OEA | Más derechos para más gente

CNBV | COMISIÓN NACIONAL BANCARIA Y DE VALORES

ESTADO DE LA CIBERSEGURIDAD EN EL SISTEMA FINANCIERO MEXICANO

ESTADO DE LA CIBERSEGURIDAD EN EL SISTEMA FINANCIERO MEXICANO

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

ESTADO DE LA CIBERSEGURIDAD EN EL SISTEMA FINANCIERO MEXICANO

OEA | Más derechos para más gente

CNBV
COMISIÓN NACIONAL BANCARIA Y DE VALORES

Luis Almagro
Secretario General
Organización de los Estados Americanos (OEA)

Farah Diva Urrutia
Secretaria de Seguridad Multidimensional
Organización de los Estados Americanos (OEA)

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

Equipo Técnico de la OEA

Belisario Contreras
Orlando Garcés
Jorge Bejarano
Kerry-Ann Barrett
Miguel Angel Cañada
David Moreno
Mariana Cardona
Diego Subero
Jaime Fuentes
Geraldine Vivanco
Barbara Marchiori
Gonzalo García-Belenguer

Adalberto Palma Gómez
Presidente
Comisión Nacional Bancaria y de Valores

David Esaú López Campos
Vicepresidente Técnico
Comisión Nacional Bancaria y de Valores

Equipo Técnico CNBV

Elena Calatayud Hernando
Karla Mendoza Morales
Arturo Murillo Torres
Gerardo Hernández Sánchez
Ricardo Javier Jimenez Piña
Salvador Ayala Castro
Edgar Valdovinos González

ESTADO DE LA **CIBERSEGURIDAD** EN EL SISTEMA FINANCIERO **MEXICANO**

TABLA DE CONTENIDO

RESUMEN EJECUTIVO

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

La información analizada en el presente estudio proviene de una base de datos de 240 entidades e instituciones financieras participantes del Sistema Financiero Mexicano[1]. Para llevar a cabo este análisis, la OEA diseñó, con el apoyo de expertos del sistema financiero, un instrumento específico de recolección de información. A partir del análisis efectuado con base en el instrumento empleado, se presentan a continuación los principales hallazgos.

Hallazgos significativos sobre la seguridad digital en las entidades e instituciones financieras del Sistema Financiero Mexicano:

- En relación con la preparación y gobernanza de la seguridad digital, en promedio en el 58% de las entidades e instituciones financieras del país existe un (1) nivel jerárquico entre el CEO y el máximo responsable de la seguridad digital. No obstante, el número de niveles jerárquicos que existen entre el CEO y el máximo responsable de la seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) depende también del tamaño de la organización. En referencia al número de áreas a cargo de estas temáticas, en promedio en el 70% de las entidades del sector de Banca Comercial o Múltiple de México se tiene una única área responsable por la seguridad digital, valor promedio similar al registrado en los bancos de la región de América Latina y el Caribe, en el cual el 74% tiene esta misma condición (Organización de los Estados Americanos, 2018).

- Respecto al apoyo a la gestión del riesgo de seguridad de la información (incluyendo ciberseguridad) por parte de la alta dirección de la entidad / institución financiera, se destaca que un 58% del total de las entidades e instituciones financieras del país lo demuestran fomentando la concientización, educación y capacitación, y un 49% impulsando planes de seguridad de la información. Particularmente, en el sector de

1. Las entidades e instituciones financieras participantes tienen un total de activos cercanos a los USD $682.398 millones de dólares (aproximadamente un 87% del total de activos de los sectores analizados), acumulan utilidades netas por USD $7.150 millones de dólares (31 de diciembre de 2018) y según su tamaño se distribuyen así: 3% entidades grandes, 22% entidades medianas y 75% entidades pequeñas; según su composición son: 78% entidades privadas, 15% entidades públicas y 6% entidades mixtas.

Banca Comercial o Múltiple de México, se resalta que un 73% del total de las entidades bancarias del país lo demuestran impulsando planes de seguridad de la información y un 55% fomentando la concientización, educación y capacitación y asignando mayor presupuesto, mientras que en el sector bancario de América Latina y el Caribe, es más común que se haga exigiendo la adopción de buenas prácticas de seguridad (65%), fomentando la capacitación y sensibilización en seguridad digital (63%) e impulsando planes de seguridad digital (60%) (Organización de los Estados Americanos, 2018).

- En el 50% de las entidades e instituciones financieras de México, la junta directiva recibe reportes periódicos acerca de riesgos de seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales, mientras el 65% de quienes atendieron la encuesta considera que lograr que la alta dirección de la organización invierta en soluciones de seguridad digital es medianamente o muy complejo, a pesar de la relevancia que tienen las inversiones especialmente en materia de prevención y desarrollo de capacidades. En este mismo sentido, al comparar el sector de Banca Comercial o Múltiple de México con el promedio de la región de América Latina y el Caribe, se observa que en dicho sector, en el 85% de las entidades bancarias la junta directiva recibe reportes periódicos acerca de riesgos de seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales, cifra superior a la reportada en la región (72%) (Organización de los Estados Americanos, 2018).

- Dentro de los marcos de seguridad y/o estándares internacionales más implementados en las entidades e instituciones financieras, se encuentran Information Security Management System (ISMS) – ISO/IEC 27001 e Information Technology Infrastructure Library (ITIL) & IT Service Management (ITSM) (en el 27% y 15% de las entidades financieras, respectivamente).

- En materia de conformación de equipos de profesionales de seguridad de la información (incluyendo ciberseguridad) por cada entidad / institución financiera en México, se observa que éstos se componen en promedio de nueve (9) miembros. No obstante, este valor varía dependiendo del tamaño de la entidad.

- Se resalta que el 68% de entidades e instituciones financieras encuestadas en el país considera adecuado que el equipo creciera en el corto plazo, lo cual es un reconocimiento a necesidades de gestión crecientes en los aspectos a su cargo. Estas necesidades crecientes llevan en muchos casos a requerir procesos de tercerización, siendo la actividad que más frecuentemente se contrata la relativa a la realización de pruebas de seguridad / análisis de vulnerabilidades con un 34% del total, seguida del monitoreo de la infraestructura de seguridad con un 31% del total.

- En cuanto a capacidades de detección y análisis de eventos de seguridad de la información (incluyendo ciberseguridad), que son vitales para la gestión sistemática de este tipo de riesgos, porcentajes entre el 75% y del 85% de entidades e instituciones financieras del país se centran en la implementación de los cortafuegos (firewalls) y la actualización automatizada de antivirus. Temas como la aplicación de Inteligencia Artificial y computación cognitiva para la detección y análisis de eventos de seguridad se encuentran aún muy incipientes con niveles inferiores al 10% de entidades e instituciones financieras.

- Los riesgos de seguridad de la información que consideran que merecen mayor atención por parte de las entidades e instituciones financieras de México, sin importar el tamaño de la organización, son i) la pérdida / robo de activos de información clasificada (confidencial o sensible), ii) el secuestro de información, y iii) el compromiso de credenciales de usuarios privilegiados.

• El 100% de las entidades e instituciones financieras de México manifiestan que identificaron algún tipo de evento (ataques exitosos y ataques no exitosos) de seguridad digital en su contra. Los eventos de seguridad digital más comúnmente identificados durante el año 2018 son: i) el código malicioso o malware (56% del total de entidades), ii) el phishing dirigido para tener acceso a sistemas de la entidad (47% del total de entidades) y iii) la violación de políticas de escritorio limpio (clear desk) (31% del total de entidades). Se destaca que un 19% de las entidades e instituciones financieras identifican ocurrencia de eventos de malware diariamente.

• Según las entidades e instituciones financieras en México, el tipo de eventos (ataques exitosos y ataques no exitosos) de seguridad digital que usan los ciberdelincuentes con más frecuencia contra los clientes (socios, asociados o usuarios) de servicios financieros son: i) Phishing, ii) Software espía (Malware o troyanos), y iii) Ingeniería social. También resulta importante anotar que dentro de las principales motivaciones para la realización de estos ataques se encuentran las económicas (74%), y en una menor medida las políticas, el hacktivismo, la reputación personal como hackers y el robo de información personal.

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

• Como parte de las estrategias de gestión de riesgos de seguridad digital, en promedio, el 40% de las entidades financieras realizan evaluación de madurez bajo alguna metodología de seguridad de la información. Aquellas entidades e instituciones financieras que no logran hacer este tipo de evaluaciones señalan que las principales razones son: i) insuficiencia de personal especializado (39% de entidades sin evaluación), y ii) falta de asignación de presupuesto (28% de entidades sin evaluación).

• En cuanto a la comunicación de incidentes de seguridad digital, la mayoría (55% de las entidades financieras) ofrece un mecanismo para que sus usuarios internos (empleados y contratistas) reporten incidentes (ataques exitosos) de seguridad digital sufridos y el 41% cuenta con un plan de comunicaciones que permita informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida. El 44% de las entidades financieras reporta los ataques sufridos ante una autoridad de procuración de justicia en México.

• En materia de capacitación y concientización, el 57% de entidades e instituciones financieras cuenta con planes de preparación, respuesta y capacitación en asuntos de seguridad de la información (incluyendo ciberseguridad) para sus colaboradores, los cuales se ejecutan en su mayoría anualmente. El mecanismo más efectivo a partir del cual se ha generado mayor conciencia en las entidades financieras respecto de los riesgos de seguridad digital es a través de medios de comunicación internos y el desarrollo de capacitaciones internas.

• En promedio, el retorno sobre la inversión en seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales equivale aproximadamente a 10,94%, lo que la mayoría considera que es un retorno de alta rentabilidad.

• 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 e instituciones financieras en México en 2018 fue de USD$ 107 millones aproximadamente.

Cuadro 1. Principales resultados por tamaño de entidad / institución financiera del Sistema Financiero Mexicano

ENTIDADES / INSTITUCIONES FINANCIERAS GRANDES	ENTIDADES / INSTITUCIONES FINANCIERAS MEDIANAS	ENTIDADES / INSTITUCIONES FINANCIERAS PEQUEÑAS
En el 57% existe una única área responsable de la seguridad digital	En el 53% existe una única área responsable de la seguridad digital	En el 76% existe una única área responsable de la seguridad digital
En el 50% existen dos (2) niveles jerárquicos entre el CEO y el máximo responsable de la seguridad digital	En el 54% existe un (1) nivel jerárquico entre el CEO y el máximo responsable de la seguridad digital	En el 60% existe un (1) nivel jerárquico entre el CEO y el máximo responsable de la seguridad digital
La mayoría de las entidades grandes (29%) cuenta con un equipo conformado por 121-300 miembros	La mayoría de las entidades medianas (75%) cuenta con un equipo conformado por 1-5 miembros	La mayoría de las entidades pequeñas (93%) cuenta con un equipo conformado por 1-5 miembros
Son objeto de ataques de todo tipo de eventos de seguridad digital, resaltando identificación de casi todos por la mayoría en el país	Son objeto de ataques de todo tipo de eventos de seguridad digital, resaltando identificación de algunos por la mayoría en el país	Son objeto de ataques de algunos tipos de eventos de seguridad digital, resaltando identificación de pocos por la mayoría en el país
El 43% identifican ocurrencia de eventos de malware diariamente	El 24% identifican ocurrencia de eventos de malware diariamente	El 14% identifican ocurrencia de eventos de malware diariamente
La mayoría (71%) detecta entre un 61% y un 80% de eventos con sistemas propios	La mayoría (43%) detecta entre un 0% y un 20% de eventos con sistemas propios	La mayoría (58%) detecta entre un 0% y un 20% de eventos con sistemas propios
El 43% manifiestan que han sido víctimas de ataques exitosos	El 15% manifiestan que han sido víctimas de ataques exitosos	El 6% manifiestan que han sido víctimas de ataques exitosos
El 43% realiza evaluación de madurez y adelanta las acciones correspondientes	El 30% realiza evaluación de madurez y adelanta las acciones correspondientes	El 19% realiza una evaluación de madurez y adelanta las acciones correspondientes
El 86% ofrece un mecanismo para que sus clientes reporten a la entidad incidentes (ataques exitosos) sufridos	El 40% ofrece un mecanismo para que sus clientes reporten a la entidad incidentes (ataques exitosos) sufridos	El 36% ofrece un mecanismo para que sus clientes reporten a la entidad incidentes (ataques exitosos) sufridos
El 100% cuenta con un plan de comunicaciones para informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida	El 34% cuenta con un plan de comunicaciones para informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida	El 41% cuenta con un plan de comunicaciones para informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida
El 71% reporta los incidentes sufridos ante autoridades de procuración de justicia en México	El 64% reporta los incidentes sufridos ante autoridades de procuración de justicia en México	El 37% reporta los incidentes sufridos ante autoridades de procuración de justicia en México
El 20% manifiesta que el presupuesto de seguridad digital equivale en promedio a menos del 1% del EBITDA del anterior año fiscal	El 47% manifiesta que el presupuesto de seguridad digital equivale en promedio a menos del 1% del EBITDA del anterior año fiscal	El 55% manifiesta que el presupuesto de seguridad digital equivale en promedio a menos del 1% del EBITDA del anterior año fiscal

ENTIDADES / INSTITUCIONES FINANCIERAS GRANDES	ENTIDADES / INSTITUCIONES FINANCIERAS MEDIANAS	ENTIDADES / INSTITUCIONES FINANCIERAS PEQUEÑAS
El presupuesto destinado a la seguridad digital equivale aprox. al 2,30% del EBITDA del año inmediato anterior	El presupuesto destinado a la seguridad digital equivale aprox. al 2,51% del EBITDA del año inmediato anterior	El presupuesto destinado a la seguridad digital equivale aprox. al 2,04% del EBITDA del año inmediato anterior
En el 57% el presupuesto de seguridad digital aumentó en comparación al año fiscal inmediato anterior	En el 43% el presupuesto de seguridad digital aumentó en comparación al año fiscal inmediato anterior	En el 35% el presupuesto de seguridad digital aumentó en comparación al año fiscal inmediato anterior
El presupuesto asignado en 2018 a un miembro promedio del equipo de seguridad digital equivale aproximadamente a US $67.674	El presupuesto asignado en 2018 a un miembro promedio del equipo de seguridad digital equivale aproximadamente a US $49.453	El presupuesto asignado en 2018 a un miembro promedio del equipo de seguridad digital equivale aproximadamente a US $12.488
El retorno sobre la inversión en seguridad digital equivale aproximadamente a un 15,00%	El retorno sobre la inversión en seguridad digital equivale aproximadamente a un 9,58%	El retorno sobre la inversión en seguridad digital equivale aproximadamente a un 10,36%
El 100% manifiesta que el costo total de respuesta y de recuperación ante incidentes equivale en promedio a menos del 1% del EBITDA del anterior año fiscal	El 71% manifiesta que el costo total de respuesta y de recuperación ante incidentes equivale en promedio a menos del 1% del EBITDA del anterior año fiscal	El 59% manifiesta que el costo total de respuesta y de recuperación ante incidentes equivale en promedio a menos del 1% del EBITDA del anterior año fiscal
El costo total de respuesta y de recuperación ante incidentes de seguridad digital por entidad en 2017 equivale aprox. al 1,00% del EBITDA del año inmediato anterior (USD $ 2.357.221 en 2018 aprox.)	El costo total de respuesta y de recuperación ante incidentes de seguridad digital por entidad en 2017 equivale aprox. al 1,54% del EBITDA del año inmediato anterior (USD $634.689 en 2018 aprox.)	El costo total de respuesta y de recuperación ante incidentes de seguridad digital por entidad en 2017 equivale aprox. al 1,73% del EBITDA del año inmediato anterior (USD $317.615 en 2018 aprox.)

El detalle del estudio puede apreciarse en el capítulo 3 de este documento, el cual desarrolla en profundidad los hallazgos enunciados y muchos otros aspectos que pueden resultar de interés.

PRÓLOGO

Luis Almagro
Secretario General
Organización de Estados Americanos

OEA Más derechos para más gente

La Secretaría General de la Organización de los Estados Americanos (OEA) a través del Programa de Ciberseguridad adscrito al Comité Interamericano contra el Terrorismo (CICTE), promueve y coordina la cooperación entre sus Estados miembros –como el Sistema Interamericano y otros organismos del sistema internacional- con el fin de acceder, prevenir, y responder a las amenazas a la seguridad del mundo digital.

El objetivo del Programa de Ciberseguridad es ser el principal punto de referencia en el Hemisferio Occidental para desarrollar la cooperación y la creación de capacidades en los Estados miembros de la OEA

El sector financiero ha experimentado uno de los mayores índices de digitalización en los últimos años. Cada día un mayor número de clientes del sector financiero usan medios no presenciales para realizar sus trámites, realizan transacciones por internet o pagos a través de dispositivos móviles.

Esta adaptación a nuevos modelos negocio y la explotación de canales digitales pretende 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.

El estudio presenta los resultados y análisis sobre los incidentes de seguridad de la información (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales), producto de las encuestas realizadas a diversas entidades e instituciones financieras del Sistema Financiero Mexicano.

Se basa en la recolección de información de tres secciones, la primera analiza los perfiles de las instituciones financieras; la segunda se ocupa de aspectos asociados a la gestión de riesgos de seguridad digital y la tercera aborda aspectos relacionados con el impacto de los incidentes en las mismas.

La OEA agradece a la Comisión Nacional Bancaria y de Valores (CNBV) el apoyo y las facilidades brindadas para el acercamiento con las entidades financieras que participaron del estudio. Gracias a los aportes brindados por las instituciones financieras mexicanas, así como del apoyo de la CNBV, el equipo técnico de la OEA pudo preparar el reporte que está en sus manos.

A partir de lo anterior, así como de las investigaciones realizadas con soporte en diferentes referentes abordados en el estudio, se pretende ofrecer conclusiones y recomendaciones pertinentes al Sistema Financiero Mexicano, así como a las autoridades y organismos reguladores del sistema financiero y a las autoridades de procuración de justicia del Gobierno de México con miras a contar con un entorno digital más confiable y seguro para los servicios ofrecidos por este vital sector para dicho país.

Adalberto Palma Gómez

Presidente

Comisión Nacional Bancaria y de Valores

COMISIÓN NACIONAL BANCARIA Y DE VALORES

La Comisión Nacional Bancaria y de Valores (CNBV) tiene como misión supervisar y regular a las entidades integrantes del sistema financiero en México, a fin de procurar su estabilidad y correcto funcionamiento, así como mantener y fomentar el sano y equilibrado desarrollo de dicho sistema en su conjunto, en protección de los intereses de los usuarios.

Las amenazas cibernéticas, al ser cada vez más organizadas, frecuentes, disruptivas y con un mayor alcance, representan un riesgo creciente para la estabilidad de los sistemas financieros en todo el mundo, alimentadas por diversas motivaciones: económicas, políticas (hacktivismo) o personales.

Por ello, la CNBV considera como un elemento fundamental para el logro de su misión, el realizar los esfuerzos necesarios para promover un sistema financiero más preparado y resiliente ante ciberataques, así mismo trabaja continuamente en la actualización de requerimientos normativos aplicables a las entidades supervisadas, en la mejora de las políticas, controles, procesos y cultura de ciberseguridad, además de la supervisión en materia de seguridad de la información.

La industria financiera, junto con el sector Gobierno, se encuentran históricamente entre los más atacados y los costos van en aumento.

El factor humano sigue siendo uno de los eslabones más débiles; el 64% de las organizaciones en Estados Unidos declara haber sufrido eventos de Phishing[2] y declaran sentirse vulnerables ante nuevas tecnologías (Nube, IoT) y amenazas (particularmente el ransomware).

En los últimos dos años, entidades financieras en México han sufrido con mayor frecuencia, ataques a las infraestructuras de pagos y cajeros automáticos que han representado pérdidas por montos significativos.

2. CheckPoint 2018 Security Report

La Organización de Estados Americanos (OEA), a través del "Programa de Ciberseguridad" del Comité Inter-Americano contra el terrorismo (CICTE) ha realizado un análisis de la situación en ciberseguridad de México, que ayudó a la Presidencia de la República al lanzamiento, en 2017, de la Estrategia Nacional de Ciberseguridad (ENC).

En enero de 2018, el CICTE solicitó apoyo para pedir a los bancos su participación en el "Estudio sobre la Ciberseguridad en el sector bancario de América Latina y el Caribe," conducido por la OEA mediante un cuestionario en línea, el cual fue atendido por 35 de los 51 bancos en México.

A fin de profundizar en la situación particular de México, se inició en 2018 una nueva encuesta por parte de la OEA dirigida a entidades financieras, incluyendo sectores relevantes en adición a las instituciones de crédito, tales como cooperativas de ahorro y préstamo, sociedades financieras populares, uniones de crédito, casas de bolsa y de tecnología financiera (Fintechs).

La información contenida en el reporte que aquí se presenta, resultado de dicha encuesta, así como los datos desagregados por sector, serán de gran utilidad, para identificar, de manera amplia, los sectores y las áreas de oportunidad para orientar los esfuerzos de la CNBV, de manera que los recursos sean utilizados eficientemente en el desempeño de sus facultades de supervisión y regulación en materia de seguridad de la información.

Desde la CNBV se reconocen y aprecian los esfuerzos realizados por la OEA en los últimos años, cuyos resultados enriquecen las funciones de esta Comisión.

CIBERSEGURIDAD EN LAS ENTIDADES E INSTITUCIONES DEL SISTEMA FINANCIERO MEXICANO

Según el Informe Global de Riesgos del Foro Económico Mundial 2019, *los ataques cibernéticos a gran escala y el desglose de las redes y la infraestructura esencial de la información (colapso de la infraestructura de información esencial)* son considerados riesgos tecnológicos a escala mundial que, si se producen, pueden tener un impacto negativo significativo en varios países e industrias dentro de los próximos diez años. *"La tecnología sigue desempeñando una función profunda en la conformación del panorama de riesgos mundiales para individuos, gobiernos y compañías. En la GRPS, el "fraude y robo de datos masivo" se ubicó en el número cuatro de riesgo mundial por probabilidad, en un lapso de 10 años, con los "ataques cibernéticos" situados en el número cinco. Esto mantiene un patrón que se registró el año pasado, con la consolidación de la posición de los riesgos cibernéticos junto a los riesgos ambientales en el cuadrante de alto impacto y alta probabilidad del panorama de riesgos mundiales."* (WEF, 2019).

Estos riesgos son actualmente gestionados por sectores altamente digitalizados como el sector financiero que a su vez afronta grandes retos estructurales bajo fuertes procesos de transformación digital. De esta manera, la ciberseguridad es un aspecto crítico actualmente y las entidades e instituciones financieras tienen que estar preparados para recibir ataques sin precedentes que no sólo pretenderán obtener sus recursos económicos y los de sus clientes (socios, asociados o usuarios) sino también y cada vez más información sobre estos últimos.

En particular, el Sistema Financiero Mexicano está integrado por: i) autoridades y órganos reguladores del sistema financiero, ii) entidades e instituciones financieras de diversos sectores que brindan atención a los diferentes segmentos de la población y iii) instrumentos (activos financieros) y mercados financieros.

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

Gráfica 1. Autoridades del Sistema Financiero Mexicano

Fuente: SG/OEA a partir de información recolectada de CNBV

A continuación, las autoridades y órganos que actualmente conforman dicho sistema en México:

- *Secretaría de Hacienda y Crédito Público (SHCP):* tiene como misión proponer, dirigir y controlar la política del Gobierno Federal en materia financiera, fiscal, de gasto, de ingresos y deuda pública, con el propósito de consolidar un país con crecimiento económico de calidad, equitativo, incluyente y sostenido, que fortalezca el bienestar de los mexicanos.

- *Comisión Nacional Bancaria y de Valores (CNBV):* es un órgano desconcentrado de la SHCP, con facultades en materia de autorización, regulación, supervisión y sanción sobre los diversos sectores y entidades que integran el Sistema Financiero Mexicano, así como sobre aquellas personas físicas y morales que realicen actividades previstas en las leyes relativas al sistema financiero.

- *Comisión Nacional de Seguros y Fianzas (CNSF):* es un Órgano Desconcentrado de la SHCP, encargada de supervisar que la operación de los sectores asegurador y afianzador se apegue al marco normativo, preservando la solvencia y estabilidad financiera de las instituciones de Seguros y Fianzas, para garantizar los intereses del público usuario, así como promover el sano desarrollo de estos sectores con el propósito de extender la cobertura de sus servicios a la mayor parte posible de la población.

- *Comisión Nacional de Sistemas de Ahorro para el Retiro (CONSAR):* su labor fundamental es la de regular el Sistema de Ahorro para el Retiro (SAR) que está constituido por las cuentas individuales a nombre de los trabajadores que manejan las Administradoras de Fondos para el Retiro (AFORE).

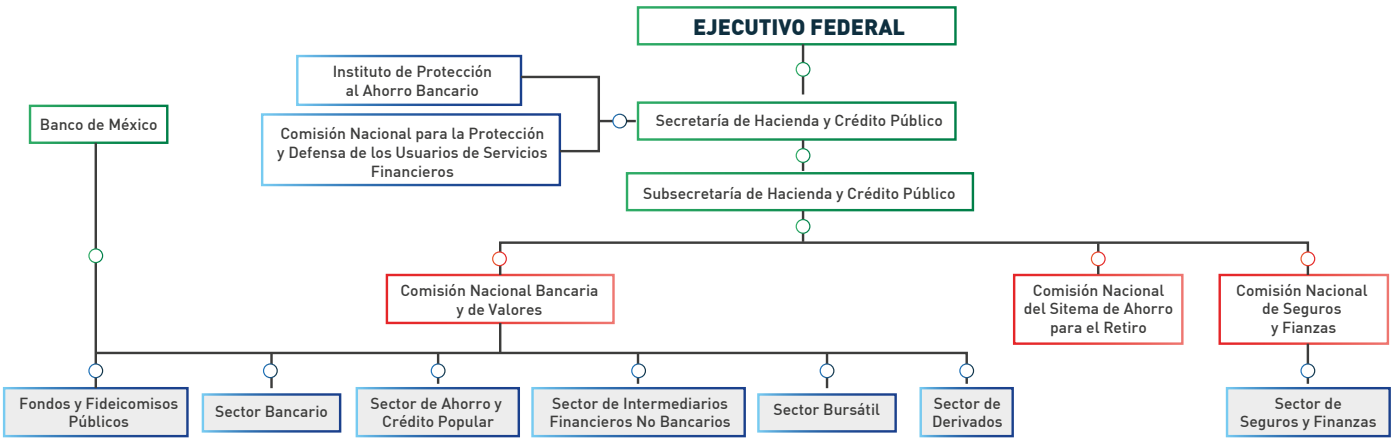
- *Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF):* es una institución pública dependiente de la Secretaría de Hacienda y Crédito Público, que defiende y promueve los derechos e intereses de los mexicanos como usuarios de productos y servicios financieros, además de fomentar la educación financiera.

- *Instituto para la Protección al Ahorro Bancario (IPAB):* es la institución del Gobierno Federal encargada de administrar el Seguro de Depósitos Bancarios en beneficio y protección de los ahorradores mexicanos.

- *Servicio de Administración Tributaria (SAT):* es un órgano descentralizado que depende de la SHCP, a partir del cual se llevan a cabo tareas específicas para poder dar aplicación a la legislación fiscal y aduanera a las personas físicas y morales del país.

Por otra parte, las entidades e instituciones entidades e instituciones financieras captan, administran y canalizan los recursos financieros y dirigen el ahorro y la inversión de los mexicanos en diversos sectores tales como: el Sector Bancario, el Sector de Ahorro y Crédito Popular, el Sector de Intermediarios Financieros No Bancarios, el Sector Bursátil, entre otros.

Gráfica 2. Sectores del Sistema Financiero Mexicano



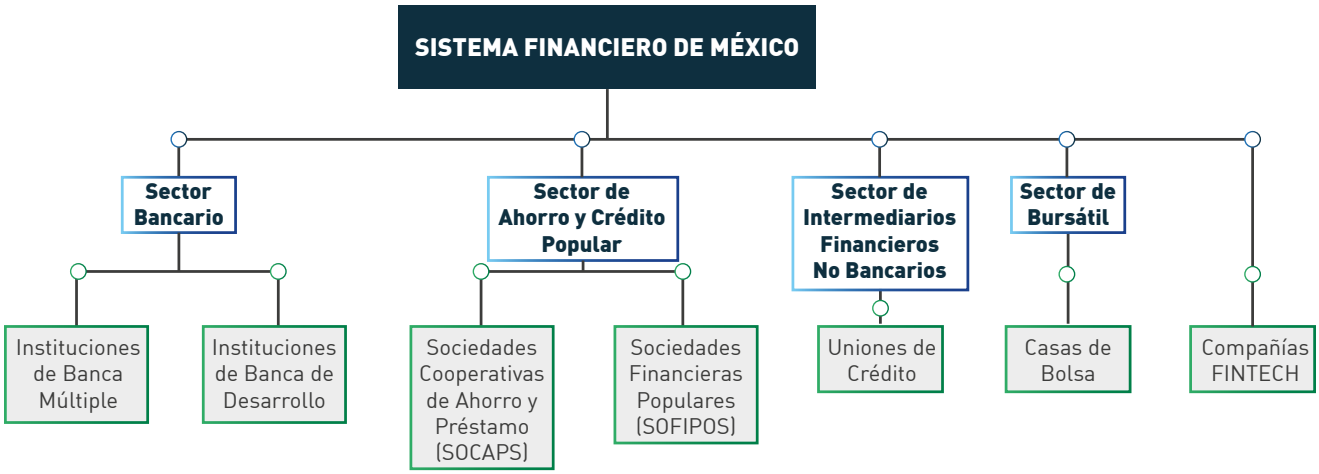
Fuente: SG/OEA a partir de información recolectada de CNBV

A continuación, las entidades e instituciones financieras del Sistema Financiero Mexicano consideradas para el presente reporte:

- Instituciones de Banca Múltiple (Sector Bancario)
- Instituciones de Banca de Desarrollo (Sector Bancario)
- Sociedades Cooperativas de Ahorro y Préstamo -SOCAP- (Sector de Ahorro y Crédito Popular)
- Sociedades Financieras Populares -SOFIPO- (Sector de Ahorro y Crédito Popular)
- Uniones de Crédito (Sector de Intermediarios Financieros No Bancarios)
- Casas de Bolsa (Sector Bursátil)
- Compañías FINTECH[3]

3.El presente reporte incluye este tipo de entidad / institución financiera teniendo en cuenta que la CNBV autoriza, regula y supervisa a las instituciones de tecnología financiera (ITF) creadas por la Ley para Regular las Instituciones de Tecnología Financiera y que reforma, adiciona o deroga disposiciones de diversas leyes financieras, aprobada por el Congreso y el Decreto y publicada en el Diario Oficial el 9 de marzo de 2018 (Ley FinTech).

Gráfica 3. Muestra de las entidades e instituciones del Sistema Financiero Mexicano para el desarrollo del reporte



Fuente: SG/OEA a partir de información recolectada de CNBV

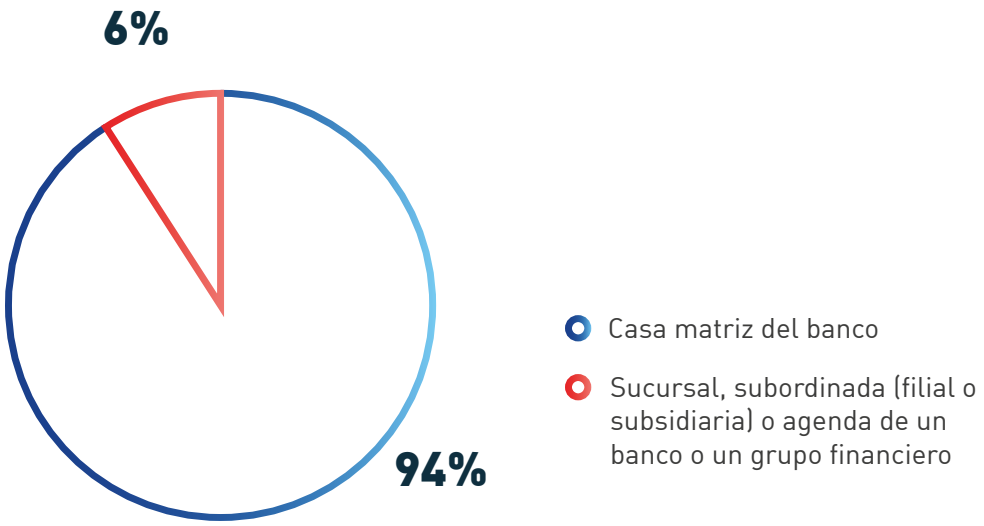
3.1. Caracterización de la entidad / institución financiera

De un total de 282 respuestas obtenidas durante el periodo de publicación del instrumento de recolección de información (meses comprendidos durante el cuarto trimestre del año 2018), se estableció una base de datos con registros de 240 entidades e instituciones financieras con cubrimiento en las treinta y dos (32) entidades federativas de México. Se estima que la muestra de entidades e instituciones financieras a partir de las cuales se presentan los resultados de este estudio alcanza unos activos de USD $682.398 millones de dólares y unas utilidades netas de USD $7.150 millones de dólares a 31 de diciembre de 2018.

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

De esta manera, el 94% de las entidades e instituciones financieras entrevistadas corresponden a casa matriz de la entidad / institución financiera o de un grupo financiero, mientras que el 6% corresponden a una sucursal, subordinada (filial o subsidiaria), oficina de representación o agencia de la entidad / institución financiera o de un grupo financiero.

Gráfica 4. Casa Matriz o Sucursal, Subordinada, oficina de representación o agencia de la entidad / institución financiera o de un grupo financiero



Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

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

A continuación, se presenta la clasificación de las 240 entidades e instituciones financieras considerando la cantidad de empleados y de sucursales que tiene la entidad a la cual pertenecía el funcionario que rellenó el cuestionario (en el estado federativo en el que se encontraba). Por ejemplo, del total de la muestra se aprecia que 84 entidades e instituciones financieras tienen menos de 300 empleados y poseen hasta 10 sucursales o que 4 entidades tienen más de 5.000 empleados y poseen más de 151 sucursales.

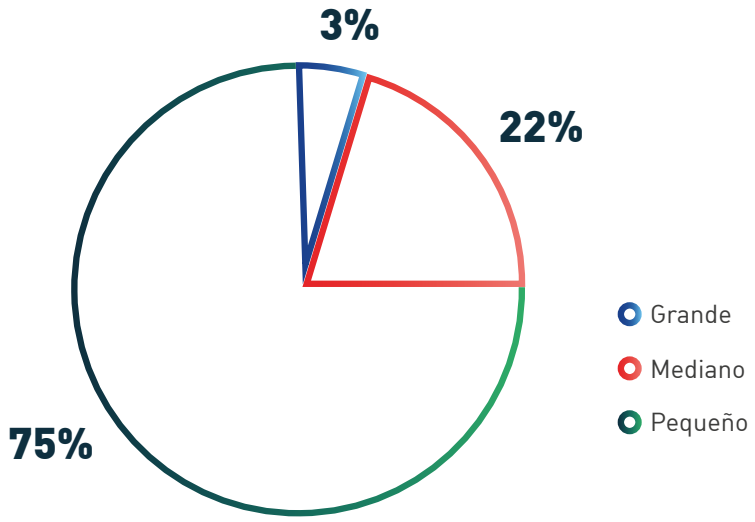
Cuadro 2. Distribución de las entidades e instituciones financieras por cantidad de empleados y de sucursales

Cantidad de Empleados	Cantidad de Sucursales					
	Sin sucursales	Hasta 10 sucursales	De 11 a 50 sucursales	De 51 a 150 sucursales	Más de 151 sucursales	Total
Hasta 300 empleados	89	84	23	2		198
Entre 301 y 999 empleados	2	5	11	3		21
Entre 1.000 y 4.999 empleados	3	1	6	4	2	16
Más de 5.000 empleados			1		4	5
TOTAL	**94**	**90**	**41**	**9**	**6**	**240**

Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Con la información anterior, las entidades e instituciones financieras se clasifican por tamaño así: el 75% de la muestra se consideran como entidades pequeñas, el 22% como entidades medianas y el 3% como entidades grandes. Esta clasificación es primordial ya que todo el análisis, las conclusiones y las recomendaciones respecto de la gestión de riesgos de seguridad digital y del impacto de los incidentes de seguridad digital en el presente capítulo tienen en cuenta el tamaño de la organización.

Gráfica 5. Distribución de las entidades e instituciones financieras por tamaño (grandes, medianas y pequeñas)



Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

De esta manera, se aprecia que el 47% del total de entidades e instituciones financieras entrevistadas presta servicios en el sector de ahorro y crédito popular (Sector de Ahorro y Crédito Popular -SOCAP- y Sector de Ahorro y Crédito Popular -SOFIPO-), el 25% del total presta servicios en el sector de intermediarios financieros no bancarios, el 18% del total presta servicios en el sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo), el 7% del total presta servicios en el sector FINTECH y el 4% del total presta servicios en el sector bursátil.

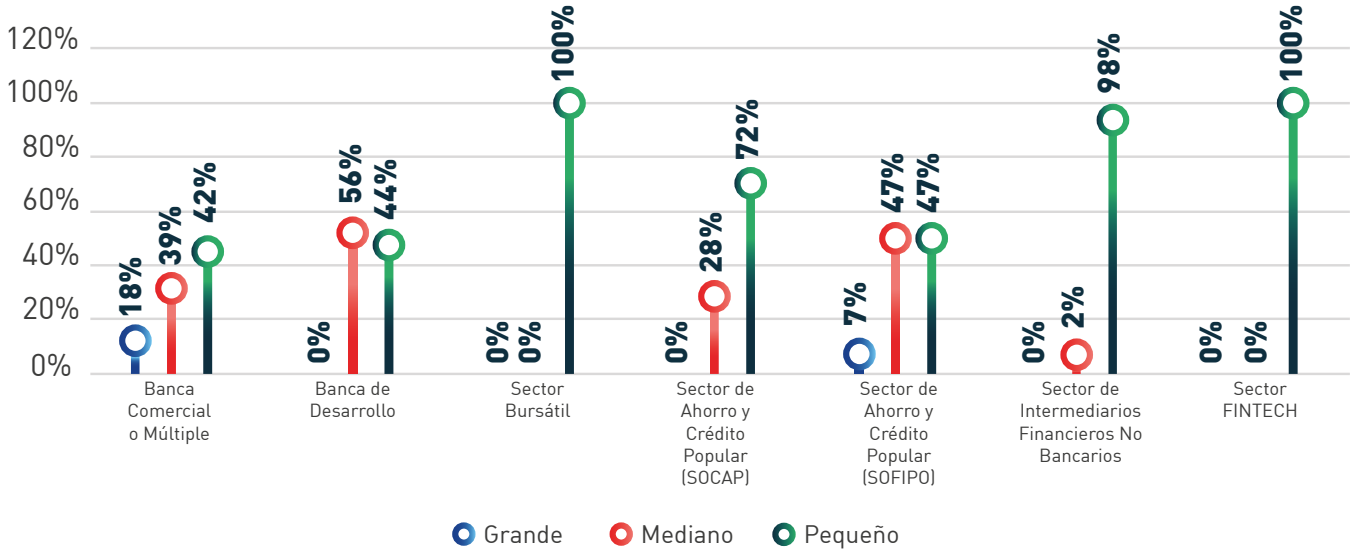
Cuadro 3. Distribución de las entidades e instituciones financieras por tipo de actor

	Grande	Mediana	Pequeña	Total	%
Banca Comercial o Múltiple	6	13	14	33	14%
Banca de Desarrollo		5	4	9	4%
Sector Bursátil			9	9	4%
Sector de Ahorro y Crédito Popular (SOCAP)		27	71	98	41%
Sector de Ahorro y Crédito Popular (SOFIPO)	1	7	7	15	6%
Sector de Intermediarios Financieros No Bancarios		1	58	59	25%
Sector FINTECH			17	17	7%
SISTEMA FINANCIERO MEXICANO	7	53	180	240	100%

Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Al analizar por tamaño de entidad y por tipo de sector se aprecia que existe representatividad para las tres (3) categorías de tamaño (grande, mediana y pequeña) para los bancos comerciales o múltiples y para las sociedades financieras populares (SOFIPOs). Por su parte existe representatividad de entidad mediana y pequeña para los bancos de desarrollo, las sociedades cooperativas de ahorro y préstamo (SOCAPs) y las uniones de crédito. Finalmente, en la muestra se obtuvo respuesta de casas de bolsa y compañía FINTECH de tamaño pequeña.

Gráfica 6. Tipo de actor en la muestra del Sistema Financiero Mexicano



Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Del total de la muestra, se estima que las entidades e instituciones financieras encuestadas prestan sus servicios a más de 46 millones de clientes (socios, asociados o usuarios) de servicios financieros en el país. Se destaca que el 78% de dichos clientes son usuarios de servicios de banca comercial o múltiple.

Cuadro 4. Distribución de los clientes (socios, asociados o usuarios) de servicios financieros de la muestra

	Grande	Mediana	Pequeña	Total
Banca Comercial o Múltiple	26.500.000	9.528.000	59.500	36.087.500
Banca de Desarrollo		4.807.000	20.000	4.827.000
Sector Bursátil			74.500	74.500
Sector de Ahorro y Crédito Popular (SOCAP)		2.328.000	1.821.500	4.149.500
Sector de Ahorro y Crédito Popular (SOFIPO)	500.000	475.000	15.500	990.500
Sector de Intermediarios Financieros No Bancarios		1.000	76.500	77.500
Sector FINTECH			169.500	169.500
SISTEMA FINANCIERO MEXICANO	27.000.000	17.139.000	2.237.000	46.376.000

Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Teniendo en cuenta el tipo de capital de la entidad / institución financiera al cual pertenece el empleado que respondió la encuesta, se aprecia que el 78% del total de la muestra son entidades e instituciones financieras privadas (100% de capital privado), el 15% son entidades e instituciones financieras públicas (100% de capital público) y el 6% son entidades e instituciones financieras mixtas (compuesto por capital tanto público como privado).

Al analizar por tamaño, el 100% de las entidades e instituciones financieras grandes son entidades e instituciones financieras privadas mientras que tan sólo el 17% de las entidades e instituciones financieras medianas son públicas. Al analizar por tamaño, se destaca que el 14% de las entidades e instituciones financieras grandes tienen capital compuesto por capital tanto público como privado, mientras que el 6% de las entidades e instituciones financieras medianas y el 6% de las entidades e instituciones financieras pequeñas tienen capital mixto.

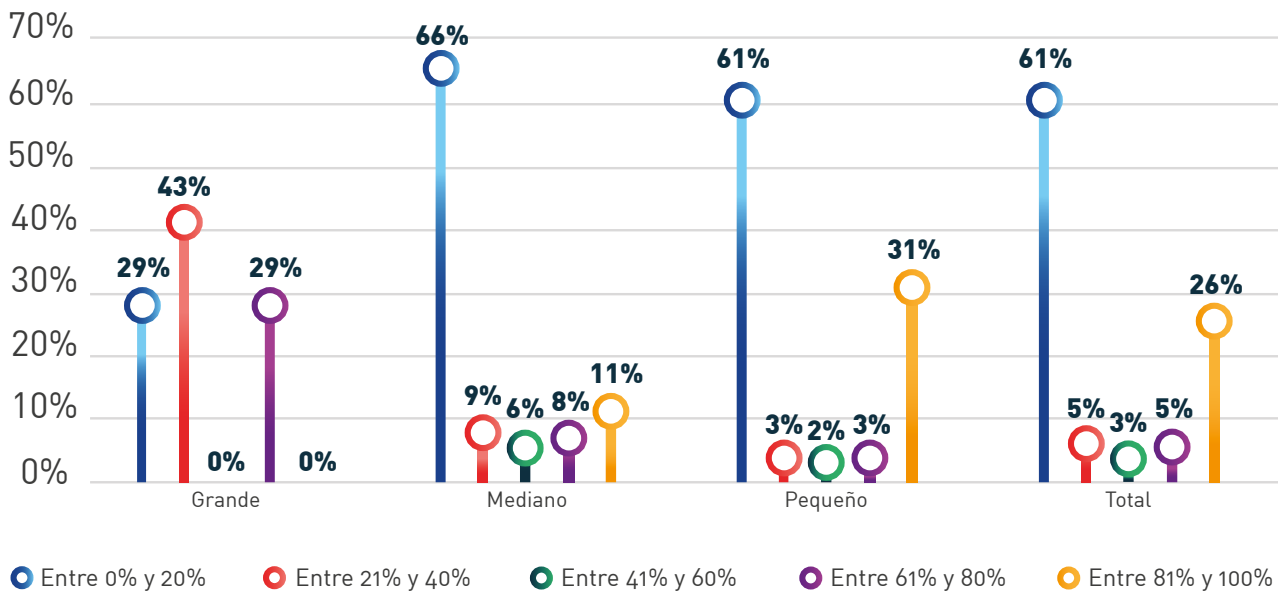
Ahora, el 95% de las entidades e instituciones financieras entrevistadas tienen mayoría del capital social de origen nacional, mientras que tan sólo el 5% de las mismas tienen capital con mayoría de recursos de origen extranjero.

Al analizar el porcentaje de operaciones que se realizan en la entidad / institución financiera por medio de canales transaccionales no presenciales (Internet, transacciones electrónicas, cajeros automáticos, pagos automáticos, aplicaciones móviles y audio respuesta -IVR-) del total de operaciones de la entidad durante el año 2018, se aprecia que el 61% de las entidades e instituciones financieras de la muestra tienen entre un 0% y un 20% de sus operaciones por medio de canales transaccionales no presenciales.

Al analizar por tamaño de las entidades e instituciones financieras, se aprecia por ejemplo que más del 60% tanto de las entidades medianas como de las pequeñas realizan entre un 0% y 20% de sus operaciones por medio de canales transaccionales no presenciales mientras que el 29% de las entidades grandes realizan operaciones en dicho rango. Se destaca el hecho que en sectores como el de FINTECH se alcanza un promedio de 76% de entidades e instituciones financieras que realizan entre un 81% y un 100% de sus operaciones por medio de canales transaccionales no presenciales. Asimismo, se observa que en ese mismo rango de operaciones el 21% de instituciones en el sector de Banca Comercial o Múltiple realiza sus actividades por medio de canales transaccionales no presenciales[4], lo cual duplica el promedio registrado por las entidades bancarias de América Latina y el Caribe que está en el 10% (Organización de los Estados Americanos, 2018).

4. La gráfica 34 del Anexo 2 presenta la comparación del resultado Porcentaje de operaciones que se realizaron por medio de canales transaccionales no presenciales entre los diferentes sectores analizados del Sistema Financiero Mexicano.

Gráfica 7. Porcentaje de operaciones que se realizaron por medio de canales transaccionales no presenciales



Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

3.2. Gestión de riesgos de seguridad digital

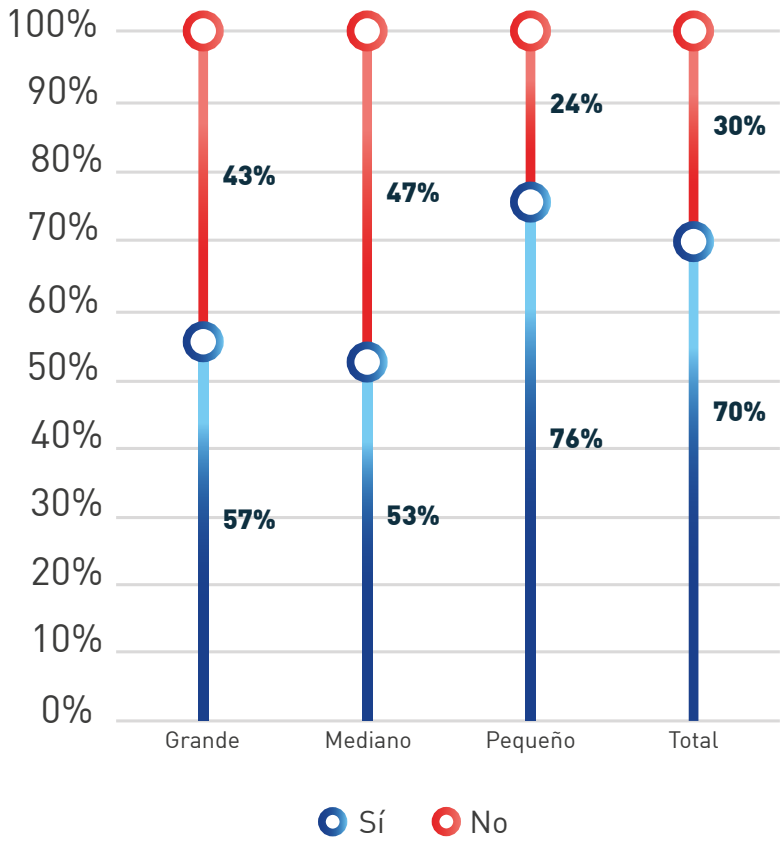
Como parte del estudio a las entidades e instituciones financieras en México, se realizaron una serie de preguntas con respecto a la gestión de riesgo de seguridad digital. Estas preguntas se formularon con el propósito de evaluar los principales aspectos y asuntos relacionados con los siguientes temas:

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

3.2.1. Preparación y gobernanza

La mayoría de las entidades e instituciones financieras entrevistadas (70%) mencionan que en su organización existe una única área responsable por la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude ocurridos a través de medios digitales. Vale la pena destacar que a medida que crece la entidad / institución financiera aumentan las áreas responsables de la seguridad digital, ya que el 76% de las entidades pequeñas tienen una única área versus el 57% de las entidades grandes.

Gráfica 8. Área única responsable de la seguridad digital en la entidad / institución financiera



Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Estas diferencias se acentúan aún más en sectores como el de Intermediarios Financieros No Bancarios donde se evidencia que en el 90% de sus entidades e instituciones financieras existe una única área responsable por la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude ocurridos a través de medios digitales[5]. Por su parte, en el 60% de las entidades e instituciones financieras del sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México existe una única área responsable mientras que en la región de América Latina y el Caribe las entidades bancarias registran un promedio del 74% (Organización de los Estados Americanos, 2018).

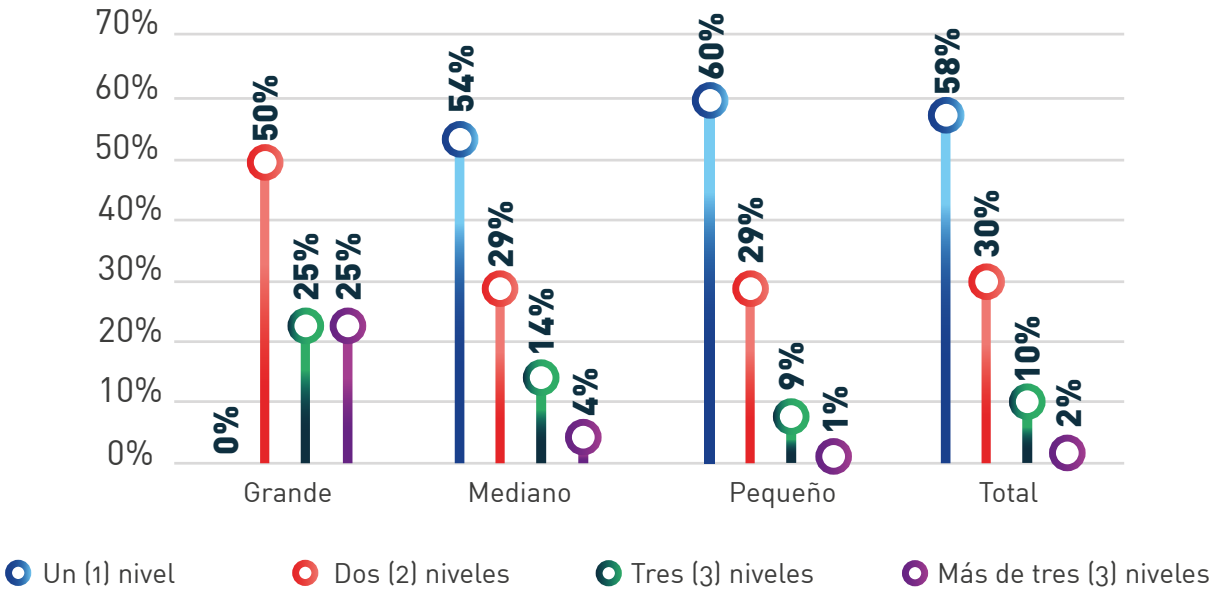
Entendiendo que el CEO (Chief Executive Officer) de la entidad / institución financiera se consideraría la cabeza de la entidad y a partir de los resultados obtenidos, se concluye que los niveles jerárquicos que existen entre el CEO y el máximo responsable de la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude ocurridos a través de medios digitales dependen también del tamaño de la organización en el país. Por ejemplo, en el 60% de las entidades pequeñas el máximo responsable reporta directamente al CEO, es decir, está a un (1) solo nivel, mientras que en ninguna entidad grande ocurre dicha situación. En el 50% de las entidades grandes existen dos (2) niveles entre el CEO y el máximo responsable de la seguridad digital. A medida que crece la entidad, 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 58% de las entidades e instituciones financieras existe un (1) nivel jerárquico entre el CEO y el máximo responsable de la seguridad digital[6].

Al comparar el sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México con el promedio de la región de América Latina y el Caribe, se observa que en dicho sector, el 33% de bancos pequeños reportan directamente al CEO, mientras que en la región se registra un promedio de 46% de bancos pequeños donde el máximo responsable de seguridad digital reporta directamente al CEO (Organización de los Estados Americanos, 2018).

5. La gráfica 35 del Anexo 2 presenta la comparación del resultado: *Área única responsable de la seguridad digital en la entidad / institución financiera* entre los diferentes sectores analizados del Sistema Financiero Mexicano.
6. La gráfica 36 del Anexo 2 presenta la comparación del resultado: *Número de niveles jerárquicos que hay entre el CEO y el máximo responsable de la seguridad digital* entre los diferentes sectores analizados del Sistema Financiero Mexicano.

Gráfica 9. Número de niveles jerárquicos que hay entre el CEO y el máximo responsable de la seguridad digital



Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

En el Sistema Financiero Mexicano, la denominación más común del cargo que tiene el máximo responsable de la seguridad de la información (incluyendo ciberseguridad) es *Oficial Principal de Seguridad de la Información* (CISO), situación que es igual para las entidades e instituciones financieras grandes (42%). Por su parte, la denominación Gerente de TI (ITM) también es común para las entidades medianas (17%) como para las pequeñas (19%). Sin embargo, dentro del sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México, así como en el sector bancario de la región América Latina y el Caribe, la denominación más común del cargo que tiene el máximo responsable de la seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) es *Oficial de Seguridad de la Información* (ISO) (Organización de los Estados Americanos, 2018).

Un aspecto importante sobre la preparación y gobernanza en torno a la seguridad digital es la tercerización de actividades relacionadas con la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude ocurridos a través de medios digitales por parte de la organización. En promedio y sin distinción por tamaño de entidad / institución financiera, los servicios más contratados con un externo de la organización son: las *Pruebas de seguridad / Análisis de vulnerabilidades* (34% del total), el *Monitoreo de la Infraestructura de Seguridad* (31% del total), la *gestión de cumplimiento regulatorio* (18%) y los *Servicios de Seguridad en la Nube* (18% del total).

Se destaca que en el sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México, la tercerización de actividades de *Pruebas de seguridad / Análisis de vulnerabilidades* llega a un 76%, coincidiendo con lo registrado en la región América Latina y Caribe, donde en promedio y sin distinción por tamaño de banco, los servicios más contratados por parte de las entidades bancarias de la región con un externo de la organización son: *las Pruebas de Seguridad* (65% del total).

Con respecto del tamaño del equipo que maneja procesos asociados a la seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales, se aprecia que en promedio una entidad / institución financiera en México cuenta con un equipo conformado por nueve (9) personas. No obstante, este valor varía significativamente dependiendo del tamaño y sector de la entidad, pues mientras en la Banca Comercial el promedio es de treinta y siete (37) profesionales, en sectores como el de Ahorro y Crédito Popular (SOCAP y SOFIPO) es tan solo de tres (3).

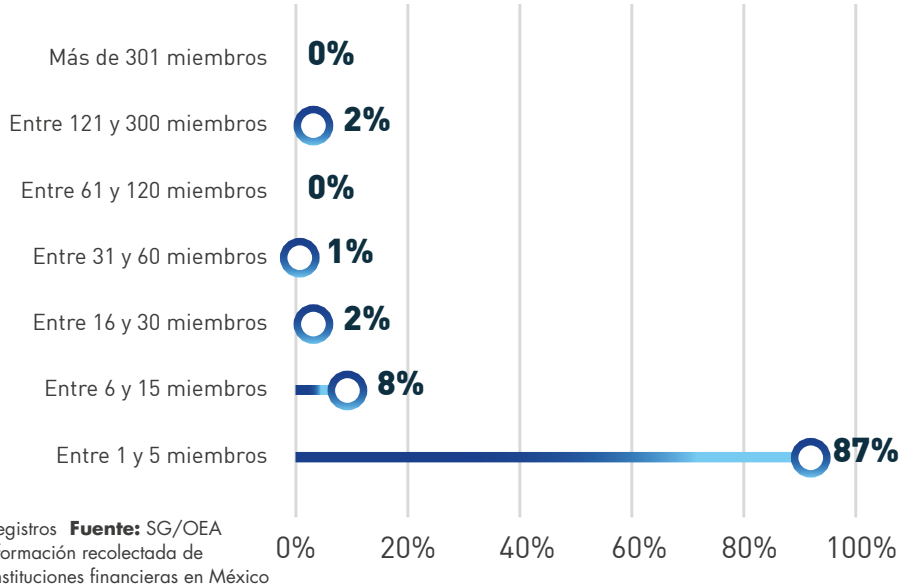
Cuadro 5. Promedio de profesionales de seguridad de la información (incluyendo ciberseguridad) por sector y tamaño de entidad / institución financiera en México

	Grande	Mediana	Pequeña	Total
Banca Comercial o Múltiple	91	25	24	37
Banca de Desarrollo		10	7	9
Sector Bursátil			36	36
Sector de Ahorro y Crédito Popular (SOCAP)		4	3	3
Sector de Ahorro y Crédito Popular (SOFIPO)	3	3	3	3
Sector de Intermediarios Financieros No Bancarios		3	3	3
Sector FINTECH			4	4
SISTEMA FINANCIERO MEXICANO	79	9	7	9

Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Al estimar dicho personal por tamaño de entidad / institución financiera, se obtiene lo siguiente: un equipo de setenta y nueve (79) personas en promedio en una entidad grande, un equipo de nueve (9) personas en promedio en una entidad mediana y un equipo de siete (7) personas en promedio en una entidad pequeña.

Gráfica 10. Personas que conforman la totalidad de equipos que manejan procesos asociados a la seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales



Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

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

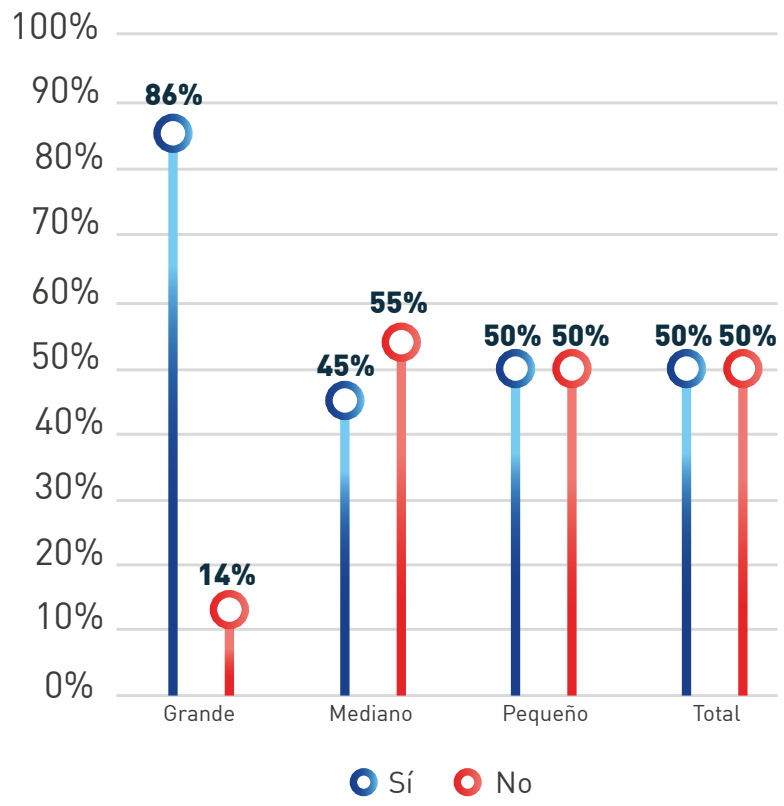
Pese a la presencia de equipos responsables de la seguridad digital en este tipo de organizaciones, el 68% de entidades e instituciones financieras en México considera adecuado que este equipo creciera en el corto plazo, esto teniendo en cuenta que el 82% de las entidades bancarias en la región de América Latina y el Caribe opina lo mismo (Organización de los Estados Americanos, 2018). Al analizar por tamaño, se aprecia que el 100% de las entidades grandes, el 89% de las entidades medianas y el 60% de las entidades pequeñas consideran que el tamaño de los equipos debe aumentar. Así mismo se identifica que el único sector que mayoritariamente (56%) considera que no es adecuado que el equipo crezca en el corto plazo es el sector de Intermediarios Financieros No Bancarios[7].

Como parte del modelo de gobierno de las entidades e instituciones financieras, el Consejo de Administración o Consejo Directivo o Junta Directiva del 50% de las entidades e instituciones financieras en el país recibe reportes periódicos acerca de indicadores, riesgos y gestión de riesgos de seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales. Se destaca la diferencia entre entidades grandes con entidades medianas, en donde se aprecia que mientras el 86% de las primeras mantiene dicha práctica, tan solo el 45% de las segundas lo hace.

Sobresalen sectores como el bursátil, donde el 100% de las entidades e instituciones financieras manifiesta que el Consejo de Administración o Consejo Directivo o Junta Directiva recibe estos reportes de manera periódica[8], y el bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México, donde el porcentaje es del 83% y que supera el promedio del sector bancario de la región América Latina y el Caribe, en el que el promedio de bancos que realizan dicha práctica es 72% (Organización de los Estados Americanos, 2018).

7. La gráfica 37 del Anexo 2 presenta la comparación del resultado: *¿Se considera adecuado que este equipo creciera en el corto plazo?* entre los diferentes sectores analizados del Sistema Financiero Mexicano.
8. La gráfica 38 del Anexo 2 presenta la comparación del resultado: ¿El Consejo de Administración o Consejo Directivo o Junta Directiva recibe reportes periódicos acerca de riesgos de seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales? entre los diferentes sectores analizados del Sistema Financiero Mexicano.

Gráfica 11. ¿El Consejo de Administración o Consejo Directivo o Junta Directiva recibe reportes periódicos acerca de riesgos de seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales?



Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Según los resultados, el manejo de la gestión de la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude ocurridos a través de medios digitales en la mayoría de las entidades e instituciones financieras en México se prepara en el marco de un Comité de Riesgos (25% del total). En las entidades e instituciones financieras del país también existen otras instancias de manejo estratégico en relación con el tema como el Comité de Auditoría (23% del total) o un Comité Técnico o de Tecnología (13% del total).

Se destaca que en el sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México se utiliza mayormente el Comité de Riesgos con un 36%, similar a lo reportado por las entidades bancarias en la región América Latina y el Caribe, donde el 39% de la gestión de la seguridad de la información se prepara en el marco de dicho Comité (Organización de los Estados Americanos, 2018).

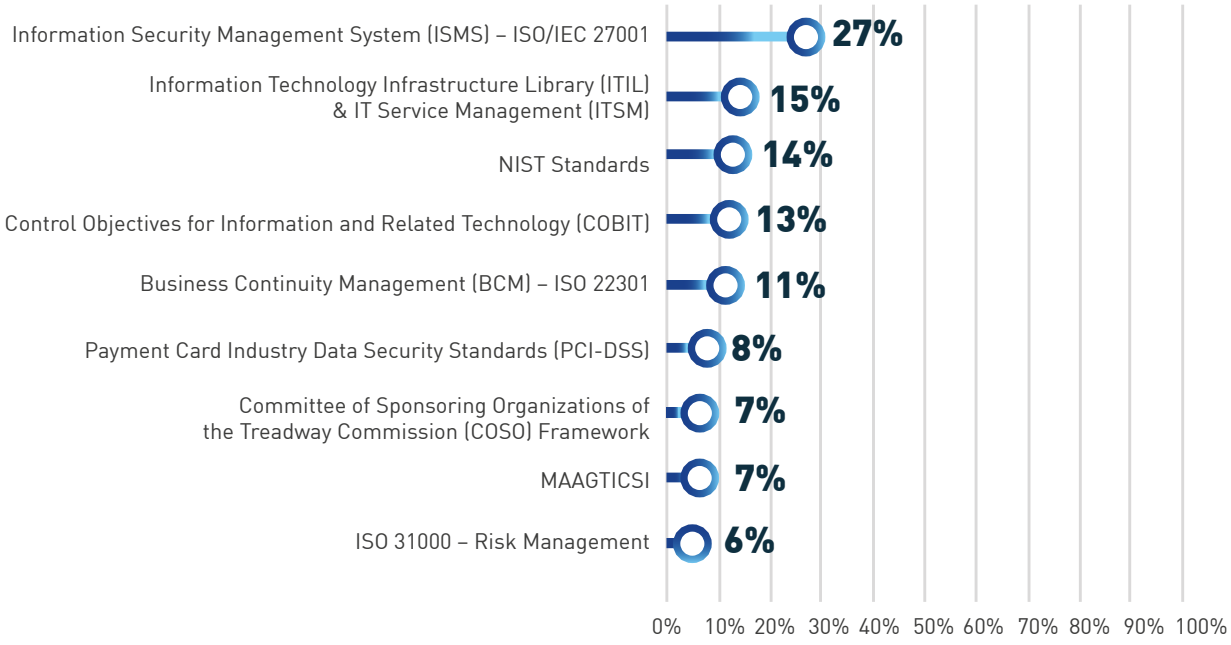
Respecto al apoyo a la gestión de riesgos de seguridad de la información (incluyendo ciberseguridad) y fraudes ocurridos a través de medios digitales por parte de la alta dirección (Dirección General o Gerencia General o Presidencia), se destaca que un 58% del total de las entidades e instituciones financieras lo demuestran fomentando la capacitación y sensibilización en seguridad digital mientras que el 49% lo hace impulsando planes de seguridad de la información.

Otro aspecto identificado es que, mientras en el sector bancario de la región América Latina y el Caribe el apoyo de la alta dirección a la gestión de riesgos de seguridad de la información se da principalmente (con un 65%) *exigiendo la adopción de buenas prácticas de seguridad* (Organización de los Estados Americanos, 2018), el sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México registra apenas un promedio de 36% para este ítem.

El rol que juega la alta dirección y la junta de las organizaciones respecto de la seguridad digital es fundamental. A nivel país, el presente estudio encuentra que para la mayoría de las entidades e instituciones financieras (48% del total), es medianamente complejo lograr que la alta dirección de la organización tome decisiones de inversión en soluciones de seguridad digital, mientras que tan sólo el 17% de las organizaciones lo consideran altamente complejo. Se destaca el hecho de que sectores como el FINTECH y el Sector de Ahorro y Crédito Popular (SOFIPO) encuentran mayoritariamente (ambos con un 53%) que es poco complejo que la alta dirección tome decisiones de inversión en soluciones de seguridad digital.

Finalmente, en asuntos de preparación y gobernanza, vale la pena resaltar la adopción de marcos de seguridad y/o estándares internacionales en torno a la seguridad de la información (incluyendo la ciberseguridad) por parte de las entidades e instituciones financieras del país. El 27% del total de entidades e instituciones financieras menciona que ha adoptado las normas I*nformation Security Management System* (ISMS) – *ISO 27001*, el 15% del total ha adoptado el *Information Technology Infrastructure Library* (ITIL) *& IT Service Management* (ITSM), el 14% los *NIST Standards* y el 13% el *Control Objectives for Information and Related Technology* (COBIT).

Gráfica 12. Marcos de seguridad y/o estándares internacionales adoptados



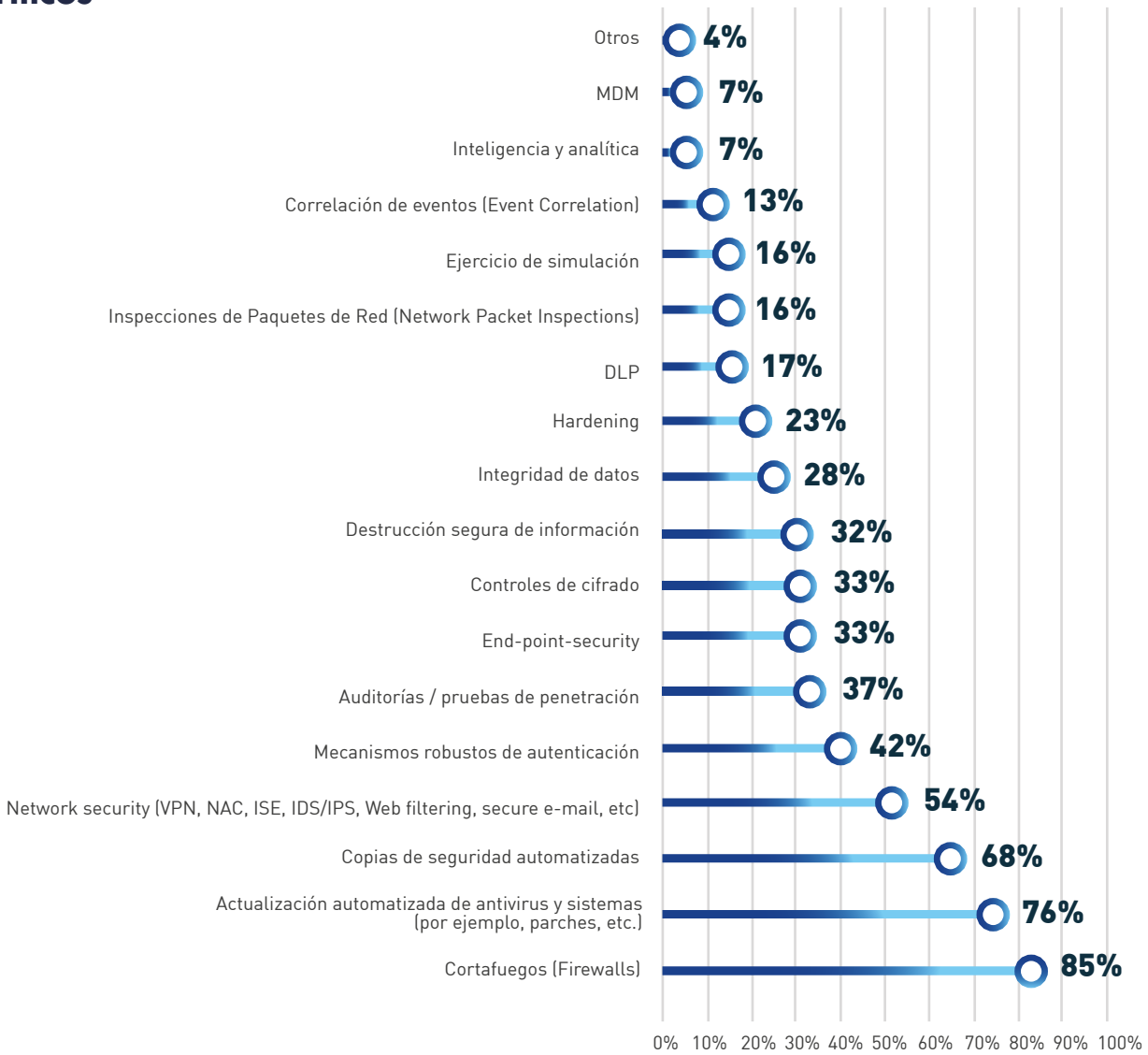
Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Se destaca que la aplicación de prácticas y adopción de normas en torno a Information Security Management System (ISMS) – ISO 27001 en el sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México, registra un promedio del 71%, en concordancia a lo que ocurre en el sector bancario de la región de América Latica y el Caribe, donde el 68% del total de entidades bancarias menciona que ha adoptado dichas normas (Organización de los Estados Americanos, 2018).

3.2.2. Detección y análisis de eventos de seguridad digital

Las acciones de detección y análisis de eventos de seguridad digital son fundamentales en el marco de gestión sistemática de este tipo de riesgos. Las principales acciones y medidas técnicas de la seguridad de la información (incluyendo ciberseguridad) que las entidades e instituciones financieras de México llevan a cabo son: i) los cortafuegos (85% del total), ii) la actualización automatizada de antivirus y sistemas (por ejemplo, parches, etc.) (76% del total), iii) las copias de seguridad automatizadas (68% del total) y iv) el network security (VPN, NAC, ISE, IDS/IPS, Web filtering, secure e-mail, etc.) (54%). Se destaca que el 100% de las grandes entidades e instituciones financieras implementan medidas como Cortafuegos, actualización automatizada de antivirus y sistemas, Network Security, Mecanismos robustos de autenticación, Auditorías / pruebas de penetración y Controles de cifrado.

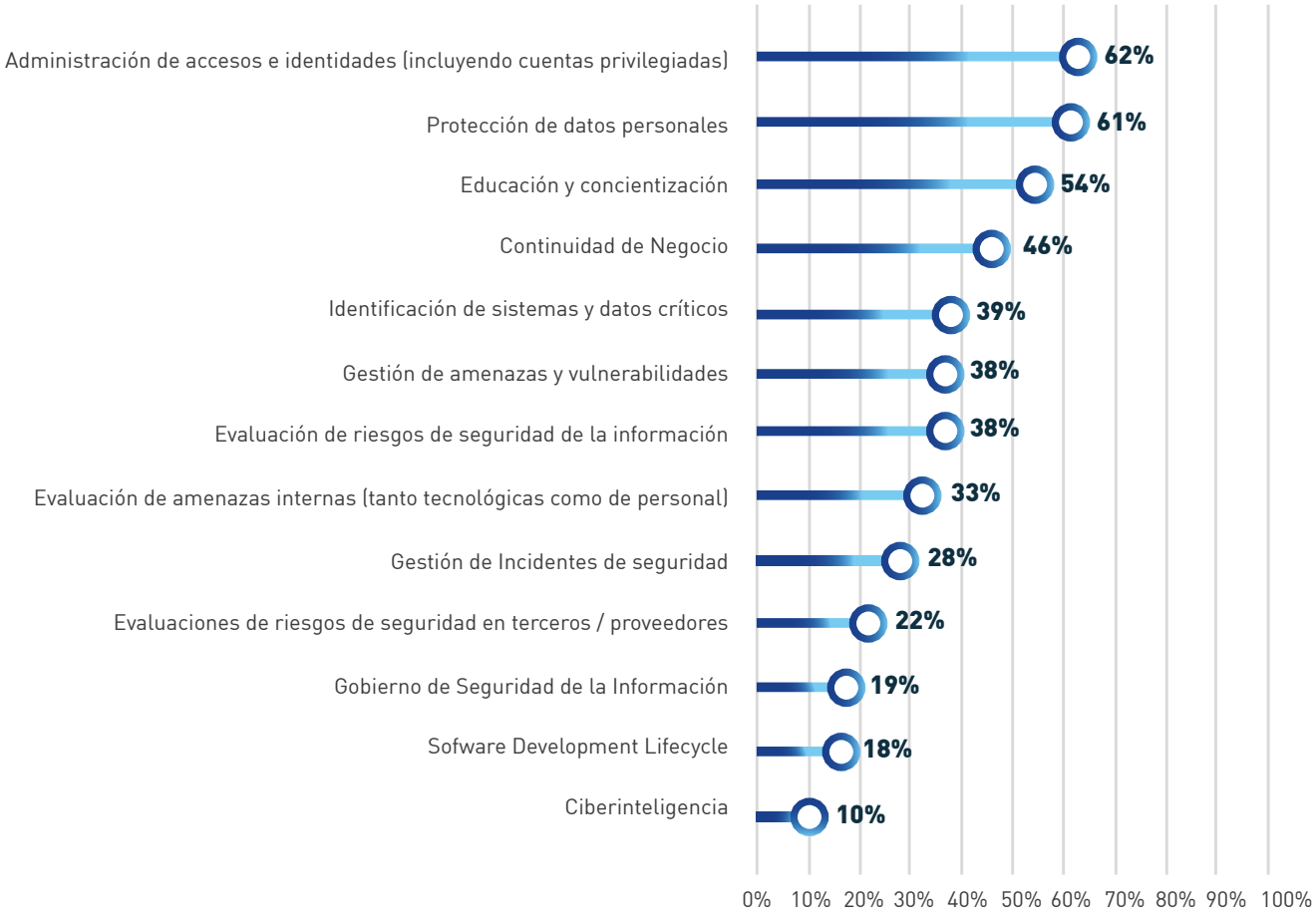
Gráfica 13. Acciones y medidas técnicas de seguridad de la información (incluyendo ciberseguridad) para proteger los sistemas de información críticos



Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Adicionalmente, los procesos / programas implementados en las entidades e instituciones financieras del país más comunes asociados a la seguridad digital son: i) la *administración de accesos e identidades (incluyendo cuentas privilegiadas)* (62%), ii) la *protección de datos personales* (61%), iii) la *educación y concientización* (54%), y iv) la *continuidad del negocio* (46%). Se destaca que en el sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México, el 100% de los bancos grandes implementan: *Gobierno de Seguridad de la Información, Identificación de sistemas y datos críticos, Evaluación de riesgos de seguridad de la información, Educación y concientización, Gestión de amenazas y vulnerabilidades y Protección de datos personales.*

Gráfica 14. Procesos / programas respecto a la seguridad digital implementados actualmente por las entidades e instituciones financieras

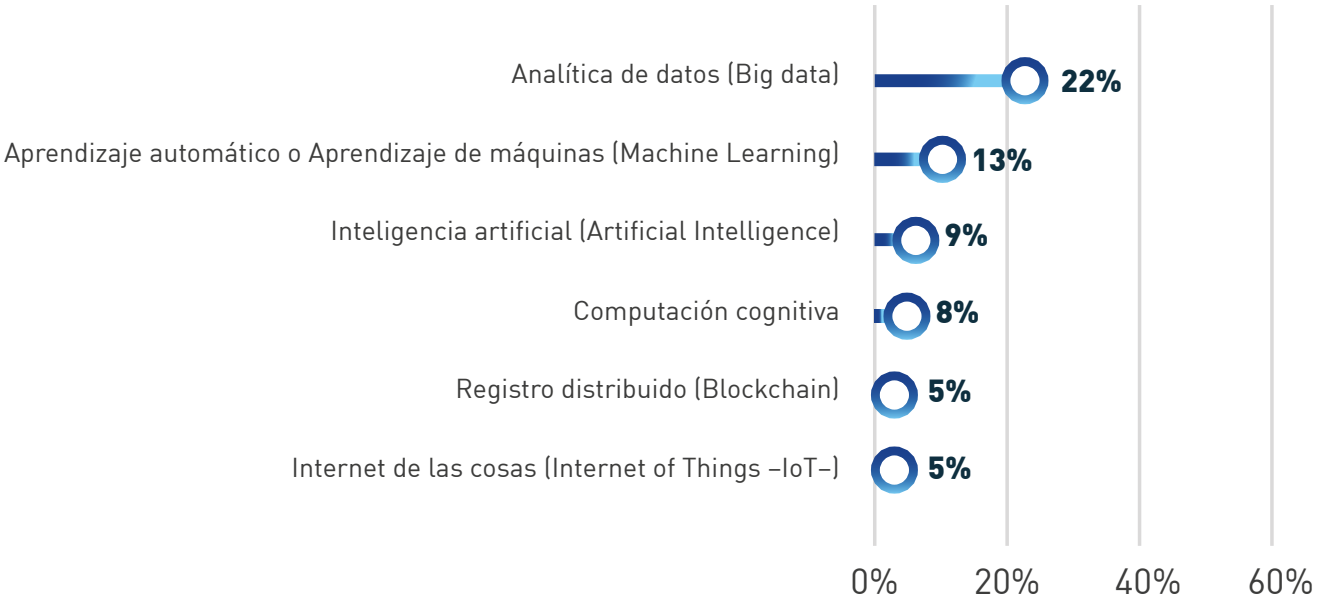


Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

El uso de tecnologías digitales emergentes aplicadas a herramientas, controles o procesos de seguridad digital en entidades e instituciones financieras en México se encuentra aún rezagado. Tan sólo el 22% del total de entidades e instituciones financieras implementan analítica de datos en herramientas, controles o procesos, el 13% del total de entidades e instituciones financieras implementan el aprendizaje automático o Aprendizaje de máquinas (Machine Learning) y el 9% del total de entidades e instituciones financieras implementan inteligencia artificial (Artificial Intelligence).

Se destaca el hecho de que en el sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México, el uso de Analítica de datos (Big Data) registra un promedio del 45%[9], lo cual supera significativamente el promedio del sector financiero y el promedio del sector bancario de la región América Latina y el Caribe (29% del total) (Organización de los Estados Americanos, 2018).

Gráfica 15. Tecnologías digitales emergentes aplicadas a herramientas, controles o procesos de seguridad digital en la entidad / institución financiera



Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

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

9. La gráfica 39 del Anexo 2 presenta la comparación del resultado: Tecnologías digitales emergentes aplicadas a herramientas, controles o procesos de seguridad digital en la entidad / institución financiera entre los diferentes sectores analizados del Sistema Financiero Mexicano.

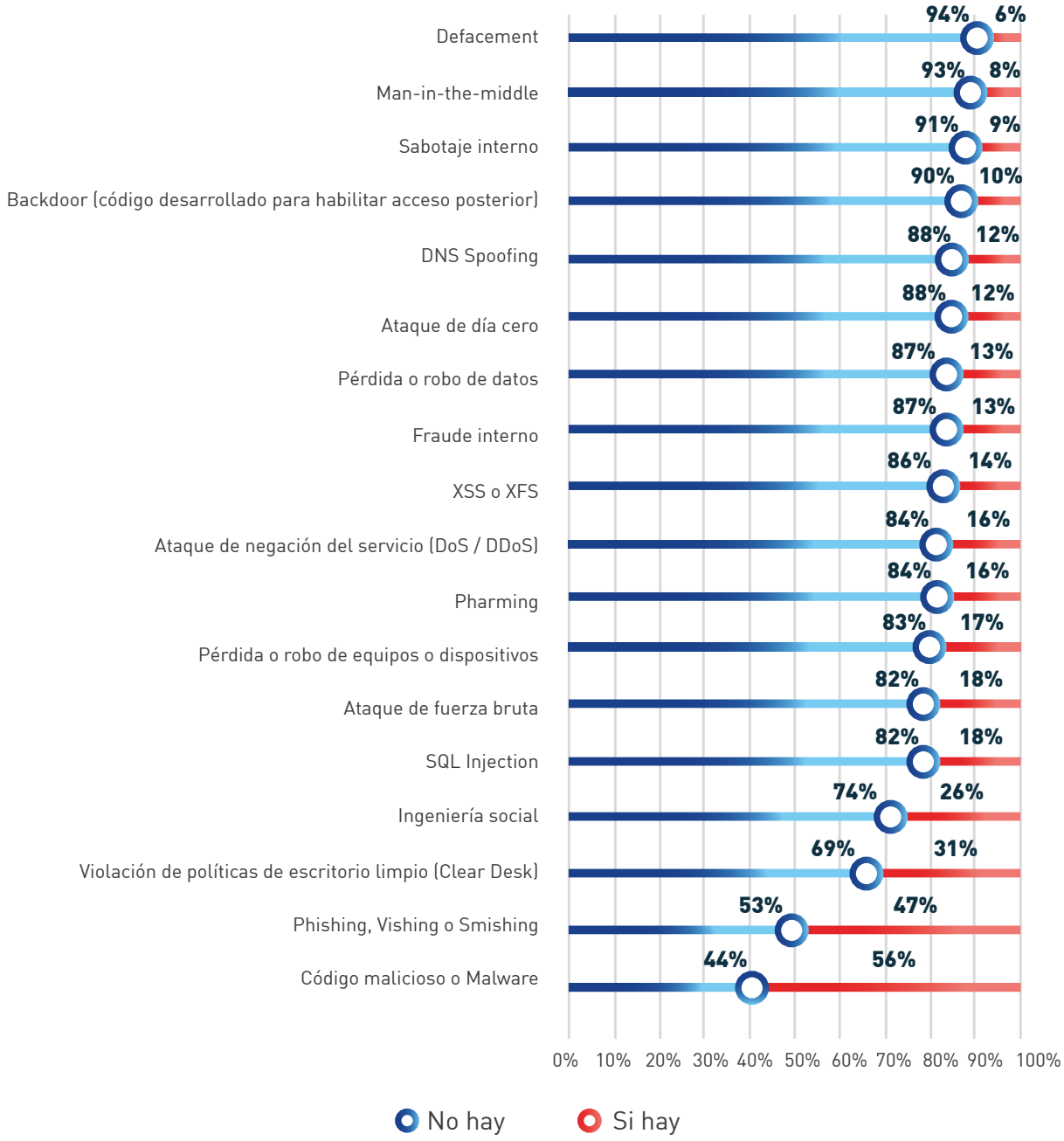
Cuadro 6. Riesgos cibernéticos que merecen mayor atención por parte de la entidad / institución financiera

	Grande	Mediana	Pequeña	Total
Pérdida / robo de activos de información clasificada (confidencial o sensible)	1,71	2,35	2,64	**2,55**
Secuestro de información	4,71	3,18	2,75	**2,91**
Compromiso de credenciales de usuarios privilegiados	2,29	3,08	3,24	**3,17**
Sabotaje o fraude a través de un insider (personal interno)	2,43	3,04	3,35	**3,25**
Denegación del servicio	4,57	3,80	3,88	**3,88**
Defacement – alteración en sitio web	5,29	5,00	4,66	**4,76**

Nota: 240 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 e instituciones financieras en México

Adicionalmente, los eventos de seguridad digital más comúnmente identificados por las entidades e instituciones financieras de México durante el año 2018 son: i) el *código malicioso o malware* (56% del total de entidades), ii) el *phishing dirigido para tener acceso a sistemas de la entidad* (47% del total de entidades) y iii) la *violación de políticas de escritorio limpio* (clear desk) (31% del total de entidades). En contraste, las entidades e instituciones financieras en el país mencionan que los eventos de seguridad menos comunes son: i) *defacement* (tan sólo el 6% del total de entidades), ii) *Man-in-the-middle* (tan sólo el 8% del total de entidades), y iii) *sabotaje interno* (tan sólo el 9% del total de entidades). Es importante considerar la similitud con los eventos de seguridad digital más comúnmente identificados por las entidades bancarias de la región América Latina y el Caribe durante el año 2017, los cuales fueron: i) el *código malicioso o malware* (80% del total de Bancos), ii) la *violación de políticas de escritorio limpio* (clear desk) (63% del total de Bancos), y iii) el *phishing dirigido para tener acceso a sistemas del banco* (57% del total de Bancos) (Organización de los Estados Americanos, 2018).

Gráfica 16. Eventos (ataques exitosos y ataques no exitosos) de seguridad de la información (incluyendo ciberseguridad) contra las entidades e instituciones financieras que se han identificado durante los últimos doce meses

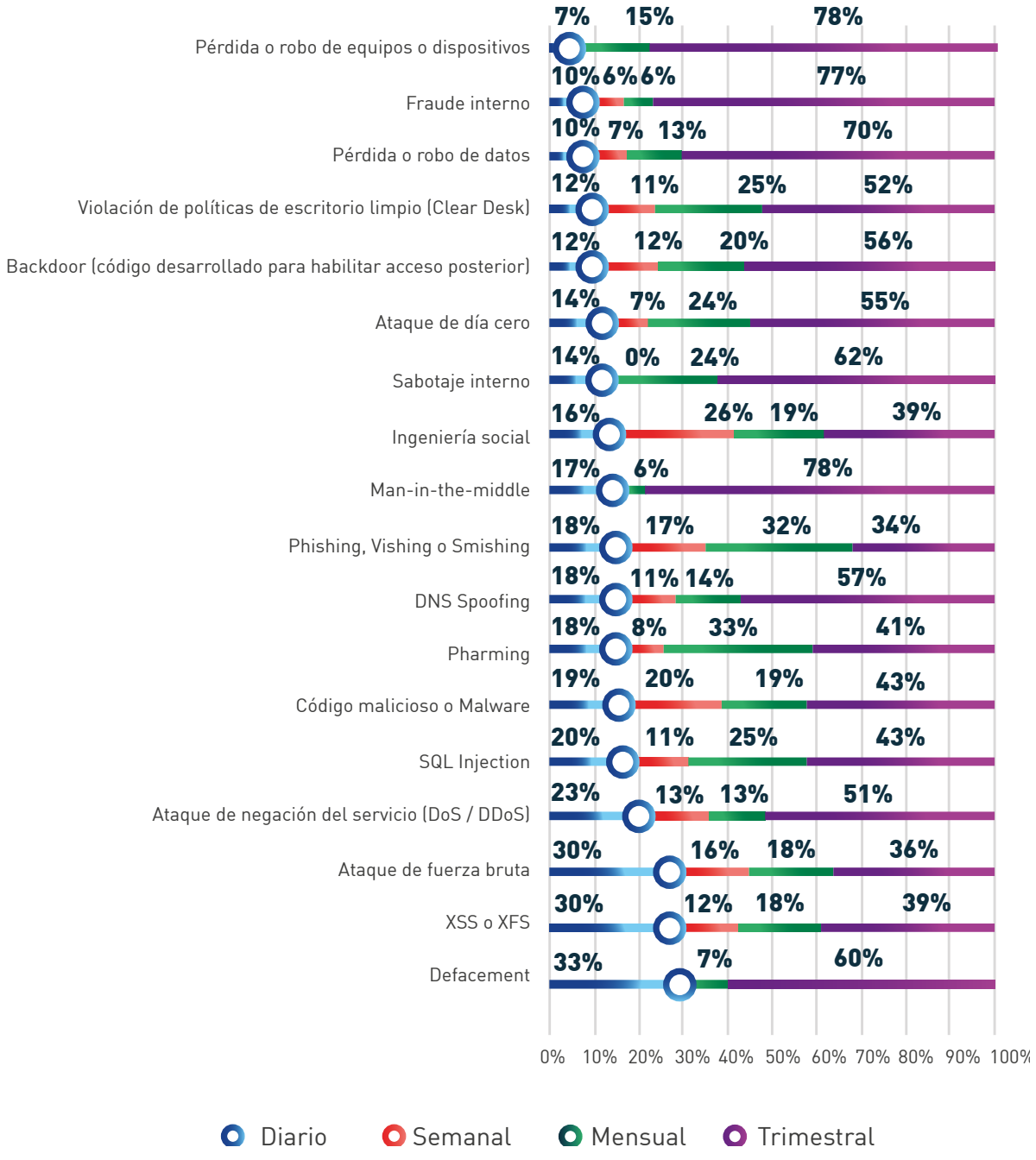


Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Al analizar los resultados respecto a la frecuencia aproximada de ocurrencia de eventos identificados por las entidades e instituciones financieras en México durante el año 2018, se aprecia una dinámica particular por tipo de evento que depende también del tamaño de la organización. Por ejemplo, al revisar la frecuencia con la que ocurren eventos relacionados con *código malicioso o malware* para el total de entidades e instituciones financieras en el país se aprecia lo siguiente: i) un 19% de las entidades identifican ocurrencia de eventos de *malware* diariamente, ii) un 20% del

total lo identifican semanalmente, iii) un 19% del total lo identifican mensualmente, y iv) un 43% del total lo identifican trimestralmente. Con respecto al *Phishing, Vishing o Smishing* se aprecia lo siguiente: i) un 18% de las entidades identifican ocurrencia de este tipo de eventos diariamente, ii) un 17% del total lo identifican semanalmente, iii) un 32% del total lo identifican mensualmente, y iv) un 34% del total lo identifican trimestralmente.

Gráfica 17. Frecuencia en la ocurrencia de eventos de seguridad de la información (incluyendo ciberseguridad) contra las entidades e instituciones financieras



Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

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

Por ejemplo, se observa que las entidades grandes del Sistema Financiero Mexicano son objeto de ataques de todo tipo de eventos de seguridad digital, resaltando identificación de casi todos por la mayoría de dichas entidades en el país. Los eventos (ataques exitosos y ataques no exitosos) de seguridad digital más comúnmente identificados por las entidades grandes de México durante el año 2018 son: i) el *código malicioso o malware* (100% del total de entidades grandes), ii) la *violación de políticas de escritorio limpio (clear desk)* (100% del total de entidades grandes) y iii) el *Pishing, Vishing o Smishing* (100% del total de entidades grandes).

Al revisar la frecuencia con la que ocurren eventos relacionados con *código malicioso o malware* para el total de entidades grandes en México se aprecia lo siguiente: i) un 43% de las entidades grandes detectan eventos de *malware* diariamente y ii) un 57% del total lo identifican semanalmente. 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 las entidades grandes en el país.

Cuadro 7. Eventos de seguridad digital contra entidades e instituciones financieras grandes que se han identificado durante los últimos doce meses

	No hay	Si hay	Total	Diario	Semanal	Mensual	Trimestral	Total
Ingeniería social	14%	86%	**100%**	0%	50%	17%	33%	**100%**
Código malicioso o Malware	0%	100%	**100%**	43%	57%	0%	0%	**100%**
Phishing, Vishing o Smishing	0%	100%	**100%**	14%	43%	14%	29%	**100%**
Pharming	29%	71%	**100%**	0%	40%	20%	40%	**100%**
Pérdida o robo de datos	71%	29%	**100%**	0%	0%	0%	100%	**100%**
Pérdida o robo de equipos o dispositivos	43%	57%	**100%**	0%	0%	25%	75%	**100%**
Ataque de día cero	100%	0%	**100%**	0%	0%	0%	0%	**0%**
Ataque de negación del servicio (DoS / DDoS)	29%	71%	**100%**	0%	20%	0%	80%	**100%**
DNS Spoofing	71%	29%	**100%**	0%	0%	0%	100%	**100%**
Violación de políticas de escritorio limpio (Clear Desk)	0%	100%	**100%**	14%	14%	14%	57%	**100%**
Sabotaje interno	86%	14%	**100%**	0%	0%	0%	100%	**100%**
Fraude interno	57%	43%	**100%**	0%	0%	33%	67%	**100%**
Defacement	86%	14%	**100%**	0%	0%	0%	100%	**100%**
Backdoor (código desarrollado para habilitar acceso posterior)	100%	0%	**100%**	0%	0%	0%	0%	**0%**
SQL Injection	29%	71%	**100%**	20%	40%	0%	40%	**100%**
XSS o XFS	29%	71%	**100%**	20%	40%	0%	40%	**100%**
Ataque de fuerza bruta	29%	71%	**100%**	20%	40%	20%	20%	**100%**
Man-in-the-middle	86%	14%	**100%**	0%	0%	0%	100%	**100%**

Nota: 7 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

En relación con las entidades medianas del Sistema Financiero Mexicano, se destaca que también son objeto de ataques de todo tipo de eventos de seguridad digital, resaltando identificación de algunos por la mayoría de dichas entidades en el país. Los eventos (ataques exitosos y ataques no exitosos) de seguridad digital más comúnmente identificados por las entidades medianas durante el año 2018 son: i) el código malicioso o malware (69% del total de entidades medianas), ii) el phishing, vishing o smishing (62% del total de entidades medianas), y iii) la violación de políticas de escritorio limpio (clear desk) (40% del total de entidades medianas).

Al revisar la frecuencia de ocurrencia de eventos relacionados con código malicioso o malware para el total de entidades medianas en el país se aprecia lo siguiente: i) un 24% de las entidades medianas identifican ocurrencia de eventos de malware diariamente, ii) un 24% del total lo identifican semanalmente, iii) un 13% del total lo identifican mensualmente, y iv) un 39% del total lo identifican 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 las entidades medianas en México.

Cuadro 8. Eventos de seguridad digital contra entidades e instituciones financieras medianas que se han identificado durante los últimos doce meses

	No hay	Si hay	Total	Diario	Semanal	Mensual	Trimestral	Total
Ingeniería social	55%	45%	**100%**	24%	16%	28%	32%	**100%**
Código malicioso o Malware	31%	69%	**100%**	24%	24%	13%	39%	**100%**
Phishing, Vishing o Smishing	38%	62%	**100%**	21%	18%	29%	32%	**100%**
Pharming	73%	27%	**100%**	20%	7%	40%	33%	**100%**
Pérdida o robo de datos	82%	18%	**100%**	10%	10%	40%	40%	**100%**
Pérdida o robo de equipos o dispositivos	71%	29%	**100%**	6%	0%	25%	69%	**100%**
Ataque de día cero	75%	25%	**100%**	14%	0%	29%	57%	**100%**
Ataque de negación del servicio (DoS / DDoS)	76%	24%	**100%**	23%	23%	15%	38%	**100%**
DNS Spoofing	76%	24%	**100%**	8%	15%	15%	62%	**100%**
Violación de políticas de escritorio limpio (Clear Desk)	60%	40%	**100%**	14%	9%	32%	45%	**100%**
Sabotaje interno	87%	13%	**100%**	14%	0%	43%	43%	**100%**
Fraude interno	76%	24%	**100%**	8%	15%	8%	69%	**100%**
Defacement	85%	15%	**100%**	25%	0%	13%	63%	**100%**
Backdoor (código desarrollado para habilitar acceso posterior)	84%	16%	**100%**	11%	11%	22%	56%	**100%**
SQL Injection	65%	35%	**100%**	16%	0%	26%	58%	**100%**
XSS o XFS	76%	24%	**100%**	23%	0%	23%	54%	**100%**
Ataque de fuerza bruta	64%	36%	**100%**	25%	5%	30%	40%	**100%**
Man-in-the-middle	85%	15%	**100%**	13%	0%	13%	75%	**100%**

Nota: 53 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Por último, en relación con las entidades pequeñas del Sistema Financiero Mexicano, se destaca que son objeto de ataques de algunos tipos de eventos de seguridad digital, resaltando identificación de pocos por la mayoría de dichas entidades en el país. Los eventos (ataques exitosos y ataques no exitosos) de seguridad digital más comúnmente identificados por las entidades pequeñas durante el año 2018 son: i) el código malicioso o malware (68% del total de entidades medianas), ii) la violación de políticas de escritorio limpio (clear desk) (45% del total de entidades medianas) y iii) el phishing dirigido para tener acceso a sistemas de la entidad (42% del total de entidades medianas).

Al revisar la frecuencia de ocurrencia de eventos relacionados con código malicioso o malware para el total de entidades pequeñas en México se aprecia lo siguiente: i) un 14% de las entidades pequeñas identifican ocurrencia de eventos de malware diariamente, ii) un 16% del total lo identifican semanalmente, iii) un 22% del total lo identifican mensualmente, y iv) un 48% del total lo identifican 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 las entidades pequeñas del país.

Cuadro 9. Eventos de seguridad digital contra entidades e instituciones financieras pequeñas que se han identificado durante los últimos doce meses

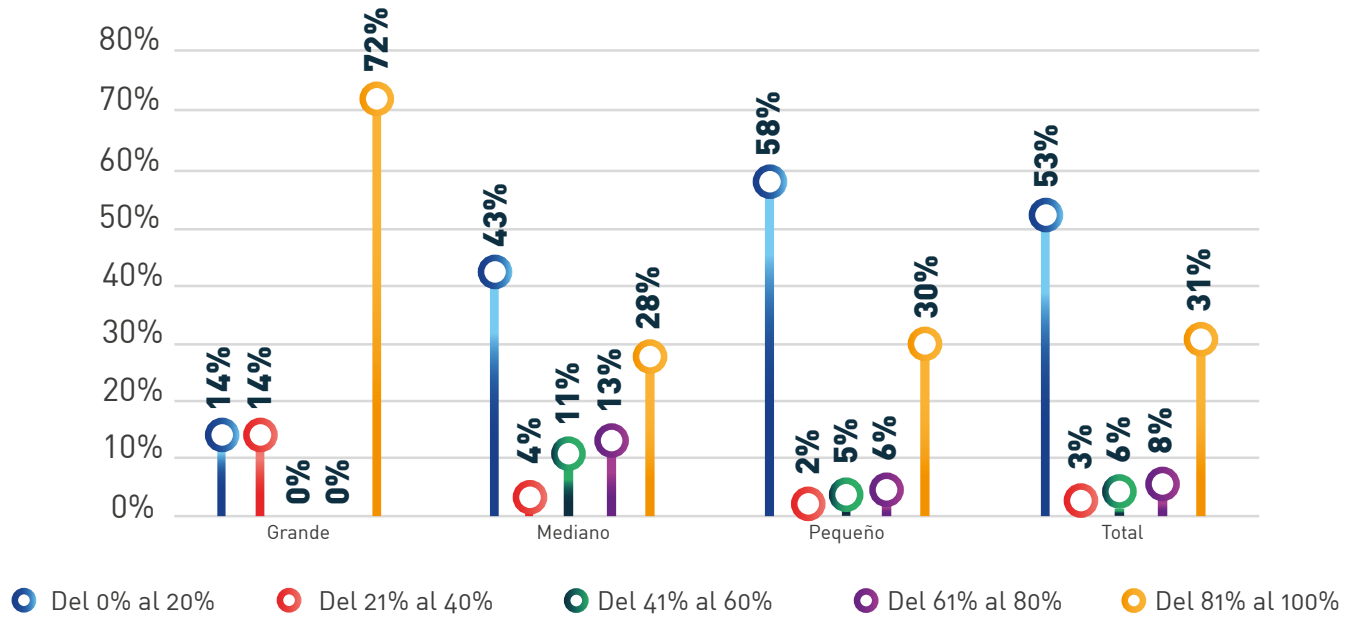
	No hay	Si hay	Total	Diario	Semanal	Mensual	Trimestral	Total
Ingeniería social	83%	17%	**100%**	13%	29%	13%	45%	**100%**
Código malicioso o Malware	49%	51%	**100%**	14%	16%	22%	48%	**100%**
Phishing, Vishing o Smishing	60%	40%	**100%**	17%	14%	35%	35%	**100%**
Pharming	89%	11%	**100%**	21%	0%	32%	47%	**100%**
Pérdida o robo de datos	90%	10%	**100%**	11%	6%	0%	83%	**100%**
Pérdida o robo de equipos o dispositivos	88%	12%	**100%**	10%	0%	5%	86%	**100%**
Ataque de día cero	92%	8%	**100%**	13%	13%	20%	53%	**0%**
Ataque de negación del servicio (DoS / DDoS)	88%	12%	**100%**	29%	5%	14%	52%	**100%**
DNS Spoofing	93%	7%	**100%**	31%	8%	15%	46%	**100%**
Violación de políticas de escritorio limpio (Clear Desk)	74%	26%	**100%**	11%	11%	24%	54%	**100%**
Sabotaje interno	93%	7%	**100%**	15%	0%	15%	69%	**100%**
Fraude interno	92%	8%	**100%**	13%	0%	0%	87%	**100%**
Defacement	97%	3%	**100%**	50%	0%	0%	50%	**100%**
Backdoor (código desarrollado para habilitar acceso posterior)	91%	9%	**100%**	13%	13%	19%	56%	**0%**
SQL Injection	89%	11%	**100%**	25%	15%	30%	30%	**100%**
XSS o XFS	92%	8%	**100%**	40%	13%	20%	27%	**100%**
Ataque de fuerza bruta	89%	11%	**100%**	37%	21%	5%	37%	**100%**
Man-in-the-middle	95%	5%	**100%**	22%	0%	0%	78%	**100%**

Nota: 180 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Al analizar el tipo de eventos (ataques exitosos y ataques no exitosos) de seguridad digital que usan los ciberdelincuentes contra los clientes (socios, asociados o usuarios) de servicios financieros, las entidades e instituciones financieras en México mencionan que los eventos de i) *Phishing*, ii) *Software espía (Malware o troyanos)*, y iii) *Ingeniería social* son los más frecuentes en el país, similar a lo registrado por el sector bancario en la región América Latina y el Caribe en el año 2017 (Organización de los Estados Americanos, 2018). Por otra parte, los eventos de seguridad digital contra clientes (socios, asociados o usuarios) menos comunes son: i) *Fraudes internos (realizados por funcionarios de clientes corporativos)*, ii) *Robo de identidad RFID (tarjetas de crédito / teléfonos móviles)*, y iii) *Software falso que suplanta el software real de la entidad*.

Finalmente, en asuntos de detección y análisis de eventos de seguridad digital, se resalta que en promedio el 53% de las entidades e instituciones financieras en el país detectan mediante sistemas propios (y no de terceros) entre un 0% y un 20% de eventos (ataques exitosos y ataques no exitosos) de seguridad de la información (incluyendo ciberseguridad), el 3% de las entidades detecta entre un 21% y un 40% de eventos con sistemas propios, el 6% de las entidades detecta entre un 41% y un 60% de eventos con sistemas propios, el 8% de las entidades detecta entre un 61% y un 80% de eventos con sistemas propios y el 31% de las entidades detecta entre un 81% y un 100% de eventos con sistemas propios. Se destaca que en sectores como el Bursátil y el FINTECH, más del 75% de las entidades e instituciones financieras de dichos sectores detectan mediante sistemas propios (y no de terceros) entre un 81% y un 100% de eventos de seguridad de la información[10].

Gráfica 18. Porcentaje de eventos de seguridad digital que son detectados mediante sistemas propios (y no de terceros) de detección de la entidad / institución financiera



Nota: 237 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

10. La gráfica 40 del Anexo 2 presenta la comparación del resultado: Porcentaje de eventos de seguridad digital que son detectados mediante sistemas propios (y no de terceros) de detección de la entidad / institución financiera entre los diferentes sectores analizados del Sistema Financiero Mexicano.

Al analizar por tamaño de entidad, la mayoría de las entidades grandes (71%) detecta entre un 81% y un 100% de eventos con sistemas propios, la mayoría de las entidades medianas (43%) detecta entre un 0% y un 20% de eventos con sistemas propios y la mayoría de las entidades pequeñas (58%) detecta entre un 0% y un 20% de eventos con sistemas propios. Se destaca el caso del sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México donde el 83% de los bancos grandes detecta entre 81% y un 100% de eventos con sistemas propios, mientras que en promedio un 30% de los bancos grandes de la región América Latina y el Caribe detectan en dicho rango (Organización de Estados Americanos, 2018).

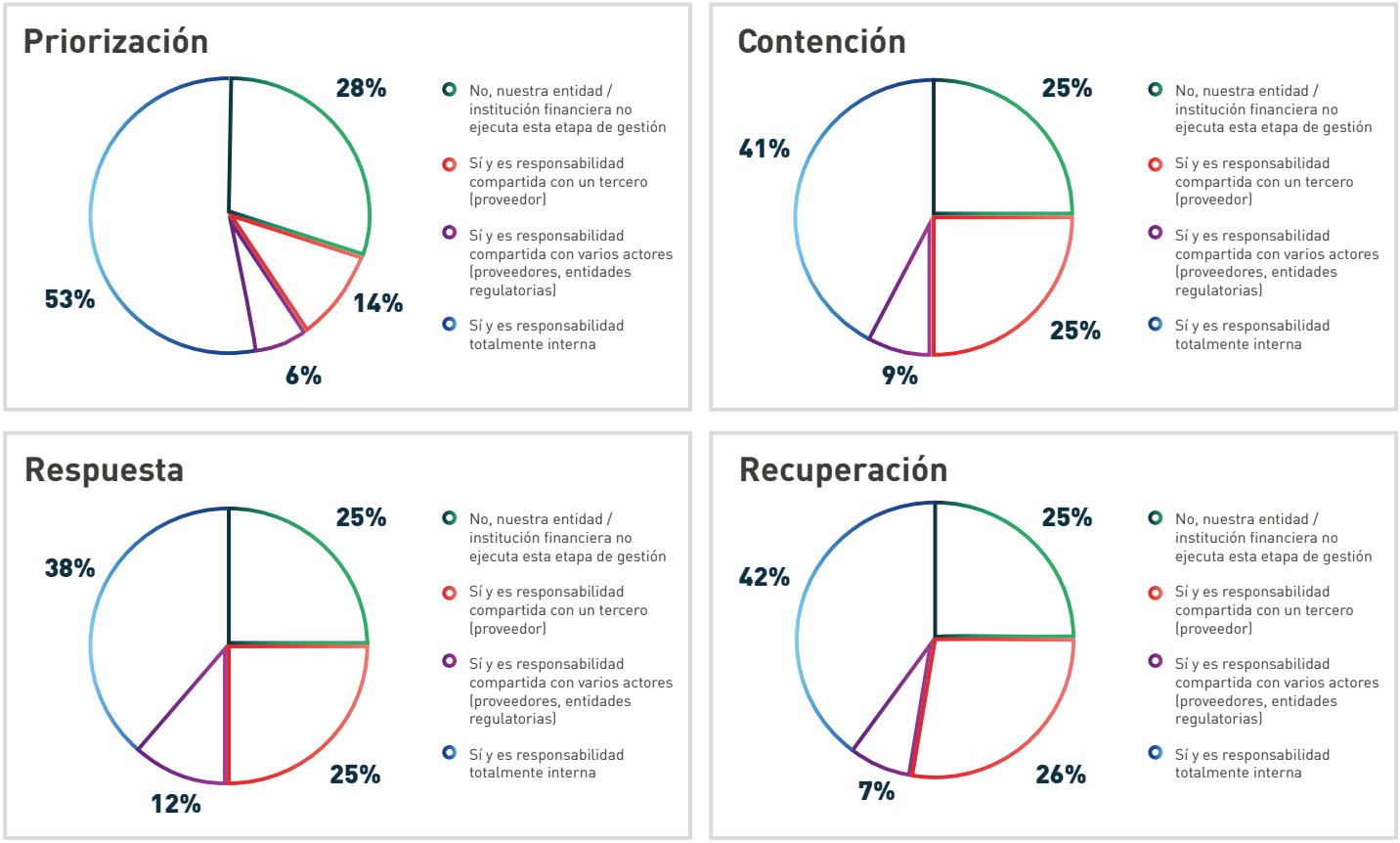
3.2.3. Gestión, respuesta y recuperación ante incidentes de seguridad digital

Teniendo en cuenta la distinción que se presentó en el instrumento de recolección de información enviado a las entidades e instituciones financieras entre evento de seguridad de la información (incluyendo ciberseguridad) (suma de ataques exitosos y de ataques no exitosos que sufrió la entidad / institución financiera durante un periodo de tiempo) e incidente de seguridad de la información (incluyendo ciberseguridad) (total de ataques exitosos que sufrió la entidad / institución financiera 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 etapas de gestión frente a incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad) se destaca que: i) el 53% de las entidades del país cuentan y ejecutan una estrategia de priorización de incidentes bajo la responsabilidad interna de la organización, ii) el 41% de las entidades del país cuentan y ejecutan una estrategia de contención de incidentes bajo la responsabilidad interna de la organización, iii) el 38% de las entidades del país cuentan y ejecutan una estrategia de respuesta de incidentes bajo la responsabilidad interna de la organización, y iv) el 42% de las entidades del país cuentan y ejecutan una estrategia de recuperación de incidentes bajo la responsabilidad interna de la organización. Es decir, al menos un tercio de las entidades del país cuentan con estrategias de gestión, respuesta y recuperación ante incidentes de seguridad digital.

Al analizar por sectores del Sistema Financiero Mexicano, se observa que los sectores Bancario (Banca Comercial o Múltiple y Banca de Desarrollo), Bursátil y FINTECH reportan porcentajes superiores al 74% en la ejecución de una estrategia de priorización de incidentes bajo la responsabilidad interna de la organización, algo levemente superior al promedio del 70% de los bancos de la región América Latina y el Caribe (Organización de los Estados Americanos, 2018). Por su parte, los sectores Entidades de Ahorro y Crédito Popular (SOCAP y SOFIPO) y de Intermediarios no Financieros reportan promedios inferiores al 44% sobre esa misma etapa.

Gráfica 19. Estrategias frente a incidentes (ataques exitosos) de seguridad digital

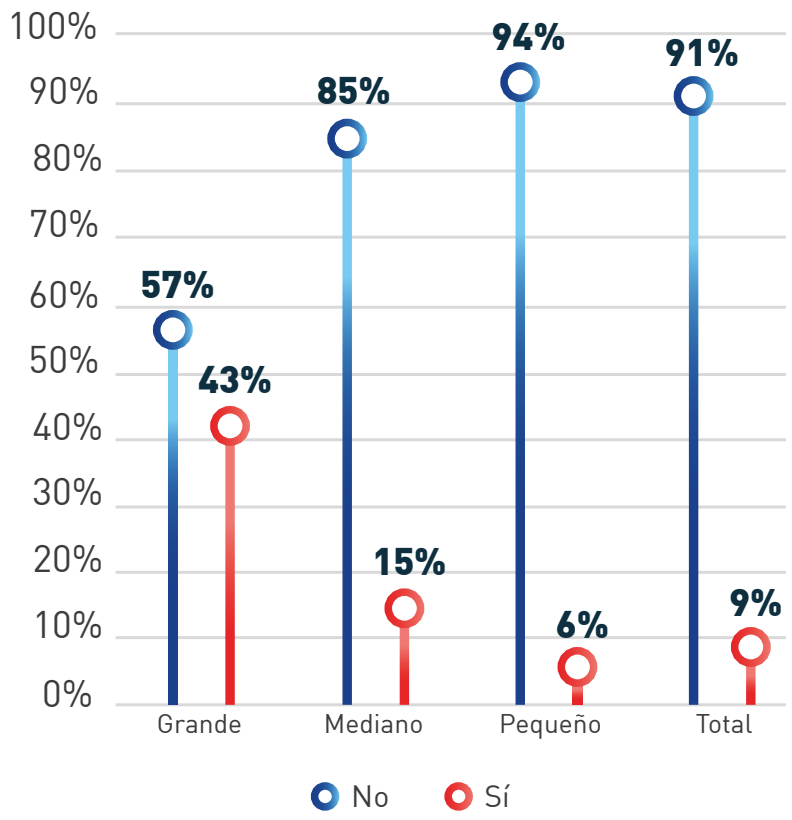


Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

En relación con la materialización de incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad) en las entidades e instituciones financieras en el país durante el 2018, se resalta que el 43% de las entidades grandes manifiestan que fueron víctimas de ataques exitosos, mientras que entre las entidades medianas el porcentaje es del 15% y entre las pequeñas, del 6%. Se resalta el hecho de que en el sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México, el promedio es superior con respecto a otros sectores del Sistema Financiero Mexicano, reportando la materialización de incidentes (ataques exitosos) en un 50% en entidades grandes, 22% en entidades medianas y 11% en entidades pequeñas[11]. No obstante, es inferior con respecto a lo evidenciado en el sector bancario de la región América Latina y el Caribe, donde un 65% de las entidades bancarias grandes, un 43% de las medianas y un 19% de las pequeñas admiten haber sido víctimas de ataques exitosos de seguridad de la información (incluyendo ciberseguridad).

11. La gráfica 41 del Anexo 2 presenta la comparación del resultado: ¿La entidad / institución financiera a la cual usted pertenece (en el país en el que se encuentra), como organización, fue víctima de incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad) durante los últimos doce meses? entre los diferentes sectores analizados del Sistema Financiero Mexicano.

Gráfica 20. ¿La entidad / institución financiera a la cual usted pertenece (en el país en el que se encuentra), como organización, fue víctima de incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad) durante los últimos doce meses?



Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

En específico y tomando como base las entidades e instituciones financieras que son víctimas de incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad) (22 entidades), se destaca que la gran mayoría (86% en promedio) investigan la fuente que generó dichos incidentes. A nivel sectorial, la totalidad de entidades en los sectores bancario (Banca Comercial o Múltiple y Banca de Desarrollo) y bursátil investigan la fuente[12].

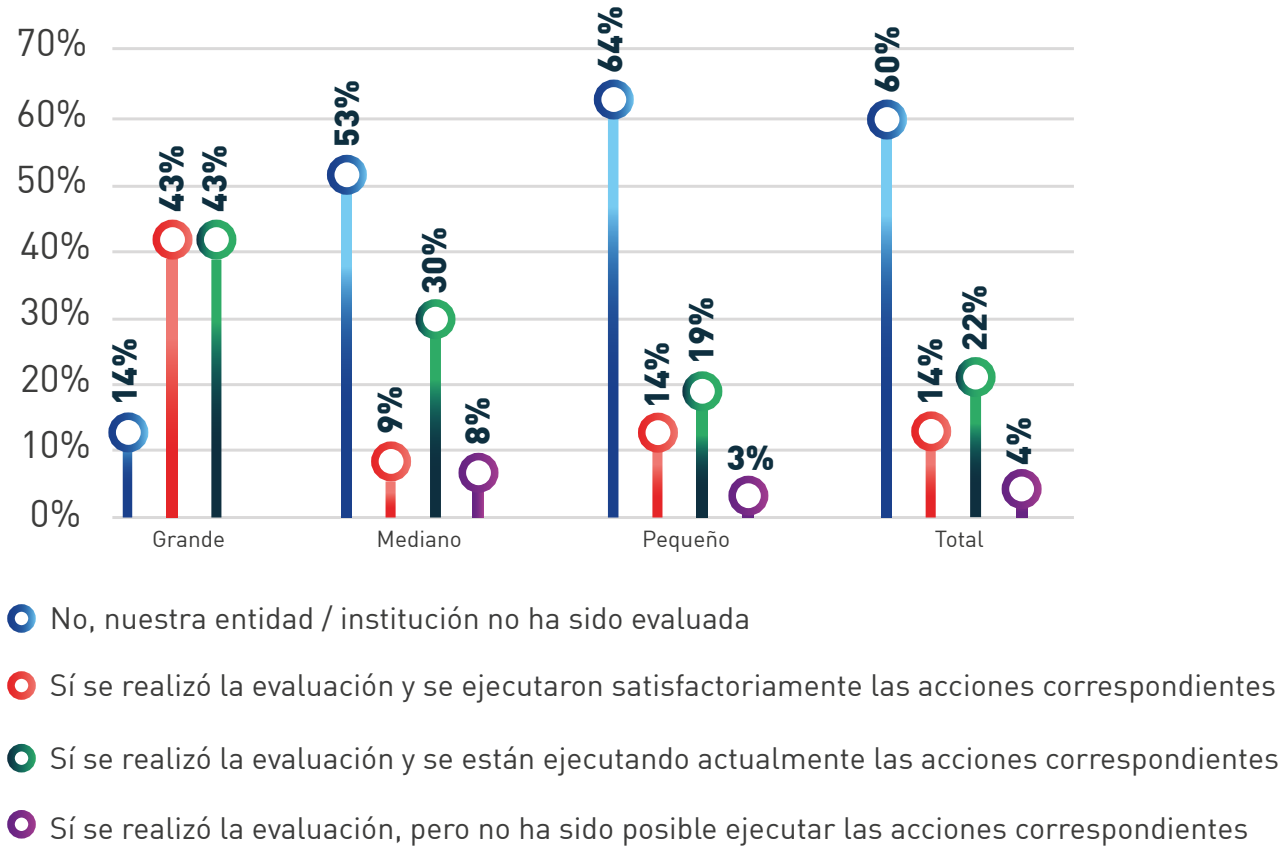
Además, y como resultado de las investigaciones, dichas entidades e instituciones financieras en el país identifican y priorizan las principales motivaciones de dichos incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad) sufridos durante el año 2018, siendo éstas: i) *motivos económicos* (74% de las entidades víctimas), ii) *motivos políticos / hacktivismo* (32% de las entidades víctimas), y iii) *robo de información personal* (26% de las entidades víctimas).

Con respecto al sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo), las principales motivaciones son las mismas, pero con porcentajes superiores de ocurrencia (89% de bancos víctimas por *motivos económicos*, 56% de los bancos víctimas por *motivos políticos / hacktivismo* y 33% de los bancos víctimas por *robo de información personal*). Vale la pena destacar que, en el sector bancario de la región de América Latina y el Caribe, el apartado *Motivos políticos / hacktivismo* no es considerado como una de las principales causas de motivación para generar ataques informáticos (Organización de los Estados Americanos, 2018).

12. La gráfica 42 del Anexo 2 presenta la comparación del resultado: ¿La entidad / institución financiera a la cual usted pertenece investigó la fuente que generó dichos incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad)? entre los diferentes sectores analizados del Sistema Financiero Mexicano.

Al preguntar si las entidades e instituciones financieras completan totalmente una evaluación de la madurez bajo una metodología de seguridad de la información (incluyendo ciberseguridad) o ejecutando todas sus acciones derivadas, se encuentran diferencias según el tamaño de la organización. Mientras que el 43% de las entidades grandes de México realiza dicha evaluación y lleva a cabo las acciones correspondientes, tan sólo el 30% de las entidades medianas y el 19% de las entidades pequeñas reflejan dicha situación. En contraste, preocupa que el 53% de las entidades medianas y el 64% de las entidades pequeñas no evalúan la madurez de seguridad digital. A nivel sectorial, igualmente preocupa que más del 70% de las entidades e instituciones financieras de los sectores Ahorro y Crédito Popular (SOCAP y SOFIPO) e Intermediarios financieros no bancarios de México indican que no han sido evaluadas[13].

Gráfica 21. ¿La entidad / institución financiera a la cual usted pertenece ha sido evaluada externamente en los últimos dos (2) años bajo alguna metodología de seguridad de la información (incluyendo ciberseguridad) para determinar su nivel de madurez?



Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

13. La gráfica 43 del Anexo 2 presenta la comparación del resultado: ¿La entidad / institución financiera a la cual usted pertenece ha sido evaluada externamente en los últimos dos (2) años bajo alguna metodología de seguridad de la información (incluyendo ciberseguridad) para determinar su nivel de madurez? entre los diferentes sectores analizados del Sistema Financiero Mexicano.

Las entidades e instituciones financieras del Sistema Financiero Mexicano que manifestaron que no completan totalmente una evaluación de la madurez de la seguridad digital o no ejecutan las acciones derivadas atribuyen esta situación principalmente a: i) insuficiencia de personal especializado (39% de entidades sin evaluación), ii) falta de asignación de presupuesto (28% de entidades sin evaluación), y iii) bajo conocimiento del impacto de las amenazas (27% de entidades sin evaluación).

Las principales causas reportadas por las cuales en promedio los bancos del sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México no completan totalmente una evaluación de la madurez de la seguridad digital o no ejecutan sus acciones derivadas coincide con las principales causas reportadas por el sector bancario en la región de América Latina y el Caribe: i) I*nsuficiente personal especializado* (un 36% en México versus un 46% en la región), ii) F*alta de asignación de presupuesto* (un 24% en México versus un 45% en la región), iii) *Falta de regulación específica que exija su implementación* (un 21% en México versus un 34% en la región) (Organización de los Estados Americanos, 2018).

3.2.4. Reportes de incidentes de seguridad digital

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

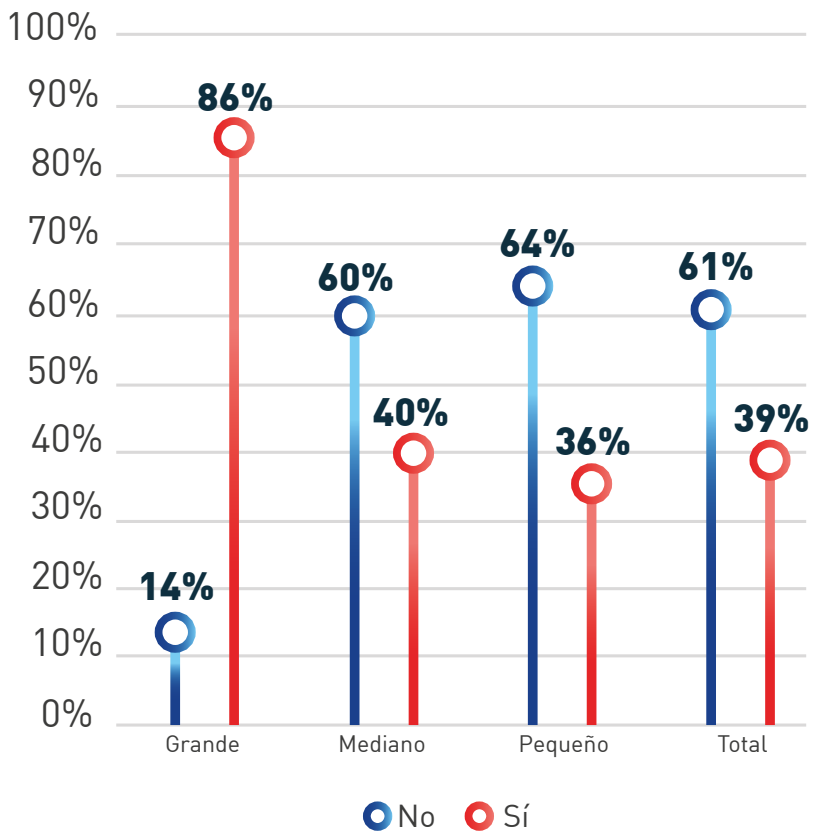
En términos generales, se aprecia que más de la mitad de las entidades e instituciones financieras de México – grandes (86%), medianas (57%) y pequeñas (53%) – ofrece un mecanismo para que sus colaboradores (empleados y contratistas) reporten incidentes (ataques exitosos) de seguridad digital sufridos, y en sectores como el sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México se alcanzan índices del 93%[14], superando incluso el promedio de la región de América Latina y el Caribe (68% de los bancos de la región) (Organización de los Estados Americanos, 2018).

En contraste con lo anterior, la existencia de mecanismos para que sus clientes (socios, asociados o usuarios) de servicios financieros reporten a la entidad incidentes (ataques exitosos) de seguridad digital sufridos varía según el tamaño de la entidad. Se aprecia que el 86% de las entidades grandes ofrece un mecanismo para que sus clientes de servicios financieros reporten a la entidad incidentes (ataques exitosos) de seguridad digital sufridos, en contraste con el 40% de las entidades medianas y el 36% de las entidades pequeñas del país.

En este caso, un 67% de los bancos del sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México ofrece este tipo de mecanismos a sus clientes[15], igualando el promedio de los bancos de la región de América Latina y el Caribe (68% del total) (Organización de los Estados Americanos, 2018).

14. La gráfica 44 del Anexo 2 presenta la comparación del resultado: ¿La entidad / institución financiera a la cual usted pertenece ofrece un mecanismo para que sus colaboradores (empleados y contratistas) reporten incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales)? entre los diferentes sectores analizados del Sistema Financiero Mexicano.
15. La gráfica 45 del Anexo 2 presenta la comparación del resultado: ¿La entidad / institución financiera a la cual usted pertenece ofrece un mecanismo para que sus clientes (socios, asociados o usuarios) de servicios financieros reporten incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales)? entre los diferentes sectores analizados del Sistema Financiero Mexicano.

Gráfica 22. ¿La entidad / institución financiera a la cual usted pertenece ofrece un mecanismo para que sus clientes (socios, asociados o usuarios) de servicios financieros reporten incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales)?



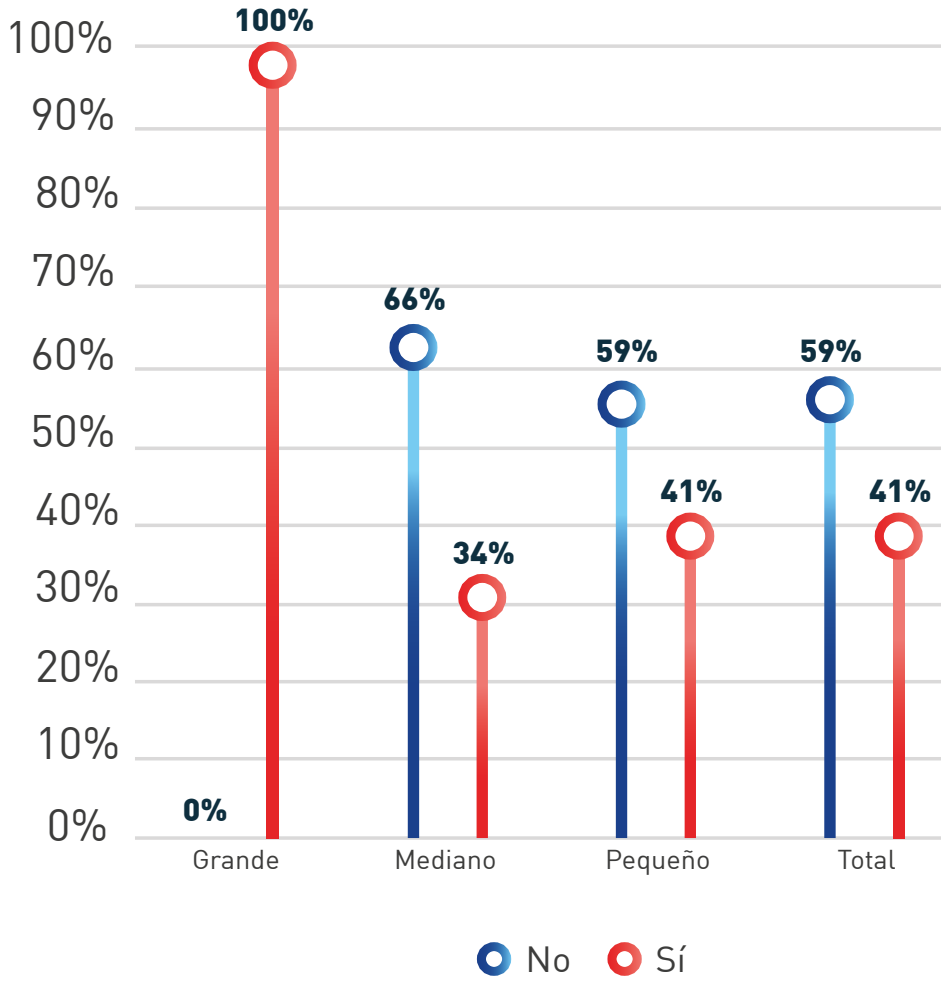
Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

De igual manera, la existencia de un plan de comunicaciones que permita informar a los clientes (socios, asociados o usuarios) de servicios financieros cuando su información personal se haya visto comprometida varía según el tamaño de la entidad. Se aprecia que en todas las entidades grandes existe un plan de comunicaciones para informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida, en contraste con un tercio de las entidades medianas (34%) del país y un poco más de un tercio de las entidades pequeñas (41%).

Al realizar un análisis sectorial dentro del Sistema Financiero Mexicano, también se evidencian contrastes como el presentado entre el sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México con un 81% del total de bancos con el mencionado plan de comunicaciones y el sector de Ahorro y Crédito Popular (SOCAP y SOFIPO) con tan solo un 23% de entidades que reportan la existencia del mismo[16].

16. La gráfica 46 del Anexo 2 presenta la comparación del resultado: ¿La entidad / institución financiera a la cual usted pertenece cuenta con un plan de comunicaciones que permita informar a sus clientes (socios, asociados o usuarios) de servicios financieros cuando su información personal se haya visto comprometida? entre los diferentes sectores analizados del Sistema Financiero Mexicano.

Gráfica 23. ¿La entidad / institución financiera a la cual usted pertenece cuenta con un plan de comunicaciones que permita informar a sus clientes (socios, asociados o usuarios) de servicios financieros cuando su información personal se haya visto comprometida?

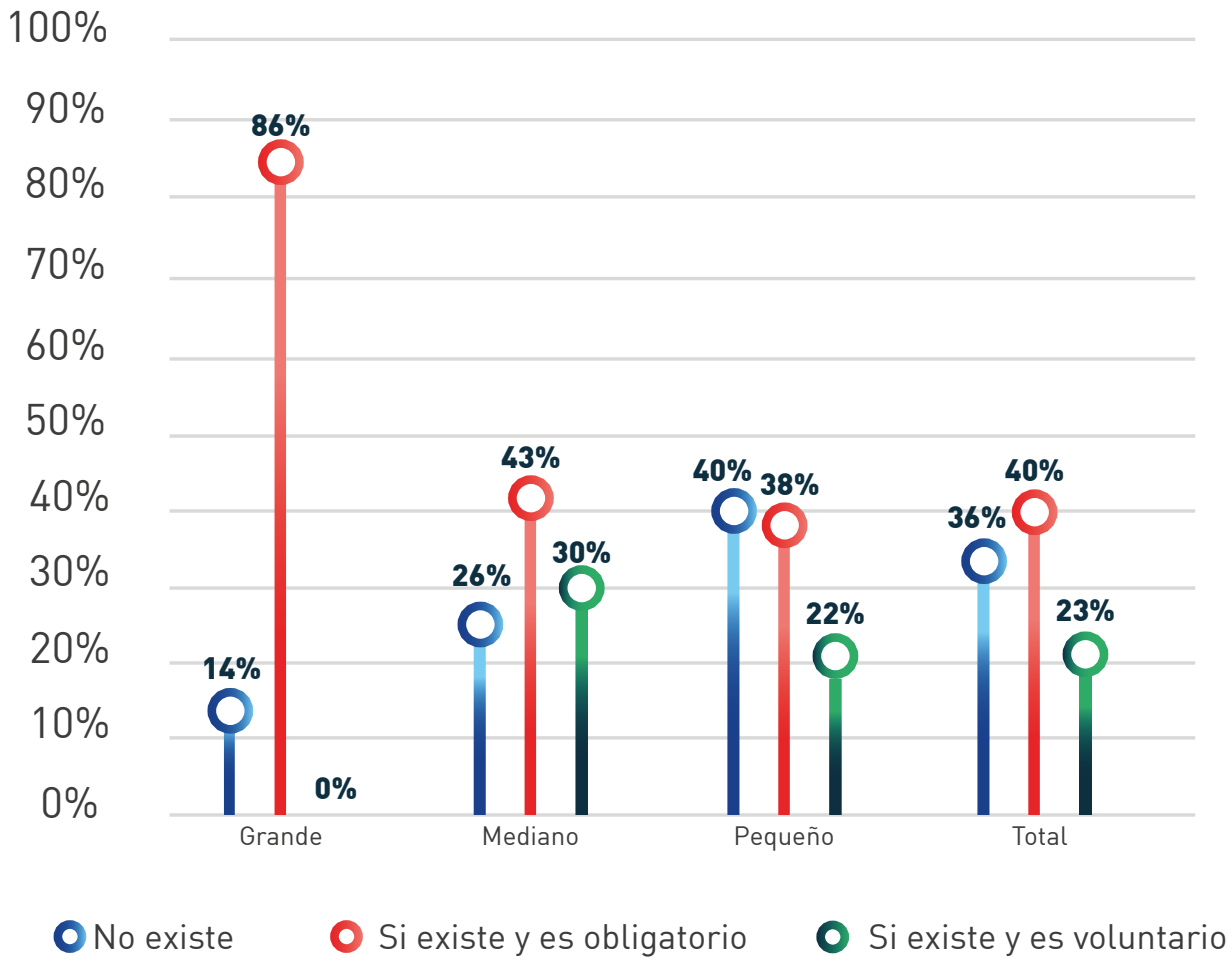


Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

En relación con el reporte de incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales) ante una autoridad de regulación en México por parte de las entidades e instituciones financieras, también se aprecian diferencias entre entidades grandes frente a entidades medianas y pequeñas. El 86% de las entidades grandes versus el 43% de las entidades medianas y el 38% de las entidades pequeñas manifiestan que conocen algún mecanismo para reportar incidentes y es obligatorio debido a la existencia de disposiciones establecidas por alguna autoridad de regulación. Por otra parte, se resalta que tan sólo el 14% de las entidades grandes del país en contraste con el 40% de las entidades pequeñas manifiesta que no existe mecanismo alguno de reporte de incidentes sufridos ante una autoridad de regulación[17].

17. La gráfica 47 del Anexo 2 presenta la comparación del resultado: ¿Conoce algún mecanismo para reportar incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales) sufridos por la entidad / institución financiera a la cual usted pertenece ante una autoridad de regulación en México? entre los diferentes sectores analizados del Sistema Financiero Mexicano.

Gráfica 24. ¿Conoce algún mecanismo para reportar incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales) sufridos por la entidad / institución financiera a la cual usted pertenece ante una autoridad de regulación en México?

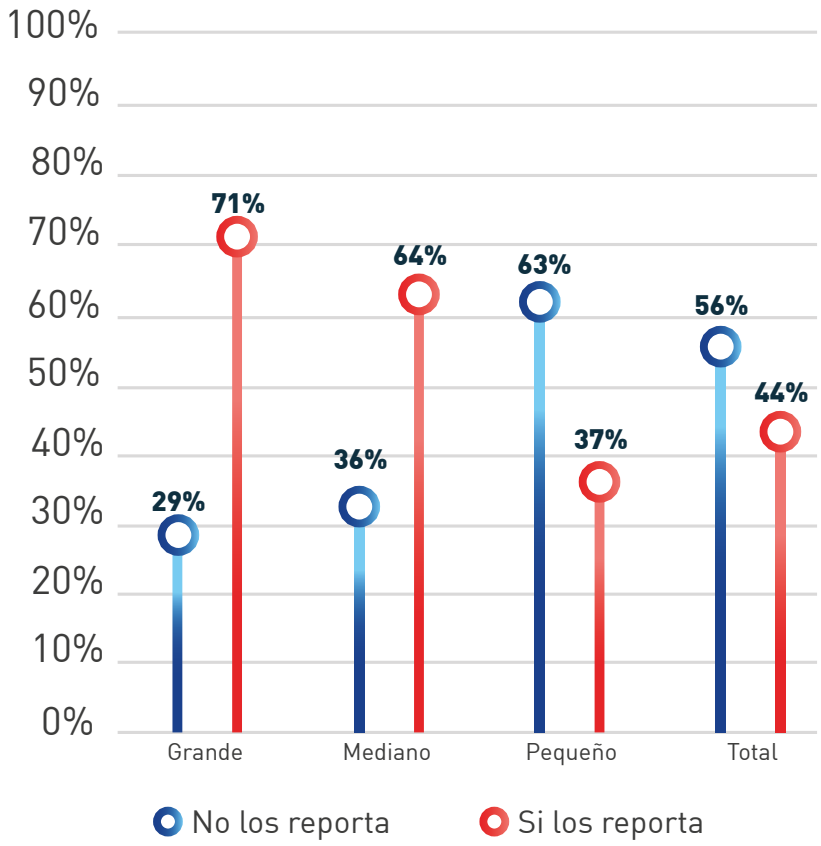


Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Adicionalmente, se aprecia que a medida que crece el tamaño de la entidad / institución financiera aumenta el reporte de incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales) sufridos ante una autoridad de procuración de justicia en México. El 71% de las entidades grandes, el 64% de las entidades medianas y el 37% de las entidades pequeñas reportan los incidentes sufridos ante este tipo de autoridad en el país. Esta situación contrasta con el hecho de que en sectores como el de Ahorro y Crédito Popular (SOCAP y SOFIPO), el Bursátil, el de Intermediarios Financieros No Bancarios y el FINTECH, menos del 40% del total de entidades realizan este tipo de reportes ante dichas autoridades[18].

18. La gráfica 48 del Anexo 2 presenta la comparación del resultado: ¿La entidad / institución financiera a la cual usted pertenece reporta los incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales) sufridos ante una autoridad de procuración de justicia en México? entre los diferentes sectores analizados del Sistema Financiero Mexicano.

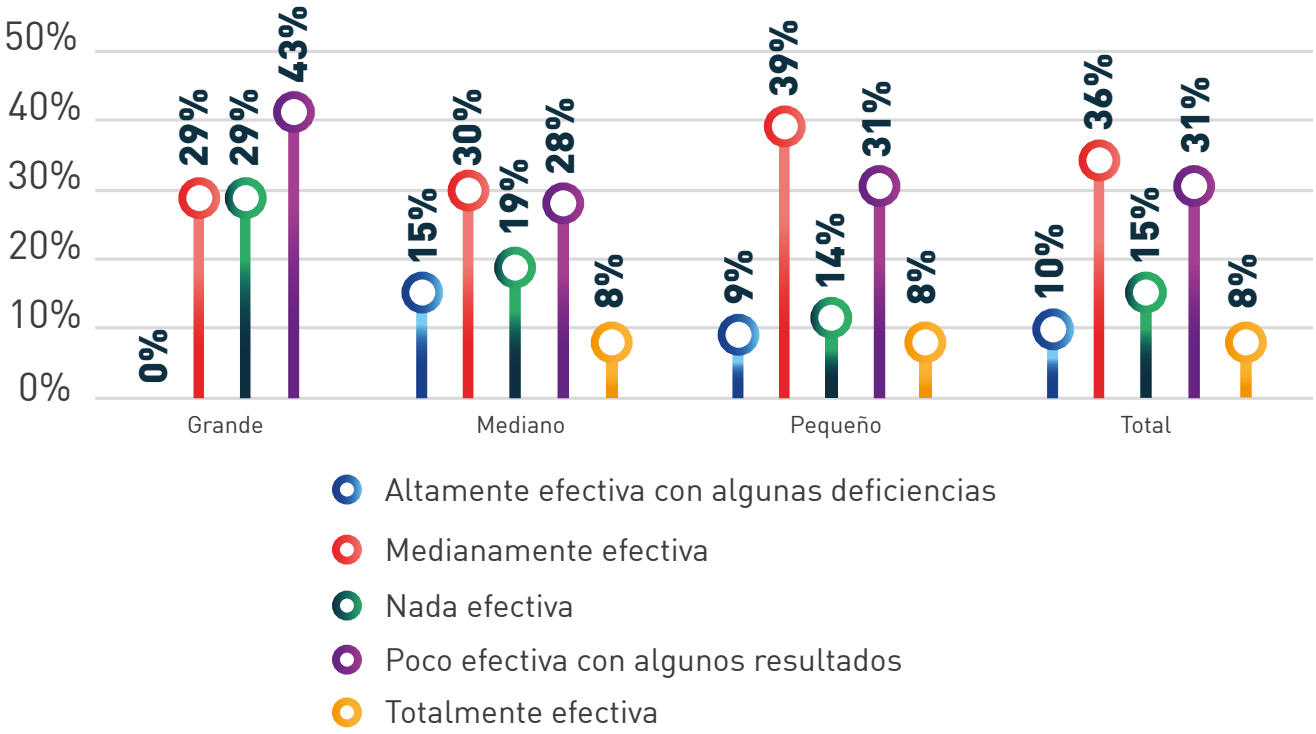
Gráfica 25. ¿La entidad / institución financiera a la cual usted pertenece reporta los incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad y fraudes ocurridos a través de medios digitales) sufridos ante una autoridad de procuración de justicia en México?



Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Finalmente, e independientemente del tamaño de la entidad / institución financiera, el 36% de entidades en México considera como medianamente efectivo el papel de las autoridades de procuración de justicia respecto a la investigación y judicialización de los ciberdelincuentes, mientras que el 31% considera como poco efectivo con algunos resultados el papel de las mencionadas autoridades.

Gráfica 26. ¿Cómo considera la efectividad de las autoridades de procuración de justicia en México respecto a la investigación y judicialización de los ciberdelincuentes?



Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Al analizar los resultados para el sector bancario mexicano versus los resultados para el sector bancario de la región América Latina y el Caribe, se concluye que existen coincidencias respecto de la consideración de efectividad de las mencionadas autoridades: i) medianamente efectiva (36% de los bancos de México versus 31% de los bancos de la región) y ii) poco efectiva con algunos resultados (31% de los bancos de México versus 37% de los bancos de la región) (Organización de los Estados Americanos, 2018).

3.2.5. Capacitación y concientización

Finalmente, la gestión sistemática de riesgos de seguridad digital debe contar con acciones de capacitación y concientización dentro de las organizaciones. En particular y sin distinguir por tamaño de la entidad / institución financiera, más de la mitad (57%) de las entidades e instituciones financieras de México cuenta con planes de concientización y formación en asuntos de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales para sus colaboradores. Se destaca que el 100% de las entidades grandes del Sistema Financiero Mexicano y el 100% de entidades del Sector Bursátil cuentan con dichos planes en el país[19].

19. La gráfica 49 del Anexo 2 presenta la comparación del resultado: *¿Cuenta la entidad / institución financiera a la cual usted pertenece con planes de concientización y formación en asuntos de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales para sus colaboradores?* entre los diferentes sectores analizados del Sistema Financiero Mexicano.

Considerada la base de entidades e instituciones financieras de México que cuentan con planes de preparación, respuesta y capacitación en asuntos de seguridad digital para sus colaboradores, se destaca que el 61% de los mismos se ejecutan anualmente, el 24% semestralmente y el 15% trimestralmente[20].

Por otra parte, el 67% de las entidades e instituciones financieras en el país prueban la capacidad de los colaboradores de la entidad para responder adecuadamente a eventos (ataques exitosos y no exitosos) de seguridad de la información (incluyendo ciberseguridad) y amenazas tales como phishing e ingeniería social con periodicidad anual, el 20% con periodicidad semestral y el 13% con periodicidad trimestral[21].

Finalmente, en relación con asuntos de capacitación y concientización, las entidades e instituciones financieras identifican que los mecanismos más efectivos a partir de los cuales se ha generado mayor conciencia en la entidad respecto de los riesgos de seguridad digital son: i) Capacitaciones y medios de comunicación internos, ii) Acciones debidas al cumplimiento de requisitos legales y/o regulatorios, y iii) Publicaciones gratuitas en revistas, sitios web y listas de correo. Estos tres (3) mecanismos fueron también priorizados por los sectores bancario (Banca Comercial o Múltiple y Banca de Desarrollo) y Ahorro y Crédito Popular (SOCAP y SOFIPO) de México.

Cuadro 10. Mecanismo más efectivo a partir del cual se ha generado mayor conciencia en la entidad / institución financiera respecto de los riesgos de seguridad digital

	Grande	Mediana	Pequeña	Total
Capacitaciones y medios de comunicación internos	1,29	2,05	2,28	**2,19**
Requisitos legales y/o regulatorios	2,17	2,67	2,68	**2,66**
Publicaciones gratuitas en revistas, sitios web y listas de correo	4,75	3,65	4,14	**4,05**
Documentación de organismos especializados en la materia	4,40	4,48	4,27	**4,32**
Redes sociales	4,00	5,12	4,29	**4,46**
Presentaciones y debates en conferencias	4,33	4,74	4,66	**4,66**
Servicios especializados por suscripción	5,75	5,41	5,36	**5,39**
Asociaciones profesionales	7,25	5,91	5,23	**5,43**
Otro	**7,50**	**6,80**	**7,18**	**7,10**

Nota: : 236 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 e instituciones financieras en México

20. La gráfica 50 del Anexo 2 presenta la comparación del resultado: ¿Con que frecuencia se ejecutan dichos planes de concientización y formación? entre los diferentes sectores analizados del Sistema Financiero Mexicano.
21. La gráfica 51 del Anexo 2 presenta la comparación del resultado: ¿Con qué frecuencia se prueba la capacidad de los empleados de la institución financiera a la cual usted pertenece a responder adecuadamente frente a 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? entre los diferentes sectores analizados del Sistema Financiero Mexicano.

3.3. Impacto de los incidentes de seguridad digital

Una vez caracterizadas las entidades e instituciones financieras que participaron en el desarrollo del presente estudio y presentados los resultados encontrados sobre la gestión de riesgos de seguridad digital por parte del Sistema Financiero Mexicano, a continuación, se presenta el análisis del impacto de los incidentes de seguridad digital en entidades e instituciones financieras en México durante el año 2018.

Como se mencionó, la muestra de entidades e instituciones financieras a partir de las cuales se presentan los siguientes resultados alcanza unos activos de USD $682.398 millones de dólares y unas utilidades netas de USD $7.150 millones de dólares a 31 de diciembre de 2018, lo que permite afirmar que dicha muestra contiene una representatividad de los distintos niveles de activos y patrimonio del país. Se destaca que los activos reportados por los bancos del sector de Banca Comercial o Múltiple aporta USD $429.368 millones de dólares de los activos, correspondientes a casi un 63% del total de la muestra.

Cuadro 11. Distribución del valor estimado de Activos por sector del Sistema Financiero Mexicano (millones de dólares americanos)

	Grande	Mediana	Pequeña	Total
Banca Comercial o Múltiple	150.503	217.664	61.201	**429.368**
Banca de Desarrollo		68.538	27.876	**96.414**
Sector Bursátil			17.998	**17.998**
Sector de Ahorro y Crédito Popular (SOCAP)		2.780	2.558	**5.338**
Sector de Ahorro y Crédito Popular (SOFIPO)	3	213	14	**230**
Sector de Intermediarios Financieros No Bancarios		18	2.903	**2.921**
Sector FINTECH			130.130	**130.130**
SISTEMA FINANCIERO MEXICANO	150.506	289.213	242.679	**682.398**

Nota: 235 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

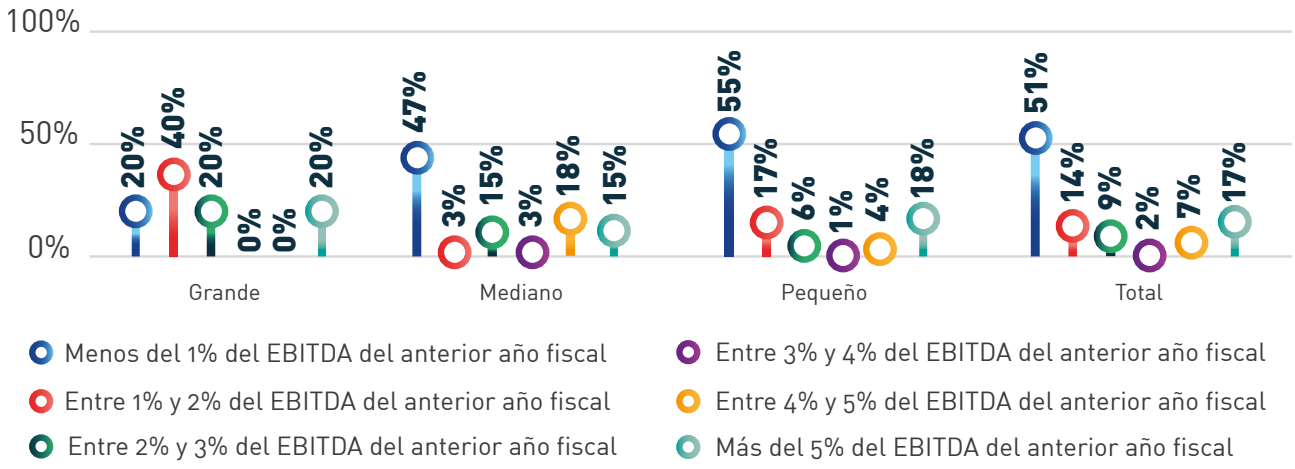
Cuadro 12. Distribución del valor estimado de EBITDA por sector del Sistema Financiero Mexicano (millones de dólares americanos)

	Grande	Mediana	Pequeña	Total
Banca Comercial o Múltiple	1.650	636	564	**2.850**
Banca de Desarrollo		1.490	738	**2.228**
Sector Bursátil			58	**58**
Sector de Ahorro y Crédito Popular (SOCAP)		47	165	**211**
Sector de Ahorro y Crédito Popular (SOFIPO)	0,005	18	1	**19**
Sector de Intermediarios Financieros No Bancarios		0,05	793	**794**
Sector FINTECH			**991**	**991**
SISTEMA FINANCIERO MEXICANO	**1.650**	**2.190**	**3.310**	**7.150**

Nota: 235 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

A partir de las entidades e instituciones financieras que presentaron información, se observa que el 51% de las entidades en la región manifiestan que el presupuesto de seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) equivale en promedio a menos del 1% del EBITDA del anterior año fiscal, el 14% de las entidades afirman que el valor de dicho presupuesto está entre el 1% y el 2% del EBITDA del anterior año fiscal, el 9% de las entidades lo sitúan entre el 2% y el 3% del EBITDA del anterior año fiscal, el 2% de las entidades entre el 3% y el 4% del EBITDA del anterior año fiscal, el 7% de las entidades entre el 4% y el 5% del EBITDA del anterior año fiscal y el 17% de las entidades manifiestan que dicho presupuesto equivale a un valor mayor al 5% del EBITDA del anterior año fiscal.

Gráfica 27. Presupuesto de seguridad de la información (incluyendo ciberseguridad) como % del EBITDA del año inmediato anterior



Nota: 235 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Se destacan las diferencias entre las estimaciones de dicho presupuesto entre el sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México con el promedio del sector bancario de la región América Latina y el Caribe[22], en donde se aprecia que el 43% de bancos en México versus el 61% de bancos en la región manifiestan que dicho presupuesto equivale en promedio a menos del 1% del EBITDA del anterior año fiscal, el 37% de bancos en México versus el 34% de bancos en la región afirman que el valor de dicho presupuesto está entre el 1% y el 5% del EBITDA del anterior año fiscal y el 20% de bancos en México versus el 5% de bancos en la región sitúan el valor de dicha partida por encima del 5% del EBITDA del anterior año fiscal (Organización de los Estados Americanos, 2018).

Del análisis de los resultados de la muestra se puede inferir que el valor del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales como porcentaje del EBITDA del anterior año fiscal equivale al 2,18%. También se estima que este presupuesto para entidades grandes equivale al 2,30% del EBITDA del anterior año fiscal, para entidades medianas al 2,51% del EBITDA del anterior año fiscal y para entidades pequeñas al 2,04% del EBITDA del anterior año fiscal.

22. La gráfica 52 del Anexo 2 presenta la comparación del resultado Dinámica del presupuesto de seguridad digital en el último año entre los diferentes sectores analizados del Sistema Financiero Mexicano.

Cuadro 13. Presupuesto de la seguridad digital como % del EBITDA del año inmediato anterior por sector del Sistema Financiero Mexicano

	Grande	Mediana	Pequeña	Total
Banca Comercial o Múltiple	2,30%	3,05%	1,88%	2,38%
Banca de Desarrollo		1,63%	2,50%	2,00%
Sector Bursátil			2,57%	2,57%
Sector de Ahorro y Crédito Popular (SOCAP)		2,26%	1,65%	1,90%
Sector de Ahorro y Crédito Popular (SOFIPO)		3,33%	5,00%	4,00%
Sector de Intermediarios Financieros No Bancarios			1,82%	1,82%
Sector FINTECH			2,65%	2,65%
SISTEMA FINANCIERO MEXICANO	2,30%	2,51%	2,04%	2,18%

Nota: 235 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

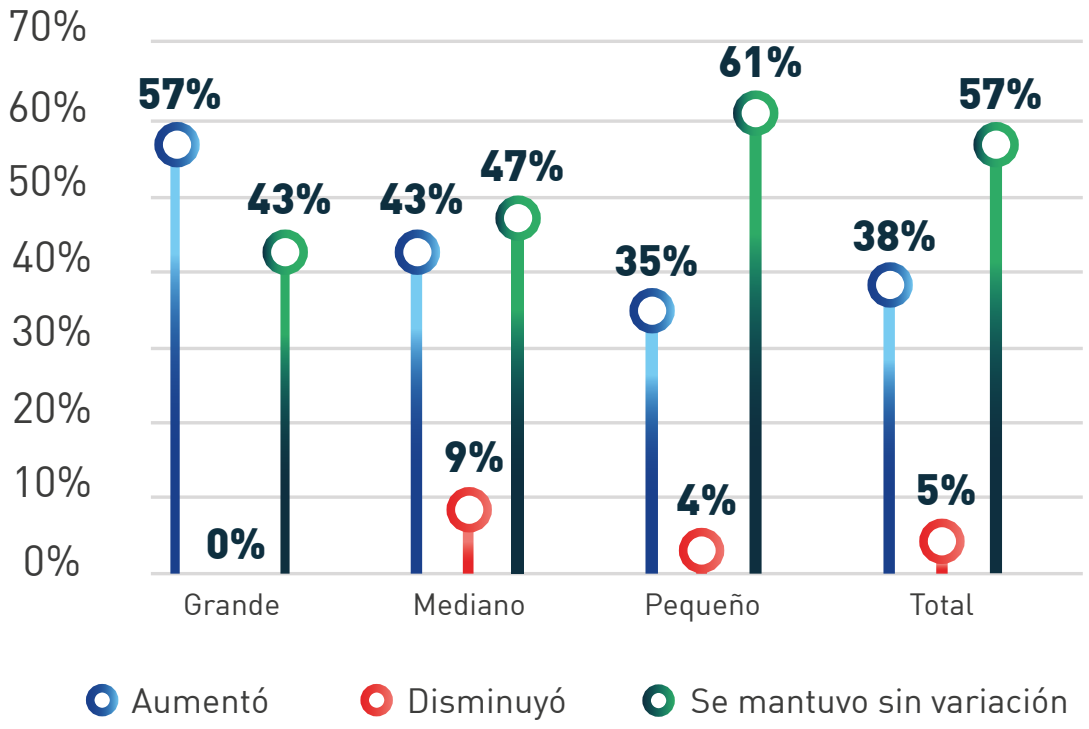
Al analizar por sector del Sistema Financiero Mexicano, se aprecia por ejemplo que el presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales para el sector de banca comercial o múltiple equivale al 2,38% del EBITDA del anterior año fiscal, mientras que dicho presupuesto para el sector de intermediarios financieros no bancarios equivale al 1,82% del EBITDA del anterior año fiscal.

Además, en comparación al año fiscal inmediato anterior, el 57% de las entidades e instituciones financieras en el país manifiestan que se mantuvo sin variación el presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales, el 38% manifiesta que había aumentado y tan sólo el 5% manifiesta que se había disminuido. No obstante, los resultados específicos para el sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México son diferentes: el 31% de los bancos en el país señala que se mantiene sin variación dicho presupuesto; el 64%, que aumenta, y tan sólo el 5% asegura que disminuye.

Al analizar en detalle, se apreciaron diferencias en los resultados para cada tamaño de entidad / institución financiera para el Sistema Financiero Mexicano. Se destaca que para el 57% de las entidades grandes, el 43% de las entidades medianas y el 35% de las entidades pequeñas, el presupuesto de seguridad digital aumenta en comparación al año fiscal inmediato anterior. Por otro lado, para el 43% de las entidades grandes, el 47% de las entidades medianas y el 61% de las entidades pequeñas, el presupuesto de seguridad digital se mantiene igual a aquel del año fiscal inmediato anterior[23].

23. La gráfica 53 del Anexo 2 presenta la comparación del resultado Crecimiento del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales de la entidad / institución financiera entre los diferentes sectores analizados del Sistema Financiero Mexicano.

Gráfica 28. Dinámica del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales en el último año

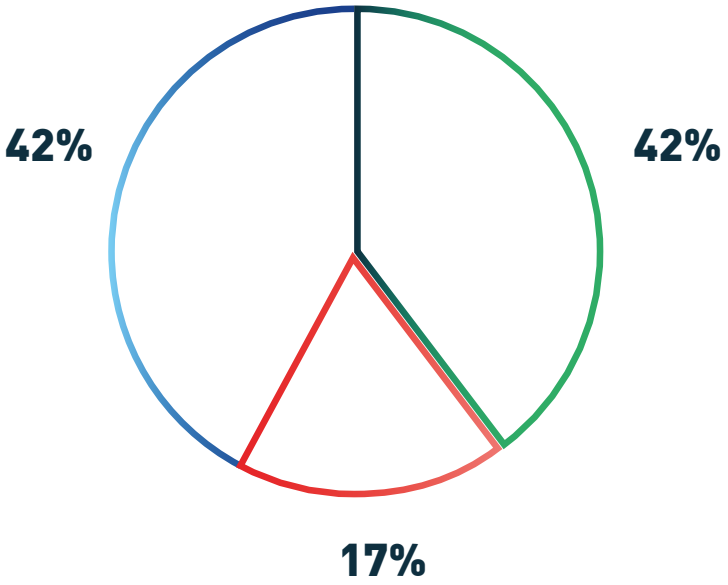


Nota: 235 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Del total de entidades e instituciones financieras que manifiestan que el presupuesto de seguridad digital aumenta en comparación al año fiscal inmediato anterior, el 76% indicó que dicho aumento se debe a *Cumplimiento Regulatorio*, el 54% que es por *Cumplimiento de nuevas políticas internas*, y el 38% a *Continuidad de negocio / recuperación de desastres*. En relación con el sector bancario, se aprecia que en promedio los bancos de México y los bancos de la región América Latina y el Caribe coinciden en que principalmente el aumento se debe a *Cumplimiento Regulatorio* (70% de bancos en México versus 62% de bancos en la región) y *Nuevas amenazas de ciberseguridad por el uso de NTIC* (48% de bancos en México versus 54% de bancos en la región) (Organización de los Estados Americanos, 2018).

Por otro lado, del total de entidades e instituciones financieras que manifiestan que el presupuesto de seguridad digital disminuye en comparación al año fiscal inmediato anterior, el 42% señala que se debe a una *Disminución de la Utilidad de la entidad / institución financiera, el 42% a Ajuste presupuestal por altos costos asociados a la seguridad de la información y el 17% a Cambio y transformación del negocio con impacto en el apetito de riesgo.*

Gráfica 29. Razones de la disminución del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales

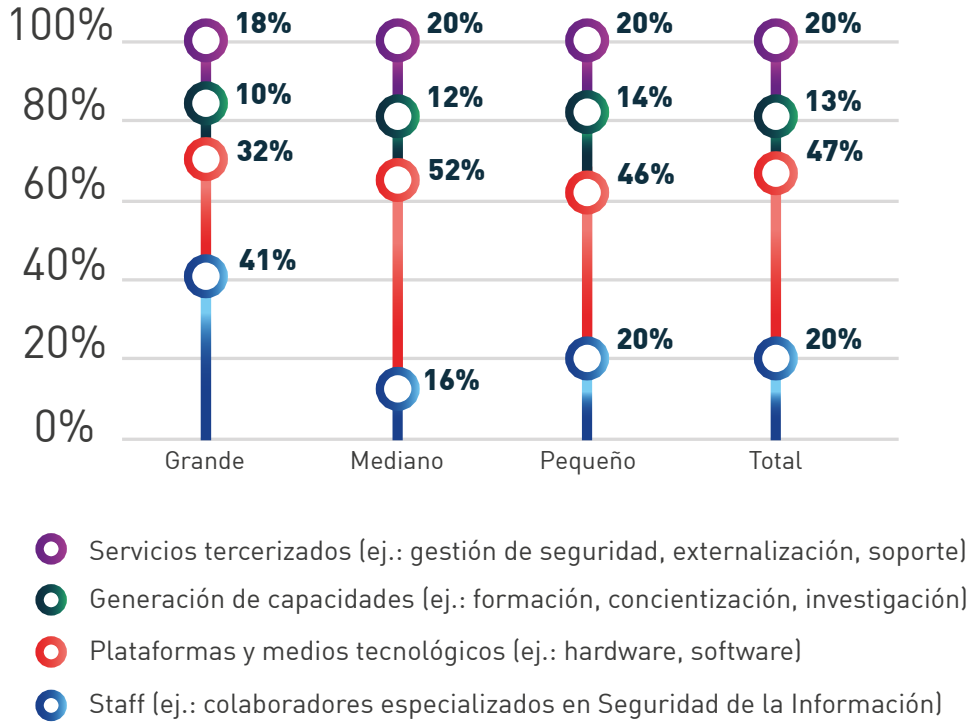


- Ajuste presupuestal por altos costos asociados a la seguridad de la información
- Cambio o transformación del negocio con impacto en el apetito de riesgo
- Disminución de la utilidad de la entidad / institución financiera

Nota: 12 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

El presupuesto destinado por parte de una entidad / institución financiera promedio del Sistema Financiero Mexicano a seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales se distribuye del siguiente modo: el 47% en *Plataformas y medios tecnológicos (ej.: hardware, software)*, el 20% en *Staff (ej.: colaboradores especializados en Seguridad de la Información)*, el 20% en *Servicios tercerizados (ej.: gestión de seguridad, externalización, soporte)* y el 13% en *Generación de capacidades (ej.: formación, concientización, investigación)*.

Gráfica 30. Distribución del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales de la entidad / institución financiera



Nota: 196 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Al comparar la distribución del mencionado presupuesto entre el sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México con el promedio del sector bancario de la región América Latina y el Caribe[24] se aprecia lo siguiente: i) el 35% en México versus el 43% en la región para *Plataformas y medios tecnológicos (ej.: hardware, software)*, ii) el 23% en México versus el 22% en la región para *Staff (ej.: colaboradores especializados en Seguridad de la Información)*, iii) el 31% en México versus el 22% en la región para *Servicios tercerizados (ej.: gestión de seguridad, externalización, soporte)* y iv) el 11% en México versus el 13% en la región para *Generación de capacidades (ej.: formación, concientización, investigación)* (Organización de los Estados Americanos, 2018).

A partir de la estimación del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales como porcentaje del EBITDA del año inmediato anterior que dedican las entidades e instituciones financieras en el país por tamaño de la organización y de la estimación del porcentaje de presupuesto destinado a recursos humanos (Staff), se desprende que: i) el presupuesto asignado a un miembro promedio del equipo de seguridad digital por una entidad grande en el país en 2018 es de USD $67.674 al año aproximadamente, ii) el presupuesto asignado a un miembro promedio del equipo de seguridad digital por una entidad mediana en el país en 2018 fue de USD $49.453 al año aproximadamente, y iii) el presupuesto asignado a un miembro promedio del equipo de seguridad digital por una entidad pequeña en el país en 2018 fue de USD $12.488 al año aproximadamente.

24. La gráfica 54 del Anexo 2 presenta la comparación del resultado Distribución del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales de la entidad / institución financiera entre los diferentes sectores analizados del Sistema Financiero Mexicano.

El valor promedio para el Sistema Financiero Mexicano sin distinción de tamaño equivale a USD $25.557 al año aproximadamente versus un presupuesto asignado a un miembro promedio del equipo de seguridad digital por un banco en la región América Latina y el Caribe de USD $19.437 al año aproximadamente (Organización de los Estados Americanos, 2018).

Por otro lado, de la información recolectada de la muestra de entidades e instituciones financieras se estima que el retorno de inversión (ROI) en seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales equivale aproximadamente a 10,94%. Al analizar por tamaño de entidad se obtiene: i) un 15% para una entidad grande en el país (representado por la Banca Comercial o Múltiple), ii) un 9,58% para una entidad mediana en el país, y iii) un 10,36% para una entidad pequeña del Sistema Financiero Mexicano.

Cuadro 14. Retorno de inversión (ROI) en seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales

	Grande	Mediana	Pequeña	Total
Banca Comercial o Múltiple	15,00%	7,50%	17,50%	**11,56%**
Banca de Desarrollo				
Sector Bursátil			2,50%	**2,50%**
Sector de Ahorro y Crédito Popular (SOCAP)		13,75%	5,00%	**9,38%**
Sector de Ahorro y Crédito Popular (SOFIPO)				
Sector de Intermediarios Financieros No Bancarios			17,50%	**17,50%**
Sector FINTECH			12,50%	**12,50%**
SISTEMA FINANCIERO MEXICANO	**15,00%**	**9,58%**	**10,36%**	**10,94%**

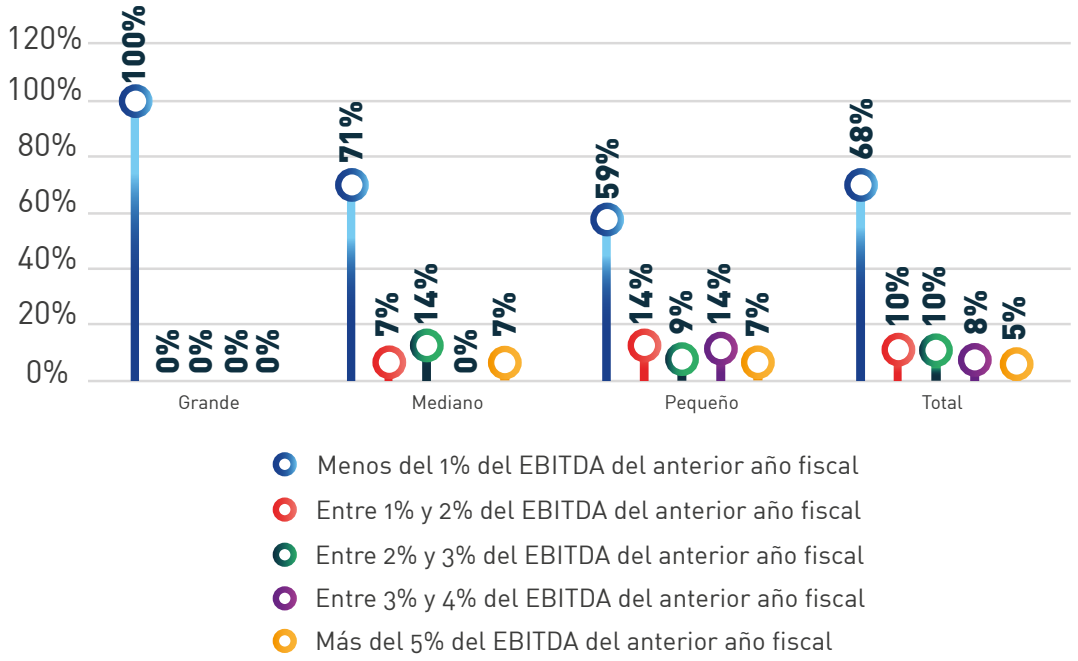
Nota: 19 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Respecto a las estimaciones del retorno sobre la inversión en seguridad digital, i) el 33% de las entidades medianas y el 20% de las entidades pequeñas consideran que son retornos de baja rentabilidad, ii) el 20% de las entidades pequeñas los ven como retornos de media rentabilidad, iii) el 100% de las entidades grandes, el 33% de las entidades medianas y el 40% de las entidades pequeñas opinan que son retornos de alta rentabilidad, y iv) el 33% de las entidades medianas y el 20% de las entidades pequeñas los definen como retornos de muy alta rentabilidad.

Ahora, a partir de las entidades e instituciones financieras que presentaron información[25], se destaca que el 68% de las entidades en la región manifiestan que el costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) equivale en promedio a menos del 1% del EBITDA del anterior año fiscal, el 10% de las entidades calculan que el valor de dicho costo está entre el 1% y el 2% del EBITDA del anterior año fiscal, el 10% de las entidades ubican el valor de dicho costo entre el 2% y el 3% del EBITDA del anterior año fiscal, el 8% de las entidades sitúan esa partida entre el 3% y el 4% del EBITDA del anterior año fiscal y el 5% manifiestan que el valor de dicho costo está por encima del 5% del EBITDA del anterior año fiscal.

Del análisis también se puede inferir que a medida que aumenta el tamaño de la entidad / institución financiera disminuye el costo total de respuesta y de recuperación ante incidentes de seguridad digital como % del EBITDA del año inmediato anterior. Por ejemplo, el 100% de las entidades grandes manifiestan que el valor de dicho costo es menor del 1% del EBITDA del anterior año fiscal, mientras que el 71% de las entidades medianas y el 59% de las entidades pequeñas manifiestan que dicho costo se encuentra en ese rango.

Gráfica 31. Costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) como % del EBITDA del año inmediato anterior



Nota: 40 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

25. La gráfica 55 del Anexo 2 presenta la comparación del resultado ¿La entidad / institución financiera a la cual usted pertenece estimó el costo total de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) para el último año fiscal? entre los diferentes sectores analizados del Sistema Financiero Mexicano.

Destaca la similitud entre las estimaciones de dicho costo en el sector bancario (Banca Comercial o Múltiple y Banca de Desarrollo) de México y el promedio del sector bancario de la región América Latina y el Caribe[26]: el 76% de bancos en México versus el 73% de bancos en la región manifiestan que dicho costo equivale en promedio a menos del 1% del EBITDA del anterior año fiscal y el 24% de bancos en México versus el 27% de bancos en la región manifiestan que el valor de dicho presupuesto está entre el 1% y el 5% del EBITDA del anterior año fiscal (Organización de los Estados Americanos, 2018).

Del análisis de los resultados de la muestra se puede inferir que el valor del costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) como % del EBITDA del año inmediato anterior equivale al 1,59%. También se estima que este presupuesto para entidades grandes equivale al 1% del EBITDA del anterior año fiscal, para entidades medianas equivale al 1,54% del EBITDA del anterior año fiscal y para entidades pequeñas equivale al 1,73% del EBITDA del anterior año fiscal.

Cuadro 15. Costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) por sector del Sistema Financiero Mexicano

	Grande	Mediana	Pequeña	Total
Banca Comercial o Múltiple	1,00%	1,39%	1,80%	**1,42%**
Banca de Desarrollo		1,00%	1,00%	**1,00%**
Sector Bursátil			2,50%	**2,50%**
Sector de Ahorro y Crédito Popular (SOCAP)		2,00%	1,13%	**1,56%**
Sector de Ahorro y Crédito Popular (SOFIPO)			1,00%	**1,00%**
Sector de Intermediarios Financieros No Bancarios			1,70%	**1,70%**
Sector FINTECH			2,63%	**2,63%**
SISTEMA FINANCIERO MEXICANO	**1,00%**	**1,54%**	**1,73%**	**1,59%**

Nota: 40 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

26. La gráfica 56 del Anexo 2 presenta la comparación del resultado Costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) como % del EBITDA del año inmediatamente anterior entre los diferentes sectores analizados del Sistema Financiero Mexicano.

Al analizar por sector del Sistema Financiero Mexicano, se aprecia por ejemplo que el costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) para el sector de banca comercial o múltiple equivale al 1,42% del EBITDA del anterior año fiscal, mientras que para el sector bursátil equivale al 2,50% del EBITDA del anterior año fiscal.

A partir de la información recolectada de las entidades e instituciones financieras en México que participaron en el desarrollo del presente estudio, se hizo posible analizar algunos indicadores promedio para el país y por tamaño de organización que permiten estimar el impacto de los incidentes de seguridad digital durante el año 2018, por ejemplo: i) el presupuesto y costo total anual relacionados con la seguridad digital como % del EBITDA del año inmediato anterior, ii) el costo total anual de respuesta y de recuperación ante incidentes de seguridad digital por entidad / instituciones financieras del Sistema Financiero Mexicano, y iii) el costo total anual de respuesta y de recuperación ante incidentes de seguridad digital de las entidades e instituciones financieras del Sistema Financiero Mexicano.

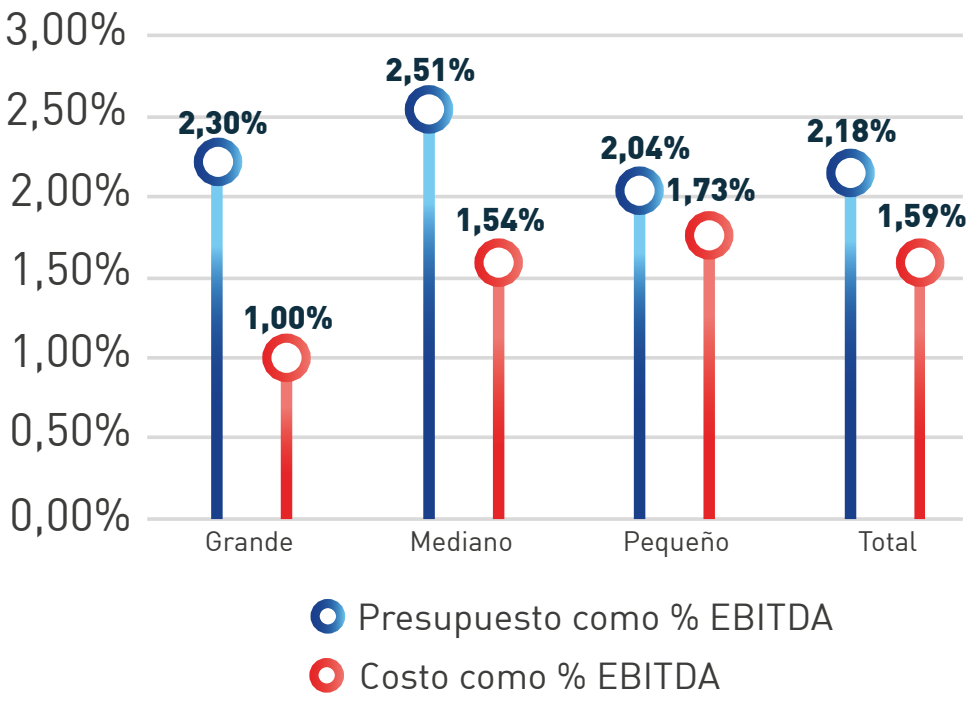
Cuadro 16. Estimación del presupuesto y del costo total anual relacionados con la seguridad digital del año inmediato anterior (millones de dólares americanos)

	Presupuesto por sector				Costo por sector			
	Grande	Mediana	Pequeña	Total	Grande	Mediana	Pequeña	Total
Banca Comercial o Múltiple	38	19	11	**68**	17	9	10	**35**
Banca de Desarrollo		24	18	**43**		15	7	**22**
Sector Bursátil			1	**1**			1	**1**
Sector de Ahorro y Crédito Popular (SOCAP)		1	3	**4**		1	2	**3**
Sector de Ahorro y Crédito Popular (SOFIPO)		1	0	**1**		0	0	**0**
Sector de Intermediarios Financieros No Bancarios			14	**14**			13	**13**
Sector FINTECH			26	**26**			26	**26**
SISTEMA FINANCIERO MEXICANO	**38**	**45**	**74**	**157**	**17**	**34**	**57**	**107**

Fuente: SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

De lo analizado en el presente capítulo del documento, a partir de la muestra de entidades e instituciones financieras del Sistema Financiero Mexicano que reportaron información en promedio se concluye que: i) el presupuesto destinado a la seguridad digital por una entidad / institución financiera promedio en la región equivale aproximadamente al 2,18% del EBITDA del año inmediato anterior (versus el 2,09% para el sector bancario de la región América Latina y el Caribe), y ii) el costo total de respuesta y de recuperación ante incidentes de seguridad digital para una entidad / institución financiera promedio en la región equivale aproximadamente al 1,59% del EBITDA del año inmediato anterior (versus el 1,52% para el sector bancario de la región América Latina y el Caribe).

Gráfica 32. Presupuesto y costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) como % del EBITDA del año inmediato anterior



Fuente: SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

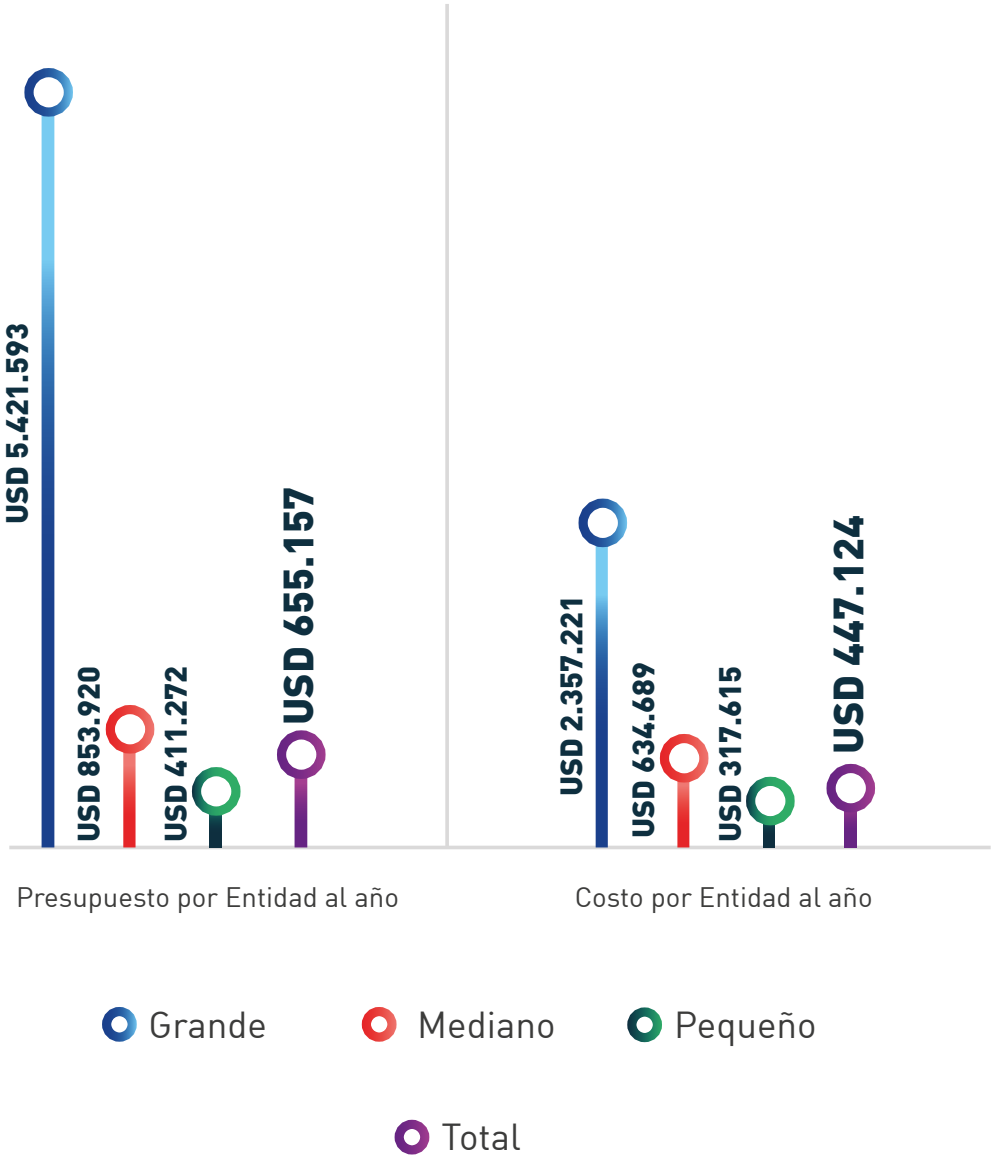
Cuadro 17. Presupuesto y costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) como % del EBITDA del año inmediato anterior por sector

	Presupuesto por sector como % del EBITDA				Costo por sector como % del EBITDA			
	Grande	Mediana	Pequeña	Total	Grande	Mediana	Pequeña	Total
Banca Comercial o Múltiple	2,30%	3,05%	1,88%	**2,38%**	1,00%	1,39%	1,80%	**1,42%**
Banca de Desarrollo		1,63%	2,50%	**2,00%**		1,00%	1,00%	**1,00%**
Sector Bursátil			2,57%	**2,57%**			2,50%	**2,50%**
Sector de Ahorro y Crédito Popular (SOCAP)		2,26%	1,65%	**1,90%**		2,00%	1,13%	**1,56%**
Sector de Ahorro y Crédito Popular (SOFIPO)		3,33%	5,00%	**4,00%**			1,00%	**1,00%**
Sector de Intermediarios Financieros No Bancarios			1,82%	**1,82%**			1,70%	**1,70%**
Sector FINTECH			2,65%	**2,65%**			2,63%	**2,63%**
SISTEMA FINANCIERO MEXICANO	2,30%	2,51%	2,04%	**2,18%**	1,00%	1,54%	1,73%	**1,59%**

Fuente: SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

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 una entidad grande promedio equivale aproximadamente a US $2.357.221 al año, para una entidad mediana promedio supone aproximadamente US $634.689 al año y para una entidad pequeña promedio equivale aproximadamente a US $317.615 al año.

Gráfica 33. Presupuesto y costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad)



Fuente: SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Cuadro 18. Presupuesto y costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) por sector (miles de dólares americanos)

	Presupuesto por entidad / institución financiera				Costo por entidad / institución financiera			
	Grande	Mediana	Pequeña	Total	Grande	Mediana	Pequeña	Total
Banca Comercial o Múltiple	6.325	1.492	759	**2.060**	2.750	680	725	**1.075**
Banca de Desarrollo		4.843	4.613	**4.740**		2.980	1.845	**2.476**
Sector Bursátil			167	**167**			162	**162**
Sector de Ahorro y Crédito Popular (SOCAP)		39	38	**38**		35	26	**28**
Sector de Ahorro y Crédito Popular (SOFIPO)		84	7	**43**		0	1	**1**
Sector de Intermediarios Financieros No Bancarios			249	**245**			233	**229**
Sector FINTECH			1.544	**1.544**			1.530	**1.530**
SISTEMA FINANCIERO MEXICANO	**5.422**	**854**	**411**	**655**	**2.357**	**635**	**318**	**447**

Fuente: SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

4 RECOMENDACIONES DE CIBERSEGURIDAD PARA EL SISTEMA FINANCIERO MEXICANO

Con base en los hallazgos encontrados, se establecieron un conjunto de recomendaciones de ciberseguridad para el Sistema Financiero Mexicano. Para el efecto se establecen dos (2) grupos objetivo como destinatarios de las recomendaciones: i) las entidades e instituciones financieras de México, y ii) las autoridades y órganos reguladores del sistema financiero y las autoridades de procuración de justicia del Gobierno de México.

4.1. Para las entidades e instituciones financieras del Sistema Financiero Mexicano

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 e instituciones financieras en el país y sus diferentes niveles de desarrollo y madurez en los aspectos de seguridad digital. Las recomendaciones se agrupan usando la misma estructura temática abordada por el instrumento de recolección de información usado.

4.1.1. En aspectos de preparación y gobernanza

- En lo posible, tener una única instancia responsable u órgano de gobierno corporativo para liderar la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude ocurridos a través de medios digitales, principalmente en los sectores bancario (Banca Comercial o Múltiple y Banca de Desarrollo) y de Ahorro y Crédito Popular (SOCAP y SOFIPO).

- Aunque a medida que el tamaño de la entidad bancaria aumenta se pretenda especializar en varias áreas de la organización la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude ocurridos a través de medios digitales, se debe garantizar que las mismas funcionen de manera coordinada y efectiva.

- Dimensionar adecuadamente los equipos de trabajo dedicados a los aspectos de seguridad de la información, efectuar evaluaciones de seguridad de los colaboradores, segregar adecuadamente roles y funciones, garantizar

procesos de gestión del conocimiento 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 de la información (incluyendo ciberseguridad) por parte de las instancias de decisión en las organizaciones (Dirección General o Gerencia General o Presidencia) y hacer procesos de sensibilización de manera periódica con la activa participación de sus miembros, a efecto de elevar la prioridad y apoyo a estas temáticas, principalmente en entidades medianas y pequeñas de los sectores de Ahorro y Crédito Popular (SOCAP y SOFIPO), de Intermediarios Financieros No Bancarios y FINTECH.

- Efectuar una revisión habitual de mejores prácticas en marcos de gobierno, seguridad y/o estándares internacionales, así como del marco regulatorio local e internacional aplicable a los diversos sectores y entidades e instituciones financieras, haciendo un proceso de mapeo y priorización para su aplicación.

- 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.

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

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

- Se debe contar con mecanismos de contrastación de las capacidades propias de detección y análisis de eventos de seguridad, preferiblemente mediante colaboración con equipos de respuesta a incidentes públicos o privados principalmente en las entidades e instituciones financieras de los sectores de Ahorro y Crédito Popular (SOCAP y SOFIPO) y de Intermediarios Financieros No Bancarios. 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, especialmente en las entidades e instituciones financieras de los sectores de Ahorro y Crédito Popular (SOCAP y SOFIPO) y de Intermediarios Financieros No Bancarios.

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

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

• Garantizar el diseño e implementación de una estrategia de priorización, contención, respuesta y recuperación frente a eventos (ataques exitosos y ataques no exitosos) de seguridad de la información (incluyendo ciberseguridad) contra las entidades e instituciones financieras, en especial de los sectores de Ahorro y Crédito Popular (SOCAP y SOFIPO) y de Intermediarios Financieros No Bancarios, 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).

• Investigar la fuente que genera incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad), principalmente en las entidades e instituciones financieras del sector de Ahorro y Crédito Popular (SOCAP y SOFIPO).

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

• Participar activamente de alianzas en las que se logre compartir las conclusiones y lecciones aprendidas sobre la gestión de eventos (ataques exitosos y ataques no exitosos), que faciliten la identificación y prevención de delitos, así como el desarrollo de soluciones holísticas para gestionar el riesgo cibernético.

• Capacitar y especializar al personal destinando presupuestos adecuados para realizar procesos de evaluación de la madurez bajo una metodología de seguridad de la información (incluyendo ciberseguridad) de manera periódica por parte de agentes externos idóneos, que permitan establecer las oportunidades de mejora, la priorización y la actualización de los planes y estrategias relacionados, especialmente en entidades e instituciones financieras medianas y pequeñas de los sectores Bursátil, de Ahorro y Crédito Popular (SOCAP y SOFIPO) y de Intermediarios Financieros No Bancarios.

• 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 su ciclo de vida, incluyendo como mínimo: i) Evaluaciones periódicas de vulnerabilidad para aplicaciones e infraestructura, ii) Remediación oportuna de los problemas encontrados en esas evaluaciones, iii) Adopción de metodologías de desarrollo seguras para minimizar el riesgo de que se introduzcan nuevas vulnerabilidades en la producción de soluciones para el negocio, iv) Adoptar controles para restringir el uso de soluciones sin soporte de fabricante (por condiciones de ciclo de vida de producto) y / o software ilegal, y v) Adoptar procesos para realizar la instalación de actualizaciones de seguridad de forma sistemática, entre otros.

• Garantizar la adecuada comunicación hacia los clientes de los mecanismos de reporte de que disponga la entidad / institución financiera en el caso de que resulten víctimas de incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad).

4.1.4. En aspectos de capacitación y concientización

• Infundir conceptos y buenas prácticas de ciberseguridad, especialmente con enfoque en aquellas áreas más relacionadas con procesos de innovación y transformación digital, en especial entidades e instituciones financieras medianas y pequeñas de los sectores Bursátil, de Ahorro y Crédito Popular (SOCAP y SOFIPO) y de Intermediarios Financieros No Bancarios.

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

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

• 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) Software espía (Malware o troyanos), iii) Ingeniería social y iv) Robo de credenciales de clientes (socios, asociados o usuarios) de servicios financieros.

• Aumentar el porcentaje de inversión destinado en la entidad bancaria para la generación de capacidades (ej.: formación, concientización, investigación) de la fuerza de trabajo, en especial en el desarrollo temprano de las mismas para cerrar la brecha en el personal ciber capacitado y para aumentar o mantener la fuerza laboral disponible en asuntos de seguridad digital con el fin de desarrollar y fortalecer una fuerza laboral ágil de resiliencia cibernética, la cual puede requerir una mayor capacidad educativa e incentivos.

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

- Invertir en seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales, principalmente en los sectores Bursátil, de Ahorro y Crédito Popular (SOCAP y SOFIPO) y de Intermediarios Financieros No Bancarios.

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

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

- Establecer de la manera más precisa posible la tasa de retorno de las inversiones efectuadas en relación con la seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales. 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.

4.2. Para las autoridades y órganos reguladores del sistema financiero y las autoridades de procuración de justicia del Gobierno de México

- Efectuar la revisión del catálogo de infraestructuras críticas y ver los niveles de dependencia que tienen las entidades / instituciones financieras del Sistema Financiero Mexicano, de forma que se valore su estado actual, la priorización de la gestión de sus riesgos asociados y en particular el impacto y la afectación que ataques a otras infraestructuras (por ejemplo, telecomunicaciones o energía) podrían tener sobre el mencionado sistema financiero.

- Coordinar esfuerzos con gremios o asociaciones relacionadas con el Sistema Financiero Mexicano 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 de entidades / instituciones del Sistema Financiero Mexicano, 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 en el Sistema Financiero Mexicano.

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

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

- 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 Sistema Financiero Mexicano, y de ser necesario emitir los instrumentos legales necesarios para su aplicación.

- Al momento de crear o actualizar regulación relacionada con ciberseguridad, adoptar reglamentaciones acordes a marcos ya establecidos por los emisores de estándares internacionales, reduciendo la fragmentación regulatoria, aprovechando las lecciones aprendidas y brindando estabilidad a través de todo el Sistema Financiero Mexicano.

- Establecer una estrategia de aseguramiento de la cadena que conforma la estabilidad del Sistema Financiero Mexicano, en especial, el Sistema de Pagos Electrónicos Interbancarios (SPEI) y desarrollar un marco legal para facilitar la persecución transnacional de los cibercriminales.

- 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.

- Realizar evaluaciones periódicas a las recientes disposiciones que ha venido estableciendo la Comisión Nacional Bancaria y de Valores (CNBV), en particular, el cumplimiento de la formulación de planes directores de seguridad y la materialización de la figura del oficial de seguridad que reporte directamente al director general de la entidad / institución financiera, a efecto de medir su grado de implementación y efectividad de las medidas.

- Establecer mecanismos de divulgación y socialización de resultados de los avances del Grupo de Respuesta a Incidentes (GRI) entre autoridades del Sistema Financiero Mexicano: Banco de México, SHCP, CNBV, CONSAR, CONDUSEF, CNSF y PGR; y disponer de ejercicios que pongan en práctica el protocolo de reacción del GRI, analizar su desempeño y orientar acciones para su mejora permanente.

- Evaluar la efectividad de la obligación para las entidades / instituciones financieras de reportar de los incidentes de seguridad digital que sufran, conforme a lo dispuesto por el Consejo de Estabilidad del Sistema Financiero -CESF-. 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 / instituciones financieras actores.

- Verificar en las entidades / instituciones financieras 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 éstos.

- Implementar mecanismos de intercambio de información entre el sector público y privado que facilite la detección temprana de patrones para permitir a las organizaciones protegerse mejor contra los ciberataques. Una legislación sólida para el intercambio de información facilita que los

sectores público y privado compartan información sobre amenazas cibernéticas de manera oportuna; permite que el gobierno desclasifique cierta información de amenazas para que pueda ser utilizada por el sector privado para su protección; y proporciona protección fuerte frente a las responsabilidades de las organizaciones que comparten información apropiada de amenazas cibernéticas.

- Establecer un tablero de mando unificado que permita cuantificar y facilitar la valoración de los avances de materialización de los "Principios para reforzar la seguridad de la información en el sistema financiero", emitidos por el CESF.

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

5 BIBLIOGRAFÍA

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: https://www.felaban.net/archivos_publicaciones/archivo20150702202150PM.pdf

OEA. (2018). Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. Obtenido de www.oas.org: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

SECRETARÍA DE COMUNICACIONES Y TRANSPORTE DE MÉXICO Y OEA. (2019). Estudio sobre hábitos de los usuarios en Ciberseguridad en México. Obtenido de: https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf

WEF. (2019). Informe Global de Riesgos del Foro Económico Mundial 2019. Obtenido de www.weforum.org: https://www.weforum.org/reports/the-global-risks-report-2019

ANEXO 1

Información de la muestra de entidades e instituciones del Sistema Financiero Mexicano

Cuadro 19. Información del Sistema Financiero Mexicano teniendo en cuenta reportes de la Comisión Nacional Bancaria y de Valores de México

	Grande	Mediana	Pequeña	Total	
Banca Comercial o Múltiple	6	13	14	**33**	
Banca de Desarrollo		5	4	**9**	
Sector Bursátil			9	**9**	
Sector de Ahorro y Crédito Popular (SOCAP)		27	71	**98**	
Sector de Ahorro y Crédito Popular (SOFIPO)	1	7	7	**15**	
Sector de Intermediarios Financieros No Bancarios		1	58	**59**	
Sector FINTECH			17	**17**	
SISTEMA FINANCIERO MEXICANO	**7**	**53**	**180**	**240**	**entidades**

	ACTIVOS			
	Grande (millones de dólares)	Mediano (millones de dólares)	Pequeño (millones de dólares)	Total (millones de dólares)
Banca Comercial o Múltiple	USD 150.503	USD 217.664	USD 61.201	**USD 429.368**
Banca de Desarrollo	**USD 0**	USD 68.538	USD 27.876	**USD 96.414**
Sector Bursátil	USD 0	USD 0	USD 17.998	**USD 17.998**
Sector de Ahorro y Crédito Popular (SOCAP)	USD 0	USD 2.780	USD 2.558	**USD 5.338**
Sector de Ahorro y Crédito Popular (SOFIPO)	USD 3	USD 213	USD 14	**USD 230**
Sector de Intermediarios Financieros No Bancarios	USD 0	USD 18	USD 2.903	**USD 2.921**
Sector FINTECH	USD 0	USD 0	USD 130.130	**USD 130.130**
SISTEMA FINANCIERO MEXICANO	**USD 150.506**	**USD 289.213**	**USD 242.679**	**USD 682.398**

millones

	Info CNBV				
	Fecha de reporte CNBV	Tipo de Cambio	Entidades	Activos (millones de pesos mex)	Activos (millones de dólares)
Banca Comercial o Múltiple	dic-18	$19,6566	50	**$9.475.000**	**USD 482.026**
Banca de Desarrollo	**sep-18**	$18,7231	6	**$1.973.600**	**USD 105.410**
Sector Bursátil	sep-18	$18,7231	35	**$627.800**	**USD 33.531**
Sector de Ahorro y Crédito Popular (SOCAP)	sep-18	$18,7231	157	**$149.539**	**USD 7.987**
Sector de Ahorro y Crédito Popular (SOFIPO)	sep-18	$18,7231	46	**$32.459**	**USD 1.734**
Sector de Intermediarios Financieros No Bancarios	sep-18	$18,7231	84	**$63.254**	**USD 3.378**
Sector FINTECH					
SISTEMA FINANCIERO MEXICANO			**378**		**87%**

del total de activos

	% entidades muestra del total en México	% activos muestra del total en México
Banca Comercial o Múltiple	66%	89%
Banca de Desarrollo	150%	91%
Sector Bursátil	26%	54%
Sector de Ahorro y Crédito Popular (SOCAP)	62%	67%
Sector de Ahorro y Crédito Popular (SOFIPO)	33%	13%
Sector de Intermediarios Financieros No Bancarios	70%	86%
Sector FINTECH		
SISTEMA FINANCIERO MEXICANO	63%	del total de entidades

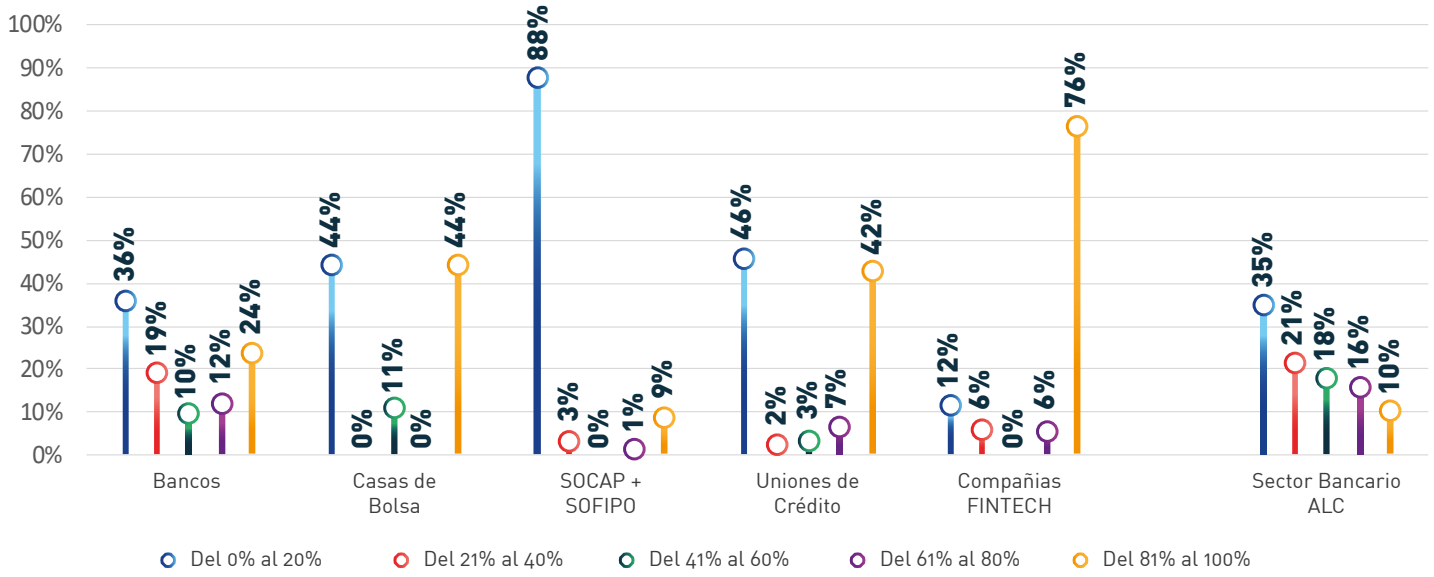
	EBITDA			
	Grande (millones de dólares)	Mediano (millones de dólares)	Pequeño (millones de dólares)	Total (millones de dólares)
Banca Comercial o Múltiple	USD 1.650	USD 636	USD 564	USD 2.850
Banca de Desarrollo	USD 0	USD 1.490	USD 738	USD 2.228
Sector Bursátil	USD 0	USD 0	USD 58	USD 58
Sector de Ahorro y Crédito Popular (SOCAP)	USD 0	USD 47	USD 165	USD 211
Sector de Ahorro y Crédito Popular (SOFIPO)	USD 0	USD 18	USD 1	USD 19
Sector de Intermediarios Financieros No Bancarios	USD 0	USD 0	USD 793	USD 794
Sector FINTECH	USD 0	USD 0	USD 991	USD 991
SISTEMA FINANCIERO MEXICANO	USD 1.650	USD 2.190	USD 3.310	USD 7.150 millones

Fuente: SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

ANEXO 2

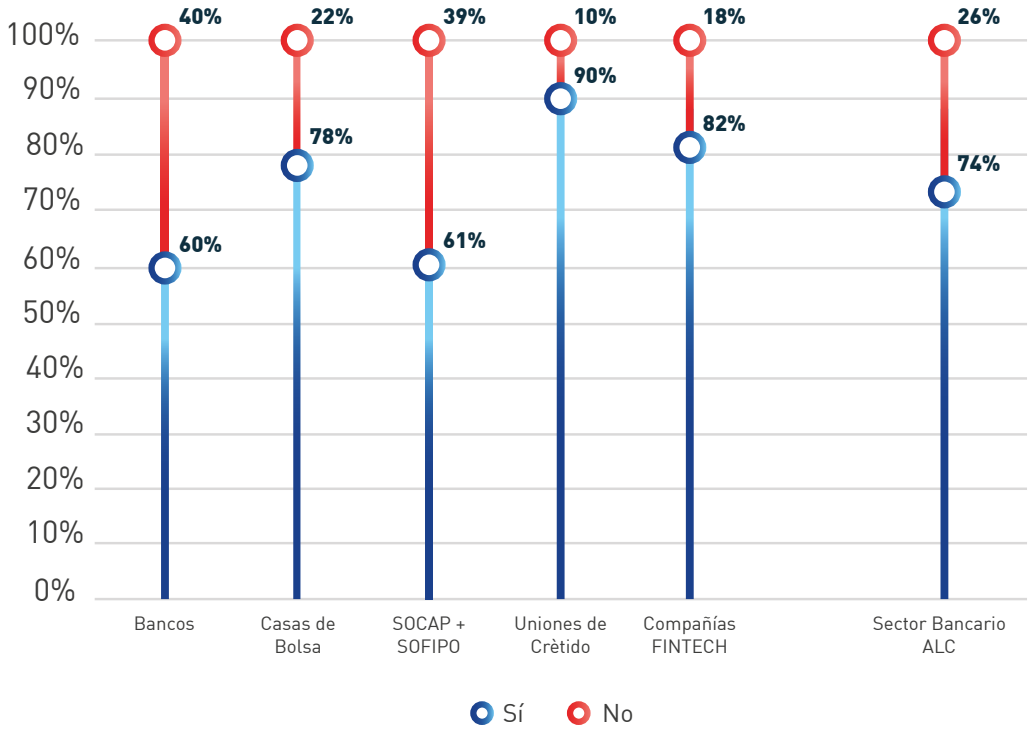
Análisis comparativo entre sectores del Sistema Financiero Mexicano

Gráfica 34. Porcentaje de operaciones que se realizaron por medio de canales transaccionales no presenciales – Comparación entre sectores



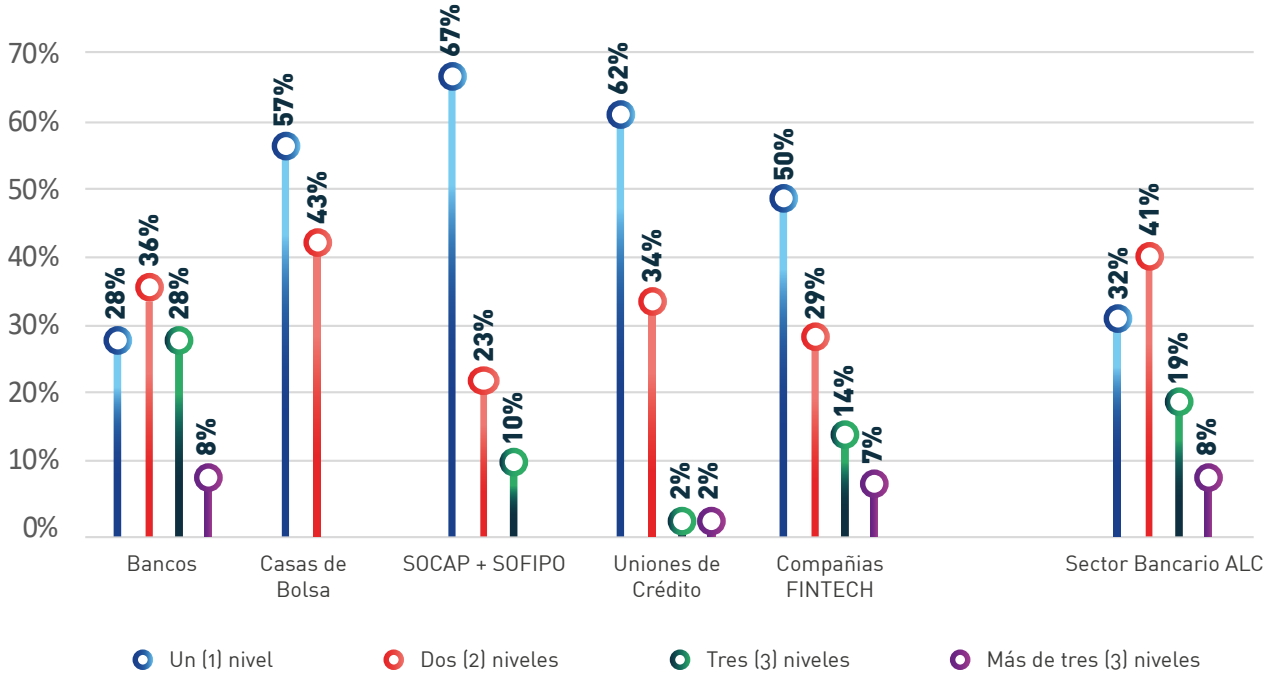
Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 35. Área única responsable de la seguridad digital en la entidad / institución financiera – Comparación entre sectores



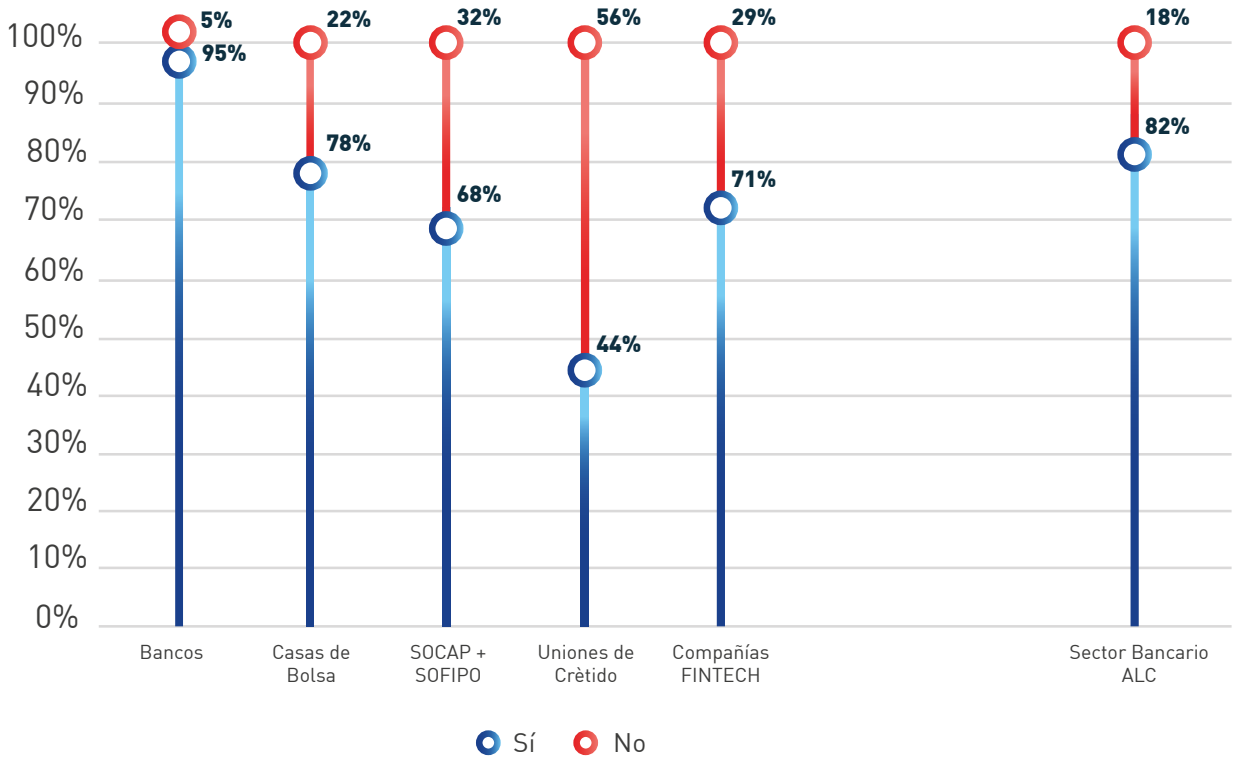
Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 36. Número de niveles jerárquicos que hay entre el CEO y el máximo responsable de la seguridad digital – Comparación entre sectores



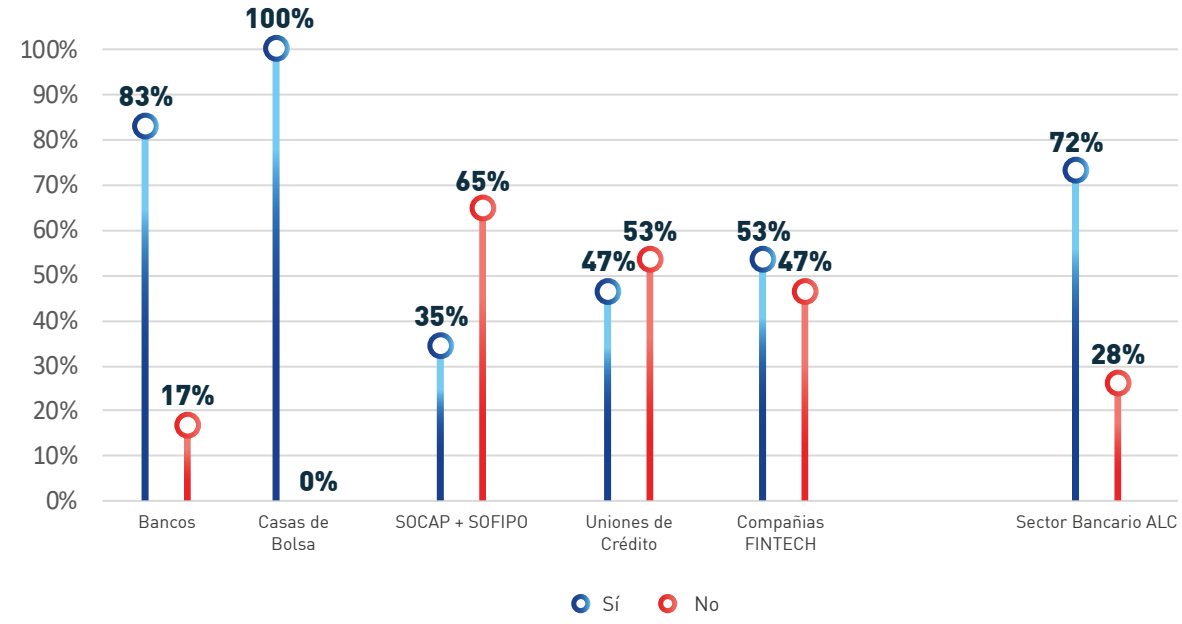
Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 37. ¿Se considera adecuado que este equipo creciera en el corto plazo? – Comparación entre sectores



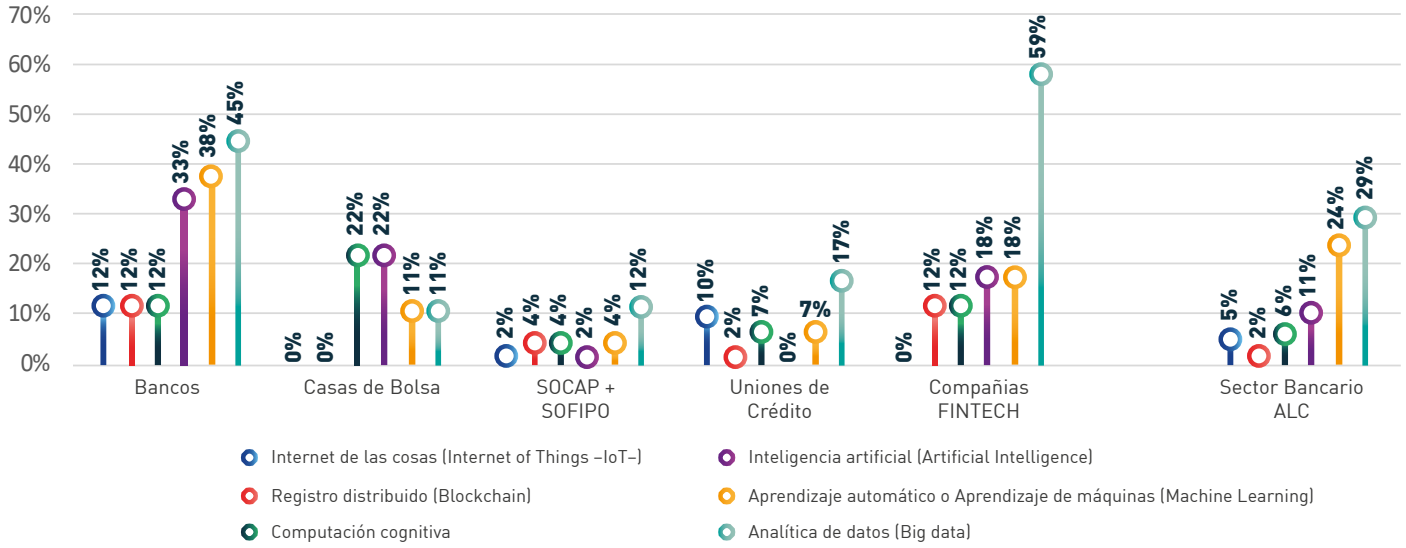
Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 38. ¿El Consejo de Administración o Consejo Directivo o Junta Directiva recibe reportes periódicos acerca de riesgos de seguridad de la información? – Comparación entre sectores



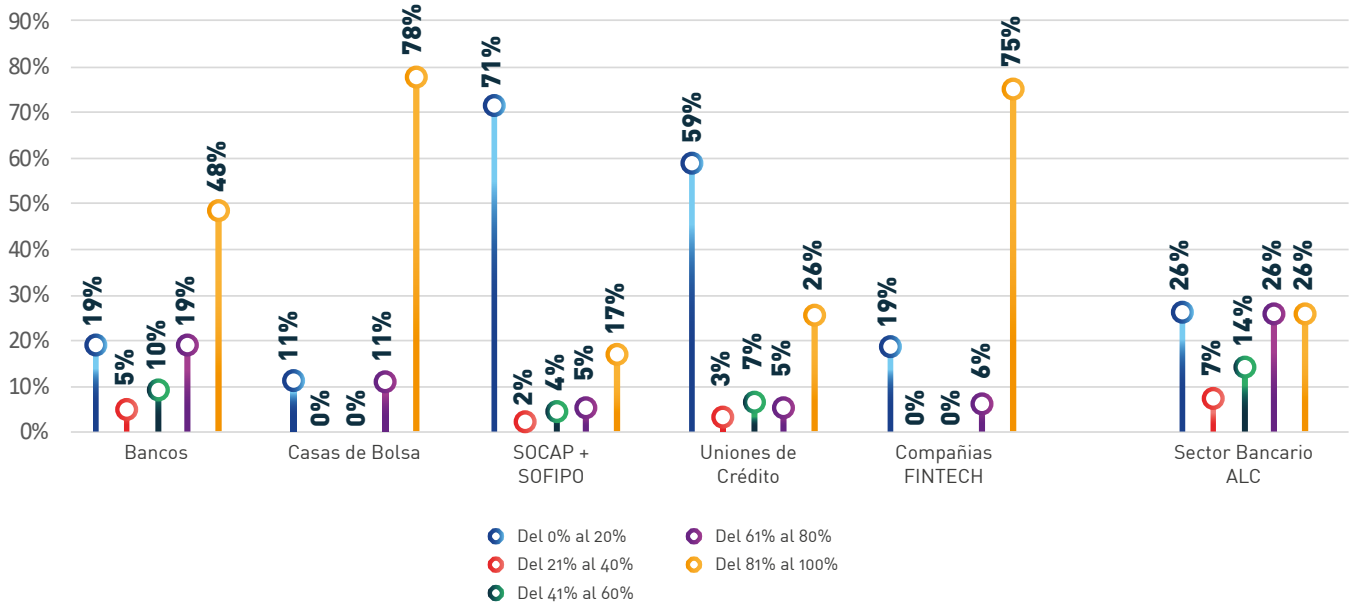
Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 39. Tecnologías digitales emergentes aplicadas a herramientas, controles o procesos de seguridad digital en la entidad / institución financiera – Comparación entre sectores



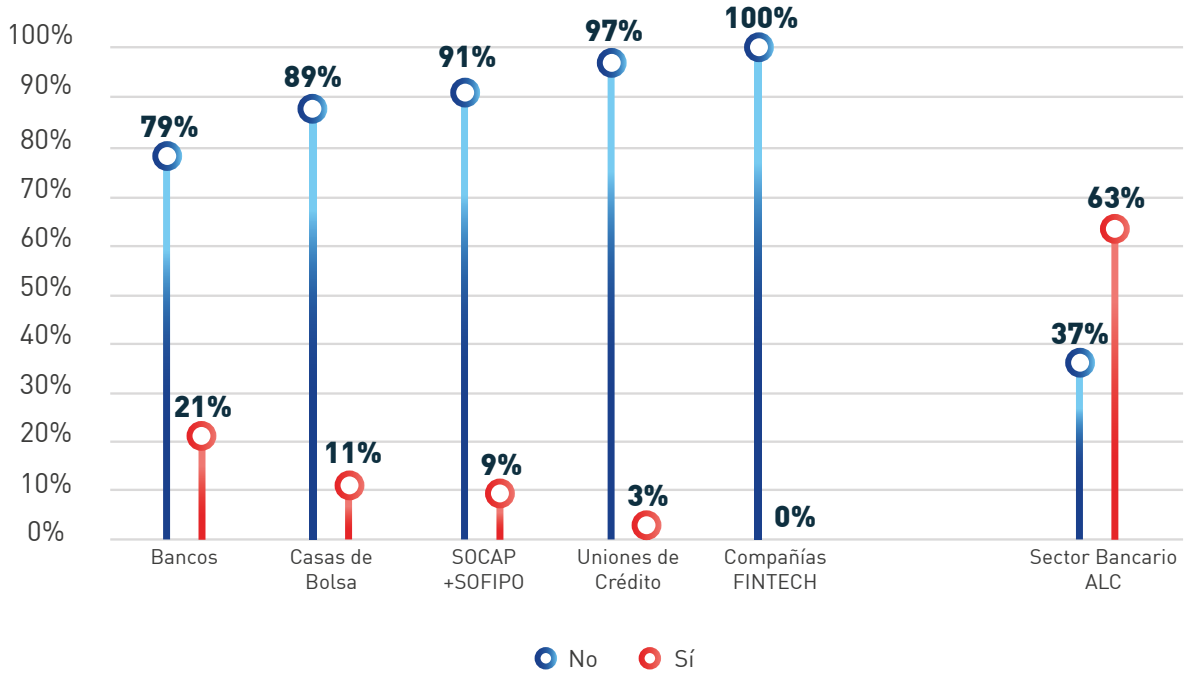
Nota: 240 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 40. Porcentaje de eventos de seguridad digital que son detectados mediante sistemas propios (y no de terceros) de detección de la entidad / institución financiera – Comparación entre sectores



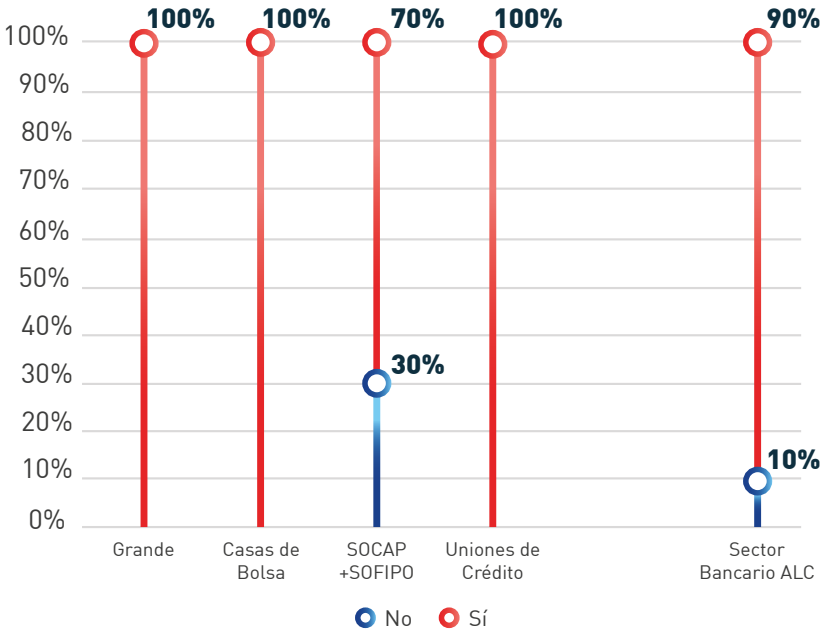
Nota: 237 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 41. ¿La entidad / institución financiera fue víctima de incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad) durante los últimos doce meses? – Comparación entre sectores



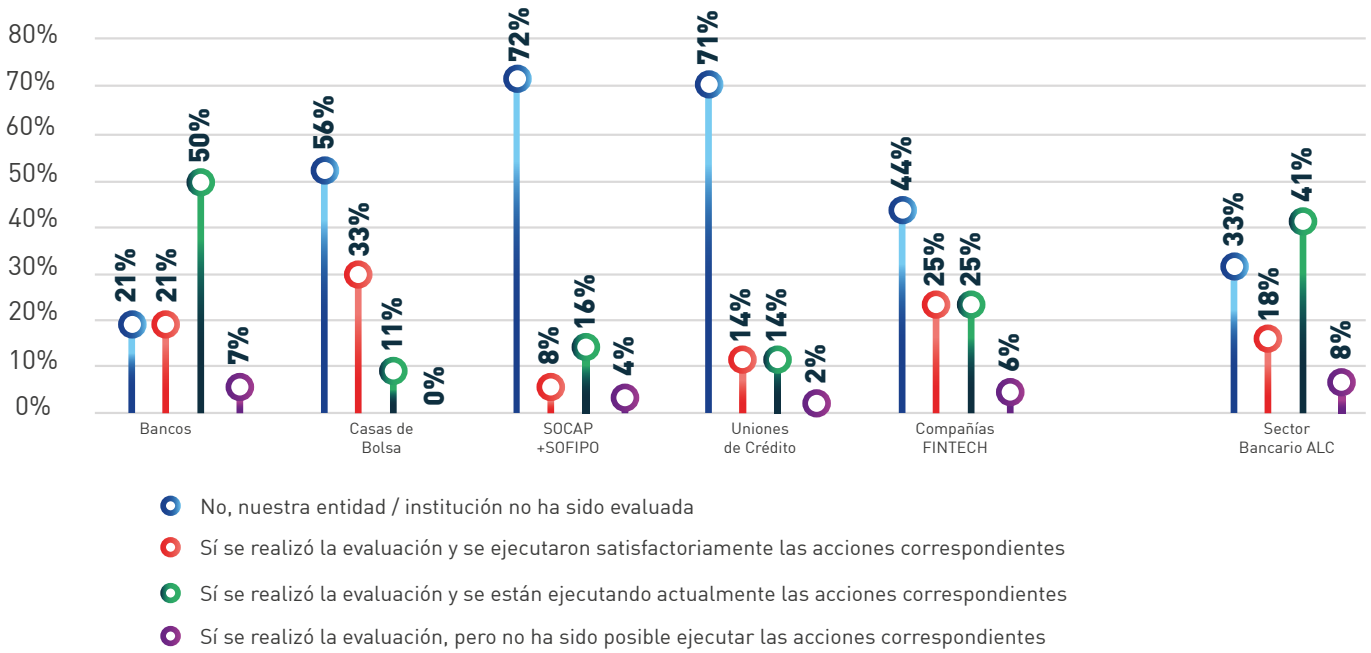
Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 42. ¿La entidad / institución financiera a la cual usted pertenece investigó la fuente que generó dichos incidentes (ataques exitosos) de seguridad de la información (incluyendo ciberseguridad)? – Comparación entre sectores



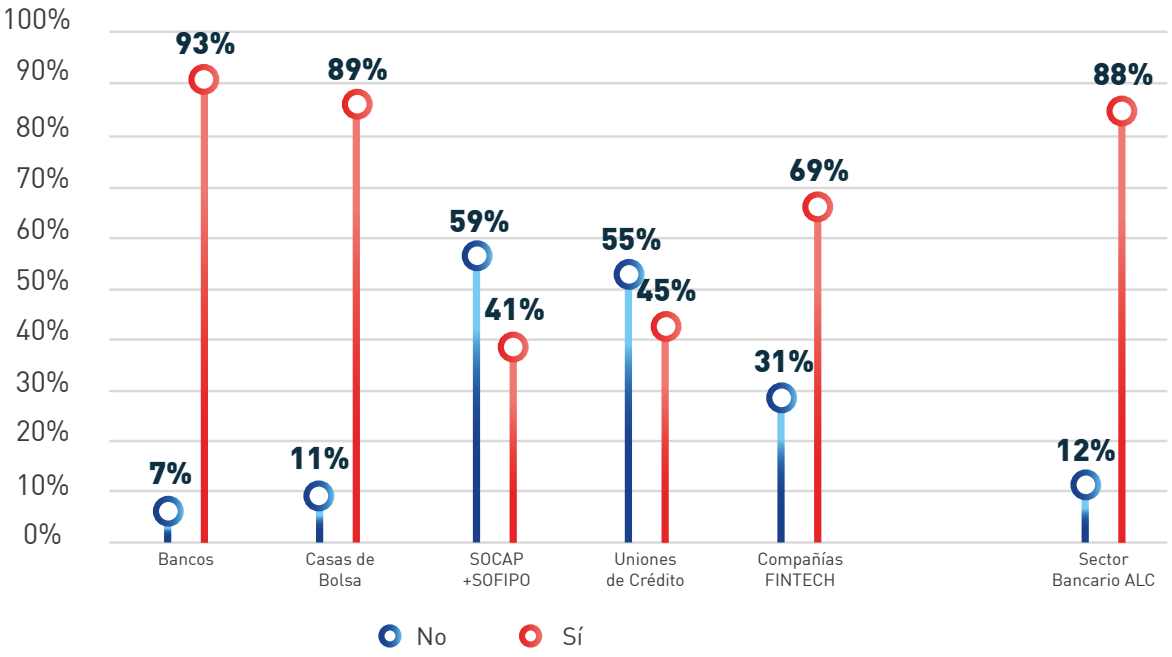
Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 43. ¿La entidad / institución financiera a la cual usted pertenece ha sido evaluada externamente en los últimos dos (2) años bajo alguna metodología de seguridad de la información (incluyendo ciberseguridad) para determinar su nivel de madurez? – Comparación entre sectores



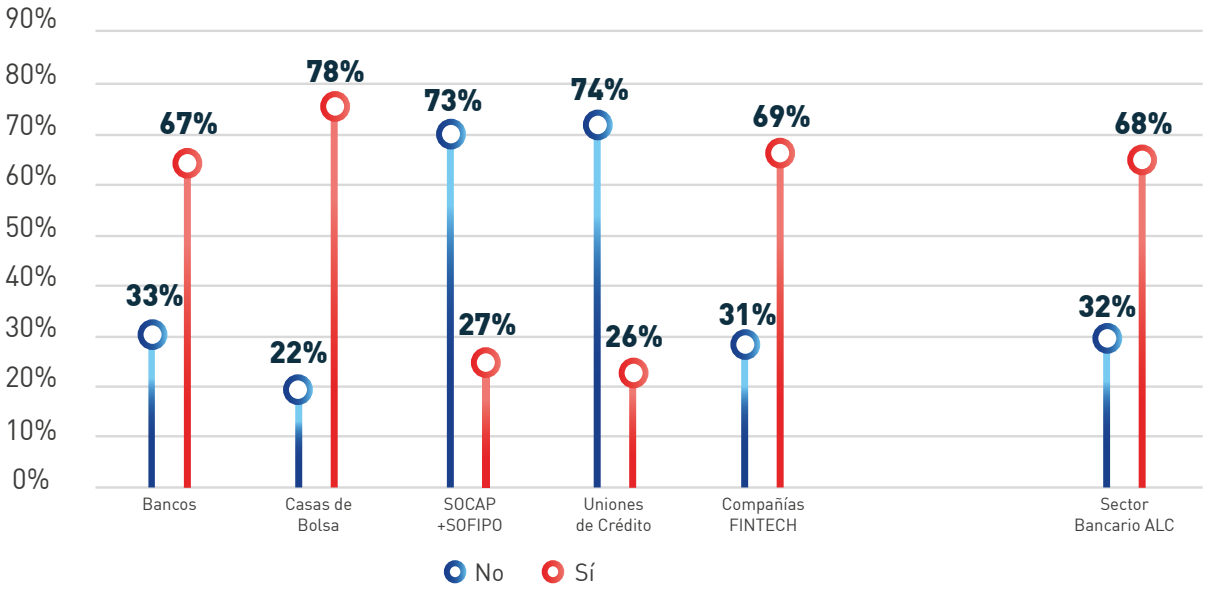
Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 44. ¿La entidad / institución financiera ofrece un mecanismo para que sus colaboradores (empleados y contratistas) reporten incidentes (ataques exitosos)? – Comparación entre sectores



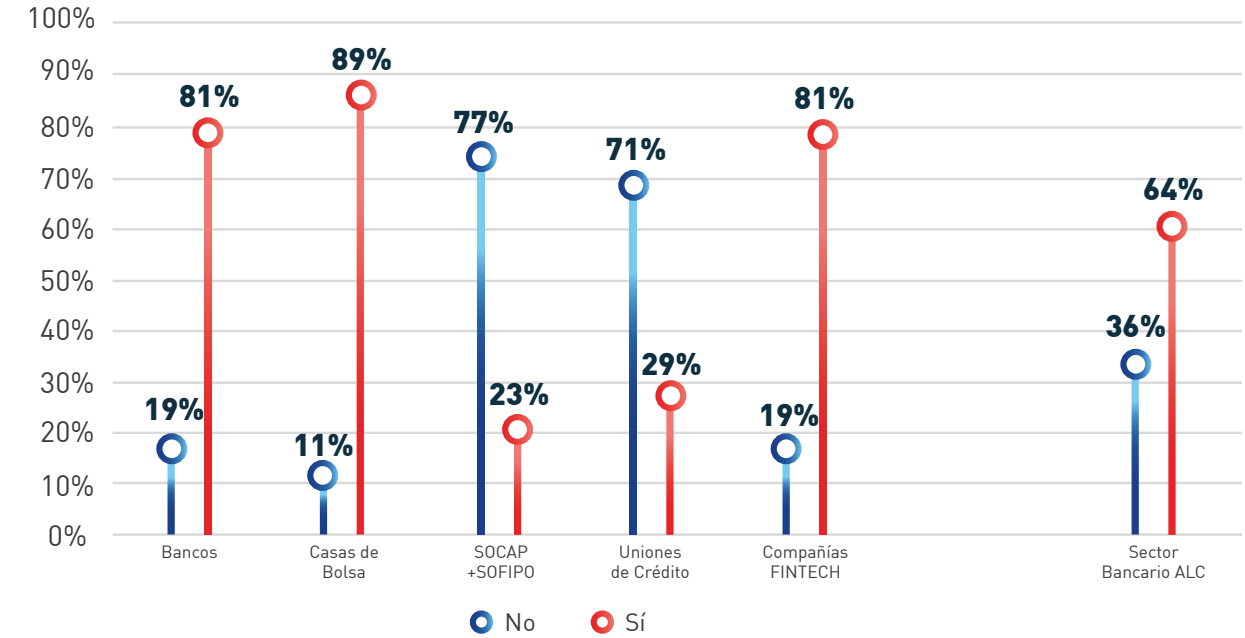
Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 45. ¿La entidad / institución financiera ofrece un mecanismo para que sus clientes (socios, asociados o usuarios) reporten incidentes (ataques exitosos)? – Comparación entre sectores



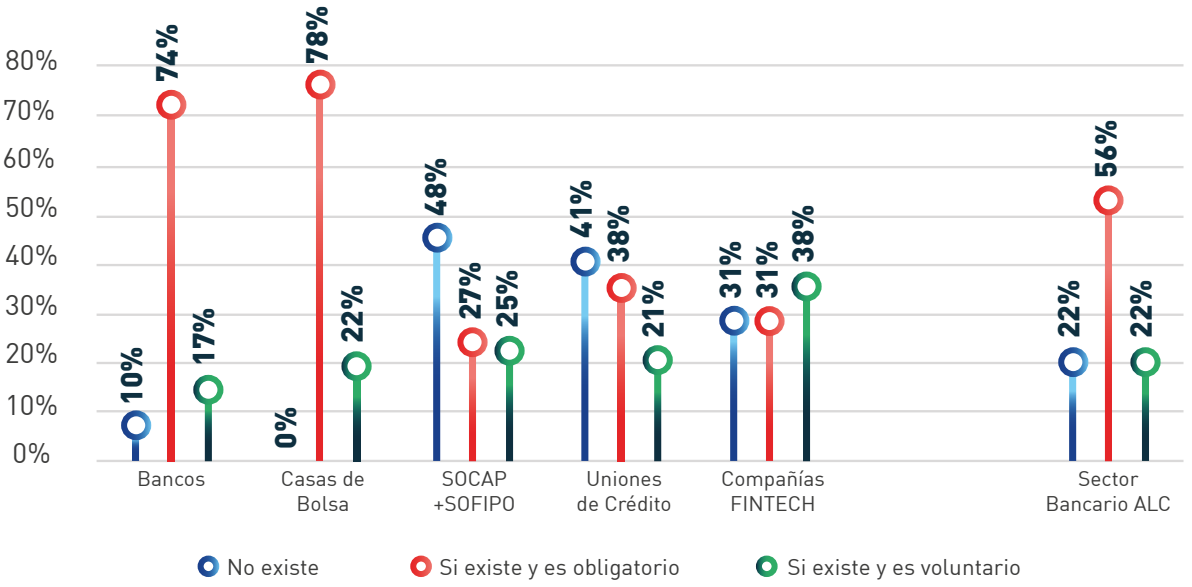
Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 46. ¿La entidad / institución financiera cuenta con un plan de comunicaciones que permita informar a sus clientes (socios, asociados o usuarios) de servicios financieros cuando su información personal se haya visto comprometida? – Comparación entre sectores



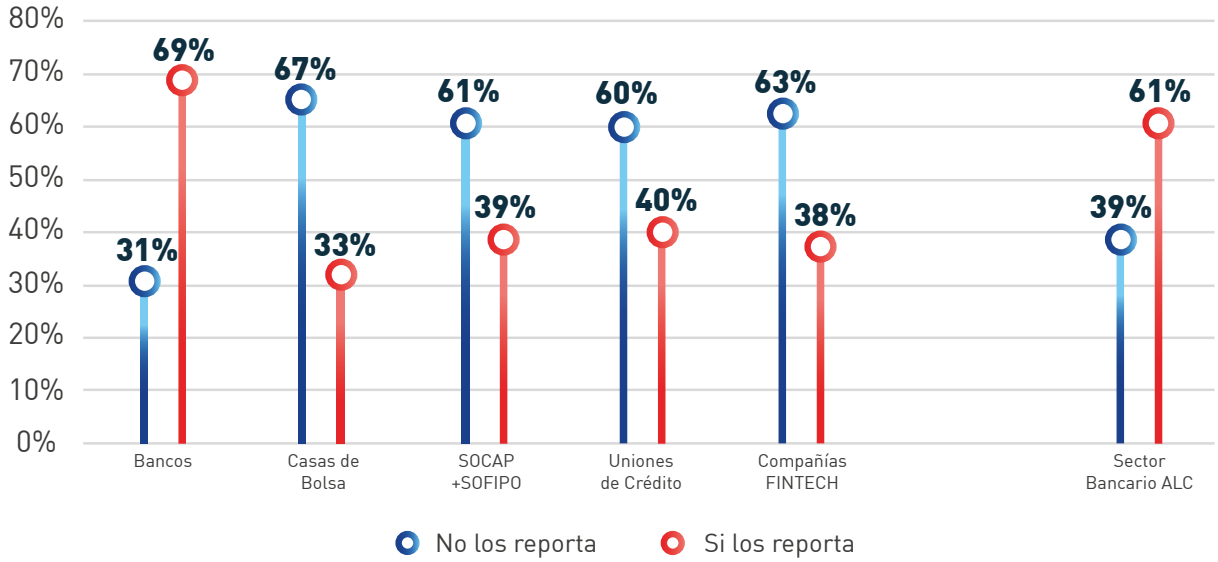
Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 47. ¿Conoce algún mecanismo para reportar incidentes (ataques exitosos) sufridos por la entidad / institución financiera a la cual usted pertenece ante una autoridad de regulación en México? – Comparación entre sectores



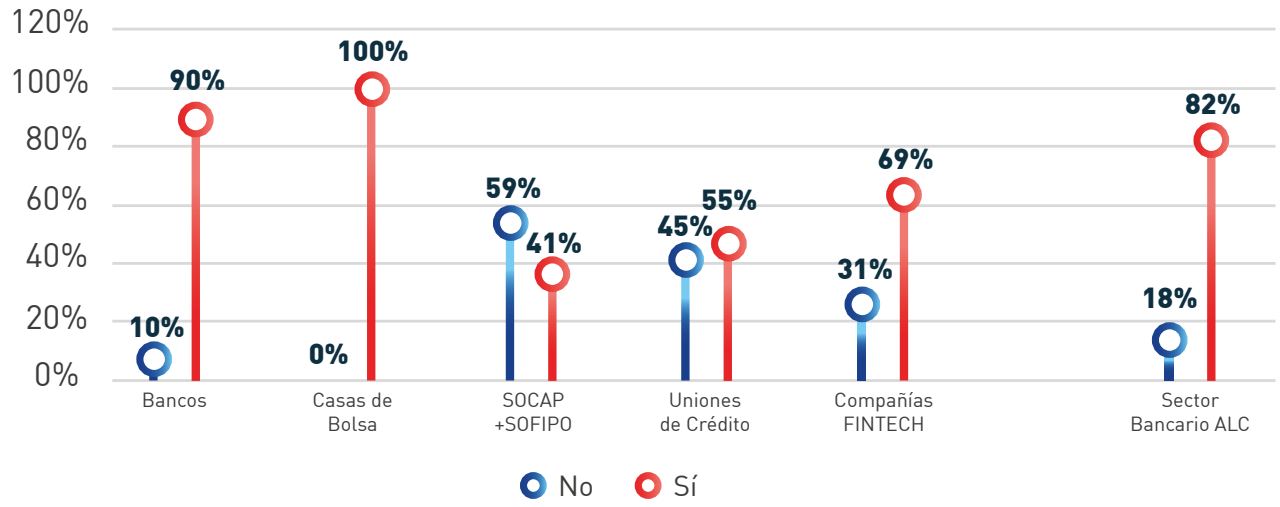
Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 48. ¿La entidad / institución financiera reporta los incidentes (ataques exitosos) sufridos ante una autoridad de procuración de justicia en México? – Comparación entre sectores



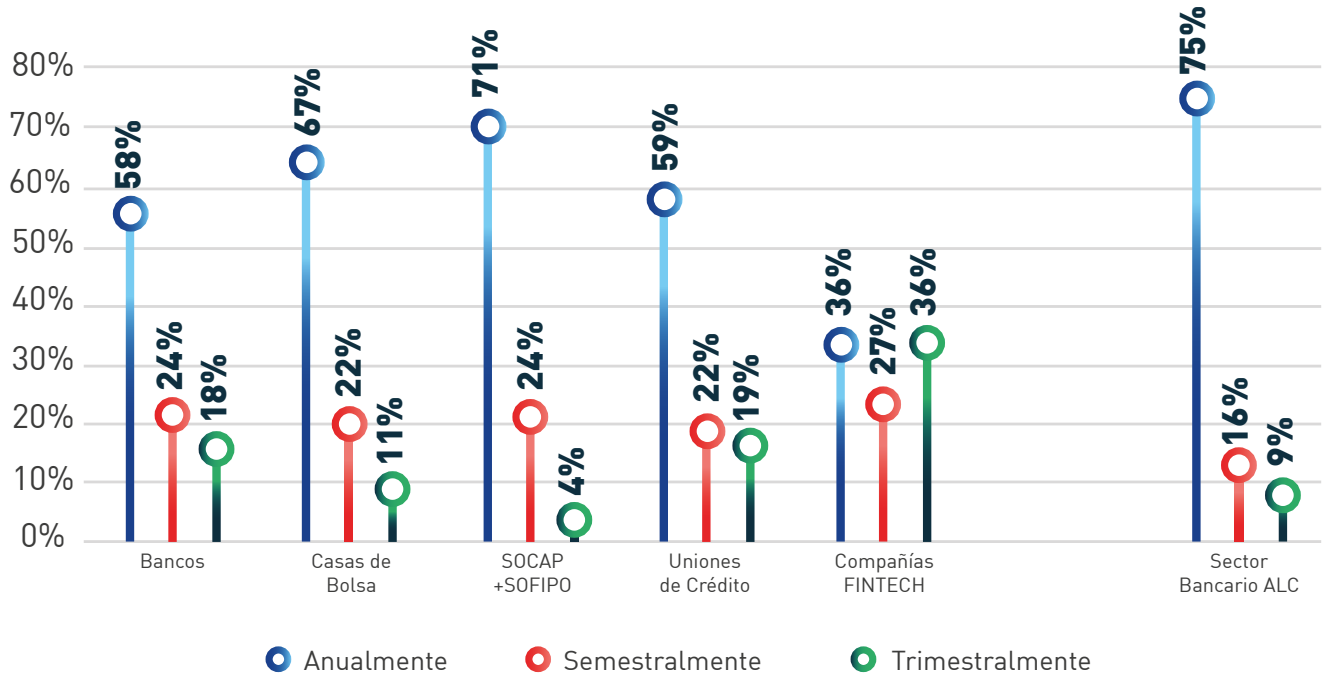
Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 49. ¿Cuenta la entidad / institución financiera con planes de concientización y formación en asuntos de seguridad de la información para sus colaboradores? – Comparación entre sectores



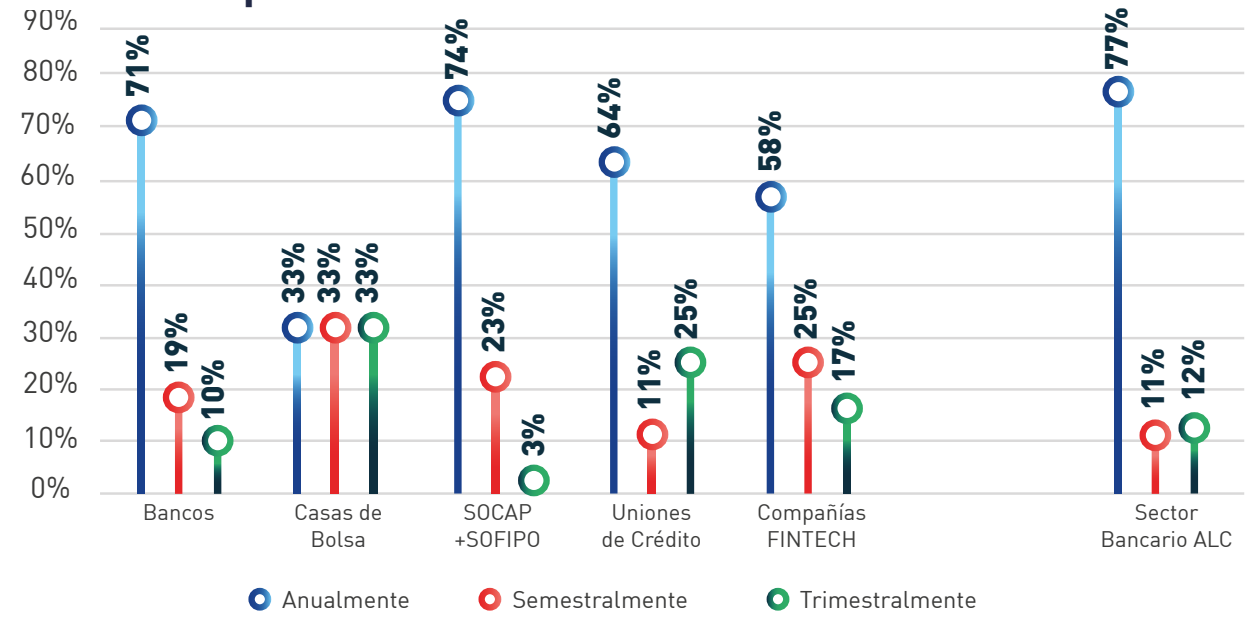
Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 50. ¿Con qué frecuencia se ejecutan dichos planes de concientización y formación? – Comparación entre sectores



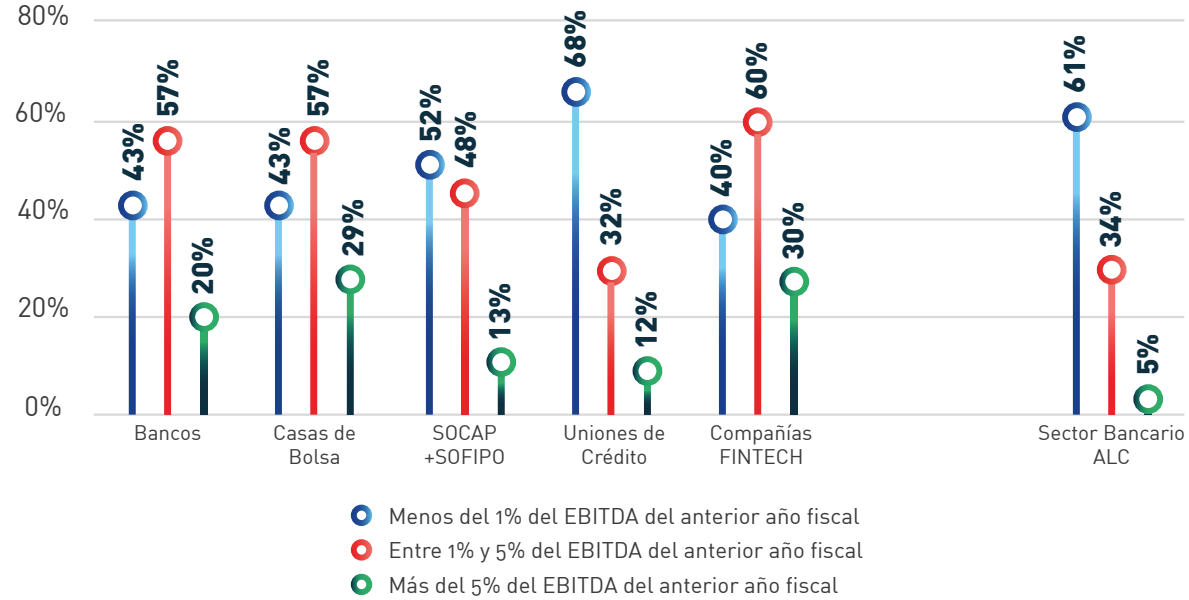
Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 51. ¿Con qué frecuencia se prueba la capacidad de los empleados de la institución financiera de responder adecuadamente frente a incidentes (ataques exitosos) y esquemas de phishing e ingeniería social? – Comparación entre sectores



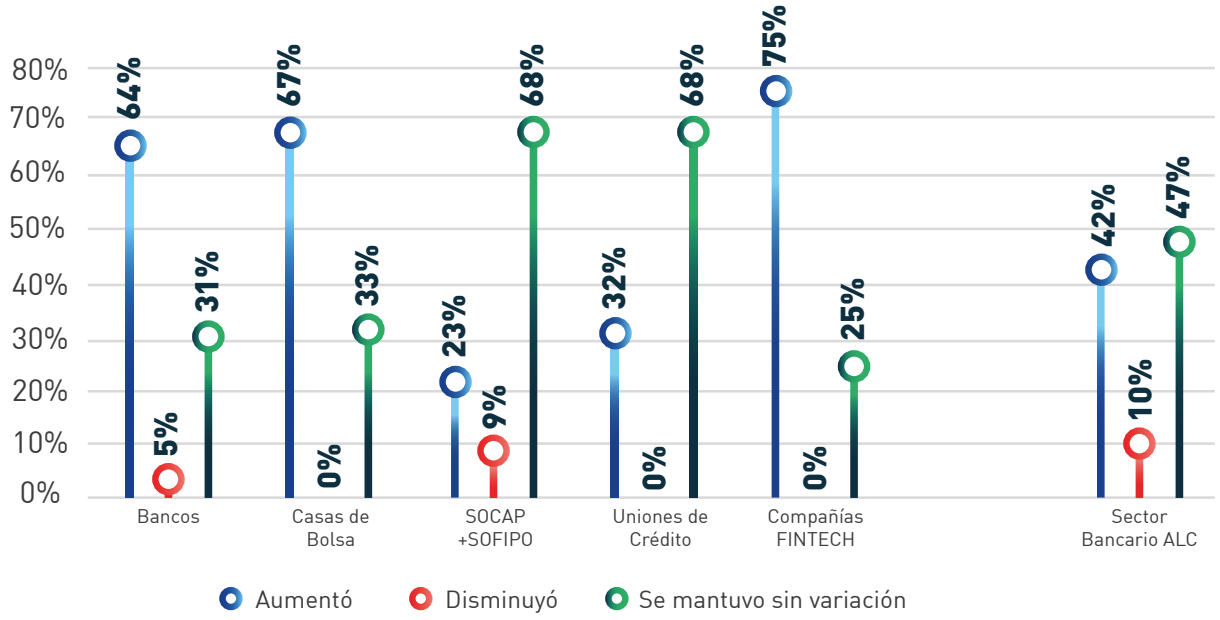
Nota: 236 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 52. Dinámica del presupuesto de seguridad digital en el último año – Comparación entre sectores



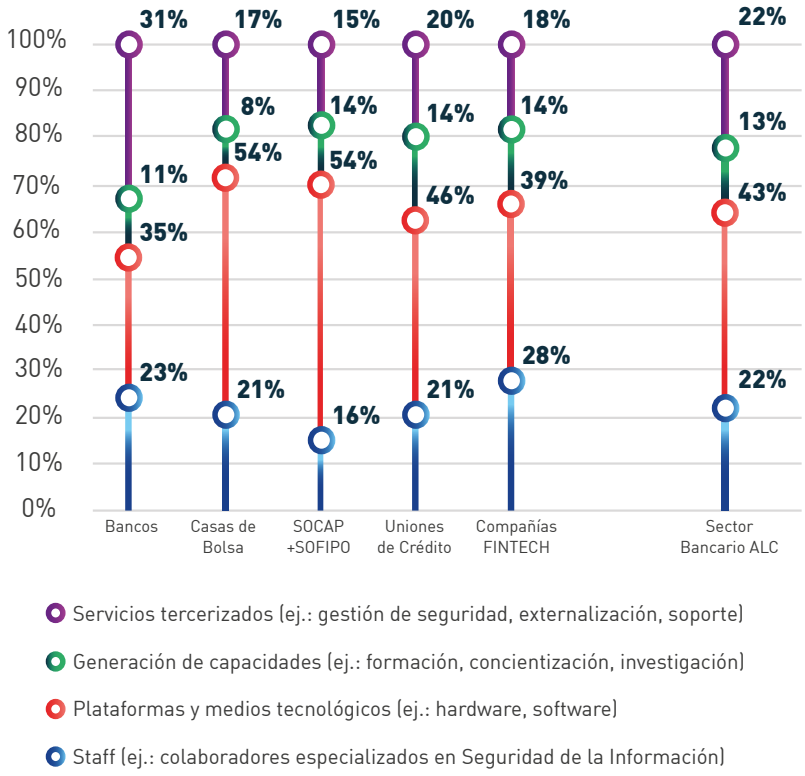
Nota: 235 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 53. Crecimiento del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales de la entidad / institución financiera – Comparación entre sectores



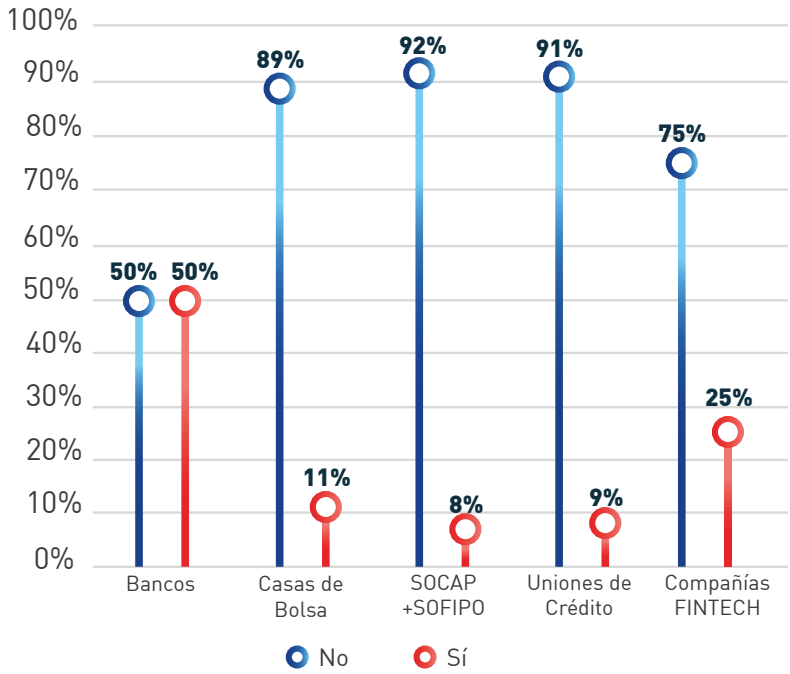
Nota: 235 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 54. Distribución del presupuesto de seguridad de la información (incluyendo ciberseguridad) y prevención del fraude a través de medios digitales de la entidad / institución financiera – Comparación entre sectores



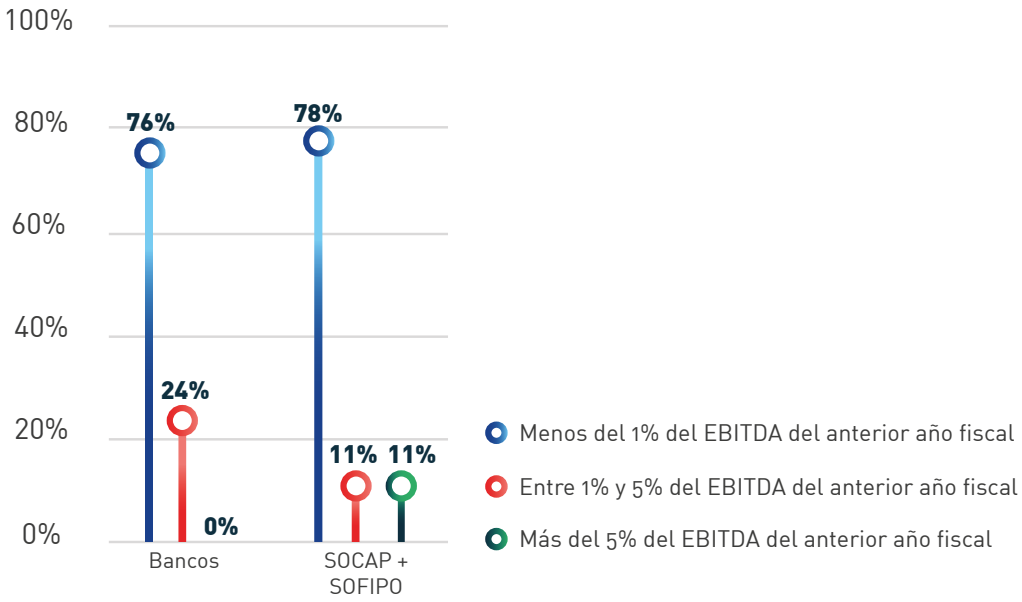
Nota: 196 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 55. ¿La entidad / institución financiera a la cual usted pertenece estimó el costo total de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) para el último año fiscal? – Comparación entre sectores



Nota: 233 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

Gráfica 56. Costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad de la información (incluyendo ciberseguridad) para la entidad / institución a la cual usted pertenece (en México) para el último año fiscal – Comparación entre sectores



Nota: 40 registros **Fuente:** SG/OEA a partir de información recolectada de entidades e instituciones financieras en México

ESTADO DE LA **CIBERSEGURIDAD** EN EL SISTEMA FINANCIERO **MEXICANO**

ESTADO DE LA CIBERSEGURIDAD EN EL SISTEMA FINANCIERO MEXICANO

Con el apoyo
financiero de

Foreign &
Commonwealth
Office