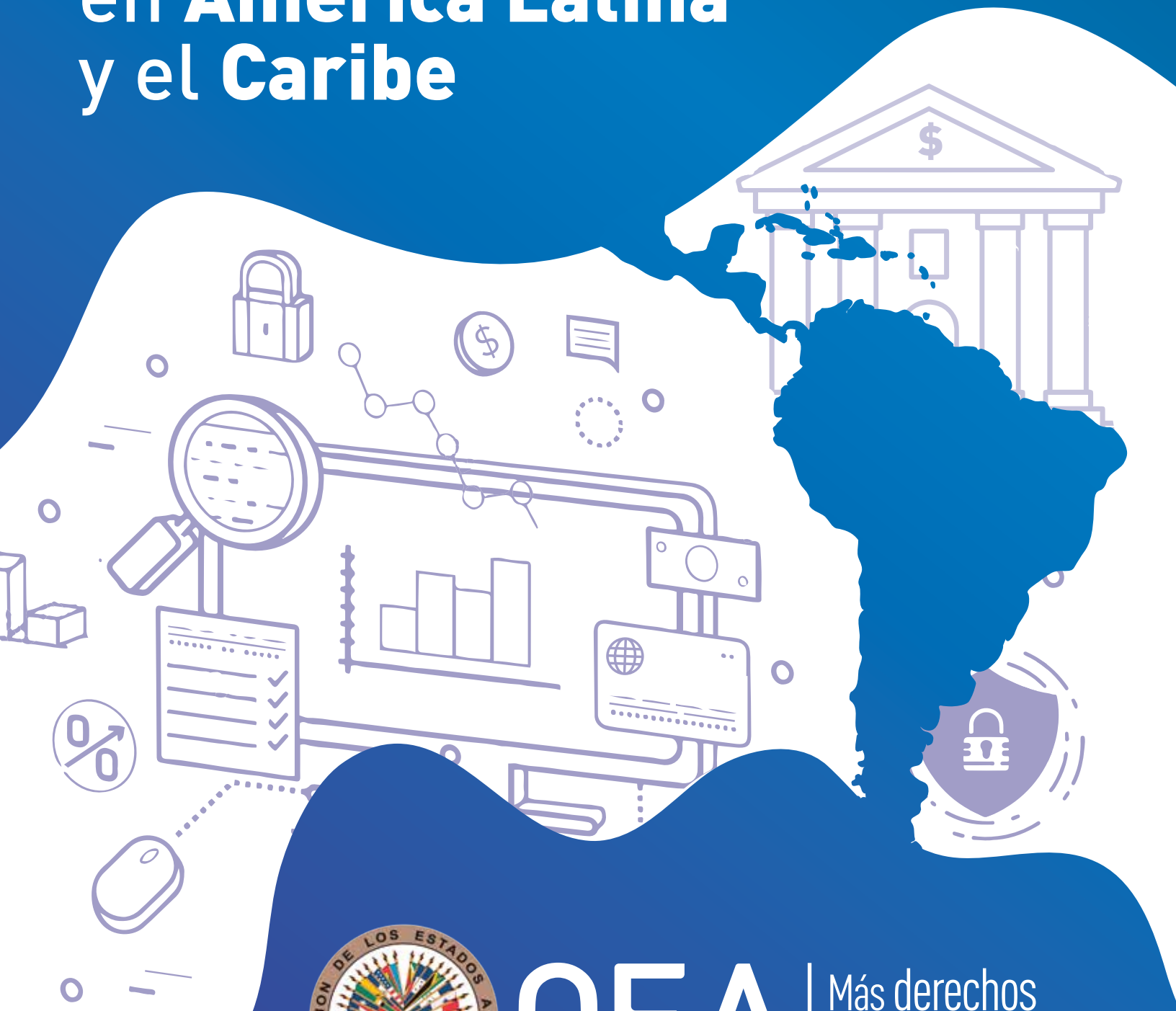
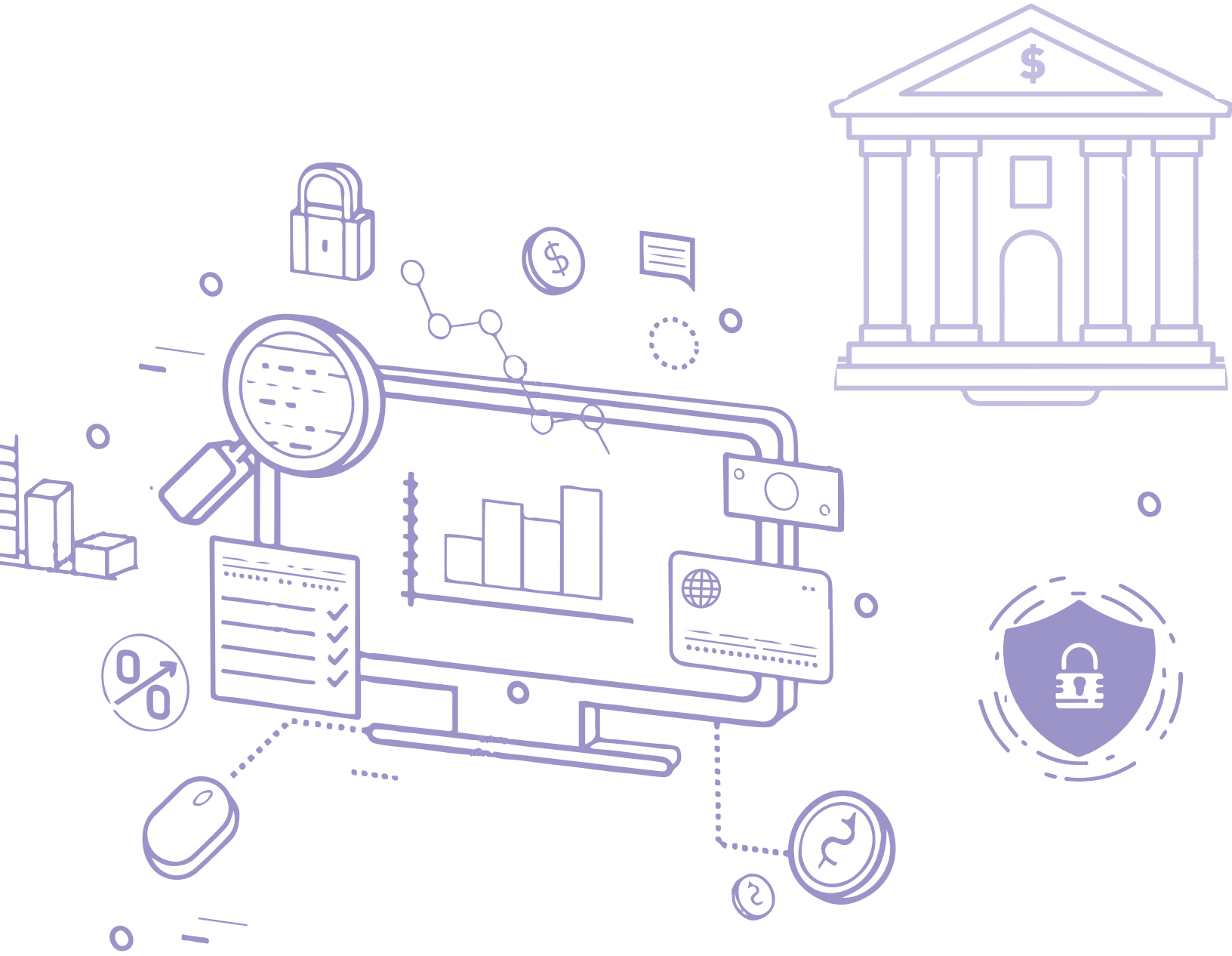
Estado de la **Ciberseguridad** en el **Sector Bancario** en **América Latina** y el **Caribe**



OEA | Más derechos para más gente



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 contra el Terrorismo
Organización de los Estados Americanos

Equipo Técnico
Belisario Contreras
Barbara Marchiori
Kerry-Ann Barrett
Mariana Cardona
Nathalia Foditsch
Gonzalo García-Belenguer

Equipo Consultor
Orlando Garcés
Jorge Bejarano

Colaboradores
Harold Coronado
Anderson Mota
José Marangunich Racchumi
César Augusto Tobón Betancur
Rodrigo Munari
José Gomes Fernandes
Fabio Moraes Benedito
Maria Teresa Tolu Brasil
Andre Salgado

Esta publicación ha sido posible gracias
al apoyo financiero del gobierno de

Canada

01

02

03

04

05

06

07

01

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 Sector Bancario en América Latina y el Caribe. 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 nuestra región.

La información analizada en el presente estudio tuvo dos (2) frentes. El primero está orientado a las entidades bancarias, y para ello se analizaron datos de 191 entidades bancarias de toda la región. El otro frente está enfocado en los clientes del sistema bancario[1], y para este fin se analizaron los aportes de 722 usuarios[2] de la región. Para llevar a cabo este análisis, la OEA diseñó, con el apoyo de expertos del sector bancario, instrumentos específicos para cada grupo objetivo. A partir del análisis efectuado en base a los instrumentos empleados, se presentan a continuación los principales hallazgos.

Hallazgos significativos sobre la seguridad digital en las entidades del sector bancario en América Latina y el Caribe:

- En relación con la preparación y gobernanza de la seguridad digital, en promedio en el 41% de las entidades bancarias en la región existen dos (2) niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital. No obstante, se encontró que 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) dependen también del tamaño de la organización. En referencia al número de áreas a cargo de estas temáticas, en promedio en el 74% de las entidades bancarias se tiene una única área responsable por la seguridad digital.

- Respecto al apoyo a la gestión del riesgo de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) por parte de la alta dirección de la entidad bancaria, se destaca que más del 60% del total de las entidades bancarias en la región lo demuestran i) exigiendo la adopción de buenas prácticas de seguridad (65%), ii) fomentando la capacitación y sensibilización en seguridad digital (63%) y iii) impulsando planes de seguridad digital (60%).

- En el 72% de las entidades bancarias la junta directiva recibe reportes periódicos acerca de indicadores y gestión de riesgos de seguridad digital, sin embargo, el 60% de quienes atendieron la encuesta considera que convencer a la alta dirección de la organización de invertir en soluciones de seguridad digital es medianamente complejo, a pesar de la relevancia que tienen las inversiones especialmente en materia de prevención y desarrollo de capacidades.

- Dentro de los estándares, mejores prácticas y marcos metodológicos más implementados en las entidades bancarias de la región, se encuentran las normas ISO 27001 y COBIT (en el 68% y 50% de las entidades bancarias, respectivamente).

- En materia de conformación de los equipos responsables de los procesos de seguridad digital, se observa que éstos se componen en promedio de diecisiete (17) miembros, para un banco típico de la región. No obstante, este valor varía dependiendo del tamaño de la entidad.

• Se resalta que el 82% de entidades encuestadas en la región 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 contratan la relativa a la realización de pruebas de seguridad (65% del total).

• En cuanto a capacidades de detección y análisis de eventos de seguridad digital, que son vitales para la gestión sistemática de este tipo de riesgos, más del 90% de entidades bancarias en la región han implementado los cortafuegos y las actualizaciones automatizadas de virus y sistemas. El 85% de las entidades bancarias de la región han implementado tanto Sistemas de Detección / Prevención de intrusiones (IDS e IPS), como Procesos de Monitoreo de Amenazas y Vulnerabilidades.

• Resulta significativo que el 49% de las entidades bancarias aún no están implementando herramientas, controles o procesos usando Tecnologías Digitales Emergentes, tales como Big Data, Machine Learning o Inteligencia Artificial, las cuales resultan muy importantes a la hora de prevenir ciberataques o determinar patrones sospechosos asociados a fraude, entre otras capacidades de detección.

• Los riesgos de seguridad digital que merecen la mayor atención por parte de las entidades bancarias son: i) el robo de base de datos crítica, ii) el compromiso de credenciales de usuarios privilegiados, y, iii) la pérdida de datos.

• El 92% de las entidades bancarias manifiestan que identificaron algún tipo de evento (ataques exitosos y ataques no exitosos) de seguridad digital en contra de la entidad financiera. Los eventos más identificados fueron: i) el código malicioso o malware (80% del total de entidades bancarias), ii) la violación de políticas de escritorio limpio (clear desk) (63% del total de entidades bancarias), y, iii) el phishing dirigido para tener acceso a sistemas del banco (57% del total de entidades bancarias). Destaca además la detección de eventos con frecuencia diaria de malware y phishing dirigido para tener acceso a sistemas del banco (un 24% y 22% de las entidades bancarias los identificaron, respectivamente).

• Según las entidades bancarias, los eventos de i) phishing, ii) ingeniería social, y, iii) software espía (malware o troyanos) fueron los más frecuentes contra sus usuarios de servicios financieros, situación que resulta congruente con lo manifestado por los usuarios al ser consultados por los incidentes experimentados. También resulta importante anotar que, en promedio, un 26% de las entidades bancarias detectaron estos tipos de eventos mediante sistemas propios.

• Respecto a la gestión, respuesta y recuperación ante incidentes de seguridad digital, al menos la mitad de las entidades bancarias de la región contaron con estrategias de gestión, respuesta y recuperación ante incidentes de seguridad digital.

• El 37% de entidades bancarias manifestaron que sí fueron víctimas de incidentes (ataques exitosos) y la principal motivación de dichos ataques durante el año 2017 fueron Motivos Económicos (79% de las entidades bancarias víctimas).

• Como parte de las estrategias de gestión de riesgos de seguridad digital, en promedio, el 41% de las entidades bancarias realizó una evaluación de madurez y está

llevando a cabo actualmente las acciones correspondientes derivadas. Aquellas entidades bancarias que no logran hacer este tipo de evaluaciones señalan que las principales razones son: i) insuficiencia de personal especializado (46% de entidades bancarias sin evaluación), y, ii) falta de asignación de presupuesto (45% de entidades bancarias sin evaluación).

• En cuanto a la comunicación de incidentes de seguridad digital, la gran mayoría (88% de las entidades bancarias) ofrece un mecanismo para que sus usuarios internos (empleados y contratistas) reporten incidentes (ataques exitosos) de seguridad digital sufridos y el 64% cuenta con un plan de comunicaciones que permita informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida. La mayoría (el 61 % de los encuestados) reporta los ataques sufridos ante una autoridad de aplicación de la ley.

• En materia de capacitación y concientización, el 82% de entidades bancarias cuenta con planes de preparación, respuesta y capacitación en asuntos de seguridad digital para sus empleados e insourcing bancarios, los cuales se ejecutan en su mayoría anualmente. El mecanismo más efectivo a partir del cual se ha generado mayor conciencia en las entidades bancarias respecto de los riesgos de seguridad digital es el desarrollo de capacitaciones internas de información.

• En cuanto al impacto de los incidentes de seguridad digital, el 61% manifestó que el presupuesto de seguridad digital equivale en promedio a menos del 1% del EBITDA del anterior año fiscal, el 34% señaló que corresponde a entre el 1% y el 5% del EBITDA del anterior año fiscal y solo el 5% dijo que es mayor al 5% del EBITDA del anterior año fiscal. El presupuesto aumenta según el tamaño de la entidad.

• El presupuesto destinado a la seguridad digital por una entidad bancaria promedio en la región equivale aproximadamente al 2,09% del EBITDA del año inmediatamente anterior, y estos recursos se mantuvieron sin variación para el 46% de las entidades bancarias, aumentaron para el 42% (siendo la principal razón de aumento en el presupuesto aspectos de Cumplimiento Regulatorio) y disminuyeron para el 10% (siendo la principal razón para esta reducción la disminución de la utilidad del banco).

• El presupuesto como % de EBITDA del año anterior para entidades que son Casa Matriz en el país disminuye a medida que el tamaño del banco aumenta, mientras que el presupuesto como % de EBITDA para entidades que son Sucursal, Subordinada o Agencia de la entidad bancaria en el país aumenta a medida que el tamaño del banco aumenta.

• El presupuesto en seguridad digital se invierte en un 43% en Plataformas y medios tecnológicos, un 22% en Recursos Humanos, un 22% en Servicios tercerizados y un 13% en Generación de capacidades. En promedio, el presupuesto asignado a un miembro promedio del equipo de seguridad digital fue de US $19.437 en el año 2017, valor que varía dependiendo del tamaño de la entidad.

• En promedio, el retorno sobre la inversión en seguridad digital equivale aproximadamente a un 23,78%, lo que la mayoría considera que es un retorno de media rentabilidad.

• El 73% manifestó que el costo total de respuesta y de recuperación ante incidentes de seguridad digital equivale a menos del 1% del EBITDA del anterior año fiscal y el 27% señaló que entre el 1% y el 5% del EBITDA del anterior año fiscal.

• El costo total de respuesta y de recuperación ante incidentes de seguridad digital para una entidad bancaria promedio en la región supone aproximadamente el 1,52% del EBITDA del año inmediatamente anterior, equivalente a US$ 1.913.000 al año, valor que varía en función del tamaño del banco.

• El costo total como % de EBITDA del año anterior aumenta a medida que el tamaño del banco aumenta, independientemente de si la entidad bancaria es Casa Matriz o Sucursal, Subordinada o Agencia de la entidad bancaria.

• Finalmente, 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 bancarias de la región América Latina para 2017 fue de USD$ 809 millones aproximadamente.

Cuadro 1. Principales resultados por tamaño de entidad bancaria

Bancos GRANDES	Bancos MEDIANOS	Bancos PEQUEÑOS
En el 67% existe una única área responsable de la seguridad digital	En el 74% existe una única área responsable de la seguridad digital	En el 79% existe una única área responsable de la seguridad digital
En el 61% existen dos (2) niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital	En el 38% existen dos (2) niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital	En el 46% existe un (1) nivel jerárquico entre el CEO y el máximo responsable de la seguridad digital
La mayoría de los Bancos grandes (27%) cuenta con un equipo conformado por 16-30 miembros	La mayoría de los Bancos medianos (48%) cuenta con un equipo conformado por 1-5 miembros	La mayoría de los Bancos pequeños (94%) cuenta con un equipo conformado por 1-5 miembros
El 26% no están implementando herramientas, controles o procesos usando tecnologías digitales emergentes	El 44% no están implementando herramientas, controles o procesos usando tecnologías digitales emergentes	El 67% no están implementando herramientas, controles o procesos usando tecnologías digitales emergentes
Fueron objeto de ataques de todo tipo de eventos de seguridad digital, resaltando identificación de casi todos por la mayoría en la región	Fueron objeto de ataques de todo tipo de eventos de seguridad digital, resaltando identificación de algunos por la mayoría en la región	Fueron objeto de ataques de algunos tipos de eventos de seguridad digital, resaltando identificación de pocos por la mayoría en la región
El 40% identificaron ocurrencia de eventos de malware diariamente	El 28% identificaron ocurrencia de eventos de malware diariamente	El 9% identificaron ocurrencia de eventos de malware diariamente
La mayoría (41%) detecta entre un 61% y un 80% de eventos con sistemas propios	La mayoría (28%) detecta entre un 61% y un 80% de eventos con sistemas propios	La mayoría (40%) detecta entre un 0% y un 20% de eventos con sistemas propios
El 65% manifiestan que sí fueron víctimas de ataques exitosos	El 43% manifiestan que sí fueron víctimas de ataques exitosos	El 19% manifiestan que sí fueron víctimas de ataques exitosos

El 73% realizó una evaluación de madurez y está adelantando actualmente las acciones correspondientes	El 47% realizó una evaluación de madurez y está adelantando actualmente las acciones correspondientes	El 21% realizó una evaluación de madurez y está adelantando actualmente las acciones correspondientes
El 85% ofrece un mecanismo para que sus clientes reporten a la entidad incidentes (ataques exitosos) sufridos	El 72% ofrece un mecanismo para que sus clientes reporten a la entidad incidentes (ataques exitosos) sufridos	El 56% ofrece un mecanismo para que sus clientes reporten a la entidad incidentes (ataques exitosos) sufridos
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 65% cuenta con un plan de comunicaciones para informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida	El 56% cuenta con un plan de comunicaciones para informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida
El 81% reportan los incidentes sufridos ante autoridad de aplicación de la ley	El 65% reportan los incidentes sufridos ante autoridad de aplicación de la ley	El 46% reportan los incidentes sufridos ante autoridad de aplicación de la ley
El 57% manifestaron que el presupuesto de seguridad digital equivale en promedio a menos del 1% del EBITDA del anterior año fiscal	El 59% manifestaron que el presupuesto de seguridad digital equivale en promedio a menos del 1% del EBITDA del anterior año fiscal	El 67% manifestaron 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 1,86% del EBITDA del año inmediatamente anterior	El presupuesto destinado a la seguridad digital equivale aprox. al 2,14% del EBITDA del año inmediatamente anterior	El presupuesto destinado a la seguridad digital equivale aprox. al 2,27% del EBITDA del año inmediatamente anterior
En el 65%, el presupuesto de seguridad digital aumentó en comparación al año fiscal inmediatamente anterior	En el 47%, el presupuesto de seguridad digital aumentó en comparación al año fiscal inmediatamente anterior	En el 25%, el presupuesto de seguridad digital aumentó en comparación al año fiscal inmediatamente anterior
El presupuesto asignado en 2017 a un miembro promedio del equipo de seguridad digital fue de US $22.713	El presupuesto asignado en 2017 a un miembro promedio del equipo de seguridad digital fue de US $21.766	El presupuesto asignado en 2017 a un miembro promedio del equipo de seguridad digital fue de US $13.927
El retorno sobre la inversión en seguridad digital equivale aproximadamente a un 24,1%	El retorno sobre la inversión en seguridad digital equivale aproximadamente a un 23,85%	El retorno sobre la inversión en seguridad digital equivale aproximadamente a un 23,33%
El 53% manifestaron 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 81% manifestaron 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 83% manifestaron 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 en 2017 equivale aprox. al 1,86% del EBITDA del año inmediatamente anterior (US $5.253.000 en 2017 aprox.)	El costo total de respuesta y de recuperación ante incidentes de seguridad digital en 2017 equivale aprox. al 1,38% del EBITDA del año inmediatamente anterior (US $605.000 en 2017 aprox.)	El costo total de respuesta y de recuperación ante incidentes de seguridad digital en 2017 equivale aprox. al 1,36% del EBITDA del año inmediatamente anterior (US $161.000 en 2017 aprox.)

Hallazgos significativos sobre la ciberseguridad desde la perspectiva de los usuarios de las entidades del sector bancario en América Latina y el Caribe:

• Los usuarios 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 éstos, ya que el 53% de los encuestados revisa transacciones y saldos usando teléfonos inteligentes más que los que consultan en el banco (29%) o por línea telefónica (23%), e igualmente prefieren transferir fondos a través de Banca Móvil (43%) que trasladándose al banco (37%).

• Dentro del uso de medios digitales, se evidencia un incremento en la utilización de funcionalidades o servicios novedosos: Un 20% de los encuestados ya hacen operaciones de depósito móvil (cuando por ejemplo se puede depositar el monto de un cheque mediante la captura de su imagen y el endoso usando la cámara del teléfono inteligente), y cerca de un 7% de usuarios ya realizan retiros de dinero con opciones de retiro en ATM sin tarjeta (cuando por ejemplo el banco brinda la opción de que si el usuario no dispone del plástico pueda solicitar un token al celular y hacer el retiro en un ATM).

• Servicios que fueron antes muy comunes, hoy se ven desplazados por nuevas opciones: El uso de medios de pago virtuales con tarjetas vinculadas a Smartphones (27%) ya supera las transacciones de venta telefónica (10%), así como el porcentaje de uso de Bitcoins como medio de pago (6,50%) ya supera el de pago mediante cheques (5,86%).

• Los usuarios están empezando a pasar de ser consumidores "omnidigitales", es decir, aquellos que prefieren interactuar digitalmente con su banco sin preferencia por usar una computadora portátil, una tableta o un teléfono inteligente, a preferir el teléfono inteligente. En este análisis se destaca que en el caso de los más jóvenes (entre 18 y 24 años), el uso de los dispositivos móviles iguala al de computadoras portátiles (39% en ambos casos), y en el siguiente rango (entre 25 y 34 años) es muy cercano (36% móviles y 38% portátiles)

• 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 (59%) la principal motivación de quienes no utilizan los medios digitales para realizar sus operaciones bancarias.

• Respecto a cultura de seguridad digital la mayoría de los usuarios (85%) conocían muchas o todas las definiciones referidas a distintos tipos de incidentes cibernéticos y se mantienen informados principalmente a través de noticias en sitios web, blogs y sitios especializados (78,11%), así como mediante las redes sociales (66,73%). Apenas un 40% 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. Igualmente y no obstante es cierto que cada vez existe más información disponible sobre las nuevas formas de ataques y amenazas de seguridad, aunque es cierto también que las mismas no parecen estar siendo aún muy difundidas en los medios de comunicación tradicionales como los periódicos, la TV y las radios locales, ya que este tipo de medios

quedó en un cuarto (4to) lugar entre los que emplean los usuarios como fuente.

• En cuanto a las medidas de seguridad implementadas por los usuarios para prevenir incidentes digitales, la más frecuente fue la de usar antivirus en sus computadores (84,2%), 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%), y el uso de tokens o medios complementarios de autenticación (53,09%).

• 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 62,45% afirmó no haber sufrido este tipo de incidentes, mientras que el 27,30% indicó que sí había sido afectado y un 10,26% respondió no saber y/o conocer el asunto. Del total de usuarios afectados, los tipos de incidentes digitales experimentados más frecuentes fueron el fraude de phishing e ingeniería social de correo electrónico con un 49,68%, otros tipos de compromiso con 36,94% (no catalogados dentro de las opciones de respuesta) y la infección con software malintencionado con 35,67%. La frecuencia con la que los usuarios expresan haber sido víctimas dio como resultado que en su mayoría (62,75%) sufrieron incidentes de esta naturaleza una sola vez, lo cual contrasta con quienes indicaron padecerlos una vez al mes (22,88%), una vez a la semana (6,54%) y diariamente (3,27%), lo que hace evidente que los usuarios no necesariamente son conscientes de estar siendo afectados por la ocurrencia de incidentes cibernéticos, porque no todos ellos han adoptado mecanismos o medidas de seguridad que entre otros aspectos les permitan ser advertidos de este tipo de situaciones[3].

• El efecto negativo de los incidentes sufridos por los usuarios fue la afectación o pérdida de imagen que tenían sobre la entidad bancaria (48,67%), acompañado de la imposibilidad de acceso oportuno al servicio (44,67%), la pérdida de recursos financieros (42,67%) y la exposición de sus datos a terceros (40,67%). En cuanto al impacto económico para los afectados, un 47% afirmó no haber perdido dinero, frente a un 21% que manifestó haber perdido entre 101 a 500 USD$, a un 15% que expresó haber perdido entre 10 y 100 USD$ y a un 11% que registró haber perdido entre 500 y 1.000 USD$. De la totalidad de los usuarios que efectivamente tuvieron pérdida económica, el 44,87% manifestó haber sido reparado o compensado totalmente, frente a un 25,64% que indicó haberlo sido parcialmente y un 29,49% que expresó no haber recibido ningún tipo de indemnización.

• Sobre los mecanismos de reporte, los usuarios entrevistados indicaron en su mayoría, que la institución bancaria sí ofrece un mecanismo para reportar incidentes (64,71%) y que en efecto han reportado el incidente ante su banco (71,24%). Por su parte, se resalta la manifestación de que, conforme a las respuestas, solo el 37,25% afirma que en su país existe 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. 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% han elevado a estas instancias los incidentes que les han afectado.

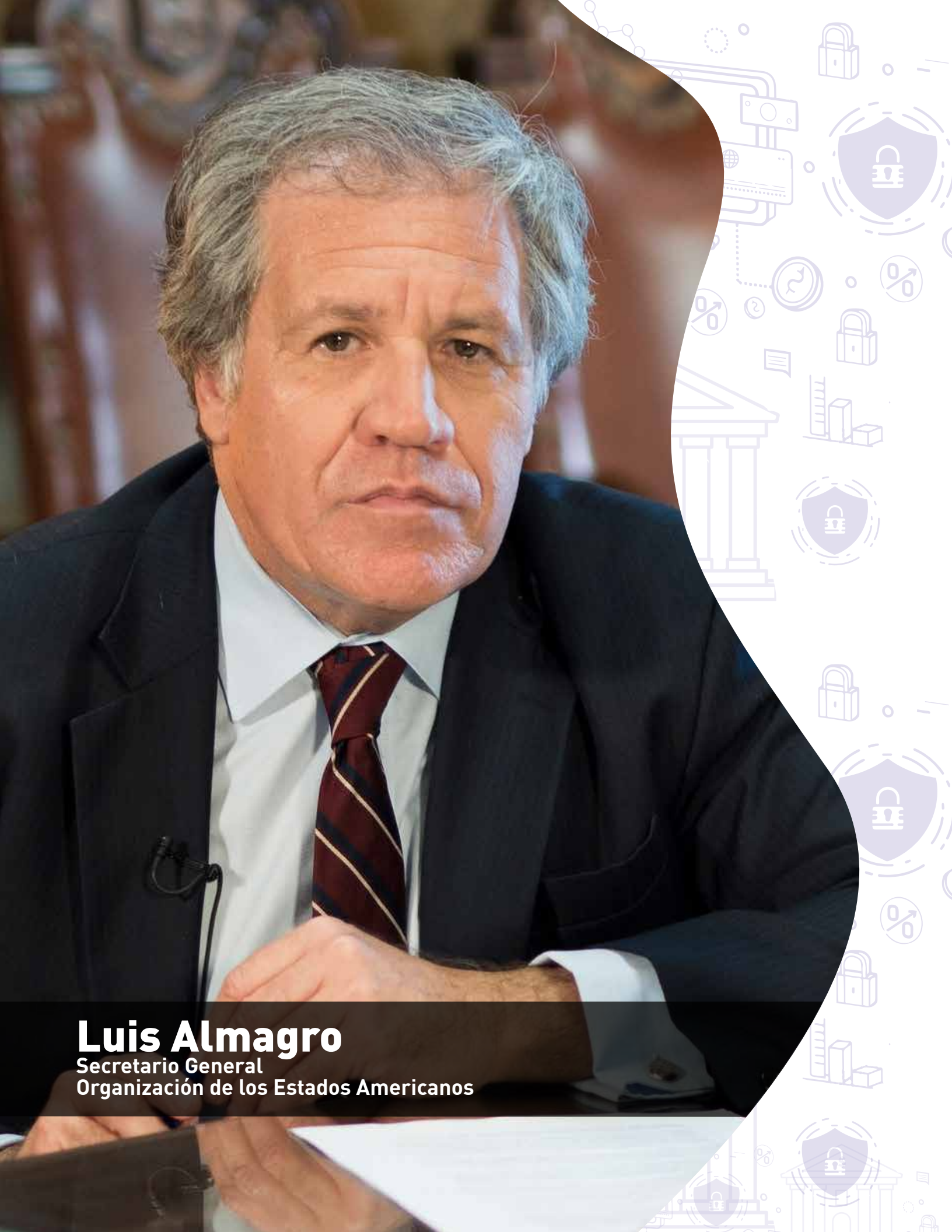
• Respecto a la percepción de los usuarios sobre la evolución de los riegos de que ocurran incidentes cibernéticos, un 79,54% indica que han empeorado en el último año, frente a un 10,85% y 9,61% que indicó no percibir ese aumento o desconocerlo, respectivamente.

• Finalmente, otro de los hallazgos importantes del estudio es que un 67,08% considera que la existencia de riesgos derivados de incidentes cibernéticos afecta su decisión de usar o no los medios digitales en este sector, lo que resalta la importancia de fortalecer la gestión de riesgos de seguridad digital, de manera integral, de forma que los usuarios y empresas encuentren un entorno digital que genere confianza para todos.

El detalle del estudio, que puede apreciarse en los numerales 4 y 5 de este documento, desarrolla en profundidad los hallazgos enunciados y muchos otros aspectos que pueden resultar de interés. Igualmente, los anexos incluidos ofrecen información complementaria de utilidad en el marco del objeto de estudio.

02

PRÓLOGO



Luis Almagro

Secretario General
Organización de los Estados Americanos

La Secretaría General de la Organización de los Estados Americanos (OEA), a través del Programa de Ciberseguridad adscrito a la Secretaría del Comité Interamericano contra el Terrorismo (CICTE), promueve y coordina la cooperación entre los Estados miembros de la OEA y, entre ellos, el Sistema Interamericano y otros organismos en el sistema internacional, con el fin de acceder, prevenir, confrontar, y responder de manera efectiva a las amenazas a la seguridad, a efectos de ser el principal punto de referencia en el Hemisferio para desarrollar la cooperación y la creación de capacidad en los Estados miembros de la OEA.

El sector financiero y en particular la banca, ha sido uno de los sectores con mayores índices de digitalización. Cada día un mayor número de clientes del sector financiero son usuarios de la banca electrónica, realizan transacciones por internet o pagos a través de dispositivos móviles. Esta adaptación de los modelos de negocio y la explotación de canales digitales pretenden aprovechar las ventajas de las tecnologías, que tiene como contrapartida la aparición de nuevos riesgos que se deben prevenir con el fin de mitigar los posibles ataques y situaciones de fraude a los que está expuesto actualmente el sector y, por supuesto sus usuarios.

En esta línea, el presente estudio elaborado por la OEA, tiene por objeto presentar los resultados y análisis sobre los incidentes de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) que se evidenciaron después de aplicar las encuestas correspondientes al interior de diversas entidades bancarias dentro de América Latina y el Caribe y sus usuarios; así como su impacto en la región. Este documento estructura un estudio sobre la Ciberseguridad en el sector bancario de América Latina y el Caribe.

Uno de los principales insumos del presente estudio fueron las encuestas aplicadas a entidades bancarias, 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 sector Bancario en América Latina y el Caribe: Los instrumentos aplicados ofrecen información en tres secciones. La primera ofrece información sobre los perfiles de las características de las entidades bancarias; 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 desde la perspectiva de los usuarios de las entidades del sector Bancario en América Latina y el Caribe: 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.

Adicionalmente a los resultados específicos obtenidos con los instrumentos citados, hemos contado con importantes aportes de representantes de los organismos más importantes en relación con la Banca de América Latina y el Caribe, así como de organizaciones que a nivel internacional aportan en temáticas que tienen alto impacto en el sector. Para la organización es un privilegio contar con aportes de organizaciones tan relevantes como el Foro Económico Mundial (WEF por sus siglas en inglés), la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT por sus siglas en inglés), el Grupo de Acción Financiera contra el blanqueo de capitales (FATF por sus siglas en inglés), la Federación Latinoamericana de Bancos (FELABAN) y la Asociación Caribeña de Bancos (CAB, por sus siglas en inglés) que con sus artículos nos permiten contar con elementos significativos para contextualizar los retos que supone abordar la ciberseguridad para la Banca de América Latina y el Caribe.

A partir de lo anterior, así como de las investigaciones realizadas con soporte en diferentes referentes abordados en el estudio, se pretende ofrecer conclusiones y recomendaciones pertinentes al sector bancario y sus usuarios, así como a los Gobiernos y sus órganos reguladores con miras a contar con un entorno digital más confiable y seguro para los servicios ofrecidos por este vital sector para la región.

03

APORTES

3.1 Foro Económico Mundial: El panorama de las amenazas a la ciberseguridad en los Bancos de América Latina y el Caribe

Troels Oerting
Director del Centro de Seguridad Cibernética
Foro Económico Mundial (WEF)

Sean Doyle
Investigador Líder Global; Líder del proyecto, Gobernanza y Política, Centro de Seguridad Cibernética
Foro Económico Mundial (WEF)

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

En 2018, los ataques a los Bancos de México y Chile, que fueron destacados en las noticias, dejaron en claro que los servicios financieros de América Latina son un blanco de los delincuentes cibernéticos extranjeros y respaldados por estados. Junto con esta relativamente nueva atención internacional, también es probable que crezcan los recursos de los delincuentes cibernéticos de origen latinoamericano, con una clara evidencia de que programas maliciosos (malware) especializados y desarrollados en América Latina se estén adaptando para el mercado de exportación.

Los delincuentes cibernéticos están organizados, bien financiados y no tienen limitación geográfica. Los ladrones ya no necesitan ingresar a una sucursal bancaria, ni siquiera al país en el que se encuentra su blanco. Los delincuentes sofisticados atacarán el banco que proporcione el mayor retorno de la inversión, independientemente de dónde esté ubicado. Por lo tanto, todos los Bancos deben asegurarse de tener suficientes recursos técnicos, personal adecuadamente capacitado y procedimientos apropiados para defenderse de los delincuentes cibernéticos y garantizar que el negocio sea lo suficientemente resiliente. En América Latina y en todo el mundo, la resiliencia cibernética requiere un compromiso desde el nivel de junta directiva hasta el nivel de sucursal.

Si bien son vitales los esfuerzos individuales para mejorar la seguridad, los delincuentes cibernéticos también identifican debilidades en el ecosistema de un país o en los Bancos de una región, por ejemplo, las prácticas comunes en el procesamiento de pagos o el software de uso común. En consecuencia, es probable que un ataque a un banco lleve a ataques similares a muchos Bancos de la región. Por esta razón, el intercambio eficiente de información entre los Bancos, y entre los Bancos y las agencias estatales, es un factor importante para

aumentar la resiliencia en todo el sistema y reducir tanto el costo financiero como el de reputación de los ataques.

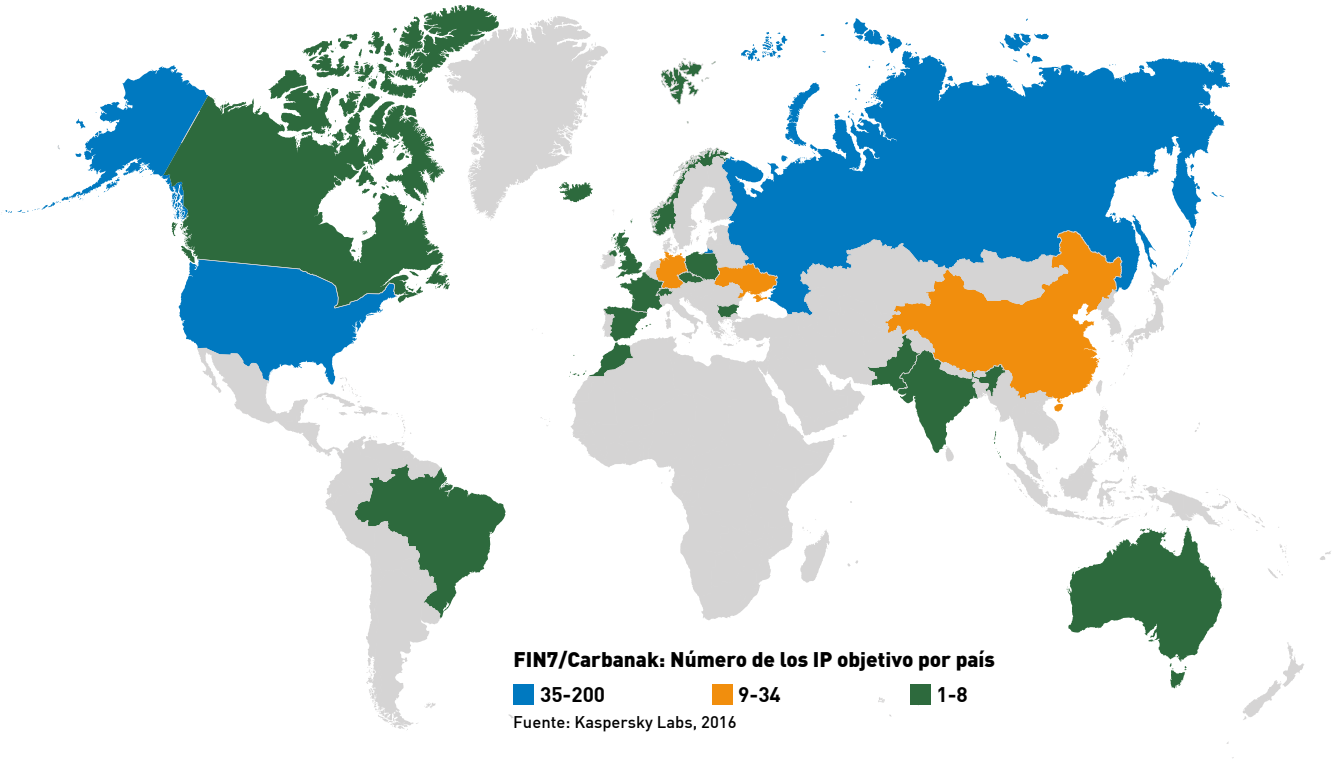
Grupos de delincuentes cibernéticos

Cada vez más, los grupos de delincuentes cibernéticos que le apuntan al sistema financiero son altamente especializados y han adquirido experiencia en sistemas bancarios centrales, sistemas comunes de trabajo bancario, así como métodos para infiltrar y subvertirlos. Estos grupos suelen ser disciplinados, con seguridad operativa efectiva, operaciones estandarizadas, técnicas sofisticadas, con acceso a recursos de desarrollo de software de alta gama, un conocimiento profundo de las redes objetivo y una capacidad de mantener actividades dentro de la red de un banco por un período que dura meses.[4]

Imagen 1: Organización típica de un grupo de delincuentes cibernéticos

Esta sofisticación les permite a estos criminales atacar globalmente. La imagen a continuación proporciona una descripción general de las jurisdicciones que son el blanco de un solo grupo de delincuentes cibernéticos, el grupo Fin7 (también conocido como Carbanak). Se ha determinado que Fin7 ha robado al menos USD 1.000 millones a operadores de servicios financieros en el período 2013-2016, antes de ampliar sus objetivos a una serie de otros sectores en 2016-2018.[5]

Imagen 2: Jurisdicciones en las que el grupo Fin7/Carbanak tuvo como objetivo a los Bancos



Cuando las fuerzas policiales comenzaron a arrestar a miembros de Fin7 en marzo-agosto de 2018[6], se requirió la cooperación de Estados Unidos, Ucrania, Alemania y España, entre otros. En general, la distribución geográfica tanto de los Bancos seleccionados, como de las personas que realizan los ataques, hace que sea difícil para que los Bancos, por separado, preparen defensas efectivas cuando actúan por su cuenta, y complica las gestiones de aplicación de la ley para rastrear y arrestar a los delincuentes después de un ataque exitoso.

Bancos de América Latina y el Caribe

Si bien los informes públicos sobre ataques cibernéticos sofisticados en Bancos de América Latina y el Caribe son menos frecuentes que en América del Norte, Europa y Asia, hay evidencia reciente que muestra que la relativa tranquilidad de la región está llegando a su fin. A mediados de 2018, los Bancos en México fueron blanco de grupos con las características de Amenaza Persistente Avanzada (APT, por sus siglas en inglés) respaldadas por estados[7].

También en 2018, al menos un banco en Chile fue robado por una organización con capacidades importantes, aunque no está claro si esto se atribuye más a delincuentes cibernéticos o a unos APT más avanzados.[8]

Ataques a cajeros automáticos:

Además de ser un objetivo para grupos delictivos internacionales en el futuro cercano, los Bancos latinoamericanos también deben enfrentar a atacantes sofisticados locales. Los ataques a cajeros automáticos (ATM, por sus siglas en inglés) son un área en la que se encuentran entre los líderes mundiales los delincuentes cibernéticos de América Latina. Los logros generados por latinoamericanos con cajeros automáticos, como la familia de malware Ploutus, han demostrado ser tan efectivos y adaptables que los delincuentes latinoamericanos decidieron comercializar con éxito este software para exportación. Por ejemplo, a principios de 2018, la firma de seguridad especializada en Internet de las Cosas (IoT, por sus siglas en inglés), Zingbox,

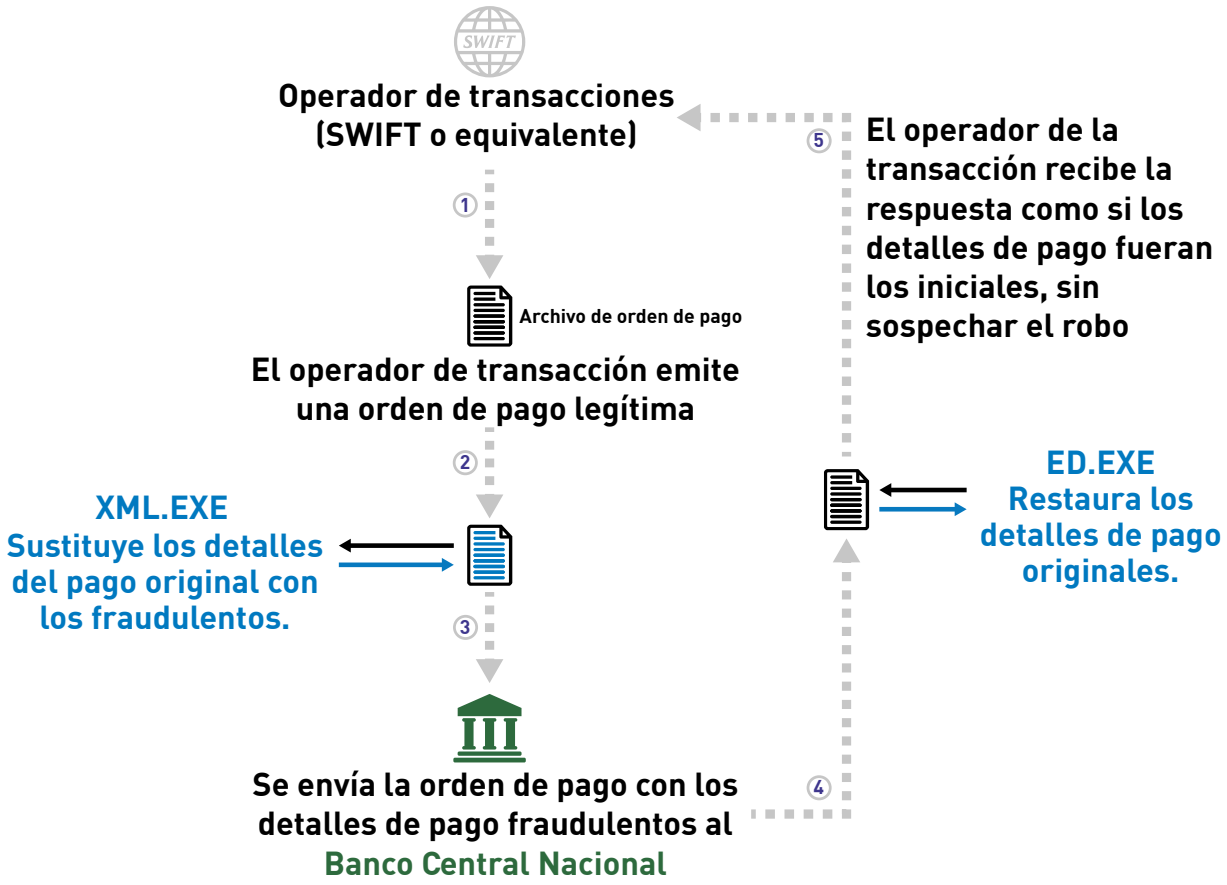
informó que las variaciones de malware Ploutus se estaban vendiendo bajo licencia a agrupaciones delincuenciales en EE. UU. Esta operación fue tan sofisticada que se informó que el sistema de licencias incluía servicios adicionales para el cliente, como capacitación a la fuerza laboral[9].

Estos dos ejemplos, Fin7 y ataques a cajeros automáticos, indican cómo una actividad delictiva que ha demostrado ser efectiva en tener como blancos a Bancos en una región, eventualmente se abrirá camino hacia mercados de América Latina y el Caribe, de la misma manera como el malware ATM Ploutus desarrollado por Latinoamérica pudo llegar a América del Norte.

La nueva superficie de ataque para América Latina: sistemas de pago

Violaciones a los sistemas de pago, como SWIFT, o las variantes nacionales, como el SPEI de México, ocurren en todas las regiones. Estos ataques aprovechan las deficiencias de la arquitectura y los procesos de los sistemas de los Bancos y, en general, no son el resultado de deficiencias de la propia infraestructura de pagos. Por ejemplo, SWIFT, en respuesta a un ataque a un banco latinoamericano en marzo - abril de 2018, declaró que desconocía la "prueba de que la propia red de SWIFT o los servicios centrales de mensajería se habían visto comprometidos alguna vez. Más bien, en cada uno de los incidentes, los clientes sufrieron por primera vez violaciones de seguridad en sus entornos locales"[10]

Imagen 3: Anatomía de un ataque a los sistemas de pagos



La manipulación de estos puntos finales relativamente débiles parece ser la próxima tendencia en la actividad de la delincuencia cibernética. A finales de 2017, la firma privada de seguridad de la información Grupo IB encontró indicios de que grupos sofisticados de delincuencia cibernética especializados en ataques a servicios financieros, como el grupo "MoneyTaker" de habla rusa, estaban recopilando inteligencia sobre los sistemas de pago transfronterizos utilizados por los Bancos en América Latina y América del Norte[11]. Parece claro que esta información está siendo recopilada por delincuentes para lanzar ataques futuros contra Bancos latinoamericanos o caribeños, quizás para lograr resultados similares a los que tuvieron delincuentes cibernéticos que efectivamente subvirtieron el sistema de pago de SPEI en la primavera de 2018[12]. Este ataque fue similar a la supuesta manipulación de la red de transferencia de UniTeller, comprometida por un grupo de Asia oriental en junio de 2016[13].

Es probable que se produzcan ataques selectivos adicionales en el futuro cercano, particularmente a medida que continúen mejorando las defensas sistémicas y con enfoque sectorial en los mercados de América del Norte, Europa y Asia a través de una cooperación mejorada y una regulación más efectiva.

Conclusión

Ante adversarios sofisticados, la seguridad cibernética debe verse ahora como un bien común que depende de un estándar mínimo elevado, en todo el sector y a través de las fronteras.

El costo incurrido por los delincuentes cibernéticos para preparar y ejecutar un ataque está disminuyendo y el riesgo de ser arrestado sigue siendo bajo. En consecuencia, el Centro de Seguridad Cibernética del Foro Económico Mundial estima que los ataques de sofisticación de nivel bajo a medio crecerán en volumen, mientras que la experiencia de un número limitado de grupos no estatales de Amenaza Persistente Avanzada continuará aumentando.

Para neutralizar lo anterior, los Bancos pueden primero concentrarse en acertar en lograr fundamentos técnicos, de fuerza laboral y de gobernanza de la seguridad cibernética. Esto a menudo requiere sacar la seguridad cibernética de su nicho aislado en el negocio y extender la responsabilidad de esta a nivel de junta directiva, que pueda garantizar que la seguridad cibernética sea una problemática central en el momento de definir los productos de la empresa, sus servicios y cómo planea crecer.

Siendo el sector más atacado por delincuentes cibernéticos, los Bancos de América Latina y el Caribe tienen el potencial de observar un panorama detallado de amenazas cibernéticas y los vectores de ataque. La oportunidad de llevar a cabo análisis estratégicos de amenazas emergentes es mayor que en casi cualquier otro sector y podría mejorar significativamente la identificación y contención de ataques si los Bancos trabajan juntos para lograrlo.

Los delincuentes operan de manera transfronteriza y pueden robar o comprar información sobre las redes internas de los Bancos y sus procedimientos operativos. Esta asimetría de la información deja a los Bancos en desventaja. No existe una solución perfecta para este problema, pero hay ejemplos que pueden ser adaptados de otras regiones.

En Estados Unidos, el Centro de Análisis e Intercambio de Información de Servicios Financieros (FS-ISAC)[14] es un foro exitoso para la colaboración entre Bancos y entre Bancos y agencias gubernamentales. En Europa, el Centro del Delito Cibernético de Europol[15] actúa como un punto de recolección, análisis y distribución de inteligencia para la aplicación de la ley en toda la UE. Los proyectos individuales, como el proyecto "No más rescate"[16] dirigido por la policía holandesa y apoyado por el sector privado, han reducido el atractivo que tienen las empresas y organizaciones europeas para los secuestradores de archivos a cambio de un rescate (ransomware). En el Reino Unido, un pequeño número de Bancos se unió a la policía para crear la Alianza de Defensa Cibernética[17] para aumentar la dificultad de atacar a múltiples Bancos con las mismas técnicas.

Cada uno de estos modelos es único, pero todos apuntan al tipo correcto de solución para América Latina: solo a través de una mayor asociación entre Bancos y entre el sector financiero y reguladores y la aplicación de la ley hasta podemos comenzar a combatir este problema. El Centro de Seguridad Cibernética del Foro Económico Mundial está presto a ayudar a desarrollar la capacidad de defensa y fomentar estas asociaciones.

3.2 SWIFT: Nueve mejores prácticas de seguridad cibernética que lo ayudarán a proteger su institución

Juan Martinez
Director Ejecutivo de SWIFT para América Latina y el Caribe

El sector financiero se encuentra entre los sectores económicos más avanzados en lo que respecta al uso de TI y, lógicamente, ha invertido muchos recursos en dichos sistemas de seguridad. Además, es una de las industrias más interconectadas, y un objetivo claro para los ciberdelincuentes. La amenaza y el impacto de los ataques en la industria está aumentando, y el sector está buscando cada vez más formas de enfrentar el riesgo cibernético y la ciberseguridad.

De acuerdo con el Foro Económico Mundial, los ciberataques forman parte de los principales riesgos mundiales. Un análisis reciente indicó que los ataques cibernéticos estuvieron en los 10 principales riesgos en 2016; y entre los primeros 5 en 2017; mientras que para este 2018, figuran entre los tres principales riesgos para la economía global.[18]

Si bien ningún sistema puede ser perfectamente seguro, existe una serie de mejores prácticas que el sector bancario puede emplear para protegerse de los complejos métodos despejados en su contra. Aquí hay nueve mejores prácticas de seguridad cibernética que se aplican en instituciones altamente seguras:

1. Resguarde su entorno

La integración de la seguridad al diseño de la arquitectura de red debería ser un principio fundamental. Esto debe incluir medidas de seguridad físicas, como limitar los derechos de acceso a espacios susceptibles, y procesos establecidos para controlar y monitorear activamente quién entra en dichas áreas. Además, el personal autorizado debe seleccionarse y capacitarse adecuadamente.

2. Conocer el acceso y limitarlo

Después de levantar estas defensas para impedir que los intrusos entren por la puerta principal, hay que instaurar procedimientos y procesos para limitar y proteger los privilegios

de administrador y del sistema. Una vez restringidos, es necesario gestionar las identificaciones con máximo rigor, utilizando reglas de contraseña y perfil aplicables en todo momento y de manera estricta con el fin de garantizar controles de acceso básicos.

3. Detectar y reaccionar

Las medidas preventivas pueden llevarse a extremos, sin embargo, la detección y capacidad de respuesta son igualmente críticas. Las capacidades adecuadas de detección de intrusos, fundamentales para la detección y reacción oportuna deben consistir en una serie de desencadenadores y trampas que detonen una alerta ante cualquier actividad sospechosa.

4. Conozca a su adversario

Para protegerse de un adversario es fundamental conocerlo. La inteligencia sobre las amenazas es pieza fundamental en el desarrollo y las actualizaciones del software antivirus y sus aplicaciones.

5. Limite su exposición

Solo debe hacer negocios con contrapartes de confianza y mantener relaciones con aquellos en los que confía. Controlar cualquier cambio en las relaciones y eliminar cualquier relación no actual es otra forma clave en la que puede limitar su exposición a amenazas potenciales.

6. Implemente controles de seguridad

Participar en ejercicios regulares de evaluación comparativa de seguridad y auditoría de seguridad permite detectar brechas y fallas en sus controles de seguridad. Para ayudar, SWIFT, en conjunto con expertos de la industria, ha publicado un conjunto de controles de seguridad basados en la última inteligencia de amenazas cibernéticas. Éstos reflejan buenas prácticas de seguridad y también deberían aplicarse más allá de la infraestructura relacionada con SWIFT ya que pueden ayudar a fortalecer a su entorno operativo.

7. Implemente controles de negocio

Entender los riesgos crediticios y de cumplimiento de las contrapartidas potenciales es clave para tomar decisiones sobre si hacer negocios con ellos y cómo hacerlo. Las consideraciones cibernéticas también deben formar parte integral de estos procesos Know Your Customer (Conozca a su cliente) de rutina.

8. Otros controles comerciales

Al desplegar más controles comerciales, puede tomar medidas preventivas y correctivas oportunas contra actividades sospechosas. Por ejemplo, al filtrar los mensajes salientes con un conjunto de reglas estrechamente configuradas, puede controlar sus pagos salientes para detectar flujos de mensajes ilícitos o inusuales. Ser capaz de detectar dichos mensajes fuera de la política antes de que se envíen puede alertarlo sobre un posible compromiso, permitirle tomar medidas correctivas inmediatas y, en última instancia, evitar las solicitudes de transferencia fraudulentas incluso cuando los fondos salen de su organización.

9. Plan para respuesta al incidente

La seguridad no es un estado absoluto, prepararse para lo peor es tan importante como defenderse contra ella. Debe desarrollar e instituir una política de recuperación para garantizar que esté equipado para responder rápidamente a la actividad fraudulenta. Si se detectan actividades fraudulentas o sospechosas, deben tomarse medidas apropiadas de inmediato. Con los procesos correctos, los clientes pueden tener la oportunidad de minimizar la pérdida de fraude o aumentar la probabilidad de que se puedan recuperar los fondos.

Igualmente, es importante asegurarse de comprender las acciones internas que debe tomar al responder a un incidente, así como los procesos ensayados para respaldarlos. Lo anterior, debido a que los grupos detrás de los ciberataques están desplegando técnicas cada

vez más creativas para tener acceso a los activos críticos de los usuarios, como por ejemplo, obtener los derechos de administrador para los sistemas operativos, manipular el software en memoria y alterar la funcionalidad legítima para resistir la autenticación de dos factores, etc.

Cómo SWIFT está ayudando a reforzar la seguridad de la industria financiera SWIFT, como una cooperativa de la industria y ante este panorama, se ha comprometido en desempeñar un papel importante en el refuerzo y la protección de la seguridad de un ecosistema más amplio a través del Programa de Seguridad del Cliente de SWIFT, dirigido a clientes de todas las formas y tamaños en geografías cercanas y remotas, sofisticadas y en desarrollo, lanzado en 2016. El objetivo de éste es mejorar el intercambio de información en toda la comunidad, optimizar las herramientas relacionadas con SWIFT para los clientes y proporcionar un Marco de Control de Seguridad del Cliente, compartiendo las mejores prácticas para detectar fraudes y responder a las amenazas cibernéticas más rápidamente.

En concreto, al desarrollar y desplegar el programa regularmente nos comunicamos y consultamos con los reguladores y hemos estado, y seguimos estando, fuertemente comprometidos con nuestros clientes en todo el mundo. Asimismo, hemos realizado seminarios web y talleres, roadshows y mesas redondas, sesiones de capacitación y entrenamientos, atrayendo a más de 14,500 miembros de la comunidad SWIFT, en nuestra apuesta por crear conciencia, competencia y transferir habilidades.

Además, hemos visto evidencia de iniciativas locales construidas y seguidas por las nuestras, con comunidades individuales que eligen trabajar juntas para diseminar conocimiento y compartir experiencias, o con reguladores locales que se enfocan más en la ciberseguridad e incluso obligan a la adopción de nuestra guía. El programa es transformacional porque es la primera vez que el problema de ciberseguridad se ha abordado de manera sistémica y global a través de un enfoque comunitario, independientemente del tamaño, ubicación o el potencial de ingresos de los clientes.

La idea central consiste en proteger los sistemas y redes, así como tener conciencia de que ningún sistema es totalmente seguro, sin embargo, existen formas en que los clientes pueden protegerse mejor de los complejos métodos implementados en su contra, incluyendo su entorno local, administrar el riesgo de seguridad en sus interacciones con contrapartes, compartir información relevante y actuar de manera oportuna con la información de riesgo de seguridad que recibe.

Los adversarios están preparados para invertir una gran cantidad de tiempo en la planeación y preparación de sus ataques. La determinación, paciencia y astucia que demuestre la industria financiera permitirá que los clientes implementen y mantengan rápidamente herramientas y medidas básicas de cuidado cibernético.

3.3 GAFI: IMPLEMENTAR MARCOS LEGISLATIVOS EFECTIVOS PARA COMBATIR EL LAVADO DE DINERO EN LA ECONOMÍA DIGITAL GLOBAL

Santiago Otamendi
Presidente (2017-2018)
Grupo de Acción Financiera Internacional (GAFI)

El delito es un hecho de la especie humana, un hecho únicamente de esa especie.[19] Mientras haya personas que busquen obtener ganancias financieras del delito, es necesario que separen los ingresos del crimen subyacente. El lavado de dinero ayuda a que prospere el crimen organizado, lo que, a su vez, representa una amenaza para la seguridad civil y pone en peligro la estabilidad y el crecimiento económico.

El papel del GAFI es comprender los riesgos del lavado de dinero y el financiamiento del terrorismo, desarrollar y promover políticas y estándares globales para contrarrestar estos riesgos y evaluar a los países en relación a esos estándares y así contribuir a la seguridad.

El primer paso es desarrollar un marco legislativo eficaz para prevenir y castigar el lavado de dinero, protegiendo la integridad del sistema financiero. Este marco les debe proporcionar a los países la autoridad suficiente para identificar, evaluar y comprender cómo los delincuentes lavan el producto de su delito.

Desde la emisión del primer grupo de Recomendaciones del GAFI[20] en 1989 para ayudar a los países a combatir el lavado de dinero, en las que después se introdujeron estándares para contrarrestar el financiamiento del terrorismo, los gobiernos de todo el mundo han logrado avances significativos para implementar un sólido sistema de financiamiento contra el lavado de dinero y contra el terrorismo (ALD/CFT). A medida que los países implementan salvaguardas para detectar, prevenir y sancionar el blanqueo de dinero proveniente de actividades delictivas y el flujo de fondos relacionados con el terrorismo, terroristas y delincuentes continúan adaptándose y encontrando formas de eludir estas salvaguardas para continuar financiando sus actividades delictivas.

Una de las fortalezas del GAFI radica en su capacidad para responder a los riesgos cambiantes del sistema financiero, crear conciencia sobre amenazas nuevas o en evolución y actualizar, si es necesario, sus normas en consecuencia para que los países continúen teniendo las herramientas más fuertes posibles para proteger la integridad del sistema financiero.

Durante los 30 años de existencia del GAFI, la innovación tecnológica ha tenido un impacto significativo en nuestra sociedad y nuestra vida cotidiana. También ha cambiado el panorama financiero, introduciendo servicios y productos que no existían hace tan solo 10 años.

Durante siglos, la estructura bancaria tradicional ha dominado el mercado de servicios financieros. Hoy, la innovación digital ha introducido productos alternativos y nuevas formas para que los clientes administren sus activos y transacciones financieras. La innovación financiera ha entregado eficiencias y tiene el potencial de aumentar la inclusión financiera al ofrecer soluciones digitales a clientes sin acceso a servicios bancarios regulares, particularmente en regiones de bajos ingresos. Sin embargo, también significan nuevos riesgos que deben mitigarse para garantizar que no se abuse de ellos para blanquear dinero o financiar el terrorismo.

La cantidad de proveedores de servicios financieros continúa creciendo. Los proveedores tradicionales de servicios bancarios han respondido introduciendo innovaciones financieras competitivas para mantener su base de clientes. Han invertido de manera importante para desarrollar la experiencia necesaria y tecnología innovadora para competir con los nuevos proveedores de servicios de tecnología financiera (Fintech, por sus siglas en inglés). La innovación financiera ha tenido un impacto en la forma en que se brindan los servicios financieros y también ha introducido nuevos productos financieros, como los cripto-activos.

Los cripto-activos (a veces llamados monedas virtuales o cripto-tokens) pueden ser descentralizados, prácticamente imposibles de sufrir ataques y anónimos. Estas características son atractivas para muchos, incluidos aquellos que desean utilizarlos para el lavado de dinero y el financiamiento del terrorismo. Los cripto-activos involucran una variedad de modelos comerciales, a menudo con muchas partes que operan desde diferentes jurisdicciones. La naturaleza segmentada y transfronteriza de la industria dificulta la regulación. Ha habido una amplia gama de respuestas gubernamentales a los cripto-activos. Algunos gobiernos los clasifican como monedas. Otros los clasifican como productos básicos. Otros más han optado por prohibirlos por completo. Esto ha resultado en una colcha de retazos de diferentes enfoques regulatorios. Esta falta de enfoque común por parte de los gobiernos tiene un impacto negativo sobre la transparencia y crea los espacios para el abuso por parte de los criminales y terroristas.

La naturaleza transnacional de los cripto-activos requiere un enfoque regulatorio global. El GAFI ha identificado oportunidades para mejorar su comprensión de los posibles riesgos de lavado de dinero o financiamiento del terrorismo y está trabajando para desarrollar una estrategia más consistente para gestionar estos riesgos, mientras apoya la innovación financiera responsable y fomenta la inclusión financiera de acuerdo con los requisitos ALD/CFT.

El GAFI reconoce el enorme potencial de la innovación financiera y apoya un desarrollo responsable que no aumente el riesgo de lavado de dinero y financiamiento del terrorismo. La inteligencia artificial y las tecnologías de aprendizaje automático tienen el potencial de contribuir significativamente a una política

ALD/CFT efectiva. Sin embargo, persisten desafíos, como reunir en un solo lugar toda la información relevante que necesitan los Bancos, las autoridades públicas y los desarrolladores de tecnología, de tal manera que no comprometa la privacidad y la confidencialidad.

El GAFI está monitoreando de cerca estos problemas y se está involucrado directamente con las comunidades de tecnología financiera y de tecnología regulatoria (Regtech, por sus siglas en inglés). Después de todo, también les conviene que los productos que desarrollan se consideren que protegen la integridad del sistema financiero y no se consideren vehículos para mover fondos vinculados con el delito o el terror.

En 2015, como parte de un enfoque por etapas para monitorear los avances en la innovación financiera y su impacto en los estándares del GAFI, nuestra entidad emitió la Guía para un enfoque basado en el riesgo para las monedas virtuales *(Guidance for a Risk-Based Approach to Virtual Currencies)*[21]. Esta guía se enfoca en la aplicación de sus estándares relevantes a los cambistas de monedas virtuales convertibles, es decir, el punto de intersección con el sistema regulado.

Desde entonces, el GAFI ha aumentado su comprensión de la innovación financiera y las posibles vulnerabilidades relacionadas con el lavado de dinero y el financiamiento del terrorismo. Con el apoyo del G20, el GAFI ahora revisará sus estándares para identificar dónde podrían necesitar ajustarse o fortalecerse para proporcionarles a países herramientas actualizadas para implementar, dentro de sus marcos legales, regulatorios y operativos nacionales.

El GAFI se dedica a más que solo establecer los estándares globales para combatir el lavado de dinero y el financiamiento del terrorismo. Al igual que la Organización de los Estados Americanos (OEA), los estados miembros de GAFI se responsabilizan unos a otros.

El sistema financiero global es tan fuerte como su eslabón más débil. Por lo tanto, es esencial que haya una implementación global de medidas ALD/CFT sólidas y efectivas. A través de nueve (9) Órganos Regionales al estilo de GAFI (FSRB, por sus siglas en inglés), el GAFI ha establecido una red de 204 países que se han comprometido al más alto nivel político a implementar plena y efectivamente los Estándares del GAFI. El GAFI y cada FSRB evalúan la efectividad de la implementación de los Estándares del GAFI por parte de sus miembros utilizando procedimientos[22] universales basados en la metodología de evaluación del GAFI.

El sólido programa de revisión por pares del GAFI (el proceso[23] de evaluación mutua) se encuentra ahora en su cuarto ciclo, centrándose en la efectividad de los sistemas ALD/CFT de los países evaluados. Los ciclos anteriores demostraron que los países a menudo adoptaban un enfoque de 'casilla de verificación' al implementar medidas ALD/CFT. A veces lograban un alto nivel de cumplimiento técnico con los estándares del GAFI, pero sus medidas no siempre entregaron los resultados esperados como para que fueran considerados efectivos, como procesar con éxito a los delincuentes por estos delitos y confiscar sus ganancias ilegales.

El ciclo actual de evaluaciones tiene un enfoque doble. El cumplimiento técnico, o sea, asegurándose de que las leyes, regulaciones y medidas operativas estén funcionando, sigue siendo importante. Estas medidas son los pilares de un marco sólido para enfrentar el crimen financiero. Sin embargo, un marco efectivo ALD/CFT se basa en la identificación, comprensión y evaluación que tiene un país de los riesgos específicos de lavado de dinero y financiamiento del terrorismo que enfrenta. Las Américas enfrentan riesgos diferentes de los que enfrentan países nórdicos de Europa o Asia, de modo que las medidas que los países deben implementar para lograr que los fondos con vínculos al crimen o al terrorismo se

mantengan fuera del sistema financiero son diferentes. Este enfoque basado en el riesgo es esencial. Le permite a un país usar sus recursos de manera eficiente, enfocándolos en las áreas donde los riesgos son más altos.

En una revisión por pares del GAFI, un país debe poder demostrar que la acción que está tomando está entregando los resultados esperados. Cada evaluación le entrega al país evaluado dos conjuntos de calificaciones que reflejan la medida en que un país ha implementado los requisitos técnicos de las Recomendaciones del GAFI y el nivel de efectividad de sus medidas. Más importante aún, la evaluación da como resultado recomendaciones claras sobre las acciones prioritarias que el país debe tomar. Un sólido proceso de seguimiento asegura que los países tomen las medidas necesarias para abordar las deficiencias reveladas por su evaluación y responsabiliza a aquellos que no toman las medidas necesarias para fortalecer sus sistemas.

Para ayudar a lograr un crecimiento económico fuerte, sostenible e incluyente, promover una mayor inclusión y reducir la desigualdad, el GAFI debe seguir enfocado en la inclusión financiera, en línea con los Estándares del GAFI y los Principios de Alto Nivel del G20 para la Inclusión Financiera Digital. Además, está claro que la eliminación de riesgos y la desmercantilización por parte de los Bancos globales puede llevar a la exclusión financiera y aumentar los riesgos del lavado de dinero y el financiamiento del terrorismo que enfrenta la sociedad, incluso por el aumento del uso de efectivo y de canales no regulados.
La innovación está trayendo muchos desarrollos positivos a la forma en que vivimos, trabajamos y administramos nuestros activos. La innovación financiera, en particular, mejora la inclusión financiera para aquellos que no tienen acceso a productos financieros tradicionales que a menudo son comunidades vulnerables en regiones de alto riesgo.

Ahora más que nunca tenemos que trabajar juntos para asegurarnos de que los delincuentes y los terroristas no se beneficien de la innovación financiera para ocultar su identidad y llevar a cabo sus actividades ilícitas sin ser detectados. El GAFI continuará monitoreando nuevos desarrollos y trabajará con otras organizaciones relevantes para mitigar los riesgos de ALD/CFT. Continuará su diálogo con las comunidades Fintech y Regtech para aumentar la comprensión y conocimiento, y garantizar que la innovación financiera se desarrolle teniendo en cuenta las vulnerabilidades de lavado de dinero y financiamiento del terrorismo.

El GAFI trabajará para desarrollar un enfoque más consistente para gestionar las vulnerabilidades de la innovación financiera y para reducir las lagunas que están surgiendo como resultado de los distintos marcos regulatorios en diferentes países.

3.4 FELABAN: LA CIBERSEGURIDAD EN LA BANCA DE AMÉRICA LATINA Y EL CARIBE

Santiago F. Rodríguez V.
Presidente
Comité Latinoamericano de Seguridad Bancaria
Federación Latinoamericana de Bancos (FELABAN)

La seguridad bancaria ha tenido una evolución progresiva con base en los avances tecnológicos, a los riesgos y amenazas a los que ha estado sometida la banca por la prestación de sus servicios financieros.

Las modalidades delincuenciales en el tiempo cada vez se han ido perfeccionando y han ido buscando vulnerabilidades a los servicios financieros que la banca ha presentado a sus clientes. A partir de los años 90 con el nacimiento del Internet comienzan los primeros ataques informáticos.

La utilización del internet no tiene una conciencia adecuada por parte de los usuarios, comienza la dependencia hacia los proveedores sin establecer medidas de seguridad adecuadas y la información se empieza a almacenar en dispositivos extraíbles de igual manera con pocas medidas de seguridad. Ante este desarrollo, los delincuentes informáticos inician a buscar vulnerabilidades.

En los años 2000, los ataques empiezan a dirigirse a las herramientas encargadas de proteger la información, comienza a extenderse de forma masiva el uso de redes sociales, aparece el riesgo de seguridad derivado de los empleados insatisfechos (insiders) y comienzan a producirse fraudes online.

Para el año 2010, empieza a despegar la Gestión de Seguridad en donde la banca regional comienza a implementar planes sólidos de conciencia en seguridad de la información, los departamentos legales buscan legislación para proteger las infraestructuras críticas, también se busca mayor control relacionado con la privacidad de la información para evitar su fuga y se comienza a utilizar herramientas de cifrado de información.

Con la evolución antes expuesta de los tres (3) factores en referencia a Tecnología, Servicios Financieros y Riesgos, se da paso a la

Ciberseguridad, ya que se emplea la detección de riesgos y amenazas a la Seguridad de información y ésta se brinda básicamente por el uso frecuente de ordenadores.

De aquí en adelante en el caso de América Latina y el Caribe, los principales riesgos informáticos que se presentaron en la banca fueron la clonación de tarjetas, la suplantación de identidad en compras no presenciales y el "phishing". Este último término es utilizado para describir un modelo de abuso informático en el que un ciberdelincuente se hace pasar por la institución financiera para obtener información confidencial del cliente de forma fraudulenta. Sin embargo, para esta fecha ya existieron importantes avances en materia de ciberseguridad y preparación para combatir los delitos informáticos. Se incorporó la tecnología chip en las tarjetas de débito y crédito y el uso en las compras online de un token de seguridad.

A esto se sumó la aparición de un mercado negro de venta de números de cuentas, tarjetas y contraseñas que tuvieron su origen principalmente en Rusia, pero que buscó alianzas con ciberdelincuentes en los diferentes mercados de América Latina y el Caribe.

Estos ciberdelincuentes ampliaron su negocio en la región, porque detectaron que las infraestructuras eran vulnerables y que las entidades bancarias actuaban de manera reactiva, con lo cual los esfuerzos preventivos eran escasos.

Los Bancos en la región estamos enfrentando un avance tecnológico a pasos agigantados que no se ha parado, continúa y continúa más fuerte que nunca. En este campo ya se viene experimentando y enfrentando retos como la digitalización que representa un desafío para el sector financiero, tanto por su giro de negocio como por su seguridad. El sistema financiero se ha convertido en una vía indispensable para tener acceso a los satisfactores básicos y a las oportunidades de desarrollo. Hay diferentes estudios que concluyen que el acceso a los servicios financieros mejora la calidad de vida de las personas e impulsa el desarrollo económico de los países. La innovación y la tecnología han tomado el reto de desarrollar nuevos esquemas y formas de dar un mayor y mejor acceso a las finanzas, pero acompañado de un fuerte esquema en seguridad, con la finalidad de minimizar las diferentes modalidades de los ciberdelincuentes.

Ante estos cambios profundos en la demanda de servicios financieros, los Bancos de la región están respondiendo al reto de la digitalización y la ciberseguridad, con distintas aproximaciones y a distintas velocidades, ya que no todas las entidades bancarias entienden de igual forma el significado de transformarse para ser un banco digital. ¿Pero qué es la banca digital? La literatura no ofrece una definición concisa de este nuevo concepto que, en cualquier caso, contempla cuestiones como la generación de oferta, distribución y venta de productos y servicios financieros a través de canales digitales, la explotación de las últimas tecnologías para conocer mejor al cliente y adelantarse a sus necesidades de forma ágil y conveniente, la omnicanalidad o posibilidad de que el cliente se comunique por todos los canales (analógicos y digitales) con su banco o la automatización de servicios. En general, se espera que la banca digital anteponga las necesidades del cliente final a la creación de productos, siendo éste el centro sobre el que se define la oferta.

En este sentido, los Bancos tradicionales de la región que están apostando por la banca digital están atravesando una transformación que les permita posicionarse en el nuevo ecosistema.

Este posicionamiento en el ecosistema de la banca digital debe ir acompañado de un esquema de seguridad, siendo esto una realidad que determina las estrategias

marcadas por las entidades financieras a nivel regional y mundial. El cliente define sus prioridades exigiendo una experiencia diferente, inmediata y digital, pero con un respaldo de aseguramiento de su información y transacciones. La combinación de estos mundos, banca digital, experiencia de cliente y seguridad, descubre la experiencia del cliente digital seguro, imprescindible en la actualidad y en todos los sectores de la economía, pero particularmente relevante en la construcción del sector bancario futuro.

Los atacantes se han sofisticado y cada vez más buscan objetivos precisos y que ofrezcan una recompensa económica elevada, en lugar de ataques a gran escala al mayor número de usuarios posibles.

La lucha contra la ciberdelincuencia en la región durante el 2016 dio grandes pasos, ya que se incrementaron los recursos a la Ciberseguridad. Sin embargo, ante la mayor investigación y protección contra las amenazas, los ciberdelincuentes continuaron cambiando su modo de actuar y ampliaron sus objetivos, en numerosas ocasiones con unos presupuestos más elevados que los encargados de defender.

A nivel mundial y regional el 2017 fue un año complicado para la Ciberseguridad, donde la banca en la región tuvo que enfrentar ciberataques a gran escala y amenazas contra la seguridad informática como el Ransomware, WannaCry y Petya.

Dmitry Bestuzhev, director del Equipo de Investigación y Análisis para América Latina en Kaspersky Lab, señala que "la seguridad de un banco no es una estrategia estática, sino que necesita evolucionar y adaptarse constantemente, basándose en la inteligencia obtenida sobre las tendencias, las nuevas amenazas y las técnicas de seguridad más recientes para mantener verdaderamente segura la red".

Para estos próximos años uno de los principales riesgos para la banca y que será un reto para la Ciberseguridad en el mundo y en la región, será el Internet de las cosas, que se describe como un mundo donde las cosas están conectadas y son capaz de compartir datos.

GARTNER (Gartner Inc. es una empresa consultora y de investigación de las tecnologías de la información) calcula que el número de dispositivos del Internet de las Cosas conectado a internet en 2025 superará los 75 mil millones. Cada uno de estos dispositivos con su propio sistema operativo, normalmente un firmware simple con un pequeño microprocesador capaz de realizar las tareas simples necesarias para la operación del aparato, su propia dirección IP y siempre conectado.

Muchos millones de estos dispositivos funcionarán con firmware vulnerable, algunos más que otros. No existe la seguridad perfecta, a corto plazo tampoco parece haber un interés de mantener responsabilidad sobre todo aquello que se está fabricando para que sea conectado a Internet. Con 75 mil millones de dispositivos y accesorios online, muchos de ellos con facilidad de ser vulnerados y usados para realizar ataques, estaremos frente a una verdadera bomba.

Para enfrentar y defendernos de este tipo y otros tipos de riesgos, los equipos de ciberseguridad deberán utilizar inteligencia artificial, pero al mismo tiempo los ciberdelincuentes también podrían utilizarla; es decir podrían manipular a lo que hoy son amigables bots y convertirlos en armas letales para vulnerar y penetrar los esquemas de seguridad de las entidades financieras.

De igual manera, para enfrentar esta avalancha de ciberataques, los Bancos en la región están perfeccionando sus esquemas de seguridad y entre las principales gestiones está la implementación de un equipo de respuesta a incidentes de Seguridad Digital (CSIRT), equipo

con la responsabilidad de recibir, revisar, analizar y responder a todo aquel reporte y actividad relacionada con problemas de seguridad de la información.

Otra de las medidas para mitigar los ciberataques en la que ya se trabaja, es la Vigilancia Digital que nos permite ser preventivos y proactivos, con la finalidad de estar preparados para afrontar y resolver los mayores retos de seguridad en el mundo digital. Es decir, ser los ojos y los oídos en el ecosistema, para gestionar y enfrentar el creciente volumen de ciberataques al sistema financiero de la región.

Similar medida a la Vigilancia Digital en la que ya trabajan los equipos de seguridad en la región, son las técnicas de obtención, análisis, elaboración y difusión de datos en fuentes abiertas, donde se puede descubrir relaciones ocultas, seguimiento de modalidades "ciber-delincuenciales" y análisis de patrones. Además de extracción de información no visible a primera vista y que sirva para la toma de decisiones.

Las tendencias de los servicios financieros en la región muestran un panorama fuerte de evolución, adopción de tecnología y mayor conciencia en Ciberseguridad.

Los nuevos vectores de ataque irán creciendo paulatinamente y será necesario un esquema de gestión apropiado en respuesta a las amenazas acompañado de un equipo de seguridad multidisciplinario, organizado, integrado e incorporado dentro de los equipos de transformación digital, para enfrentar las modalidades "ciber-delincuenciales".

Los ataques tendrán un amplio alcance y el cibercrimen continuará profesionalizándose, pues cada vez está más organizado.

3.5 CAB: Retos en la promoción de una industria de servicios financieros cibersegura del Caribe

Joanna Charles
Presidenta
Asociación Caribeña de Bancos (CAB)

CARIBBEAN ASSOCIATION OF BANKS
Keeping the Industry Proactive, Protected and Profitable

Los sistemas financieros mundiales y regionales están cada vez más interconectados, lo que da lugar a importantes economías de escala, una mayor eficiencia y menores costos de transacción para los consumidores. Curiosamente, en general se cree que el sector de servicios financieros es el objetivo más lucrativo para los ataques cibernéticos. A medida que los bancos avanzan para cerrar la brecha tecnológica, los delincuentes cibernéticos también explotan estos avances para organizar ataques cada vez más sofisticados. De hecho, el Informe Global de Riesgos de 2018 del Foro Económico Mundial (WEF, por sus siglas en inglés) ha identificado las amenazas cibernéticas[24] como uno de los cuatro principales riesgos en los que deben concentrarse. Entonces, ¿cómo gestionan los bancos regionales indígenas este riesgo dinámico?

La respuesta a esta pregunta puede ser difícil de entender, en un panorama en el que constantemente cambian y evolucionan las amenazas cibernéticas y la tecnología está redefiniendo continuamente la forma en que los bancos llevan a cabo sus negocios. Además, las características singulares del entorno bancario del Caribe presentan sus propios desafíos. Se puede dividir el espacio financiero regional en tres grandes categorías: bancos extranjeros, que son sucursales o subsidiarias de grupos bancarios norteamericanos mucho más grandes; grandes grupos bancarios indígenas; y pequeños bancos indígenas[25]. El clima operativo que prevalece es el de una economía con uso intensivo de efectivo, con una base de clientes cambiante, avances en nuevas tecnologías financieras, y riesgos derivados del no riesgo por parte de los bancos corresponsales[26].

La disparidad en el tamaño de las instituciones financieras en el Caribe resalta el hecho de que en la mayoría de los casos no se puede emplear un enfoque de 'un modelo único' y se deberán adaptar las soluciones de seguridad cibernética a las necesidades de cada banco por separado. Sin embargo, dado el clima económico similar en el que operan los bancos, se presentan oportunidades únicas para adoptar un enfoque de colaboración en el abordaje de los riesgos cibernéticos. La Asociación de Bancos del Caribe (CAB, por sus siglas en inglés) se ha posicionado estratégicamente para facilitar esta colaboración y promover el intercambio de mejores prácticas. La CAB se estableció en 1974 y actualmente representa setenta y ocho (78) instituciones miembros. El alcance de la membresía de la CAB se extiende desde las Bahamas, en el norte,

hasta Guyana y Suriname en el sur y comprende tanto el Caribe de habla inglesa como holandesa.

Las instituciones financieras caribeñas son plenamente conscientes de la importancia de contar con una organización ciberresistente y de las consecuencias catastróficas que tendría una violación cibernética, que incluye daños a la reputación del banco, pérdida de la confianza y lealtad de los clientes, y severas sanciones legales y regulatorias. La mitigación de estos riesgos acarrea cargas adicionales a los recursos limitados de los bancos caribeños más pequeños; recursos que también se deben utilizar para abordar cuestiones tales como el cumplimiento de los cambiantes requisitos regulatorios nacionales, regionales e internacionales, y un clima sensible de banca corresponsal. Sin embargo, los bancos caribeños le están otorgando gran importancia a cada paso del ciclo de seguridad cibernética, que se puede definir en prevención, detección y respuesta. También están tomando las medidas necesarias para combatir y mitigar las amenazas cibernéticas.

Estas medidas pueden tomar muchas formas. En general, deberían ser factores habilitantes para la resiliencia cibernética en el banco y pueden incluir pasos como[27]:

1. Establecer la estructura correcta de gobernabilidad para hacer de la seguridad cibernética una prioridad a nivel de junta directiva y desarrollar indicadores líderes para identificar las brechas de manera temprana;

2. Identificar los riesgos para la seguridad de las instituciones financieras al definir su apetito de riesgo y su perfil cibernético, implementar mecanismos de monitoreo efectivos y evaluar constantemente el panorama de las amenazas;

3. Identificar y proteger procesos comerciales críticos; y

4. Mejorar la recopilación, el análisis y el informe de la inteligencia cibernética y alinear la seguridad cibernética con los procesos del negocio.

Las instituciones financieras deben garantizar que existan numerosas redes de seguridad y niveles de supervisión en caso de violación, ya que independientemente de cuán preparados estén, habrá brechas que probablemente explotarían los cibercriminales. Por ejemplo, aunque los miembros de CAB adelantan capacitación en seguridad cibernética de manera rutinaria para su personal, todavía se están reportando incidentes de suplantación de identidad (phishing).

La armonización de la seguridad cibernética, la privacidad de los datos y la legislación sobre tecnología de la información y las comunicaciones (TIC) son un componente fundamental para facilitar el desarrollo de una industria cibersegura de servicios financieros. Si bien la CAB celebra el progreso que la CARICOM ha logrado en este sentido, es necesario un mayor sentido de urgencia y voluntad política para implementar las legislaciones armonizadas requeridas. La falta de armonización de la legislación inhibe la capacidad de aprovechar eficazmente las mejores prácticas de otras instituciones de servicios financieros en la región a la vez que limita el intercambio de ideas y la posibilidad de consolidación de funciones clave para navegar de manera efectiva el panorama de la amenaza cibernética. Hasta cierto punto, estas ineficiencias limitan la combinación de recursos y experiencia que podrían asignarse hacia estructuras de seguridad cibernética más sólidas.

Además, no puede subestimarse la necesidad de desarrollar una mayor capacidad de profesionales de seguridad cibernética en la región. Es importante fomentar un entorno propicio que facilite el desarrollo de estos profesionales en diversos sectores, como en las fuerzas de la ley, los servicios financieros, las telecomunicaciones y otros órganos económicos críticos, públicos y privados. Los programas educativos para generar experiencia en los profesionales cibernéticos

y para crear concienciar en los profesionales de servicios financieros sobre la importancia de la seguridad cibernética son también un componente estratégico clave para afrontar esta amenaza regional.

En este sentido, la CAB se ha dedicado activamente a educar a sus miembros en la necesidad de mitigar las amenazas cibernéticas y la resiliencia. Varias conferencias CAB han incluido paneles y presentaciones, por parte de importantes compañías, sobre la necesidad de contar con seguridad cibernética y sobre cómo pueden gestionar eficazmente las instituciones financieras sus riesgos cibernéticos. Estas presentaciones facilitan el diálogo abierto entre los presidentes, gerentes, personal técnico y expertos en seguridad cibernética, y crea una plataforma en la que los líderes de la banca regional incluyen a los profesionales de seguridad cibernética. Además de la Conferencia de la CAB anual, la CAB organiza conferencias para su afiliada, la Asociación Caribeña de Miembros del Comité de Auditoría, y destaca la seguridad cibernética como una problemática importante para crear conciencia en todos los frentes.

El nuevo Reglamento General de Protección de Datos de la Unión Europea (RGPD) es otra área en la que la CAB ha brindado capacitación y conocimiento a la Región. La consecuencia del incumplimiento de esta regulación son multas de hasta dos por ciento (2%) de la facturación global o diez millones de euros (lo que sea mayor) por incumplimiento de primer nivel, y hasta cuatro por ciento (4%) de la facturación global o veinte millones de euros (lo que sea mayor) por incumplimiento de alto nivel. Consciente de las graves implicaciones que tiene esta regulación para las instituciones financieras regionales y cómo estas gestionan la privacidad de los datos y la seguridad cibernética, la CAB organizó un seminario en línea sobre RGPD para la industria, así como un panel de debate en el Foro de Presidentes de la CAB, que fue facilitado por sus miembros de servicio Deloitte e Hitachi Systems. Además, la CAB hizo una presentación ante el Consejo para las Finanzas y Planificación (COFAP) de CARICOM para que los jefes de los gobiernos regionales estuvieran al tanto del problema y redactaran una respuesta regional necesaria.

Para ayudar a las instituciones financieras regionales a medir su nivel de "preparación en seguridad cibernética", la CAB hizo circular el Cyber Resilience Review (CRR), un paquete de autoevaluación desarrollado por la Universidad Carnegie Mellon y el gobierno de Estados Unidos y alentó a los miembros a diligenciar la evaluación para determinar dónde existían sus deficiencias o lagunas.

La CAB también proporciona Protección de Seguros Grupales a instituciones financieras regionales a través de su alianza con Howden UK Group Limited. Howden ofrece protección a las instituciones financieras del Caribe en la Política Integral de Delitos, Delitos Cibernéticos y Responsabilidad Civil de CAB. Actualmente, la cobertura ofrecida por Howden es de entre USD 2,000,000 y USD 20,000,000 por banco miembro. Desde 2012, Howden ha liquidado el 100% de las reclamaciones, que incluyen instrucciones de pago fraudulentas, clonación de tarjetas de plástico (skimming), robo a cajeros automáticos y delitos cibernéticos.

De ninguna manera ha estado la industria de servicios financieros del Caribe apartada de las amenazas cibernéticas y, si bien los bancos regionales continúan utilizando recursos para garantizar la continuidad de las operaciones digitales y la competitividad, también están invirtiendo en mecanismos para mitigar los riesgos cibernéticos. A la luz de esta gran amenaza que enfrenta el sector financiero en la región, la CAB cree fervientemente que es oportuno que todas las partes interesadas desempeñen su papel e implementen los mecanismos habilitantes para mitigar los riesgos cibernéticos, asegurando así el crecimiento continuo, la estabilidad y la seguridad de la industria financiera regional.

04

CIBERSEGURIDAD EN LAS ENTIDADES DEL SECTOR BANCARIO EN AMÉRICA LATINA Y EL CARIBE

Según el Informe Global de Riesgos del Foro Económico Mundial 2018, los ciberataques a gran escala y las filtraciones o robos masivos de datos están considerados dentro de los cinco (5) principales riesgos más probables en la próxima década a nivel global. "Los riesgos de ciberseguridad también están creciendo, tanto en su prevalencia como en su potencial disruptivo. Los ataques contra empresas casi se han duplicado en cinco años, y los incidentes que una vez se consideraron extraordinarios se están volviendo cada vez más comunes." (WEF, 2018).

Teniendo en cuenta que el sector de servicios financieros, el cual incluye al sector bancario, se considera como uno de los sectores económicos con más alto grado de digitalización, el cual se apoya fuertemente en las Tecnologías de la Información y las Comunicaciones, en especial el Internet; dada la creciente relevancia del entorno digital sobre las actividades de las entidades bancarias en la región América Latina y el Caribe, y su alto dinamismo e incidencia en otros sectores económicos, esta situación ha traído consigo en los últimos años un conjunto de riesgos, amenazas, vulnerabilidades e incidentes de diversos tipos, a los que han estado expuestos tanto estas organizaciones como sus usuarios.

Según la información recolectada por la *Federación Latinoamericana de Bancos* (FELABAN), el volumen de los activos bancarios (sin descontar el pasivo de las entidades) en América Latina alcanzó unos USD $4,2 billones de dólares a 31 de diciembre de 2017. Adicionalmente, las utilidades netas (ganancias) acumuladas por el conjunto del sistema bancario en la región a la misma fecha fueron de USD $53 mil millones de dólares, con un incremento del 13,9% aproximadamente respecto del año anterior. Según FELABAN, "con corte diciembre de 2017, el sistema bancario de América Latina incrementó sus activos en un ritmo de 2,53% anual. El año 2017 resultó ser un año de recuperación de las principales economías que sufrieron las consecuencias de una recesión o de una desaceleración de la economía. En el año 2017 la leve recuperación económica regional, aunada a un ambiente favorable para las finanzas a nivel internacional, una inflación doméstica controlada, y una gestión prudente de los administradores de las entidades bancarias, ha dado como fruto algunos hechos que bien vale la pena mencionar."

Con el fin de elaborar el presente Estudio sobre el Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe, la Secretaría General de la Organización de los Estados Americanos (SG/OEA) elaboró un instrumento con el fin de obtener información sobre los aspectos relacionados y sobre incidentes de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) en entidades bancarias y su impacto en la región.

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

- Caracterización de las entidades bancarias
- Gestión de riesgos de seguridad digital
- Impacto de los incidentes de seguridad digital

Con el propósito de asegurar la confidencialidad de la información tanto para las personas responsables que respondieron el cuestionario como para las organizaciones a las cuales pertenecen, es importante tener en cuenta que la SG/OEA no solicitó información alguna que pudiera ser identificada tanto a nivel personal como de la organización. Todas las respuestas fueron compiladas, analizadas y distribuidas a nivel agregado, es decir, por bloques temáticos, sin que la misma se haga disponible a persona o institución alguna en detalle.

Adicionalmente y para mayor claridad durante la tramitación del instrumento se informó a los participantes de que un evento de seguridad digital se consideraría como la suma de ataques exitosos y de ataques no exitosos que sufrió la institución durante un periodo de tiempo, y de igual manera se consideraría como un incidente de seguridad digital al total de ataques exitosos que sufrió la institución durante el mismo periodo de tiempo.

4.1 Caracterización de la entidad bancaria

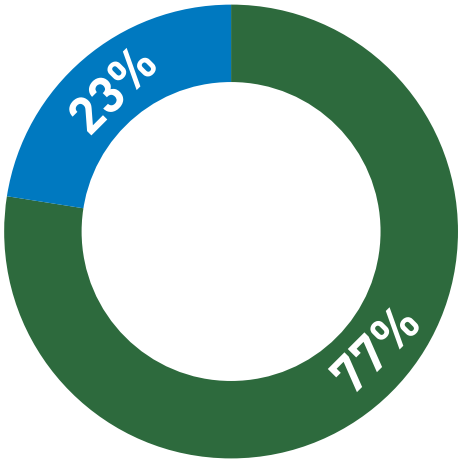
De un total de 552 respuestas obtenidas durante el periodo de publicación del instrumento de recolección de información (meses comprendidos durante el primer trimestre del año 2018) y a partir de la revisión detallada, se estableció una base de datos con registros de 191 entidades bancarias en diecinueve (19) países de la región América Latina y el Caribe. Se estima que la muestra de entidades bancarias a partir de las cuales se presentan los resultados de este estudio alcanzó unos activos bancarios de USD $1 billón de dólares y unas utilidades netas de USD $10,5 mil millones de dólares a 31 de diciembre de 2017.

Las preguntas del instrumento estuvieron orientadas a ser respondidas por la entidad bancaria a la cual el funcionario que respondió pertenecía a nivel local (es decir, el banco que operaba en el país en el que se encontraba), aun cuando la institución fuera la casa matriz del banco o fuera una sucursal, subordinada (filial o subsidiaria) o agencia de un banco 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 23% de las entidades bancarias entrevistadas correspondían a casa matriz del banco, mientras que el 77% correspondían a una sucursal, subordinada (filial o subsidiaria) o agencia de un banco o un grupo financiero.

Gráfica 1. Casa Matriz o Sucursal, Subordinada o Agencia de la entidad bancaria

Con el fin de clasificar a las entidades bancarias de la región América Latina y el Caribe por tamaño se tuvo en cuenta la metodología presentada en el estudio Banco Interamericano de Desarrollo (BID) y la Federación Latinoamericana de Bancos (FELABAN) del 2014, en donde se considera un Banco Pequeño a una entidad que tiene menos de 300 empleados, o que contando con más de 300 empleados posee hasta 10 sucursales, un Banco Mediano a una entidad bancaria que tiene entre 301 y



Nota: 191 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

5.000 empleados y entre 11 y 150 sucursales y un Banco Grande a una entidad bancaria que posee más de 150 sucursales.

A continuación, se presenta la clasificación de las 191 entidades teniendo en cuenta la cantidad de empleados y de sucursales que tiene el banco al cual pertenecía el funcionario que rellenó el cuestionario (en el país en el que se encontraba). Por ejemplo, del total de la muestra se aprecia que 57 entidades bancarias tienen menos de 300 empleados y poseen hasta 10 sucursales o que 23 entidades tienen más de 5.000 empleados y poseen más de 151 sucursales.

Cuadro 2. Distribución de las entidades bancarias por cantidad de empleados y de sucursales

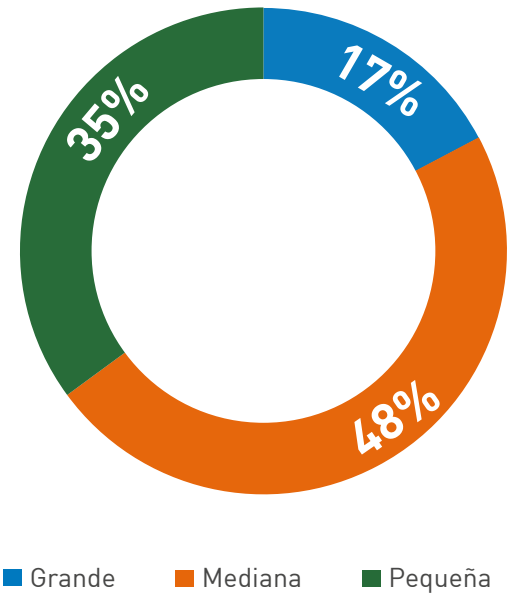
Cantidad de Empleados	Cantidad de Sucursales				
	Hasta 10 sucursales	De 11 a 50 sucursales	De 51 a 150 sucursales	Más de 151 sucursales	Total
Hasta 300 empleados	57	10			67
Entre 301 y 999 empleados	16	22	2		40
Entre 1.000 y 4.999 empleados	5	17	29	8	59
Más de 5.000 empleados	2			23	25
Total	80	49	31	31	191

Nota: 191 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Con la información anterior, se logró clasificar a las entidades bancarias por tamaño así: el 35% de la muestra se consideran como Bancos pequeños, el 48% como Bancos medianos y el 17% como Bancos 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 tiene en cuenta el tamaño de la organización.

Gráfica 2. Distribución de las entidades bancarias por tamaño (grandes, medianos y pequeños)

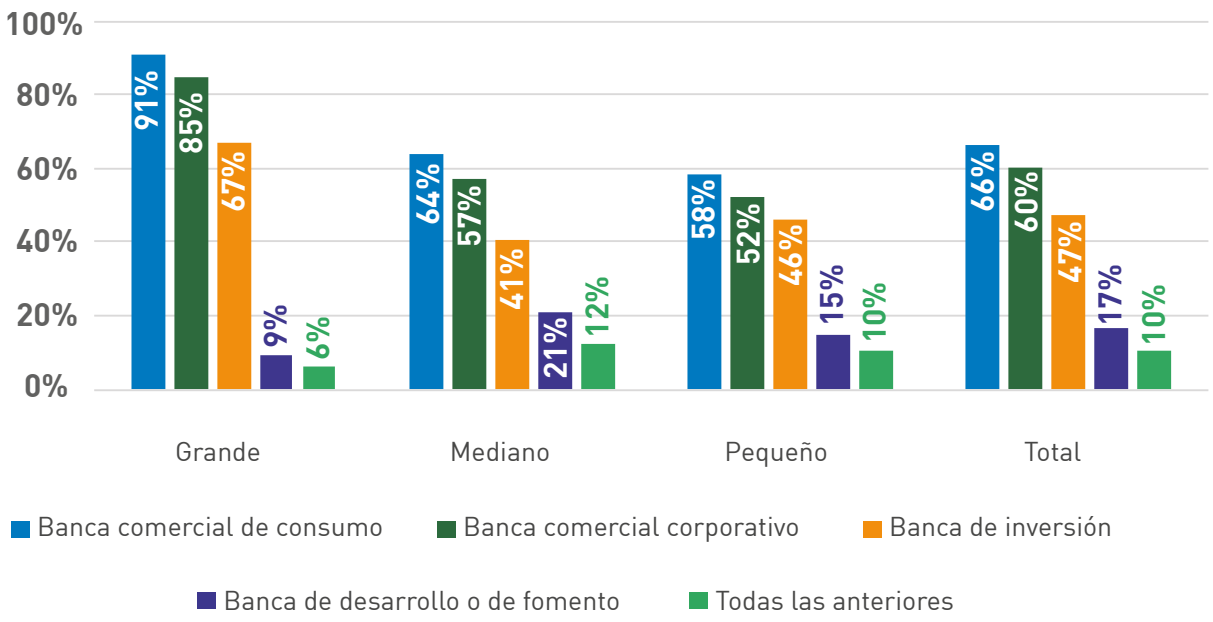


Nota: 191 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

De esta manera, se aprecia que el 66% del total de entidades bancarias entrevistadas prestaba servicios de banca comercial de consumo (en el país en el que se encontraba el empleado que respondió al instrumento), el 60% del total prestaba servicios de banca comercial corporativa, el 47% del total prestaba servicios de banca de inversión, el 17% del total prestaba servicios de banca de desarrollo o de fomento y el 10% del total prestaba todos los anteriores servicios.

Al analizar por tamaño de banco y por tipo de servicios de banca se aprecian algunas situaciones particulares. Por ejemplo, mientras que el 91% de los Bancos grandes presta servicios de banca comercial de consumo tan sólo el 58% de los Bancos pequeños lo hace, o mientras que tan sólo el 9% de los Bancos grandes prestan servicios de banca de desarrollo o de fomento, el 21% de los Bancos medianos prestan dichos servicios.

Gráfica 3. Tipo de banca



Nota: 191 registros

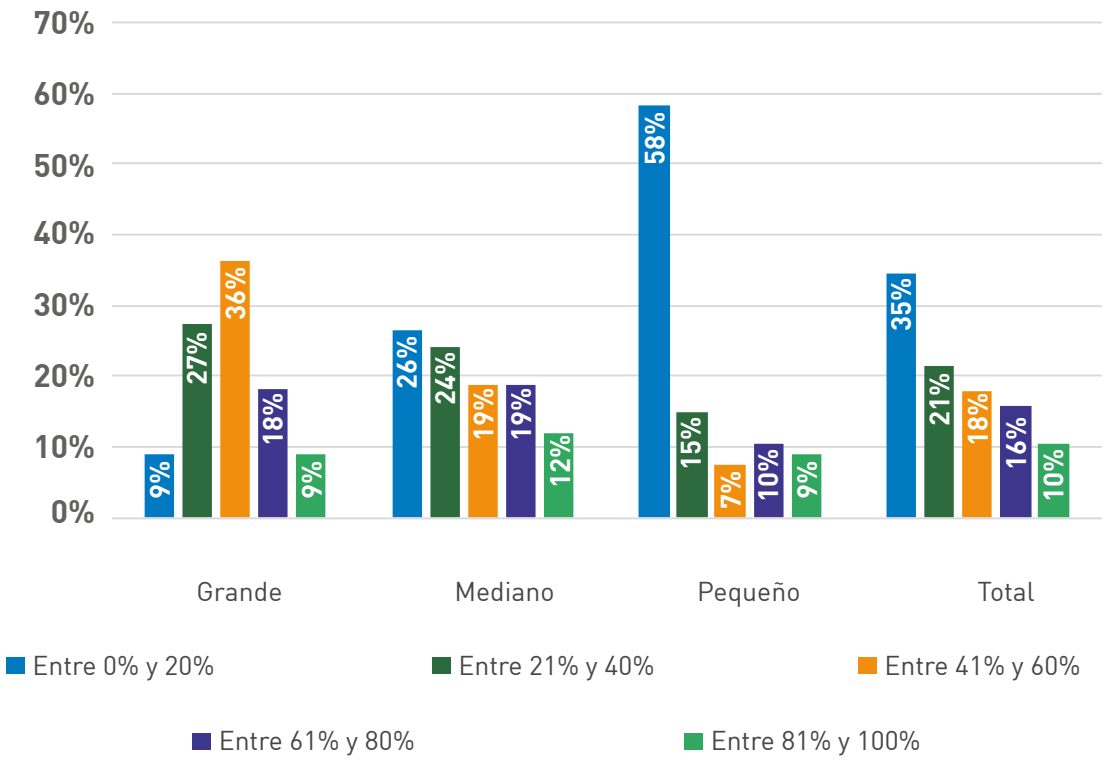
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Teniendo en cuenta el tipo de propiedad del banco al cual pertenece el empleado que respondió la encuesta (en el país en el que se encontraba), se aprecia que el 79% del total de la muestra son Bancos privados (100% de capital privado), el 13% son Bancos públicos (100% de capital público) y el 8% son Bancos mixtos (compuesto por capital tanto público como privado). Al analizar por tamaño de banco, tan sólo el 3% de los Bancos grandes son Bancos públicos mientras que el 20% de los Bancos medianos son públicos. De igual manera, mientras que el 15% de los Bancos grandes son Bancos mixtos tan sólo el 3% de los Bancos pequeños tienen capital compuesto por capital tanto público como privado.

Ahora, el 77% de las entidades bancarias entrevistadas (en el país en el que se encontraba el empleado que respondió el instrumento) tienen mayoría del capital social de origen nacional, mientras que el 23% de los Bancos tienen capital con mayoría de recursos de origen extranjero.

Al analizar el porcentaje de operaciones que se realizaron en el banco por medio de canales transaccionales no presenciales (Internet, transacciones electrónicas, cajeros automáticos, pagos automáticos, telefonía móvil y audio respuesta) del total de operaciones del banco durante el año 2017, se aprecia que el 35% de los Bancos de la muestra tuvieron entre un 10% y 20% de sus operaciones por medio de canales transaccionales no presenciales. Al analizar por tamaño de banco, se aprecia por ejemplo que tan sólo un 9% de los Bancos grandes tuvieron entre un 10% y 20% de sus operaciones por medio de canales transaccionales no presenciales mientras que el 58% de los Bancos pequeños tuvieron operaciones en dicho rango.

Gráfica 4. Porcentaje de operaciones que se realizaron por medio de canales transaccionales no presenciales



Nota: 191 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

A medida que crece el banco, crecen las operaciones por medio de canales transaccionales no presenciales en la región y por consiguiente aumenta su presencia en el entorno digital, sus riesgos de seguridad digital y su necesidad de fortalecer su estrategia de transformación digital. "*Con el 85% de los Bancos identificando la implementación de un programa de transformación digital como prioridad comercial para 2018, la inversión en tecnología para impulsar la eficiencia, gestionar los riesgos en evolución y beneficiarse de las oportunidades de crecimiento será fundamental para el éxito sostenible*" (EY, 2018).

4.2 Gestión de riesgos de seguridad digital

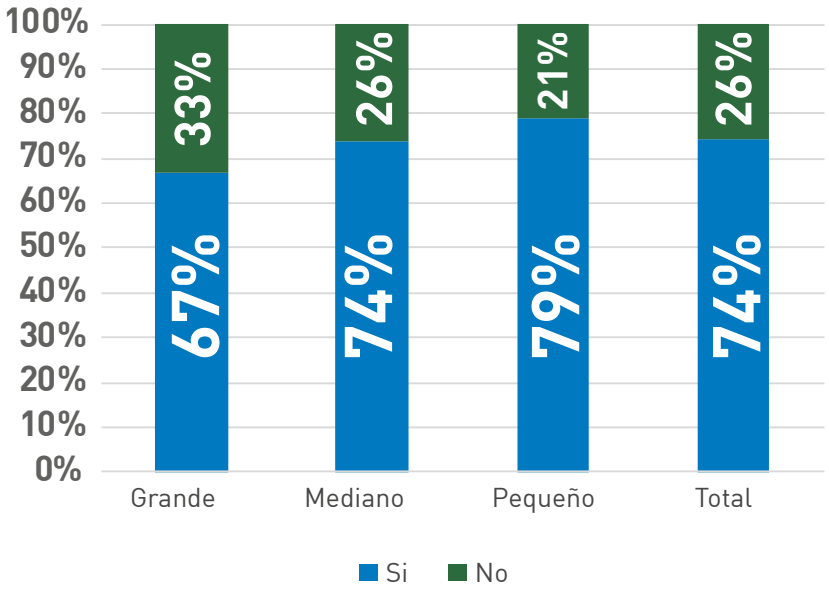
Como parte del estudio a entidades bancarias, se realizaron una serie de preguntas con respecto a la gestión de riesgo de seguridad digital. Estas preguntas se formularon con el propósito de evaluar los principales aspectos y asuntos relacionados con los siguientes temas:

- Preparación y gobernanza
- 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 bancarias entrevistadas (74%) mencionaron que en su organización y en el país en el que se encontraba el funcionario que respondió el instrumento, existe una única área responsable de la seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales). Vale la pena destacar que a medida que crece el banco, aumentan las áreas responsables de la seguridad digital, ya que el 79% de los Bancos pequeños tienen una única área versus el 67% de los Bancos grandes.

Gráfica 5. Área única responsable de la seguridad digital en la entidad bancaria

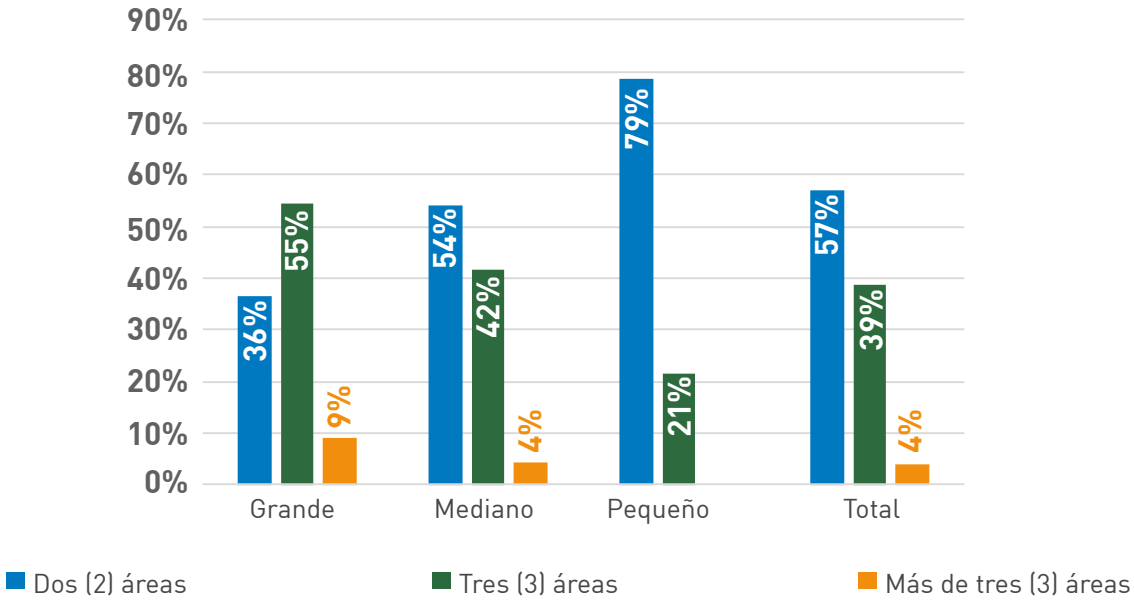


Nota: 191 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Así, del total de entidades bancarias que mencionaron que existían varias áreas con la máxima responsabilidad en materia de seguridad digital (49 de 191), se concluye que el número de dichas áreas depende del tamaño de la organización. Por ejemplo, al analizar la situación para los Bancos grandes se aprecia que el 36% tienen dos (2) áreas, el 55% tienen tres (3) áreas y el 9% tienen más de tres (3) áreas. Por su parte, el 79% de los Bancos pequeños tienen dos (2) áreas, mientras que el resto (21%) tienen tres (3) áreas.

Gráfica 6. Áreas responsables de la seguridad digital en la entidad bancaria al no existir un área única



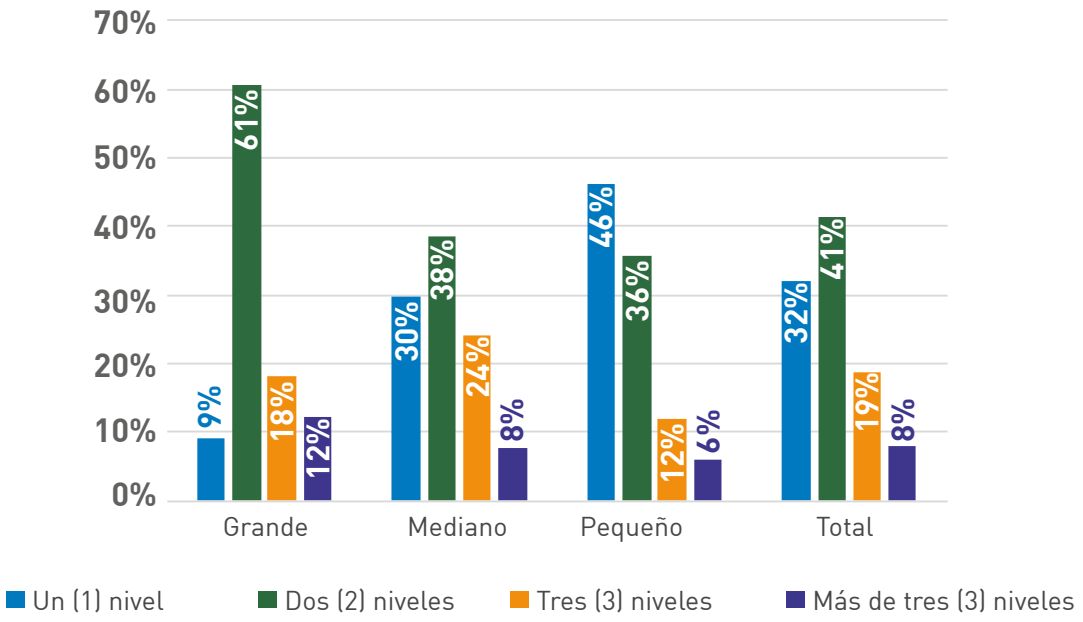
Nota: 49 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Entendiendo que el Director Ejecutico (CEO) del banco se consideraría la cabeza de la entidad bancaria en el país (Nivel 0 o Nivel A) 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 digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) dependen también del tamaño de la organización en la región. Por ejemplo, en el 46% de los Bancos pequeños el máximo responsable reporta directamente al CEO, es decir está a un (1) solo nivel, mientras que tan sólo en el 9% de los Bancos grandes ocurriría dicha situación. En el 61% de los Bancos grandes existirían dos (2) niveles entre el CEO y el máximo responsable de la seguridad digital. A medida que crece el banco, aumentan el número de niveles jerárquicos entre el CEO y el responsable de la seguridad digital.

Al analizar la muestra completa, se aprecia que en el 41% de los Bancos en la región existen dos (2) niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital. Esta situación promedio guarda relación con otros estudios relacionados tales como ISACA (2018) que concluye: *"El 43% de los encuestados indica que su función de seguridad informa a un puesto específico de seguridad de nivel C."*

Gráfica 7. Número de niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital



Nota: 191 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

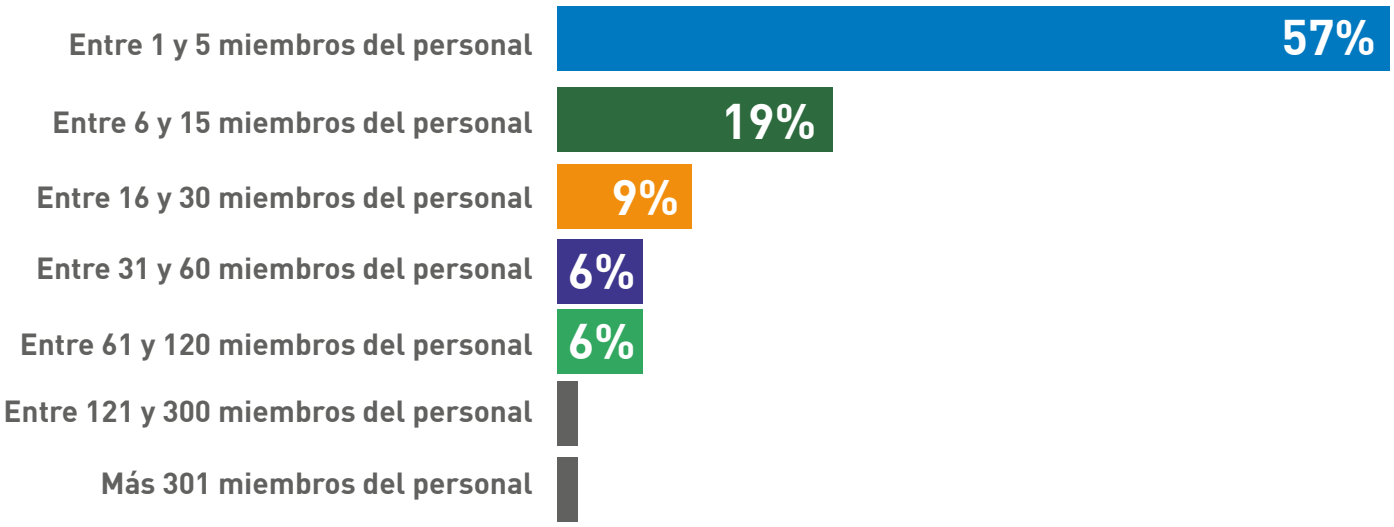
En el sector bancario de la región América Latina y el Caribe, la denominación más común del cargo que tiene el máximo responsable de la seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) es *Oficial de Seguridad de la Información (ISO).* No obstante, en la mayoría de los Bancos grandes (42%) la denominación es *Oficial Principal de Seguridad de la Información (CISO), mientras que en el 23% de los Bancos medianos se denomina Gerente de Seguridad de la Información (ISM).*

Un aspecto importante en torno a la preparación y gobernanza en torno a la seguridad digital es la tercerización de actividades relacionadas con la seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) por parte de la organización. 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), el Monitoreo de la Infraestructura de Seguridad (37% del total), el Monitoreo de Controles de Seguridad (20% del total) y los Servicios de Seguridad en la Nube* (19% del total).

Los resultados para el sector bancario en la región son consistentes con otros estudios realizados a organizaciones a nivel global. Por ejemplo, el estudio CISCO (2018) concluyó del análisis de su muestra que *"entre los profesionales de seguridad, el 49 por ciento dijo que subcontrató servicios de monitoreo en 2017; (...) 47 por ciento de respuesta a incidentes tercerizados en 2017"*. Ahora, respecto de la contratación de servicios tercerizados por parte de las entidades bancarias, es importante reconocer que dicha acción podría aumentar la exposición a incidentes de seguridad digital: *"Casi la mitad del riesgo de seguridad que corren las organizaciones surge porque tienen múltiples proveedores y productos de seguridad"* (CISCO, 2018).

Con respecto del tamaño del equipo que maneja procesos asociados a la seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales), se aprecia que en promedio un banco en la región América Latina y el Caribe cuenta con un equipo conformado por diecisiete (17) personas. Al estimar dicho personal por tamaño de entidad, se obtiene lo siguiente: un equipo de cuarenta y nueve (49) personas en promedio en un banco grande, un equipo de dieciséis (16) personas en promedio en un banco mediano y un equipo de cuatro (4) personas en promedio en un banco pequeño. En comparación con otros estudios a nivel global, se destaca la conclusión del estudio CISCO (2018): "*En 2017, la mediana del número de profesionales de seguridad en las organizaciones fue de 40, un aumento significativo con respecto a la mediana de 2016 de 33*".

Gráfica 8. Personas que conforman la totalidad de equipos que manejan procesos asociados a la seguridad digital



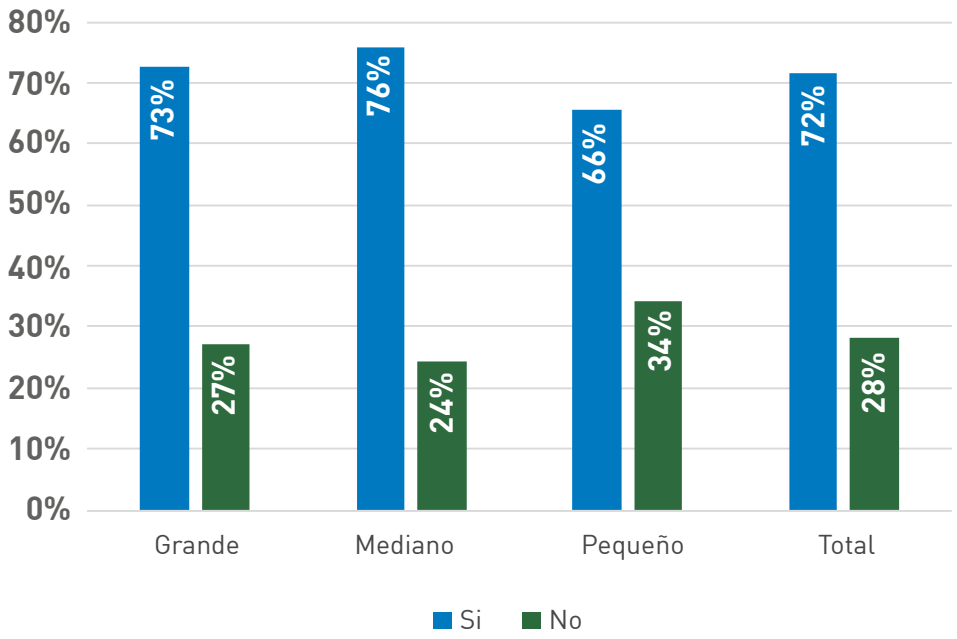
Nota: 191 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Pese a la presencia de equipos responsables de la seguridad digital en este tipo de organizaciones, el 82% de entidades bancarias en la región considera adecuado que este equipo creciera en el corto plazo. Se destaca que el 15% de los Bancos grandes, el 16% de los Bancos medianos y el 22% de los Bancos pequeños consideran que el tamaño de los equipos se debería mantener.

Como parte del modelo de gobierno de las entidades bancarias, la junta directiva del 72% de los Bancos en la región recibe reportes periódicos acerca de indicadores y gestión de riesgos de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales). Se destaca la diferencia entre Bancos grandes y medianos con Bancos pequeños, en donde se aprecia que el 66% de éstos últimos mantienen dicha práctica.

Gráfica 9. ¿La junta directiva de la entidad bancaria recibe reportes periódicos acerca de indicadores y gestión de riesgos de seguridad digital?



Nota: 191 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

El conocimiento de la gestión de riesgos de seguridad digital por parte de las instancias de decisión en las organizaciones, y en especial en el sector bancario, es fundamental con el fin de priorizar esfuerzos y destinar recursos de manera eficiente. Esto se ha reconocido por varios estudios de ciberseguridad en torno a la materia a nivel internacional:

- *"Los equipos de liderazgo de los Bancos reconocen que la ciberseguridad es una prioridad fundamental, particularmente en lo que se refiere a la protección contra ataques externos." (EY, 2018)*

- *"Los CEO de todo el mundo identifican las amenazas cibernéticas como la amenaza comercial más preocupante. (...) El 87% de los CEO globales dicen que están invirtiendo en ciberseguridad para generar confianza con los clientes." (PwC, 2018).*

- *"La ciberseguridad sigue siendo una preocupación de alto riesgo, para el 84% de los ejecutivos y directores, seguido por el riesgo de cumplimiento (49%) y el riesgo estratégico (38%)." (BANKDIRECTOR, 2018)*

Según los resultados, el manejo de la gestión de la seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) en la mayoría de las entidades bancarias en la región América Latina y el Caribe se prepara en el marco de un Comité de Riesgos (39% del total). En los Bancos de la región también existen otras instancias de manejo estratégico en relación con el tema como el Comité de Seguridad (23% del total) o un Comité Técnico o de Tecnología (21% del total). Dicha situación es similar a la analizada

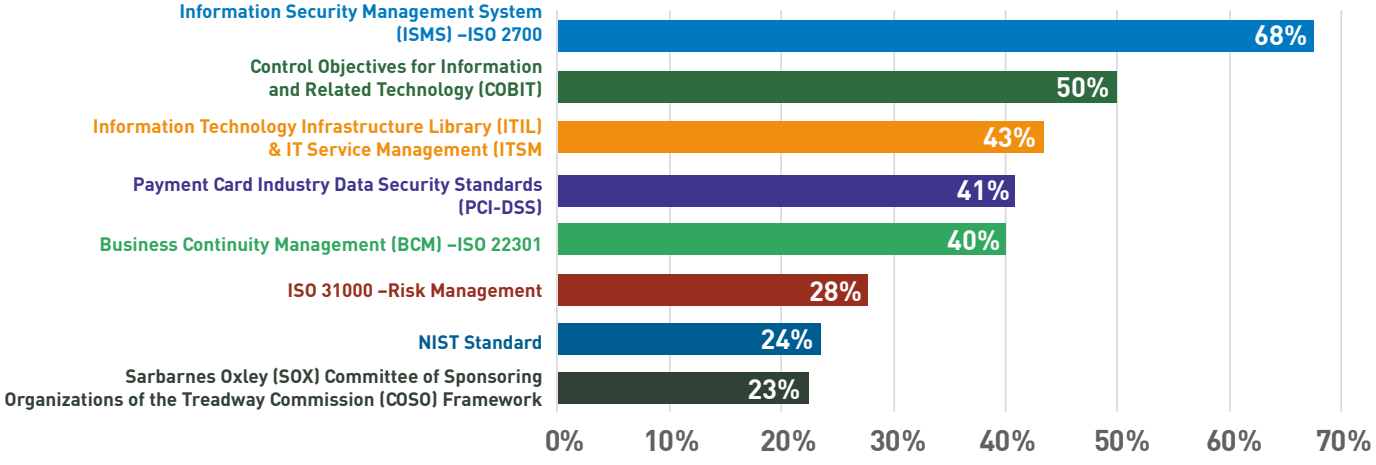
por BANKDIRECTOR (2018) en un estudio a Bancos de Estados Unidos para el año 2017, en donde se encontró que el 34% de los Bancos en dicho país maneja la gestión de la seguridad digital en el marco de un Comité de Riesgos, el 29% en el marco de Junta Directiva, el 19% en el marco de un Comité Técnico o de Tecnología, el 15% en el marco de un Comité de Auditoría y el 4% en otra instancia.

Respecto al apoyo a la gestión del riesgo de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) por parte de la alta dirección del banco, se destaca que más del 60% del total de las entidades bancarias en la región lo demuestran, i) exigiendo la adopción de buenas prácticas de seguridad (65%), ii) fomentando la capacitación y sensibilización en seguridad digital (63%), y, iii) impulsando planes de seguridad digital (60%).

El rol que juega la alta dirección y la junta de las organizaciones respecto de la seguridad digital es fundamental. A nivel global, EY (2018) encontró que *"el 90% de los Bancos encuestados a nivel global consideran como la principal prioridad del negocio el Mejorar la ciberseguridad y la seguridad de los datos"*. A nivel América Latina y el Caribe el presente estudio encuentra que para la mayoría de las entidades bancarias en la región (60% del total), el convencer a la alta dirección de la organización es medianamente complejo, mientras que tan sólo el 19% de las organizaciones lo consideran altamente complejo. Es importante resaltar lo concluido por ISACA (2018): *"Las organizaciones tienen un poco más de confianza en el apoyo de la alta dirección y de la junta respecto a los esfuerzos de seguridad en comparación con el año pasado. 69% por ciento de las organizaciones participantes creen que la junta directiva ha dado prioridad adecuada a la seguridad de la información."*

Finalmente, en asuntos de preparación y gobernanza, vale la pena resaltar la eficiente adopción de marcos de seguridad y/o estándares internacionales en torno a la seguridad digital por parte de los Bancos de la región. El 68% del total de entidades bancarias menciona que ha adoptado las normas *Information Security Management System (ISMS) – ISO 27001*, el 50% del total ha adoptado *Control Objectives for Information and Related Technology (COBIT)*, el 43% del total ha adoptado *Information Technology Infrastructure Library (ITIL) & IT Service Management (ITSM)* y el 41% del total ha adoptado *Payment Card Industry Data Security Standards (PCI-DSS)*.

Gráfica 10. Marcos de seguridad y/o estándares internacionales adoptados



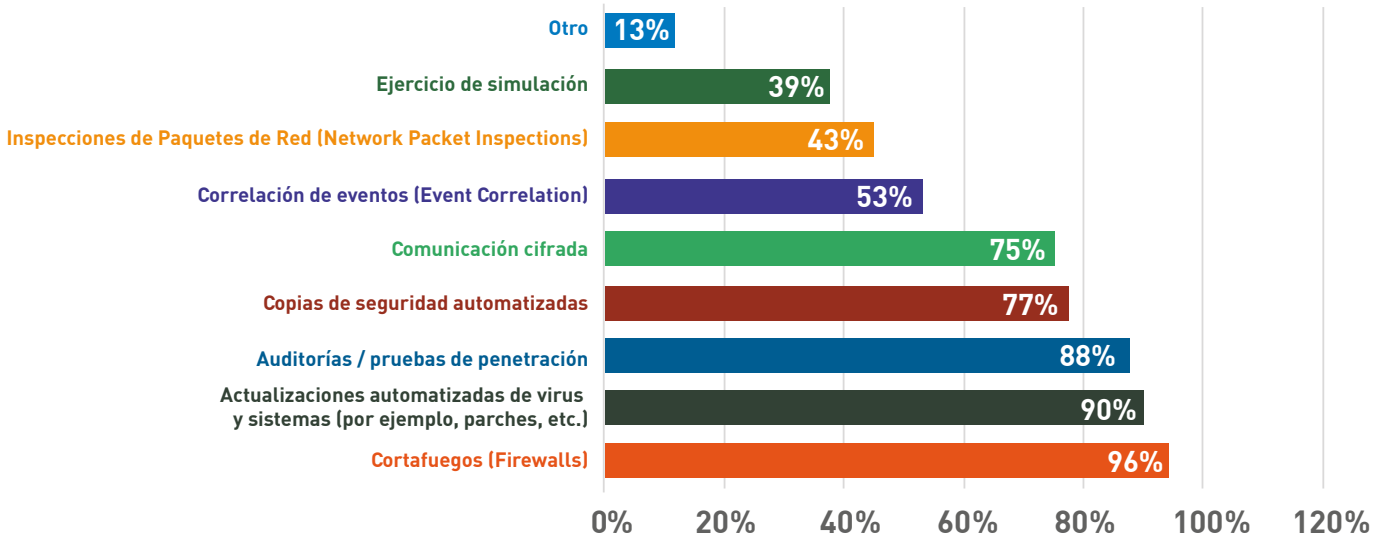
Nota: 191 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

4.2.2 Detección y análisis de eventos de seguridad digital

Según PwC (2017), "*los delincuentes apuntan a las entidades financieras porque ahí es donde está el dinero. El cibercrimen no ha cambiado esto, pero ha acelerado la velocidad y las consecuencias. Las entidades deben equilibrar estar abiertas con estar seguras.*" 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 seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) que los Bancos de la región América Latina y el Caribe llevan a cabo son i) los cortafuegos (96% del total), ii) las actualizaciones automatizadas de virus y sistemas (por ejemplo, parches, etc.) (90% del total), iii) las auditorías / pruebas de penetración (88%), y iv) las copias de seguridad automatizadas (77% del total).

Gráfica 11. Acciones y medidas técnicas de seguridad digital para proteger los sistemas de información críticos



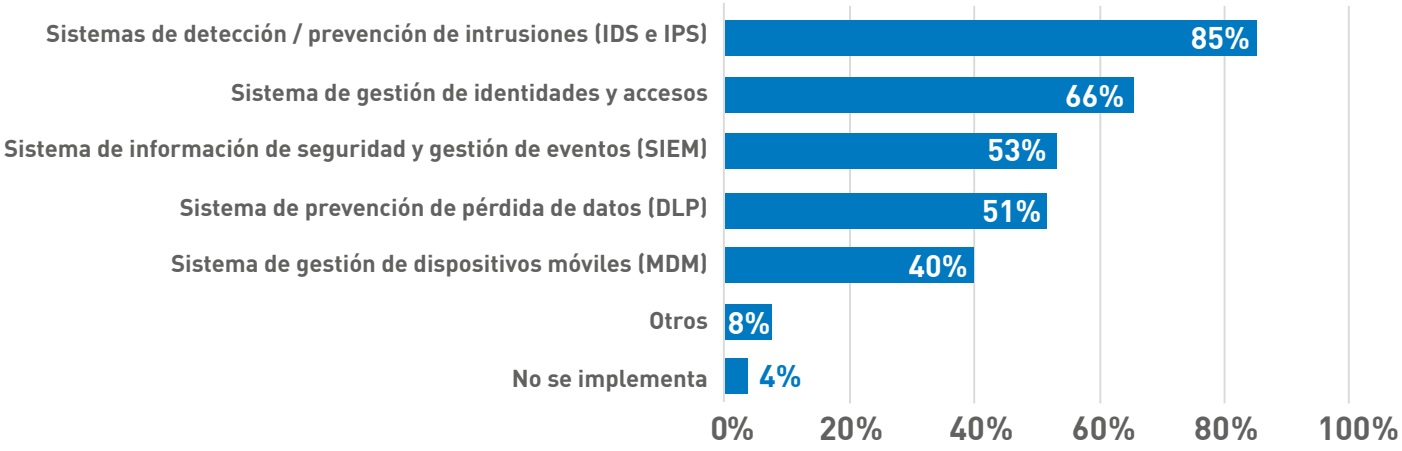
Nota: 191 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

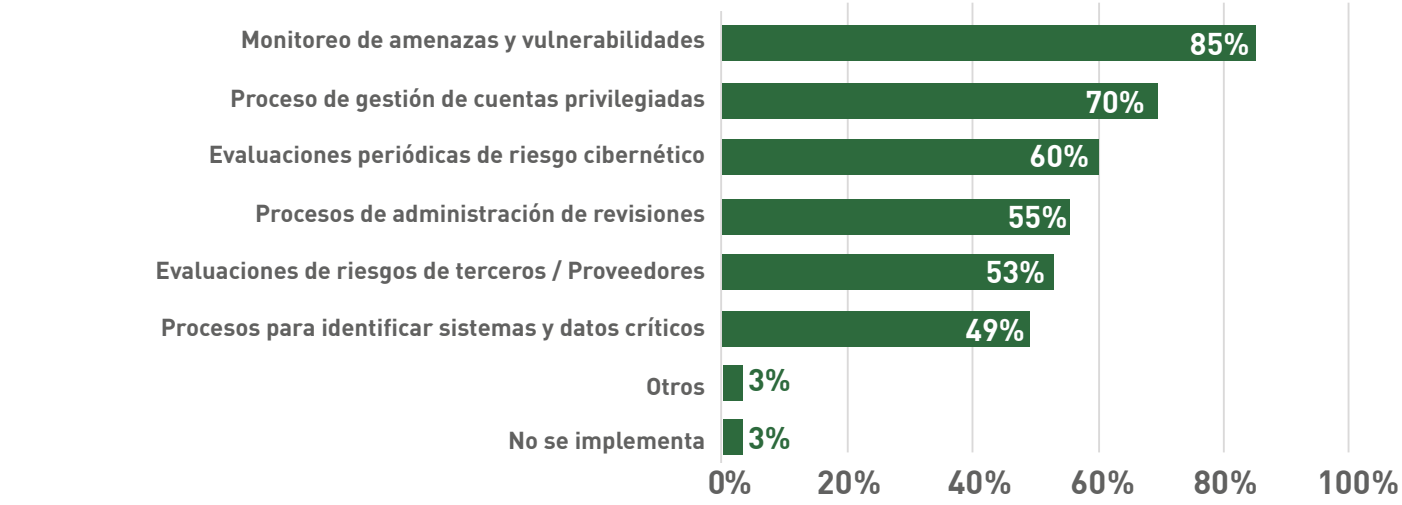
Adicionalmente, los sistemas implementados en las entidades bancarias de la región más comunes asociados a la seguridad digital son los sistemas de detección / prevención de intrusiones (IDS e IPS) (85% del total de Bancos) y los sistemas de gestión de identidades y accesos (66% del total de Bancos). Por su parte, los procesos implementados más comunes son el monitoreo de amenazas y vulnerabilidades (85% del total de Bancos) y el proceso de gestión de cuentas privilegiadas (70% del total de Bancos). Es necesario hacer énfasis en la implementación eficiente de este tipo de herramientas, controles y procesos en la región. Según ACCENTURE (2017), a nivel global tan "solo el 40% de los Bancos tiene sistemas y procesos que están diseñados adecuadamente de acuerdo con los requisitos de resiliencia cibernética."

Gráfica 12. Herramientas, controles y procesos implementados en la entidad bancaria

Sistemas



Procesos

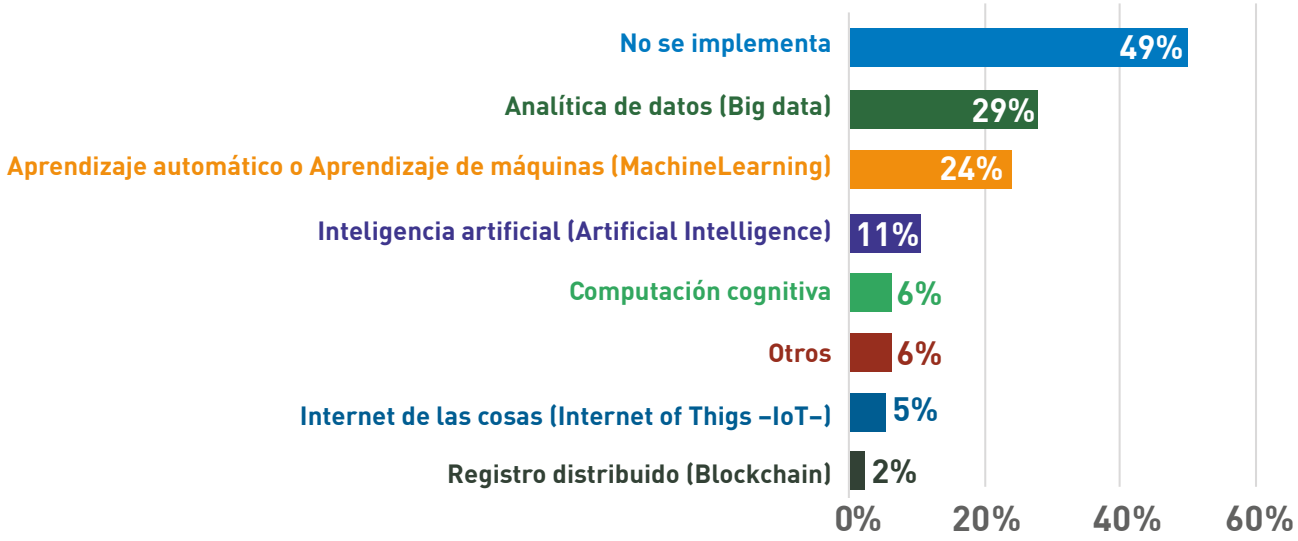


Nota: 191 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Con respecto al uso de tecnologías digitales emergentes aplicadas a herramientas, controles o procesos de seguridad digital en entidades bancarias, EY (2018) concluye que a nivel global "los Bancos que están invirtiendo o comenzando a invertir en nuevas tecnologías en los próximos tres años están adoptando múltiples enfoques para incorporar las capacidades de las tecnologías. (...) La inteligencia artificial (IA) y la analítica avanzada desempeñarán un papel clave en la prevención de los ciberataques, la reducción del riesgo de conducta y la mejora de la supervisión para evitar el delito financiero". En América Latina y el Caribe, el 26% de los Bancos grandes, el 44% de los Bancos medianos y el 67% de los Bancos pequeños mencionan que no están implementando actualmente herramientas, controles o procesos de seguridad digital usando alguna de las siguientes tecnologías digitales emergentes.

Gráfica 13. Tecnologías digitales emergentes aplicadas a herramientas, controles o procesos de seguridad digital en la entidad bancaria



Nota: 187 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Considerando el grupo de Bancos que han implementado herramientas, controles o procesos de seguridad digital usando alguna tecnología digital emergente, se destaca el uso de: i) analítica de datos (big data) con el 29% de los Bancos de la muestra, ii) el aprendizaje automático o aprendizaje de máquinas (Machine Learning) con el 24% de los Bancos de la muestra, y, iii) inteligencia artificial (Artificial Intelligence) con el 11% de los Bancos de la muestra. Vale la pena anotar que "los profesionales de la seguridad esperan gastar más en herramientas que usan artificial intelligence y machine learning en un intento por mejorar las defensas y ayudar a soportar la carga de trabajo." (CISCO, 2018).

Por otra parte, SYMANTEC (2017) concluye que "las instituciones financieras se enfrentan a ataques en múltiples frentes. Los dos tipos principales son ataques contra sus clientes y ataques contra su propia infraestructura." Los riesgos cibernéticos que consideran que merecen mayor atención 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.

Cuadro 3. Riesgos cibernéticos que merecen mayor atención por parte de la entidad bancaria

	Grande	Mediano	Pequeño	Total
Robo de base de datos crítica	2,87	2,83	2,83	**2,83**
Compromiso de credenciales de usuarios privilegiados	3,18	3,18	3,18	**3,18**
Pérdida de datos	3,57	3,61	3,57	**3,61**
Secuestro de información	3,77	3,70	3,73	**3,70**
Denegación del servicio	4,25	4,29	4,33	**4,29**
Sabotaje a través de un insider	4,80	4,82	4,78	**4,82**
Defacement – alteración en sitio web	5,56	5,57	5,58	**5,57**

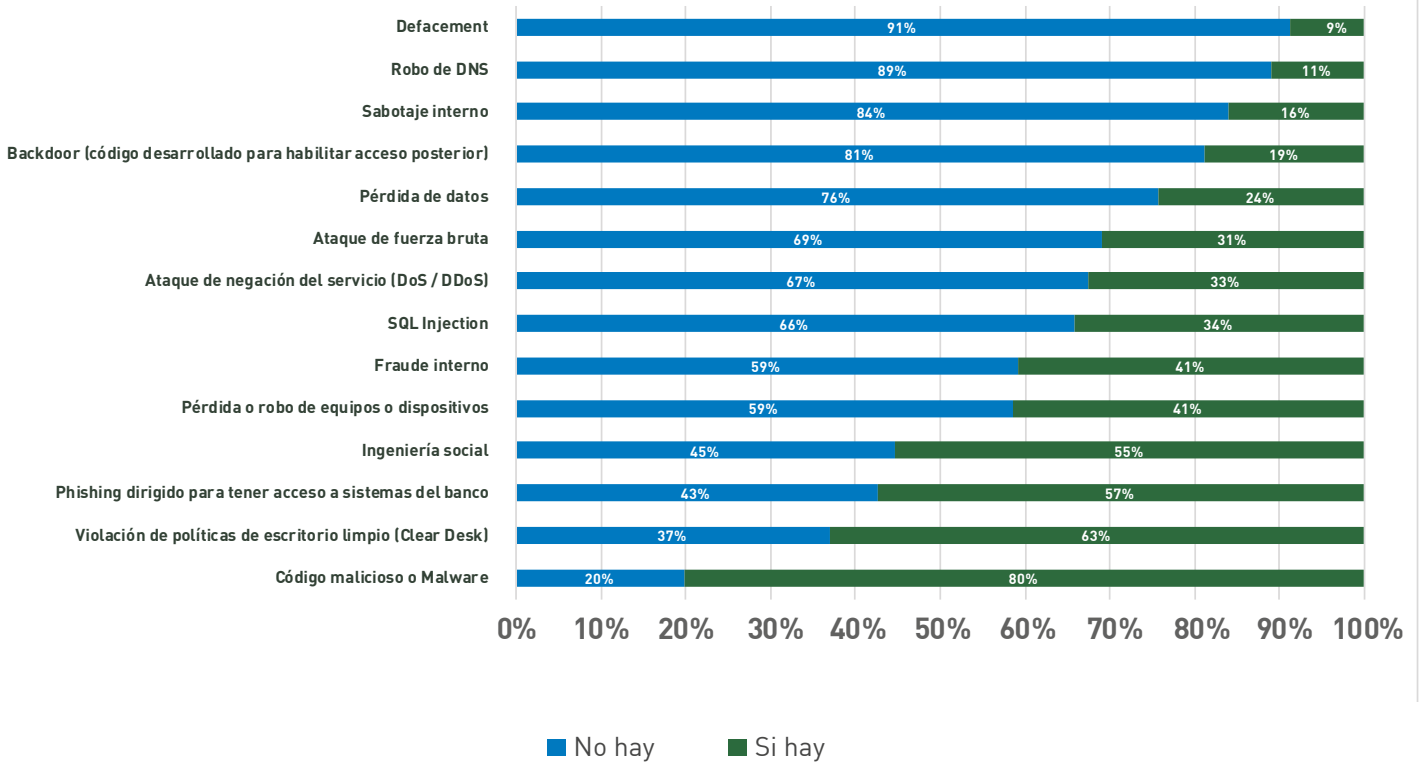
Nota: 187 registros y los entrevistados priorizaban los riesgos del 1 al 7, siendo el 1 el riesgo más alto y 7 el riesgo más bajo.
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

En el mismo estudio SYMANTEC (2017) destaca para el año 2017 que "*otra tendencia notable es el aumento de los ataques contra las empresas y las instituciones financieras en sí. En promedio, el 38 por ciento de todas las detecciones de amenazas financieras se realizaron en corporaciones. Una vez que los atacantes identifiquen una infección de este tipo, iniciarán sesión de forma remota y, con el tiempo, aprenderán cómo se realizan las transacciones. Dependiendo de las oportunidades presentadas, pueden intentar inyectar transacciones fraudulentas en las órdenes de pago de facturas mensuales o, en el caso de un banco, intentar y enviar sus propias transferencias interbancarias.*" Adicionalmente, "*el sector financiero se enfrenta a casi tres veces los ciberataques en comparación con las otras industrias*" (BDO, 2017)

A este respecto, se resalta que 176 de las 191 entidades financieras (92% del total) manifestaron que identificaron algún evento (ataques exitosos y ataques no exitosos) de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) durante el año 2017. Así, los eventos de seguridad digital más comúnmente identificados por las entidades bancarias de la región durante el año 2017 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). En contraste, los Bancos en la región mencionaron que los eventos de seguridad menos comunes son: i) defacement (tan sólo el 9% del total de

Bancos), ii) robo de DNS (tan sólo el 11% del total de Bancos), y, iii) sabotaje interno (tan sólo el 16% del total de Bancos).

Gráfica 14. Eventos de seguridad digital contra las entidades bancarias que se han identificado durante los últimos doce meses



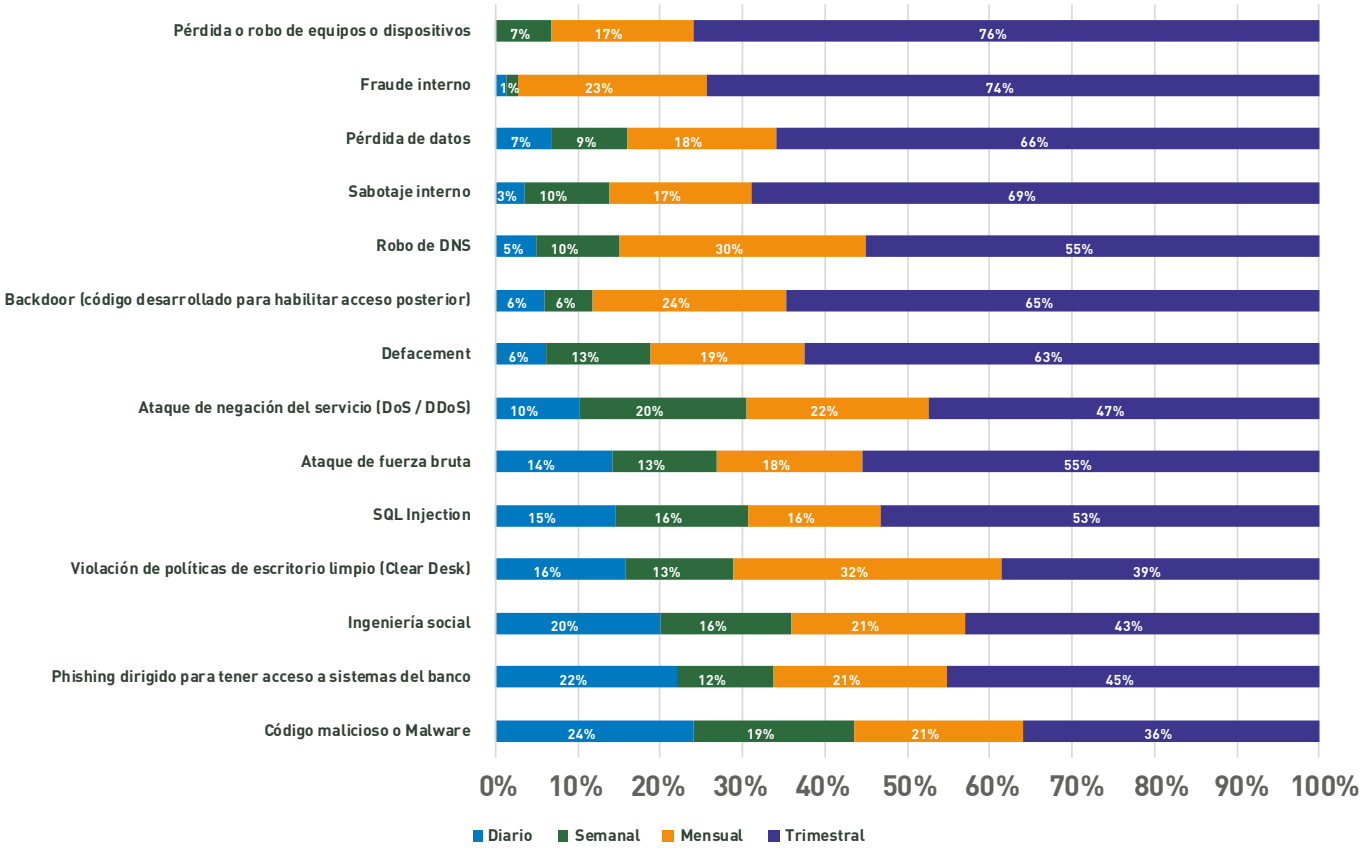
Nota: 181 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Los anteriores resultados son comparables con estudios que tienen relación con la identificación de incidentes en el sector financiero, tales como OFR (2017), que establece que "los ataques cibernéticos son esfuerzos deliberados para interrumpir, robar, alterar o destruir los datos almacenados en los sistemas de TI. Las tácticas incluyen encontrar debilidades en el software para ingresar a sistemas de TI, atacar contraseñas (spear-phishing), atacar sitios web para infectar a los usuarios con software malicioso (malware) y colocar software que bloquea a los usuarios fuera de sus propios sistemas (ransomware)".

Al analizar los resultados respecto a la frecuencia aproximada de ocurrencia de eventos identificados por las entidades bancarias en la región América Latina y el Caribe durante el año 2017, 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 Bancos en la región se apreció lo siguiente: i) un 24% de los Bancos identificaron ocurrencia de eventos de malware diariamente, ii) un 19% del total lo identificaron semanalmente, iii) un 21% del total lo identificaron mensualmente, y iv) un 36% del total lo identificaron trimestralmente. Con respecto al Phishing dirigido para tener acceso a sistemas del banco se apreció lo siguiente: i) un 22% de los Bancos identificaron ocurrencia de este tipo de eventos diariamente, ii) un 12% del total lo identificaron semanalmente, iii) un 21% del total lo identificaron mensualmente, y iv) un 45% del total lo identificaron trimestralmente.

Gráfica 15. Frecuencia en la ocurrencia de eventos de seguridad digital contra las entidades bancarias



Nota: 181 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

El análisis bajo el enfoque del sector bancario a nivel regional respecto de la dinámica de frecuencia de ocurrencia de eventos (ataques exitosos y ataques no exitosos) de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) permite observar una realidad promedio de ocurrencia. No obstante, al revisar los resultados por tamaño de banco se presentan dinámicas particulares. El **Anexo 2** presenta el análisis de cada uno de los eventos por tamaño de entidad bancaria.

Por ejemplo, se destaca que los Bancos grandes fueron objeto de ataques de todo tipo de eventos de seguridad digital, resaltando identificación de casi todos por la mayoría de dichas entidades en la región. Los eventos (ataques exitosos y ataques no exitosos) de seguridad digital más comúnmente identificados por los Bancos grandes de la región durante el año 2017 fueron: i) el código malicioso o malware (89% del total de Bancos grandes), ii) la violación de políticas de escritorio limpio (clear desk) (86% del total de Bancos grandes), y, iii) la ingeniería social (86% del total de Bancos grandes).

Al revisar la frecuencia con la que ocurren eventos relacionados con código malicioso o malware para el total de Bancos grandes en la región se apreció lo siguiente: i) un 40% de los Bancos grandes detectaron eventos de malware diariamente, ii) un 24% del total lo identificaron semanalmente, iii) un 24% del total

lo identificaron mensualmente, y iv) un 12% del total lo identificaron trimestralmente. Finalmente, se aprecia una dinámica de identificación de ocurrencia de una variedad de eventos de seguridad digital diaria, semanal, mensual y trimestralmente por parte de los Bancos grandes en la región.

Cuadro 4. Eventos de seguridad digital contra entidades bancarias grandes que se han identificado durante los últimos doce meses

	Grandes		
	No hay	Si hay	Total
Ingeniería social	14%	86%	100%
Código malicioso o Malware	11%	89%	100%
Phishing dirigido para tener acceso a sistemas del banco	32%	68%	100%
Pérdida de datos	61%	39%	100%
Pérdida o robo de equipos o dispositivos	39%	61%	100%
Ataque de negación del servicio (DoS / DDoS)	43%	57%	100%
Robo de DNS	75%	25%	100%
Violación de políticas de escritorio limpio (Clear Desk)	14%	86%	100%
Sabotaje interno	71%	29%	100%
Fraude interno	21%	79%	100%
Defacement	75%	25%	100%
Backdoor (código desarrollado para habilitar acceso posterior)	50%	50%	100%
SQL Injection	36%	64%	100%
Ataque de fuerza bruta	46%	54%	100%

Cuadro 4.

	Grandes				
	Diario	Semanal	Mensual	Trimestral	Total
Ingeniería social	21%	21%	25%	33%	100%
Código malicioso o Malware	40%	24%	24%	12%	100%
Phishing dirigido para tener acceso a sistemas del banco	37%	11%	5%	47%	100%
Pérdida de datos	9%	18%	27%	45%	100%
Pérdida o robo de equipos o dispositivos	0%	24%	24%	53%	100%
Ataque de negación del servicio (DoS / DDoS)	6%	31%	0%	63%	100%
Robo de DNS	0%	0%	29%	71%	100%
Violación de políticas de escritorio limpio (Clear Desk)	17%	25%	33%	25%	100%
Sabotaje interno	0%	25%	25%	50%	100%
Fraude interno	0%	5%	45%	50%	100%
Defacement	14%	14%	0%	71%	100%
Backdoor (código desarrollado para habilitar acceso posterior)	7%	7%	21%	64%	100%
SQL Injection	22%	22%	6%	50%	100%
Ataque de fuerza bruta	27%	27%	7%	40%	100%

Nota: 33 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

En relación con los Bancos medianos, se destaca que también fueron objeto de ataques de todo tipo de eventos de seguridad digital, resaltando identificación de algunos por la mayoría de dichas entidades en la región. Los eventos (ataques exitosos y ataques no exitosos) de seguridad digital más comúnmente identificados por los Bancos medianos de la región durante el año 2017 fueron: i) el código malicioso o malware (86% del total de Bancos medianos), ii) la violación de políticas de escritorio limpio (clear desk) (69% del total de Bancos medianos), y, iii) el phishing dirigido para tener acceso a sistemas del banco (66% del total de Bancos medianos).

Al revisar la frecuencia de ocurrencia de eventos relacionados con código malicioso o malware para el total de Bancos medianos en la región se apreció lo siguiente: i) un 28% de los Bancos medianos identificaron ocurrencia de eventos de malware diariamente, ii) un 16% del total lo identificaron semanalmente, iii) un 25% del total lo identificaron mensualmente, y iv) un 32% del total lo identificaron trimestralmente. Finalmente, se aprecia una dinámica de identificación de ocurrencia de algunos eventos de seguridad digital diariamente y del resto de eventos una dinámica de ocurrencia mensual y trimestralmente por parte de los Bancos medianos en la región.

Cuadro 5. Eventos de seguridad digital contra entidades bancarias medianas que se han identificado durante los últimos doce meses

	Medianas		
	No hay	Si hay	Total
Ingeniería social	40%	60%	100%
Código malicioso o Malware	14%	86%	100%
Phishing dirigido para tener acceso a sistemas del banco	34%	66%	100%
Pérdida de datos	68%	32%	100%
Pérdida o robo de equipos o dispositivos	49%	51%	100%
Ataque de negación del servicio (DoS / DDoS)	66%	34%	100%
Robo de DNS	89%	11%	100%
Violación de políticas de escritorio limpio (Clear Desk)	31%	69%	100%
Sabotaje interno	83%	17%	100%
Fraude interno	52%	48%	100%
Defacement	92%	8%	100%
Backdoor (código desarrollado para habilitar acceso posterior)	82%	18%	100%
SQL Injection	63%	38%	100%
Ataque de fuerza bruta	67%	33%	100%

Cuadro 5.

	Medianas				
	Diario	Semanal	Mensual	Trimestral	Total
Ingeniería social	23%	11%	21%	45%	100%
Código malicioso o Malware	28%	16%	25%	32%	100%
Phishing dirigido para tener acceso a sistemas del banco	21%	10%	26%	43%	100%
Pérdida de datos	4%	7%	14%	75%	100%
Pérdida o robo de equipos o dispositivos	0%	2%	18%	80%	100%
Ataque de negación del servicio (DoS / DDoS)	10%	10%	33%	47%	100%
Robo de DNS	10%	10%	30%	50%	100%
Violación de políticas de escritorio limpio (Clear Desk)	18%	11%	38%	33%	100%
Sabotaje interno	7%	7%	20%	67%	100%
Fraude interno	2%	0%	17%	81%	100%
Defacement	0%	14%	43%	43%	100%
Backdoor (código desarrollado para habilitar acceso posterior)	0%	0%	31%	69%	100%
SQL Injection	9%	9%	27%	55%	100%
Ataque de fuerza bruta	3%	7%	28%	62%	100%

Nota: 91 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Por último, en relación con los Bancos pequeños, se destaca que fueron objeto de ataques de algunos tipos de eventos de seguridad digital, resaltando identificación de pocos por la mayoría de dichas entidades en la región. Los eventos (ataques exitosos y ataques no exitosos) de seguridad digital más comúnmente identificados por los Bancos pequeños de la región durante el año 2017 fueron: i) el código malicioso o malware (68% del total de Bancos medianos), ii) la violación de políticas de escritorio limpio (clear desk) (45% del total de Bancos medianos), y, iii) el phishing dirigido para tener acceso a sistemas del banco (42% del total de Bancos medianos).

Al revisar la frecuencia de ocurrencia de eventos relacionados con código malicioso o malware para el total de Bancos pequeños en la región se apreció lo siguiente: i) un 9% de los Bancos pequeños identificaron ocurrencia de eventos de malware diariamente, ii) un 23% del total lo identificaron semanalmente, iii) un 11% del total lo identificaron mensualmente, y iv) un 57% del total lo identificaron trimestralmente. Finalmente, se aprecia una dinámica de identificación de ocurrencia de algunos eventos de seguridad digital diariamente y del resto de eventos una dinámica de ocurrencia semanal, mensual y trimestralmente por parte de los Bancos pequeños de la región.

Cuadro 6. Eventos de seguridad digital contra entidades bancarias pequeñas que se han identificado durante los últimos doce meses

	Pequeñas		
	No hay	Si hay	Total
Ingeniería social	65%	35%	100%
Código malicioso o Malware	32%	68%	100%
Phishing dirigido para tener acceso a sistemas del banco	58%	42%	100%
Pérdida de datos	92%	8%	100%
Pérdida o robo de equipos o dispositivos	80%	20%	100%
Ataque de negación del servicio (DoS / DDoS)	80%	20%	100%
Robo de DNS	95%	5%	100%
Violación de políticas de escritorio limpio (Clear Desk)	55%	45%	100%
Sabotaje interno	91%	9%	100%
Fraude interno	85%	15%	100%
Defacement	97%	3%	100%
Backdoor (código desarrollado para habilitar acceso posterior)	94%	6%	100%
SQL Injection	83%	17%	100%
Ataque de fuerza bruta	82%	18%	100%

Cuadro 6.

	Pequeñas				
	Diario	Semanal	Mensual	Trimestral	Total
Ingeniería social	13%	22%	17%	48%	100%
Código malicioso o Malware	9%	23%	11%	57%	100%
Phishing dirigido para tener acceso a sistemas del banco	15%	15%	22%	48%	100%
Pérdida de datos	20%	0%	20%	60%	100%
Pérdida o robo de equipos o dispositivos	0%	0%	8%	92%	100%
Ataque de negación del servicio (DoS / DDoS)	15%	31%	23%	31%	100%
Robo de DNS	0%	33%	33%	33%	100%
Violación de políticas de escritorio limpio (Clear Desk)	10%	7%	21%	62%	100%
Sabotaje interno	0%	0%	0%	100%	100%
Fraude interno	0%	0%	0%	100%	100%
Defacement	0%	0%	0%	100%	100%
Backdoor (código desarrollado para habilitar acceso posterior)	25%	25%	0%	50%	100%
SQL Injection	18%	27%	0%	55%	100%
Ataque de fuerza bruta	25%	8%	8%	58%	100%

Nota: 67 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Al analizar el tipo de eventos (ataques exitosos y ataques no exitosos) de seguridad digital que usan los ciberdelincuentes contra los usuarios de servicios financieros, las entidades bancarias mencionaron que los eventos de i) phishing, ii) ingeniería social, y, iii) software espía (malware o troyanos) fueron los más frecuentes en la región. Por otra parte, los eventos de seguridad digital contra usuarios menos comunes fueron: i) el auto fraude (fraude realizado por la misma persona que reclama), ii) el key logger, y, iii) los fraudes internos (realizados por funcionarios de clientes corporativos).

En relación con los eventos de seguridad digital contra la entidad bancaria identificados por los Bancos, es importante rescatar algunas conclusiones de otros estudios con ámbito global en torno a la materia:

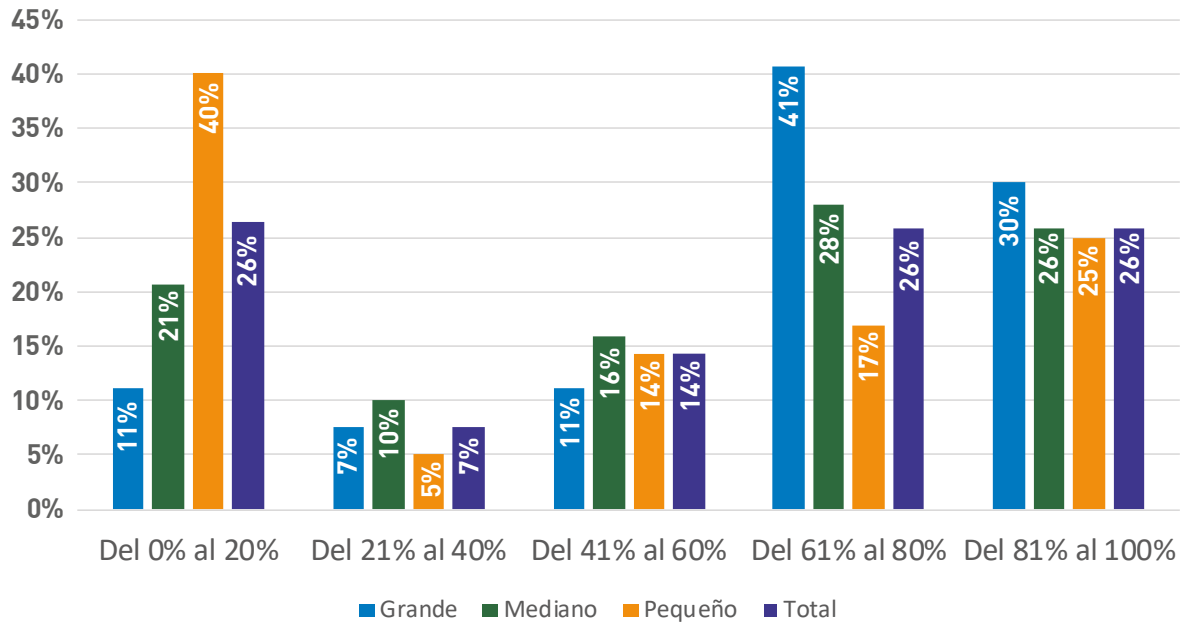
- *"No importa cuánto cambie el panorama de las amenazas, el correo electrónico malicioso y el correo no deseado siguen siendo herramientas vitales para que los adversarios distribuyan malware porque llevan las amenazas directamente al punto final. Al aplicar la combinación correcta de técnicas de ingeniería social, como phishing y enlaces maliciosos y archivos adjuntos, los adversarios solo tienen que sentarse y esperar a que los usuarios desprevenidos activen sus exploits." (CISCO, 2018)*

- *"La ingeniería social sigue desempeñando un papel importante en muchos ataques. A medida que la autenticación de transacciones a través de aplicaciones móviles o mensajes de texto crece en popularidad, también se ve un aumento en el malware móvil que intenta robar estas credenciales." (SYMANTEC, 2017)*

- *"Los ataques no solo apuntan a los clientes de los Bancos. Hemos visto varios ataques contra las propias instituciones financieras, con atacantes que intentan transferir grandes sumas en transacciones interbancarias fraudulentas." (SYMANTEC, 2017)*

Finalmente, en asuntos de detección y análisis de eventos de seguridad digital, se resalta que en promedio el 26% de los Bancos en la región detectan mediante sistemas propios (y no de terceros) entre un 0% y un 20% de eventos (ataques exitosos y ataques no exitosos) de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales), el 7% de los Bancos detecta entre un 21% y un 40% de eventos con sistemas propios, el 14% de los Bancos detecta entre un 41% y un 60% de eventos con sistemas propios, el 26% de los Bancos detecta entre un 61% y un 80% de eventos con sistemas propios y el 26% de los Bancos detecta entre un 81% y un 100% de eventos con sistemas propios.

Gráfica 16. Porcentaje de eventos de seguridad digital que son detectados mediante sistemas propios (y no de terceros) de detección de la entidad bancaria



Nota: 174 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

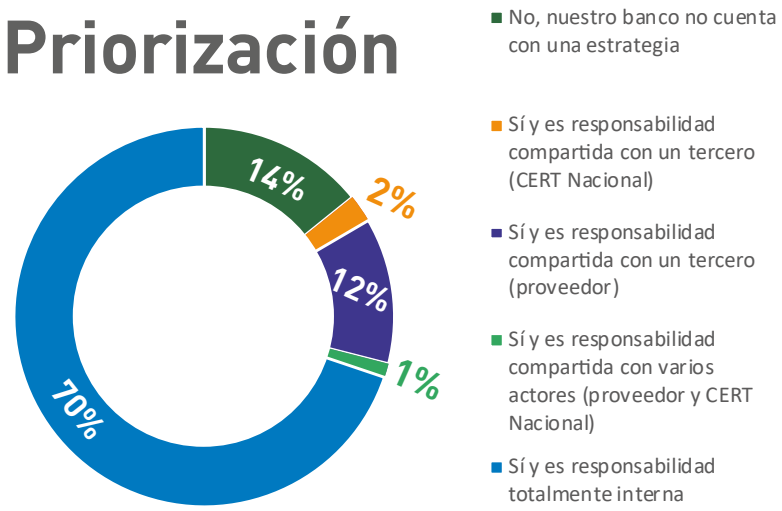
Al analizar por tamaño de banco, la mayoría de los Bancos grandes (41%) detecta entre un 61% y un 80% de eventos con sistemas propios, la mayoría de los Bancos medianos (28%) detecta entre un 61% y un 80% de eventos con sistemas propios y la mayoría de los Bancos pequeños (40%) detecta entre un 0% y un 20% de eventos con sistemas propios.

4.2.3 Gestión, respuesta y recuperación ante incidentes de seguridad digital

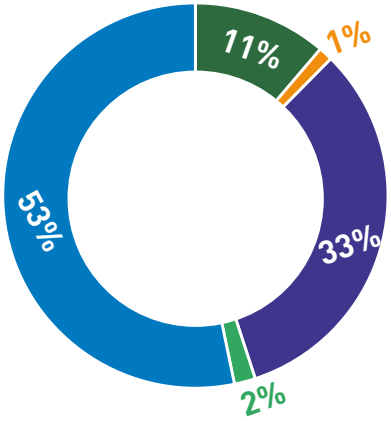
Teniendo en cuenta la distinción que se presentó en el instrumento de recolección de información enviado a las entidades bancarias entre evento de seguridad digital (suma de ataques exitosos y de ataques no exitosos que sufrió la institución durante un periodo de tiempo) e incidente de seguridad digital (total de ataques exitosos que sufrió la institución durante el mismo periodo de tiempo), se analizan los resultados a continuación haciendo énfasis a este último concepto: la gestión, respuesta y recuperación ante incidentes de seguridad digital.

Al analizar las estrategias frente a incidentes (ataques exitosos) de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) se destaca que: i) el 70% de los Bancos de la región contaron y ejecutaron una estrategia de priorización de incidentes bajo la responsabilidad interna de la organización, ii) el 53% de los Bancos de la región contaron y ejecutaron una estrategia de contención de incidentes bajo la responsabilidad interna de la organización, iii) el 52% de los Bancos de la región contaron y ejecutaron una estrategia de respuesta de incidentes bajo la responsabilidad interna de la organización, y iv) el 53% de los Bancos de la región contaron y ejecutaron una estrategia de recuperación de incidentes bajo la responsabilidad interna de la organización. Es decir, al menos la mitad de los Bancos de la región contaron con estrategias de gestión, respuesta y recuperación ante incidentes de seguridad digital.

Gráfica 17. Estrategias frente a incidentes (ataques exitosos) de seguridad digital

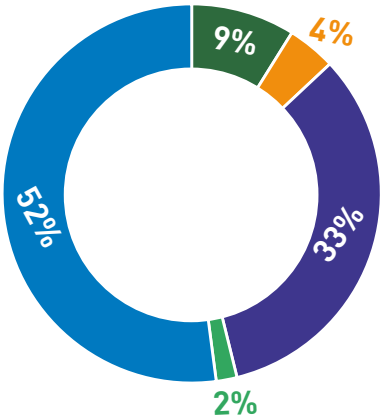


Contención



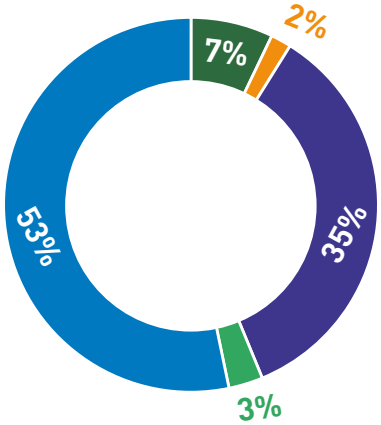
- No, nuestro banco no cuenta con una estrategia
- Sí y es responsabilidad compartida con un tercero (CERT Nacional)
- Sí y es responsabilidad compartida con un tercero (proveedor)
- Sí y es responsabilidad compartida con varios actores (proveedor y CERT Nacional)
- Sí y es responsabilidad totalmente interna

Respuesta



- No, nuestro banco no cuenta con una estrategia
- Sí y es responsabilidad compartida con un tercero (CERT Nacional)
- Sí y es responsabilidad compartida con un tercero (proveedor)
- Sí y es responsabilidad compartida con varios actores (proveedor y CERT Nacional)
- Sí y es responsabilidad totalmente interna

Recuperación



- No, nuestro banco no cuenta con una estrategia
- Sí y es responsabilidad compartida con un tercero (CERT Nacional)
- Sí y es responsabilidad compartida con un tercero (proveedor)
- Sí y es responsabilidad compartida con varios actores (proveedor y CERT Nacional)
- Sí y es responsabilidad totalmente interna

Nota: 169 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Cuadro 7. Estrategias frente a incidentes (ataques exitosos) de seguridad digital por tamaño de entidad bancaria

Priorización

	Grande	Mediano	Pequeño	**Total**
No, nuestro banco no cuenta con una estrategia	3	7	14	**24**
Sí y es responsabilidad compartida con un tercero (CERT Nacional)		1	3	**4**
Sí y es responsabilidad compartida con un tercero (proveedor)	6	8	7	**21**
Sí y es responsabilidad compartida con varios actores (proveedor y CERT Nacional)		2		**2**
Sí y es responsabilidad totalmente interna	17	62	39	**118**
	26	**80**	**63**	**169**

	Grande	Mediano	Pequeño	**Total**
No, nuestro banco no cuenta con una estrategia	12%	9%	22%	**14%**
Sí y es responsabilidad compartida con un tercero (CERT Nacional)	0%	1%	5%	**2%**
Sí y es responsabilidad compartida con un tercero (proveedor)	23%	10%	11%	**12%**
Sí y es responsabilidad compartida con varios actores (proveedor y CERT Nacional)	0%	3%	0%	**1%**
Sí y es responsabilidad totalmente interna	65%	78%	62%	**70%**
	100%	**100%**	**100%**	**100%**

Cuadro 7.

Contención

	Grande	Mediano	Pequeño	**Total**
No, nuestro banco no cuenta con una estrategia	1	6	12	**19**
Sí y es responsabilidad compartida con un tercero (CERT Nacional)			2	**2**
Sí y es responsabilidad compartida con un tercero (proveedor)	16	25	14	**55**
Sí y es responsabilidad compartida con varios actores (proveedor y CERT Nacional)		2	1	**3**
Sí y es responsabilidad totalmente interna	9	47	34	**90**
	26	**80**	**63**	**169**

	Grande	Mediano	Pequeño	**Total**
No, nuestro banco no cuenta con una estrategia	4%	8%	19%	**11%**
Sí y es responsabilidad compartida con un tercero (CERT Nacional)	0%	0%	3%	**1%**
Sí y es responsabilidad compartida con un tercero (proveedor)	62%	31%	22%	**33%**
Sí y es responsabilidad compartida con varios actores (proveedor y CERT Nacional)	0%	3%	2%	**2%**
Sí y es responsabilidad totalmente interna	35%	59%	54%	**53%**
	100%	**100%**	**100%**	**100%**

Cuadro 7.

Respuesta

	Grande	Mediano	Pequeño	**Total**
No, nuestro banco no cuenta con una estrategia		6	9	**15**
Sí y es responsabilidad compartida con un tercero (CERT Nacional)		4	3	**7**
Sí y es responsabilidad compartida con un tercero (proveedor)	16	22	18	**56**
Sí y es responsabilidad compartida con varios actores (proveedor y CERT Nacional)		2	1	**3**
Sí y es responsabilidad totalmente interna	10	46	32	**88**
	26	**80**	**63**	**169**

	Grande	Mediano	Pequeño	**Total**
No, nuestro banco no cuenta con una estrategia	0%	8%	14%	**9%**
Sí y es responsabilidad compartida con un tercero (CERT Nacional)	0%	5%	5%	**4%**
Sí y es responsabilidad compartida con un tercero (proveedor)	62%	28%	29%	**33%**
Sí y es responsabilidad compartida con varios actores (proveedor y CERT Nacional)	0%	3%	2%	**2%**
Sí y es responsabilidad totalmente interna	38%	58%	51%	**52%**
	100%	**100%**	**100%**	**100%**

Cuadro 7.

Recuperación

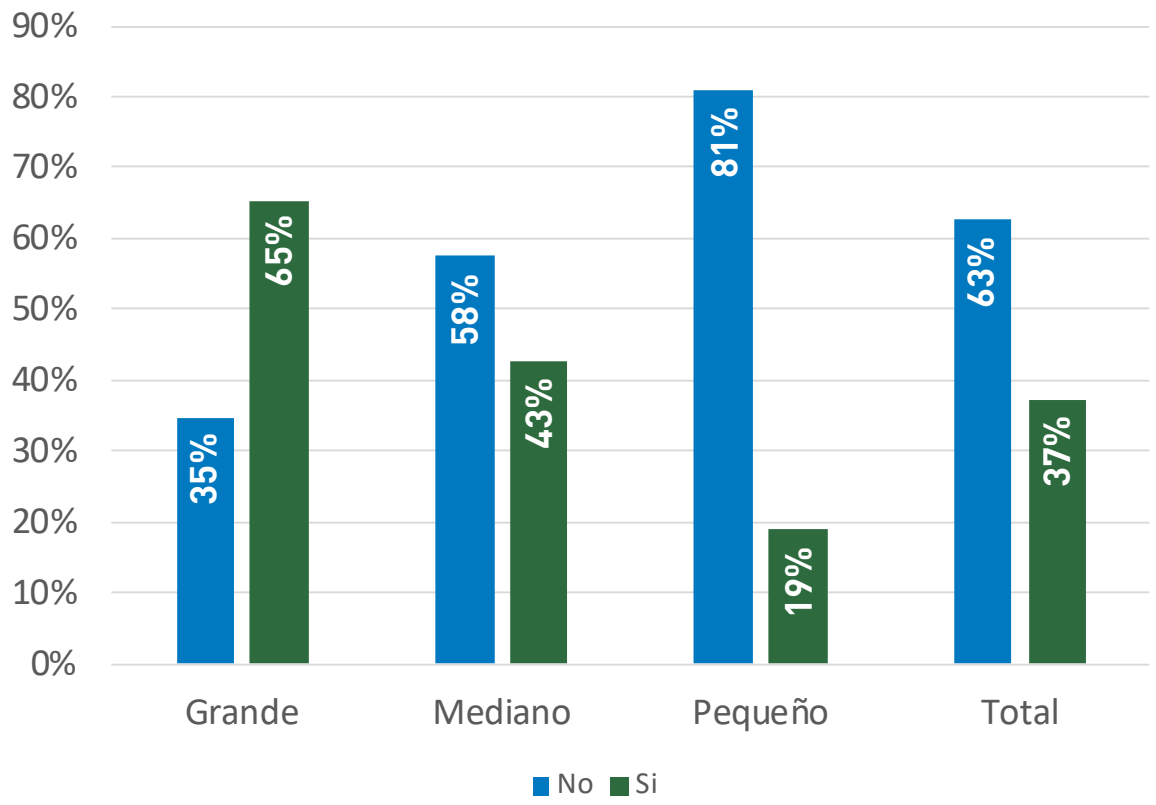
	Grande	Mediano	Pequeño	**Total**
No, nuestro banco no cuenta con una estrategia	1	3	8	**12**
Sí y es responsabilidad compartida con un tercero (CERT Nacional)			3	**3**
Sí y es responsabilidad compartida con un tercero (proveedor)	16	25	18	**59**
Sí y es responsabilidad compartida con varios actores (proveedor y CERT Nacional)		4	1	**5**
Sí y es responsabilidad totalmente interna	9	48	33	**90**
	26	**80**	**63**	**169**

	Grande	Mediano	Pequeño	**Total**
No, nuestro banco no cuenta con una estrategia	4%	4%	13%	**7%**
Sí y es responsabilidad compartida con un tercero (CERT Nacional)	0%	0%	5%	**2%**
Sí y es responsabilidad compartida con un tercero (proveedor)	62%	31%	29%	**35%**
Sí y es responsabilidad compartida con varios actores (proveedor y CERT Nacional)	0%	5%	2%	**3%**
Sí y es responsabilidad totalmente interna	35%	60%	52%	**53%**
	100%	**100%**	**100%**	**100%**

No obstante lo anterior, existe una particularidad al analizar los resultados anteriores por tamaño de organización. La gran mayoría de Bancos grandes, medianos y pequeños llevan a cabo la ejecución de estrategias de priorización bajo responsabilidad totalmente interna en la organización. Sin embargo, la gran mayoría de Bancos grandes realizan la ejecución de estrategias de contención, respuesta y recuperación bajo responsabilidad compartida con un tercero (proveedor) mientras que la gran mayoría de Bancos medianos y pequeños lo hacen bajo responsabilidad totalmente interna en la organización.

En relación con la materialización de incidentes (ataques exitosos) de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) en las entidades bancarias en la región durante el 2017, se resalta que el 65% de los Bancos grandes manifiestan que sí fueron víctimas de ataques exitosos, mientras que entre los Bancos medianos el porcentaje es del 43% y entre los pequeños, del 19%.

Gráfica 18. ¿La entidad bancaria, como organización, fue víctima de incidentes (ataques exitosos) de seguridad digital durante los últimos doce meses?



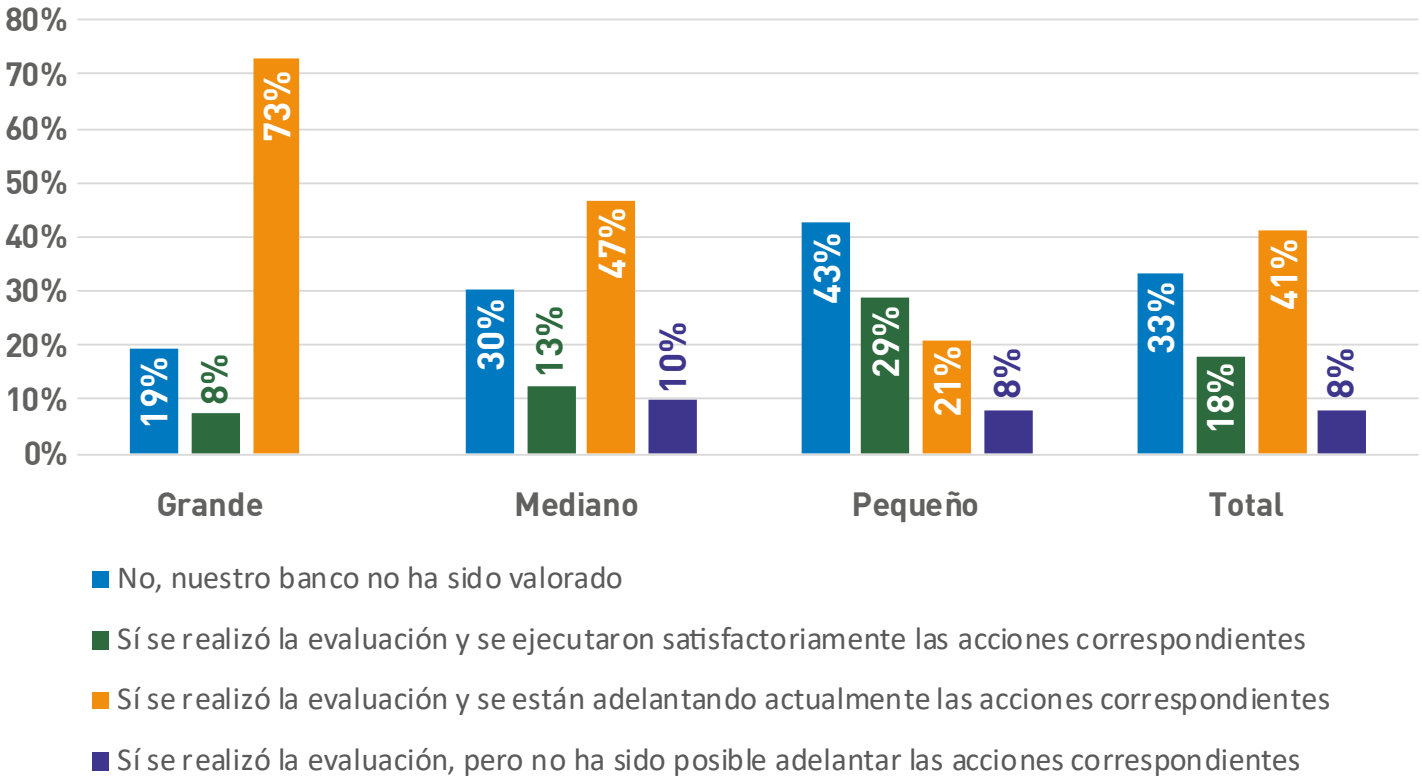
Nota: 169 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

En específico y tomando como base las entidades bancarias que manifestaron que fueron víctimas de incidentes (ataques exitosos) de seguridad digital (63 entidades), se destaca que casi todas (90% en promedio) investigaron la fuente que generó dichos incidentes.

Además, y como resultado de las investigaciones, dichas entidades bancarias en la región identificaron y priorizaron las principales motivaciones de dichos incidentes (ataques exitosos) de seguridad digital sufridos durante el año 2017, siendo éstas: i) motivos económicos (79% de los Bancos víctimas), ii) robo de información personal (35% de los Bancos víctimas), y, iii) generación de daño reputacional al banco (23% de los Bancos víctimas).

Al preguntar si las entidades bancarias fueron valoradas externamente en los últimos dos (2) años bajo alguna metodología de evaluación de la madurez de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) y si han completado dicha evaluación, se encontraron diferencias según el tamaño de la organización. Mientras que el 73% de los Bancos grandes de la región realizó dicha evaluación y están llevando a cabo actualmente las acciones correspondientes, tan sólo el 47% de los Bancos medianos y el 21% de los Bancos pequeños reflejan dicha situación. En contraste, preocupa que el 30% de los Bancos medianos y el 43% de los Bancos pequeños nunca han evaluado la madurez de seguridad digital.

Gráfica 19. ¿La entidad bancaria ha sido valorada externamente en los últimos dos (2) años bajo alguna metodología de evaluación de la madurez de seguridad digital y ha completado dicha evaluación?



Nota: 168 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Frente a este tipo de actividad, por ejemplo, BANKDIRECTOR (2018) concluye en un estudio de entidades bancarias en los Estados Unidos que "*todos los encuestados dicen que su banco tiene un plan de respuesta a incidentes establecido para abordar un incidente cibernético, pero el 37% no está seguro si ese plan es efectivo. 69% dice que el banco realizó un ejercicio de mesa, esencialmente, un ciberataque simulado en 2017.*" Tomando como base las entidades bancarias que manifestaron que no han completado totalmente una evaluación de la madurez de la seguridad digital o no han ejecutado todas sus acciones derivadas, dichas entidades bancarias lo atribuyen principalmente a: i) insuficiencia de personal especializado (46% de Bancos sin evaluación), ii) falta de asignación de presupuesto (45% de Bancos sin evaluación), y, iii) falta de regulación específica que exija su implementación (34% de Bancos sin evaluación).

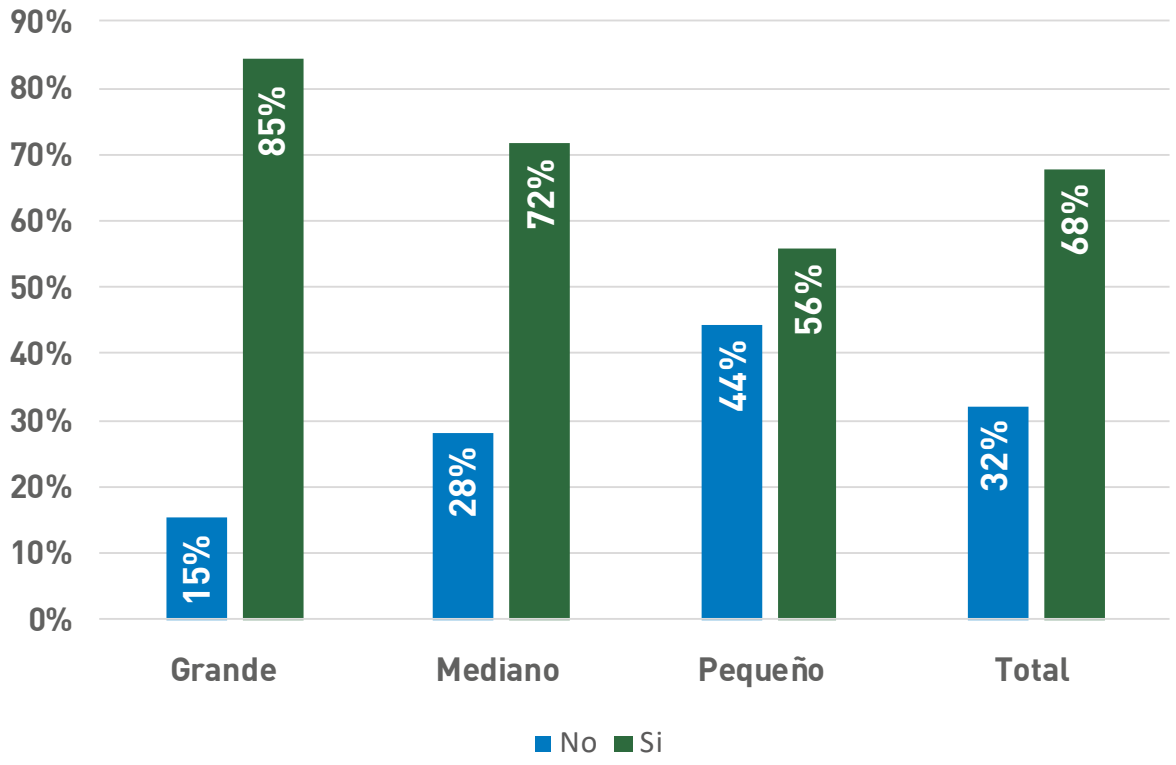
4.2.4 Reportes de incidentes de seguridad digital

Del análisis de resultados respecto al reporte de incidentes de seguridad digital (total de ataques exitosos que sufrió la institución durante el mismo periodo de tiempo) es importante revisar si las organizaciones cuentan con mecanismos o planes internos de reporte, así como la existencia de regulaciones específicas e institucionalidad frente al tema.

En términos generales, se aprecia que la gran mayoría de Bancos de la región América Latina y el Caribe – grandes (88%), medianos (92%) y pequeños (82%) – ofrece un mecanismo para que sus usuarios internos (empleados y contratistas) reporten incidentes (ataques exitosos) de seguridad digital sufridos.

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 del banco. Se aprecia que el 85% de los Bancos grandes y el 72% de los Bancos medianos de la región ofrece un mecanismo para que sus clientes de servicios financieros reporten a la entidad incidentes (ataques exitosos) de seguridad digital sufridos, en contraste con el 56% de los Bancos pequeños.

Gráfica 20. **¿La entidad bancaria ofrece un mecanismo para que sus clientes de servicios financieros reporten a la entidad incidentes (ataques exitosos) de seguridad digital sufridos?**

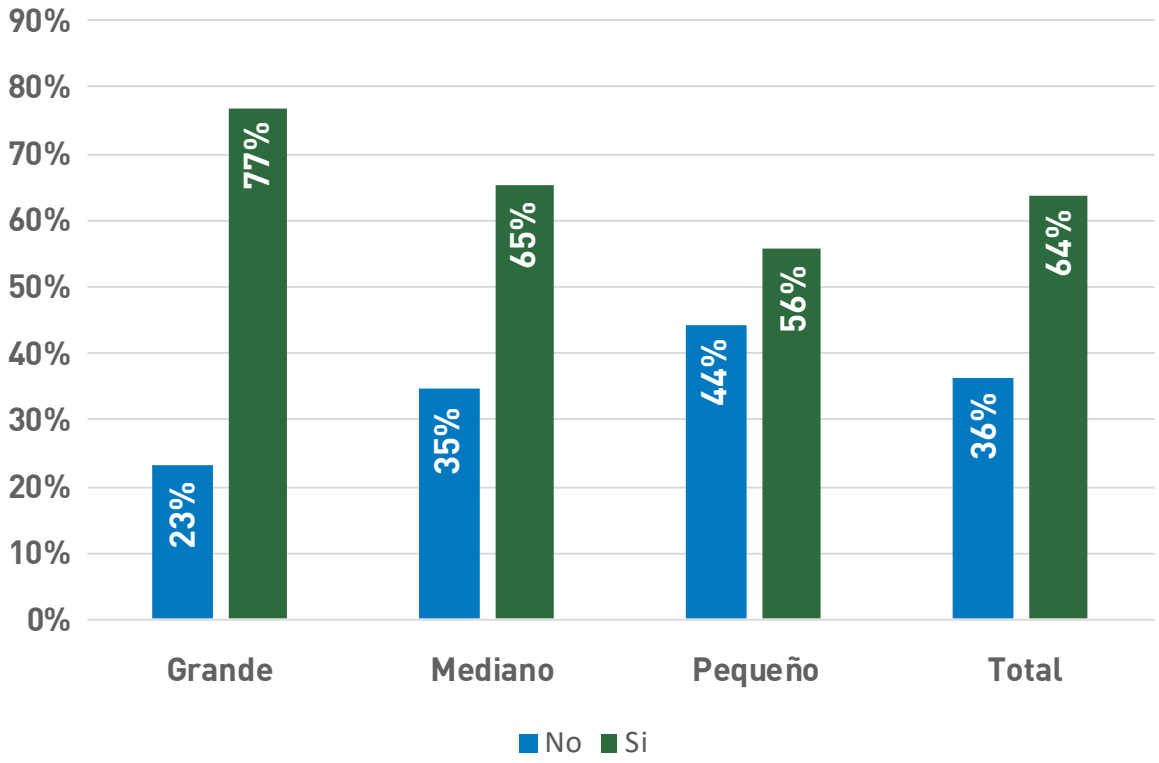


Nota: 165 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

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 del banco. Se aprecia que en la mayoría de los bancos grandes (77%) y de los bancos medianos (65%) de la región existe un plan de comunicaciones para informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida, en contraste con la mitad de los bancos pequeños (56%).

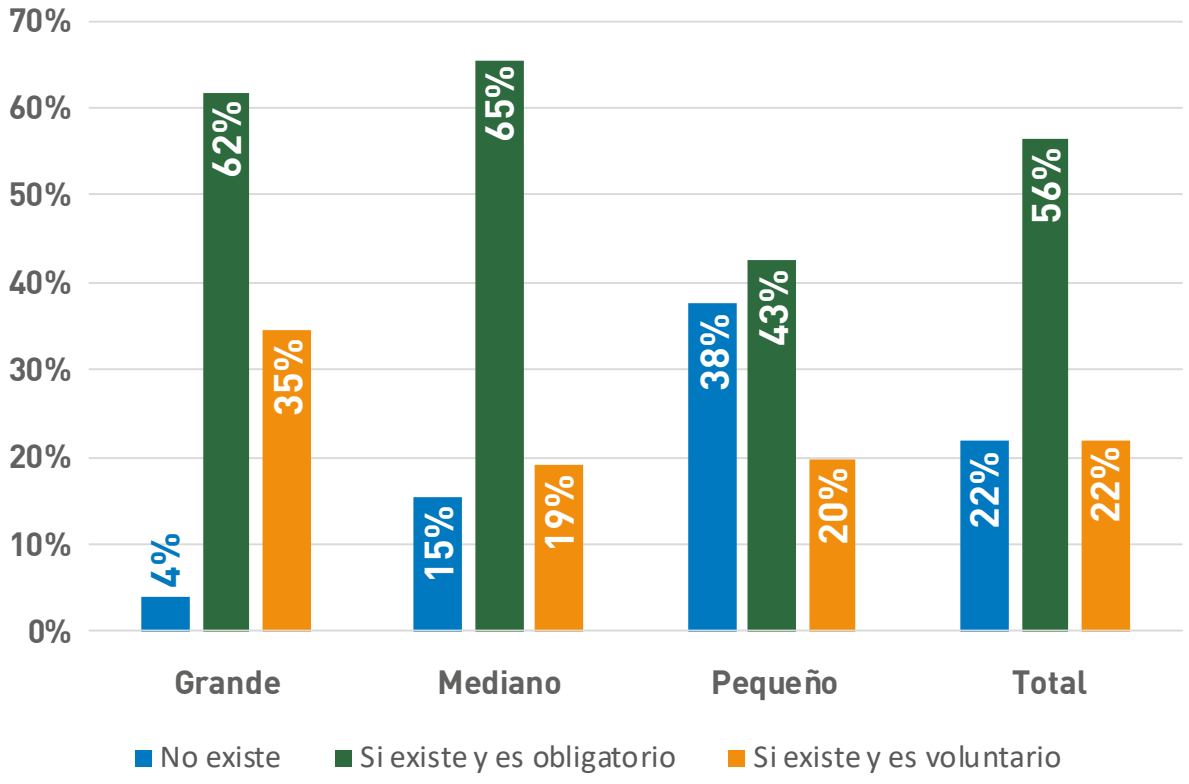
Gráfica 21. **¿La entidad bancaria cuenta con un plan de comunicaciones que permita informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida?**



Nota: 165 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

En relación con el reporte de incidentes (ataques exitosos) ante una autoridad de regulación en los países de la región por parte de las entidades bancarias, también se aprecian diferencias entre Bancos grandes y medianos frente a Bancos pequeños. El 62% de los Bancos grandes y el 65% de los Bancos medianos versus el 43% de los Bancos pequeños 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, el 35% de los Bancos grandes manifiestan que conocen algún mecanismo para reportar incidentes y es voluntaria su aplicación. También se resalta que tan sólo el 4% de los Bancos grandes de la región, en contraste con el 38% de los Bancos pequeños, manifiesta que no existe mecanismo alguno de reporte de incidentes sufridos ante una autoridad de regulación.

Gráfica 22. **¿Conoce algún mecanismo para reportar incidentes (ataques exitosos) de seguridad digital sufridos por la entidad bancaria ante una autoridad de regulación en su país?**

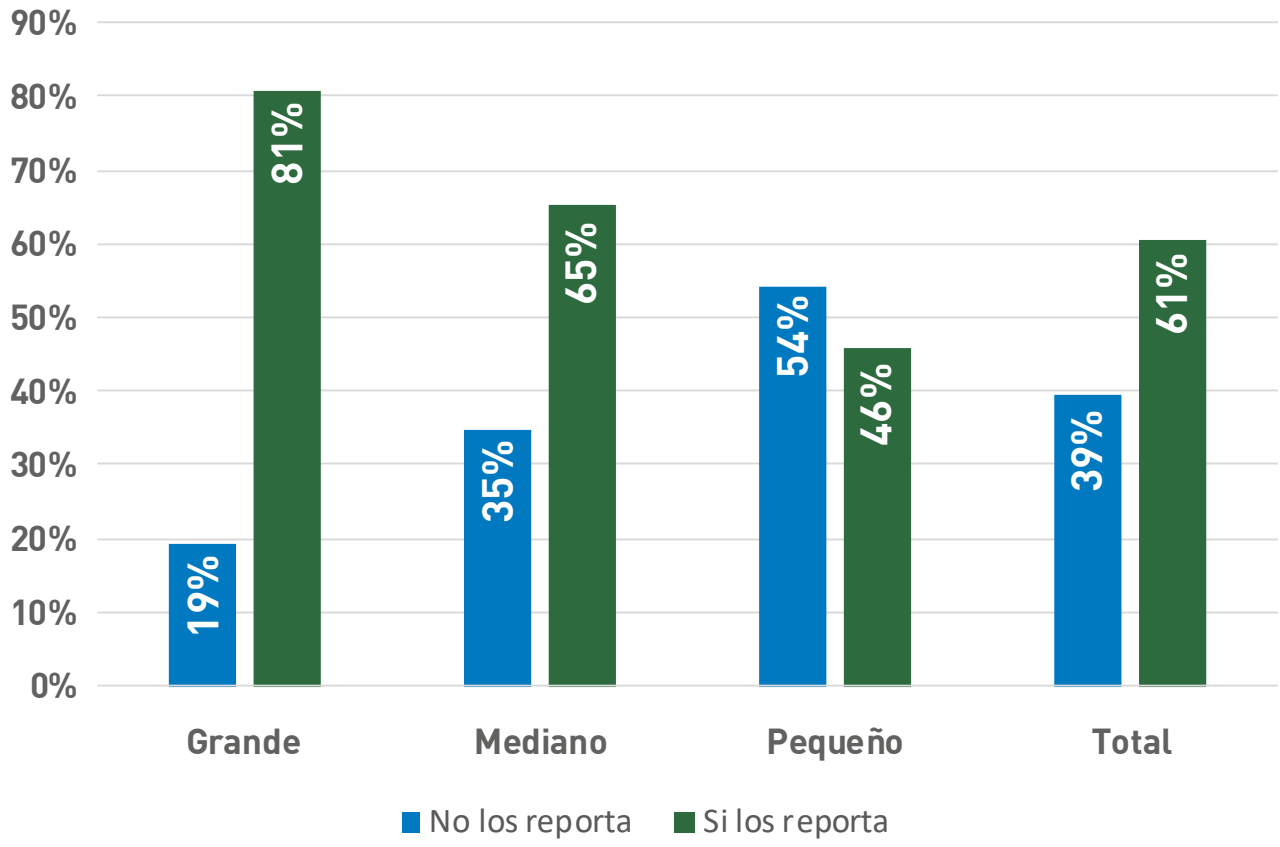


Nota: 165 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Adicionalmente, se aprecia que a medida que crece el tamaño del banco aumenta el reporte de incidentes (ataques exitosos) de seguridad digital sufridos ante una autoridad de aplicación de la ley. El 81% de los Bancos grandes, el 65% de los Bancos medianos y el 46% de los Bancos pequeños reportan los incidentes sufridos ante este tipo de autoridad en la región.

Gráfica 23. ¿La entidad bancaria reporta los incidentes (ataques exitosos) de seguridad digital sufridos ante una autoridad de aplicación de la ley?

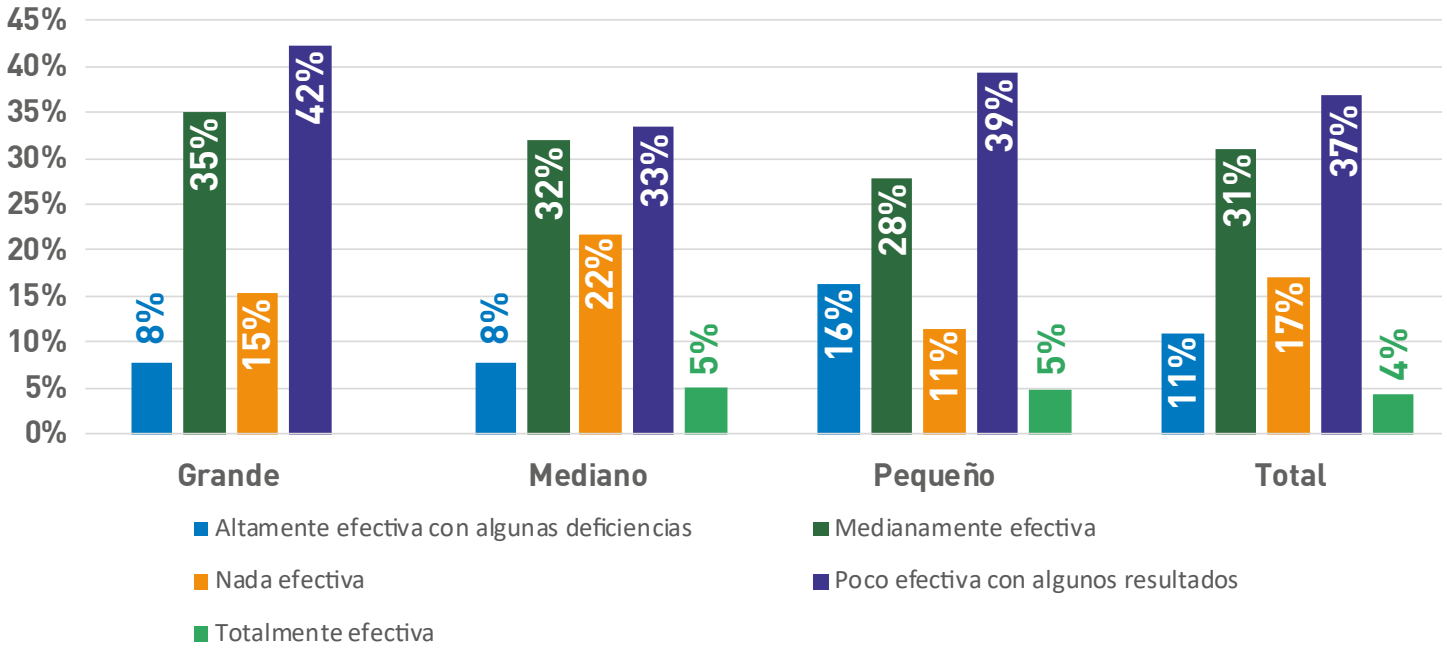


Nota: 165 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Finalmente, se destaca que independientemente del tamaño del banco, el 31% de entidades bancarias en la región América Latina y el Caribe considera como medianamente efectivo el papel de las autoridades de aplicación de la ley respecto a la respuesta, investigación y judicialización de los ciberdelincuentes, mientras que el 37% considera como poco efectivo en algunos resultados el papel de las mencionadas autoridades.

Gráfica 24. ¿Cómo considera la entidad bancaria la efectividad de las autoridades de aplicación de la ley respecto a la respuesta, investigación y judicialización de los ciberdelincuentes?



Nota: 165 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

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 este tema se destaca lo concluido en EY (2018): *"Al infundir conceptos y prácticas de ciberseguridad en todo el proceso de innovación, los Bancos podrán identificar y mitigar mejor el riesgo digital. Los tiempos de ciclo se pueden reducir diseñando la seguridad desde el principio, y se genera un mayor valor cuando la justificación de la ciberseguridad pasa de prevenir las infracciones a permitir la innovación y el crecimiento."* En particular y sin distinguir por tamaño del banco, la gran mayoría (82%) de las entidades bancarias en la región América Latina y el Caribe contaba con planes de preparación, respuesta y capacitación en asuntos de seguridad digital para sus empleados e insourcing bancarios. Se destaca que tan sólo el 70% de los Bancos pequeños cuentan con dichos planes en la región.

Considerada la base de entidades bancarias de la región que cuentan con planes de preparación, respuesta y capacitación en asuntos de seguridad digital para sus empleados e insourcing bancarios, se destaca que el 75% de los mismos se ejecutan anualmente, el 16% se ejecutan semestralmente y el 9% se ejecutan anualmente.

Por otra parte, el 77% de las entidades bancarias en la región prueban la capacidad de los empleados de la entidad bancaria para responder adecuadamente frente a incidentes de seguridad digital y esquemas de phishing e ingeniería social con periodicidad anual, el 11% con periodicidad semestral y el 12% con periodicidad trimestral.

Finalmente, en relación con asuntos de capacitación y concientización, las entidades bancarias identificaron que los mecanismos más efectivos a partir de los cuales se ha generado mayor conciencia en la entidad bancaria respecto de los riesgos de seguridad digital son: i) las capacitaciones internas de información, ii) las acciones debidas al cumplimiento de requisitos legales y/o regulatorios, y, iii) las presentaciones y debates en conferencias.

Cuadro 8. Mecanismo más efectivo a partir del cual se ha generado mayor conciencia en la entidad bancaria respecto de los riesgos de seguridad digital

	Grande	Mediano	Pequeño	**Total**
Capacidades internas de información	2,00	2,02	2,03	**2,02**
Requisitos legales y/o regulatorios	3,37	3,39	3,42	**3,39**
Presentaciones y debates en conferencias	4,52	4,41	4,47	**4,41**
Publicaciones gratuitas en revistas, sitios web y listas de correo	4,45	4,52	4,47	**4,52**
Redes sociales	4,64	4,72	4,69	**4,72**
Documentación de organismos especializados en la materia	5,49	5,50	5,49	**5,50**
Servicios especializados por suscripción	6,09	6,05	6,04	**6,05**
Asociaciones profesionales	6,22	6,16	6,18	**6,16**
Otro	8,22	8,22	8,22	**8,22**

Nota: 165 registros y se priorizan todos los mecanismos otorgándoles un número del 1 al 9, siendo el 1 el mecanismo más efectivo y 9 el mecanismo menos efectivo

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

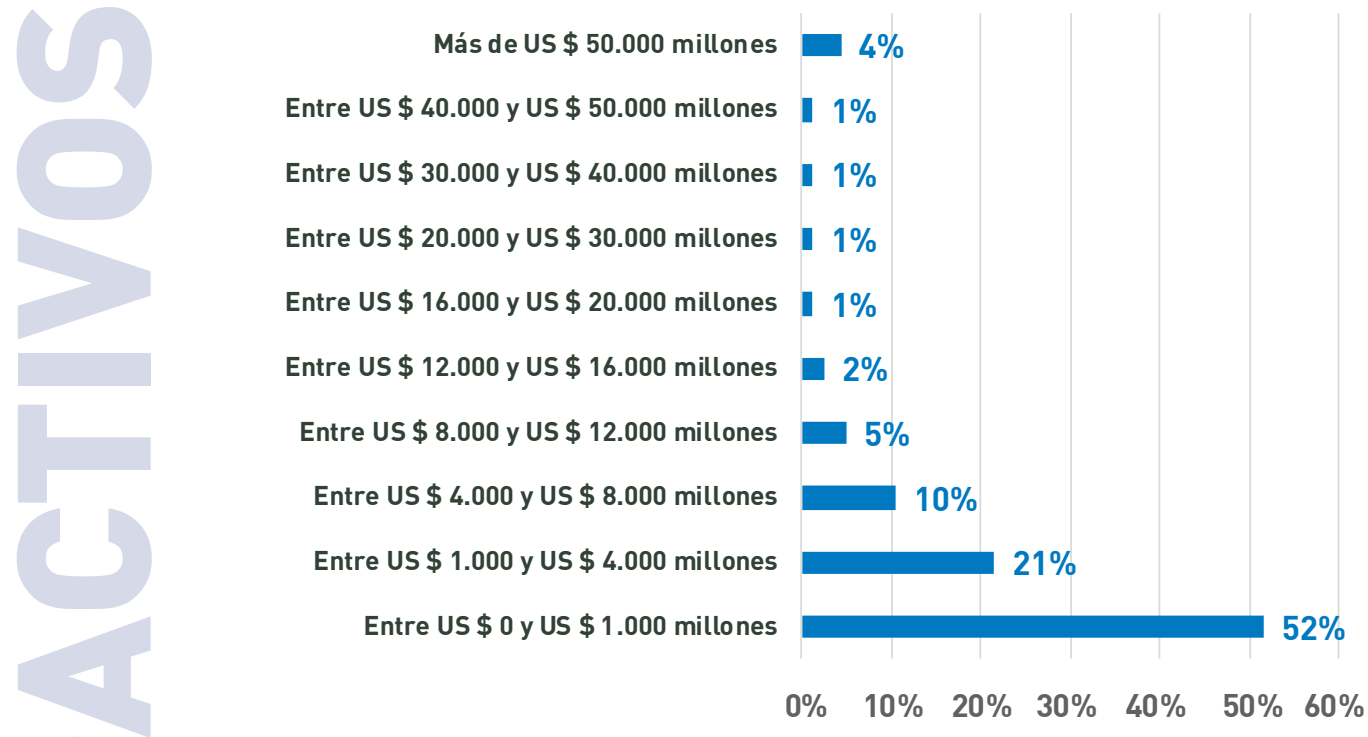
4.3 Impacto de los incidentes de seguridad digital

Una vez caracterizadas las entidades bancarias que participaron en el desarrollo del presente estudio y presentados los resultados encontrados sobre la gestión de riesgos de seguridad digital por parte del sector bancario en la región América Latina y el Caribe, a continuación se presenta el análisis del impacto de los incidentes de seguridad digital en entidades bancarias durante el año 2017.

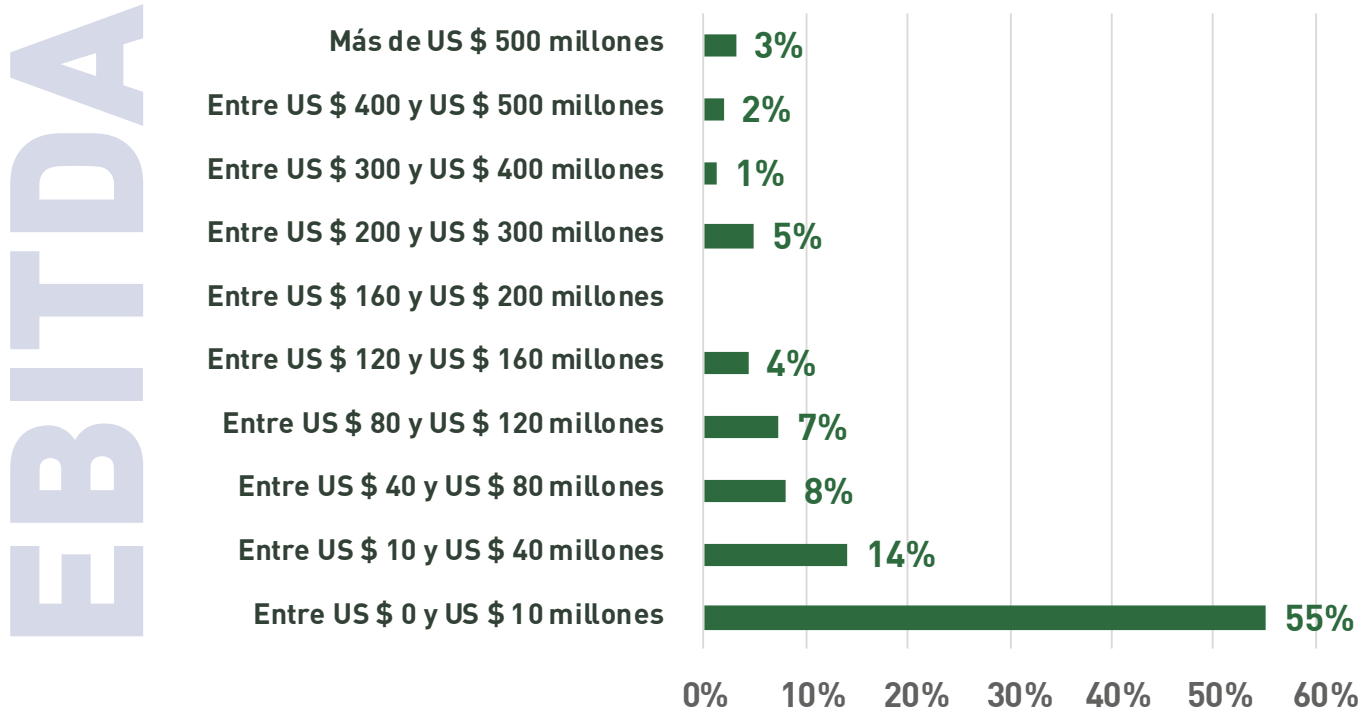
Como se mencionó, la muestra de entidades bancarias a partir de las cuales se presentan los siguientes resultados alcanzó unos activos bancarios de USD $1 billón de dólares y unas utilidades netas de USD $10,5 mil millones de dólares a 31 de diciembre de 2017, lo que permite afirmar que dicha muestra contiene una representatividad de los distintos niveles de activos y patrimonio de la región América Latina y el Caribe.

Se destaca que el 52% de las entidades bancarias manifestaron que alcanzaron activos totales a 31 de diciembre de 2017 entre USD $0 y USD $1.000 millones, el 21% entre USD $1.000 y USD $4.000 millones, el 10% entre USD $4.000 y USD $8.000 millones y el 17% unos activos totales superiores a US $8.000 millones a 31 de diciembre de 2017. Por otra parte, el 55% de las entidades bancarias manifestaron que obtuvieron un EBITDA (en inglés, Earnings Before Interests, Taxes, Depreciations and Amortizations) a 31 de diciembre de 2017 entre US $0 y USD $10 millones, el 14% entre US $ 10 y US $40 millones, el 8% entre US $40 y US $80 millones y el 23% un EBITDA mayor a US $80 millones.

Gráfica 25. Distribución de entidades bancarias por valores del año inmediatamente anterior



Gráfica 25.

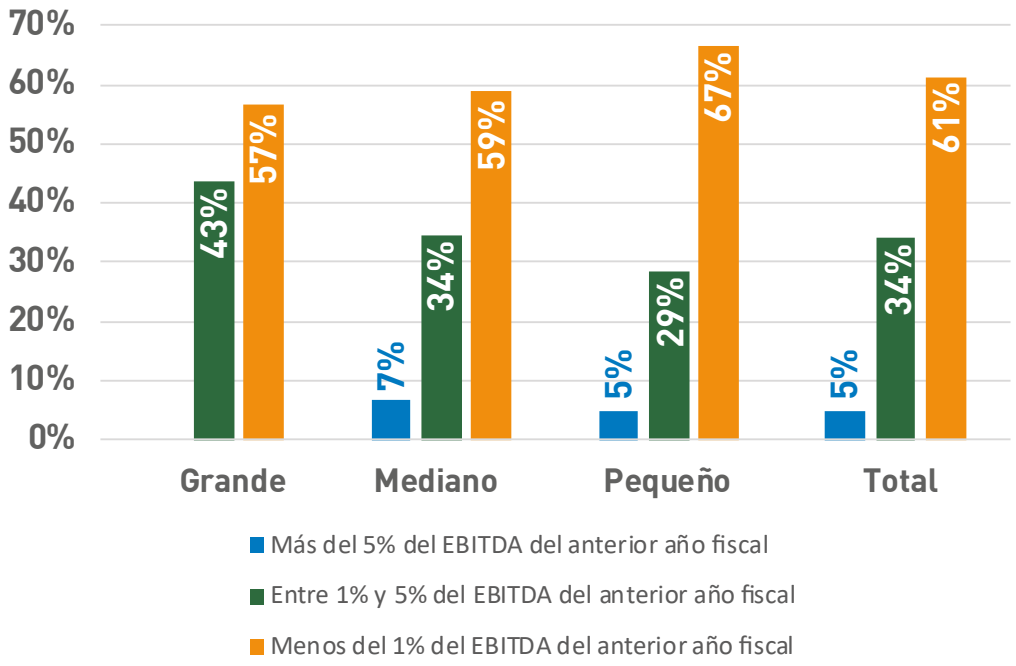


Nota: 163 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

A partir de las entidades bancarias que presentaron información, se destaca que el 61% de las entidades bancarias en la región manifestaron 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 34% de las entidades bancarias manifestaron que el valor de dicho presupuesto estuvo entre el 1% y el 5% del EBITDA del anterior año fiscal y el 5% manifestaron que el valor de dicho presupuesto equivale a un valor mayor al 5% del EBITDA del anterior año fiscal.

Del análisis también se puede inferir que a medida que aumenta el tamaño del banco aumenta el presupuesto de la seguridad digital como % del EBITDA del año inmediatamente anterior. Por ejemplo, el 43% de los Bancos grandes manifestaron que el valor de dicho presupuesto estuvo entre el 1% y el 5% del EBITDA del anterior año fiscal, mientras que el 34% de los Bancos medianos y el 29% de los Bancos pequeños manifestaron que el presupuesto dedicado se encontraba en ese rango.

Gráfica 26. Presupuesto de la seguridad digital como % del EBITDA del año inmediatamente anterior



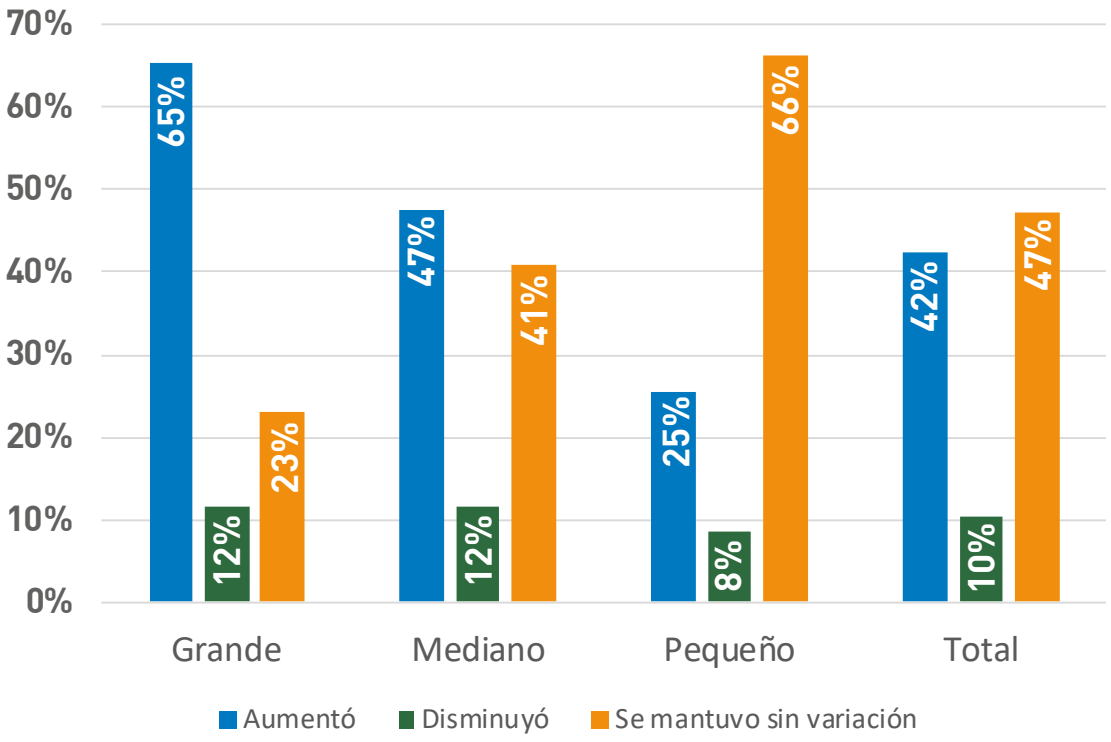
Nota: 126 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Vale la pena anotar que otros estudios dirigidos al sector bancario presentan estimaciones que podrían guardar correspondencia en las magnitudes obtenidas en el presente estudio. Por ejemplo, según BANKDIRECTOR (2018), el 52% de los Bancos en su estudio dedicó entre 1% y 5% de los ingresos como presupuesto de la seguridad digital para 2017, el 46% dedicó menos del 1% de los ingresos y tan sólo el 2% dedicó más del 5% de los ingresos. Adicionalmente ACCENTURE (2017) encontró que "*cuatro de cada diez entidades bancarias gastan entre un 7% y un 10% de su presupuesto de TI en ciberseguridad*".

Además, en comparación al año fiscal inmediatamente anterior, el 46% de las entidades bancarias en la región manifestaron que se mantuvo sin variación el presupuesto de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales), el 42% manifestó que había aumentado y tan sólo el 10% manifestó que se había disminuido.

Al analizar en detalle, se apreciaron diferencias en los resultados para cada tamaño de entidad bancaria. Se destaca que para el 65% de los Bancos grandes, el 47% de los Bancos medianos y el 25% de los Bancos pequeños el presupuesto de seguridad digital había aumentado en comparación al año fiscal inmediatamente anterior. Por otro lado, para el 23% de los Bancos grandes, el 41% de los Bancos medianos y el 66% de los Bancos pequeños el presupuesto de seguridad digital se mantuvo igual a aquel del año fiscal inmediatamente anterior. Finalmente, se aprecia un porcentaje similar de Bancos grandes (12%), medianos (12%) y pequeños (8%) en donde dicho presupuesto había disminuido.

Gráfica 27. Dinámica del presupuesto de seguridad digital en el último año



Nota: 163 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

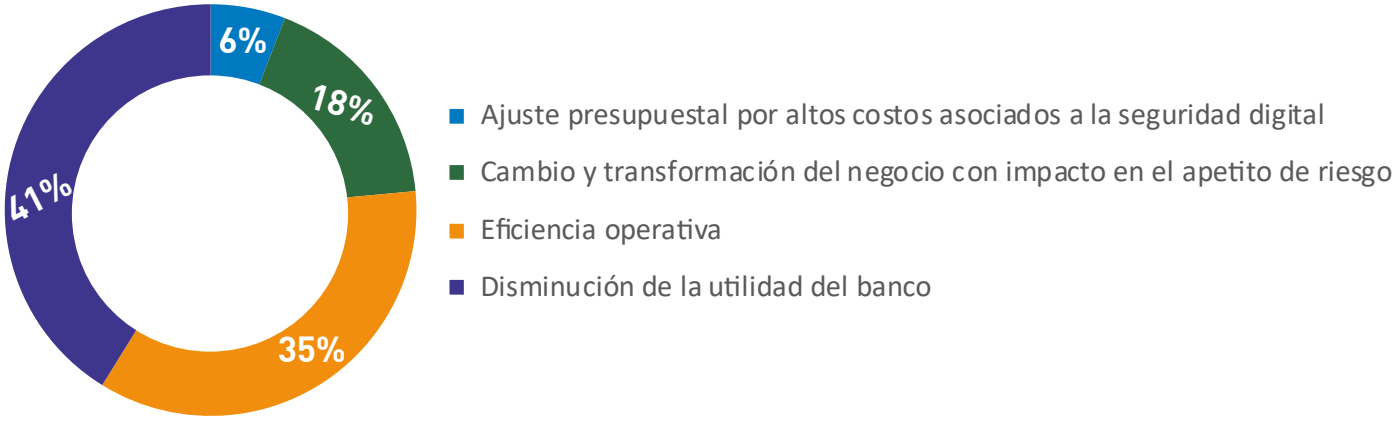
Estas estimaciones obtenidas del análisis de la muestra de entidades bancarias en la región América Latina y el Caribe también guardan correspondencia con algunas estimaciones presentadas por ISACA (2017) -*"El 50% de las organizaciones aumentaron los presupuestos de seguridad de 2016 a 2017"*- o por ISACA (2018), en donde se concluye que tan sólo el 8% de las organizaciones encuestadas indicó que el presupuesto de seguridad digital disminuirá, mientras que el 28% indicó que se mantendrá sin variación y el 64% que el presupuesto se incrementará.

Adicionalmente, según BANKDIRECTOR (2018), el 55% de los Bancos en su estudio incrementó el presupuesto de seguridad digital en 2018 hasta un 10% en comparación con aquel destinado en 2017, el 23% de los Bancos lo aumentó entre un 10% y un 25% con respecto al año anterior, el 6% lo incrementó entre un 25% y un 50% y tan sólo el 1% tuvo un crecimiento superior al 50%. Se destaca que el 15% de los Bancos de la muestra se mantuvo sin variación entre 2017 y 2018.

Del total de entidades bancarias que manifestaron que el presupuesto de seguridad digital había aumentado en comparación al año fiscal inmediatamente anterior, el 62% indicó que su aumento se debió a Cumplimiento Regulatorio, el 55% de dicha muestra se debió a Cambios y Transformación del Negocio, y el 54% a Nuevas amenazas de ciberseguridad por el uso de NTIC. Vale la pena destacar que CISCO (2018) concluye que *"los factores más importantes que impulsan las inversiones futuras y, por lo tanto, las mejoras en la tecnología y los procesos, parecen ser infracciones. En 2017, el 41 por ciento de los profesionales de seguridad dijeron que las brechas de seguridad están impulsando una mayor inversión en tecnologías y soluciones de seguridad, un aumento del 37 por ciento en 2016."*

Por otro lado, del total de entidades bancarias que manifestaron que el presupuesto de seguridad digital había disminuido en comparación al año fiscal inmediatamente anterior, el 41% señaló que se debió a una *Disminución de la Utilidad del Banco, el 35% a razones de Eficiencia Operativa, el 18% a Cambio y transformación del negocio con impacto en el apetito de riesgo y el 6% a Ajuste presupuestal por altos costos asociados a la seguridad digital.*

Gráfica 28. Razones de la disminución del presupuesto de seguridad digital



Nota: 17 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

En relación con la disminución de presupuestos dedicados a la seguridad digital, es interesante traer a colación algunas conclusiones de otros estudios sobre el tema, por ejemplo:

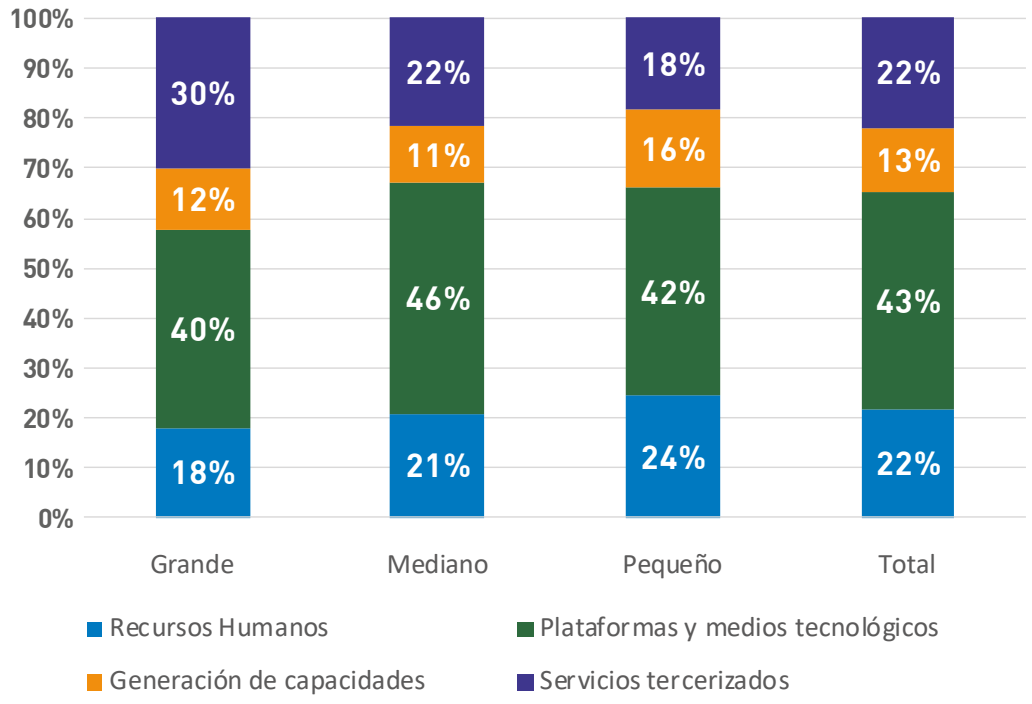
- *"Los Bancos deben tratar la seguridad cibernética como un problema comercial, no como un problema de TI, ya que una seguridad deficiente no solo generará costos de incumplimiento y litigios, sino que también erosionará la confianza del cliente en la organización." (CAPGEMINI, 2017)*

- *"Los profesionales de la seguridad citan el presupuesto, la interoperabilidad y el personal como sus principales limitaciones a la hora de administrar la seguridad (...). La falta de personal capacitado también se menciona como un desafío para la adopción de tecnología y procesos de seguridad avanzados." (CISCO, 2018)*

- *Según CISCO (2018), los principales obstáculos para adoptar tecnología y procesos de seguridad avanzados en las organizaciones en Latinoamérica (Argentina, Chile y Colombia) son: Restricciones presupuestarias, falta de cultura organizacional y problemas de compatibilidad con sistemas heredados.*

Ahora, del presupuesto de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) destinado por las entidades bancarias en el actual año fiscal, se apreció la siguiente distribución del mismo, la cual fue muy similar al hacer el análisis por tamaño de organización: el 43% en *Plataformas y medios tecnológicos (ej.: hardware, software)*, el 22% en *Recursos Humanos (ej.: empleados en la nómina)*, el 22% en *Servicios tercerizados (ej.: gestión de seguridad, externalización, soporte)* y el 13% en *Generación de capacidades (ej.: capacitación, concientización, investigación)*. Sobre esta última categoría se destaca lo encontrado por ACCENTURE (2017): *"Sólo el 13% invertiría en capacitación sobre ciberseguridad".*

Gráfica 29. Distribución del presupuesto de seguridad digital de la entidad bancaria



Nota: 162 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

En relación con el presupuesto destinado a la contratación de servicios tercerizados, se rescatan las conclusiones presentadas en WBG (2018): *"Las instituciones financieras dependen cada vez más de diversos proveedores de servicios de TI. Los servicios en la nube, en particular, están evolucionando, pasando de proporcionar solo "infraestructura como servicio" (IaaS) a "plataforma como servicio" (PaaS) e incluso a "software como servicio" (SaaS)." y "Las instituciones de todos los tamaños y perfiles de riesgo deben confiar, al menos parcialmente, en aplicaciones de software patentadas (por lo tanto, de fuente cerrada) desarrolladas por terceros, que a su vez normalmente se construyen sobre muchas bibliotecas diferentes desarrolladas por terceros adicionales completamente desconocidos para el banco."*

A partir de la estimación del presupuesto de la seguridad digital como porcentaje del EBITDA del año inmediatamente anterior que dedican las entidades bancarias en la región por tamaño de la organización y de la estimación del porcentaje de presupuesto destinado a recursos humanos, se desprende que: i) el presupuesto asignado a un miembro promedio del equipo de seguridad digital por un banco grande en la región en 2017 fue de US $22.713 al año, ii) el presupuesto asignado a un miembro promedio del equipo de seguridad digital por un banco mediano en la región en 2017 fue de US $21.766 al año, y, iii) el presupuesto asignado a un miembro promedio del equipo de seguridad digital por un banco pequeño en la región en 2017 fue de US $13.927 al año.

Cuadro 9. Presupuesto anual promedio asignado a Recursos Humanos estimado a un miembro del equipo de seguridad digital de la entidad bancaria

Tamaño	Hasta 300 empleados	Entre 301 y 999 empleados	Entre 1.000 y 4.999 empleados	Más de 5.000 empleados	Promedio Total
Grande	-	-	$20.523	$23.809	**$22.713**
Mediano	-	$15.119	$27.556	-	**$21.766**
Pequeño	$13.927	-	-	-	**$13.927**
Promedio Total	**$13.927**	**$15.119**	**$26.260**	**$23.809**	**$19.437**

Nota: 116 registros

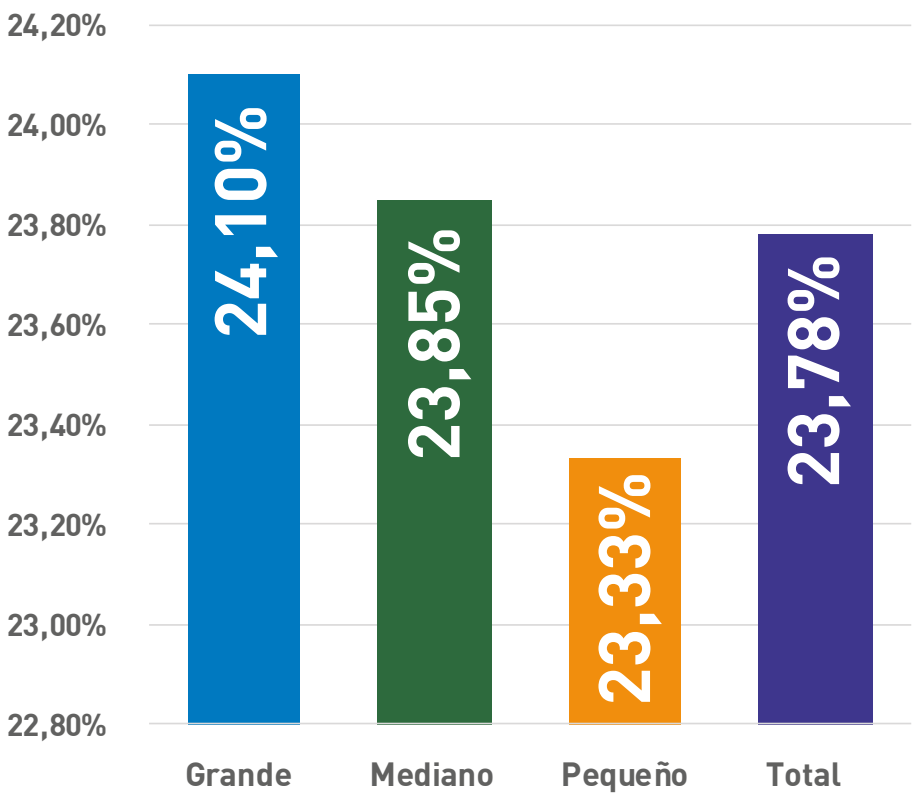
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Estas cifras promedio guardan una adecuada relación con las que se reflejan en el estudio GLOBAL KNOWLEDGE (2017), que indica que el salario promedio anual para expertos en funciones de Ciberseguridad es de US$ 36.025, si se tiene en cuenta que las áreas de ciberseguridad cuentan además de estos profesionales con personal asistencial y administrativo, lo que podría explicar la diferencia con los montos promedios obtenidos frente a lo asignado a Recursos Humanos del equipo de seguridad digital de la entidad bancaria.

Respecto a la importancia de destinar y mantener el Recurso Humano adecuado destinado a llevar a cabo actividades relacionadas con la gestión de riesgos de seguridad, se destaca lo concluido por EY (2018): *"El riesgo cibernético es el principal riesgo en evolución. Nuestra encuesta de perspectivas de la banca global revela que la mejora de la ciberseguridad se ha convertido en la principal prioridad para los Bancos en el próximo año. Sin embargo, como los equipos de liderazgo bancario se enfocan en invertir en personas y tecnología para mejorar la seguridad cibernética, es probable que enfrenten una serie de nuevos problemas, tales como encontrar el talento adecuado cuando existe una escasez de habilidades de ciberseguridad y cómo integrar expertos cibernéticos en sus organizaciones. Contratar personas con las habilidades cibernéticas correctas es una cosa; ayudarlos a desarrollar el negocio correcto y las habilidades de riesgo para un entorno bancario es otra."*

Por otro lado, de la información recolectada de la muestra de entidades bancarias se estima que el retorno sobre la inversión en seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) equivale aproximadamente a: i) un 24,1% para un banco grande en la región, ii) un 23,85% para un banco mediano en la región, y, iii) un 23,33% para un banco pequeño en la región.

Gráfica 30. Retorno sobre la inversión en seguridad digital



Nota: 32 registros

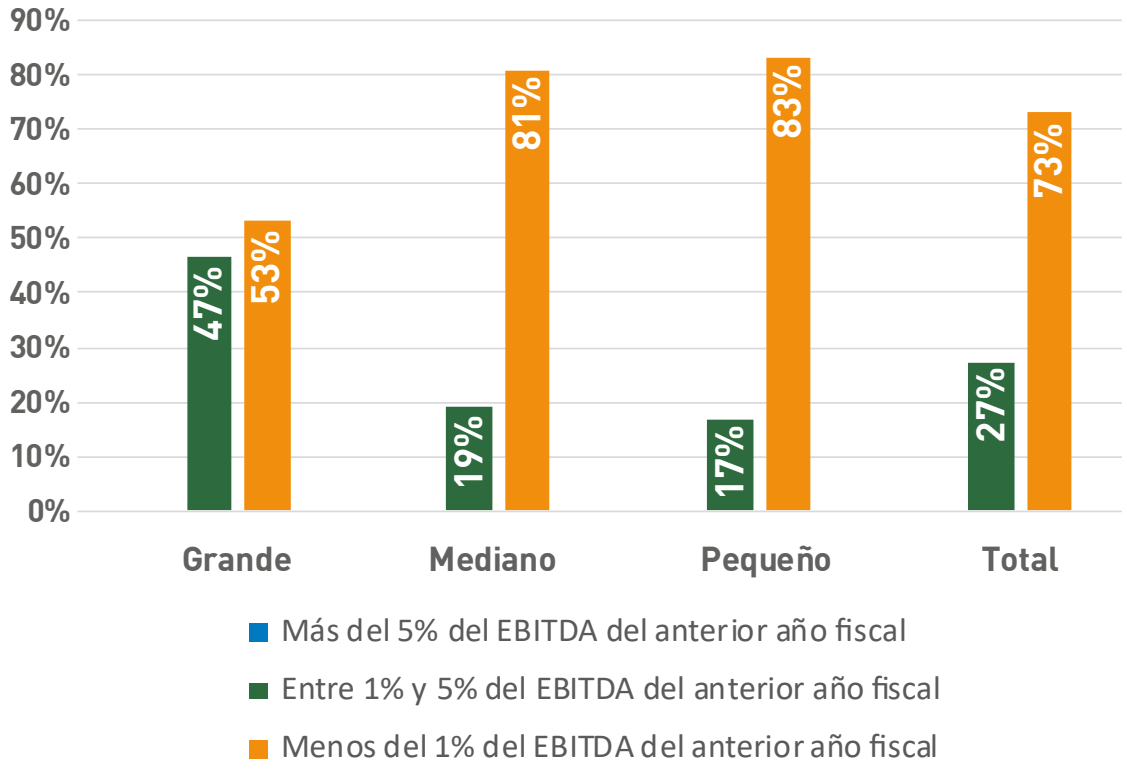
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Respecto a las estimaciones del retorno sobre la inversión en seguridad digital: i) el 20% de los Bancos grandes, el 8% de los Bancos medianos y el 22% de los Bancos pequeños consideran que son retornos de baja rentabilidad, ii) el 70% de los Bancos grandes, el 54% de los Bancos medianos y el 56% de los Bancos pequeños consideran que son retornos de media rentabilidad, iii) el 10% de los Bancos grandes, el 31% de los Bancos medianos y el 2% de los Bancos pequeños consideran que son retornos de alta rentabilidad, y iv) tan sólo el 8% de los Bancos medianos la consideran como de muy alta rentabilidad.

Ahora, a partir de las entidades bancarias que presentaron información, se destaca que el 73% de las entidades bancarias en la región manifestaron que el costo total de respuesta y de recuperación ante incidentes de seguridad digital equivale a menos del 1% del EBITDA del anterior año fiscal y el 27% de las entidades bancarias manifestaron que el valor de dicho costo estuvo entre el 1% y el 5% del EBITDA del anterior año fiscal.

Del análisis también se puede inferir que a medida que aumenta el tamaño del banco aumenta el costo total de respuesta y de recuperación ante incidentes de seguridad digital como % del EBITDA del año inmediatamente anterior. Por ejemplo, el 47% de los Bancos grandes manifestaron que el valor de dicho costo estuvo entre el 1% y el 5% del EBITDA del anterior año fiscal, mientras que el 19% de los Bancos medianos y el 17% de los Bancos pequeños manifestaron que dicho costo se encontraba en ese rango.

Gráfica 31. Costo total de respuesta y de recuperación ante incidentes de seguridad digital como % del EBITDA del año inmediatamente anterior



Nota: 48 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

A partir de la información recolectada de las entidades bancarias de la región América Latina y el Caribe que participaron en el desarrollo del presente estudio se hizo posible analizar algunos indicadores promedio para la región y por tamaño de organización que permiten estimar el impacto de los incidentes de seguridad digital durante el año 2017. Por ejemplo: i) el presupuesto y costo relacionados con la seguridad digital como % del EBITDA del año inmediatamente anterior, ii) el costo total anual de respuesta y de recuperación ante incidentes de seguridad digital por entidad bancaria, y, iii) el costo total anual de respuesta y de recuperación ante incidentes de seguridad digital de las entidades bancarias en América Latina y el Caribe.

Cuadro 10. Estimación del presupuesto y del costo relacionados con la seguridad digital como % del EBITDA del año inmediatamente anterior

Bancos que estimaron presupuesto y costos de seguridad digital

				Presupuesto SegDig		Costo SegDig			
Tamaño	# de Bancos	Activos (mill. de US$)	EBITDA (mill. de US$)	Presupuesto como % EBITDA estimado	Total (mill. de US$)	Costo como % EBITDA estimado	Total (mill. de US$)	Presupuesto por Banco al año (mill. de US$)	Costo por Banco al año (mill. de US$)
Grande	14	269.000	3.960	1,86%	73,5	1,86%	73,5	USD 5,253	USD 5,253
Mediano	21	59.500	920	2,14%	19,7	1,38%	12,7	USD 0,939	USD 0,605
Pequeño	11	62.500	130	2,27%	3,0	1,36%	1,8	USD 0,269	USD 0,161
Total	**46**	**391.000**	**5.010**	**2,09%**	**96**	**1,52%**	**88**	**USD 2,091**	**USD 1,913**
Participación en 191 Bancos		40%	47%				**Utilidad/Activos**	**1,28%**	

Cuadro 10.

Bancos que estimaron presupuesto de seguridad digital

	# de Bancos	Activos (mill. de US$)	EBITDA (mill. de US$)	Presupuesto como % EBITDA estimado	Total (mill. de US$)
Total	126	724.500	9.265	1,87%	171
Participación en 191 Bancos		74%	87%		

Utilidad/Activos **1,28%**

Bancos con respuestas completas

	# de Bancos	Activos (mill. de US$)	EBITDA (mill. de US$)
Total	191	977.500	10.675

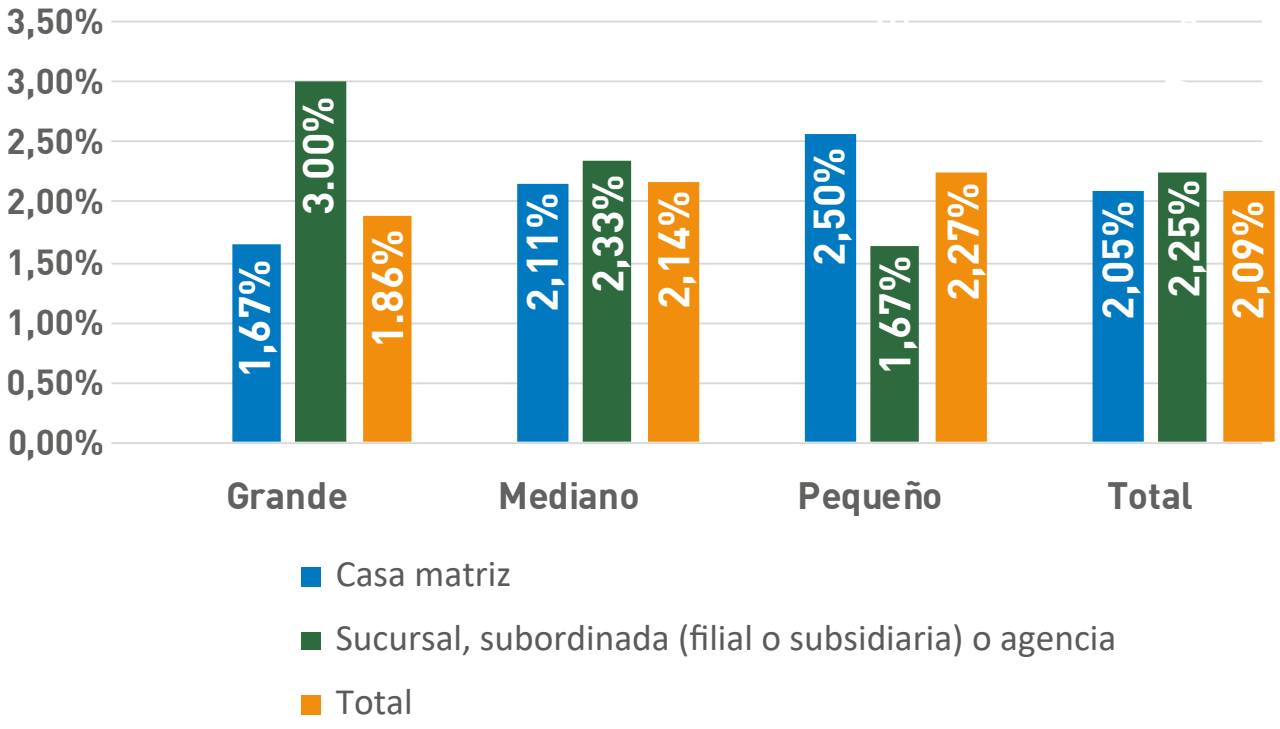
Utilidad/Activos **1,28%**

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Por ejemplo, a partir de la muestra de entidades bancarias que reportaron información en promedio se concluye que: i) el presupuesto destinado a la seguridad digital por una entidad bancaria promedio en la región equivale aproximadamente al 2,09% del EBITDA del año inmediatamente anterior, y, ii) el costo total de respuesta y de recuperación ante incidentes de seguridad digital para una entidad bancaria promedio en la región equivale aproximadamente al 1,52% del EBITDA del año inmediatamente anterior.

Al analizar por tamaño de la organización, se destaca que el presupuesto destinado a la seguridad digital por un banco grande promedio en la región equivale aproximadamente al 1,86% del EBITDA del año inmediatamente anterior, al 2,14% de dicho EBITDA para un banco mediano promedio y a un 2,27% de dicho EBITDA para un banco pequeño promedio. Del análisis, se destaca que el presupuesto como % de EBITDA del año anterior para entidades que son Casa Matriz en el país disminuye a medida que el tamaño del banco aumenta, mientras que el presupuesto como % de EBITDA para entidades que son Sucursal, Subordinada o Agencia de la entidad bancaria en el país aumenta a medida que el tamaño del banco aumenta.

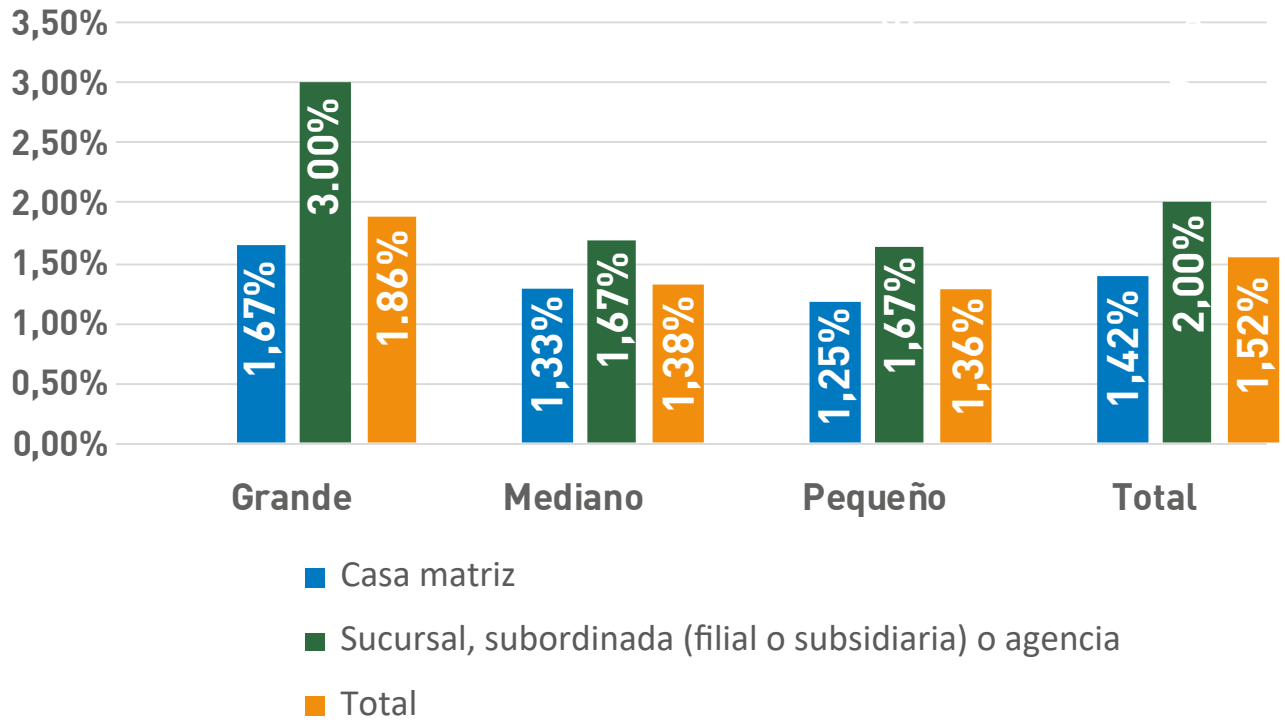
Gráfica 32. Presupuesto destinado a la seguridad digital como % del EBITDA del año inmediatamente anterior, teniendo en cuenta si es i) Casa Matriz o ii) Sucursal, Subordinada o Agencia de la entidad bancaria



Nota: 46 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Por su parte, el costo total de respuesta y de recuperación ante incidentes de seguridad digital para un banco grande promedio en la región equivale aproximadamente al 1,86% del EBITDA del año inmediatamente anterior, al 1,38% de dicho EBITDA para un banco mediano promedio y a un 1,36% de dicho EBITDA para un banco pequeño promedio. En contraste con lo encontrado en relación con el presupuesto destinado a seguridad digital, se destaca que el costo total como % de EBITDA del año anterior aumenta a medida que el tamaño del banco aumenta, independientemente de si la entidad bancaria es Casa Matriz o Sucursal, Subordinada o Agencia.

Gráfica 33. Costo total de respuesta y de recuperación ante incidentes de seguridad digital como % del EBITDA del año inmediatamente anterior, teniendo en cuenta si es i) Casa Matriz o ii) Sucursal, Subordinada o Agencia de la entidad bancaria

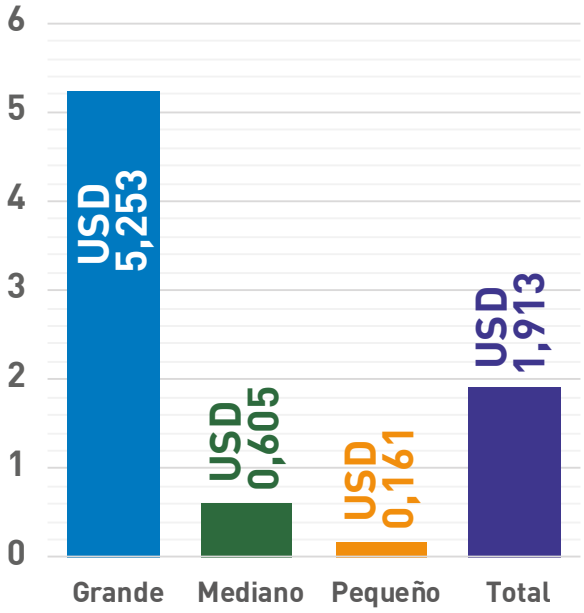


Nota: 46 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Al hacer los análisis de los resultados en términos absolutos, se estima que el costo total de respuesta y de recuperación ante incidentes de seguridad digital para un banco grande promedio equivale aproximadamente a US $5.253.000 al año, para un banco mediano promedio equivale aproximadamente a US $605.000 al año y para un banco pequeño promedio equivale aproximadamente a US $161.000 al año.

Gráfica 34. Costo total anual de respuesta y de recuperación ante incidentes de seguridad digital por entidad bancaria (millones de dólares americanos)



Nota: 46 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Estas estimaciones guardan correspondencia con resultados de otros estudios regionales y globales en la materia:

- Según BANKDIRECTOR (2018), los Bancos en Estados Unidos que tienen activos mayores a US$10.000 millones presupuestaron en promedio US$5 millones para los gastos de seguridad digital (incluido el personal y la tecnología), los Bancos que tienen activos entre US$1.000 millones y US$10.000 millones presupuestaron en promedio entre US$200.000 y US$450.000 y los Bancos que tienen activos menores a US$1.000 millones presupuestaron entre US$50.000 y US$105.000.

- *"Las infracciones causan un daño económico real a las organizaciones, daños que pueden tardar meses o años en resolverse. Según los encuestados del estudio, más de la mitad (53 por ciento) de todos los ataques resultaron en daños financieros de más de USD $500,000, que incluyen, entre otros, pérdida de ingresos, clientes, oportunidades y costos de bolsillo."* (CISCO, 2018)

- *"Los encuestados informan que los Bancos presupuestaron una mediana de US$200,000 para gastos de ciberseguridad, incluyendo personal y tecnología."* (BANKDIRECTOR, 2018)

Finalmente, a partir de la muestra de entidades bancarias que reportaron información en promedio se estima que el costo total de respuesta y de recuperación ante incidentes de seguridad digital de las entidades bancarias en América Latina y el Caribe alcanzó los US $809 millones de dólares para el año 2017.

Estimación del costo total anual de respuesta y de recuperación ante incidentes de seguridad digital de las entidades bancarias en América Latina y el Caribe (millones de dólares americanos)

Utilidad Neta Acumulada Entidades Bancarias LAC Dic2017 (FELABAN) = USD $ 53.172 millones aprox.

Costo total de respuesta y de recuperación ante incidentes de seguridad digital como % del EBITDA = 1,52%

Costo total anual de respuesta y de recuperación ante incidentes de seguridad digital de las entidades bancarias en LAC en 2017 = USD $ 53.172 millones x 1,52% = USD $ 809 millones aprox.

4.4 Análisis econométrico de los resultados

A continuación, se realizan estimaciones econométricas en las que se tiene por objetivo encontrar los factores que determinan si una entidad bancaria fue víctima de ataques a la seguridad digital. Se tiene como punto de partida información de corte transversal en la que la unidad de análisis corresponde a entidades bancarias de América Latina que respondieron la encuesta respectiva. Se incluyen como variables dependientes un conjunto de indicadores que tratan de capturar las características propias de la entidad financiera, gestión de riesgos de seguridad digital, preparación y gobernanza, detección y análisis de eventos de seguridad digital, herramientas, controles y procesos implementados en la entidad bancaria, gestión, respuesta y recuperación ante incidentes de seguridad digital, reporte de incidentes de seguridad digital, capacitación y concientización, impacto de los incidentes de seguridad digital.

El modelo utilizado en la estimación presenta variable dependiente discreta {0,1}, del tipo LOGIT o PROBIT, escogido de acuerdo con el mejor ajuste. Este tipo de modelos es ampliamente utilizado en la literatura y emplea una función de distribución acumulativa (FDA) normal. En este caso la variable dependiente (y) toma el valor de 1 si la entidad bancaria fue víctima de eventos a la seguridad digital y 0 de lo contrario. Como se mencionó en el párrafo anterior, se incluyeron variables independientes relacionadas a los tópicos mencionados con el fin de estimar la probabilidad de existencia de eventos a la seguridad digital o de otra interpretación y encontrar los factores que determinan que un banco tenga la característica "eventos a la seguridad digital".

Respecto a la estimación de este tipo de modelos, se lleva a cabo a través del método de máxima verosimilitud empleando iteraciones sucesivas. A través de la estimación se pretende establecer la significancia global del modelo estimado. Asimismo, se enfoca en la significancia individual de las variables independientes para establecer la relevancia de las mismas como factor explicativo de la probabilidad de eventos a la seguridad digital en las entidades bancarias. Lo anterior con el objeto de determinar si el factor asociado aumenta o disminuye la probabilidad de ocurrencia del evento. Finalmente, se calcularán los efectos marginales de las variables explicativas sobre la probabilidad de existencia de eventos a la seguridad digital para determinar su contribución.

La descripción de las variables utilizadas y que potencialmente pueden hacer parte del modelo se muestra en la siguiente tabla:

Cuadro 11. Variables utilizadas en el modelo utilizado del tipo LOGIT - Bancos

TIPO	VARIABLE	DESCRIPCIÓN
Características propias de la entidad financiera	Propiedad	Teniendo en cuenta el tipo de propiedad, el banco al cual usted pertenece (en el país en el que se encuentra), corresponde a un
Características propias de la entidad financiera	Capital social	Indique de dónde proviene la mayoría del capital social del banco al cual usted pertenece (en el país en el que se encuentra)
Características propias de la entidad financiera	Empleados	¿Cuántos empleados tiene el banco al cual usted pertenece (en el país en que se encuentra)?
Características propias de la entidad financiera	Sucursales	¿Cuántas sucursales tiene el banco al cual usted pertenece (en el país en que se encuentra)?
Características propias de la entidad financiera	Operaciones no presenciales	Del total de operaciones del banco al cual usted pertenece (en el país en que se encuentra), que porcentaje se realizó por medio de canales transaccionales no presenciales (Internet, transacciones electrónicas, cajeros automáticos, pagos automáticos, telefonía móvil y audio respuesta) durante los últimos doce meses.
Preparación y gobernanza	Área de Seguridad digital	¿En el banco al cual usted pertenece (en el país en el que se encuentra) existe una única área responsable por la seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales)?
Preparación y gobernanza	Responsabilidad de seguridad digital	¿Cuantas áreas tienen la máxima responsabilidad por la seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) en el banco al cual usted pertenece (en el país en el que se encuentra)?
Preparación y gobernanza	Niveles jerárquicos	Entendiendo que el CEO del banco al cual usted pertenece (en el país en el que se encuentra) es la cabeza de la institución (Nivel 0), ¿Cuántos niveles jerárquicos hay entre el CEO y el máximo responsable de la seguridad digital (incluidos aspectos de seguridad de la informa-ción, ciberseguridad y prevención del fraude usando medios digitales)? (por ejemplo, si el máximo responsable reporta directamente al CEO, sería un nivel)
Preparación y gobernanza	Cargo responsable de seguridad digital	¿Cuál es la denominación del cargo que tiene el máximo responsable de la seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) en el banco al cual usted pertenece (en el país en el que se encuentra)?
Preparación y gobernanza	Servicios externos relacionados con seguridad digital	¿Cuáles servicios externos (outsourcing) tiene contratado el banco al cual usted pertenece (en el país en el que se encuentra) para adelantar las siguientes actividades relacionadas con la seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales)? Múltiples respuestas pueden ser posibles

TIPO	VARIABLE	DESCRIPCIÓN
Preparación y gobernanza	Equipos asociados a la seguridad digital	¿Cuántas personas conforman la totalidad de equipos que manejan procesos asociados a la seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) en el banco al cual usted pertenece (en el país en el que se encuentra), sin incluir personal de empresas que prestan servicios externos (outsourcing)? ¿Considera usted adecuado que este equipo creciera en el corto plazo?
Detección y análisis de eventos de seguridad digital	Reportes de seguridad digital	Como parte del modelo de gobierno de la institución ¿La junta directiva del banco al cual usted pertenece (en el país en el que se encuentra) recibe reportes periódicos acerca de indicadores y gestión de riesgos de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales)?
Detección y análisis de eventos de seguridad digital	Alta dirección en gestión de seguridad digital	¿Cómo maneja la alta dirección del banco al cual usted pertenece (en el país en el que se encuentra) la gestión de la seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales)?
Detección y análisis de eventos de seguridad digital	Apoyo de alta dirección en riesgo de seguridad digital	¿Cómo demuestra la alta dirección del banco al cual usted pertenece (en el país en el que se encuentra) el apoyo a la gestión del riesgo de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales)? Múltiples respuestas pueden ser posibles.
Detección y análisis de eventos de seguridad digital	Inversión en soluciones de seguridad digital	¿Cuán complejo es, en su opinión, convencer a la alta dirección del banco al cual usted pertenece (en el país en el que se encuentra) en invertir en soluciones de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales)?
Herramientas, controles y procesos implementados en la entidad bancaria	Marcos de seguridad	¿El banco al cual usted pertenece (en el país en el que se encuentra) ha adoptado los siguien-tes marcos de seguridad y/o estándares internacionales? Múltiples respuestas pueden ser posibles.
Herramientas, controles y procesos implementados en la entidad bancaria	Acciones / medidas técnicas de seguridad digital	¿Qué tipo de acciones y medidas técnicas de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) tiene el banco al cual usted pertenece (en el país en el que se encuentra) para proteger los sistemas de información críticos? Múltiples respuestas pueden ser posibles.
Herramientas, controles y procesos implementados en la entidad bancaria	Herramientas actuales de seguridad digital	¿El banco al cual usted pertenece (en el país en el que se encuentra) está implementando actualmente herramientas, controles o procesos de seguridad digital usando alguna de las siguientes tecnologías digitales emergentes? Múltiples respuestas pueden ser posibles.
Herramientas, controles y procesos implementados en la entidad bancaria	Herramientas / procesos de seguridad digital	¿El banco al cual usted pertenece (en el país en el que se encuentra) está implementando actualmente herramientas, controles o procesos de seguridad digital usando alguna de las siguientes tecnologías digitales emergentes? Múltiples respuestas pueden ser posibles.
Herramientas, controles y procesos implementados en la entidad bancaria	Soluciones con tecnologías digitales emergentes.	De ser posible, comente o contribuya con la OEA con información adicional sobre soluciones de seguridad digital implementadas usando tecnologías digitales emergentes como las señaladas en el punto anterior.

TIPO	VARIABLE	DESCRIPCIÓN
Gestión de riesgos de seguridad digital	Riesgos cibernéticos	¿Cuáles son los riesgos cibernéticos que considera usted merecen mayor atención por parte del banco al cual usted pertenece (en el país en el que se encuentra)? Priorice todos los riesgos otorgándoles un número del 1 al 7, siendo el 1 el riesgo más alto y 7 el riesgo más bajo.
Detección y análisis de eventos de seguridad digital	Eventos en contra de seguridad digital	¿Qué tipos de eventos (ataques exitosos y ataques no exitosos) de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) contra el banco al cual usted pertenece (en el país en el que se encuentra) se han identificado durante los últimos doce meses? Para cada tipo, por favor indique la frecuencia aproximada de ocurrencia.
Detección y análisis de eventos de seguridad digital	Eventos de seguridad digital usados por ciberdelincuentes	¿Qué tipos de eventos (ataques exitosos y ataques no exitosos) de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) usan los ciberdelincuentes contra los usuarios de servicios financieros del banco al cual usted pertenece (en el país en el que se encuentra)? Priorice todos los eventos otorgándoles un número del 1 al 12, siendo el 1 el evento más frecuente y 12 el evento menos frecuente.
Detección y análisis de eventos de seguridad digital	Porcentaje de eventos detectados por sistemas propios	¿Qué porcentaje de eventos (ataques exitosos y ataques no exitosos) de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) son detectados mediante sistemas propios (y no de terceros) de detección del banco al cual usted pertenece (en el país en el que se encuentra)?
Gestión, respuesta y recuperación ante inci-dentes de seguridad digital	Estrategias contra incidentes de seguridad digital	¿El banco al cual usted pertenece (en el país en el que se encuentra) cuenta y ejecuta las siguientes estrategias frente a incidentes (ataques exitosos) de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales)?
Gestión, respuesta y recuperación ante incidentes de seguridad digital	Actuales incidentes de seguridad digital	¿El banco al cual usted pertenece (en el país en el que se encuentra), como organización, fue víctima de incidentes (ataques exitosos) de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) durante los últimos doce meses?
Reporte de incidentes de seguridad digital, capaci-tación y concientización	Fuentes de incidentes de seguridad digital	¿El banco al cual usted pertenece (en el país en el que se encuentra) investigó la fuente que generó dichos incidentes (ataques exitosos) de seguridad digital (incluidos aspectos de segu-ridad de la información, ciberseguridad y prevención del fraude usando medios digitales)?
Reporte de incidentes de seguridad digital, capaci-tación y concientización	Motivaciones de incidentes actuales de seguridad digital	¿Cuáles considera fueron las principales motivaciones de dichos incidentes (ataques exitosos) de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) sufridos por el banco al cual usted pertenece (en el país en el que se encuentra) durante los últimos doce meses? Múltiples respuestas pueden ser posibles.

TIPO	VARIABLE	DESCRIPCIÓN
Gestión, respuesta y recuperación ante incidentes de seguridad digital	Valoración externa de seguridad digital	¿El banco al cual usted pertenece (en el país en el que se encuentra) ha sido valorado externamente en los últimos dos (2) años bajo alguna metodología de evaluación de la madurez de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) y ha completado dicha evaluación?
Gestión, respuesta y recuperación ante incidentes de seguridad digital	Evaluación de seguridad digital	En caso de que el banco al cual usted pertenece (en el país en el que se encuentra) no haya completado totalmente una evaluación de la madurez de la de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) o ejecutado todas sus acciones derivadas, ¿A qué lo atribuye? Múltiples respuestas pueden ser posibles.
Herramientas, controles y procesos implementados en la entidad bancaria	Mecanismos internos de seguridad digital	¿El banco al cual usted pertenece (en el país en el que se encuentra) ofrece un mecanismo para que sus usuarios internos (empleados y contratistas) reporten incidentes (ataques exitosos) de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) sufridos?
Herramientas, controles y procesos implementados en la entidad bancaria	Mecanismos para clientes financieros de seguridad digital	¿El banco al cual usted pertenece (en el país en el que se encuentra) ofrece un mecanismo para que sus clientes de servicios financieros reporten al banco incidentes (ataques exitosos) de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) sufridos?
Herramientas, controles y procesos implementados en la entidad bancaria	Plan de comunicaciones	¿El banco al cual usted pertenece (en el país en el que se encuentra) cuenta con un plan de comunicaciones que permita informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida?
Herramientas, controles y procesos implementados en la entidad bancaria	Mecanismos de reporte de seguridad digital	¿Conoce algún mecanismo para reportar incidentes (ataques exitosos) de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) sufridos por el banco al cual usted pertenece (en el país en el que se encuentra) ante una autoridad de regulación en su país?
Herramientas, controles y procesos implementados en la entidad bancaria	Reportes ante la ley de incidentes de seguridad digital	¿El banco al cual usted pertenece (en el país en el que se encuentra) reporta los incidentes (ataques exitosos) de seguridad digital sufridos ante una autoridad de aplicación de la ley?
Herramientas, controles y procesos implementados en la entidad bancaria	Efectividad de autoridades frente a ciberdelicnuentes	En general, ¿cómo considera la efectividad de las autoridades de aplicación de la ley respecto a la respuesta, investigación y judicialización de los ciberdelincuentes?
Herramientas, controles y procesos implementados en la entidad bancaria	Planes de preparación, respuesta y capacitación de seguridad digital	¿Cuenta el banco al cual usted pertenece (en el país en el que se encuentra) con planes de preparación, respuesta y capacitación en asuntos de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) para sus empleados e insourcing bancarios?

TIPO	VARIABLE	DESCRIPCIÓN
Herramientas, controles y procesos implementados en la entidad bancaria	Tiempos de realización de planes	¿Con que frecuencia se ejecutan dichos planes de preparación, respuesta y capacitación?
Herramientas, controles y procesos implementados en la entidad bancaria	Pruebas de capacidad de respuesta frente a incidentes de seguridad digital	¿Con qué frecuencia se prueba la capacidad de los empleados del banco al cual usted pertenece (en el país en el que se encuentra) a responder adecuadamente frente incidentes (ataques exitosos) seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) y esquemas de phishing e ingeniería social?
Herramientas, controles y procesos implementados en la entidad bancaria	Mecanisnos efectivos frente a riesgos de seguridad digital	¿Cuál ha sido el mecanismo más efectivo a partir del cual se ha generado mayor conciencia en el banco al cual usted pertenece (en el país en el que se encuentra) respecto de los riesgos de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales)? Priorice todos los mecanismos otorgándoles un número del 1 al 9, siendo el 1 el mecanismo más efectivo y 9 el mecanismo menos efectivo.
Impacto de los incidentes de seguridad digital	Activos totales	¿Cuál fue el valor de activos totales del banco al cual usted pertenece (en el país en que se encuentra) en el año fiscal inmediatamente anterior?
Impacto de los incidentes de seguridad digital	EBITDA	¿Cuál fue el valor del EBITDA (en inglés, Earnings Before Interests, Taxes, Depreciations and Amortizations) del banco al cual usted pertenece (en el país en que se encuentra) en el año fiscal inmediatamente anterior?
Impacto de los incidentes de seguridad digital	Presupuesto de seguridad digital	¿Cuál fue el presupuesto de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) del banco al cual usted pertenece (en el país en que se encuentra) para el actual año fiscal?
Impacto de los incidentes de seguridad digital	Incremento de presupuesto de seguridad digital	En comparación al año fiscal inmediatamente anterior ¿Cuánto ha aumentado el presupuesto de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) del banco al cual usted pertenece (en el país en que se encuentra) para el actual año fiscal? Si se presentó un aumento en el presupuesto de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales), identifique las tres (3) razones principales que llevaron a dicho aumento:
Impacto de los incidentes de seguridad digital	% Presupuesto	Del presupuesto de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) del banco al cual usted pertenece (en el país en que se encuentra) en el actual año fiscal, por favor estime el porcen-taje asignado a cada una de las siguientes cuatro (4) categorías (Las opciones tienen que sumar 100%).

TIPO	VARIABLE	DESCRIPCIÓN
Impacto de los incidentes de seguridad digital	ROI de seguridad digital	¿El banco al cual usted pertenece (en el país en que se encuentra) ha llevado a cabo cálculos de retorno sobre la inversión en seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales)?
Impacto de los incidentes de seguridad digital	% ROI de seguridad digital	¿Cuál fue el retorno sobre la inversión en seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) para su banco en el año fiscal inmediatamente anterior? Por favor exprese su respuesta como un número entero equivalente a un porcentaje (por ejemplo; 30 indica 30%).
Impacto de los incidentes de seguridad digital	Costo de respuesta y recuperación de inci-dentes de seguridad digital	¿El banco al cual usted pertenece (en el país en que se encuentra) estimó el costo total de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) para el último año fiscal?
Impacto de los incidentes de seguridad digital	Costo actual de inciden-tes de seguridad digital.	¿Cuál fue el costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) para el banco al cual usted pertenece (en el país en que se encuentra) para el último año fiscal?

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Respecto a los resultados de las estimaciones, se corrieron modelos del tipo Logit, teniendo como unidad de análisis las entidades bancarias. Se estimaron diferentes modelos incluyendo las variables independientes antes descritas. Adicionalmente se trabajó con información de 191 observaciones (entidades bancarias).

Luego de probar diferentes formas funcionales y variables independientes se escoge el modelo con mejor ajuste –LOGIT–. En general el modelo presenta un buen ajuste global, cuya probabilidad se acerca a niveles de cero. Lo anterior indica que el modelo estimado como un todo es una buena representación de la variable dependiente, en este caso particular, la probabilidad de que una entidad bancaria fue víctima de eventos a la seguridad digital. A continuación, se presentan los resultados del modelo mencionado.

Cuadro 12. Resultados de las estimaciones del modelo LOGIT donde la variable dependiente (y) toma el valor de 1 si la entidad bancaria fue víctima de eventos a la seguridad digital y 0 de lo contrario

Logistic regression	**Number of obs**	**=**	**191**
	LR chi2(9)	**=**	**33.19**
	Prob > chi2	**=**	**0.0001**
Log likelihood = -104.51284	**Pseudo R2**	**=**	**0.1370**

VictimaInc	Coef.	Std. Err.	z	P>|z|	[95% Conf.	Interval]
costo	.2439135	.122274	1.99	0.046	.0042606	.4835665
miembros	-.0037382	.004924	-0.76	0.448	-.0133891	.0059126
activo	.2439135	.0000175	1.18	0.046	.0042606	.4835665
TGrande	1.014411	.5992369	1.69	0.090	-.1600722	2.188893
TMediano	1.001714	.4063689	2.47	0.014	.2052454	1.798182
casaMatriz	.768328	.4457521	1.72	0.085	-.10533	1.641986
Bprivado	1.055184	.0000175	1.73	0.084	-.1425247	2.252892
Bmixto	1.556309	.8095643	1.92	0.055	-.0304074	3.143026
areaUnicaSD	.7641452	.4195664	1.82	0.069	-.05819	1.58648
_cons	-3.816138	.8742597	-4.36	0.000	-5.529656	-2.102621

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Se incluyeron variables de control como el *Activo, dummies* de tamaño de la entidad (de acuerdo al número de sucursales y a los empleados) y *dummies* de *Propiedad* del banco. Adicionalmente se incluyeron variables propias asociadas a la gestión de la seguridad digital de la entidad bancaria, entre ellas, el *Costo* dedicado a las acciones de seguridad digital, los *Miembros* del equipo de trabajo dedicado a la seguridad digital y si cuenta con *Área Única* dedicada a la seguridad digital.

En cuanto a las variables de control relacionadas a características propias de las entidades bancarias se encuentra que el monto de los *Activos* no es significativo. Por su parte, de acuerdo con los resultados del modelo, aquellos Bancos de tamaño grande y de tamaño mediano presentan una mayor probabilidad de incidentes de seguridad digital, respecto a los Bancos pequeños. También se reporta que aquellos Bancos privados y mixtos presentan una mayor probabilidad de incidentes de seguridad digital, respecto a los Bancos públicos.

Es importante mencionar la inclusión de la variable *Costo*. Se encuentra en el modelo que es significativa presentando un signo positivo, indicando que aquellos Bancos que han asumido un mayor *Costo* total de respuesta y de recuperación ante incidentes de seguridad digital en 2017, presentaron una mayor probabilidad de haber presentado incidentes en el periodo. Por su parte, se incluyó como variable dependiente el número de *Miembros* del personal dedicado exclusivamente al equipo de seguridad digital. Se encuentra que la variable presenta signo negativo y significativo en la estimación. Lo anterior sugiere que aquellas entidades que dedican mayor personal a estas tareas disminuyen su probabilidad de presentar incidentes de seguridad digital.

Adicionalmente, se analizaron varios modelos con buen ajuste con el fin de explicar las siguientes variables dependientes: i) el tamaño del equipo que maneja procesos asociados a la seguridad digital, ii) el presupuesto dedicado a la seguridad digital, y, iii) el costo total de respuesta y de recuperación ante incidentes de seguridad digital.

En relación con los resultados de las estimaciones con variable dependiente a los miembros del equipo que maneja procesos asociados a la seguridad digital (o el logaritmo natural de los miembros) se aprecia que se espera un mayor número de miembros en Bancos de tamaño grande y mediano y a medida que crecen los *Activos* de la entidad. En contraste, se aprecia una relación entre el tamaño del equipo con la naturaleza del banco, es decir se esperan equipos mas pequeños en Bancos privados y mixtos en comparación con los Bancos públicos.

Cuadro 13. **Resultados de las estimaciones con variable dependiente:** personal (miembros)

Source	SS	df	MS		
Model	82037.9532	9	9115.32814	Number of obs	= 191
				F(9, 181)	= 4.59
				Prob > F	= 0.0000
Residual	359403.775	181	1985.65621	R-squared	= 0.1858
				Adj R-squared	= 0.1454
Total	441441.728	190	2323.37751	Root MSE	= 44.561

miembros	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
TGrande	52.1681	10.37778	5.03	0.000	31.69113	72.64511
TMediano	8.884608	7.470472	1.19	0.236	-5.855807	23.62502
casaMatriz	-11.38604	8.020053	-1.42	0.157	-27.21086	4.438788
Bprivado	-22.52051	10.10413	-2.23	0.027	-42.45754	-2.583481
Bmixto	-28.52225	15.07817	-1.89	0.060	-58.27385	1.229357
areaUnicaSD	1.765107	7.536372	0.23	0.815	-13.10534	16.63555
VictimaInc	-3.320306	7.428902	-0.45	0.655	-17.9787	11.33808
costoEBT	-674.5167	675.1612	-1.00	0.319	-2006.716	657.6823
activo	.000514	.0003167	1.62	0.106	-.0001108	.0011388
_cons	42.3053	15.86651	2.67	0.008	10.99819	73.61242

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Cuadro 14. **Resultados de las estimaciones con variable dependiente: logaritmo natural del** personal (lnmiembros)

Source	SS	df	MS		
Model	122.287039	9	13.5874488	Number of obs	= 191
				F(9, 181)	= 13.97
				Prob > F	= 0.0000
Residual	176.020474	181	.972488806	R-squared	= 0.4099
				Adj R-squared	= 0.3806
Total	298.307513	190	1.57003954	Root MSE	= .98615

lnmiembros	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
TGrande	1.972616	.2392491	8.25	0.000	1.50054	2.444692
TMediano	.7126999	.1706015	4.18	0.000	.3760763	1.049323
casaMatriz	-.2720873	.1775568	-1.53	0.127	-.6224348	.0782601
Bprivado	-.3132121	.2247507	-1.39	0.165	-.7566805	.1302563
Bmixto	-.1979587	.3332581	-0.59	0.553	-.8555292	.4596118
areaUnicaSD	-.1332119	.1691046	-0.79	0.432	-.4668819	.200458
VictimaInc	-.0352649	.1709216	-0.21	0.837	-.3725202	.3019903
lncosto1	.0535321	.0671529	0.80	0.426	-.0789711	.1860353
lnactivo	.0993163	.0726377	1.37	0.173	-.0440094	.242642
_cons	.5704745	.6768391	0.84	0.400	-.7650353	1.905984

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

En relación con los resultados de las estimaciones con variable dependiente el presupuesto (o el logaritmo natural del presupuesto) dedicado a la seguridad digital se aprecia que en Bancos grandes se espera mayor presupuesto dedicado, así como una relación positiva con el costo, es decir, el presupuesto dedicado se puede explicar con el costo total de respuesta asumido (a mayor costo se espera un mayor presupuesto en asuntos de seguridad digital). Como resultado de este modelo se incluyó también una variable de control *dummie* que representa si la entidad fue víctima o no de incidentes en el periodo, apreciando que las entidades que no fueron víctimas de incidentes dedicaron mas presupuesto dedicado a la seguridad digital.

Cuadro 15. Resultados de las estimaciones con variable dependiente: Presupuesto (ppto)

Source	SS	df	MS		
Model	526.735089	9	58.526121	Number of obs	= 191
				F(9, 181)	= 30.99
				Prob > F	= 0.0000
Residual	341.810824	181	1.88845759	R-squared	= 0.6065
				Adj R-squared	= 0.5869
Total	868.545913	190	4.57129428	Root MSE	= 1.3742

ppto	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
TGrande	.8317346	.3433371	2.42	0.016	.1542766	1.509193
TMediano	.2317614	.2310129	1.00	0.317	-.2240632	.6875861
activo	6.05e-06	.0000101	0.60	0.548	-.0000138	.0000259
casaMatriz	.1210165	.2472759	0.49	0.625	-.3668977	.6089306
Bprivado	.2559118	.3116485	0.82	0.413	-.3590196	.8708432
Bmixto	.6535669	.4659528	1.40	0.162	-.2658311	1.572965
areaUnicaSD	-.207409	.2323549	-0.89	0.373	-.6658817	.2510637
VictimaInc	-.0210439	.2311328	-0.09	0.928	-.4771052	.4350173
costo1	7.79e-07	6.52e-08	11.95	0.000	6.50e-07	9.07e-07
_cons	-.1681109	.432029	-0.39	0.698	-1.020572	.6843502

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Cuadro 16. **Resultados de las estimaciones con variable dependiente:**
logaritmo natural de Presupuesto (lnppto1)

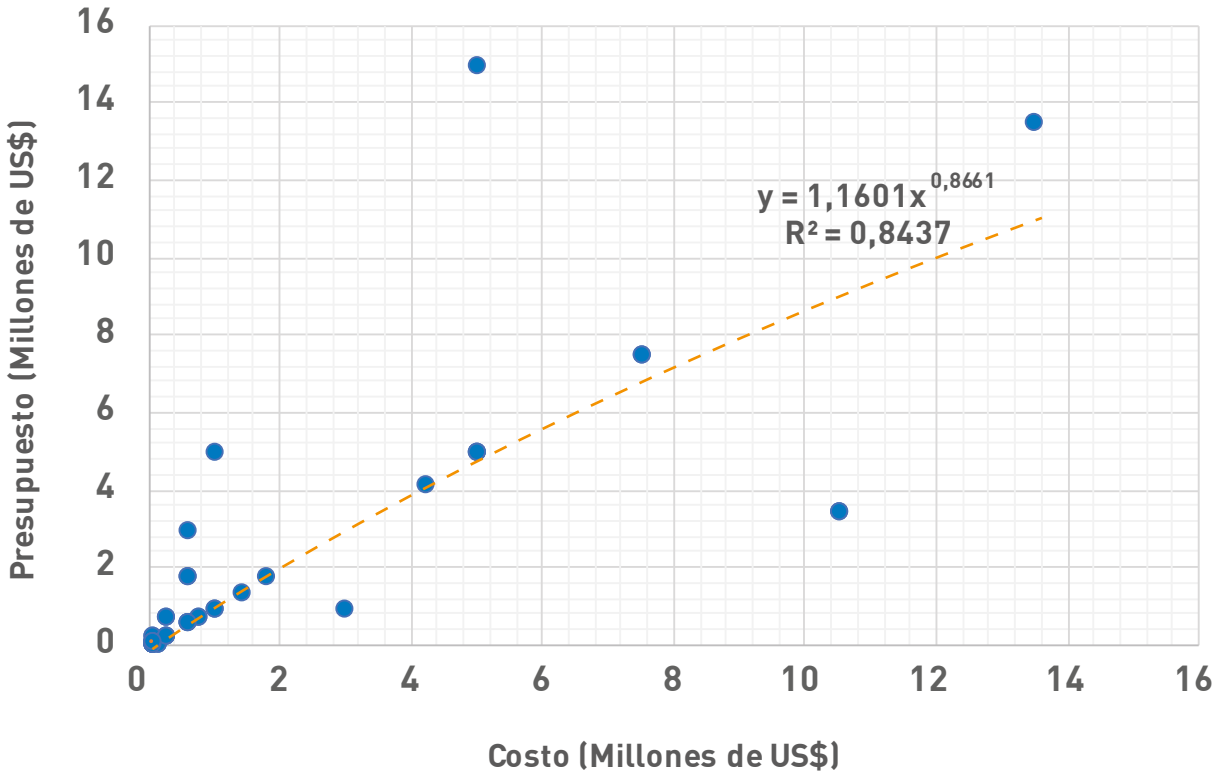
Source	SS	df	MS		
Model	967.455085	9	107.495009	Number of obs	= 191
				F(9, 181)	= 4.83
				Prob > F	= 0.0000
Residual	4031.36323	181	22.272725	R-squared	= 0.1935
				Adj R-squared	= 0.1534
Total	4998.81831	190	26.3095701	Root MSE	= 4.7194

lnppto1	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
TGrande	2.226543	1.147933	1.94	0.054	-.0385091	4.491595
TMediano	.7836754	.8167697	0.96	0.339	-.8279395	2.39529
activo	-.000067	.0000362	-1.85	0.066	-.0001383	4.37e-06
casaMatriz	1.210602	.8487889	1.43	0.156	-.4641922	.2.885395
Bprivado	1.633892	1.074449	1.52	0.130	-.4861643	3.753949
Bmixto	-.297355	1.598058	-0.19	0.853	-3.450575	2.855865
areaUnicaSD	.1493896	.7983161	0.19	0.852	-1.425813	1.724593
VictimaInc	-1.332826	.8078245	-1.65	0.101	-2.92679	.2611389
lncosto1	1.353621	.273823	4.94	0.000	.8133252	1.893917
_cons	-8.55294	3.388622	-2.52	0.012	-15.23922	-1.866657

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

La relación positiva entre las variables presupuesto dedicado a la seguridad digital y costo total de respuesta y de recuperación ante incidentes de seguridad digital se puede apreciar al hacer un análisis de correlación entre las mismas. El gráfico siguiente presenta el mismo resultado obtenido mediante el modelo econométrico, a mas costo de respuesta y recuperación mayor presupuesto dedicado a la seguridad digital. El Anexo 3 del presente documento presenta la relación de las variables mencionadas por tamaño de entidad bancaria (Bancos Grandes, Medianos y Pequeños) en América Latina y el Caribe.

Gráfica 35. Relación entre el Presupuesto destinado a Seguridad Digital y el Costo total de respuesta y de recuperación ante incidentes de seguridad para entidades bancarias en América Latina y el Caribe



Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Finalmente, en relación con los resultados de las estimaciones con variable dependiente el costo (o el logaritmo natural del costo) total de respuesta y de recuperación ante incidentes de seguridad digital, se aprecia que los Bancos grandes y medianos asumieron mayores costos durante el periodo, situación que tiene relación con el valor de los activos de la entidad (a mayor valor de activos mayor costo asumido). De igual manera, este modelo incluyó una variable de control *dummie* que representa si la entidad fue víctima o no de incidentes en el periodo, apreciando que las entidades que fueron víctimas de incidentes incurrieron en mayor costo total de respuesta y de recuperación ante incidentes de seguridad digital.

Cuadro 17. Resultados de las estimaciones con variable dependiente: Costo

Source	SS	df	MS		
Model	220.131823	8	27.5164778	Number of obs	= 191
				F(9, 181)	= 11.26
				Prob > F	= 0.0000
Residual	444.657573	182	2.44317348	R-squared	= 0.3311
				Adj R-squared	= 0.3017
Total	664.789396	190	3.49889156	Root MSE	= 1.5631

costo	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
TGrande	2.084347	.3586582	5.81	0.000	1.376684	2.792009
TMediano	.262295	.26204	1.00	0.318	-.2547319	.7793218
casaMatriz	-.1238546	.2811084	-0.44	0.660	-.6785051	.4307959
Bprivado	-.1315021	.3543434	-0.37	0.711	-.8306513	.5676472
Bmixto	-.4602598	.528888	-0.87	0.385	-1.5038	.5832807
areaUnicaSD	-.0165476	.2642839	-0.06	0.950	-.5380019	.5049067
VictimaInc	.6026437	.2590737	2.33	0.021	.0914695	1.113818
activo	.0000416	.000011	3.77	0.000	.0000198	.0000633
_cons	.1217271	.4913186	0.25	0.805	-.8476858	1.09114

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Cuadro 18. **Resultados de las estimaciones con variable dependiente:** logaritmo natural de costo

Source	SS	df	MS		
Model	272.003375	9	30.2225973	Number of obs	= 191
				F(9, 181)	= 25.46
				Prob > F	= 0.0000
Residual	214.898432	181	1.18728415	R-squared	= 0.5586
				Adj R-squared	= 0.5367
Total	486.901807	190	26.3095701	Root MSE	= 1.0896

lnppto1	Coef.	Std. Err.	t	P>|t|	[95% Conf.	Interval]
TGrande	.9784556	.3013972	3.25	0.001	.3837515	1.57316
TMediano	.535855	.1933211	2.77	0.006	.1544021	.9173079
casaMatriz	.1176836	.1972627	0.60	0.552	-.2715466	.5069138
Bprivado	-.3327028	.2484349	-1.34	0.182	-.8229038	.1574983
Bmixto	-.1866016	.3683247	-0.51	0.613	-.9133642	.5401609
areaUnicaSD	.2947919	.1858819	1.59	0.115	-.0719822	.6615661
VictimaInc	.3103659	.1874647	1.66	0.100	-.0595313	.6802631
lnactivo	.6622524	.0639145	10.36	0.000	.536139	.7883657
lnmiembros	.0653558	.0819851	0.80	0.426	-.0964136	.2271252
_cons	6.464284	.5749981	11.24	0.000	5.329723	7.598846

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

05

CIBERSEGURIDAD DESDE LA PERSPECTIVA DE LOS USUARIOS DE LAS ENTIDADES DEL SECTOR BANCARIO EN AMÉRICA LATINA Y EL CARIBE

Con el fin de elaborar el presente Estudio sobre la Ciberseguridad en el sector bancario de Latinoamérica y el Caribe, la Secretaría General de la Organización de los Estados Americanos (SG/OEA), además del instrumento ya citado con destino a las entidades del sector bancario, elaboró uno particular con el fin de obtener información sobre los aspectos relacionados con incidentes de seguridad digital (incluidos aspectos de tipos de operaciones bancarias realizadas, medios empleados, medidas de seguridad, mecanismos de reporte e impacto) con destino a los usuarios de las entidades bancarias de la región.

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

- Caracterización de los usuarios
- 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 usuarios, y en este caso no se solicitó información referida al país, 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 o institución 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 722 personas iniciaron el relleno del cuestionario durante el periodo de publicación del instrumento de recolección de información (meses comprendidos durante el primer trimestre del año 2018) y, a partir de la revisión detallada, se estableció una base de datos con registros de 562 usuarios de entidades bancarias de la región Latinoamérica y el Caribe que rellenaron la encuesta hasta su parte final. 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.

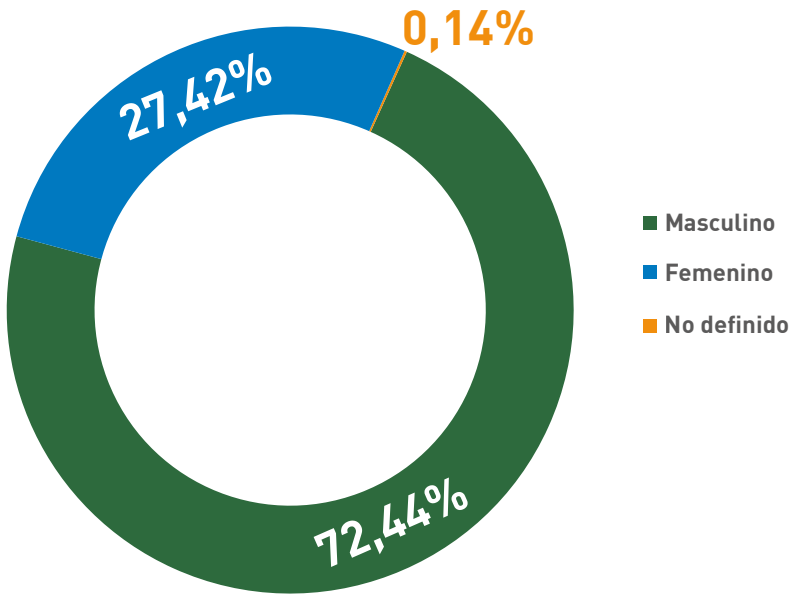
Por lo expuesto anteriormente, cada gráfica lleva asociado el número de respuestas obtenidas para la respectiva pregunta.

5.1 Caracterización del usuario

En este componente del estudio, se realizaron preguntas orientadas a establecer las características de los usuarios de Bancos que rellenaron la encuesta, en aspectos asociados al individuo (género 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 con su entidad bancaria, 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.

En cuanto a género, entre los usuarios entrevistados, el 72,44% informaron ser de género masculino, mientras que el 27,42% manifestaron ser de género femenino y el 0,14% como "no definido".

Gráfica 36. Género de los usuarios

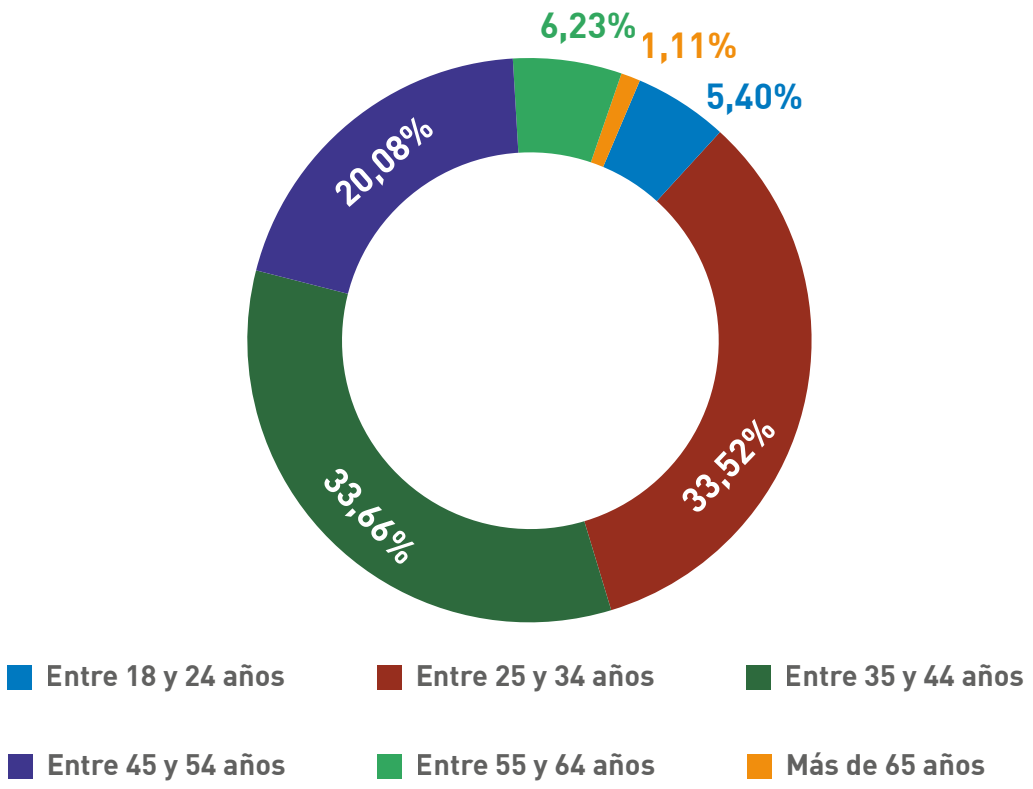


Nota: 722 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Respecto al rango de edad de los usuarios entrevistados, se tiene que el 33,66% se encuentra entre los 35 y 44 años, el 33,52% entre los 25 y 34 años, el 20,08% entre los 45 y 54 años, el 6,23% entre los 55 y 64 años, el 5,40% entre los 18 y 24 años y solo el 1,1% tiene más de 65 años de edad.

Lo anterior indica que casi el 90% de los usuarios que atendieron la encuesta tiene entre 25 y 54 años, lo cual contrasta con el apenas 1,1% de los encuestados que superan los 65 años de edad.

Gráfica 37. Rango de edad de los usuarios



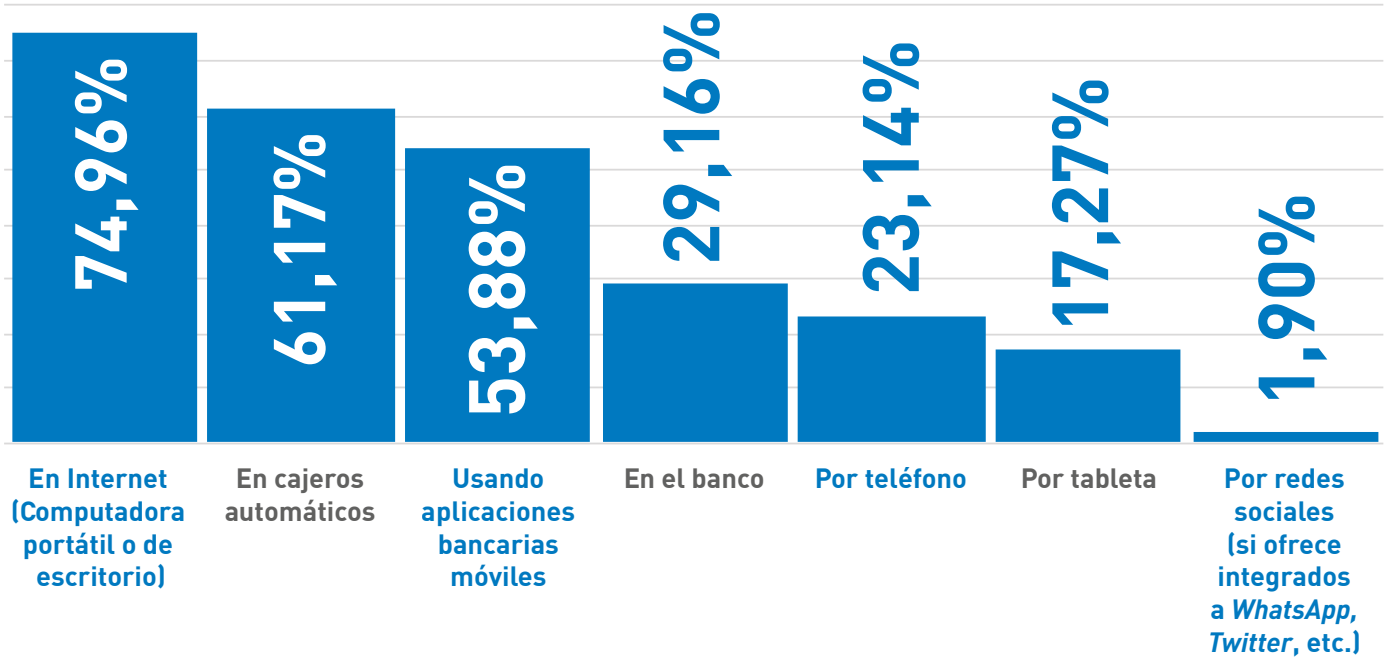
Nota: 722 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

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

Respecto de los medios empleados por los usuarios para revisar transacciones recientes y saldos disponibles, los resultados evidencian un uso significativo de computadoras portátiles o de escritorio conectadas a Internet, así como de cajeros automáticos y de aplicaciones móviles (el 74,96% indicó que empleaba computadoras conectadas a Internet, el 61,17% manifestó que usaba los cajeros automáticos, el 53,88% señaló que utilizaba aplicaciones); frente a un inferior porcentaje que señaló preferencia por el uso de canales directos en el Banco, a través del teléfono, así como de tabletas y de redes sociales en el caso de que así lo ofreciera el Banco (el 29,16% reveló que lo hacía en el banco, el 23,14% expresó que empleaba el teléfono, el 17,27% indicó que usaba la tableta y el 1,90%, servicios integrados a redes sociales).

Con base en los resultados, resulta claro que los usuarios privilegian los medios virtuales sobre los presenciales, lo cual concuerda con el alto grado de digitalización de los servicios y el impulso a la apropiación de estos por parte de los usuarios. El siguiente gráfico muestra el resumen de los resultados:

Gráfica 38. Medios para revisar transacciones recientes y saldos disponibles



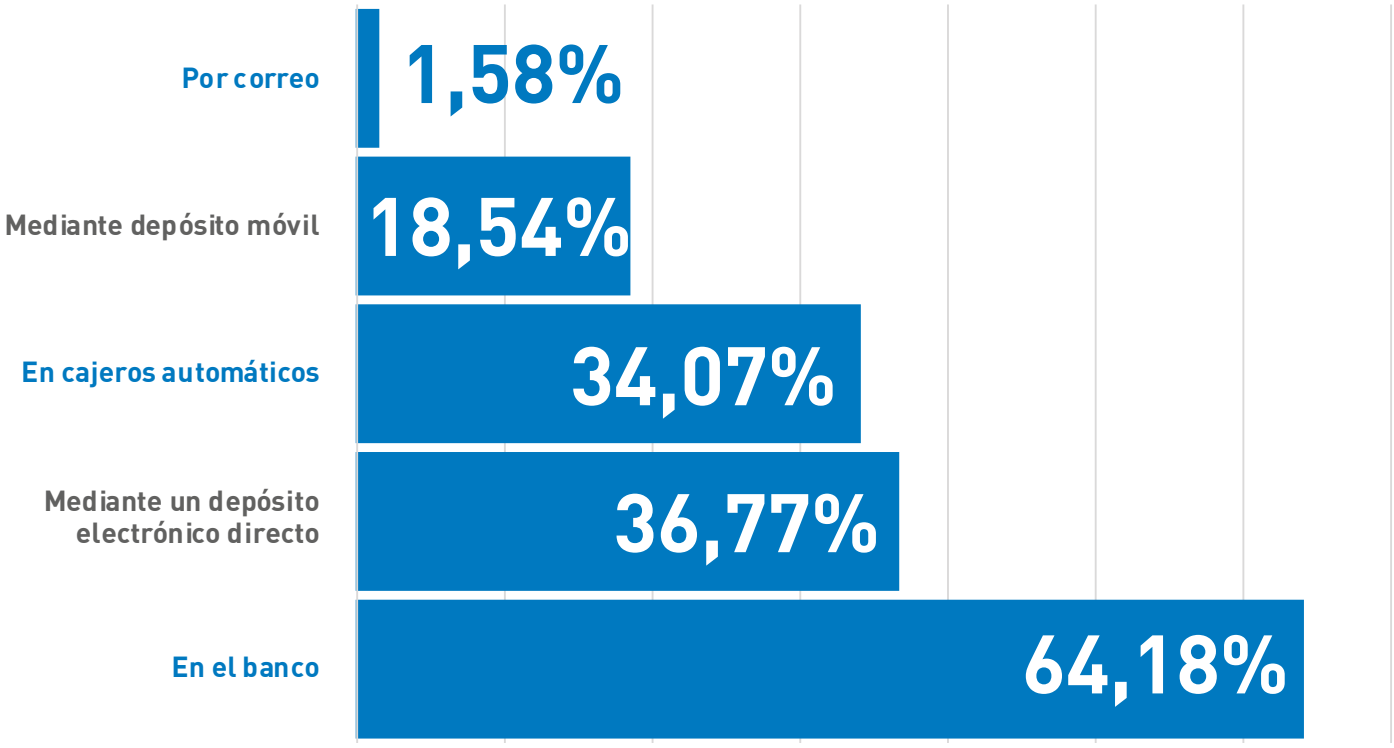
Nota: 631 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

La baja utilización de medios como las tabletas puede explicarse porque éstas no ofrecen las mismas condiciones de usabilidad (e incluso de percepción de seguridad) que los computadores. En el caso de la integración de servicios financieros en redes sociales, como por ejemplo la posibilidad de realizar transferencias por un mensaje de chat o consultar el saldo de una cuenta con un mensaje directo a la cuenta de Twitter del Banco, se trata aún de una oferta muy limitada por cuanto no son muchos los Bancos que brindan esta opción a sus clientes.

Respecto de los medios empleados por los usuarios para hacer depósito de cheques y efectivo, un alto porcentaje indicó que usaba el canal presencial del banco (64,18%), privilegiándolo sobre otros medios como depósito electrónico directo (36,77%), cajeros automáticos (34,07%) y, en mucho menos porcentaje, los depósitos móviles (18,54%) y el correo. A este respecto, se puede inferir que resulta natural que frente a este tipo de operación los usuarios acudan más al canal presencial. Sin embargo, llama la atención que se empiecen a posicionar dentro de las opciones -aunque sea en menor porcentaje- otros medios con apoyo tecnológico como cajeros automáticos que acepten efectivo o como depósitos móviles (cuando por ejemplo se puede depositar el monto de un cheque mediante la captura de su imagen y el endoso usando la cámara del teléfono inteligente). Así se evidencia que los usuarios van asimilando más los servicios de Banca Móvil, aprovechando su facilidad, conveniencia, confiabilidad y seguridad.

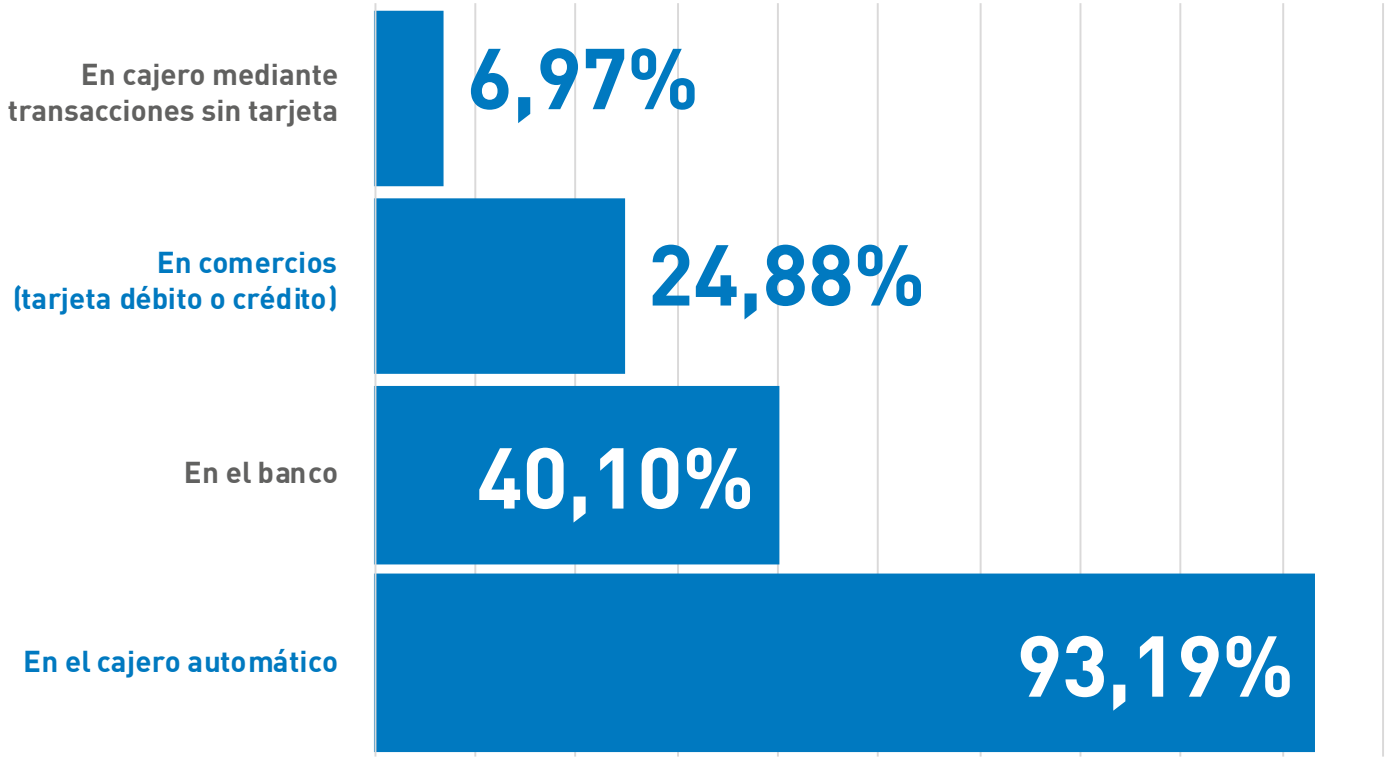
Gráfica 39. **Medios para hacer depósito de cheques / efectivo**



Nota: 631 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Respecto a los medios preferidos para obtener efectivo, los usuarios entrevistados en un porcentaje mayoritario (93,19%) manifestaron el uso prominente del cajero automático. Por su parte, un segmento inferior a la mitad de ellos (40,10%) indicó que prefería acudir presencialmente al banco, frente a un 24,88% que señaló que empleaba la tarjeta débito o crédito en establecimientos de comercio. Resulta también un avance el porcentaje de transacciones que se realizan mediante cajero sin que se disponga de la tarjeta (6,97%), dado que es una alternativa que cada vez más Bancos están ofreciendo a sus clientes y que empieza a ser aceptada por éstos.

Gráfica 40. Medios para obtener dinero en efectivo

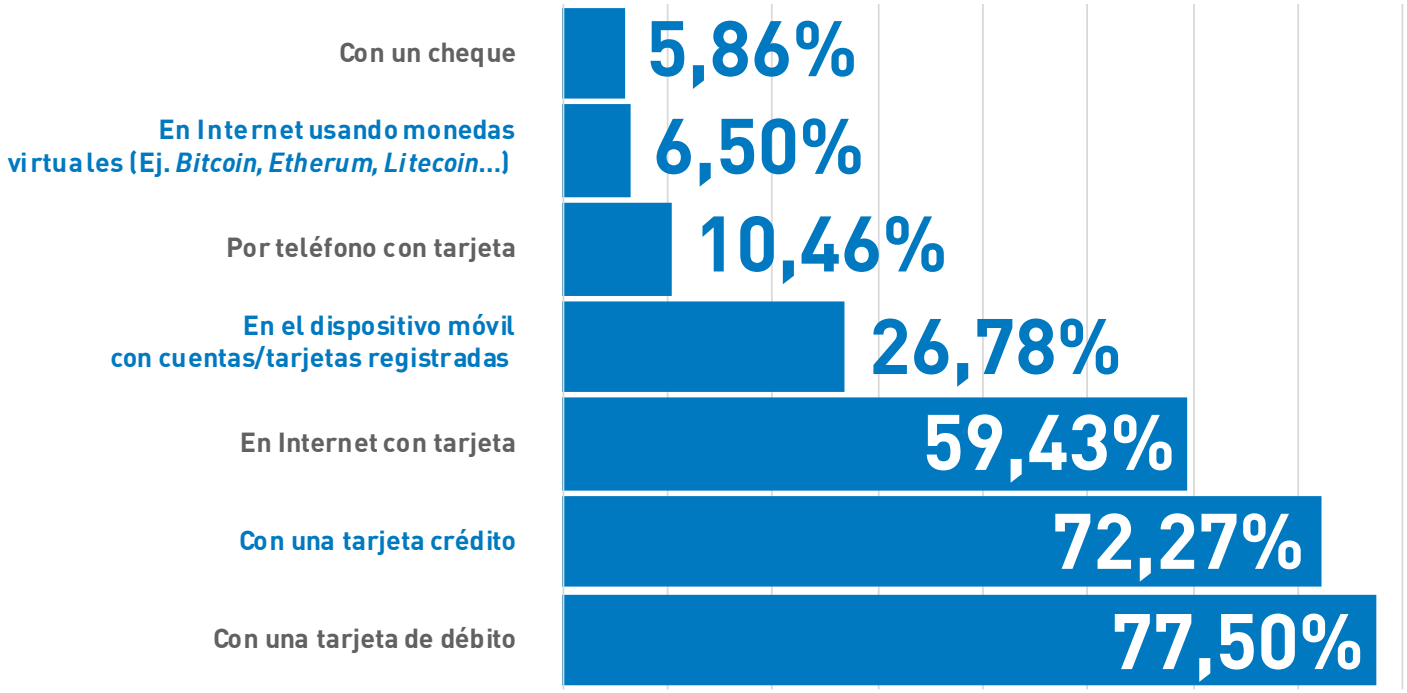


Nota: 631 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Respecto a los medios empleados por los usuarios para hacer compras, se evidencia la utilización significativa de las tarjetas débito y crédito (77,50% y 72,27%, respectivamente) tanto en canales presenciales como virtuales, así como el uso de tarjetas en compras por Internet (59,43%). En este tipo de operaciones resulta significativo que el uso de medios como el dispositivo móvil asociado con cuentas bancarias y tarjetas (26,78%) sobrepase ya su utilización respecto de otros canales tradicionales, como el de compras telefónicas con tarjeta (10,46%) y cheque (5,86%).

Otro aspecto llamativo en este estudio lo presenta un porcentaje nada despreciable del uso de monedas virtuales (6,50%) como medio para la realización de compras en Internet, el cual supera en porcentaje el uso del cheque como medio para compras (5,86%).

Gráfica 41. Medios para hacer compras

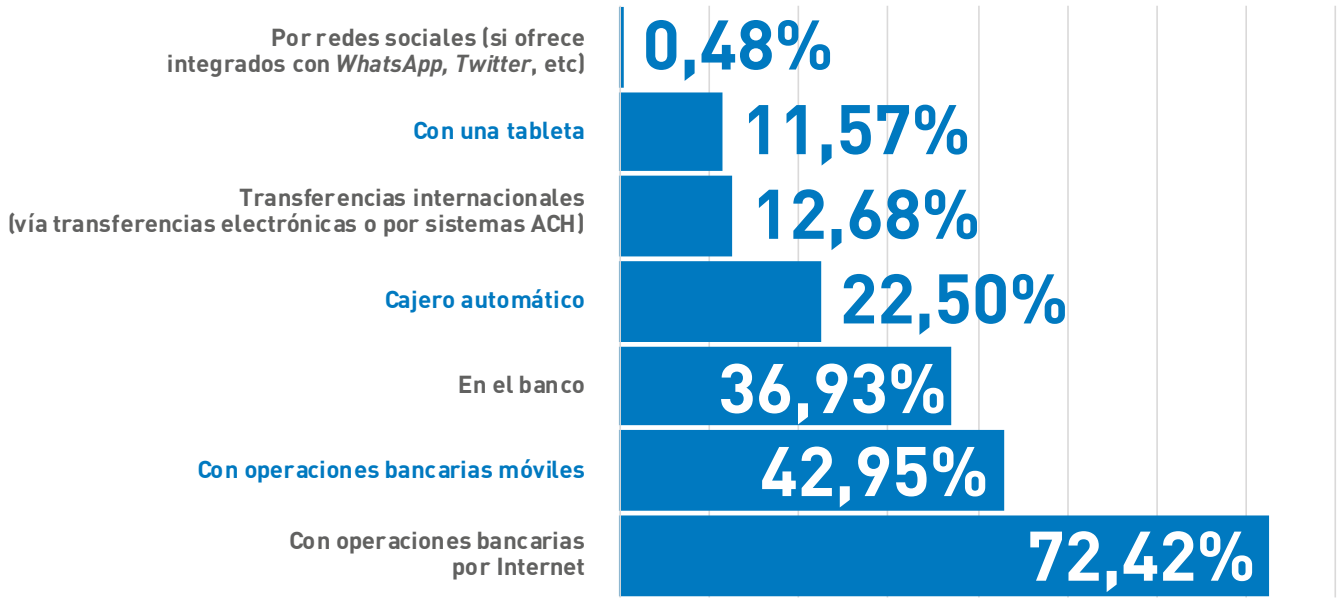


Nota: 631 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Respecto a los medios empleados para efectuar transferencias, los usuarios mayoritariamente prefieren realizar estas operaciones bancarias por Internet (72,42%), frente a un 42,95% que las realizan mediante operaciones bancarias móviles, un 36,93% que las efectúan directamente en el banco, un 12,68% a través de transferencias internacionales, un 11,57% con tableta y apenas un 0,48% en servicios integrados en redes sociales. En este tipo de operaciones, nuevamente se evidencia la preferencia por aquellas asociadas a medios digitales, reflejando una cada vez mayor asimilación entre los usuarios de este tipo de canales.

En particular, resulta muy importante que el porcentaje que representa el uso de banca móvil ya supere a la parte que prefiere realizar las transferencias directamente en las oficinas del Banco. Este resultado corrobora los obtenidos de otras fuentes, como es el caso de la *"Encuesta para consumidores de banca digital de PwC en 2018: los usuarios de teléfonos móviles establecen la agenda"*. En este informe se recuerda que en su encuesta de 2017 se apreciaba el auge de los consumidores "omnidigitales", es decir, aquellos que prefieren interactuar digitalmente con su banco sin preferencia por usar una computadora portátil, una tableta o un teléfono inteligente, pero que en la edición de 2018, los resultados destacan que se está formando una preferencia por el teléfono inteligente.

Gráfica 42. Medios para transferir fondos

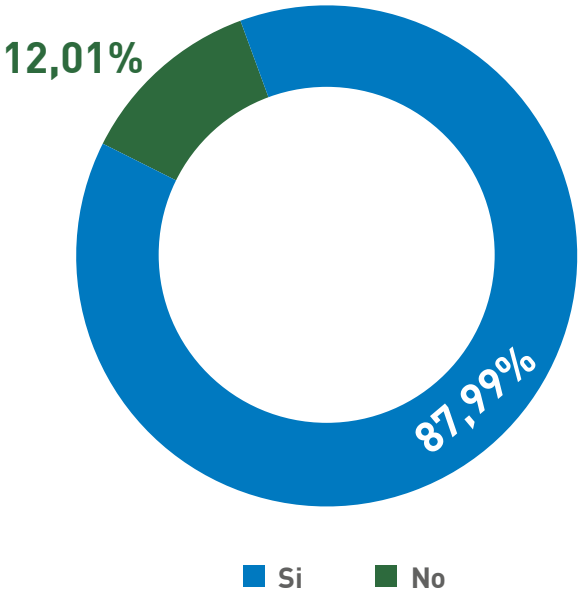


Nota: 631 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Ahora, a modo de pregunta general para valorar la apropiación de los medios digitales, se consultó si los usuarios utilizaban medios digitales para realizar sus transacciones, obteniendo como respuesta que un alto porcentaje (87,99%) efectivamente los utiliza para sus operaciones bancarias, frente a un 12,01% que indicó no usarlos. Con el resultado obtenido se evidencia que el usuario de la banca latinoamericana y del Caribe continúa evolucionando hacia un consumidor de canales virtuales para sus transacciones.

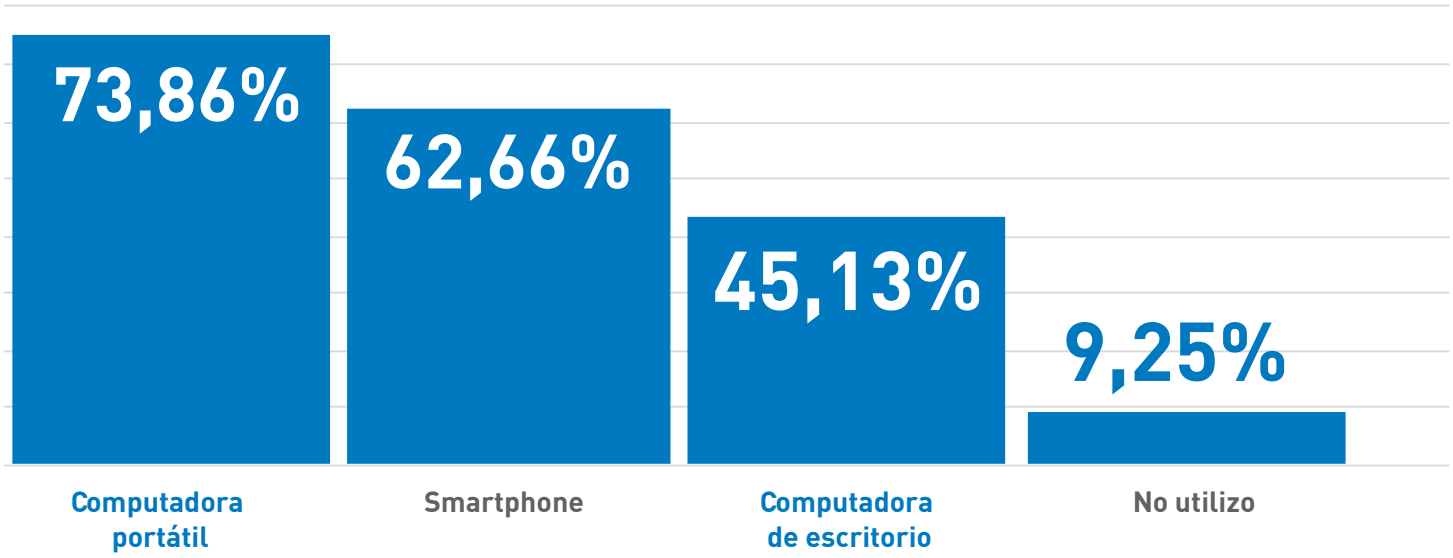
Gráfica 43. Porcentaje de usuarios que utilizan medios digitales para sus transacciones bancarias



Nota: 616 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Finalmente, respecto del uso de medios digitales para las transacciones bancarias, la computadora portátil es la que resulta con mayor preferencia de uso (73,86%), seguido por el smartphone (62,66%) y la computadora de escritorio (45,13%); en contraste con un 9,25% que manifestó no emplear ningún medio digital. Pese a que el computador portátil sigue siendo el medio de mayor uso, es importante resaltar la relevancia que han ganado los smartphones en este resultado, encontrándose ya muy cerca del primer lugar de preferencia, pues el móvil inteligente parece observar una tendencia de llegar a posicionarse como el principal dispositivo a través del cual los usuarios entran en Internet y acceden a múltiples servicios. Este resultado demuestra una dinámica de inclusión y de efectos de la revolución digital que se está viviendo en la región, en la cual el acceso a la conectividad resulta ser una condición y su masificación uno de los derroteros de sus países, aspectos impulsados tanto por las agendas de sociedad de la información de Latinoamérica y el Caribe (eLAC) como por las agendas digitales nacionales.

Gráfica 44. **Medios digitales más usados para realizar transacciones bancarias**

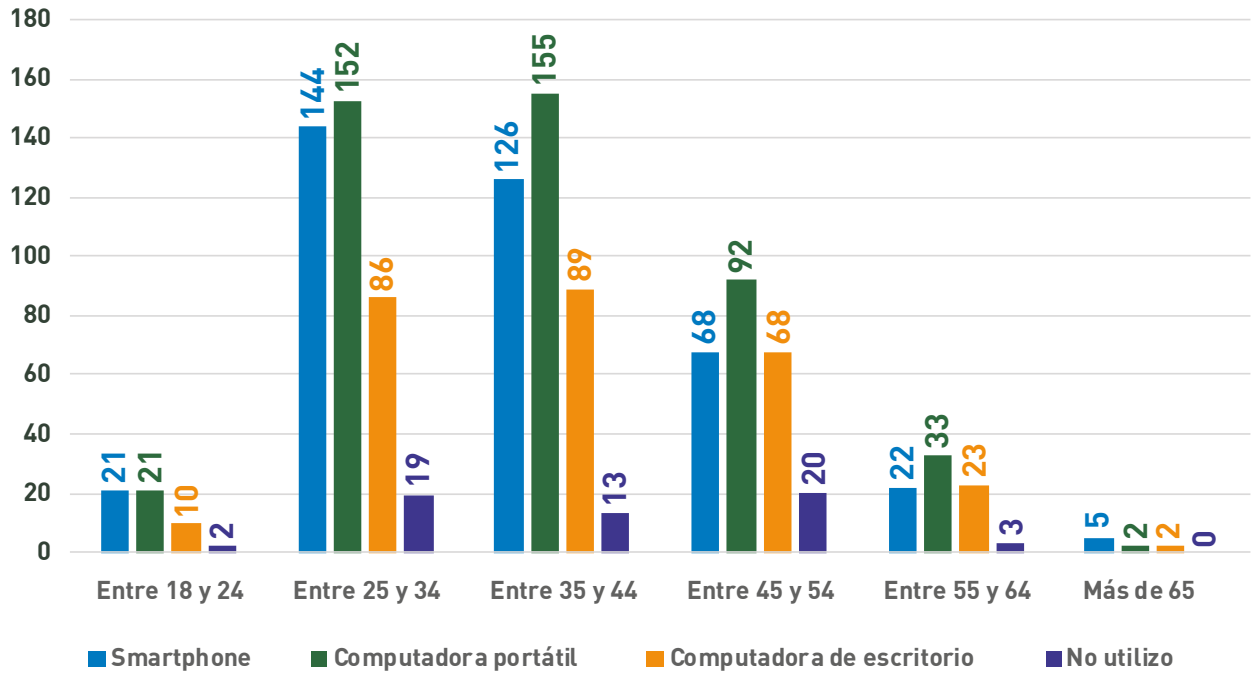


Nota: 616 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Con los datos obtenidos, se lograron analizar los medios digitales más usados para hacer transacciones bancarias y sus preferencias por rango de edad. En este análisis se destaca que en el caso de los más jóvenes (entre 18 y 24 años) el uso de los dispositivos móviles iguala al de computadoras portátiles (39% en ambos casos), y en el siguiente rango (entre 25 y 34 años) es muy cercano (36% móviles y 38% portátiles), lo cual ratifica la conclusión de la "*Encuesta para consumidores de banca digital de PwC en 2018: Los usuarios de teléfonos móviles establecen la agenda*" de *PricewaterhouseCoopers* (PwC, 2018), en el sentido de reflejar la creciente inclinación de los usuarios a usar este tipo de dispositivos, algo impulsado por los grupos poblacionales de menor edad. Otro aspecto que se observa es que la mayor resistencia o no utilización de los medios digitales para realizar transacciones se da en el rango entre 45 y 54 años, alcanzando un 8,06% (no se tiene en cuenta para esta conclusión el correspondiente a más de 65 años, como quiera que la muestra resulta muy limitada para este rango).

Gráfica 45. Medios digitales más usados para realizar transacciones bancarias



Nota: 616 registros

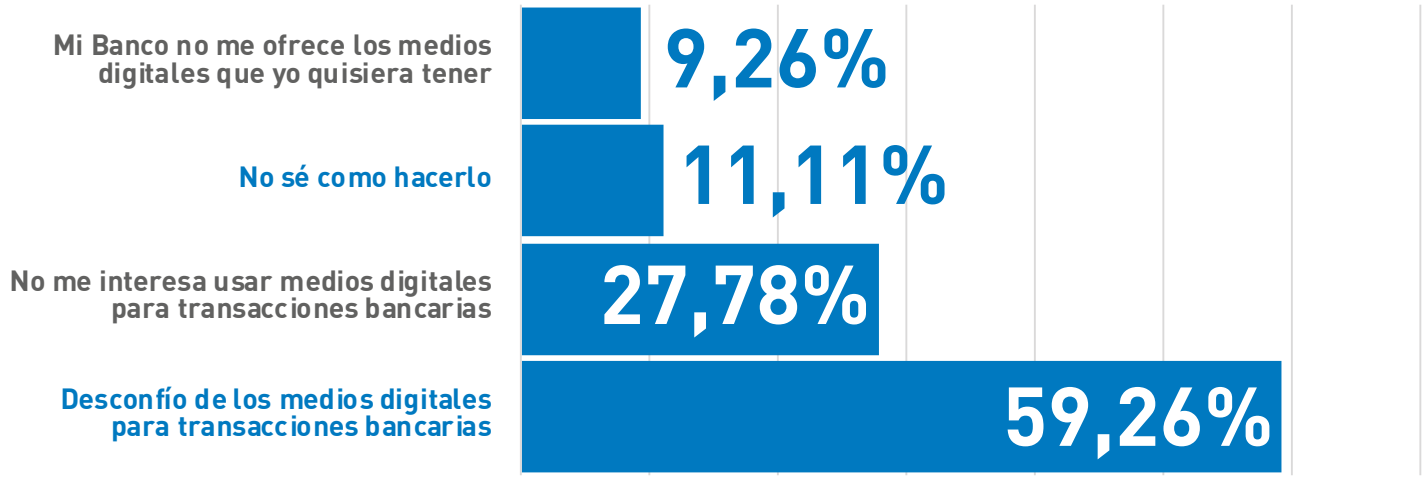
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Ahora bien, respecto al segmento de usuarios entrevistados que dijeron no utilizar medios digitales para realizar transacciones bancarias, se profundizó con el objeto de conocer las razones para no usarlos, observándose principalmente una percepción de desconfianza en los mismos (59,26%), 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%). Este resultado deja claro que el primer paso para incentivar a los usuarios en el uso de los medios digitales es, además de mostrar las bondades de estos canales, generar confianza y seguridad en los mismos.

La percepción de desconfianza de aquellos usuarios que no utilizan medios digitales para realizar transacciones bancarias se incrementa gracias a que existe más divulgación de los incidentes que han afectado a múltiples organizaciones y usuarios del entorno digital, especialmente en aspectos relacionados con las pérdidas de datos personales, la suplantación de identidad y las vulneraciones que han experimentado entidades financieras. Esto se puede ratificar en referentes externos, como es el caso del reciente estudio de *The Financial Brand* (The Financial Brand, 2018), cuyos resultados establecen que el 81% de los usuarios de servicios de banca en línea y banca móvil encuestados se encuentran preocupados por robos de datos personales y suplantación de identidad y un 65% manifiesta su preocupación por las vulneraciones de datos a entidades financieras.

De otra parte, la falta de interés en el uso de medios digitales obtuvo un resultado que no se puede ignorar y que denota que aún existen usuarios que no aprecian (o posiblemente desconocen) los beneficios que pueden obtener de los servicios ofrecidos por estos medios. Beneficios típicos tales como los ahorros en tiempo y desplazamientos, se suman a características propias de los aportes que ofrecen soluciones disruptivas como las que se asocian a *FinTech*, tales como la personalización de servicios, opciones de crédito en minutos, crowfunding, etc.

Gráfica 46. **Razones expuestas por aquellos que no utilizan medios digitales para realizar transacciones bancarias**



Nota: 54 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

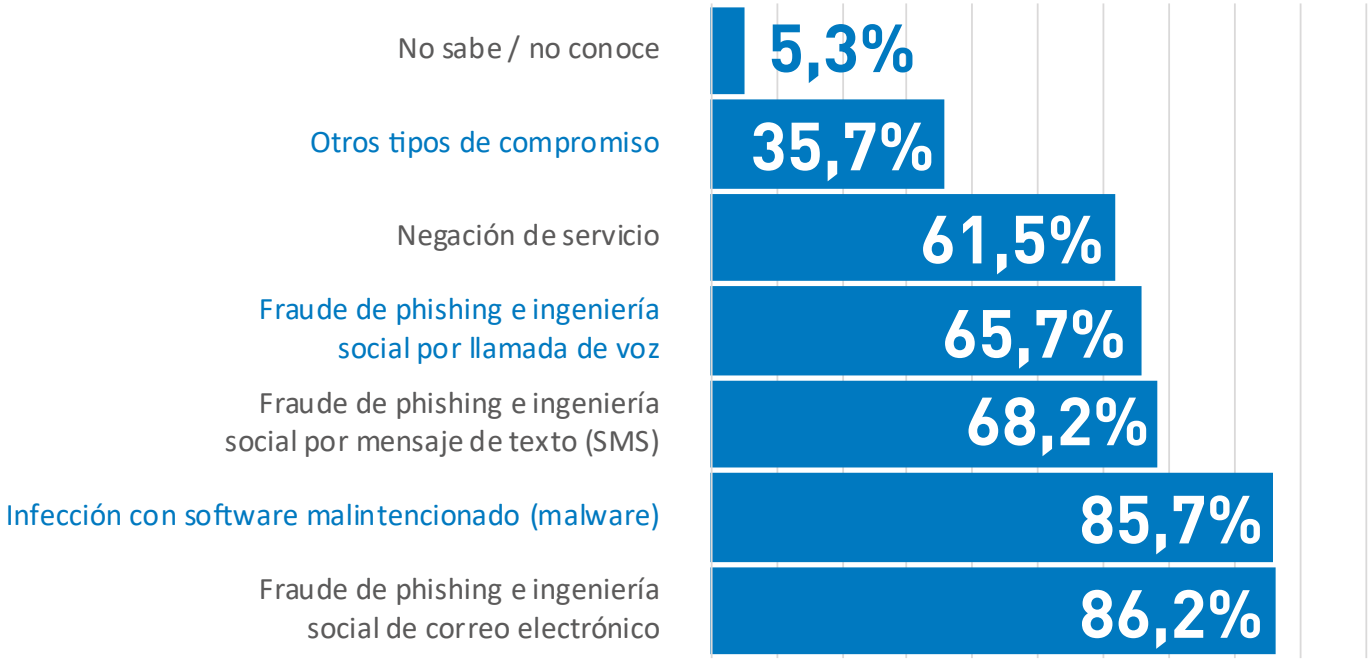
5.2 Cultura de Seguridad Digital

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 Bancos que completaron la encuesta, 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.

En respuesta a la pregunta sobre el tipo de incidentes digitales sobre los cuales los usuarios creían tener conocimiento, resulta evidente que el fraude de phishing e ingeniería social de correo electrónico, junto con la infección con software, resultan ser los más indicados por los usuarios (86,2% y 85,7% respectivamente). Por su parte, el fraude de phishing e ingeniería social por mensaje de texto ocupa un tercer lugar -no menos importante- (con el 68,2%), seguido por el fraude de phishing e ingeniería social por llamada de voz (65,7%), la negación del servicio (61,5%) y otros tipos de compromiso (35.66%).

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 usuarios entendían sobre este tipo de conceptos.

Gráfica 47. **Incidentes digitales sobre los que los usuarios creen tener conocimiento**

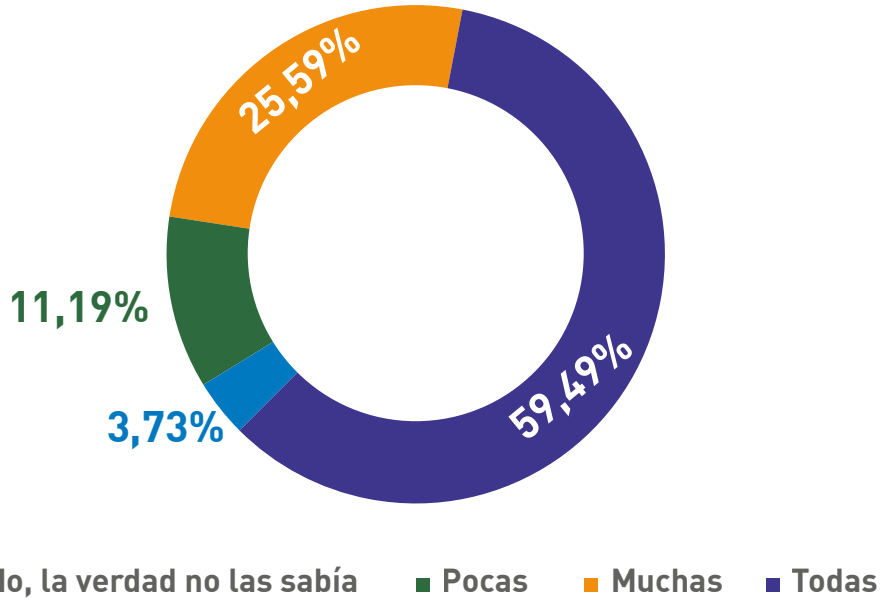


Nota: 603 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Después de que los encuestados manifestaran 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 59,49% manifestó tener conocimiento sobre todos los tipos de incidentes, mientras que un 25,59% contestó que conocía muchos de los tipos de incidentes, frente a otros usuarios que expresaron que conocían pocos de estos (11,19%), en contraste con quienes aseguraron ignorar el tema (un 3,73%). Así las cosas, según las respuestas obtenidas, un 85,08% de los usuarios contestaron que conocían muchas o todas las definiciones referidas a distintos tipos de incidentes cibernéticos.

Gráfica 48. **Nivel de conocimiento frente a las definiciones reales de los distintos tipos de incidentes cibernéticos**

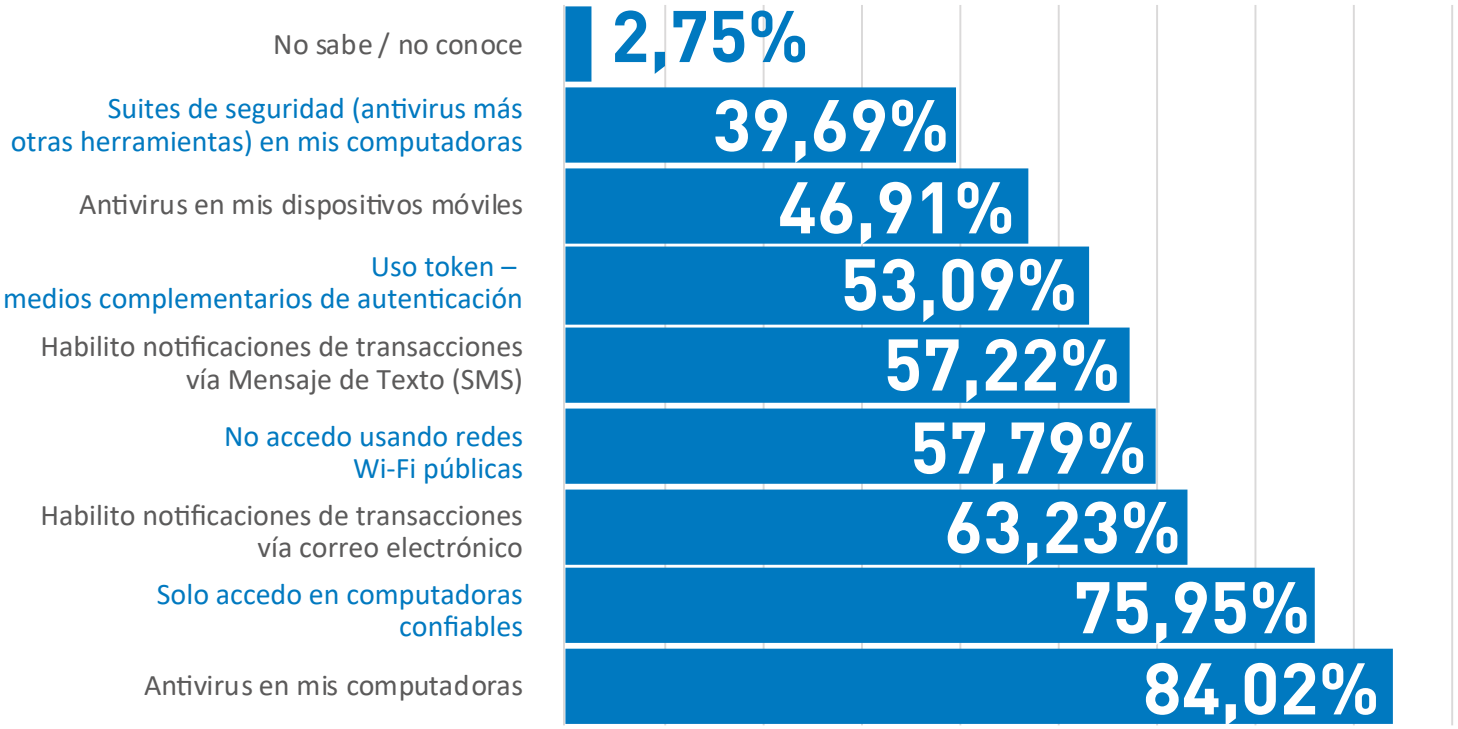


Nota: 590 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Una vez se validó el conocimiento sobre el tipo de incidentes cibernéticos, se indagó a los encuestados sobre las medidas de seguridad que hubieren implementado para prevenir incidentes digitales, a lo cual un alto porcentaje (84,2%) manifestó que usaban antivirus en sus computadores, 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%). Si bien los porcentajes para medidas como el uso de antivirus y de computadores confiables son altos, también es cierto que los resultados exponen el uso de dispositivos -en algún porcentaje- sin medidas de seguridad, lo cual deriva en altos niveles de exposición a ataques cibernéticos.

Gráfica 49. Medidas de seguridad más usadas por usuarios para prevenir incidentes digitales



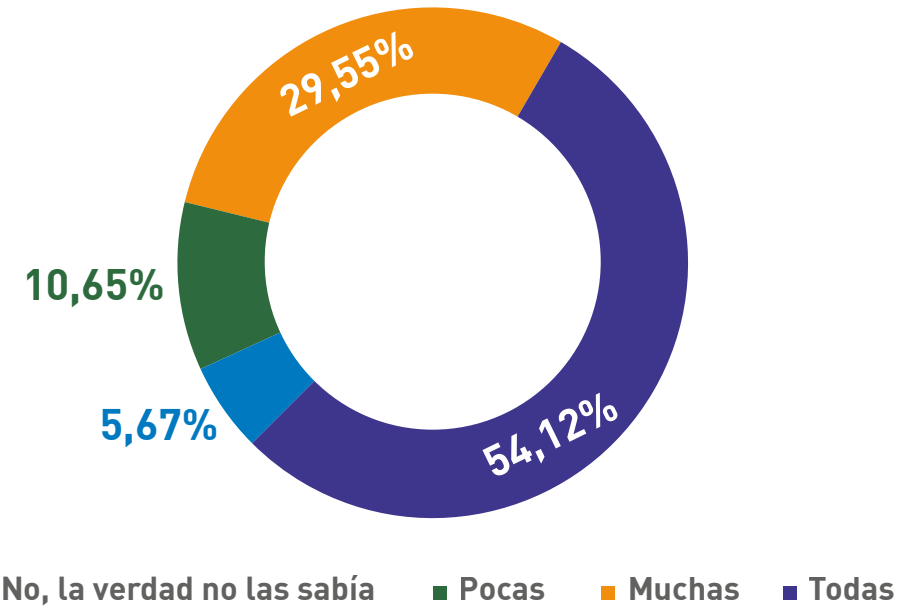
Nota: 582 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

De manera similar a la validación de conocimientos sobre los incidentes cibernéticos, cuando se consultó a los usuarios entrevistados sobre si sabían acerca de las medidas mencionadas en el punto anterior, la mayoría de ellos indicó que conocía todas las medidas (54,12%) y un segmento del 29,55% manifestó conocer muchas de ellas, en contraste con unos porcentajes inferiores que adujeron conocer pocas o ningunas de ellas (10,65% y 5,67% respectivamente). De manera consistente con las conclusiones expresadas anteriormente, se valora la existencia de conocimientos relacionados con prácticas de seguridad por parte de los usuarios entrevistados, dado que un 83,67% indicó que conocía muchas o todas las medidas.

Ahora bien, en cuanto a la efectividad de estas medidas o su nivel de aplicación, aunque no se incluyó una pregunta específica al respecto, es claro que el hecho de que se conozcan tales medidas no significa necesariamente que las mismas sean utilizadas por el usuario, dado que la mayoría de las veces se encuentran desde dificultades para su implementación (ej. Inversión que debe hacer el usuario para adquirir soluciones de protección) hasta disculpas justificadas en situaciones coyunturales (ej. Acceder al servicio de banca en línea o banca móvil a través de una red gratuita insegura por encontrarse de vacaciones), por lo que aún se requieren esfuerzos tendientes a elevar mucho más el uso consciente de este tipo de medidas.

Gráfica 50. Nivel de conocimiento frente a medidas de seguridad expuestas

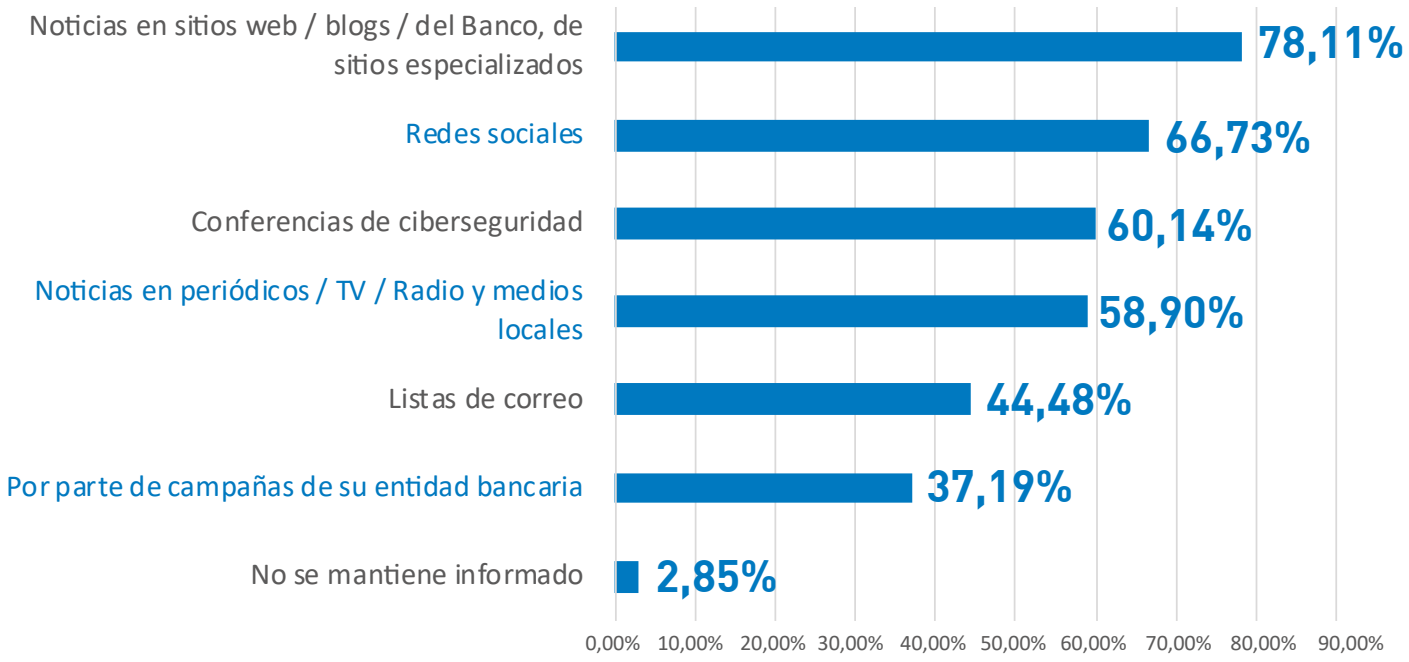


Nota: 582 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Uno de los aspectos que debería ganar más relevancia para los usuarios, ya que dependen cada vez más del entorno digital, tiene que ver con mantenerse informado sobre las nuevas formas de ataques y amenazas de seguridad. Al respecto, al consultar a los usuarios sobre las fuentes a las que más acuden para enterarse de estos aspectos, los entrevistados indican 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%).

Como se desprende de los resultados, pocos 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. No obstante, es cierto también que cada vez existe más información disponible sobre las nuevas formas de ataques y amenazas de seguridad, aunque las mismas no parecen estar siendo aún muy difundidas en los medios de comunicación tradicionales como los periódicos, la TV y radios locales, ya que este tipo de medios quedó en un cuarto (4to) lugar entre los que emplean los usuarios como fuente.

Gráfica 51. Fuentes más comunes mediante las que los usuarios se mantienen informados de las nuevas formas de ataques y amenazas de seguridad



Nota: 562 registros

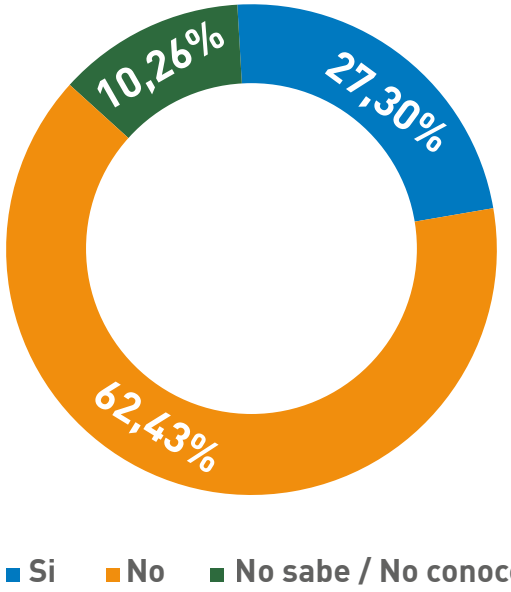
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

5.3 Impacto de los incidentes de seguridad digital

En este componente del estudio, se realizaron preguntas orientadas a establecer el impacto sufrido por los usuarios de Bancos que completaron la encuesta, 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 usuarios encuestados sobre si se habían visto comprometidos respecto a la confidencialidad, integridad o disponibilidad de su información o sus recursos financieros en su Banco, estos respondieron en su mayoría NO haber visto comprometida la confidencialidad, integridad o disponibilidad de su información o sus recursos financieros en su banco (62,45%), frente a un menor segmento que afirmó lo contrario (27,30%) y a otra fracción que declaró no saber y/o no conocer del asunto (10,26%). El resultado muestra que aproximadamente 1 de cada 4 usuarios del sector bancario han tenido algún grado de compromiso en cuanto a su información o sus recursos por incidentes cibernéticos, lo cual es digno de resaltar.

Gráfica 52. **Porcentaje de usuarios que han visto comprometida la confidencialidad, integridad o disponibilidad de su información o sus recursos financieros en su Banco**



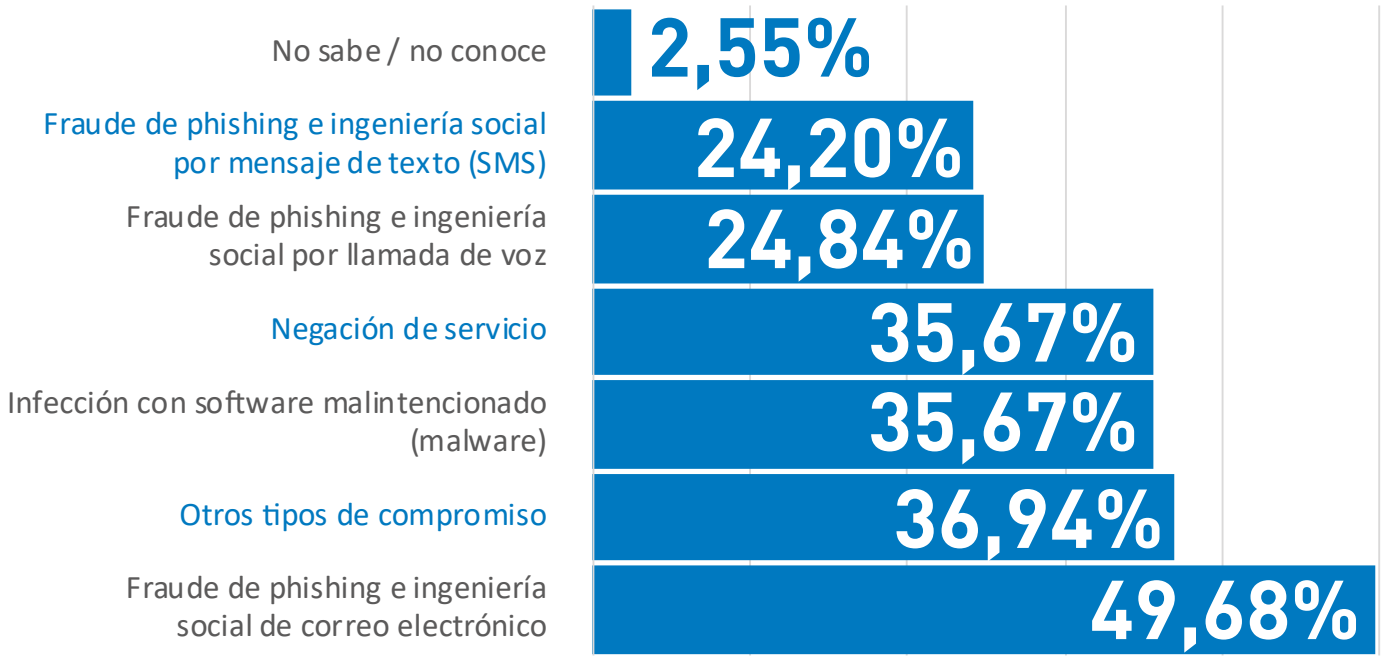
Nota: 575 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Frente a la pregunta relacionada con los tipos de incidentes digitales experimentados, la mayor parte de ellos revelaron el fraude de phishing e ingeniería social de correo electrónico (49,68%) como el más usual, incluyendo en menor porcentaje otros tipos de compromiso (36,94%), la infección con software malintencionado (35,67%), la negación del servicio (35,67%), el fraude de phishing e ingeniería social por llamada de voz (24,84%) y el fraude de phishing e ingeniería social por mensaje de texto (24,02%).

Es evidente que los ataques que utilizan como vector un correo electrónico con el objetivo de obtener la información de acceso (credenciales) de los usuarios, siguen siendo los que más comúnmente les afectan. Esto coincide con lo indicado en un análisis del panorama de las amenazas financieras publicado por los expertos de *Kaspersky Lab* (Kaspersky Lab, 2017), que además concluye que un alto porcentaje de los ataques de phishing (47,48%) tienen por objeto el hurto de dinero a los usuarios atacados.

Gráfica 53. Tipo de incidentes digitales experimentados por usuarios bancarios

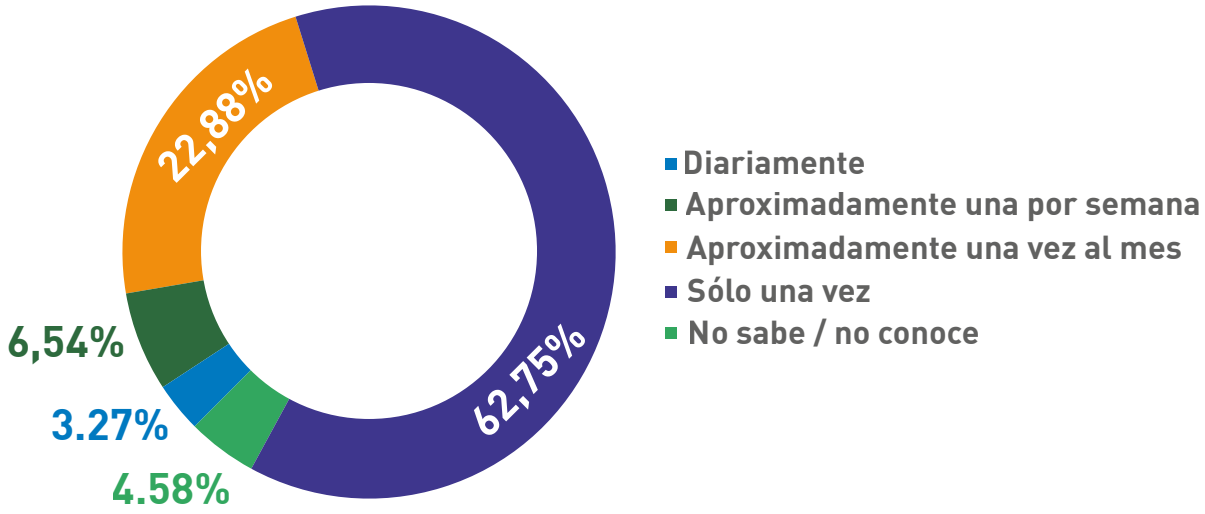


Nota: 157 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Con respecto a la pregunta sobre la frecuencia con que habían sido afectados por los incidentes cibernéticos, los usuarios manifiestan en su mayoría (62,75%) que una sola vez sufrieron incidentes de esta naturaleza. Contrasta este valor con quienes indicaron padecerlos una vez al mes (22,88%), una vez a la semana (6,54%) y diariamente (3,27%). En este punto, es importante resaltar que los usuarios no necesariamente son conscientes de estar siendo afectados por incidentes cibernéticos, 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 programarse con el banco.

Gráfica 54. Frecuencia de ocurrencia de incidentes cibernéticos sufridos por los usuarios bancarios



Nota: 153 registros

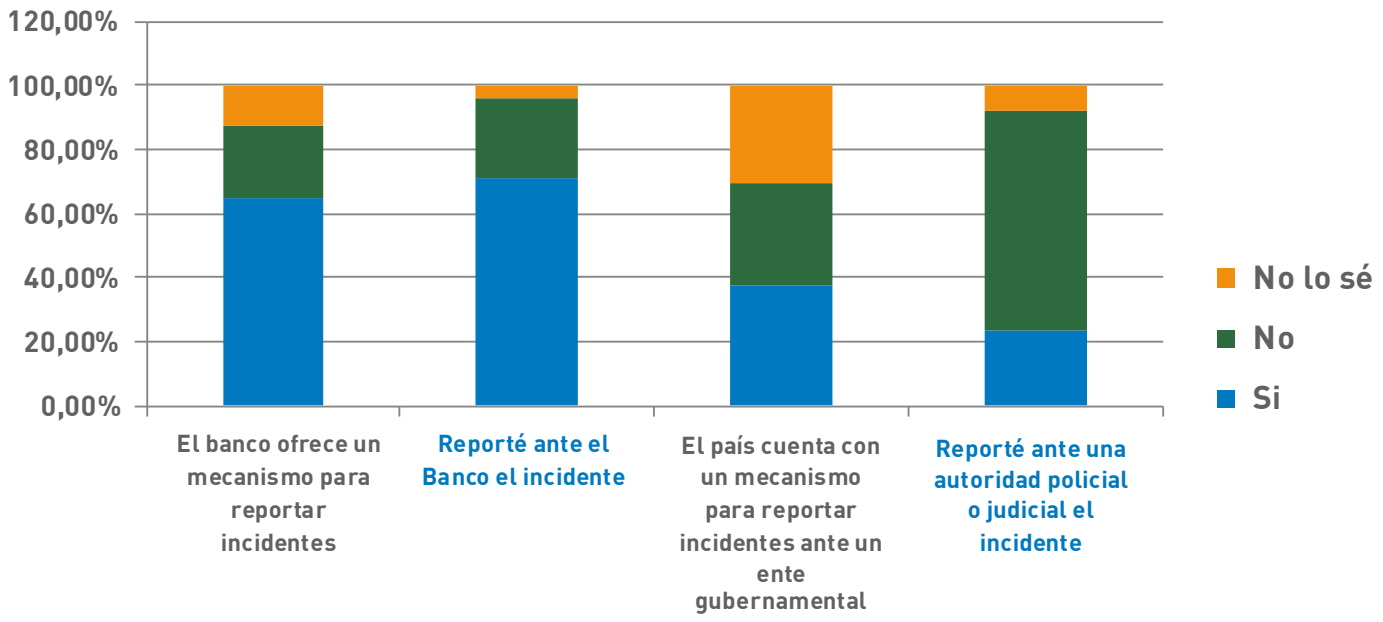
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Frente a la pregunta relacionada con mecanismos y acciones de reporte cuando ocurren incidentes cibernéticos, los usuarios entrevistados indicaron en su mayoría que la institución bancaria sí ofrece un mecanismo para reportar incidentes (64,71%) y que en efecto han reportado el incidente ante su banco (71,24%).

Por su parte, se resalta la manifestación de que, conforme a las respuestas, solo el 37,25% afirma que en su país existe 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.

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% han elevado a estas instancias los incidentes que les han afectado. Este dato exige análisis por cuanto podría denotar dificultades en cuanto a los canales de denuncia o bien, baja efectividad en las investigaciones derivadas de los casos denunciados.

Gráfica 55. Mecanismos y acciones de reporte frente a la ocurrencia de incidentes cibernéticos sufridos por usuarios bancarios



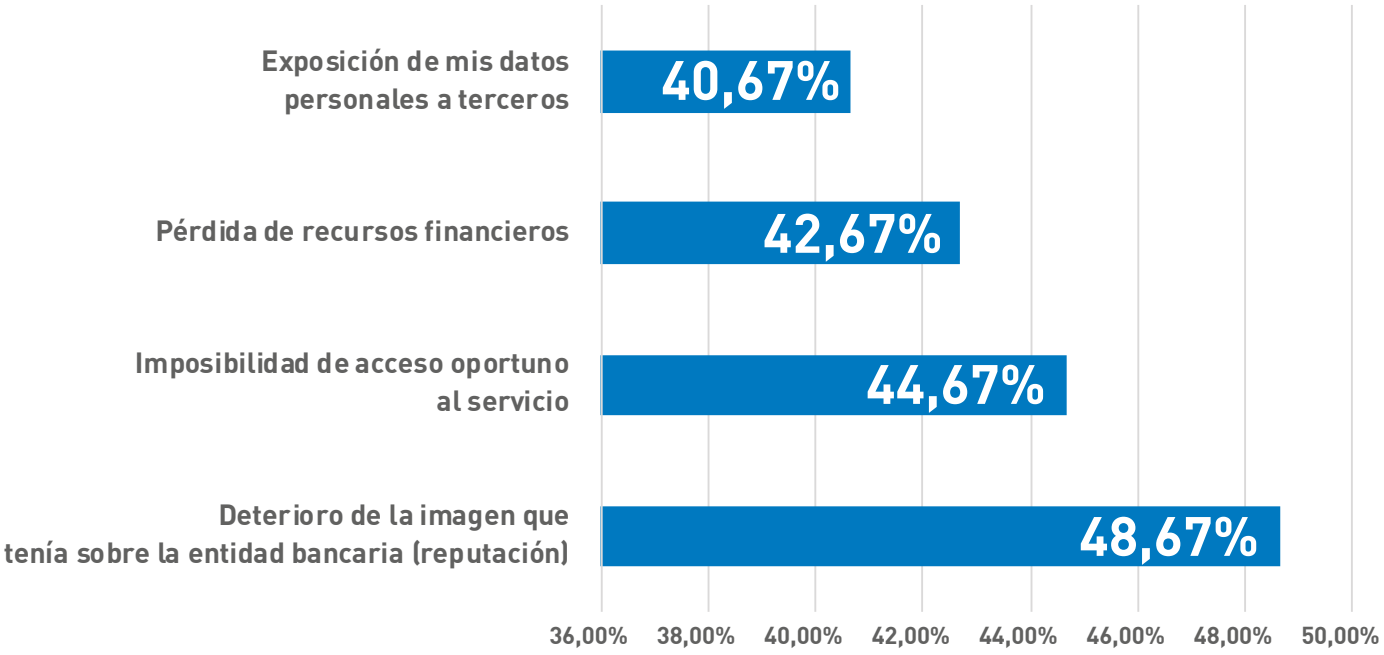
Nota: 153 registros

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Profundizando en la valoración del impacto sufrido por quienes manifestaron haber sido objeto de algún tipo de incidente, se obtuvo que el aspecto más afectado negativamente fue la imagen que tenían sobre la entidad bancaria (48,67%), acompañado de la imposibilidad de acceso oportuno al servicio (44,67%), la pérdida de recursos financieros (42,67%) y la exposición de sus datos a terceros (40,67%).

Teniendo en cuenta que esta, como muchas de las respuestas ofrecidas por los usuarios, permitía múltiples respuestas, y que en particular esta fue solo respondida por quienes fueron afectados por algún tipo de incidente cibernético, se aprecia que existe una distribución muy cercana entre los porcentajes que denotan cada consecuencia, lo cual apenas permite señalar que el mayor impacto para el usuario tiene que ver con la afectación de la imagen o reputación del Banco.

Gráfica 56. Impacto generado a usuarios bancarios por incidentes cibernéticos



Nota: 150 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

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 institución u organización por razones como la desconfianza.

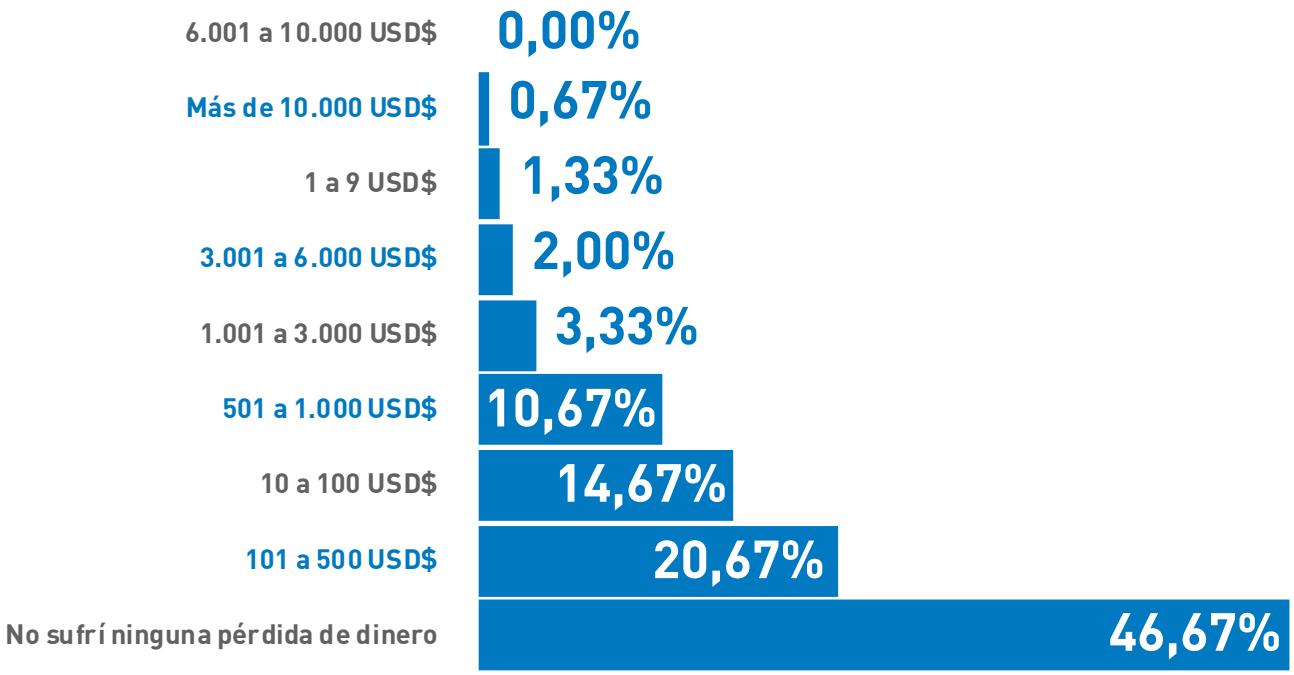
En este sentido, es necesario resaltar las conclusiones obtenidas por *Ponemon Institute e IBM* (Ponemon Institute e IBM, 2018), en cuanto al impacto financiero de una pérdida de reputación y confianza de marca después de un incidente de seguridad cibernética, el cual puede ser significativo en todas las

industrias. Este reporte indica que el sector financiero es el segundo más vulnerable a la pérdida de clientes (tan solo superado por el sector salud) y establece que el costo frente a violaciones de datos es de $4,20 millones de dólares para compañías en Estados Unidos, mientras alcanza $0,47 millones de dólares para el único país de la región incluido en el estudio, Brasil.

Retornando a la afectación desde la perspectiva de clientes, se pidió a los usuarios que afirmaron haber sido víctimas de un incidente que indicaran en qué rango estaría la afectación que sufrieron, encontrando que un 47% afirmó no haber perdido dinero, frente a un 21% que manifestó haber perdido entre 101 a 500 USD$, a un 15% que expresó haber perdido entre 10 y 100 USD$ y a un 11% que registró haber perdido entre 500 y 1000 USD$, con resultados de inferior relevancia para otros rangos de pérdida de dinero.

En el análisis del panorama de las amenazas financieras publicado por los expertos de *Kaspersky Lab* (Kaspersky Lab, 2017), se había ya resaltado que un 47,48% de los ataques de phishing tienen por objeto el hurto de dinero a los usuarios atacados. Las cifras obtenidas en este estudio son muy cercanas a lo indicado en el efectuado por *Kaspersky*, dado que precisamente de la respuesta ofrecida al tipo de incidente sufrido el 49,68% indicó que había sido objeto de Phishing e ingeniería social por correo electrónico y, además, si se suman los porcentajes que en esta respuesta indicaron que habían perdido algún monto de dinero, se obtiene como resultado que el 53,34% de los afectados por un ataque, efectivamente sufrieron pérdidas.

Gráfica 57. Rango de afectación (en USD) respecto de incidentes cibernéticos que afectaron a usuarios

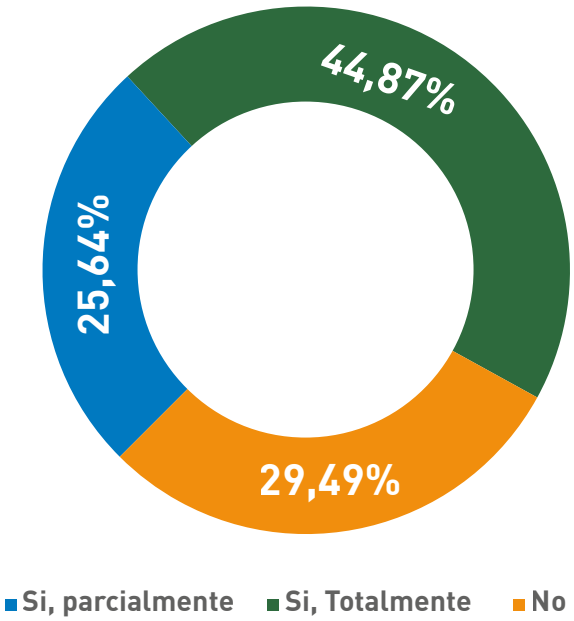


Nota: 150 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Una vez abordado el grado de afectación, se consultó a quienes afirmaron haber sido víctimas de un ataque si habían sido compensados o reparados respecto de incidentes cibernéticos. Al respecto, el 44,87% de los usuarios encuestados manifestaron haber sido reparados o compensados totalmente, frente a un 25,64% que indicó haberlo sido parcialmente y un 29,49% que expresó no haber recibido ningún tipo de indemnización.

En este sentido resulta muy relevante valorar que aquellos que no recibieron una compensación o reparación respecto del incidente del que fueron víctima, terminan desarrollando un alto grado de frustración y demás consecuencias previsibles como, por ejemplo, el incremento de la desconfianza en el uso de medios digitales para la realización de sus operaciones bancarias.

Gráfica 58. Porcentaje de usuarios bancarios que recibieron compensación o reparación respecto de incidentes cibernéticos

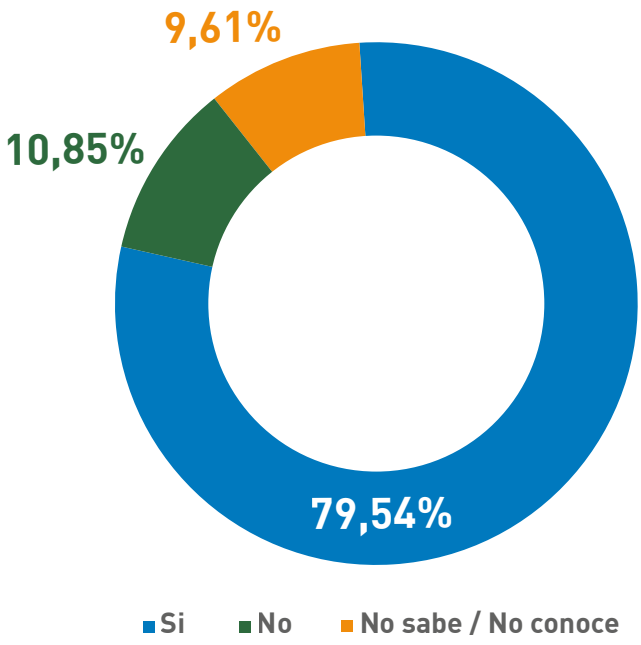


Nota: 78 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Posteriormente, se preguntó a los usuarios encuestados si consideraban que los riesgos de que ocurran incidentes cibernéticos han empeorado en el último año, encontrando una percepción mayoritaria del 79,54% en el sentido de 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.

Lo anterior, de alguna manera, refleja que la dinámica de la digitalización y sus riesgos inherentes hace que los medios de comunicación tradicionales, así como las redes sociales, vayan dando cada vez más visibilidad a situaciones relacionadas con incidentes de seguridad digital, hechos que los usuarios empiezan a ver con más frecuencia y de esta manera derivan en la percepción de que los riesgos han empeorado.

Gráfica 59. **Porcentaje de usuarios que considera que los riesgos de ocurrencia de incidentes cibernéticos han empeorado en el último año**

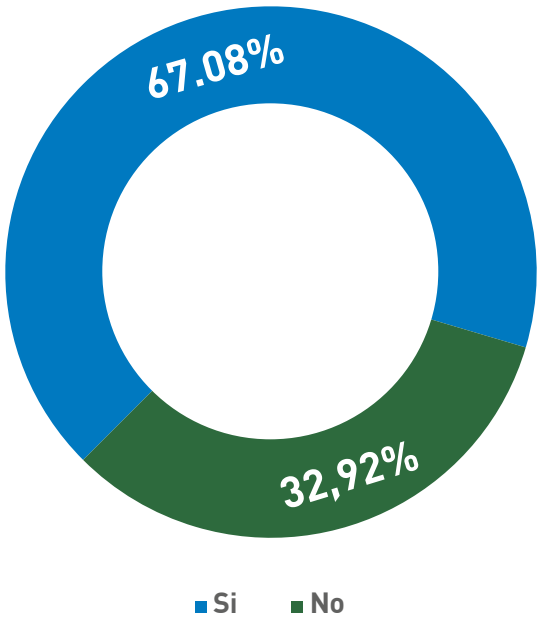


Nota: 562 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Finalmente, se consultó a los usuarios si consideraban que los riesgos de que ocurran incidentes cibernéticos afectaban su decisión de usar medios digitales en el sector financiero. La encuesta revela que la mayoría de los usuarios encuestados, un 67,08%, considera que la existencia de riesgos derivados de incidentes cibernéticos sí afecta su decisión de usar o no los medios digitales en este sector, frente a solo un 32,92% que afirma lo contrario.

Esta respuesta lleva a la reflexión sobre la importancia de fortalecer la gestión de riesgos de seguridad digital, de manera integral, de forma que los usuarios y empresas encuentren un entorno digital que genere confianza para todos.

Gráfica 60. Porcentaje de usuarios que considera que los riesgos de ocurrencia de incidentes cibernéticos afectan su decisión de usar medios digitales en el sector financiero



Nota: 562 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

5.4 Análisis econométrico de los resultados

De igual manera que en el caso de las entidades bancarias, se estimaron modelos econométricos para la base de datos que contiene información a nivel de individuos como unidad de análisis. Se realizaron estimaciones econométricas que tienen por objetivo encontrar los factores que determinan si un individuo ha sido víctima de incidentes a la ciberseguridad, con base en la pregunta *"¿Ha experimentado algún incidente o situación que ha comprometido la confidencialidad, integridad o disponibilidad de su información o sus recursos financieros en su Banco?"*

Para este caso, se incluyeron como variables dependientes un conjunto de indicadores que trataron de capturar las características propias del individuo, y se incorporaron variables asociadas a si revisa las transacciones recientes y saldos disponibles, a los distintos medios de depósito de cheques / efectivo, la manera como se obtiene dinero en efectivo, la forma de hacer compras, las diferentes maneras de transferir fondos, si utiliza algún medio digital para sus transacciones bancarias, qué medidas de seguridad ha implementado para prevenir incidentes digitales y en caso de que haya sido víctima de un incidente como los enunciados anteriormente cuál fue el tipo de incidente sufrido y cómo se mantiene informado de las nuevas formas de ataques y amenazas de seguridad de la información.

Al igual que en el caso anterior, el modelo empleado en la estimación presentó variable dependiente discreta {0,1}, del tipo logit o probit, escogido de acuerdo con el mejor ajuste. Para este caso particular la variable dependiente (y) tomó el valor de 1 si el individuo encuestado ha *"experimentado algún incidente o situación que ha comprometido la confidencialidad, integridad o disponibilidad de su información o sus recursos financieros en su Banco"* y 0 de lo contrario. Como se mencionó en el párrafo anterior, se incluyeron variables independientes relacionadas con los tópicos mencionados con el fin de estimar la probabilidad de ocurrencia de incidentes de seguridad digital o de otra interpretación para encontrar los factores que determinan que un usuario sea víctima de este tipo de incidentes.

La descripción de las variables utilizadas y que potencialmente pueden hacer parte del modelo se muestra en la siguiente tabla:

Cuadro 19. Variables utilizadas en el modelo utilizado del tipo LOGIT -Usuarios

TIPO	VARIABLE	DESCRIPCIÓN
Características propias de los usuarios de la entidad bancaria	Genero	Femenino Masculino
Características propias de los usuarios de la entidad bancaria	Revisión de transacciones	Revisa las transacciones recientes y saldos disponibles: Registro de operaciones bancarias por Internet (Computadora portátil o de escritorio) • En cajeros automáticos • Por teléfono • En el banco • Usando aplicaciones bancarias móviles • Por tableta • Por redes sociales (si el banco ofrece este servicio integrado a redes sociales como *WhatsApp, Twitter*, etc.)
Características propias de los usuarios de la entidad bancaria	Realiza depósitos de cheques / efectivo	Hace depósito de cheques / efectivo: • Mediante un depósito electrónico directo • En cajeros automáticos • En el banco • Por correo • Mediante depósito móvil
Características propias de los usuarios de la entidad bancaria	Dinero en efectivo	Obtiene dinero en efectivo: • En el cajero automático • En el banco • En comercios, cuando usted hace una compra usando su tarjeta débito o crédito • En cajero mediante transacciones sin tarjeta
Características propias de los usuarios de la entidad bancaria	Compras realizadas	Hace compras: • Con un cheque • Con una tarjeta crédito • Con una tarjeta de débito • Por teléfono con tarjeta • En Internet con tarjeta • En Internet usando monedas virtuales (Ej. *Bitcoin, Etherum, Litecoin*...) • En el dispositivo móvil con cuentas/tarjetas registradas
Características propias de los usuarios de la entidad bancaria	Transferencias de fondos	Transfiere fondos: • Cajero automático • Con operaciones bancarias por Internet (Computadora portátil o de escritorio) • Con operaciones bancarias móviles • En el banco • "Transferencias internacionales (vía transferencias electrónicas o por sistemas ACH)" • Con una tableta • Por redes sociales (si el banco ofrece este servicio integrado a redes sociales como *WhatsApp, Twitter*, etc)

TIPO	VARIABLE	DESCRIPCIÓN
Características propias de los usuarios de la entidad bancaria	Transacciones digitales	¿Utiliza algún medio digital para sus transacciones bancarias? Escoja las opciones que más realiza. • Smartphone • Computadora portátil • Computadora de escritorio • No utilizo
Cultura de seguridad digital	Medidas de seguridad de prevención de incidentes	¿Qué medidas de seguridad ha implementado para prevenir incidentes digitales? (múltiples respuestas posibles) • Antivirus en mis computadoras • Suites de seguridad (antivirus más otras herramientas) en mis computadoras • Antivirus en mis dispositivos móviles • Solo accedo en computadoras confiables • No accedo usando redes Wi-Fi públicas • Uso token – medios complementarios de autenticación • Habilito notificaciones de transacciones vía correo electrónico • Habilito notificaciones de transacciones vía Mensaje de Texto (SMS) • No sabe / no conoce
Impacto de los incidentes de seguridad digital	Experiencia de incidentes que hayan afectado la confidencialidad, integridad o disponibilidad de información o sus recursos	¿Ha experimentado algún incidente o situación que ha comprometido la confidencialidad, integridad o disponibilidad de su información o sus recursos financieros en su Banco?
Impacto de los incidentes de seguridad digital	Tipo de incidentes digitales experimentados	¿Cuáles? (múltiples respuestas posibles) • Infección con software malintencionado (malware) • Fraude de phishing e ingeniería social de correo electrónico • Fraude de phishing e ingeniería social por mensaje de texto (SMS) • Fraude de phishing e ingeniería social por llamada de voz • Negación de servicio, he intentado acceder a servicios del Banco y no funcionan • Otros tipos de compromiso • No sabe / no conoce
	Reporte de incidentes	En caso de que haya sido víctima de un incidente como los enunciados anteriormente: • El banco ofrece un mecanismo para reportar incidentes • Reporté ante el Banco el incidente • El país cuenta con un mecanismo para reportar incidentes ante un ente gubernamental • Reporté ante una autoridad policial o judicial el incidente

TIPO	VARIABLE	DESCRIPCIÓN
	Conocimientos de formas de ataques	¿Cómo se mantiene informado de las nuevas formas de ataques y amenazas de seguridad de la información? (múltiples respuestas posibles) • Listas de correo • Conferencias de ciberseguridad • Noticias en sitios web / blogs / del Banco, de sitios especializados • Noticias en periódicos / TV / Radio y medios locales • Redes sociales • Por parte de campañas de su entidad bancaria • No se mantiene informado

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Respecto a los resultados de las estimaciones, se corrieron modelos del tipo Logit, teniendo como unidad de análisis los individuos que respondieron la encuesta. Se estimaron diferentes modelos incluyendo las variables independientes antes descritas. Se trabajó con información de 516 observaciones (Individuos). Luego de probar diferentes formas funcionales y variables independientes, se escoge el modelo con mejor ajuste –Logit–. En general el modelo presenta un buen ajuste global de acuerdo con el estadístico LR chi2(22)= 63.50, con una probabilidad cercana a 0.00. Lo anterior indica que el modelo encontrado representa en buena medida la variabilidad en la ocurrencia de eventos de ciberseguridad en los individuos.

Cuadro 20. Resultados de las estimaciones del modelo Logit, la variable dependiente (y) toma el valor de 1 si el individuo encuestado "ha experimentado algún incidente o situación que ha comprometido la confidencialidad, integridad o disponibilidad de su información o sus recursos financieros en su Banco" y 0 de lo contrario

Incidente	Coef.	Std. Err.	z	P>|z|	[95% Conf.	Interval]
Genero	-.2065386	.2456746	-0.84	0.401	-.688052	.2749747
Edad	.0108815	.0111275	0.98	0.328	-.0109279	.032691
operInternet	.3615521	.3521736	1.03	0.305	-.3286955	1.0518
operTel	.02484	.2381028	0.10	0.917	-.4418329	.4915128
operCajAut	.3450024	.2608198	1.32	0.186	-.166195	.8561998
operBanco	-.2408654	.2749635	-0.88	0.381	-.7797839	.2980531
operBancaMov	-.3607537	.2963595	1.22	0.223	-.9416076	.2201002
operTableta	-.1534206	.3541618	-0.43	0.665	-.8475649	.5407238
operRedSoc~l	-.772404	.8930911	-0.86	0.387	-2.52283	.9780224
depositoCE	.3649712	.2510195	1.45	0.146	-.1270179	.8569603
depositoCA	**.6009711**	**.2373969**	**2.53**	**0.01***	**.1356818**	**1.06626**
deposiBanco	-.0066537	.2753938	0.02	0.981	-.5331083	.5464157
DeposiCorreo	-1.969646	1.350401	-1.46	0.145	-4.616383	.6770916
depositoCel	.3746377	.3068151	1.22	0.222	-.226709	.9759843
dineroCA	.3747039	.4621943	0.81	0.418	-.5311803	1.280588
dineroBanco	**.7062953**	**.2756089**	**2.56**	**0.010***	**.166111**	**1.246479**

dineroCome~o	.0050634	.2611094	0.02	0.985	-.5067017	.5168284
dintransST	.6001545	.3933962	1.53	0.127	-.1708879	1.371197
comprasCheq	**-.9572553**	**.5761834**	**-1.66**	**0.097****	**-2.0865**	**.1720434**
comprasTC	-.0748638	.2743527	-0.27	0.785	-.6125852	.4628576
comprasDebit	-.4390602	.2930469	-1.50	0.134	-1.013422	.1353012
comprasInt~j	-.396239	.2722661	-1.46	0.146	-.9298708	.1373927
comprasIntMV	.4047265	.4051272	1.00	0.318	-.3893082	1.198761
comprasCEL	**.5082132**	**.2779714**	**1.83**	**0.068****	**-.03660**	**1.053027**
transFonCA	-.2168885	.2820771	-0.77	0.442	-.7697495	.3359724
transFonIn~r	-.0697841	.3379164	-0.21	0.836	-.7320881	.5925199
transfonBM	-.0437132	.2710962	-0.16	0.872	-.5750521	.4876256
transFonBa~o	.2205555	.2672388	0.83	0.409	-.3032229	.744334
transfonTa~e	-.2086551	.4188517	-0.50	0.618	-1.029589	.6122791
transFonRS	.3766884	1.907193	0.20	0.843	-3.36134	4.114717
transSmartF	**.6252682**	**.2909906**	**2.15**	**0.032***	**.054937**	**1.195599**
tranComPor	.4134584	.2960858	1.40	0.163	-.1668592	.9937759
transComEscr	.0360544	.2252133	0.16	0.873	-.4053557	.4774644
usaAntiv	.1587091	.3296124	0.48	0.630	-.4873194	.8047376
usaSuites	.093945	.2345227	0.40	0.689	-.3657112	.5536011
usaAVCel	.0375865	.2318763	0.16	0.871	-.4168827	.4920558
usaComConfi	**-.7369588**	**.279212**	**-2.64**	**0.008***	**-1.28420**	**-.1897134**
usaWiFiPub	.0372853	.2427845	0.15	0.878	-.4385636	.5131342
usaToken	-.0678162	.251414	-0.27	0.787	-.5605787	.4249463
usaNotiMail	**.524101**	**.2829487**	**1.85**	**0.064****	**-.03046**	**1.07867**
usaNotiCel	-.2190288	.257546	-0.85	0.395	-.7238097	.2857521
_cons	-2.29986	.7265458	-3.17	0.002	-3.723864	-.8758564

Number of obs = 516, LR chi2(41) = 63.50, Prob > chi2 = 0.0136, Log likelihood = -285.29674, Pseudo R2 = 0.1001

Se incluyeron las variables independientes propias del individuo Edad y Género. Ambas no fueron significativas en el modelo a niveles convencionales del 5 y 10%. Lo anterior establece que los incidentes de seguridad digital se dan de manera similar tanto en hombres como en mujeres. Tampoco es posible concluir que los incidentes de seguridad digital en los individuos tengan relación con la edad.

Se agregaron en bloque variables asociadas a los medios para la revisión de las transacciones recientes y saldos disponibles de los individuos encuestados. Este factor fue clasificado en registro de operaciones bancarias por Internet (computadora portátil o de escritorio), en cajeros automáticos, por teléfono, en el banco, usando aplicaciones bancarias móviles, por tableta, por redes sociales (si el banco ofrece este servicio integrado a redes sociales como *WhatsApp, Twitter*, etc.). Cada una de estas características se incluyó en el modelo a través de variables *dummies*: 1 si se tiene la característica y 0 de lo contrario. Ninguna de estas variables fue significativa en el modelo estimado, considerando niveles de significancia del 5 y del 10%.

De otra parte, también se adicionó al modelo un bloque de variables relacionadas con la forma en que los usuarios (individuos) hacen depósitos en cheque o en efectivo. Ello a través de distintos canales como: Depósito electrónico directo, en cajeros automáticos, en el banco, por correo, mediante depósito móvil. Cada una de estas características se incluyó en el modelo a través de variables *dummies*: 1 si se tiene la característica y 0 de lo contrario. De este bloque de variables resulto significativa "depositoCA", es decir, depósito en cajero automático. Esta variable es altamente significativa en el modelo, presentando signo positivo, lo cual llevaría a concluir que en la medida en que los individuos utilizan medios de depósito directo en cajero automático, aumenta la probabilidad de ocurrencia de eventos de seguridad digital. Sin embargo, no fue posible establecer de manera concreta una razón o explicación sobre el resultado de esta variable dependiente, en consideración a que los depósitos en cajero automático no representan en sí mismos un factor de riesgo inherente a incidentes de seguridad digital, de la forma en la que podría presentarse expuesto un usuario al usar otros medios de base digital, tales como aplicaciones móviles o el sitio web del banco.

Igualmente, se incluyeron variables asociadas a la manera en que los individuos obtienen dinero en efectivo. En este sentido se crearon *dummies* que representaran las siguientes situaciones para el individuo: Cuando obtiene dinero en el cajero automático, en el banco, en comercios cuando hace una compra usando su tarjeta débito o crédito, y en cajero mediante transacciones sin tarjeta. De este conjunto de variables resultó significativa "dineroBanco", lo que sugeriría que aquellos individuos que obtienen dinero directamente en entidades bancarias, presentan mayor probabilidad de experimentar incidentes de seguridad digital. Esta variable fue significativa en el modelo a niveles del 5%. Al igual que en el caso anterior, no fue posible establecer de manera concreta una razón o explicación sobre el resultado de esta variable dependiente, en consideración a que los retiros de dinero en el banco no representan en sí mismos un factor de riesgo inherente a incidentes de seguridad digital.

En el modelo econométrico se incluyeron también las variables sobre la forma en que los individuos hacen compras. Para ello se incluyó un conjunto de variables que representan las distintas maneras en que los individuos compran bienes y servicios clasificados en: Compras con cheque, compras con una tarjeta crédito, con una tarjeta de débito, por teléfono con tarjeta, compras por Internet con tarjeta, compras por Internet usando monedas virtuales (Ej. Bitcoin, Etherum, Litecoin...) y compras con el dispositivo móvil con cuentas/tarjetas registradas. Se emplearon *dummies* para cada una de estas variables: 1 si el individuo tiene la respectiva característica y 0 de lo contrario. De este conjunto de variables resultó significativa al nivel del 10%, la correspondiente a "comprasCheq". En la estimación resultó con un

signo negativo, indicando que los individuos que tienen esta forma de pagar las compras, presentan menor probabilidad de incidentes de seguridad. Por su parte la variable "comprasCEL" también resultó significativa al 10%, estimada con un signo positivo. Lo anterior plantea que los individuos que emplean esta forma de hacer compras, es decir, a través de dispositivos móviles, experimentan mayor probabilidad de tener incidentes de seguridad digital.

Adicional a las variables anteriores, se incluyeron indicadores a nivel de individuo que describen la forma de transferencia de fondos. Para lo anterior, se tuvieron en cuenta los siguientes indicadores incluidos a través de *dummies*: Tomando el valor de 1 si el individuo tiene la característica y 0 de lo contrario. En total se consideraron las siguientes maneras de transferir fondos: A través de cajero automático, con operaciones bancarias por Internet (computadora portátil o de escritorio), a través de operaciones bancarias móviles, en el banco, con transferencias internacionales (vía transferencias electrónicas o por sistemas ACH), empleando una tableta y a través de redes sociales (si el banco ofrece este servicio integrado a redes sociales como *WhatsApp, Twitter*, etc.). De este conjunto de variables independientes resultó significativa al 5% y con signo positivo "transSmartF". Lo anterior se interpreta en el sentido que aquellos individuos que transfirieron fondos a través de Smartphone tienen una mayor probabilidad de eventos de incidentes de seguridad digital.

En cuanto a las medidas de seguridad que se han implementado para prevenir incidentes digitales, se recopiló información a nivel de individuo sobre una serie de comportamientos para defenderse de los ataques. Se consideraron las siguientes opciones: Uso de antivirus en las computadoras, instalación de "Suites" de seguridad (antivirus más otras herramientas) en las computadoras, uso de antivirus en los dispositivos móviles, acceso únicamente en computadoras confiables, evitar el acceso a redes Wi-Fi públicas, uso de token – medios complementarios de autenticación, habilitación de notificaciones de transacciones vía correo electrónico y habilitación de notificaciones de transacciones vía Mensaje de Texto (SMS). De la estimación se observa que la variable "usaComConfi", que se refiere al uso de computador confiable, presenta un signo negativo y significativo al 1%. Lo anterior sugiere que los usuarios que tienen esta estrategia para defenderse de los posibles ataques, efectivamente experimentaron una menor probabilidad de incidentes digitales. Por su parte, la variable "usaNotiMail", que se refiere a la habilitación de notificaciones de transacciones vía correo electrónico, resultó significativa, aunque a niveles del 10%. Esta variable resultó con un signo positivo, indicando que los individuos que utilizan este tipo de mecanismos, en promedio, tuvieron mayor probabilidad de incidentes de seguridad digital, lo cual se puede explicar en la facilidad que representa para el usuario enterarse de cualquier acceso u operación fraudulenta al recibir las notificaciones de su banco. Caso contrario, cuando los usuarios no tienen activados este tipo de servicios y solo se dan cuenta de la irregularidad frente a la revisión de sus extractos de movimientos (aunque a veces pueden pasar desapercibidas o no ser objeto de revisión por el usuario bancario) o frente a situaciones anómalas demasiado evidentes.

Por su parte, la tabla siguiente presenta los efectos marginales de las variables independientes calculadas sobre el promedio:

Cuadro 21. Resultados de los efectos marginales del modelo LOGIT

Variable	dy/dx	Std. Err.	z	P>|z|	95% C.I.]		X
Deposi~A*	.1255893	.05097	2.46	0.014	.025687	.225492	.335271
Deposi~o*	-.2325664	.07071	-3.29	0.001	-.371161	-.093971	.015504
Diner~co*	.1453612	.05721	2.54	0.011	.033241	.257481	.408915
Compra~q*	-.1538175	.0695	-2.21	0.027	-.290044	-.017591	.04845
Compra~L*	.1068385	.0606	1.76	0.078	-.011926	.225603	.281008
TransF~A*	-.0424785	.05368	-0.79	0.429	-.147686	.062729	.228682
TransS~F*	.1208319	.0535	2.26	0.024	.015981	.225683	.631783
UsaCom~i*	-.1594545	.06338	-2.52	0.012	-.283673	-.035237	.76938

Los efectos marginales (EM) muestran el cambio que se genera en la probabilidad de *"haber experimentado algún incidente o situación que ha comprometido la confidencialidad, integridad o disponibilidad de su información o sus recursos financieros en su banco"*, dado un cambio en cada variable dependiente manteniendo constantes las demás variables; en otras palabras, el EM se estima como la derivada parcial de la función de probabilidad con respecto al vector de variables independientes, evaluadas en sus medias. Se interpreta, por ejemplo, que el uso de computador confiable "usaCom~i", que fue una variable significativa al modelo, de signo negativo, disminuye la probabilidad de ocurrencia de incidente en 0.15%.

06

RECOMENDACIONES DE CIBERSEGURIDAD PARA EL SECTOR BANCARIO DE AMÉRICA LATINA Y EL CARIBE

Con base en los hallazgos encontrados, se establecieron un conjunto de recomendaciones de ciberseguridad para el sector bancario de América Latina y el Caribe. Para el efecto se establecen tres (3) grupos objetivo como destinatarios de las recomendaciones: i) las entidades bancarias de América Latina y el Caribe, ii) los usuarios de dichas entidades en la región, y, iii) las agencias del gobierno, reguladores y organismos de aplicación de la ley.

6.1 Para las entidades bancarias de América Latina y el Caribe

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 bancarias en la región 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

- En lo posible, tener una única instancia responsable u órgano de gobierno corporativo para liderar la gestión de riesgo de Seguridad Digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales).

- Aunque a medida que el tamaño de la entidad bancaria aumenta se pretenda especializar en varias áreas de la organización la gestión de los asuntos de seguridad de la información, de ciberseguridad y de prevención del fraude usando medios digitales, se debe garantizar que las mismas funcionen de manera coordinada y efectiva para lograr una eficiente gestión de riesgos de Seguridad Digital. Considerar que la gestión de estos riesgos debe estar a cargo de un grupo independiente al de Tecnología.

- Dimensionar adecuadamente los equipos de trabajo dedicados a los aspectos de Seguridad Digital, efectuar evaluaciones de seguridad de los colaboradores, segregar adecuadamente roles y funciones, garantizar procesos de gestión del conocimiento que rompan dependencias "unipersonales", y establecer mecanismos para elevar la lealtad y retención en los funcionarios apoyándose en el desarrollo del talento humano y considerando planes de incentivos.

- 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.

• Establecer mecanismos claros para asegurar el conocimiento de la gestión de riesgos de Seguridad Digital por parte de las instancias de decisión en las organizaciones (altas directivas y demás equipos de liderazgo) 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.

• Efectuar una revisión habitual de las mejores prácticas y/o estándares internacionales aplicables en torno a la Seguridad Digital, así como del marco regulatorio local e internacional aplicable a la entidad bancaria, haciendo un proceso de mapeo y priorización para su aplicación. El proceso debe incluir el análisis de brechas frente a lo requerido, la valoración de los recursos para la adopción de procesos, herramientas y tecnologías, así como procesos de capacitación del personal y gestión del cambio requeridos, entre otros.

• 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 e incluso el fortalecimiento de la cultura de seguridad.

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

• Garantizar que la priorización de acciones, procesos y medidas técnicas de Seguridad Digital para proteger los sistemas de información críticos de la entidad bancaria, 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[28].

• Se debe contar con mecanismos de contrastación de las capacidades de detección y análisis de eventos de seguridad, preferiblemente mediante colaboración con equipos de respuesta a incidentes públicos o privados. Esto significa 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.

• Priorizar 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 interaccion realizada por los usuarios, por ejemplo, incorporando soluciones de detección o prevención[29] 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 no exitosos) de Seguridad Digital, 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 entidad bancaria (por ejemplo, equipos de respuesta a incidentes del sector o del país, si aplica). Esto debería estar coordinado por una instancia (ej. Comité) que gestione las crisis cibernéticas, en la que las diferentes áreas de negocio y de soporte (tales como Tecnología. Jurídica o Legal, Cumplimiento, Operaciones, Asuntos Públicos, etc) estén debidamente representados.

• Apoyar las investigaciones y seguir los protocolos exigidos por las autoridades de aplicación de la ley y las mejores prácticas aplicables a la cadena de custodia de la evidencia digital (por ejemplo, que faciliten la cooperación transnacional), que resulten relevantes para los procesos investigativos.

• Participar activamente de alianzas en las que se logre compartir las conclusiones y lecciones aprendidas sobre la gestión de eventos de seguridad digital, que faciliten la identificación y prevención de delitos, así como el desarrollo de soluciones holísticas para gestionar el riego cibernético. Compartir las conclusiones sobre los incidentes es tan importante como cooperar con las investigaciones.

• Realizar procesos de evaluación de la madurez de Seguridad Digital 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 con Seguridad Digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales).

• 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)

• 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 el ciclo de vida de la información, 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 bancaria en el caso de que resulten víctimas de incidentes de seguridad digital.

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.

• 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 bancarios, 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.

• Aumentar y mantener la fuerza de trabajo especializada en temas de seguridad digital, mediante formación especializada e incentivos, de forma que se pueda contar con un equipo ágil y robusto que soporte la resiliencia cibernética de la organización.

• Participar activamente en espacios de discusión (foros, mesas de trabajo, congresos, etc.).

• Realizar campañas de prevención de eventos de i) phishing, ii) ingeniería social, y, iii) software espía (malware o troyanos), dirigidos a sus usuarios de servicios financieros.Aumentar el porcentaje de inversión destinado en la entidad bancaria para la generación de ciber capacidades (ej.: capacitación, 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, la cual puede requerir una mayor capacidad educativa e incentivos

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

- Establecer responsabilidades al interior de la entidad bancaria 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.

- Establecer de la manera más precisa posible la tasa de retorno de las inversiones efectuadas en relación con seguridad digital. Partir de una adecuada valoración de los activos de la entidad bancaria, así como de la estimación de los costos asociados al impacto derivado de posibles incidentes de seguridad digital.

- 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.

6.2 Para los usuarios de las entidades bancarias de América Latina y el Caribe

Los usuarios son 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 práctivas 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 bancaria. 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 bancaria 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. El hecho de que una contraseña sea expuesta podría facilitar el acceso a operaciones fraudulentas, razón por la cual deben tambien cambiarse periódicamente.

• Evitar almacenar las contraseñas de acceso a entidades bancarias 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 bancaria a través de correo electrónico o de mensajes de texto al teléfono móvil. Verificar qué opciones ofrece la entidad bancaria para el envío de estas notificaciones, incluidas las 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. Aseguarse de que tanto estas soluciones como los sistemas operativos de los equipos y dispositivos están continuamente actualizados.

• Realizar transacciones bancarias 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 bancarias 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 bancaria.

• Frente a cualquier tipo de incidente reportar a la entidad bancaria a través del mecanismo establecido para el efecto. Indagar si además del reporte del incidente a la entidad bancaria es necesario realizar cualquier otro tipo de gestión o procedimiento, por ejemplo, ante autoridades de aplicación de la ley, y ofrecer toda la información pertinente sobre el incidente.

6.3 Para agencias del Gobierno, reguladores y organismos de aplicación de la ley

• Efectuar la revisión del catálogo de infraestrucutras críticas, 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 insfraestructuras (por ejemplo, telecomunicaciones o energía) podrían tener sobre el sistema bancario.

• Coordinar esfuerzos con gremios o asociaciones bancarias tendientes al desarrollo de capacidades en materia de seguridad digital, preferiblemente regulados 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 del sector bancario, otros equipos sectoriales y del punto focal nacional, 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.

• Elevar las capacidades de las autoridades de aplicación de la ley, respecto al apoyo a la respuesta, investigación y judicialización de cibercriminales.

• Establecer y socializar protocolos para la gestión de evidencia digital y garantizar su cadena de custodia.

• Emitir 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 sector bancario, y de ser necesario emitir los instrumentos legales necesarios para su aplicación. Al momento de crear o actualizar regulación relacionada con cibersguridad, 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.

• 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.

• 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.

• Evaluar la pertinencia de establecer como obligación para las entidades bancarias el reporte de los incidentes de seguridad digital que sufran, principalmente con destino al equipo de respuesta a incidentes de carácter nacional o punto focal en la materia. 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 bancarias o actores.

• Exigir a las entidades bancarias la disposición de mecanismos de reporte a través de los cuales sus clientes puedan informar en caso de ser víctimas de incidentes de seguridad digital. Evaluar la efectividad de procesos de divulgación y socialización de estos.

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

• Asegurar el intercambio de información entre el sector público y el sector privado, lo cual permite la detección de patrones para que las organizaciones se protejan de una mejor manera contra los ciberataques.

• Promover la adecuación de una reglamentación sólida para el intercambio de información que facilitaría que los sectores público y privado compartan información sobre amenazas cibernéticas de manera oportuna, se permita que el gobierno desclasifique cierta información de amenazas para que pueda ser utilizada por el sector privado para su protección y proporcione fuertes protecciones de responsabilidad para las entidades que comparten información apropiada de amenazas cibernéticas

BIBLIOGRAFÍA
ANEXO 1
ANEXO 2
ANEXO 3
NOTAS DE REFERENCIAS

07

Bibliografía

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

Bankdirector. (2018). 2018 Risk Survey.
Obtenido de www.accenture.com;
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;
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 www.felaban.net;
www.felaban.net/archivos_publicaciones/archivo20150702202150PM.pdf

Capgemini. (2017). Top 10 Trends in Banking – 2017.
Obtenido de www.capgemini.com:
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:
www.cisco.com/c/es_co/products/security/security-reports.html#~stickynav=3

Ernst and Young . (2018). Global banking outlook 2018 - Pivoting toward an innovation-led strategy.
Obtenido de www.ey.com:
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;
www.felaban.net/archivos_publicaciones/archivo20180509104600AM.pdf

Global Knowledge. (2017). 2017 IT Skills and Salary Report. A comprehensive Study from Global Knowledge.
Obtenido de www. 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 https://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 https://cybersecurity.isaca.org/;
https://cybersecurity.isaca.org/state-of-cybersecurity

Kaspersky Lab. (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

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

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

Price Waterhouse Cooper. (2017). Top financial services issues of 2018.
Obtenido de www.pwc.se;
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;
www.pwc.com/us/en/financial-services/publications/assets/pwc-fsi-whitepaper-digital-banking-consumer-survey.pdf

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

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

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;
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;
www3.weforum.org/docs/WEF_GRR18_Report.pdf

ANEXO 1

Cuadro 22. Información del sector bancario en América Latina a partir de datos de FELABAN para 2017

País	Entidades Bancarias FELABAN Dic2017	Sucursales Bancarias FELABAN Dic2017	Sucursales por Entidad	Activos Totales Dic2017	Utilidad Neta Acumulada Dic2017	Banco con mayores Activos del país Jun2017		% participación de los activos del banco con mayores activos en los Activos Totales del país
Argentina	78	4.480	57	USD 185.261	USD 4.578	USD 36.096	Nación (Argentina)	19%
Bolivia	16	1.276	80	USD 29.838	USD 298	USD 4.482	Mercantil Santa Cruz	15%
Brasil	155	21.062	136	USD 2.492.225	USD 28.839	USD 451.114	Do Brasil	18%
Chile	20	21.080	1054	USD 358.246	USD 3.636	USD 54.731	Estado	15%
Colombia	25	5.722	229	USD 194.859	USD 2.545	USD 47.282	Bancolombia	24%
Costa Rica	16	797	50	USD 46.316	USD 297	USD 12.136	Nacional (Costa Rica)	26%
Ecuador	24	1.300	54	USD 38.975	USD 396	USD 10.296	Pichincha	26%
El Salvador	14	424	30	USD 17.072	USD 152	USD 4.376	Agricola	26%
Guatemala	18	3.572	198	USD 41.675	USD 574	USD 10.707	Industrial (Guatemala)	26%
Honduras	15	5.054	337	USD 21.246	USD 220	USD 3.785	Ficohsa	18%
México	53	12.744	240	USD 458.598	USD 7.018	USD 107.439	BBVA BANCOMER	23%
Nicaragua	8	672	84	USD 8.070	USD 171	USD 2.220	De la Producción	28%
Panamá	49	561	11	USD 101.410	USD 1.505	USD 15.131	General	15%
Paraguay	17	547	32	USD 20.852	USD 435	USD 3.384	ITAU (Paraguay)	16%
Perú	16	2.120	133	USD 111.295	USD 1.670	USD 36.909	Credito (Perú)	33%
República Dominicana	18	963	54	USD 29.557	USD 482	USD 9.431	De Reservas	32%
Uruguay	10	286	29	USD 36.352	USD 356	USD 16.465	Rep Oriental de UY	45%
TOTAL	**552**	**82.660**	**150**	**USD 4.191.847**	**USD 53.172**			**24%**
				Utilidad/Activos	**1,27%**			

Nota 1: La información de las columnas (A), (B), (D) y (E) fue tomada de https://indicadores.felaban.net/indicadores_homologados/index.php

Nota 2: La información de la columna (F) fue tomada de www.americaeconomia.com/negocios-industrias/ranking-2017-conozca-los-250-mayores-Bancos-de-america-latina

Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

ANEXO 2

Cuadro 23. Frecuencia en la ocurrencia por tipo de evento de seguridad digital contra las entidades bancarias (parte 1 de 2)

Ingeniería social

	Grande	Mediano	Pequeño	**Total**
Diario	5	12	3	**20**
Mensual	6	11	4	**21**
Semanal	5	6	5	**16**
Trimestral	8	24	11	**43**
No hay	4	35	42	**81**

	Grande	Mediano	Pequeño	**Total**
Diario	18%	14%	5%	**11%**
Mensual	21%	13%	6%	**12%**
Semanal	18%	7%	8%	**9%**
Trimestral	29%	27%	17%	**24%**
No hay	14%	40%	65%	**45%**

Código malicioso o Malware

	Grande	Mediano	Pequeño	**Total**
Diario	10	21	4	**35**
Mensual	6	19	5	**30**
Semanal	6	12	10	**28**
Trimestral	3	24	25	**52**
No hay	3	12	21	**36**

	Grande	Mediano	Pequeño	**Total**
Diario	36%	24%	6%	**19%**
Mensual	21%	22%	8%	**17%**
Semanal	21%	14%	15%	**15%**
Trimestral	11%	27%	38%	**29%**
No hay	11%	14%	32%	**20%**

Phishing dirigido para tener acceso a sistemas del banco

	Grande	Mediano	Pequeño	**Total**
Diario	7	12	4	**23**
Mensual	1	15	6	**22**
Semanal	2	6	4	**12**
Trimestral	9	25	13	**47**
No hay	9	30	38	**77**

	Grande	Mediano	Pequeño	**Total**
Diario	25%	14%	6%	**13%**
Mensual	4%	17%	9%	**12%**
Semanal	7%	7%	6%	**7%**
Trimestral	32%	28%	20%	**26%**
No hay	32%	34%	58%	**43%**

Pérdida de datos

	Grande	Mediano	Pequeño	**Total**
Diario	1	1	1	**3**
Mensual	3	4	1	**8**
Semanal	2	2		**4**
Trimestral	5	21	3	**29**
No hay	17	60	60	**137**

	Grande	Mediano	Pequeño	**Total**
Diario	4%	1%	2%	**2%**
Mensual	11%	5%	2%	**4%**
Semanal	7%	2%	0%	**2%**
Trimestral	18%	24%	5%	**16%**
No hay	61%	68%	92%	**76%**

Pérdida o robo de equipos o dispositivos

	Grande	Mediano	Pequeño	**Total**
Diario				**0**
Mensual	4	8	1	**13**
Semanal	4	1		**5**
Trimestral	9	36	12	**57**
No hay	11	43	52	**106**

	Grande	Mediano	Pequeño	**Total**
Diario	0%	0%	0%	**0%**
Mensual	14%	9%	2%	**7%**
Semanal	14%	1%	0%	**3%**
Trimestral	32%	41%	18%	**31%**
No hay	39%	49%	80%	**59%**

Ataque de negación del servicio (DoS / DDoS)

	Grande	Mediano	Pequeño	**Total**
Diario	1	3	2	**6**
Mensual		10	3	**13**
Semanal	5	3	4	**12**
Trimestral	10	14	4	**28**
No hay	12	58	52	**122**

	Grande	Mediano	Pequeño	**Total**
Diario	4%	3%	3%	**3%**
Mensual	0%	11%	5%	**7%**
Semanal	18%	3%	6%	**7%**
Trimestral	36%	16%	6%	**15%**
No hay	43%	66%	80%	**67%**

Robo de DNS

	Grande	Mediano	Pequeño	**Total**
Diario		1		**1**
Mensual	2	3	1	**6**
Semanal		1	1	**2**
Trimestral	5	5	1	**11**
No hay	21	78	62	**161**

	Grande	Mediano	Pequeño	**Total**
Diario	0%	1%	0%	**1%**
Mensual	7%	3%	2%	**3%**
Semanal	0%	1%	2%	**1%**
Trimestral	18%	6%	2%	**6%**
No hay	75%	89%	95%	**89%**

Cuadro 24. Frecuencia en la ocurrencia por tipo de evento de seguridad digital contra las entidades bancarias (parte 2 de 2)

Violación de políticas de escritorio limpio *(Clear Desk)*

	Grande	Mediano	Pequeño	**Total**
Diario	4	11	3	**18**
Mensual	8	23	6	**37**
Semanal	6	7	2	**15**
Trimestral	6	20	18	**44**
No hay	4	27	36	**67**

	Grande	Mediano	Pequeño	**Total**
Diario	14%	13%	5%	**10%**
Mensual	29%	26%	9%	**20%**
Semanal	21%	8%	3%	**8%**
Trimestral	21%	23%	28%	**24%**
No hay	14%	31%	55%	**37%**

Sabotaje interno

	Grande	Mediano	Pequeño	**Total**
Diario		1		**1**
Mensual	2	3		**5**
Semanal	2	1		**3**
Trimestral	4	10	6	**20**
No hay	20	73	59	**152**

	Grande	Mediano	Pequeño	**Total**
Diario	0%	1%	0%	**1%**
Mensual	7%	3%	0%	**3%**
Semanal	7%	1%	0%	**2%**
Trimestral	14%	11%	9%	**11%**
No hay	71%	83%	91%	**84%**

Fraude interno

	Grande	Mediano	Pequeño	**Total**
Diario		1		**1**
Mensual	10	7		**17**
Semanal	1			**1**
Trimestral	11	34	10	**55**
No hay	6	46	55	**107**

	Grande	Mediano	Pequeño	**Total**
Diario	0%	1%	0%	**1%**
Mensual	36%	8%	0%	**9%**
Semanal	4%	0%	0%	**1%**
Trimestral	39%	39%	15%	**30%**
No hay	21%	52%	85%	**59%**

Defacement

	Grande	Mediano	Pequeño	**Total**
Diario	1			**1**
Mensual		3		**3**
Semanal	1	1		**2**
Trimestral	5	3	2	**10**
No hay	21	81	63	**165**

	Grande	Mediano	Pequeño	**Total**
Diario	4%	0%	0%	**1%**
Mensual	0%	3%	0%	**2%**
Semanal	4%	1%	0%	**1%**
Trimestral	18%	3%	3%	**6%**
No hay	75%	92%	97%	**91%**

Backdoor (código desarrollado para habilitar acceso posterior)

	Grande	Mediano	Pequeño	**Total**
Diario	1		1	**2**
Mensual	3	5		**8**
Semanal	1		1	**2**
Trimestral	9	11	2	**22**
No hay	14	72	61	**147**

	Grande	Mediano	Pequeño	**Total**
Diario	4%	0%	2%	**1%**
Mensual	11%	6%	0%	**4%**
Semanal	4%	0%	2%	**1%**
Trimestral	32%	13%	3%	**12%**
No hay	50%	82%	94%	**81%**

SQL Injection

	Grande	Mediano	Pequeño	**Total**
Diario	4	3	2	**9**
Mensual	1	9		**10**
Semanal	4	3	3	**10**
Trimestral	9	18	6	**33**
No hay	10	55	54	**119**

	Grande	Mediano	Pequeño	**Total**
Diario	14%	3%	3%	**5%**
Mensual	4%	10%	0%	**6%**
Semanal	14%	3%	5%	**6%**
Trimestral	32%	20%	9%	**18%**
No hay	36%	63%	83%	**66%**

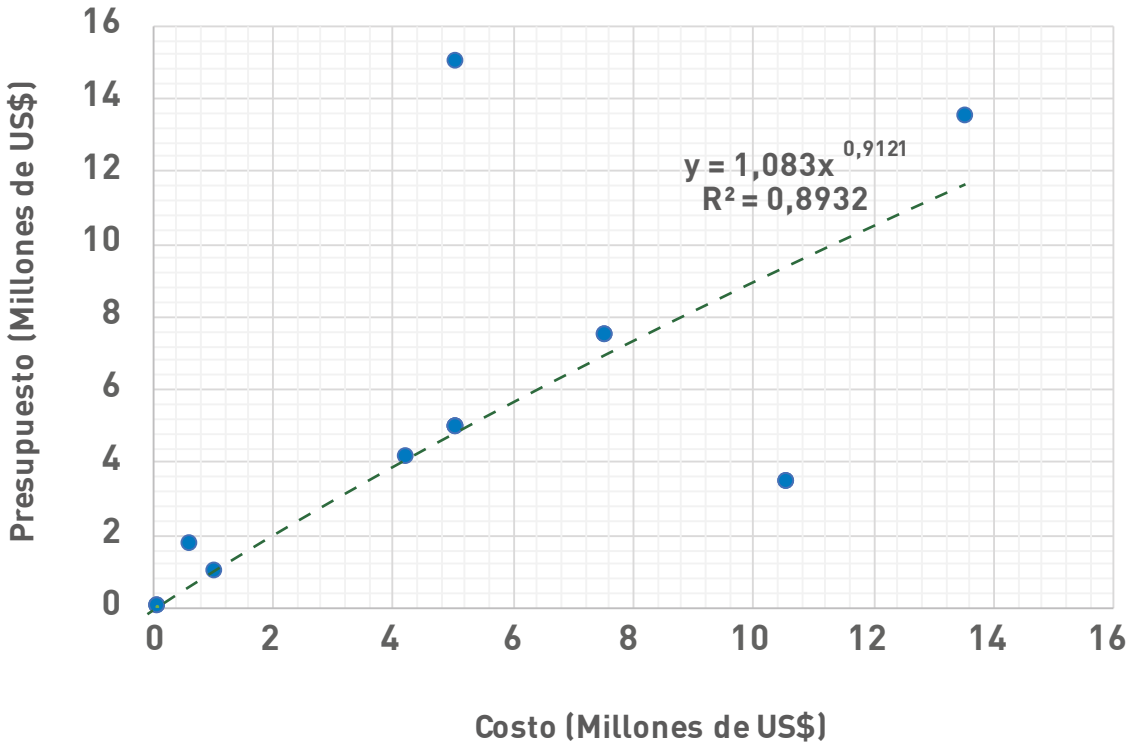
Ataque de fuerza bruta

	Grande	Mediano	Pequeño	**Total**
Diario	4	1	3	**8**
Mensual	1	8	1	**10**
Semanal	4	2	1	**7**
Trimestral	6	18	7	**31**
No hay	13	59	53	**125**

	Grande	Mediano	Pequeño	**Total**
Diario	14%	1%	5%	**4%**
Mensual	4%	9%	2%	**6%**
Semanal	14%	2%	2%	**4%**
Trimestral	21%	20%	11%	**17%**
No hay	46%	67%	82%	**69%**

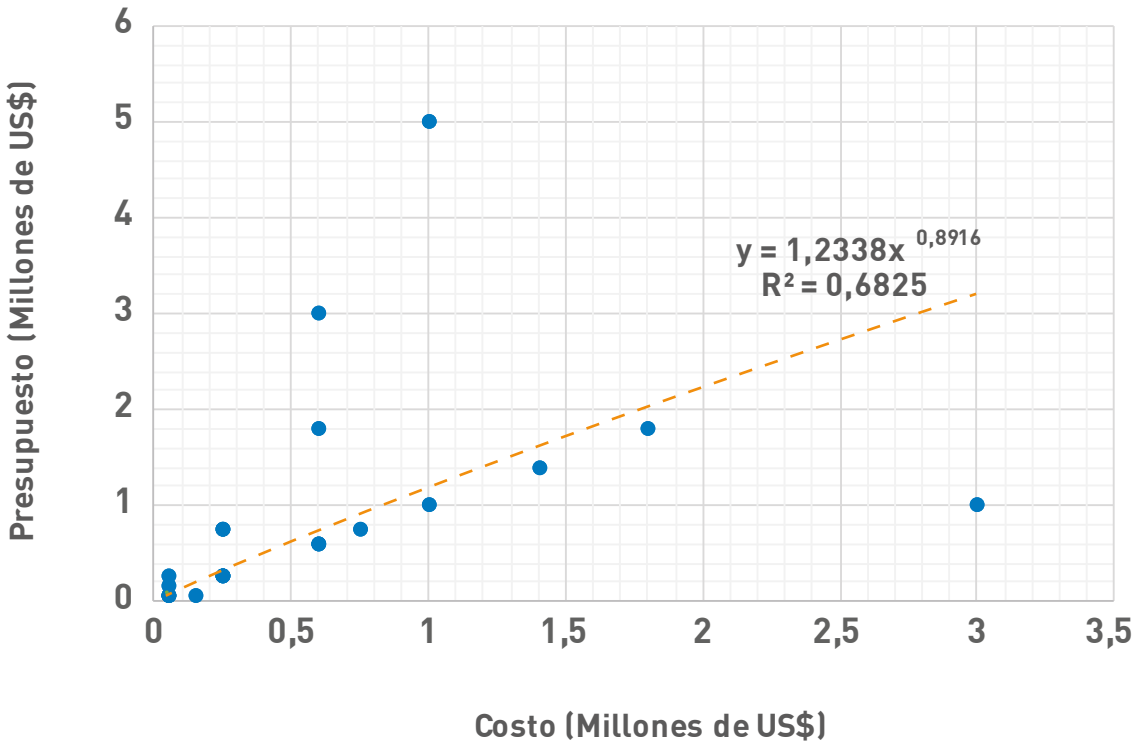
ANEXO 3

Gráfica 61. Relación entre el Presupuesto destinado a Seguridad Digital y el Costo total de respuesta y de recuperación ante incidentes de seguridad para Bancos Grandes en América Latina y el Caribe



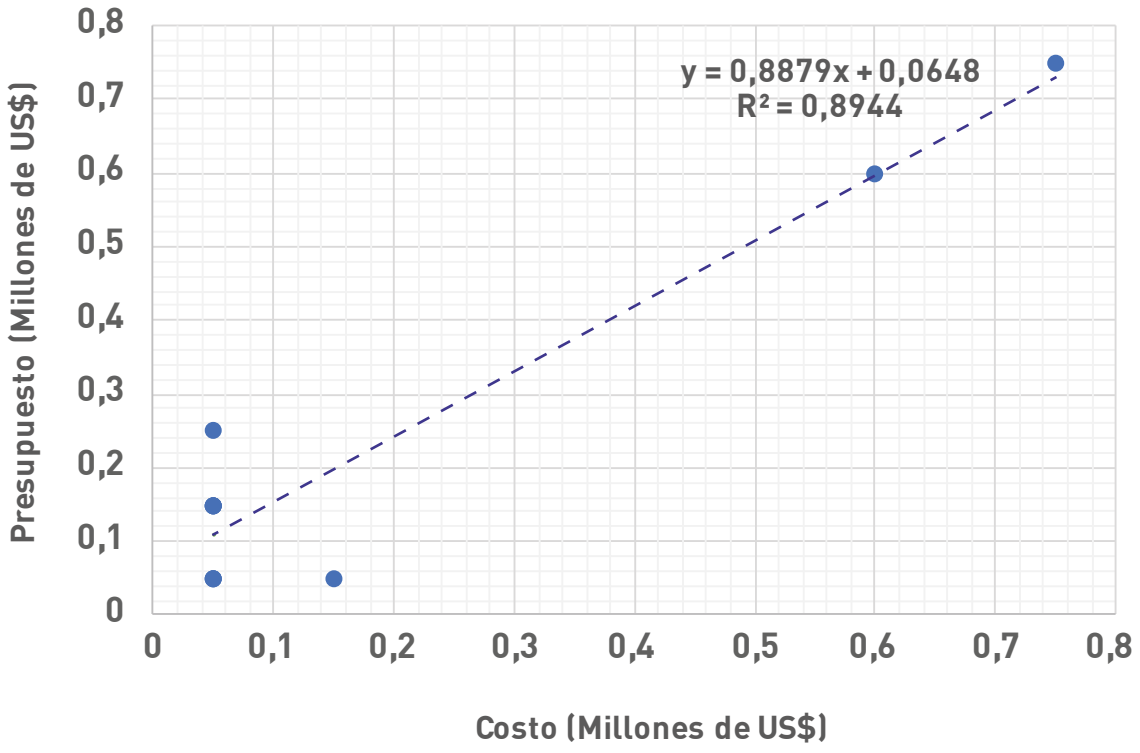
Nota: 14 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Gráfica 62. Relación entre el Presupuesto destinado a Seguridad Digital y el Costo total de respuesta y de recuperación ante incidentes de seguridad para Bancos Medianos en América Latina y el Caribe



Nota: 21 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Gráfica 63. Relación entre el Presupuesto destinado a Seguridad Digital y el Costo total de respuesta y de recuperación ante incidentes de seguridad para Bancos Pequeños en América Latina y el Caribe



Nota: 11 registros
Fuente: SG/OEA a partir de información recolectada de entidades bancarias en América Latina y el Caribe

Notas de referencias

1. Los Bancos participantes tienen un total de activos cercanos a USD$ 1 billón de dólares y acumulan utilidades netas por USD $10,5 mil millones de dólares (a 31 de diciembre de 2017) y según su tamaño se distribuyen así: 35% Bancos pequeños, 48% Bancos medianos y 17% Bancos grandes; según su composición son: 79% Bancos privados, 13% Bancos públicos y 8% Bancos mixtos

2. Los usuarios participantes informaron ser en un 72,44% de género masculino, en un 27,42% de género femenino y en un 0,14% como "no definido". En cuanto al rango de edad de los usuarios entrevistados, el 33,66% se encuentra entre los 35 y 44 años, el 33,52% entre los 25 y 34 años, el 20,08% entre los 45 y 54 años, el 6,23% entre los 55 y 64 años, el 5,40% entre los 18 y 24 años y solo el 1,1% tiene más de 65 años de edad.

3. Los usuarios pueden ser más conscientes de que están siendo afectados por un ataque con soluciones como las alertas que brindan las suites de seguridad (como resultado de la protección en tiempo real), así como con las notificaciones de acceso a plataformas virtuales o las notificaciones de transacciones u operaciones que pueden programarse con el banco.

4. See FIN7 Arrest paper. Use of "legitimate" Israeli and Ukrainian companies for funnelling of funds.

5. Oficina Federal de Investigaciones de EE. UU. (FBI), "Three members of notorious international Cybercrime Group "Fin7" in custody for role in attacking over 100 U.S. Companies", 1 de Agosto de 2018
www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100

6. Oficina Federal de Investigaciones de EE. UU. (FBI), "Three members of notorious international Cybercrime Group "Fin7" in custody for role in attacking over 100 U.S. Companies", 1 de Agosto de 2018
www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100

7. Bloomberg: "Mexico foiled a $110 million Bank Heist, Then Kept it Secret", 29 de mayo de 2018:
www.bloomberg.com/news/articles/2018-05-29/mexico-foiled-a-110-million-bank-heist-then-kept-it-a-secret

8. Reuters: "Bank of Chile trading down after hackers rob millions in cyberattack" 11 June 2018:
www.reuters.com/article/us-chile-banks-cyberattack/bank-of-chile-trading-down-after-hackers-rob-millions-in-cyberattack-idUSKBN1J72FC

9. Véase Zingbox "Meet Piolin, the first ATM Malware Jackpotting ATMs in US
www.zingbox.com/wp-content/uploads/2018/03/Meet-Piolin.pdf w8 Febrero de 2018

10. CyberScoop, "North Korea to blame for string of Latin American bank hacks, insiders say", 18 June 2018
www.cyberscoop.com/north-korea-swift-hacks-bancomext-bank-of-chile/

11. Véase Group-IB "Moneytaker: in pursuit of the invisible" and "Moneytaker: 1.5 years of silent operations," ambos con fecha del 11 de diciembre de 2017: www.group-ib.com/blog/moneytaker

12. Bloomberg, "Mexico tells banks to take steps to Guard against suspected hacks" 30 April 2018
www.bloomberg.com/news/articles/2018-04-30/banorte-is-said-to-be-among-mexican-banks-targeted-by-hackers

13. https://m.theepochtimes.com/exclusive-chinese-state-hackers-started-cyber-bank-robberies_2085775.html

14. www.fsisac.com/

15. www.europol.europa.eu/es/about-europol

16. www.nomoreransom.org/es/index.html

17. La Alianza de Ciberdefensa del Reino Unido (UK Cyber Defence Alliance) no tiene un sitio web público. Se puede encontrar una descripción de la estructura, ubicación y objetivos de la organización en Financial Times, "Banks join forces to crack down on fraudsters". 9 de agosto de 2017
www.ft.com/content/6c9030ca-7937-11e7-90c0-90a9d1bc9691

18. The Global Risks Report, Foro Económico Mundial, publicado el 17 de enero de 2018

19. Georges Bataille

20. www.fatf-gafi.org/recommendations

21. www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

22. www.fatf-gafi.org/publications/fatfgeneral/documents/universal-procedures.html

23. www.fatf-gafi.org/publications/mutualevaluations/documents/more-about-mutual-evaluations.html

24. Foro Economico Mundial. (2018). Thee Global Risks Report 2018, 13th Edition. Ginebra, Suiza: Foro Económico Mundial.

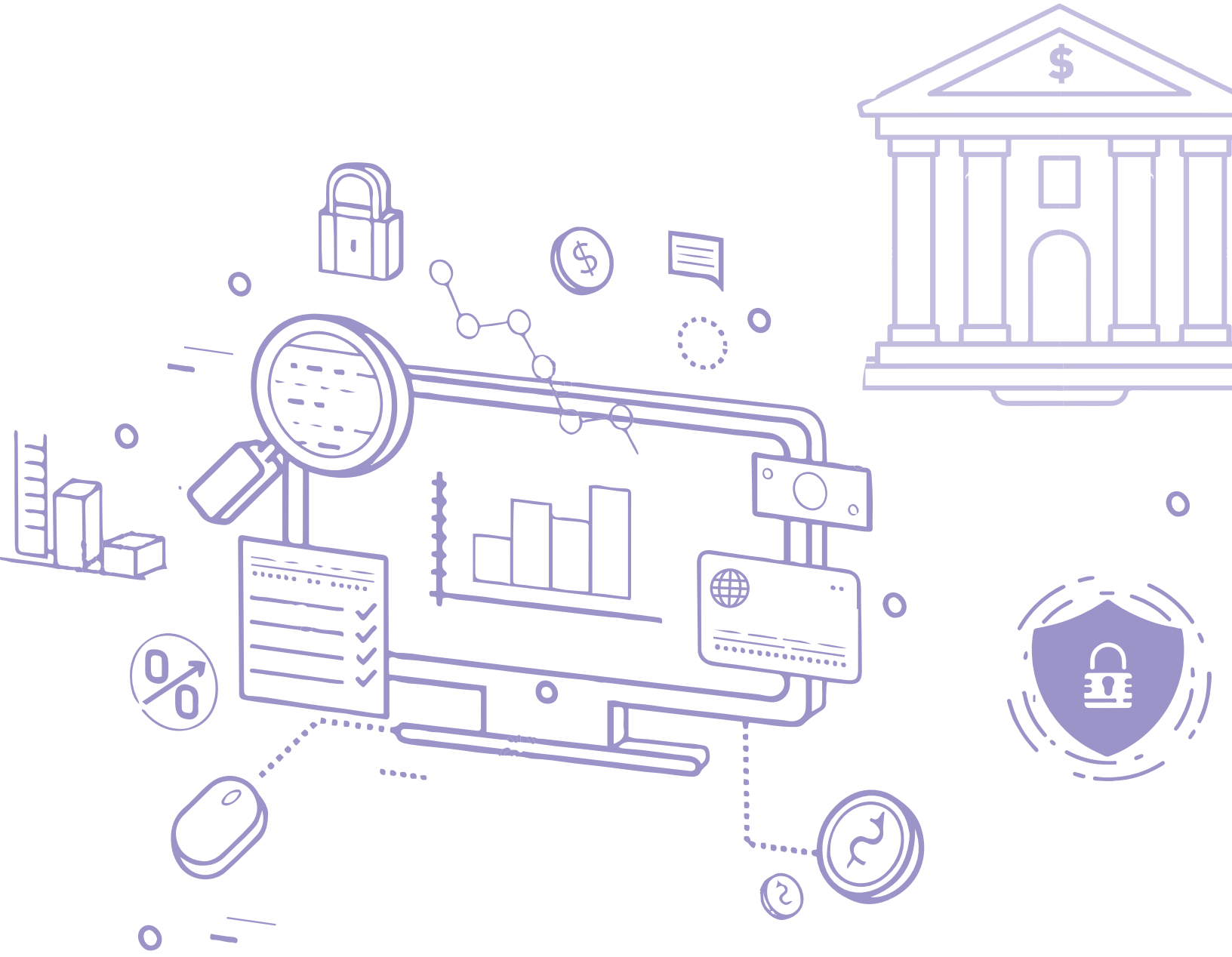
25. Wright, A., Kellman, B., & Kallicharan, S. (2018). CBR Withdrawals:Understanding the Uneven Occurence Across the Caribbean. Washington: Banco Interamericano de Desarrollo.

26. Banco Interamericano de Desarrollo. (2018, June 29). What will the Caribbean's financial sector of the future look like? Recuperado del Banco Interamericano de Desarrollo
https://blogs.iadb.org/caribbean-dev-trends/2018/06/29/8736/

27. Ernst and Young. (2016). CAACM: Cybersecurity Risks: Is your Organization Prepared. Trinidad and Tobago: Ernst and Young.
PricewaterhouseCoopers LLP. (2014). Threat Smart: Building a Cyber resilient financial institution. Delaware: PricewaterhouseCoopers LLP.

28. El concepto resiliencia cibernética se define como el grado de capacidad que tiene una organización para sentir (predecir y detectar), resisitir y reaccionar frente amenazas de índole cibernético.

29. Este tipo de soluciones incluyen recursos tales como: i) software de protección transaccional en internet, que se ofrecen para descarga desde el portal de la entidad bancaria a efecto de prevenir amenazas de fraudes a través de modalidades como Malware, Phishing y Pharming, y, ii) mecanismos de protección de identidad en aplicaciones que ofrecen sistemas mejorados para autenticación, así como el reconocimiento de los dispositivos de uso frecuente, orientado específicamente a prevenir amenzas de fraude a través de Phishing, entre otros.



OEA | Más derechos para más gente

Estado de la **Ciberseguridad** en el **Sector Bancario** en **América Latina** y el **Caribe**