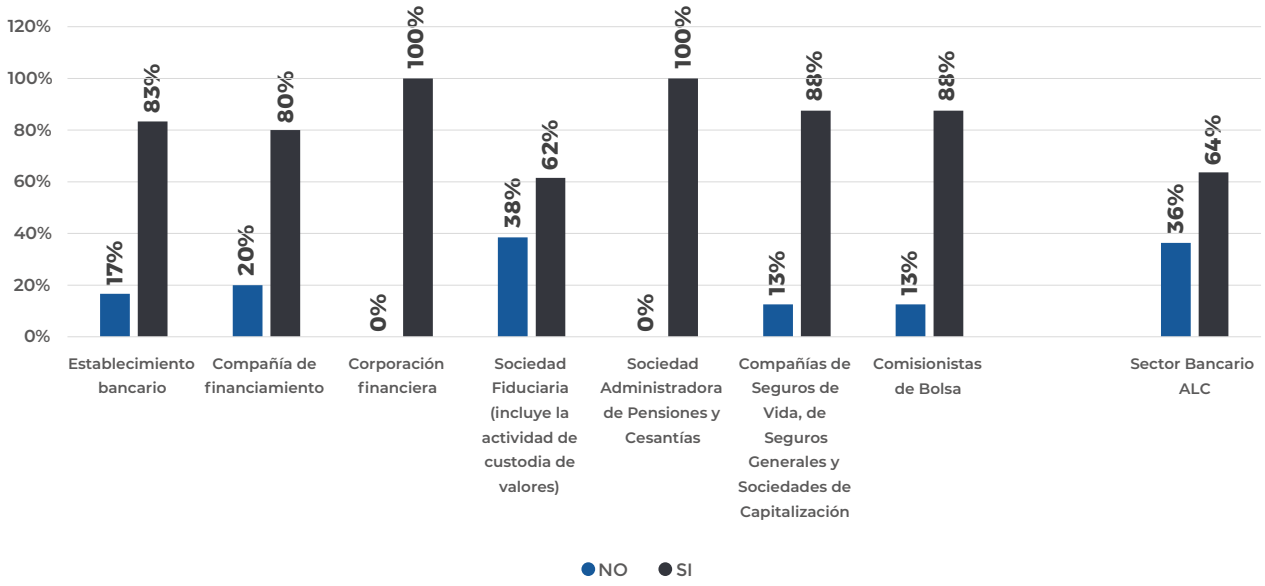


Nota: 68 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 82.

¿La entidad financiera cuenta con un plan de comunicaciones que permita informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida? – Comparación entre sectores

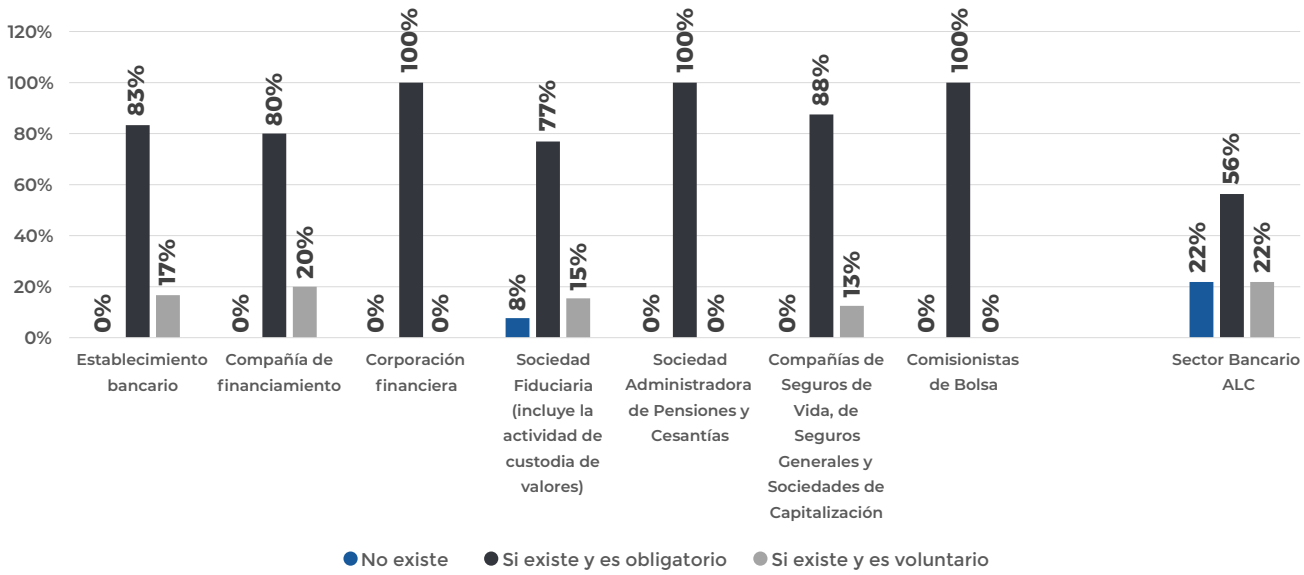


Nota: 68 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 83.

¿Conoce algún mecanismo para reportar incidentes (ataques exitosos) sufridos por la entidad financiera a la cual usted pertenece ante una autoridad de regulación en Colombia? – Comparación entre sectores

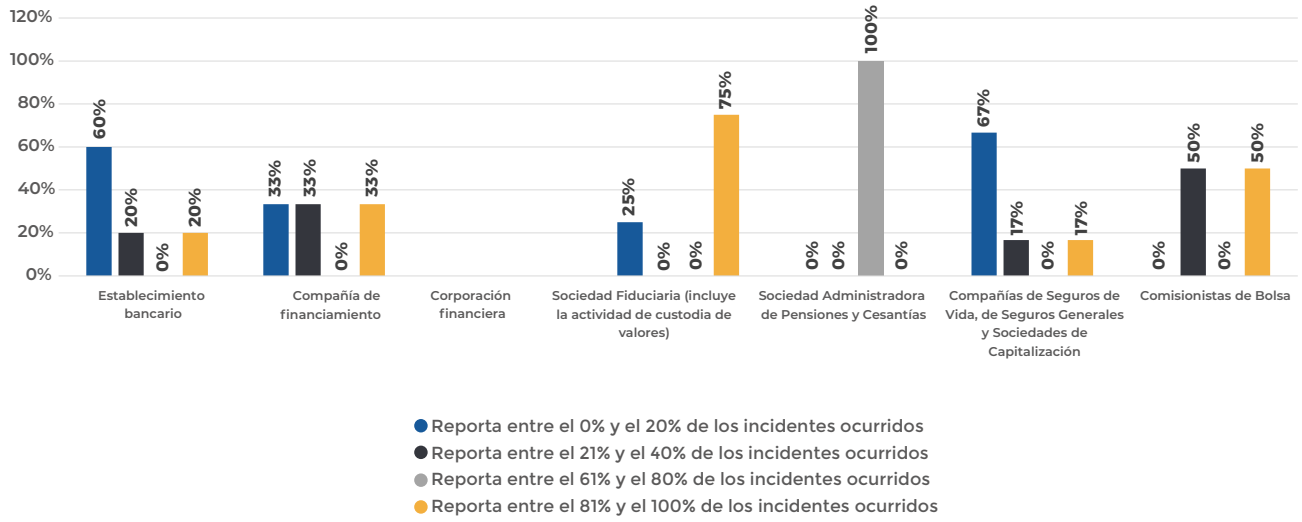


Nota: 68 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 84.

¿La entidad financiera reporta los incidentes (ataques exitosos) sufridos ante la Fiscalía General de la Nación o Policía Judicial en Colombia? – Comparación entre sectores

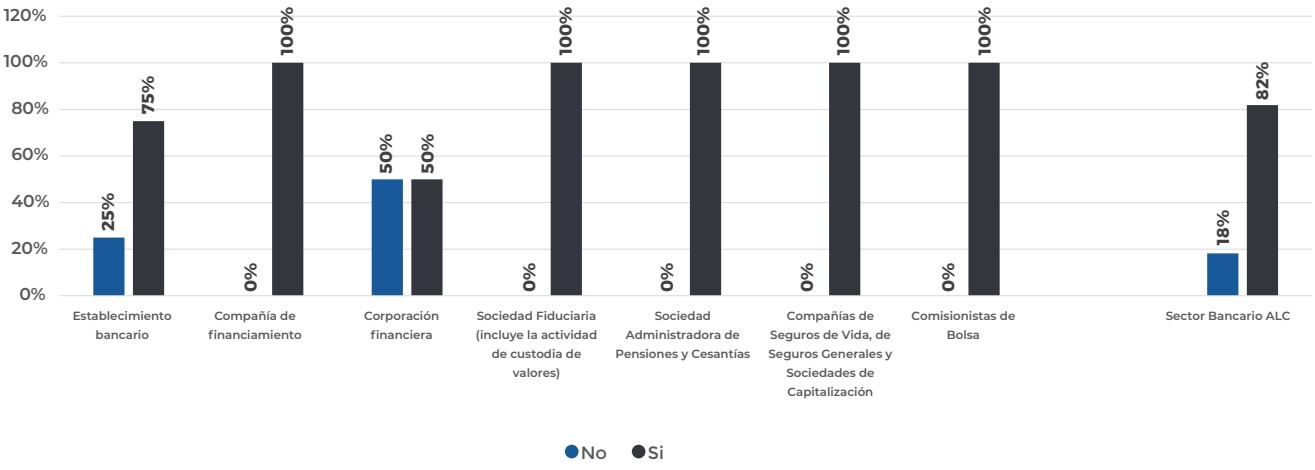


Nota: 68 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 85.

¿Cuenta la entidad financiera con planes de concientización y formación en asuntos de seguridad de la información para sus colaboradores? – Comparación entre sectores

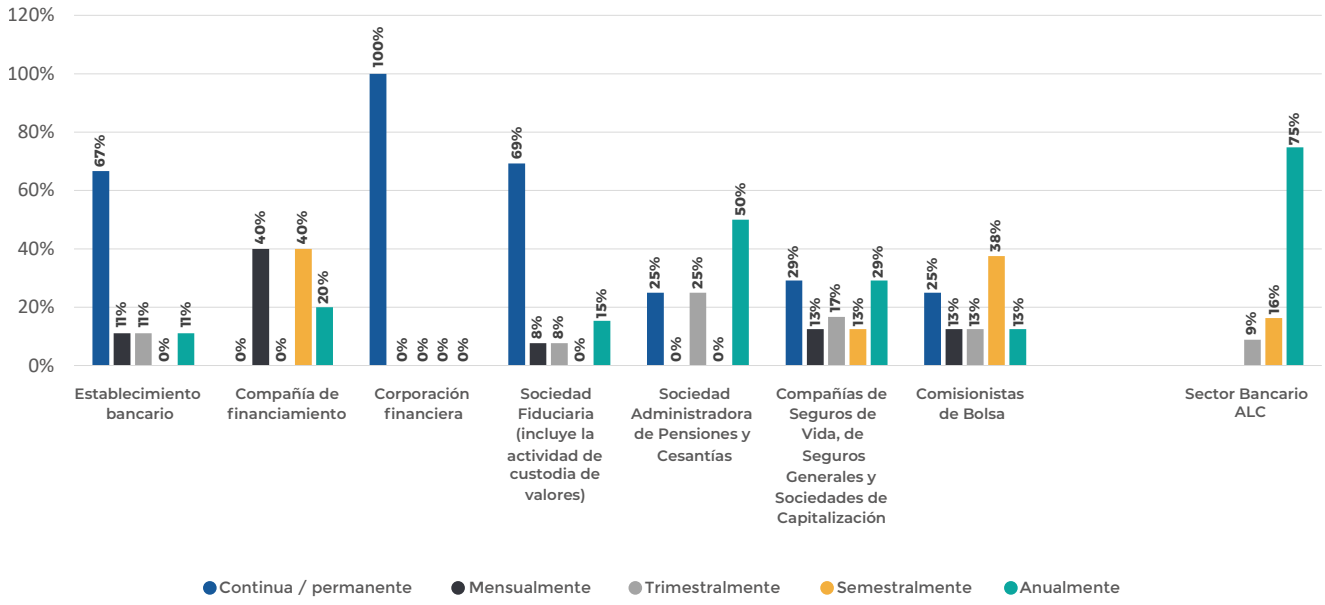


Nota: 68 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 86.

¿Con qué frecuencia se ejecutan dichos planes de concientización y formación? – Comparación entre sectores

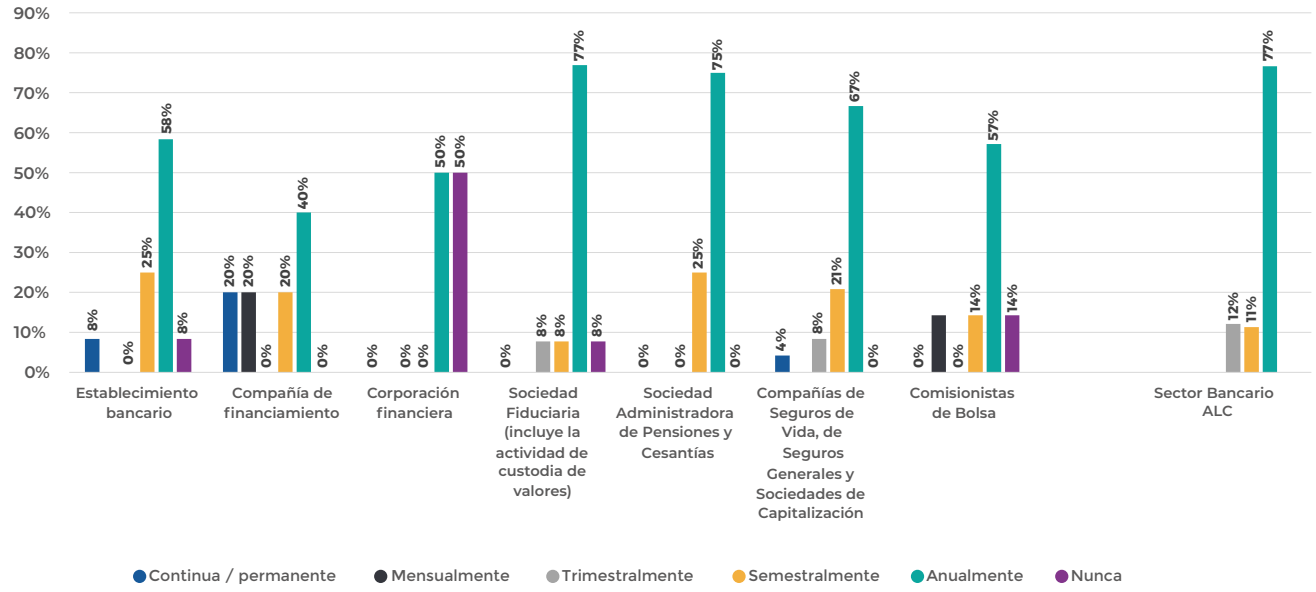


Nota: 64 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 87.

¿Con qué frecuencia se evalúa en la entidad financiera la capacidad de los colaboradores de responder adecuadamente a eventos (ataques exitosos y no exitosos) de seguridad de la información (incluyendo ciberseguridad) y amenazas tales como phishing e ingeniería social? – Comparación entre sectores

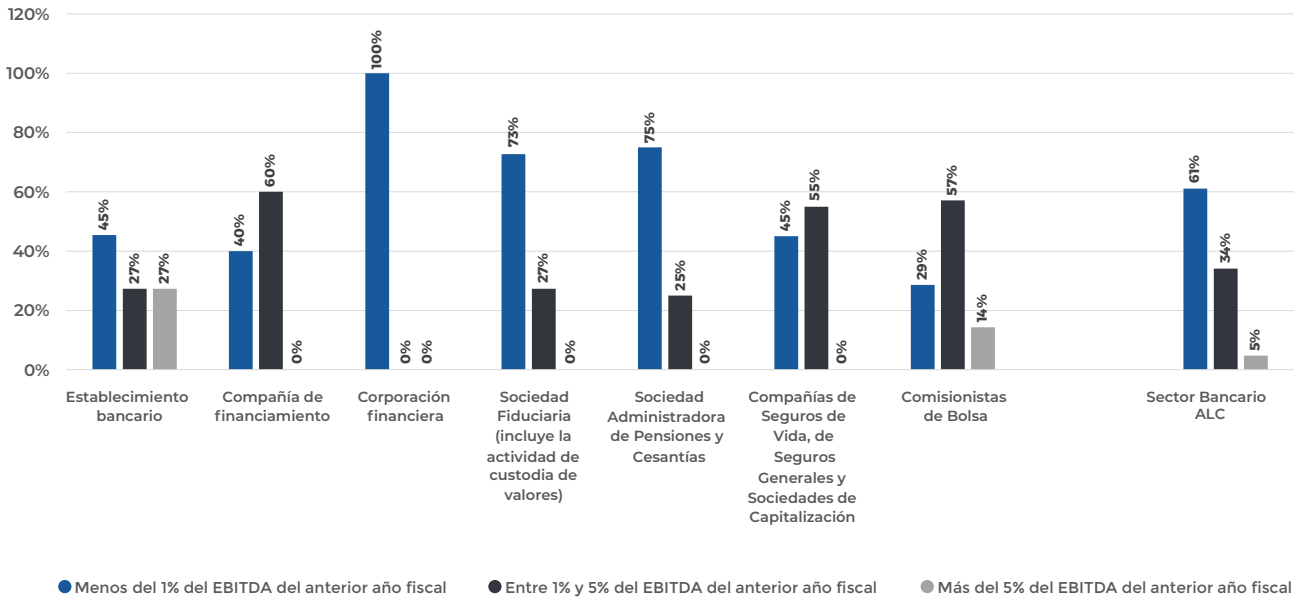


Nota: 68 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 88.

Presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales en el último año fiscal – Comparación entre sectores

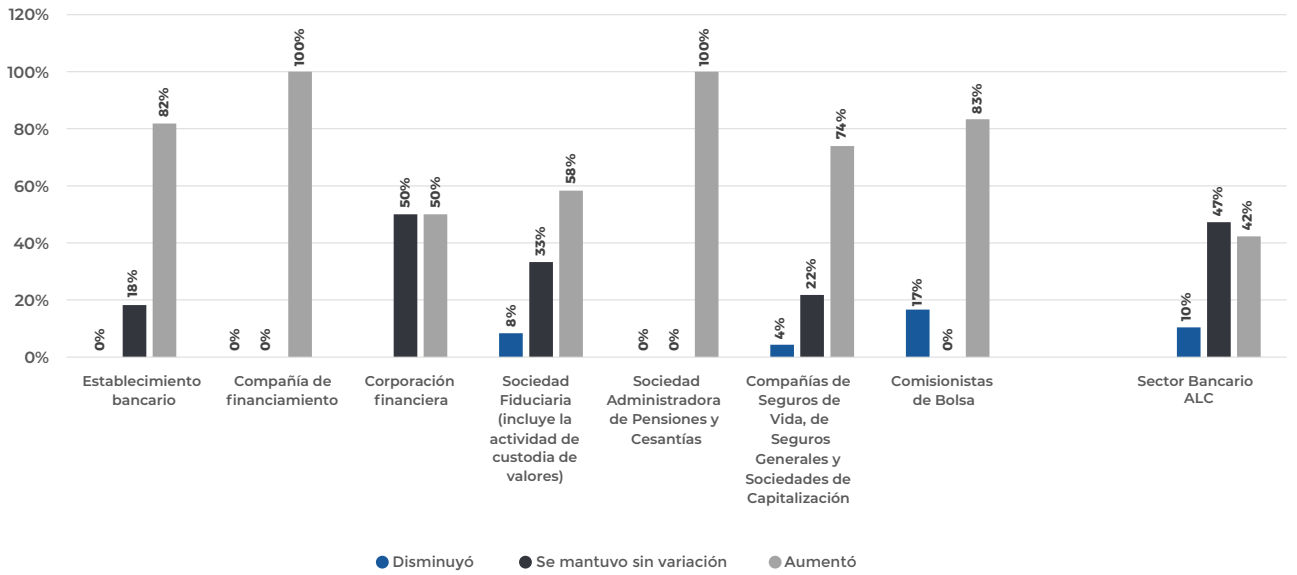


Nota: 65 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 89.

Crecimiento del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales de la entidad financiera para el actual año fiscal – Comparación entre sectores

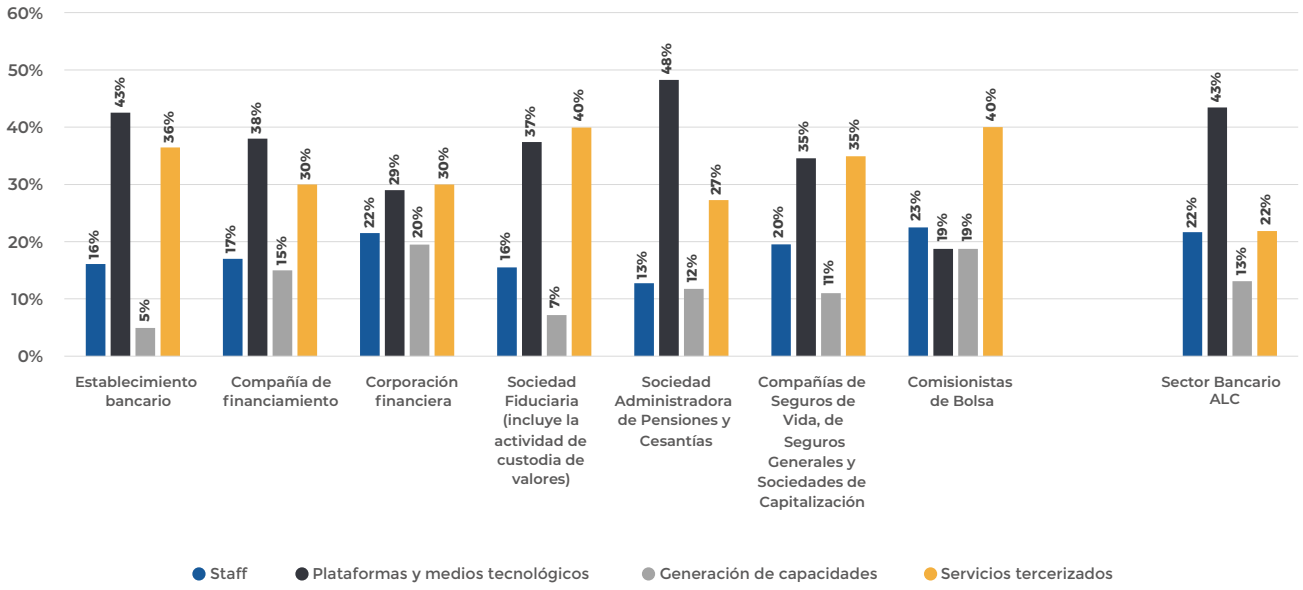


Nota: 65 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 90.

Distribución del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales de la entidad financiera (en Colombia, sin incluir en el cálculo el presupuesto de su casa matriz) – Comparación entre sectores

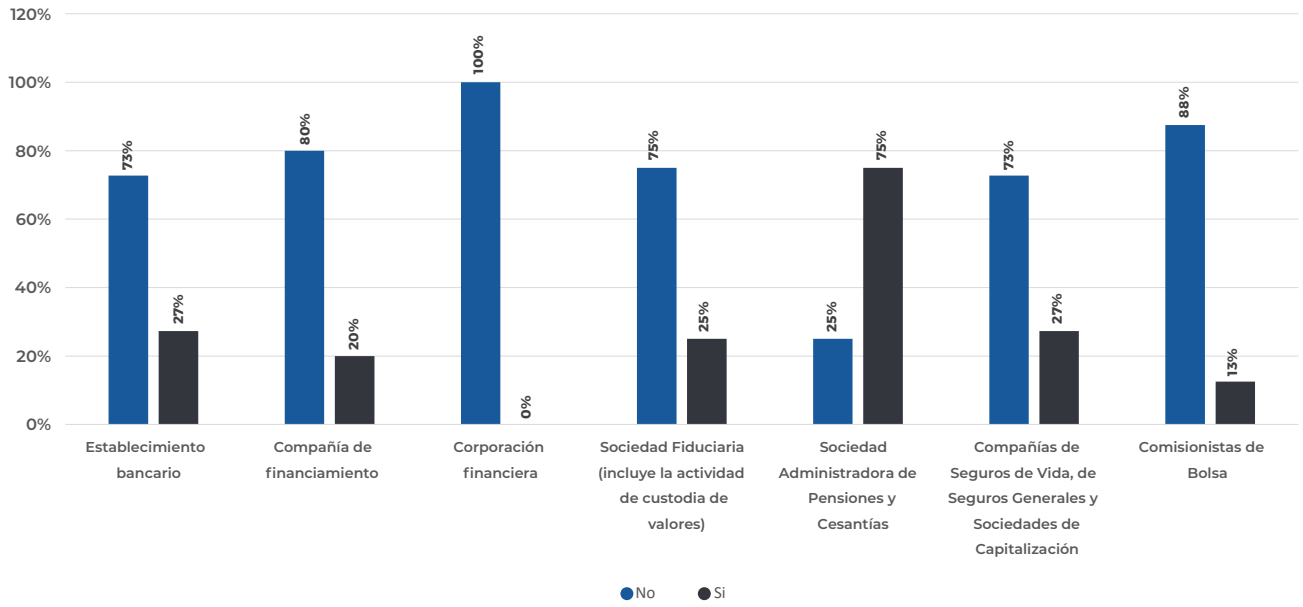


Nota: 64 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Gráfica 91.

¿La entidad financiera a la cual usted pertenece estimó el costo total de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) para el último año fiscal? – Comparación entre sectores



Nota: 64 registros

Fuente: *SG/OEA a partir de información recolectada de entidades financieras en Colombia*

Estado de la Ciberseguridad en el Sistema Financiero Colombiano

Notas a pie de página

1. Las entidades financieras participantes tienen un total de activos a 31 de diciembre de 2018 cercanos a los COL $483,8 billones de pesos (aproximadamente un 65% del total de activos de los sectores analizados), acumulan utilidades netas por COL $12,33 billones de pesos (aproximadamente un 83% del total de utilidades de los sectores analizados) y según su tamaño se distribuyen así: 8% entidades grandes, 45% entidades medianas y 47% entidades pequeñas; según su composición son: 81% entidades privadas, 3% entidades públicas y 16% entidades mixtas.

2. El valor de la utilidad a 31 de diciembre de 2018 de las entidades financieras de la muestra (Establecimientos Bancarios, Compañías de Financiamiento, Corporaciones Financieras, Sociedades Fiduciarias, Sociedades Administradoras de Pensiones y Cesantías, Compañías de Seguros de Vida, de Seguros Generales y Sociedades de Capitalización y Comisionistas de Bolsa) es equivalente a COL $14,85 billones de pesos. Dicho valor multiplicado por 2,16% equivale a COL $321 mil millones.

3. World Economic Forum. (2020). COVID-19 Risks Outlook A Preliminary Mapping and Its Implications. Obtenido de
https://www.weforum.org/reports/covid-19-risks-outlook-a-preliminary-mapping-and-its-implications

4. Comisión Económica para América Latina y el Caribe de Naciones Unidas (2020). Dimensionar los efectos del COVID-19 para pensar en la reactivación. Obtenido de
https://repositorio.cepal.org/bitstream/handle/11362/45445/1/S2000286_es.pdf

5. World Economic Forum. (2020). Cybersecurity Leadership Principles Lessons learnt during the COVID-19 pandemic to prepare for the new normal. Obtenido de https://www.weforum.org/reports/cybersecurity-leadership-principles-lessons-learnt-during-the-covid-19-pandemic-to-prepare-for-the-new-normal

6. Foro Económico Mundial, “The Global Risks Report 2020”. En
http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

7. Centro Cibernético Policial y CCIT. “Tendencias Cibercrimen Colombia 2019-2020”. En:
https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

8. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

9. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

10. Centro Cibernético Policial. “Balance cibercrimen 2020”, mayo de 2020

11. “Seguros en línea y en la vida” del Ministerio de Tecnologías de la Información y las Comunicaciones

12. https://caivirtual.policia.gov.co/

13. https://adenunciar.policia.gov.co/adenunciar/Login.aspx?ReturnUrl=/adenunciar/%20

14. La gráfica 70 del Anexo 2 presenta la comparación del resultado Porcentaje de operaciones que se realizaron por medio de canales digitales entre los diferentes sectores analizados del Sistema Financiero Colombiano.

15. La gráfica 71 del Anexo 2 presenta la comparación del resultado: Área única responsable de la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude entre los diferentes sectores analizados del Sistema Financiero Colombiano.

16. La gráfica 72 del Anexo 2 presenta la comparación del resultado: Número de niveles jerárquicos que hay entre el CEO y el máximo responsable de la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude entre los diferentes sectores analizados del Sistema Financiero Colombiano.

17. La gráfica 73 del Anexo 2 presenta la comparación del resultado: ¿Se considera adecuado que el equipo que manejan procesos asociados a la seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales creciera en el corto plazo? entre los diferentes sectores analizados del Sistema Financiero Colombiano.

18. La gráfica 74 del Anexo 2 presenta la comparación del resultado: ¿La Junta Directiva recibe reportes periódicos acerca de riesgos de seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales? entre los diferentes sectores analizados del Sistema Financiero Colombiano.

19. La gráfica 75 del Anexo 2 presenta la comparación del resultado: Tecnologías digitales emergentes aplicadas a herramientas, controles o procesos de seguridad digital en la entidad financiera entre los diferentes sectores analizados del Sistema Financiero Colombiano.

20. Con excepción del DNS Spoofing.

21. Con excepción de Ataque de día cero, Sabotaje interno y Man-in-the-middle.

22. La gráfica 76 del Anexo 2 presenta la comparación del resultado: Porcentaje de eventos (ataques exitosos y ataques no exitosos) detectados mediante sistemas operados por la entidad financiera (incluyendo los servicios provistos por la casa matriz) entre los diferentes sectores analizados del Sistema Financiero Colombiano.

23. La gráfica 77 del Anexo 2 presenta la comparación del resultado: ¿La entidad financiera a la cual usted pertenece (en el país en el que se encuentra), como organización, fue víctima de incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad) durante los últimos doce meses? entre los diferentes sectores analizados del Sistema Financiero Colombiano.

24. La gráfica 78 del Anexo 2 presenta la comparación del resultado: ¿La entidad financiera a la cual usted pertenece investigó la fuente que generó dichos incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad)? entre los diferentes sectores analizados del Sistema Financiero Colombiano.

25. La gráfica 79 del Anexo 2 presenta la comparación del resultado: ¿La entidad financiera a la cual usted pertenece ha sido evaluada externamente en los últimos dos (2) años bajo alguna metodología de seguridad de la información (incluyendo ciberseguridad) para determinar su nivel de madurez? entre los diferentes sectores analizados del Sistema Financiero Colombiano.

26. La gráfica 80 del Anexo 2 presenta la comparación del resultado: ¿La entidad financiera ofrece un mecanismo para que sus colaboradores (empleados y contratistas) reporten incidentes (ataques exitosos)? entre los diferentes sectores analizados del Sistema Financiero Colombiano.

27. La gráfica 81 del Anexo 2 presenta la comparación del resultado: ¿La entidad financiera a la cual usted pertenece ofrece un mecanismo para que sus clientes de servicios financieros reporten incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales)? entre los diferentes sectores analizados del Sistema Financiero Colombiano.

28. La gráfica 82 del Anexo 2 presenta la comparación del resultado: ¿La entidad financiera a la cual usted pertenece cuenta con un plan de comunicaciones que permita informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida? entre los diferentes sectores analizados del Sistema Financiero Colombiano.

29. La gráfica 83 del Anexo 2 presenta la comparación del resultado: ¿Conoce algún mecanismo para reportar incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales) sufridos por la entidad financiera a la cual usted pertenece ante una autoridad de regulación en Colombia? entre los diferentes sectores analizados del Sistema Financiero Colombiano.

30. La gráfica 84 del Anexo 2 presenta la comparación del resultado: ¿La entidad financiera a la cual usted pertenece reporta los incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales) sufridos en los últimos doce meses ante la Fiscalía General de la Nación o Policía Judicial en Colombia? entre los diferentes sectores analizados del Sistema Financiero Colombiano.

31. La gráfica 85 del Anexo 2 presenta la comparación del resultado: ¿Cuenta la entidad financiera a la cual usted pertenece con planes de concientización y formación en asuntos de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales para sus colaboradores? entre los diferentes sectores analizados del Sistema Financiero Colombiano.

32. La gráfica 86 del Anexo 2 presenta la comparación del resultado: ¿Con que frecuencia se ejecutan dichos planes de concientización y formación? entre los diferentes sectores analizados del Sistema Financiero Colombiano.

33. La gráfica 87 del Anexo 2 presenta la comparación del resultado: ¿Con qué frecuencia se evalúa en la entidad financiera la capacidad de los colaboradores de responder adecuadamente a eventos (ataques exitosos y no exitosos) de seguridad de la información (incluyendo ciberseguridad) y amenazas tales como phishing e ingeniería social? entre los diferentes sectores analizados del Sistema Financiero Colombiano.

34. La gráfica 88 del Anexo 2 presenta la comparación del resultado Presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales en el último año fiscal entre los diferentes sectores analizados del Sistema Financiero Colombiano.

35. La gráfica 89 del Anexo 2 presenta la comparación del resultado Crecimiento del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales de la entidad financiera entre los diferentes sectores analizados del Sistema Financiero Colombiano.

36. La gráfica 90 del Anexo 2 presenta la comparación del resultado Distribución del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales de la entidad financiera (en Colombia, sin incluir en el cálculo el presupuesto de su casa matriz) entre los diferentes sectores analizados del Sistema Financiero Colombiano.

37. La gráfica 91 del Anexo 2 presenta la comparación del resultado ¿La entidad financiera a la cual usted pertenece estimó el costo total de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) para el último año fiscal? entre los diferentes sectores analizados del Sistema Financiero Colombiano.

Estado de la Ciberseguridad en el Sistema Financiero Colombiano

ASOBANCARIA
Construyendo
la Confianza y Solidez del sector financiero

OEA
Más derechos
para más gente

Estado de la

Ciberseguridad

en el Sistema Financiero Colombiano