Proyecto Robo de Datos y Fraude a través de Canales Digitales

Unidad de Inteligencia Financiera

Departamento de Análisis

Análisis Estratégico

Contenido

Agradecimiento

La Unidad de Inteligencia Financiera (UIF), agradece a los sectores de Bancos Comerciales, Bancos Estatales, Cooperativas de Ahorro y Crédito y la Instituciones no bancarias que brindan servicios por medio de pago utilizando dinero electrónico (INDEL), por el invaluable apoyo y disposición en recabar y proporcionar la información requerida mediante el instrumento que para tal efecto se proporcionó a las referidas Instituciones Financieras.

Superando con éxito los objetivos propuestos, alcanzando a diseñar un producto final acorde a la realidad de riesgos emergentes que se puedan presentar y ser aprovechadas por los criminales para ampliar su poder sobre la economía Nacional, los clientes-usuarios y la reputación del Sistema Financiero Nacional, por la crisis sanitaria del Covid-19.

El presente proyecto será coadyuvante en la labor de detección de posibles operaciones vinculadas con los delitos precedentes de ciberdelito y fraude, relacionado con el Lavado de Activos y Financiamiento del Terrorismo; permitiendo así crear controles que aseguren la aplicación de un enfoque basado en riesgos.

Resumen Ejecutivo

El presente proyecto se ha desarrollado a fin de identificar las diferentes modalidades en las que se operan para realizar robo de datos y fraude por medio de canales digitales previo y durante la crisis sanitaria provocada por la pandemia del Covid-19, así como el posible surgimiento de riesgos en materia de LA/FT, amenazas y/o vulnerabilidades en el lanzamiento de nuevos productos y servicios, o los migrados de estos de forma presencial a digital; de tal forma sirva como referencia a los Sujetos Obligados para ajustar sus sistemas de monitoreo, control y detección; fortalecer los procesos de elaboración de Reporte de Operaciones Sospechosas (ROS) y otros productos de inteligencia financiera.

El análisis del proyecto surge de las diferentes fuentes consultadas como marco teórico y la formulación de un cuestionario el cual fue agrupado en las siguientes secciones; canales utilizados, herramientas utilizadas, nuevos productos, análisis de riesgos, capacitación interna, sensibilización del usuario, zonas geográficas con mayor incidencia, montos, Reportes de Operaciones Sospechosas (ROS); dicho cuestionario recoge la opinión de diversos sectores financieros como ser; Bancos Comerciales, Bancos Estatales, Cooperativas de Ahorro y Crédito e INDEL.

Los resultados del análisis de datos producto del cuestionario, arrojan las fortalezas y las oportunidades de mejora a nivel de sector, como en su conjunto; se obtuvo que todos los sectores menos los Bancos Estatales crearon nuevos productos previo a la pandemia por Covid-19 y durante esta, donde únicamente los Bancos Comerciales y las Cooperativas de Ahorro y Crédito crearon nuevos productos o servicios; hasta en un 25% incrementaron las transacciones por medios digitales en Bancos y Cooperativas de Ahorro y Crédito y hasta un 50% en la INDEL; se observó que al menos el 60% de los sectores evalúan el riesgo previo al lanzamiento de nuevos productos; en relación al conocimiento sobre Ciberdelito y Fraude, se obtuvo que al menos tres de los cuatro sectores evaluados conocen sobre dichos temas en un 100%, sin embargo en el caso de las Cooperativas de Ahorro y Crédito, existe un porcentaje que no conoce de los referidos temas; en caso que se sospeche sobre un ciberataque al menos 50% de los sectores cuenta con un área al cual reportar.

Por otro lado, el uso frecuente de canales digitales ha provocado el aumento de delitos como por ejemplo: suplantación de identidad y robo de datos de forma virtual; dentro de los principales controles que se toman, es la restricción de los privilegios administrativos; la cantidad de reclamos que se obtienen al año, oscilan entra 1-25 y mayores a 100 en los Bancos Comerciales; las principales zonas donde se presenta la mayoría de las denuncias o quejas corresponden a la Zona Centro y Norte; al menos el 60% de los sectores financieros realizan campañas de sensibilización a los clientes y/o usuarios, siendo las Cooperativas de Ahorro y Crédito las que representan el 40% que no lo realizan, es decir que 60% de las referidas Cooperativas no llevan a cabo campañas de sensibilización sobre los temas de Ciberdelito o Fraude y finalmente de los cuatro Sectores evaluados únicamente la INDEL ha llevado a cabo ROS, el resto no ha realizado debido a que indican que la detección no reúne los requisitos para realizar Reportes de Operaciones Sospechosas (ROS).
En consecuencia, de lo antes expuesto, se obtiene que:

Resulta fundamental fortalecer el conocimiento de los clientes y empleados acerca de los métodos y prácticas que las estructuras criminales utilizan para llevar a cabo los delitos antes mencionados, en ese sentido, como hemos visto en los resultados del análisis.

Luego de los resultados del estudio se ha comprobado que los clientes de las instituciones financieras resultan ser víctimas de estas prácticas delincuenciales afectando el patrimonio económico de los mismos, donde en la mayoría de los casos se desconoce el actor de estos delitos, dificultando el poder realizar un Reporte de Operaciones Sospechosas (ROS), en este sentido, y aprovechando las campañas de sensibilización sobre este tipo de crímenes, en paralelo se debe promover una cultura de denuncia que permita obtener más datos o elementos que motiven el análisis exhaustivo por parte de las áreas de cumplimiento para la detección temprana de este tipo de métodos que afectan los activos financieros de los clientes.

Podemos deducir que el riesgo por Ciberdelitos puede categorizarse en una escala media, lo anterior puede generar impactos adversos en el crecimiento y madurez de los productos y servicios; en vista de que no solo se necesita crecer en el ámbito tecnológico sino también en la percepción de confiabilidad de los usuarios y adopción de nuevas tecnologías que impulsen la inclusión financiera, el ambiente FINTECH adoptando desde etapas tempranas un enfoque basado en riesgo y con un marco regulatoria que facilite la implementación de proyectos innovadores en el mercado financiero nacional además de definir una política clara de protección y uso de los datos personales de los usuarios y clientes.

Datos y principios fundamentales

Un dato es un documento, una información o un testimonio que permite llegar al conocimiento de algo o deducir las consecuencias legítimas de un hecho.

Los datos representan un fragmento de una cantidad, medida, descripción o palabra, los cuales son agrupados o clasificados de una determinada manera para generación de información.

Los datos personales son cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal.

[1]Los datos se clasifican de la siguiente forma

Existen estándares para la protección de los datos personales para los Estados Iberoamericanos, del cual Honduras forma parte, dichos estándares tienen como finalidad:

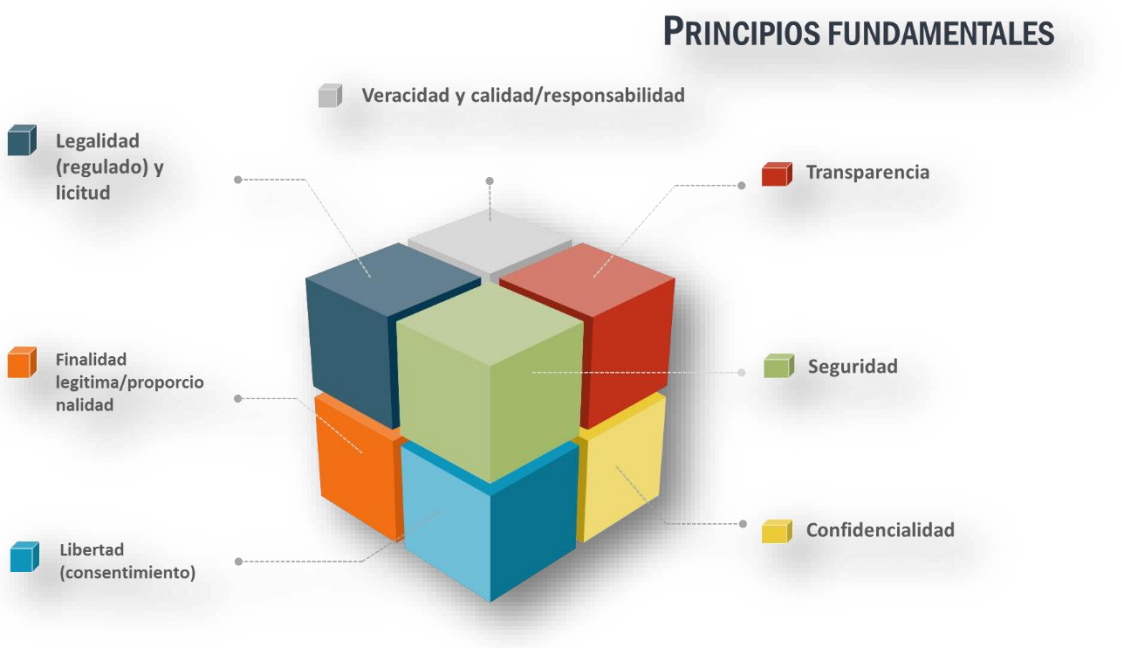
- Entender la protección de datos personales como un derecho fundamental.
- Reconocer la importancia de las iniciativas regulatorias Iberoamericana para proteger la privacidad de los ciudadanos.
- La necesidad del continuo flujo de datos entre países que tienen diversos lazos en común y una preocupación por este derecho.
- Establecer un conjunto de principios y derechos comunes (reglas homogéneas en la región.
- Favorecer la cooperación internacional entre las autoridades de control.

[1] Fuente: Seminario web Los Sistemas de Gestión de Riesgo para la protección de datos personales, impartida por Risk Consulting

[2]En el XVII encuentro Iberoamericano de protección de datos personales celebrado en México en el año 2019 en su declaración final se resalta lo siguiente:

En su declaración tercera, manifiestan un compromiso por sentar las bases de cooperación entre las Autoridades Iberoamericanas de protección de datos como un mecanismo fundamental, así como impulsar y coordinar iniciativas en los foros internacionales y establecer criterios de interés común sobre asuntos relevantes en esta materia para la región.

Los principios fundamentales desde donde pueden surgir normativas se clasifican de la siguiente forma:



Dentro de las obligaciones para garantizar el principio de responsabilidad se resumen

- Destinar recursos
- Sistemas de gestión de riesgos
- Políticas y programas para la protección de datos personales
- Capacitación y actualización del personal
- Monitoreo y seguimiento

[2] Fuente: Declaración final del XVII encuentro Iberoamericano de protección de datos personales

Características de la información

- Disponibilidad

Acceso y utilización de la información y los sistemas de tratamiento de la mima por parte de los individuos, entidades o procesos cuando lo requieren.

- Integridad

Capacidad o necesidad de mantener la exactitud y completitud de la información y sus métodos.

- Confiabilidad

La información no se pone ni se revela a individuos, entidades o procesos no autorizados.

Cabe señalar que muchas veces, aunque se trabaje en controles para evitar la materialización de los ciberataques, estos se pueden dar; por lo que lo importante en estos casos es como se van a tratar, es por ello por lo que se debe de trabajar en un plan de tratamiento frente a los ataques de cibernéticos con una política de incidentes en conjunto con un plan de sensibilización.

Ciberdelito

[3]Ciberdelito son todas las conductas ilícitas realizadas por un ser humano, susceptibles de ser sancionadas por el derecho penal en donde hace un uso indebido de cualquier medio informático para obtener la información o los datos de carácter privado de un individuo, con el propósito de lograr un beneficio.

Entrado en contexto con el ciberdelito se observa que la metodología del riesgo se divide en cuatro factores:

- **Controles**: Son acciones o actividades definidas para evitar que los riesgos se materialicen.
- **Amenazas**: Cualquier agente que tiene como finalidad afectar las características de la información (destrucción, apoderamiento o pérdida), en pocas palabras afectar los activos de información de la organización.
- **Vulnerabilidades**: Es una debilidad en un sistema, el cual permite afectar la integridad y confiabilidad de la información de la empresa.
- **Riesgo**: Es el efecto de la incertidumbre sobre los objetivos de la seguridad de la información

[3] Fuente: Seminario Web Ciberdelitos en épocas de pandemia, impartida por RIsk Consulting

Ampliando un poco más, las amenazas o factores externos que pueden afectar la seguridad de la información se encuentran los siguientes:

Phishing

Es la suplantación de sitios web conocidos, para capturar datos privados y semiprivados de personas o de organizaciones.

El método utilizado por el ciberdelincuente es enviar enlaces (links) a través de medios digitales (redes sociales y/o correos electrónicos) que son bastante llamativos para el cibernauta.

Dentro de las modalidades del phishing se encuentran los siguientes:

- Phishing de clonado o direccionamiento: El ciberdelincuente se hace pasar por alguien conocido o por una marca que cuenta con la confianza de la víctima.
- Búsqueda de navegador: Consiste en posicionar una página falsa por encima de la oficial, esto mediante las técnicas SEO, con dar un solo click se redirecciones hacia la página falsa.
- Spear phishing: Es un ataque más personalizado, en donde a través de redes se hace una perfilación de la víctima (correo electrónico, Smart phone).
- Suplantación CEO: Consiste en hacer credenciales del CEO o de cualquier otra persona con un cargo relevante de la empresa, y así enviar correos electrónicos solicitando datos confidenciales o acciones financieras.
- Smishing: Es un tipo de phishing que no se realiza mediante la suplantación de sitios web ni correos electrónicos, sino utilizando teléfonos móviles. Se hace pasar por una empresa de confianza y envía SMS con información de interés.
- Vishing: El hacker establece centros de atención telefónica, directamente realiza llamadas haciéndose pasar por algún proveedor u operadora de un área soporte.
- Malware basado en phishing: Es un ataque que se caracteriza por el envío de correos electrónicos en los que se introduce una pieza de malware como archivo adjunto descargable.

Captura de datos personales

Es el apoderamiento de información semiprivada, privada o sensible de personas y/o organizaciones a través de medios digitales.

La metodología utilizada es el engaño (ingeniería social), a través de redes sociales, correos electrónicos, o con la instalación de herramientas de malware, también conocido como spyware (software espía), el ciberdelincuente se apodera de datos personales y/o corporativos y con ello, los emplea para su aprovechamiento, iniciando acciones extorsivas bajo la modalidad coercitiva.

Un aspecto importante para considerar es que muchas de las instituciones no cuentan con política de clasificación de los datos, lo cual provoca que muchas veces la fuga de información sea por medio de funcionarios o empleados de las organizaciones.

Transferencia no consentida de activos

Está asociado a la obtención de información financiera (usuario, contraseña) del cuenta habiente y mediante canales electrónicos transfiere el dinero de la persona y/o organización a otra cuenta (money mules).

La metodología utilizada es la instalación de herramientas maliciosas (spyware) se captura la información financiera de personas u organizaciones, en donde se obtiene la contraseña y usuario.

Accesos abusivos a sistemas informáticos

Se trata de ingresos no autorizados a plataformas tecnológicas por parte de los ciberdelincuentes, aprovechando las debilidades, esquemas de seguridad que existen en las organizaciones.

La metodología es el escalamiento de privilegios sobre recursos de TI y/o la instalación de herramientas maliciosas (spyware) se captura la información de la organización, la cual es utilizada para realizar otras modalidades delictivas.

Las políticas o privilegios que realizan en las organizaciones muchas veces están mal definidos, lo que aumenta esta vulnerabilidad, la cual puede ser contrarrestado si se crea una matriz base de quien o no debería tener acceso a la información.

Para materializar los ataques se hacen uso de los malware como ser:

- Virus o worms

Son archivos que se instalan por el usuario y permanecen allí hasta su ejecución y su único propósito es afectar y/o destruir la información del equipo basado en un tema de propagación.

- Spyware

El objetivo de este malware es el robo de información.

- Adware

Esta modalidad se encarga de mostrar publicidad al usuario a través de banners, pop-ups, en donde en muchos casos el objetivo es obtener información sobre las actividades del usuario en red.

- Troyanos

Son archivos que tienen la apariencia de documentos normales, pero esconden en su interior herramientas de malware que buscan la obtención de información y/o el apoderamiento del equipo.

- Keyloggers

Son herramientas capaces de registrar todas las pulsaciones de teclado y con ello conseguir contraseñas.

- Ransomware

Este tipo de ataque es uno de los más abundantes en la actualidad y se basa en el cifrado de datos restringiendo el acceso a los archivos generándose una extorsión digital en donde se pide rescate por la información.

- Malware basado en phishing

Es un ataque que se caracteriza por el envío de correos electrónicos en los que se introduce una pieza de malware como archivo adjunto descargable.

Esto afecta tanto a la pequeña como a la mediana empresa, debido a que muchas de ellas no generan backups de la información.

Vulnerabilidades

Los agentes fuente de las vulnerabilidades son:

- Las personas por su falta de conciencia.
- Las organizaciones porque ven el tema como un gasto.
- El Estado por su falta de regulación.

Ciberseguridad en América Latina

[4]Cada año, millones de nuevos usuarios en América Latina y el Caribe se conectan a Internet por primera vez. Esto, a su vez, crea un recipiente de nuevos clientes que no son tan expertos en tecnología como los clientes digitales más maduros, lo cual propicia un ambiente de mayor riesgo.

Aunque América Latina y el Caribe ha mejorado sus capacidades de ciberseguridad desde 2016, el nivel de madurez promedio de la región todavía está entre 1 y 2, de acuerdo con el [5]CMM (en el que 1 significa etapa Inicial y 5 significa Dinámica o Avanzada).

[4] Fuente: Reporte de ciberseguridad 2020 riesgos y avances y el camino a seguir en América Latina y el Caribe

[5] Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones, ver mayor detalle en el anexo 1

Dentro de las tendencias regionales en el estado de preparación de ciberseguridad se observa el CMM; el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM, por sus siglas en inglés), que fue la base de los estudios regionales de la OEA y el BID en 2016 y 2020, sigue un enfoque integral que entiende la capacidad dentro de cinco dimensiones: (i) política y estrategia; (ii) cultura y sociedad; (iii) educación, capacitación y habilidades; (iv) marcos legales y regulatorios, y (v) estándares, organizaciones y tecnologías.
Para medir de manera confiable la capacidad de seguridad cibernética, cada dimensión se desglosa en factores, aspectos e indicadores, y cada nivel evalúa la capacidad con granularidad progresiva.

Para el año 2017 se realizó una actualización del CMM, en donde se le agregaron otros aspectos a ser tomados en cuenta al momento de la evaluación, como ser; el "modo de operación" de la capacidad de respuesta a incidentes, la "comprensión del usuario de la protección de información personal en línea", los "mecanismos para la presentación de informes", informes de incidentes cibernéticos por "medios y redes sociales", "legislación de protección de datos", "protección infantil en línea", "legislación de protección del consumidor", "legislación de propiedad intelectual", "cooperación formal" y "cooperación informal" sobre asuntos de delitos informáticos, "calidad del software", "controles técnicos de seguridad" y "controles criptográficos".
El CMM comprende cinco etapas, las cuales son.

- **Etapa inicial**: En esta etapa no existe madurez en ciberseguridad o bien se encuentra en un estadio muy embrionario. Puede haber discusiones iniciales sobre el desarrollo de capacidades de ciberseguridad, pero no se han tomado medidas concretas. Falta evidencia observable de la capacidad de seguridad cibernética.
- **Etapa formativa**: Algunos aspectos han comenzado a crecer y formularse, pero pueden ser ad hoc, desorganizados, mal definidos, o simplemente nuevos. Sin embargo, se puede demostrar claramente evidencia de este aspecto.
- **Etapa consolidada**: Los indicadores están instalados y funcionando. Sin embargo, no se le ha dado mucha consideración a la asignación de recursos. Se han tomado pocas decisiones acerca de los beneficios con respecto a la inversión relativa en este aspecto. Pero la etapa es funcional y está definida.
- **Etapa estratégica**: En esta etapa se han tomado decisiones sobre qué indicadores de este aspecto son importantes y cuáles lo son menos para la organización o el Estado en particular. La etapa estratégica refleja el hecho de que estas elecciones se han realizado condicionadas por las circunstancias particulares del Estado o de las organizaciones.
- **Etapa dinámica**: En esta etapa existen mecanismos claros para alterar la estrategia en función de las circunstancias prevalentes, como la sofisticación tecnológica del entorno de amenaza, el conflicto global o un cambio significativo en un área de preocupación (por ejemplo, delito informático o privacidad). Las organizaciones dinámicas han desarrollado métodos para cambiar las estrategias con calma. Sin

embargo, la rápida toma de decisiones, la reasignación de recursos y la atención constante al entorno cambiante son características de esta etapa.

[6]Tomando el CMM como base, se llevó a cabo un reporte de los resultados de la capacidad de seguridad cibernética de la región de América Latina y el Caribe con datos validados a diciembre de 2019. Para cada país evaluado se incluyó una tabla resumen de las cinco dimensiones y su nivel de madurez.
Con base en el reporte se observó que la mayoría de los países se encuentran en una madurez baja, en muchos casos, se puede decir que probablemente la población cuentas con más de un dispositivo celular por cada habitante, Haití y Nicaragua son los países de la región en el que menos porcentaje de la población tiene acceso al internet. Por otro lado, se aprecia que los países de Sur América representan el mayor porcentaje de población con acceso al internet y con la madurez más alta en temas de ciberseguridad, destacándose países como Chile y Uruguay. A nivel centroamericano destaca Costa Rica en donde el 71% de la población tiene acceso al internet.

Considerando las etapas del CMM para [7]Honduras, se visualiza que la mayor parte de los indicadores se encuentran entre la etapa inicial y formativa, asimismo se refleja que en muchos de los indicadores no se observó avance desde el año 2016 encontrándose todavía en la etapa inicial.
Los indicadores más bajos se concentran en; formación, capacitación y habilidades de seguridad cibernética, de igual forma en marcos legales y regulatorios; ya que a nivel de capacitación CONATEL realizó capacitación de dos días sobre ciberseguridad y no ha sido aprobada alguna ley.

Dado que el componente legal y regulatorio es uno de los temas a destacar, a nivel regional se observa que los siguientes países cuentan con legislación en tema de protección de datos o ciberseguridad; Antigua y Barbuda, Argentina, Barbados, Belice, Brasil, Chile, Costa Rica, Ecuador, El Salvador, Granada, Guyana, Jamaica, Paraguay, Perú, República Dominicana, Kitts y Nevis, San Vicente y las Granadinas, Suriname, Trinidad y Tobago, Uruguay y Venezuela.

Desde 2015, el número de países de la región que han adoptado una [8]NCS se ha más que duplicado. Colombia, que encabezó los esfuerzos en esta área al desarrollar la primera NCS de la región en 2011, actualmente está implementando la segunda iteración de su NCS.

los datos sugieren que ambos grupos, tanto funcionarios gubernamentales como usuarios de Internet en general, aún están rezagados con respecto al sector privado; y la sensibilización de los usuarios de Internet a la seguridad en general sigue siendo

[6] Ver mayor detalle en el siguiente enlace https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe
[7] Ver mayor detalle de los resultados en el anexo 2
[8] Estrategia Nacional de Ciberseguridad

relativamente baja. En este sentido, vale la pena recordar que el desarrollo de capacidades de seguridad cibernética sigue siendo un esfuerzo continuo y de toda la nación que sólo podrá tener éxito si se basa en un enfoque inclusivo que incorpore a los grupos vulnerables en toda la sociedad.

Ciertamente, los usuarios de países con legislación más avanzada y específica también informaron niveles más altos de confianza en su uso de Internet. Esto quizá se deba a que, de acuerdo con su experiencia en línea, los usuarios han percibido un aumento de la seguridad, producido gracias a leyes específicas en materia de TIC, legislación de datos, protección del consumidor y protección infantil en línea (introducidas como nuevas medidas por el modelo actualizado).

Entre 2016 y 2020 los puntajes de madurez para la "legislación sobre delitos cibernéticos sustantivos" no progresaron, posiblemente porque ese aspecto ya tiene el puntaje promedio más alto de toda la región. Este avance en la legislación sustantiva se ha complementado cada vez más con el progreso en la "legislación procesal del delito cibernético", que es el aspecto legal que ha registrado la mayor actividad en el período desde 2015. Sin embargo, la [9]legislación sustantiva experimentará mayores aumentos de capacidad en "términos reales", ya que la exigibilidad depende crucialmente de las disposiciones procedimentales.

"Divulgación responsable" fue el aspecto con el puntaje de madurez más bajo de la región. La amplitud y el enfoque integrado del CMM permiten contextualizar aún más las puntuaciones de los aspectos individuales.
En este sentido, los riesgos asociados con la falta de un mecanismo institucionalizado para compartir información sobre vulnerabilidades descubiertas y políticas sobre piratería ética (ethical hacking) podrían verse agravados por los puntajes igualmente bajos para las capacidades de respuesta interna, incluyendo "organización de protección de infraestructura crítica", "gestión de crisis", "gestión y respuesta a riesgos" y "seguro de delito informático", que se ubican en la parte inferior y han visto pocas mejoras desde 2015.
Además de los compromisos con el desarrollo de capacidades de seguridad cibernética a nivel nacional, América Latina y el Caribe ha sido más que el fundamento de una serie de iniciativas regionales muy dinámicas. Por ejemplo, en 2016 se realizó el lanzamiento de CSIRT Américas, una plataforma que permite la cooperación regional y el intercambio de información entre los equipos de respuesta a incidentes gubernamentales y nacionales de los Estados Miembros de la OEA.
Desde 2015, la propia comunidad de respuesta a incidentes ha crecido a 20 CSIRT nacionales dentro de la región.

Dado que la ciberseguridad es crítica para nuestra prosperidad y seguridad. Las actividades cibernéticas maliciosas no sólo amenazan las economías, sino también el funcionamiento mismo de nuestras democracias, libertades y valores. Nuestra seguridad futura depende de

[9] Es aquella que se encuentra prescrita en un código o ley

que sepamos transformar la capacidad para protegernos contra las amenazas cibernéticas: tanto la infraestructura civil como la capacidad militar dependen de sistemas digitales seguros.

Ciberdelito en épocas de pandemia

[10]La pandemia de la COVID-19 y el incremento de la actividad digital que ha generado en la región, ha dejado aún más en evidencia las vulnerabilidades del espacio digital de América Latina y el Caribe.

El Informe de Cibercrimen ThreatMetrix identificó a América Latina como un foco para el fraude en la creación de cuentas, con alrededor del 20% del volumen total frente a un promedio de la industria del 12,2%.

Amenazas emergentes en ciberseguridad

La pandemia mundial del COVID-19 ha marcado un punto de inflexión fundamental en nuestra senda mundial y ha acentuado como nunca nuestra dependencia de la infraestructura digital.

En un lapso de tres meses, experimentamos una aceleración de la transformación digital que se había anticipado que ocurriría en tres años

Incluso antes de la pandemia, las brechas de ciberseguridad y las filtraciones de datos se estaban convirtiendo en los principales obstáculos de la economía digital. Los cibercriminales aprovechan rápidamente los nuevos vectores de ataque y se benefician de los vacíos en la cooperación de las fuerzas del orden público en las diferentes jurisdicciones, dada la naturaleza inherentemente transnacional de sus actividades maliciosas.

Según el Informe de Riesgos Globales 2020 del Foro Económico Mundial, el riesgo de ciberataques a la infraestructura crítica y el fraude o robo de datos se clasificaron entre los principales riesgos con mayor probabilidad de ocurrir, mientras que la reciente Perspectiva de Riesgos del COVID-19 del Foro Económico Mundial identificó los ciberataques como la tercera mayor preocupación debido a nuestra actual y sostenida transición hacia los patrones de trabajo digital.

Los datos disponibles respaldan estas preocupaciones; se estima que los daños por delitos cibernéticos alcanzarán los US$6 billones para 2021, lo que equivale al producto interno bruto (PIB) de la tercera economía más grande del mundo.

A medida que la región avanza cada vez más hacia la economía digital, aumenta la necesidad de garantizar la confianza digital. Los protocolos de gestión de riesgos de seguridad digital y protección de la privacidad constituyen responsabilidades compartidas por los gobiernos,

[10] Fuente: Reporte de ciberseguridad 2020 riesgos y avances y el camino a seguir en América Latina y el Caribe

el sector privado y los usuarios individuales en una economía cada vez más impulsada por los datos.

En los últimos años, la ciberseguridad ha roto la barrera de los silos técnicos y se encuentra en la intersección de múltiples disciplinas y áreas de políticas: acceso digital y conectividad, resiliencia, justicia penal, diplomacia, seguridad y defensa internacional, y economía digital y comercio, así como las nuevas tecnologías.

Hasta la fecha, el desequilibrio entre el tiempo de comercialización y el "tiempo de seguridad" sigue siendo una cuestión predominante, debido a la presión de las fuerzas del mercado en favor de los productos de nuevas tecnologías, sin incentivos para priorizar los elementos de seguridad desde el inicio del ciclo de vida del producto.

Antes de la crisis del COVID-19, se esperaba que el gasto global en productos y servicios de seguridad cibernética aumentara en un 88% en los próximos ocho años.

La recesión económica causada por la pandemia podría conducir a la consolidación de este mercado. En los últimos cinco años, la noción de que la estrategia de ciberseguridad forma parte integral de la estrategia comercial ha ganado más tracción e implementación real por parte de las empresas.
Esta mayor conciencia a nivel del liderazgo corporativo es un primer paso crucial para potenciar la toma de decisiones corporativas informadas para la planificación de la seguridad cibernética, los mecanismos de respuesta y las inversiones la estructura económica de ALC está compuesta en un 99,5% por micro, pequeñas y medianas empresas (mipyme). Por lo tanto, aumentar la conciencia de seguridad cibernética y promover la higiene básica de seguridad cibernética en las pymes de la región debería ser una prioridad crítica en los próximos años.
Una de las formas posibles de abordar los desafíos emergentes de ciberseguridad entre los Estados sería implementar un enfoque internacional que se centre en la armonización de las capacidades de ciberseguridad.

La creación de conciencia entre los expertos técnicos, políticos y las fuerzas del orden podría ayudar a que los países sean menos vulnerables al delito cibernético. La naturaleza de los actos criminales que tienen lugar en el ciberespacio está cambiando rápidamente, por lo que los países deben invertir más en educar a su personal en la aplicación de la ley, los sistemas judiciales y otras instituciones gubernamentales relevantes. Adaptarse a las nuevas circunstancias es clave también para la puesta en marcha de asociaciones público-privadas (APP) confiables.

La armonización regional de marcos legales para abordar el delito cibernético y las mejores prácticas de aplicación de la ley podrían contribuir a obtener seguridad y estabilidad regional en el ciberespacio.

Una estrategia nacional de ciberseguridad podría funcionar como el principal instrumento de sensibilización y planificación en los diferentes Estados.
Algunas de las mejores prácticas que tenemos para continuar el trabajo a nivel nacional involucran contar con una mejor coordinación nacional y mecanismos de intercambio de información; superar las brechas entre el nivel de expertos y los principales encargados de la toma de decisiones nacionales en los sectores público y privado.

Una estrategia de seguridad cibernética a nivel de todo el gobierno, que incluya posibles medidas preventivas, legislación nacional para abordar el delito cibernético y la cooperación operativa internacional entre los Estados, debería ser uno de los requisitos más importantes para evitar actividades que exploten las vulnerabilidades críticas de la infraestructura.
Una mayor cooperación regional para desarrollar una visión compartida y aprender de las mejores prácticas de otros Estados es clave para armonizar las capacidades de ciberseguridad nacionales.

Acciones para disminuir la materialización del riesgo

Se debe gestionar el riesgo para evitar que este se materialice, existen diversos cuestionamientos que cada empresa se debe de hacer, basarse en el cumplimiento de medidas, pero no solo porque se le puede multar; por lo cual toda institución debe realizar ciertos cuestionamientos.

1. Identificar cuáles son los activos de información más importantes de la organización.
- ¿Conozco los activos de información dentro de mi organización?

Un ciberactivo es todo lo que tengo en la red, ejemplo; página web, servicios a través de la nube, servicios adquiridos a través de la web.

Es muy importante identificar de quien es el activo ya que puede ser manejado por un tercero en ese caso se debe tener claro que es lo que desea proteger.

Activo de información son también las plataformas que permiten administrar los datos

- ¿Los he clasificado de acuerdo con su criticidad?
- ¿Tenemos una matriz de responsabilidad?
  La matriz de seguridad muchas veces se hace al tanteo y no se documenta, el riesgo debe ser administrado ya no por la alta gerencia ni por las áreas de planeación sino por cada uno de los funcionarios de la compañía

2. Realizar una gestión de riesgo frente a ciberseguridad, seguridad informática y seguridad de la información.

- ¿Conozco cuáles son mis amenazas?
- ¿Distingo mis vulnerabilidades?
- ¿Se ha ponderado los riesgos de acuerdo con mi exposición?

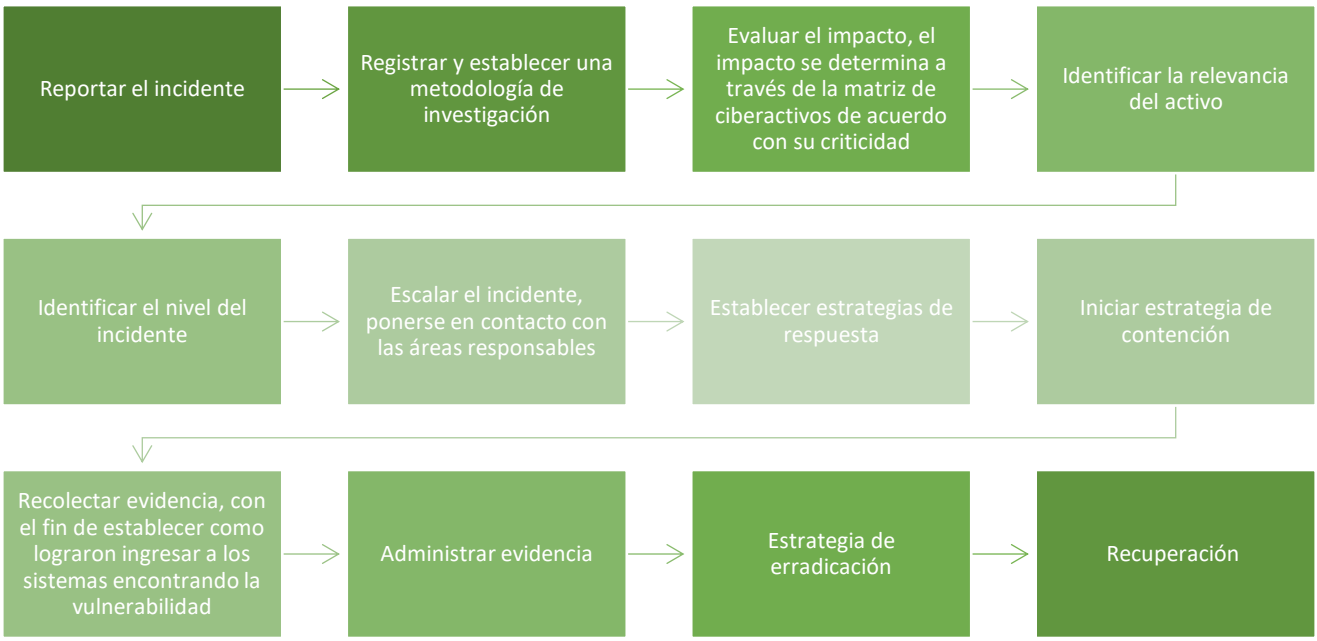
Es importante identificarlos riesgos, y que las metodologías sean entendibles, las matrices de riesgos van dirigidas a todos los funcionarios y empleados de una organización ya que si no se conocen pueden ser vulnerables, al no conocer los riesgos se pueden materializar los ataques a través de esas personas.

3. Definir políticas complementarias frente a ciberseguridad, seguridad informática y seguridad de la información

- ¿Existen políticas de ciberseguridad?
- Políticas para dispositivos móviles
- Políticas de trabajo
- Políticas de control de acceso
- Políticas de controles criptográficos
- Política de respaldo de información
- Política de transferencia de información
- Política de desarrollo seguro de software
- Política de relación con proveedores
- Política de protección de datos personales

Es importante implementar lo que se tiene por escrito tanto a nivel de seguridad informático como de ciberseguridad.

Dado el surgimiento de un Incidentes se deberían de llevar a cabo los siguientes pasos



A nivel de empresa con relación al ciberataque se puede observar que todas pueden ser objetivo de ataques cibernéticos, sin embargo, aquellas que tienen transaccionalidad pueden están más propensas y sobre todo aquellas que no tienen ningún tipo de control para proteger los datos, ya que los ciberdelincuentes lo que hacen es perfilar y determinar diferentes variables para ejecutar sus ataques.

En caso de contar con servicio externo de proveedor de una nube, es importante realizar un contrato externo con los lineamientos de cumplimiento exigidos en nuestro país.

La política de administración de incidentes debe estar a cargo de un grupo de respuesta de incidentes que no tenga dependencia de un área de TI ya que los incidentes pueden ocurrir por acción o por omisión, por lo que los incidentes pueden ocurrir por la falta de cumplimiento de una política que probablemente el área responsable de implementar esa política puede ser un área de TI.

El Hackeo ético o pruebas de vulnerabilidad son pruebas que se deben hacer periódicamente, ya que al realizar la prueba en caso de encontrar fallas y solucionarlas, luego determinar si continua o no continua y realizar el informe de remediación, en instituciones financieras se recomiendan dos pruebas de vulnerabilidad al año.

[11]Como saber si ha sido víctima de un ciberdelito

- **Infección de malware**: El equipo podría empezar a funcionar lentamente y a enviar diversos mensajes de error.

- **Ataques de phishing o pharming**: Encontrará cargos sospechosos en la tarjeta de crédito o en otras cuentas comprometidas.

- **Keylogger**: Se observan iconos extraños o sus mensajes podrían empezar a añadir texto duplicado.

- **Botnet**: Si su equipo queda atrapado por una botnet, puede resultar difícil darse cuenta de ello.

- **Crytohacking**: Su factura eléctrica aumenta.

En la recomendación 15 de GAFI, acerca de nuevas tecnologías menciona que: “Los países y las instituciones financieras deben identificar y evaluar los riesgos de lavado de activos o

[11] Fuente: Avast.com

financiamiento del terrorismo que pudieran surgir con respecto a; (a) el desarrollo de nuevos productos y nuevas prácticas comerciales, incluyendo nuevos mecanismos de envío, y (b) el uso de nuevas tecnologías o tecnologías en desarrollo para productos tanto nuevos como los existentes. En el caso de las instituciones financieras, esta evaluación del riesgo debe hacerse antes del lanzamiento de los nuevos productos, prácticas comerciales o el uso de tecnologías nuevas o en desarrollo. Los países y las instituciones financieras deben tomar medidas apropiadas para administrar y mitigar esos riesgos".

[12]A continuación, se presentan los elementos representativos de la nota interpretativa.

[12] Activo virtual: De acuerdo con el glosario de términos del GAFI lo define como una representación digital de valor que puede ser comerciada o transferida digitalmente y que puede ser usada para realizar pagos o inversiones

La aplicación de medidas preventivas deberá cumplir con los requisitos establecidos en las recomendaciones 10 a 21 y sus calificaciones para los PSAV.

Fraude

[13]Existe una serie de delitos relacionados con tarjetas de pago, cajeros y sistemas de pago como terminales de punto de venta. La frecuencia de pagos en línea ha supuesto un gran impulso para los delincuentes al abrirles un abanico de nuevas posibilidades.

Los delitos abarcan desde agresiones físicas en cajeros, por ejemplo, utilizando explosivos, a fraudes cibernéticos sofisticados como ataques “de caja negra”, en los que un dispositivo no autorizado envía comandos directamente al cajero.

[14]Según un informe de 2016 de [15]Nilson Report, en 2015 se generaron más de US$31.000 billones en todo el mundo a través del sistema de pago por tarjetas, una cantidad 7,3% mayor que la de 2014.

Datos de Nilson Report indican que las pérdidas mundiales por fraude con tarjetas se elevaron a más de **US$21.000 millones** en 2015, frente a los 8.000 millones de dólares registrados en 2010.
Para 2020, se espera que la cifra llegue a los **US$31.000 millones**. En estos costos, se incluyen, entre otros gastos, los **reembolsos** que los bancos y las compañías de tarjetas de crédito hacen a los clientes defraudados, lo que incentiva a las empresas de este tipo a realizar importantes inversiones en tecnologías antifraude.

Hay muchos tipos de fraude de tarjetas de crédito y cambian con tanta frecuencia como las nuevas tecnologías, de ahí a que sea casi imposible enumerarlos.
Pero hay dos categorías principales: los conocidos como fraudes de "tarjeta no presente" y los de "tarjeta presente".
El primer caso se trata del tipo más común y ocurre cuando la información del titular de la cuenta de banco es robada y utilizada ilegalmente sin la presencia física de la tarjeta.
Esta estafa suele ocurrir en línea y puede ser el resultado de los llamados correos electrónicos de *phishing* o suplantación de identidad, enviados por estafadores que se presentan como instituciones creíbles para robar información personal o financiera a través de un enlace con un programa malicioso.

El segundo caso, aunque resulta cada vez menos común, ocurre cuando un vendedor pasa la tarjeta por un dispositivo que almacena su información y luego la utiliza para cargarle otras compras no realizadas.

[13] Fuente: Interpol.int
[14] Fuente: bbc.com
[15] Es un comunicado diario de eventos internacionales especializado en opiniones públicas acerca de distritos escolares, gobiernos locales y negocios

[16]Además del robo de tarjeta, los delincuentes utilizan varios métodos para capturar los datos, entre ellos "skimming" (robo de datos en cajeros o máquinas expendedoras para la clonación de tarjetas) y "phishing". A menudo las personas no son conscientes de la sustracción de los datos de su tarjeta hasta que es demasiado tarde. Estos datos pueden servir para fabricar tarjetas falsas o utilizarse posteriormente para cometer fraudes sin presencia física de tarjeta.

Los estafadores utilizan la información para adquirir bienes en nombre de las víctimas o para obtener fondos no autorizados de sus cuentas. Los datos de estas tarjetas también pueden ponerse a la venta en mercados de la red oscura. En muchos casos los datos robados en un país se utilizan en otros lugares, dificultando su rastreo.

[17]El fraude con tarjetas de crédito se facilita, en parte, porque las transacciones con este sistema de pago son un proceso simple, de dos pasos: autorización y liquidación.
En un inicio, los involucrados en la transacción (el cliente, el comerciante y los bancos que realizan y reciben la transferencia) envían y reciben información para autorizar o rechazar una compra determinada.
Si la compra se autoriza, se liquida mediante un canje de dinero, que suele tener lugar varios días después de la autorización.

Pero una vez que la compra ha sido autorizada, no hay marcha atrás. Esto significa que todas las medidas de detección de fraude deben realizarse durante el primer paso de una transacción.
Sin embargo, el rechazo de una transacción solo ocurre en dos situaciones: si el saldo en la cuenta del titular de la tarjeta es insuficiente o si, sobre la base de los datos proporcionados por el banco, hay sospechas de fraude.

Mediante el seguimiento continuo del gasto e información del titular de la tarjeta, en el que se incluya el tiempo, la cantidad y las coordenadas geográficas de cada compra, es posible desarrollar un modelo informático para calcular la probabilidad de un uso fraudulento de la misma.

Si la probabilidad pasa un determinado umbral, el emisor de la tarjeta recibiría una alarma y la empresa podría decidir bloquear la tarjeta directamente, iniciar una investigación más profunda o llamar al consumidor.

La fuerza de este modelo es que apunta a maximizar una ganancia o minimizar un costo esperado.

En otras palabras, todos los cálculos estarían dirigidos a limitar la frecuencia de falsas alarmas.

[16] Fuente: Interpol.int
[17] Fuente: bbc.com

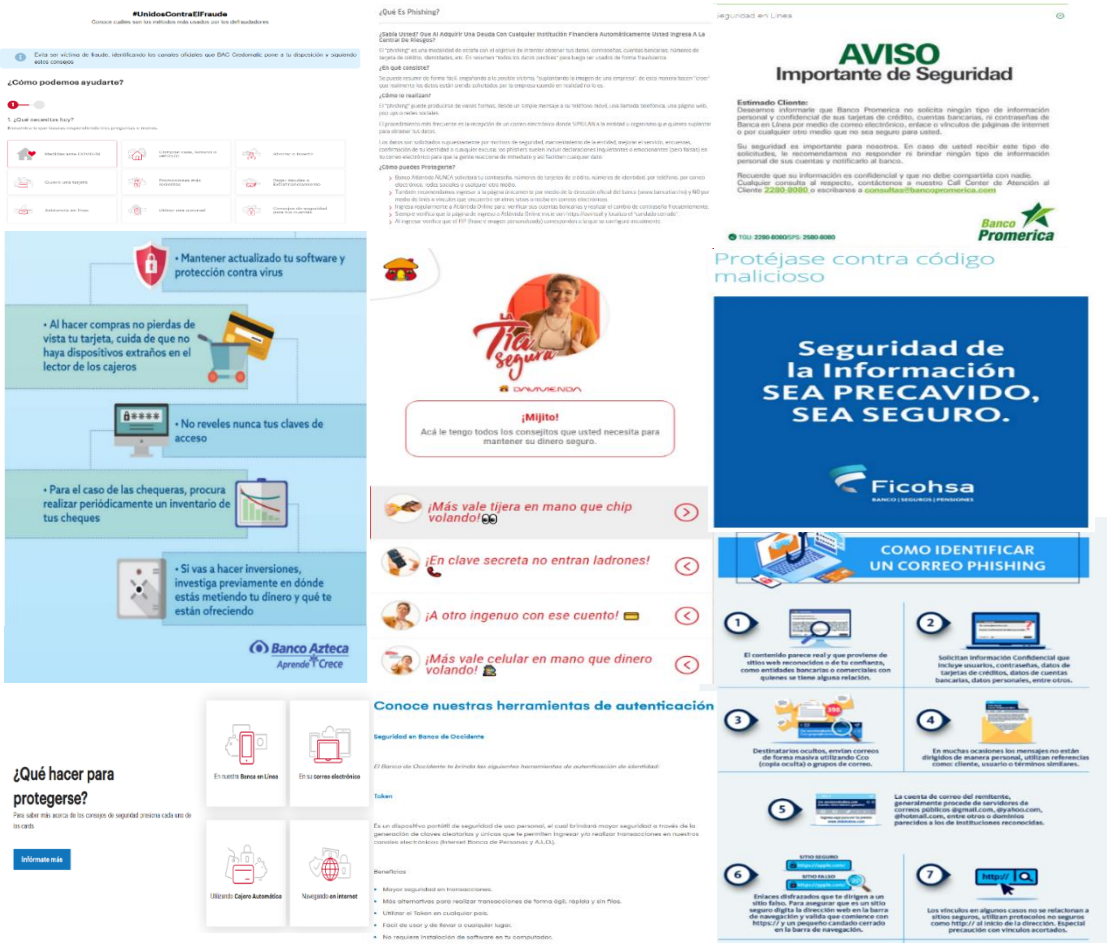
[18]Las operaciones mundiales o airport action days se realizan regularmente y tienen por objeto interceptar a viajeros que vuelan con billetes adquiridos con datos robados de tarjetas bancarias. Posteriormente, se toman medidas contra las organizaciones delictivas detrás de estos delitos. Estas operaciones están organizadas conjuntamente por Europol, INTERPOL y otras partes interesadas internacionales.

Campañas de seguridad de los sujetos obligados

Con el fin de conocer las acciones que los diferentes Sujetos Obligados realizan referente al tema de fraude y ataques cibernéticos se consultaron las páginas web de 14 bancos y 3 cooperativas. De las páginas web consultadas en la de siete instituciones no se encontró alguna campaña, al mes de enero del presente año, así como en las tres cooperativas.

Cabe señalar que la información en el total de las observaciones se encontraba en el apartado de usuario financiero, no es de fácil visualización y tampoco forma parte de los anuncios principales de las páginas web.

Se presenta a continuación un Collage de alguna de las páginas web consultadas.



[18] Fuente: interpol.int

Análisis de resultados

Es previsible que la desaceleración de las actividades económicas a nivel mundial derivada de la crisis sanitaria motivara a muchos de los segmentos económicos y financieros que tradicionalmente prestan servicios de manera presencial a migrar a nuevos medios y canales de atención no presenciales, y pudiesen experimentar aumentos en los canales digitales ya implementados previo a la pandemia por COVID-19.

Con el objetivo de poder recolectar datos para el análisis del proyecto, se elaboró un cuestionario el cual se conformó por 35 preguntas, estas a su vez fueron agrupadas en las siguientes secciones; canales utilizados, herramientas utilizadas, nuevos productos, análisis de riesgos, capacitación interna, sensibilización del usuario, zonas geográficas con mayor incidencia, montos, Reportes de Operaciones Sospechosas.

El cuestionario fue enviado a diferentes tipos de institución o sectores, como ser; Bancos Comerciales, Bancos Estatales, Cooperativas de ahorro e Instituciones no bancarias que brindan servicios de pago por medio de pago utilizando dinero electrónico (INDEL).

En total se recibieron 43 respuestas, comprendido entre 15 Bancos Comerciales, 3 Bancos Estatales, 24 Cooperativas de Ahorro y Crédito y la INDEL.

A continuación, se presentan los resultados de análisis de los datos:

Su institución ha creado nuevos Canales o servicios para la realización de transacciones no presenciales por parte de los clientes previa la pandemia por covid-19

En la ilustración N°1 (gráficos N°1-gráfico N°4) se refleja de forma gráfica por tipo de institución, si previo a la pandemia por Covid-19 las instituciones crearon nuevos productos o servicios brindados de forma no presencial, obteniendo que los cuatro tipos de institución crearon nuevos canales no presenciales, destacándose los Bancos Comerciales.

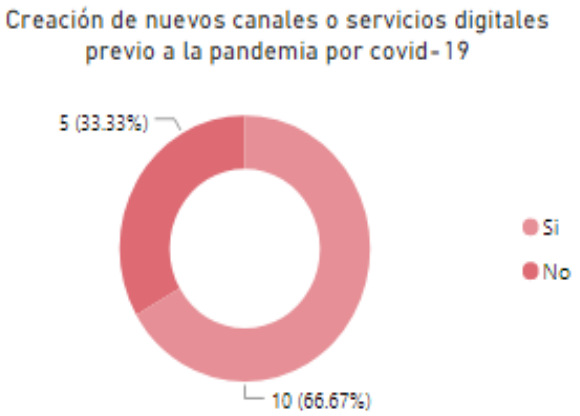


Gráfico N°1: Bancos Comerciales

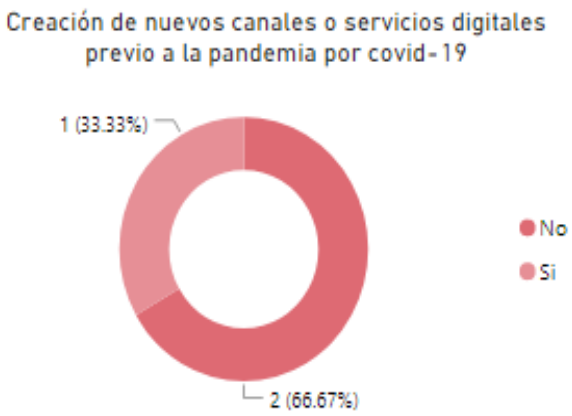


Gráfico N°2: Bancos Estatales

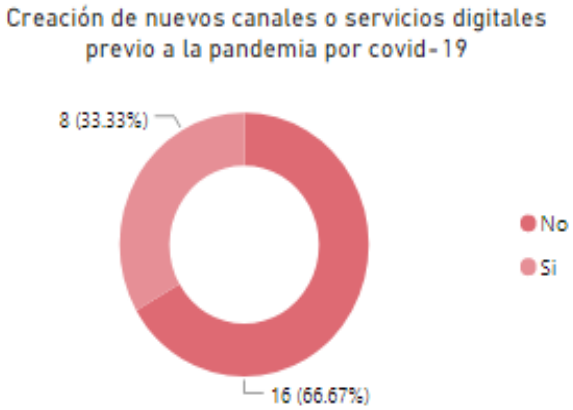


Gráfico N°3: Cooperativas de ahorro y crédito

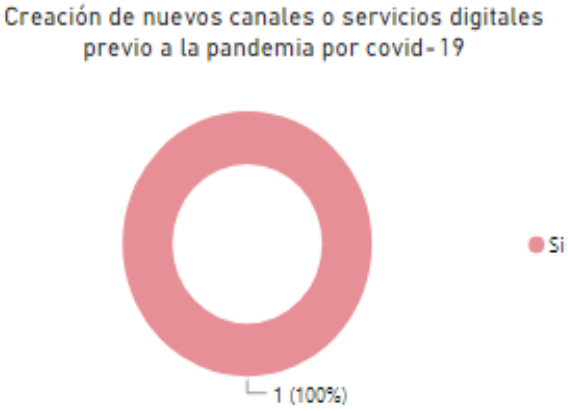


Gráfico N°4: INDEL

Ilustración 1: Creación de nuevos productos o servicios previo a la pandemia por Covid-19

<u>Su institución ha creación nuevos Canales o servicios para la realización de transacciones no presenciales por parte de los clientes durante la pandemia por covid-19</u>

Durante la pandemia por Covid-19, los Bancos Comerciales y Cooperativas de Ahorro y Crédito fueron las que establecieron nuevos productos o servicios digitales o no presenciales, como se aprecia en la ilustración N°2 (gráfico N°1-gráficoN°4). Cabe destacar, dado el tipo de actividad, catera de clientes y productos financieros ofrecidos, así como las restricciones de circulación; por tales razones ha crecido la necesidad de brindarle al cliente facilidades para poder llevar a cabo las operaciones que previo a la pandemia por Covid-19 se llevaban a cabo de manera presencial, es por ello, que las instituciones antes mencionadas se reflejan como las que crearon estos nuevos canales.

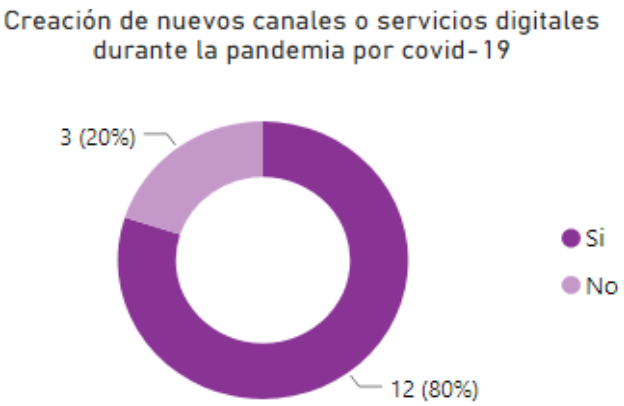


Gráfico N°1: Banco

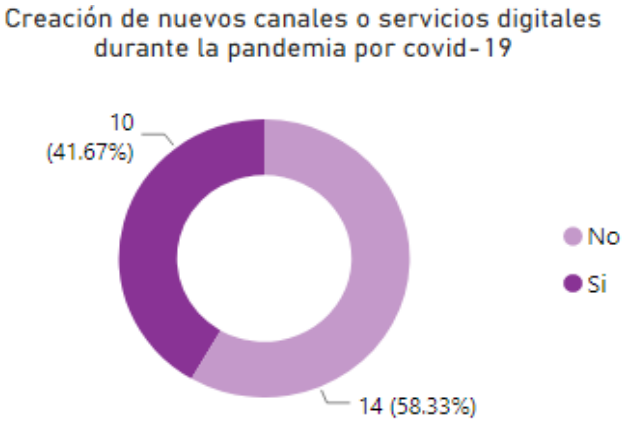


Gráfico N°2: Cooperativas de Ahorro y

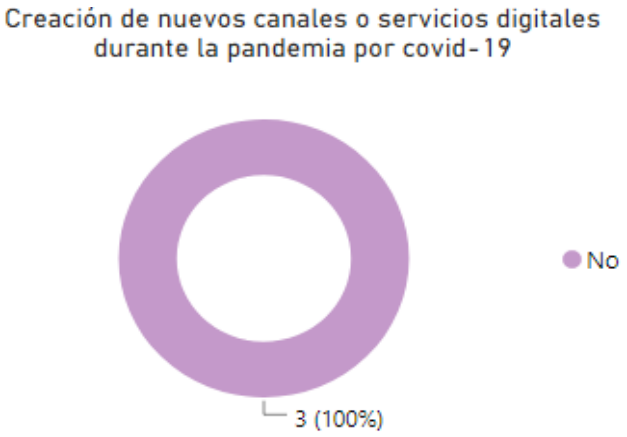


Gráfico N°3: Bancos Estatales

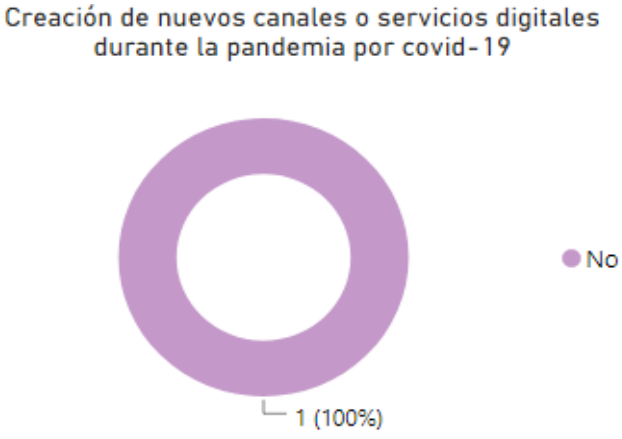


Gráfico N°4: INDEL

Ilustración 2:Creacion de nuevos productos o servicios durante la pandemia por Covid-19

De acuerdo con los datos presentados en la ilustración N°3 (gráfico N°1-gráfico N°4), de manera global, se tuvo un aumento de aproximadamente 5% en la creación de nuevos productos durante la pandemia por Covid-19, situación que como se mencionó previamente son instituciones con una amplia cartera de clientes y productos brindados, por lo que surge la necesidad de ofrecer mayores facilidades a los clientes y que estos puedan llevar a cabo sus transacciones sin verse perjudicados por la situación acontecida durante la pandemia por Covid-19.

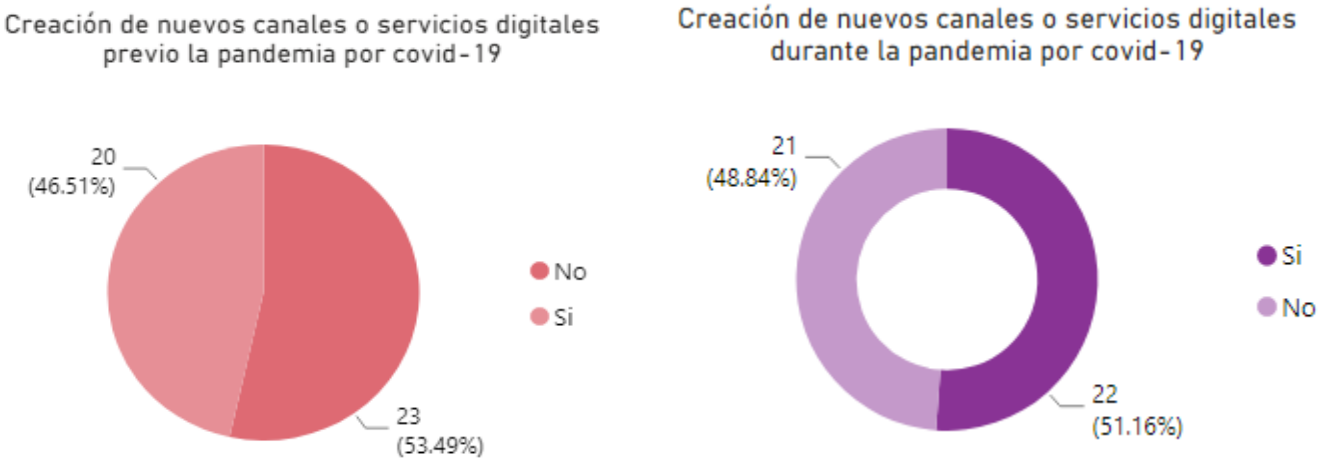


Ilustración 3: Comparativo de creación de nuevos productos o servicios antes y durante la pandemia por Covid-19

Qué tipo de canales o servicios ha creado

Con el surgimiento de necesidades encaminadas a la nueva realidad, las cuales conlleva a la creación de nuevos productos no presenciales o digitales, se estima al menos 17 nuevos canales creados entre los distintos tipos de institución. Es esencial acentuar que, si bien es cierto, algunos de estos medios digitales ya eran conocidos en algunas instituciones, para otras surgieron como parte de su catálogo de servicios brindados. Tomando como referencia los primeros cinco canales creados, como se observa en la ilustración N°4 (ilustración N°1-ilustración N°4) tenemos; aplicaciones móviles, Banca en línea, Apertura de productos no presenciales, afiliación de nuevos servicios y medios de pago sin contacto, siendo las aplicaciones móviles las que representan el 20% de los nuevos canales.

Por otro lado, se presentó la incorporación del servicio de depósito de cheques de manera no presencial, la cual se puede realizar por medio de una app móvil, tomando fotografía al frente y dorso del mismo, posteriormente siguiendo indicaciones simples, el cliente puede tener el depósito a su cuenta, ya sea un cheque propio de la institución o por compensación.

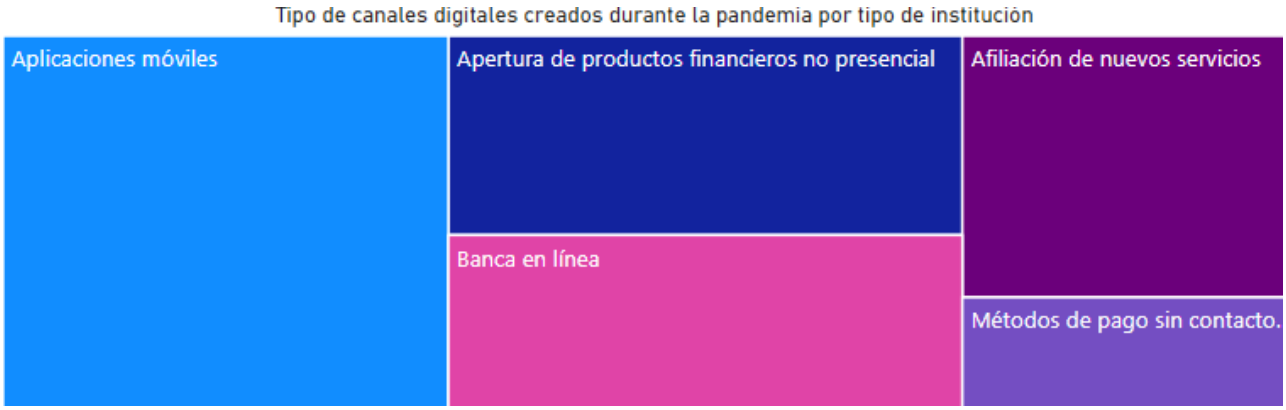
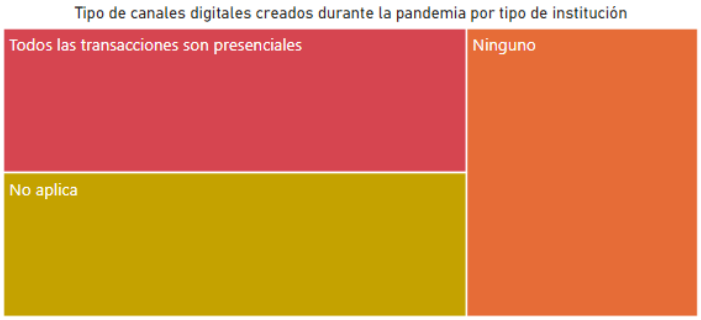


Ilustración 4:Canales o servicios creados durante la pandemia por Covid-19

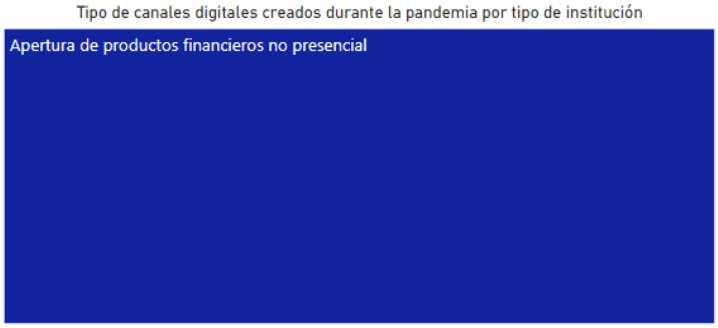
En la ilustración N°5, se observó que los Bancos Comerciales y las Cooperativas de ahorro y crédito (cuadro N°1 y cuadro N°2) respectivamente, fueron las instituciones que crearon nuevos canales no presenciales, de la ilustración N°5 se destacan las aplicaciones móviles, banca en línea y apertura de productos no presenciales.

Cuadro N°1: Bancos Comerciales

Cuadro N°2: Cooperativa de ahorro y crédito



Cuadro N°3: Bancos Estatales



Cuadro N°4: INDEL

Ilustración 5:Tipo de Canales y Servicios creados por tipo de institución

<u>En qué porcentaje han aumentado las transacciones u operaciones de los clientes por medio de canales digitales durante la pandemia por Covid-19</u>

La creación de nuevos canales o servicios no presenciales trajo consigo el incremento de tales operaciones, es por ello, en el gráfico N°1 se refleja el porcentaje en que las mismas incrementaron durante la pandemia por Covid-19; siendo de 1%-25% el mayor porcentaje de incremento de forma global.

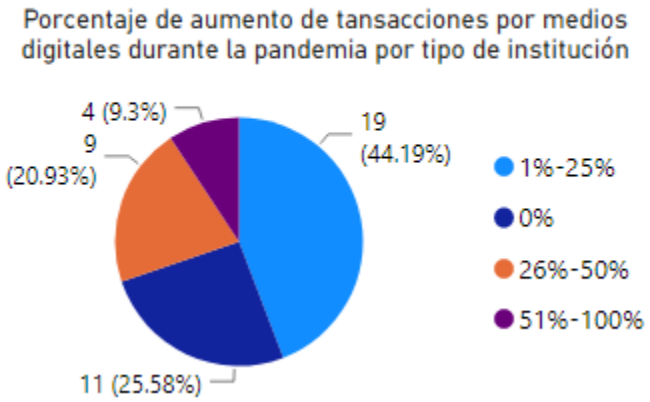


Gráfico 1:Porcentaje de incremento de transacciones por medio de canales digitales durante la pandemia por Covid-19

Por tipo de institución se observa en la ilustración N°6 (gráfico N°1-gráfico N°4), que los Bancos Comerciales (gráfico N°1) y las Cooperativas (gráfico N°2) en más del 40% han percibido un porcentaje de aumento en sus transacciones de 1%-25%, es preciso señalar que, en el caso de la INDEL, el aumento porcentual de incremento en sus operaciones oscila entre 26%-50%.

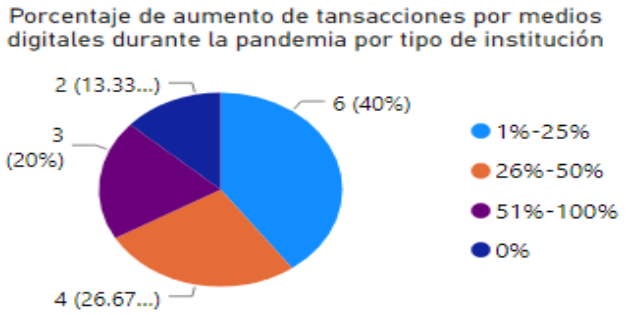


Gráfico N°1: Bancos Comerciales

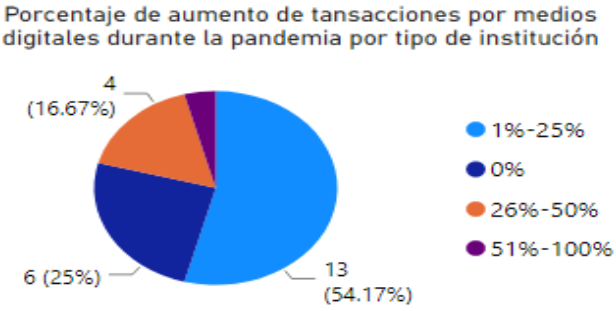


Gráfico N°2: Cooperativas de Ahorro y Crédito

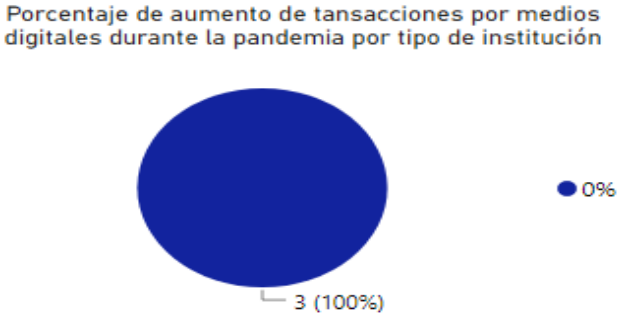


Gráfico N°3: Bancos Estatales

Gráfico N°4: INDEL

lustración 6:Porcentaje de aumento de transacciones por medio de canales digitales

Transacciones realizadas por medios digitales en el periodo de marzo a noviembre del año 2019

En la consulta realizada a fin de medir la utilización de parte de los clientes de los medios digitales para realizar sus transacciones durante el año 2019 de forma global considerando los cuatro sectores antes referidos, se determinó que previo a la Pandemia por COVID-19, los clientes no percibían las necesidad de utilizar los medios digitales para realizar sus operaciones transaccionales ya que en el gráfico N°2 refleja que el 44.19% de las instituciones indicaron operaciones transaccionales por medios digitales entre 1-1,000.00 y el 39.53% indicó que mayor de 5,000.

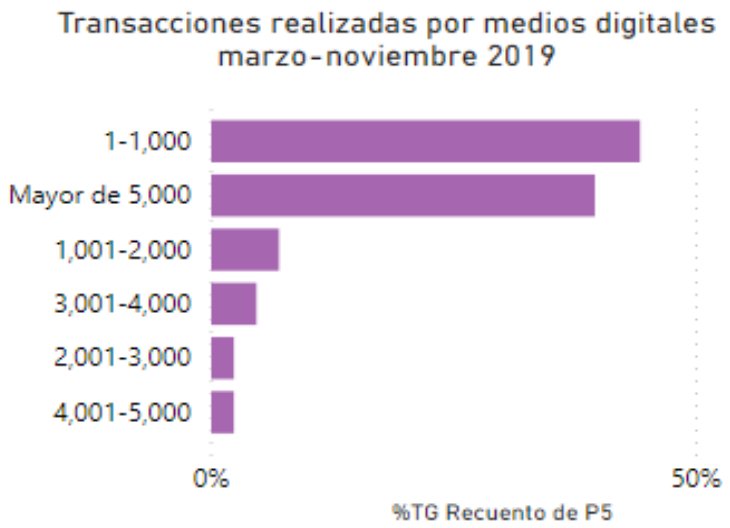


Gráfico 2:Transacciones realizada por medios digitales en el periodo de marzo a noviembre del año 2019

Pudiéndose visualizar en los gráficos N°1 y N°4 que los sectores que más han realizado transacciones por medios digitales han sido los Banco Comerciales e INDEL en un 86.67% y 100%, respectivamente indicando transacciones realizadas mayores a 5,000; debido a que en los últimos años de parte de ambos sectores se ha visualizado mayor inversión en plataformas, aplicaciones y contratación de medios electrónicos se han posicionado como una alternativa para satisfacer diferentes necesidades operativas de sus clientes.

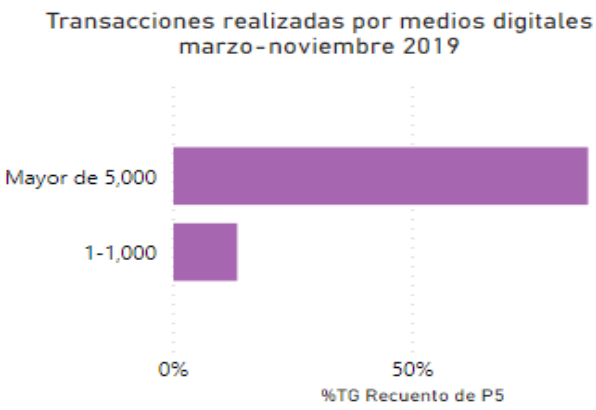


Gráfico N°1: Bancos Comerciales

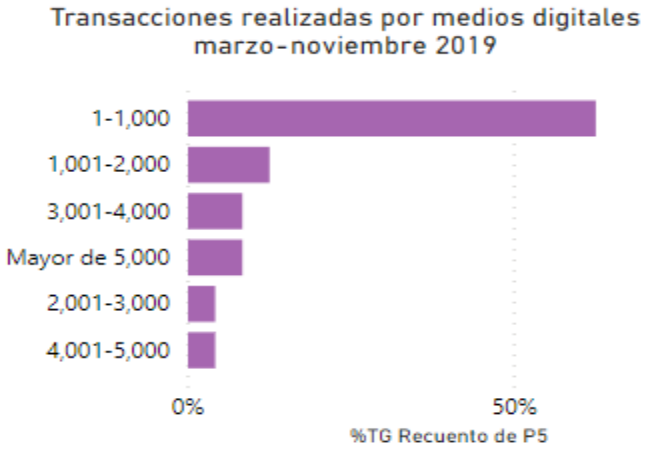


Gráfico N°2: Cooperativas de Ahorro y Crédito

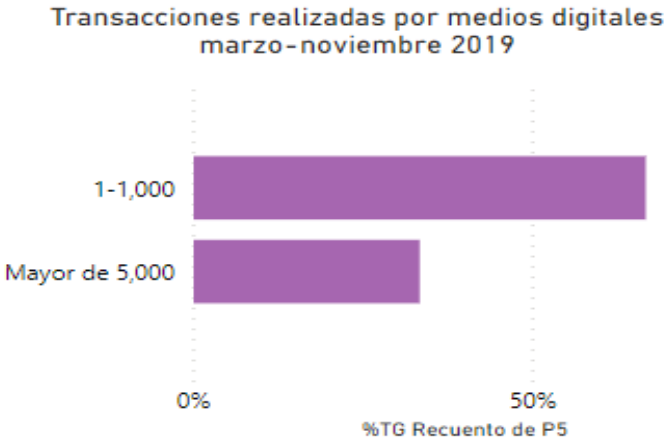


Gráfico N°3: Bancos Estatales

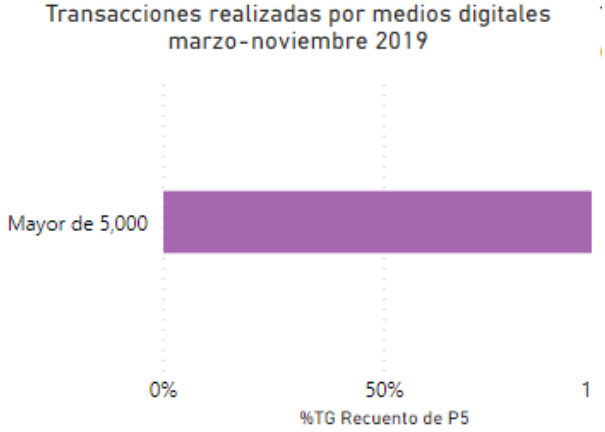


Gráfico N°4: INDEL

<u>Transacciones realizadas por medios digitales en el periodo de marzo a noviembre del año 2020</u>

El periodo de distanciamiento social por la pandemia de COVID-19 para el año 2020 ha impulsado que otras instituciones bancarias y Cooperativas de Ahorro y Crédito hayan invertido en plataformas digitales para ofrecer mayores medios digitales que puedan agilizar operaciones transaccionales para los clientes. Para el caso de los bancos estatales y las cooperativas de ahorro y crédito para el año 2019 y 2020 se mantuvieron con el mismo número de 1-1,000 transacciones digitales realizadas equivalentes a 66.67% y un 58.33%, respectivamente.

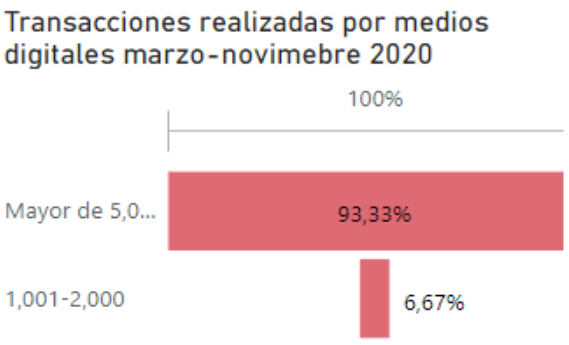


Gráfico N°1: Bancos Comerciales

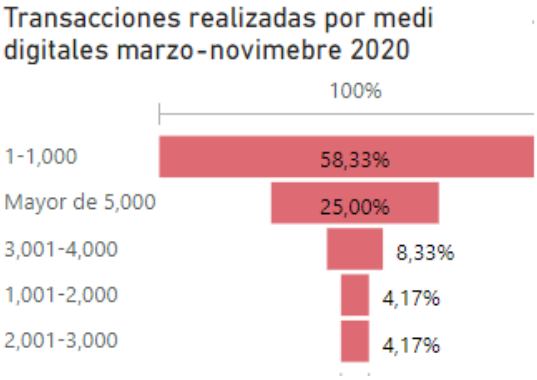


Gráfico N°2: Cooperativas de Ahorro y Crédito

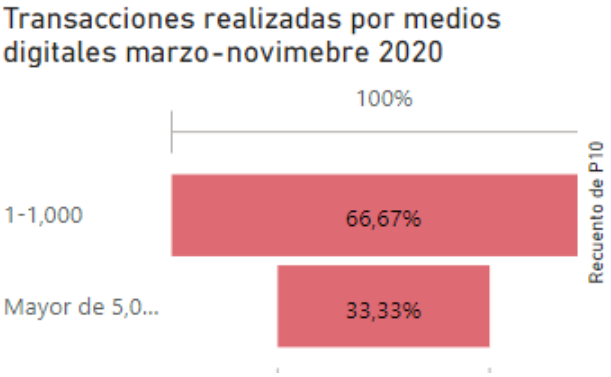


Gráfico N°3: Bancos Estatales

Gráfico N°4: INDEL

<u>Con las nuevas innovaciones tecnológicas implementadas en su institución financiera, realizó una evaluación de riesgos LA/FT previo al lanzamiento de servicio o producto</u>

El surgimiento de nuevos canales y servicios puede traer consigo riesgos implícitos, sin embargo, en el gráfico N°3 se aprecia que más del 60% de las instituciones realizan evaluación de riesgos, previo al lanzamiento de nuevos productos.

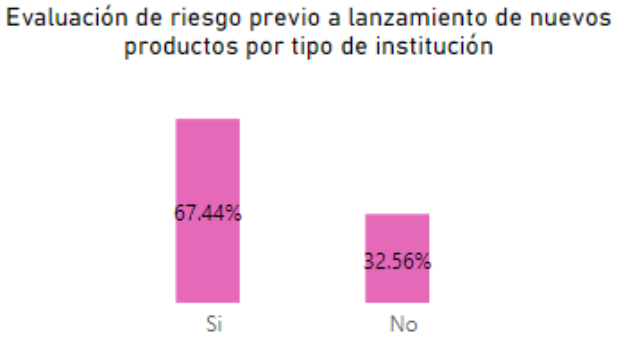


Gráfico 3:Evaluación de riesgo previo al lanzamiento de nuevos productos

La ilustración N°7 (gráfico N°1-gráfico N°4) muestra que en los cuatro tipos de institución se realiza evaluación del riesgo previo al lanzamiento de nuevos productos, destacando los Bancos Comerciales en el cual más del 90% de estos lo realizan, al igual que la INDEL, en donde se indica que el 100% lo lleva a cabo; no obstante es importante analizar que en el caso de las Cooperativas se presenta como una oportunidad de mejora, ya que al no realizar una evaluación de riesgo, se pueden materializar amenazas que puedan llegar a perjudicar al cliente y a la propia institución.

Puesto que a raíz de la pandemia por covid-19 el lanzamiento de nuevos productos está relacionado con nuevas tecnologías o procesos y servicios digitales, y haciendo acotación a la ilustración N°6 en la cual se observa, que en el caso específico de las Cooperativas de Ahorro y Crédito el porcentaje de aumento por transacciones de manera digital se encuentra englobada entre el 0%-25%; de igual forma en los Bancos Estatales se aprecia un 0% de incremento en las operaciones digitales, en donde este último tiene 0% de creación de productos digitales, ya que de acuerdo al modelo de negocio de estas instituciones no se ve en la necesidad de crear tales canales, por consiguiente no se considera la elaboración de análisis de riesgo para estos servicios, como se visualiza en la ilustración N°7, se puede decir que el riesgo al cual se ha expuesto es bajo, por otro lado, el tipo de operativa de los Bancos Estatales es de segundo piso, lo cual básicamente su transacciones son con el Estado de Honduras o por medio de intermediarios como ser los Bancos Comerciales.

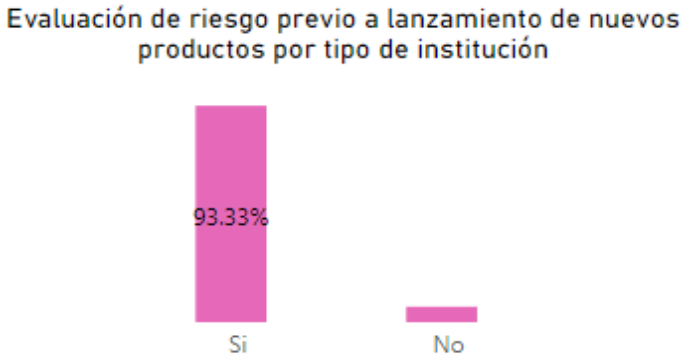


Gráfico N°1: Bancos Comerciales

Gráfico N°2: Cooperativas de Ahorro y Crédito

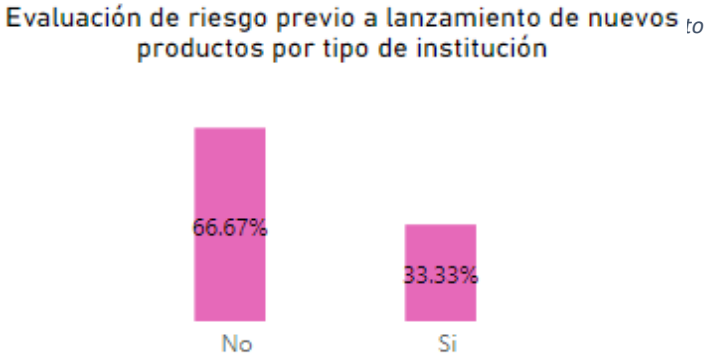


Gráfico N°3: Bancos Estatales

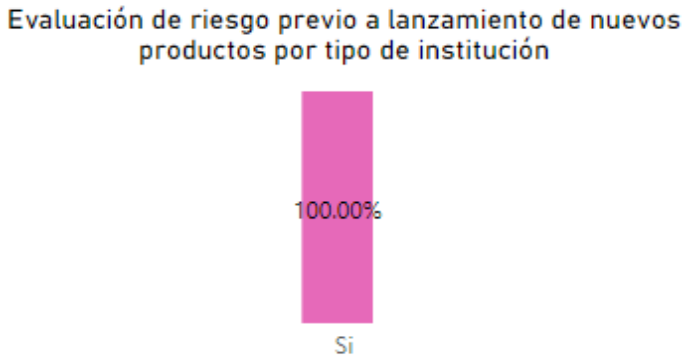


Gráfico N°4: INDEL

Conoce usted lo que es ciberdelito o delito cibernético y las prácticas asociadas al mismo

El 93% de las instituciones conocen el concepto de ciberdelito como se refleja en el gráfico N°4, de manera específica por tipo de institución, se refleja en la ilustración N°8, que en el caso de las Cooperativas de Ahorro y Crédito existe un 12% que no conoce este concepto, el cual puede traer consigo un riesgo debido a que al no conocer este concepto y al tener la implementación de nuevos productos digitales, la amenazas de un ataque a sus instituciones y la materialización del mismo incrementa exponencialmente.

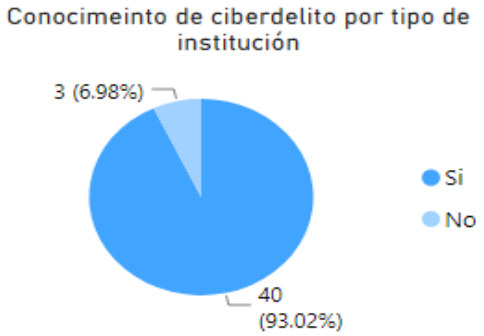


Gráfico 4:Conocimiento de Ciberdelito y sus prácticas asociadas

Gráfico N°1: Bancos Comerciales

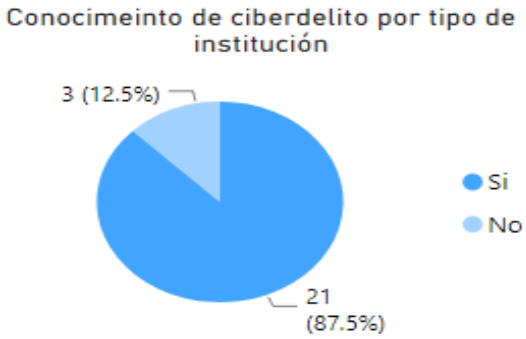


Gráfico N°2: Cooperativas de Ahorro y Crédito

Gráfico N°3: Bancos Estatales

Gráfico N°4: INDEL

Ilustración 8:Conocimiento acerca del Ciberdelito y sus prácticas asociadas

Por qué medio ha obtenido el conocimiento acerca del ciberdelito y sus prácticas asociadas

En el gráfico N°4 visto anteriormente se reflejó que al menos el 93% de las instituciones tiene el conocimiento de lo que es Ciberdelito, en la ilustración N°9 (gráfico N°1-gráfico N°4), se refleja de manera global los principales medios por los que el conocimiento fue adquirido, enfatizando los primeros tres; capacitación por parte de la institución, autocapacitación y boletines informativos, al igual por tipo de institución se reflejan los mismos tres aspectos como principales medios.

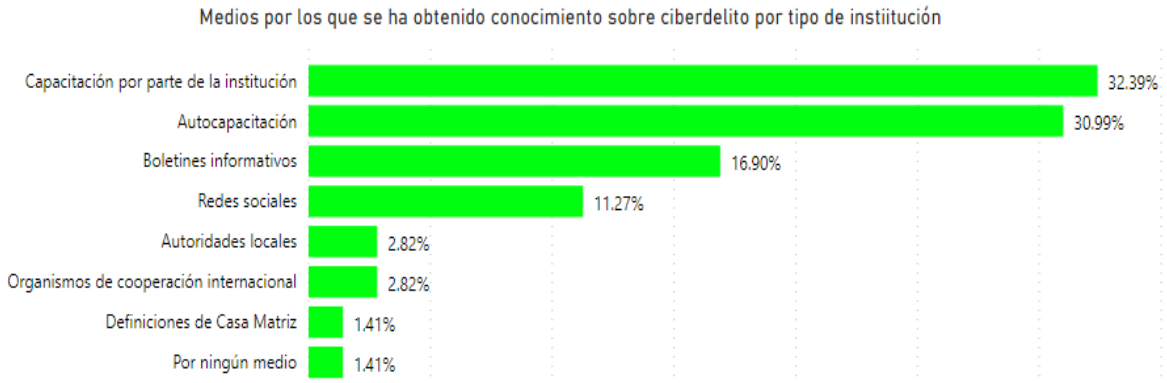


Gráfico N°4: Medios por los que se ha tenido conocimiento sobre ciberdelito

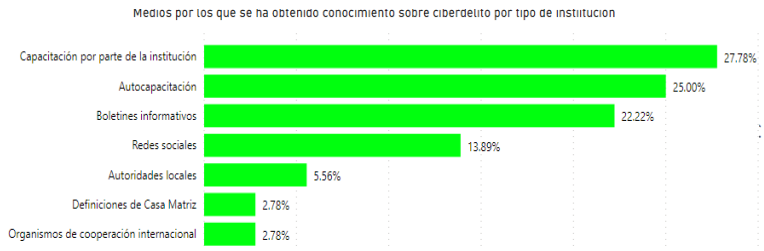


Gráfico N°1: Bancos Comerciales

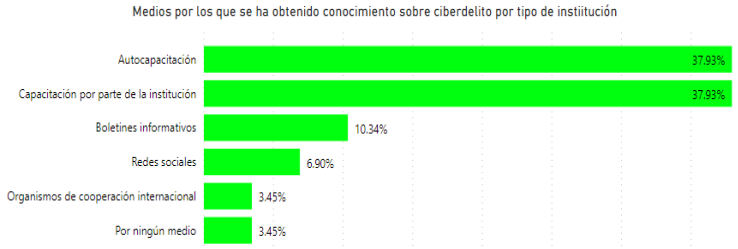


Gráfico N°2: Cooperativas de Ahorro y Crédito

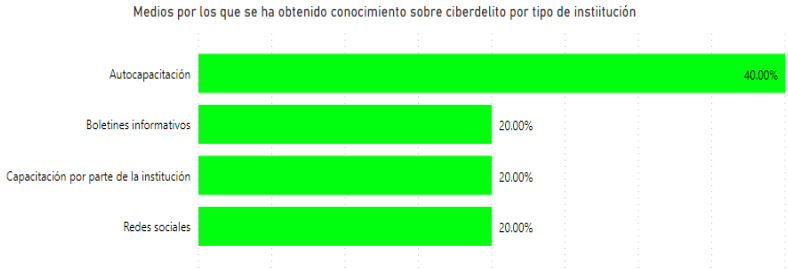


Gráfico N°3: Bancos Estatales

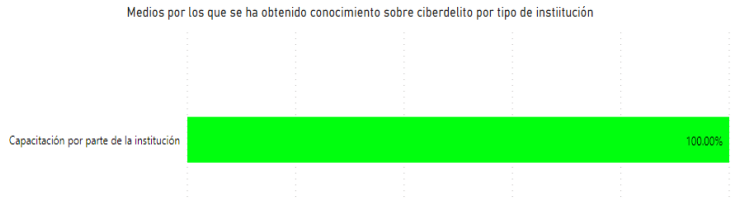


Gráfico N°4: INDEL

Ilustración 9:Medios por los cuales recibió el conocimiento de Ciberdelito

Frecuencia con la que ha recibido capacitación sobre Ciberdelito

En su conjunto se visualiza que la frecuencia que las instituciones reciben capacitación sobre Ciberdelito es 1 vez al año, tema que es de suma importancia que los colaboradores estén a la vanguardia, debido a las nuevas innovaciones tecnológicas que como consecuencia de la presente situación sanitaria que se atraviesa a nivel nacional producto de la pandemia por COVID-19, ha traído consigo la necesidad de llevar a cabo cambios en el modelo de trabajo, la seguridad de la información y el uso de nuevas herramientas tecnológicas para comunicación, ejecución y desarrollo de actividades.

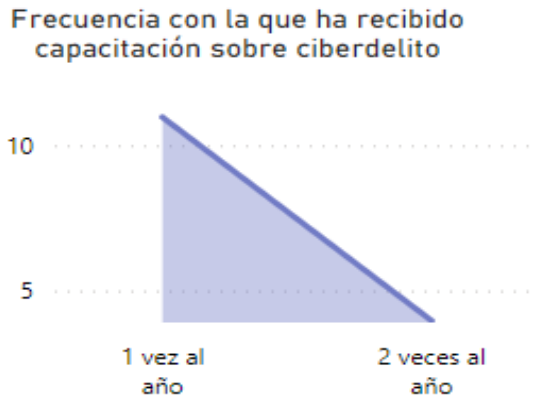


Gráfico N°1: Bancos Comerciales

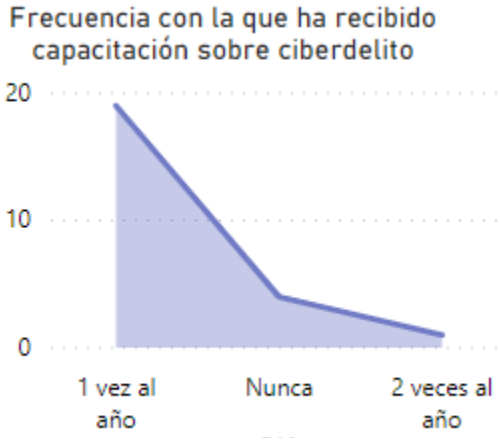


Gráfico N°2: Cooperativas de Ahorro y Crédito

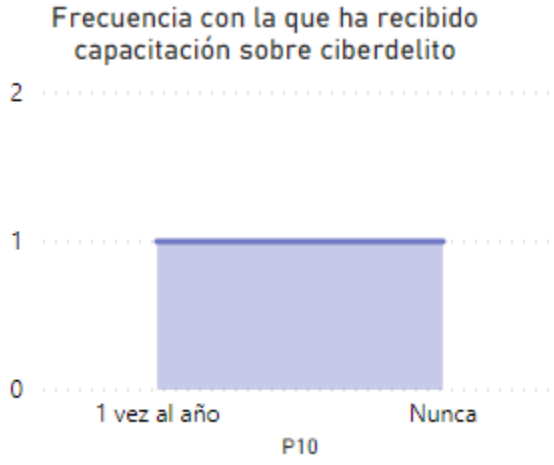


Gráfico N°3: Bancos Estatales

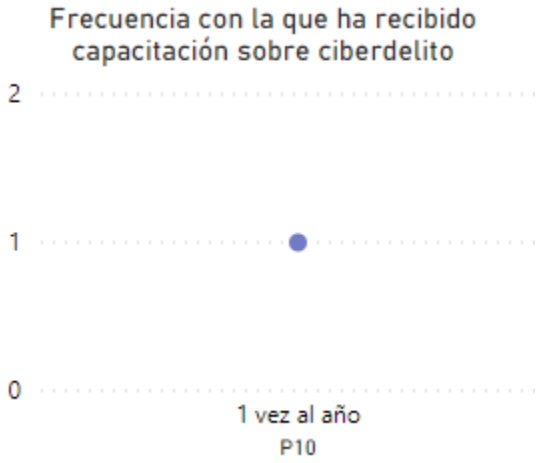


Gráfico N°4: INDEL

Conoce usted lo que es fraude y las prácticas asociadas al mismo

El conocimiento en materia de fraude de forma global es del 95%, como se refleja en el gráfico N°5, por tipo de institución como se aprecia en la ilustración N°10 (gráficos N°1-gráfico N°4), las Cooperativas de Ahorro y Crédito son las que presentan la oportunidad de mejora debido a que el 8% no conocen lo que es fraude y sus prácticas asociadas, situación que pone en vulnerabilidad y la posible materialización, así como un mecanismo de respuesta a posibles incidentes.

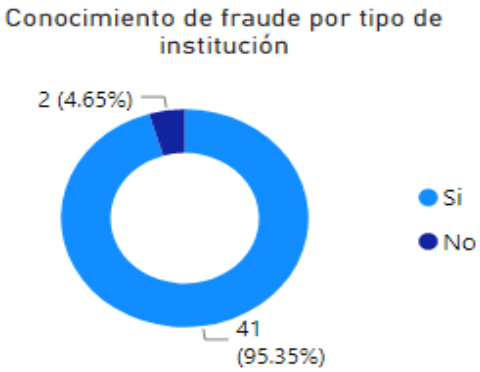


Gráfico 5: Conocimiento sobre Fraude

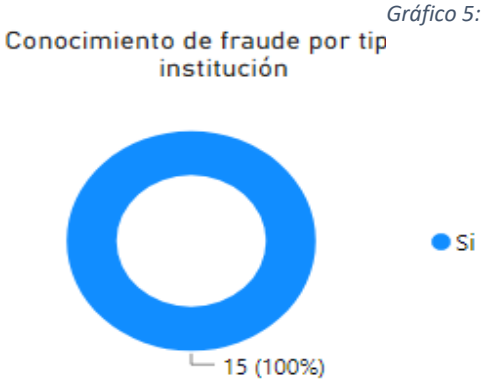


Gráfico N°1: Bancos Comerciales

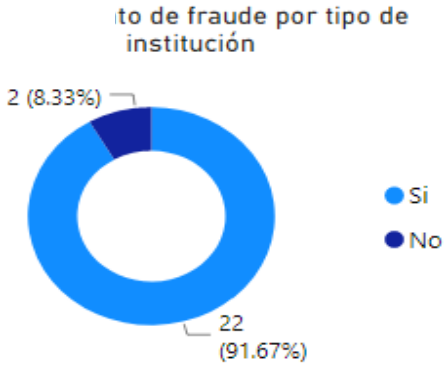


Gráfico N°2: Cooperativas de Ahorro y Crédito

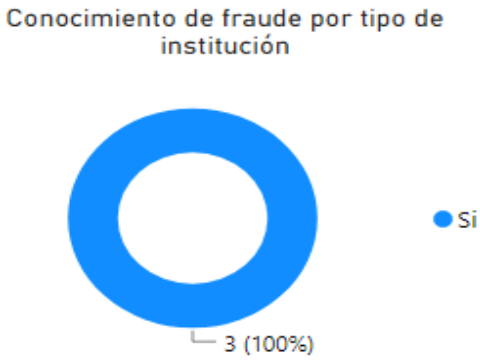


Gráfico N°3: Bancos Estatales

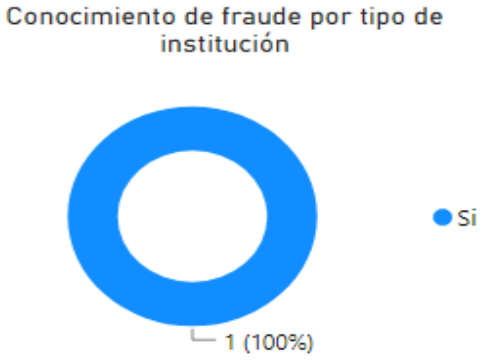


Gráfico N°4: INDEL

Ilustración 10:Conocimiento de Fraude y sus prácticas asociadas

Por qué medio ha obtenido el conocimiento acerca del fraude y sus prácticas asociadas

Como se observó en el gráfico N°6, el 95% de las instituciones tienen conocimiento sobre el concepto de fraude, en la ilustración N°11 (gráfico N°1-gráfico N°4) se presentan los medios por los cuales han recibido dicho conocimiento.

En su conjunto se registran que los principales medios por el cual se informan los colaboradores son; a través de capacitaciones por parte de la institución, seguidos de autocapacitación y boletines informativos, los cuales coinciden al analizarse de forma individual por cada tipo de institución.

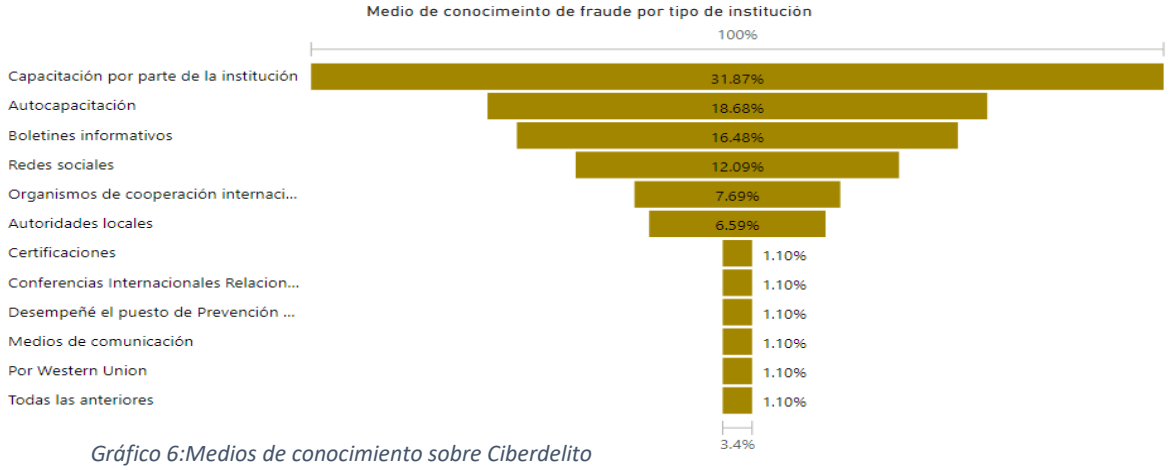


Gráfico 6:Medios de conocimiento sobre Ciberdelito

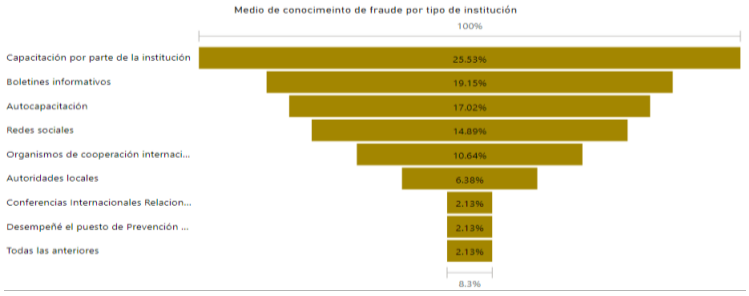


Gráfico N°1: Bancos Comerciales

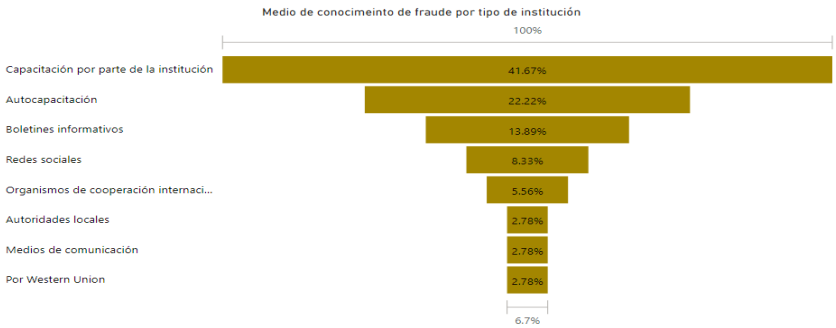


Gráfico N°2: Cooperativas de Ahorro y Crédito

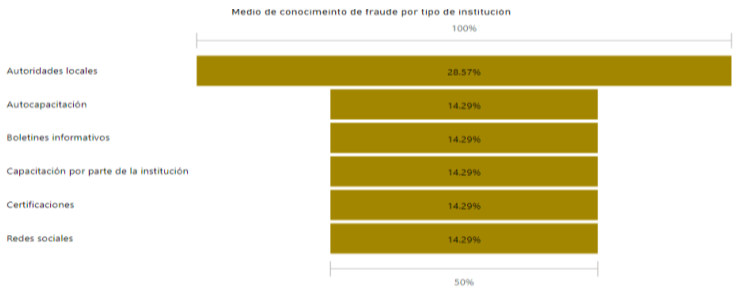


Gráfico N°3: Bancos Estatales

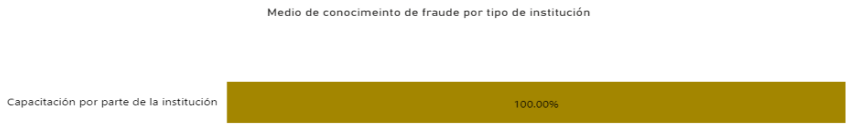


Gráfico N°4: INDEI

Ilustración 11:Medios por los que se recibió el conocimiento sobre Fraude

Qué tipo de prácticas fraudulentas conoce

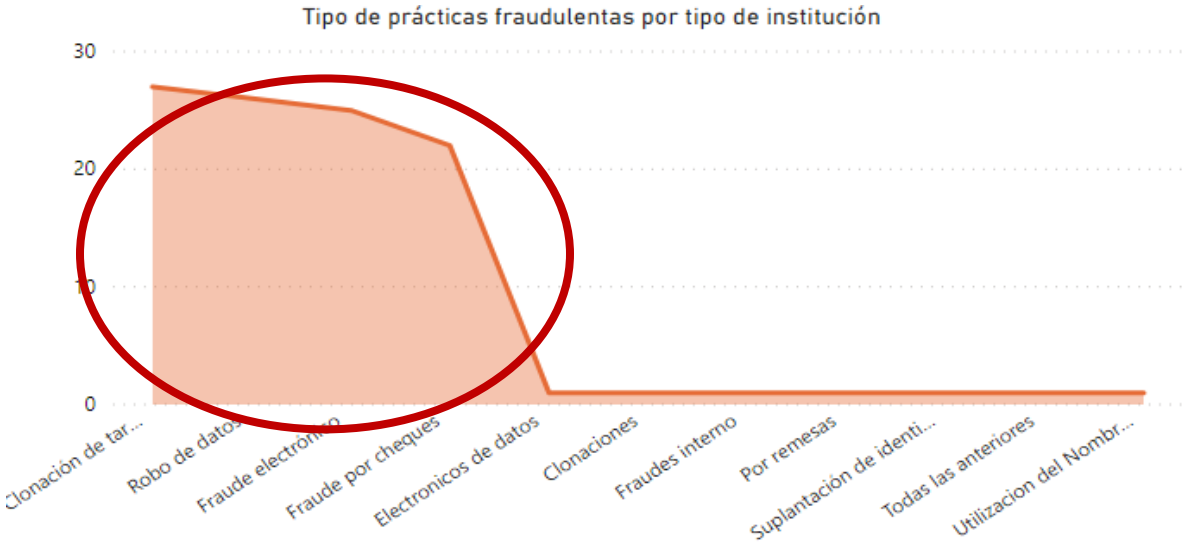


Gráfico 7: Tipo de prácticas fraudulentas

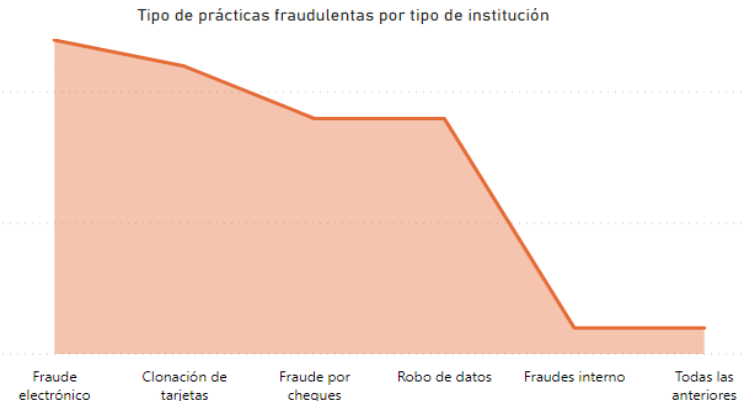


Gráfico N°1: Bancos Comerciales

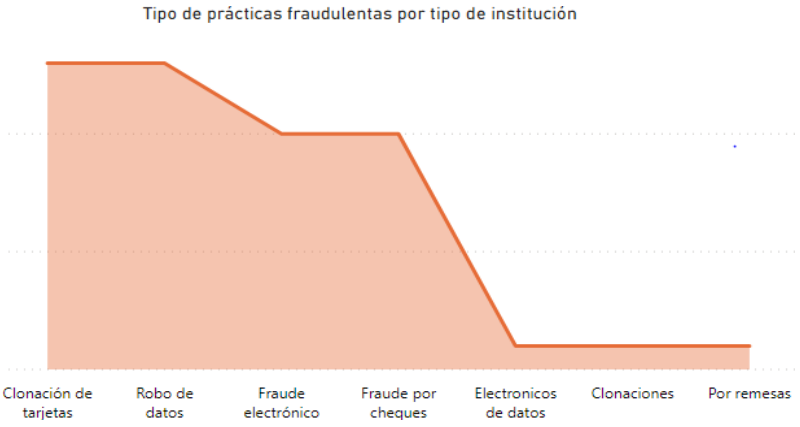


Gráfico N°2: Cooperativas de Ahorro y Crédito

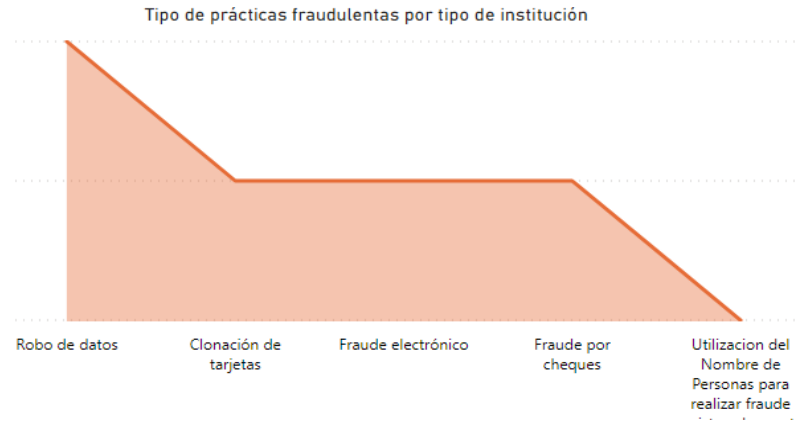


Gráfico N°3: Bancos Estatales

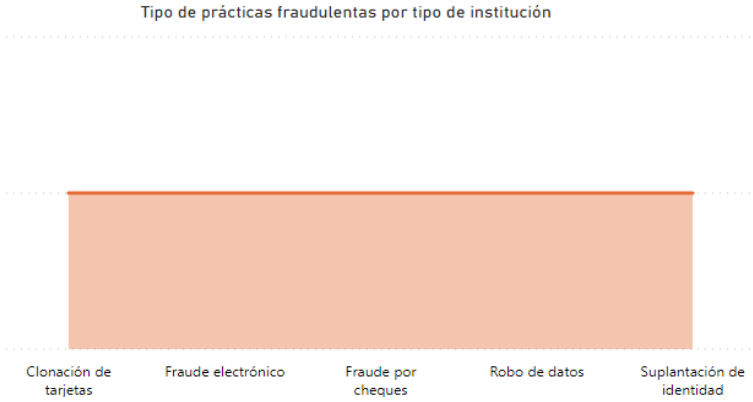


Gráfico N°4: INDEL

Ilustración 12: Tipo de prácticas fraudulentas

Dentro de las principales prácticas fraudulentas destacando de forma absoluta según la opinión de los Sujetos Obligados consultado a lo que se hace referencia en el gráfico N°7 son; clonación de tarjeta, fraude electrónico, robo de datos, fraude por cheques y electrónico de datos.

De forma particular por tipo de institución, las tres prácticas como denominador común son; clonación de tarjeta, robo de datos y fraude electrónico

Frecuencia con la que ha recibido capacitación en tema de Fraude

En su conjunto se visualiza que la frecuencia que las instituciones reciben capacitación en tema de fraude es 1 vez al año.

Gráfico N°1: Bancos Comerciales

Gráfico N°2: Cooperativas de Ahorro y Crédito

Gráfico N°3: Bancos Estatales

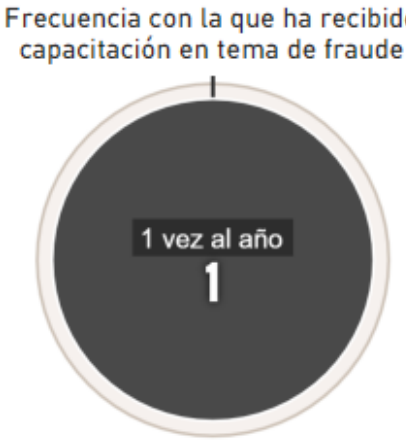
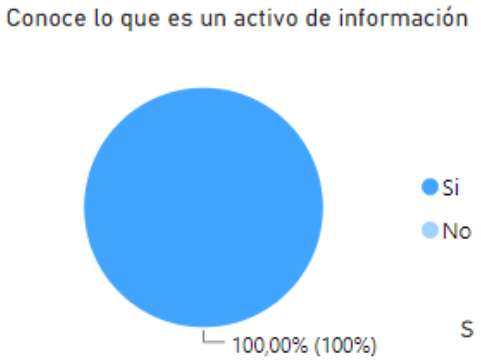


Gráfico N°4: INDEL

Conoce lo que es en activo de información

El 100% de los Sujetos Obligados indicaron conocer sobre el concepto de activo de información, lo que indica que las instituciones tienen conocimiento de la vulnerabilidad y gravedad del mal uso de este.



Los activos de información se encuentran clasificados de acuerdo con su criticidad en la organización

Las instituciones consideran que es importante clasificar los activos de información de acuerdo con su criticidad, pero llama la atención que aún hay instituciones que no los tiene clasificados, lo que podría repercutir en un riesgo en el futuro a ser víctimas de un ataque cibernético. Quienes representan el mayor porcentaje de instituciones que no clasifican su criticidad son las Cooperativas y los Bancos Estatales, factores que pueden jugar en su contra dado sobre todo en las Cooperativas por la cantidad de operaciones que realizan.

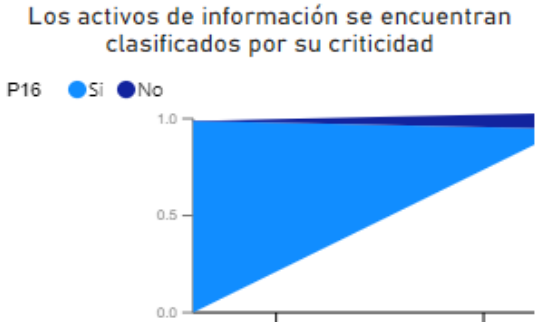


Gráfico N°1: Bancos Comerciales

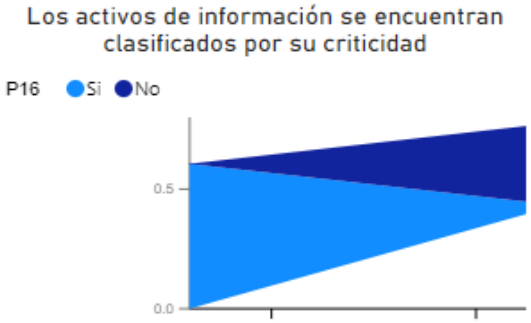


Gráfico N°2: Cooperativas de Ahorro y Crédito

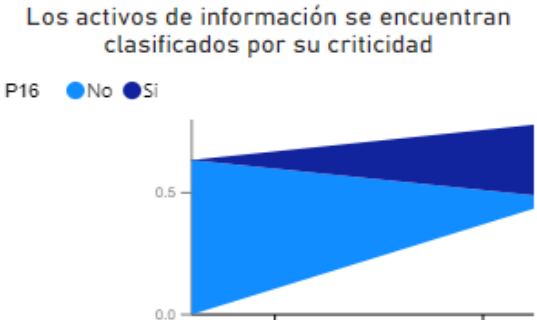


Gráfico N°3: Bancos Estatales

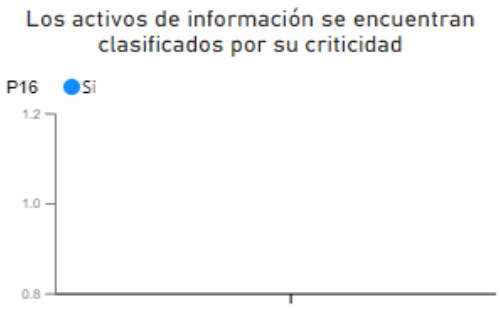


Gráfico N°4: INDEL

Es importante considerar que el crear y ofrecer productos digitales trae consigo ventajas como vulnerabilidades y amenazas, sin embargo, se puede tomar como un punto a favor el hecho que al menos 93% de los sectores reconoce el concepto de ciberdelito, y como se presenta en el gráfico N°8, 83.72% conoce de las amenazas con relación a los ataques cibernéticos, al igual en el gráfico N°9, donde el 84% distingue las vulnerabilidades; lo cual al concatenar los tres conocimientos puede facilitar la creación de estrategias que ayuden a minimizar las vulnerabilidades y amenazas.

El 16.28% que no conoce sobre las amenazas y el 16% no distingue las vulnerabilidades con relación a los ataques cibernéticos, está representada por el sector Cooperativo, lo cual indica una oportunidad para ampliar estos conocimientos dada la nueva realidad en la cual los procesos cada vez más están migrando de manera presencial a digital.

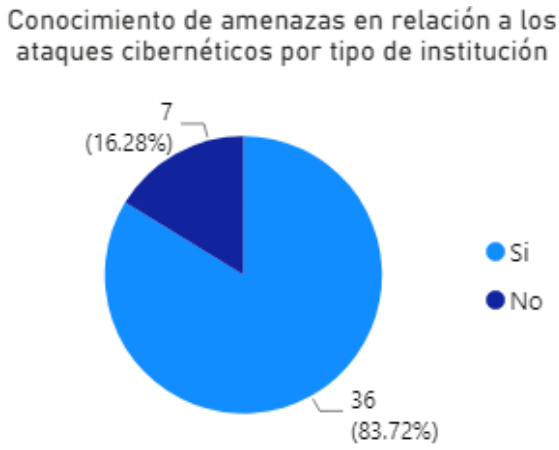


Gráfico 8:Conocimiento sobre las amenazas con relación a los ataques cibernéticos

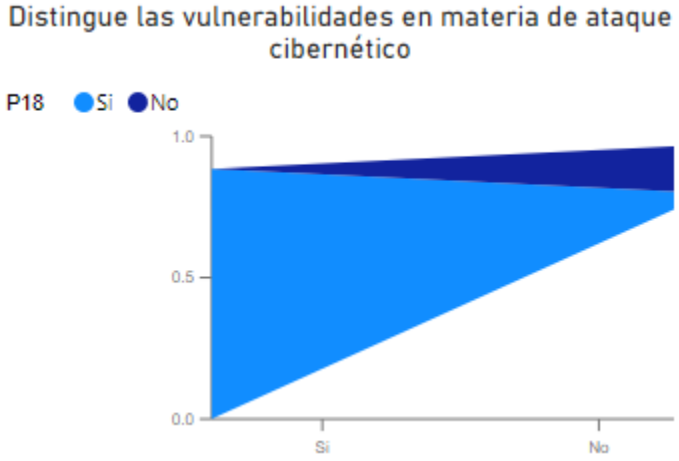


Gráfico 9: Vulnerabilidades en materia de ataque cibernético

<u>Su institución cuenta con un área encargada para reportar incidentes o sospechas de ataques cibernéticos</u>

Las instituciones manifestaron contar con un área encargada para reportar incidentes o sospechas de ataques cibernéticos, lo que ayuda a deducir que ya cuentan con políticas, procesos, procedimientos y planes de acción ante posibles ciberataques con el fin de proteger sus activos de información por el conocido “secreto profesional”.

Resulta imposible crear un entorno informático inaccesible a delincuentes informáticos, lo que sí se puede es constituir un entorno preventivo que dificulte el acceso a los hackers, incorporando medidas de buenas prácticas de detección dentro de la institución para la gestión de la fuga de información.

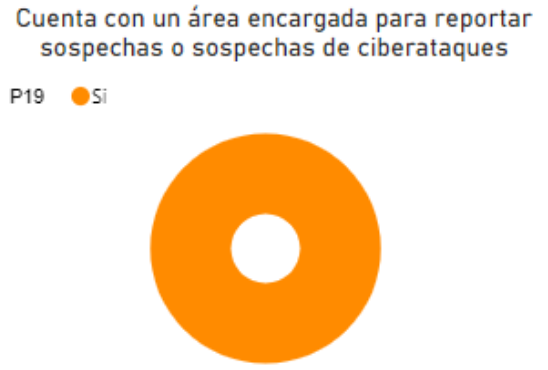


Gráfico N°1: Bancos Comerciales

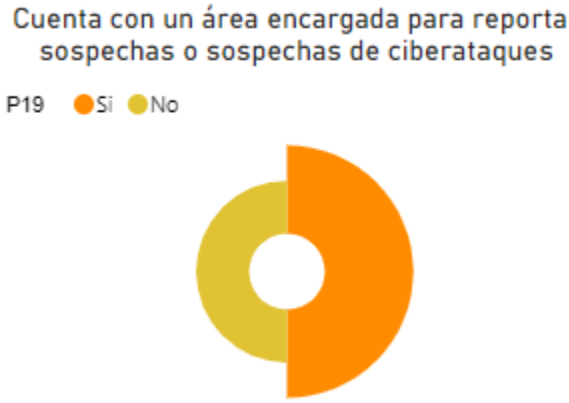


Gráfico N°2: Cooperativas de Ahorro y Crédito

Gráfico N°3: Bancos Estatales

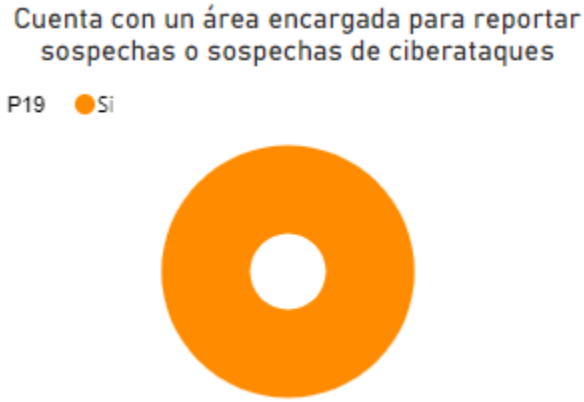
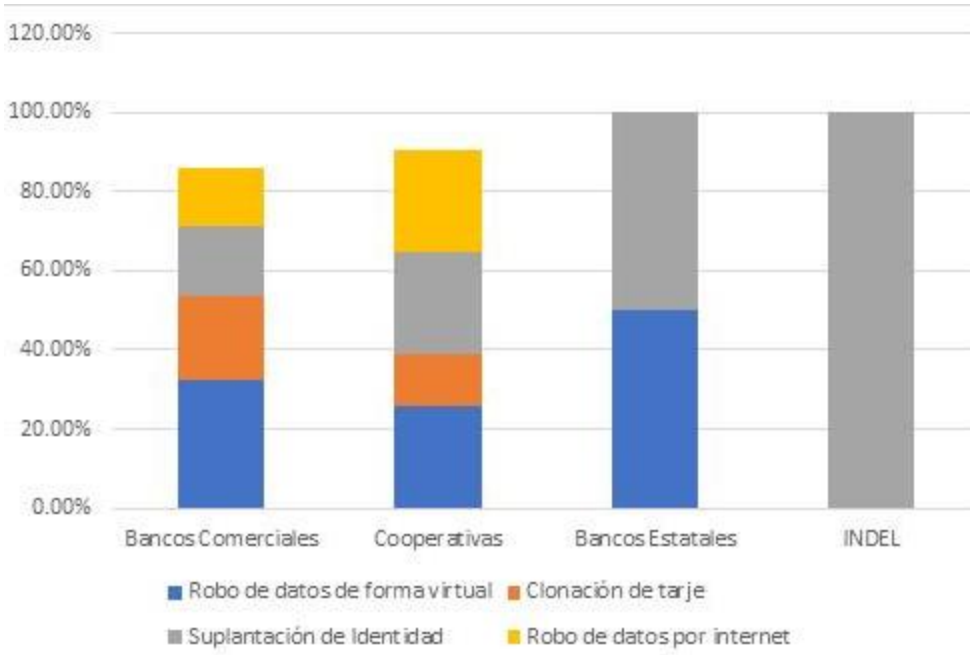


Gráfico N°4: INDEL

<u>El uso de canales digitales ha provocado un aumento de los delitos asociados a:</u>

Si bien es cierto los canales digitales han traído consigo muchos beneficios para las instituciones y los clientes/usuarios, pero a su vez la no relación cara a cara con el cliente provoca un aumento en los delitos ya que detrás de una computadora podría estar un delincuente robándose toda la información; en esta ocasión las instituciones indicaron identificar delitos como es el Robo de datos de forma virtual y la Suplantación de Identidad siendo estos los casos de delitos que más se les han presentado, siguiendo el Robo de datos por internet y la clonación de tarjetas.



Matriz de responsabilidad en los accesos de sus sistemas de información

De acuerdo con el análisis de los datos realizados, se identificó que las instituciones en un 86.67% cuentan con controles de seguridad para prevenir ataques cibernéticos en los accesos a sus sistemas de información, a excepción de la INDEL, lo que llama mucho la atención ya que por el rubro de negocio al que se dedican, podrían estar vulnerables a cualquier amenaza Cibernética.

A nivel de sector se identificó que las Cooperativas de Ahorro y Crédito, Bancos Estatales y la INDEL, mantienen un porcentaje representativo que indica que no cuentan con una matriz de responsabilidad en el acceso a sus sistemas de información; lo que a futuro aumenta el riesgo de no poder identificar posibles prácticas en el mal uso de la información con los datos de las operaciones financieras.

Gráfico N°1: Bancos Comerciales

Gráfico N°2: Cooperativas de Ahorro y Crédito

Gráfico N°3: Bancos Estatales

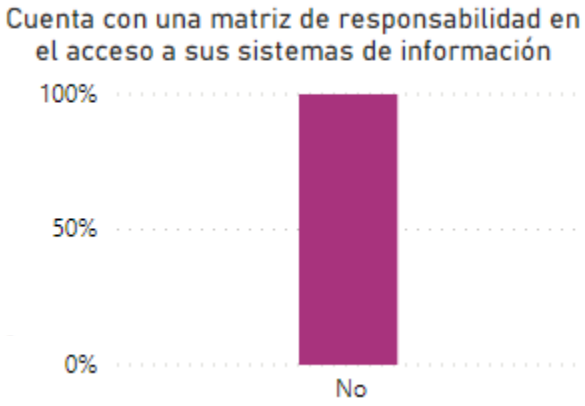


Gráfico N°4: INDEL

<u>Su institución cuenta con los siguientes controles de seguridad para prevenir los ataques cibernéticos</u>

Por las amenazas existentes resultado de la transformación digital, es necesario que todas las instituciones definan un control de seguridad para prevenir ataques cibernéticos, como se aprecia en la ilustración N°13, considerando los cuatro principales controles de manera general se obtienen; restricción de los privilegios administrativos, restricción de instalación de aplicaciones por parte de los usuarios, actualización constante de los sistemas o aplicaciones y el back up de la información.

De manera específica por cada sector como se muestra en la imagen N°14 (gráfico N°1-gráfico N°4), resaltan los mismos controles, si bien es cierto en diferente porcentaje, pero finalmente, los controles antes en mención.

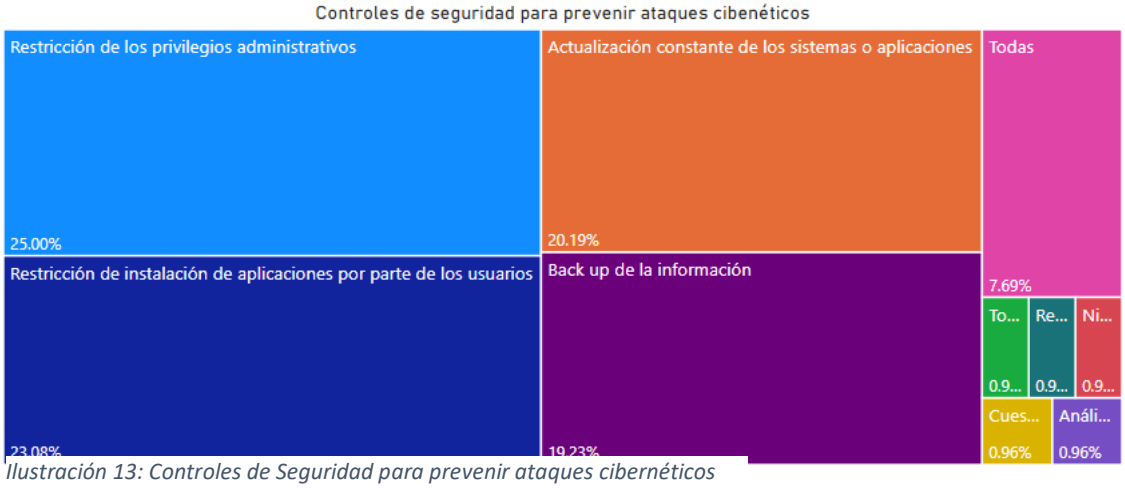


Ilustración 13: Controles de Seguridad para prevenir ataques cibernéticos

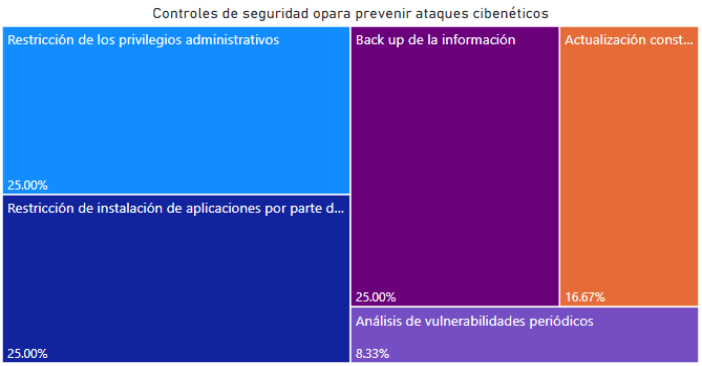


Figura N°1: Bancos Comerciales

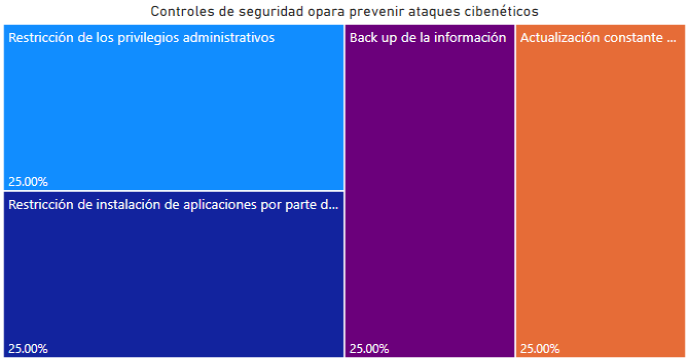


Figura N°2: Cooperativas de Ahorro y Crédito

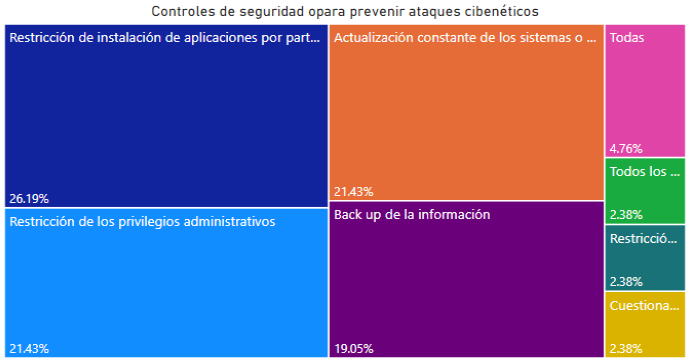


Figura N°3: Bancos Estatales

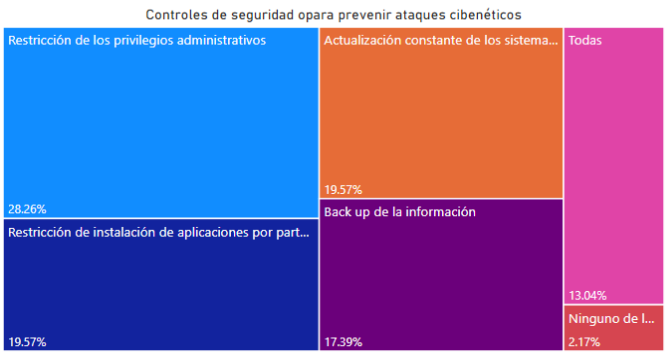


Figura N°4: INDEL

Ilustración 14:Controles de Seguridad para prevenir ataques cibernéticos

Su institución realiza campañas de sensibilización para los usuarios financieros sobre delitos cibernéticos y/o fraude

Además de los controles internos que las instituciones deben tener para la prevención de ciberdelitos y fraude, no se debe perder de vista la comunicación a nivel de clientes ya que en muchos de estos delitos fueron materializados por el desconocimiento del cliente.

De acuerdo con el gráfico N°9 se obtiene que más del 60% de los sectores realizan campañas de sensibilización.

De manera particular por cada uno de los sectores en la ilustración N°15 (gráfico N°1-gráfico N°4), se logra apreciar que las Cooperativas de Ahorro y Crédito presentan una considerable oportunidad de mejora, esto debido a que únicamente el 37% de las mismas realizan campañas; en el caso de los Bancos Estatales, aunque se observa un porcentaje considerable de no sensibilización se entiende que estos tienen servicio de intermediación con los Bancos Comerciales y no directamente con usuarios.

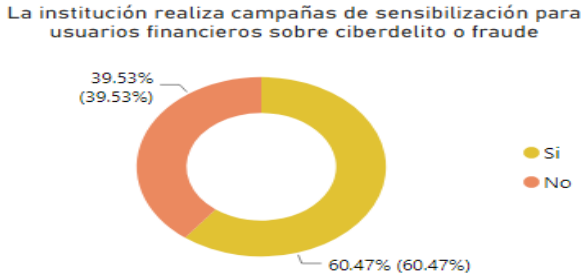


Gráfico 10: Campaña de sensibilización para usuarios financieros sobre Ciberdelito o Fraude

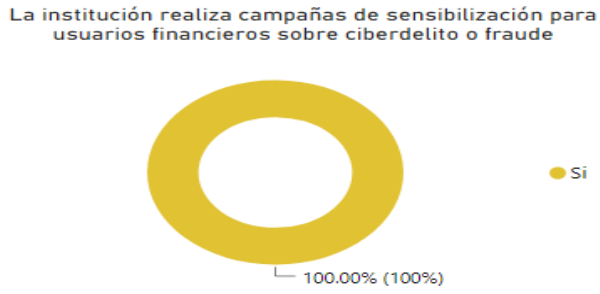


Gráfico N°1: Bancos Comerciales

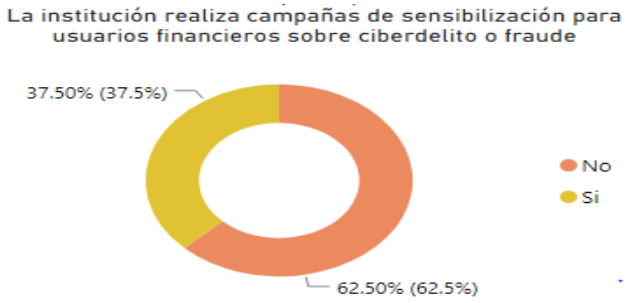


Gráfico N°2: Cooperativas de Ahorro y Crédito

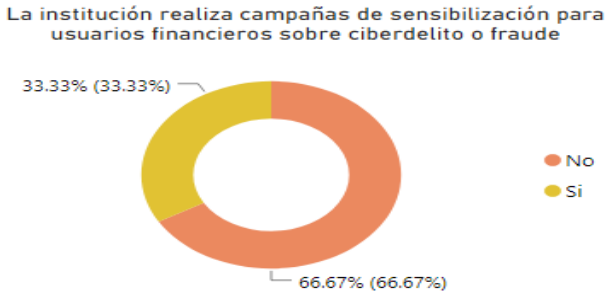


Gráfico N°3: Bancos Estatales

Gráfico N°4: INDEL

Ilustración 15:Campañas de sensibilización sobre temas de Ciberdelito y Fraude

Los medios que la institución utiliza para las campañas de sensibilización son:

Considerando aquellos sectores en los cuales, si se realizan campañas de sensibilización, en la ilustración N°16 de manera general se muestra los medios por los cuales se dan a conocer las diversas campañas, siendo las páginas web y el correo electrónico los mayores medios; con 23.26% del total se denota la opción "ninguna" dato que por el porcentaje no se puede discriminar, sin embargo, este valor refiere a aquellas instituciones que no realizan campañas de sensibilización, situación que puede dejar en vulnerabilidad a la institución debido a que el desconocimiento del cliente, puede darle ventaja a los ciberdelincuentes o defraudadores.

Particularmente en la ilustración N°17(ilustración N°1-ilustración N°4) se contempla por tipo de institución que el 23.26% de "ninguno" esta contenido en las Cooperativas de Ahorro y Crédito y en los Bancos Estatales, dato que de igual forma se valida en la ilustración N°15.

Ilustración 16:Medios que la institución utiliza para campañas de sensibilización

Figura N°1: Bancos Comerciales

Figura N°2: Cooperativas de Ahorro y Crédito

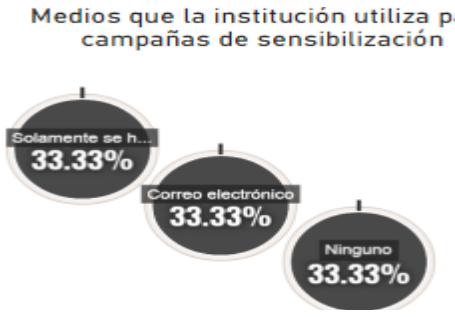


Figura N°3: Bancos Estatales

Figura N°4: INDEL

Ilu *las campañas*

Cuáles son los medios por los que se puede detectar un evento de ciberataque o fraude

Primordialmente los medios que se utilizan para la detección de posibles ataques cibernéticos o fraude son; reclamo por parte del cliente, a través de sistemas de alerta y monitoreo aleatorio de transacciones, como se muestra en el grafico N°11. Por sector de forma individual se obtiene que los medios son los mismos, como se refleja en la ilustración N°18 (gráfico N°1-gráfico N°4).

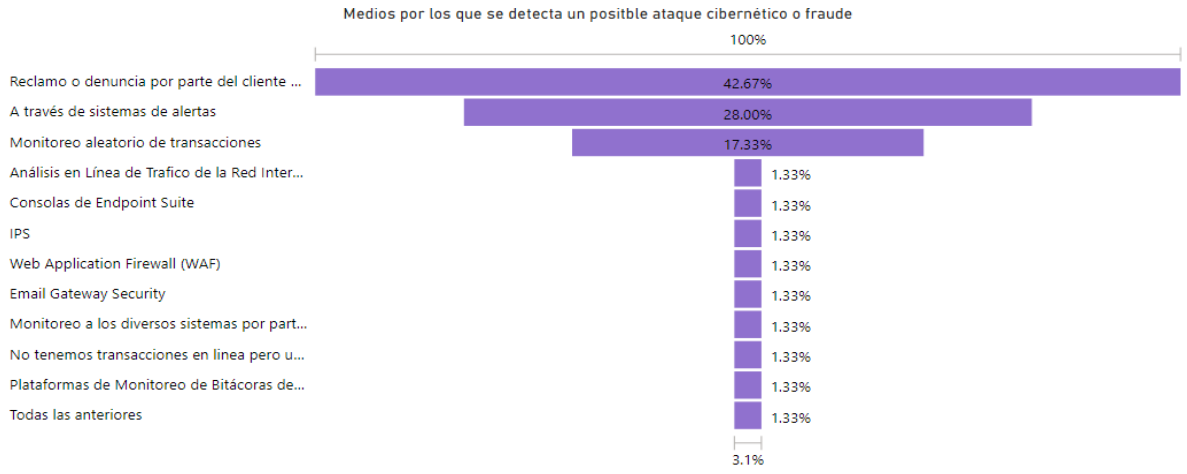


Gráfico 11:Medios por los que se detecta un posible ataque Cibernético o Fraude

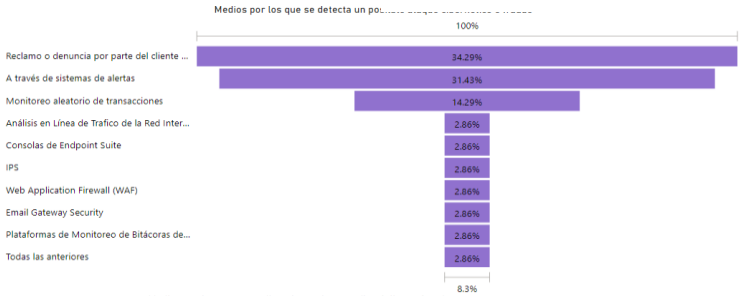


Gráfico N°1: Bancos Comerciales

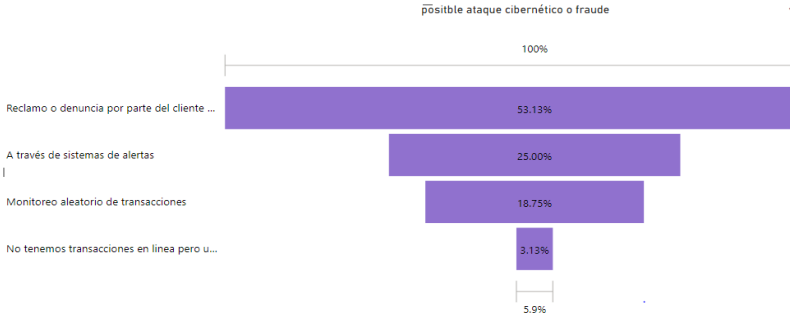


Gráfico N°2: Cooperativas de Ahorro y Crédito

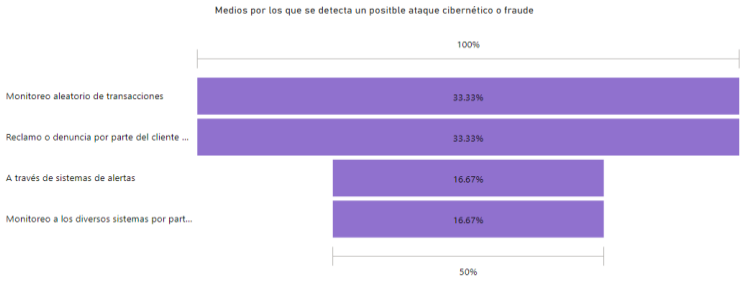


Gráfico N°3: Bancos Estatales

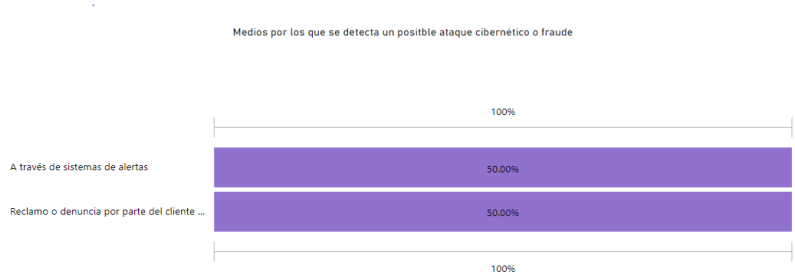


Gráfico N°4: INDEL

Ilustración 18: Medio por los que se detecta un posible ataque Cibernético o Fraude

En caso de que llegue a materializar un ataque cibernético se reporta a:

Aun y cuando las instituciones mantienen sus sistemas de monitoreo y control para prevenir ataques cibernéticos o fraudes como se mencionó en los medios por lo que se detecta un posible ataque reflejado en la ilustración N°19 (gráfico N°1-gráfico N°4). Existen ocasiones en las cuales se puede llegar a materializar, es por ellos que en el gráfico N°12 se presentan las áreas a las cuales se reportan en caso de que un incidente llegue a ocurrir, dentro de las principales se encuentran; área de tecnología de la información, comité de seguridad de la información.

Por tipo de institución o sector, se aprecia las mismas áreas, aunque en diferentes posiciones, son área de tecnología de la información, comité de seguridad de la información a las que se realizan principalmente los reportes.

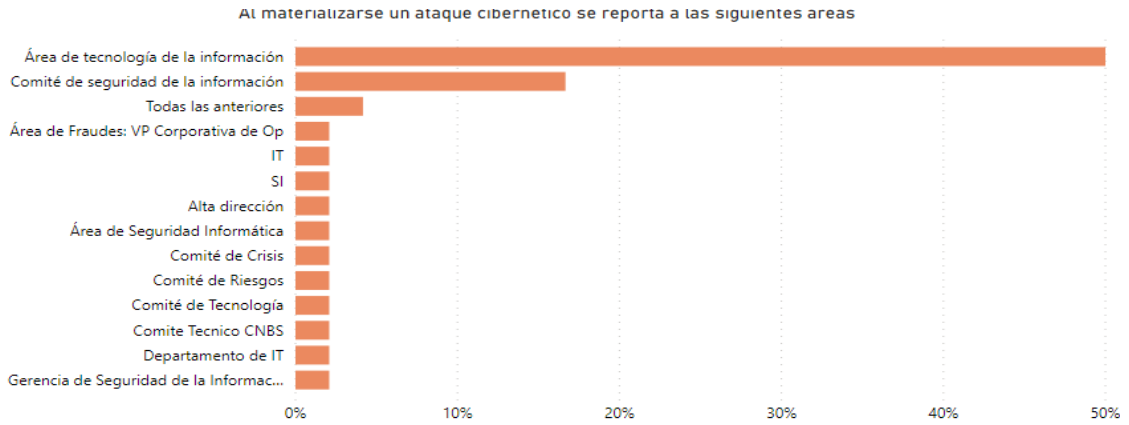


Gráfico 12: Al materializarse un ataque cibernético se reporta a:

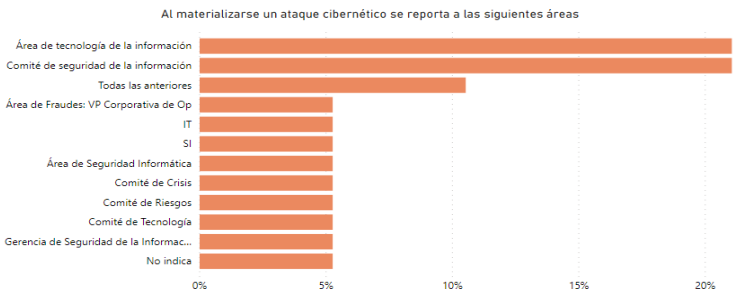


Gráfico N°1: Bancos Comerciales

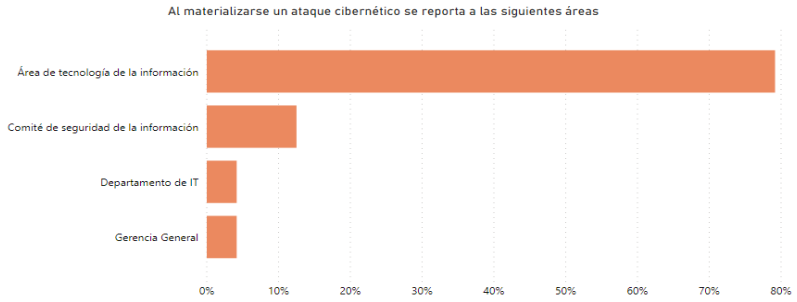


Gráfico N°2: Cooperativas de Ahorro y Crédito

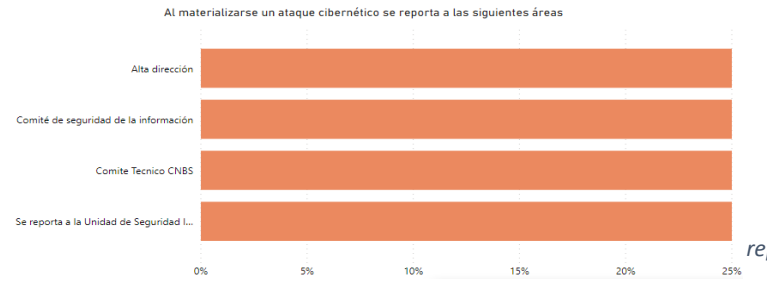


Gráfico N°3: Bancos Estatales

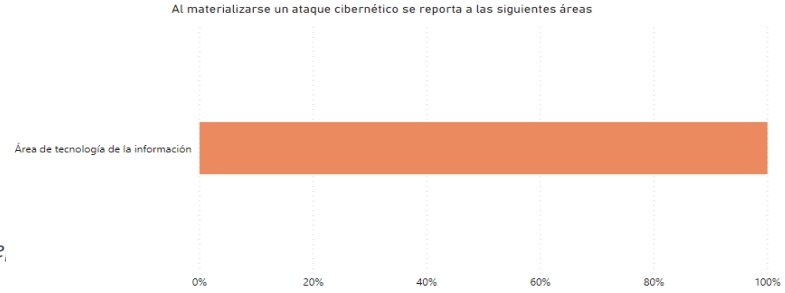


Gráfico N°4: INDEL

Su institución cuenta con un reglamento sancionatorio en caso de que por negligencia se llegara a materializar un ataque cibernético

Las instituciones financieras en un 84% cuentan con un reglamento sancionatorio en caso de que por negligencia se llegara a materializar un ataque cibernético a excepción de la INDEL, situación que puede llegar a perjudicar exponencialmente a la institución debido a que, al no contar con un reglamento, no se aducen las responsabilidades y la materialización de los ataques por negligencia pueden ser recurrentes.

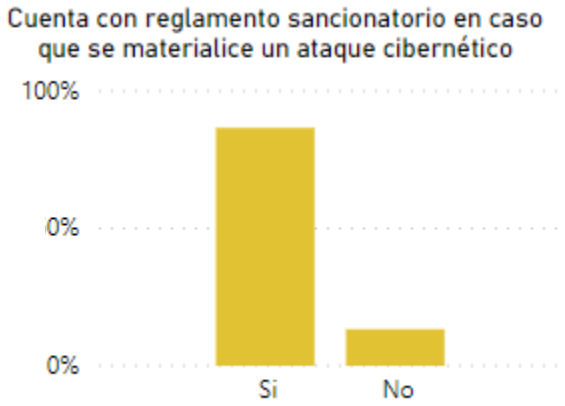


Gráfico N°1: Bancos Comerciales

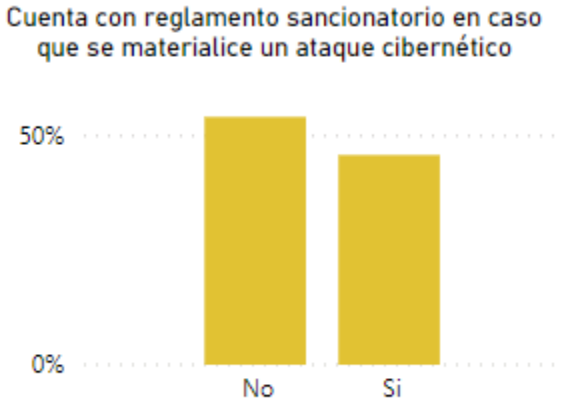


Gráfico N°2: Cooperativas de Ahorro y Crédito

Gráfico N°3: Bancos Estatales

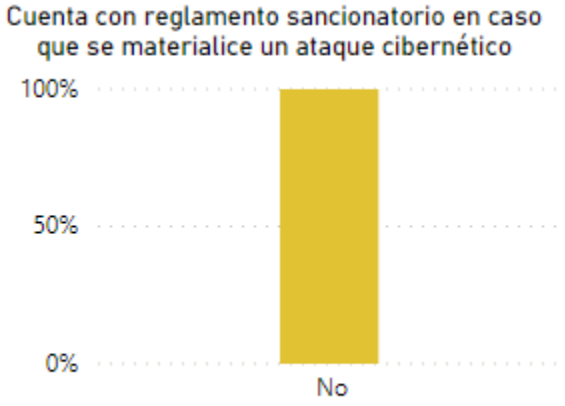


Gráfico N°4: INDEL

Por parte de qué clientes recibe la mayor cantidad de denuncias por ciberataque o fraude

Con relación al tipo de persona que realiza el mayor porcentaje de denuncia respecto a ciberataque o fraude son las personas naturales como se observa en la ilustración N°20 (imagen N°1-imagen N°4), el porcentaje que hace referencia a "ninguno" es porque en ciertas instituciones no se han detectado este tipo de incidentes.

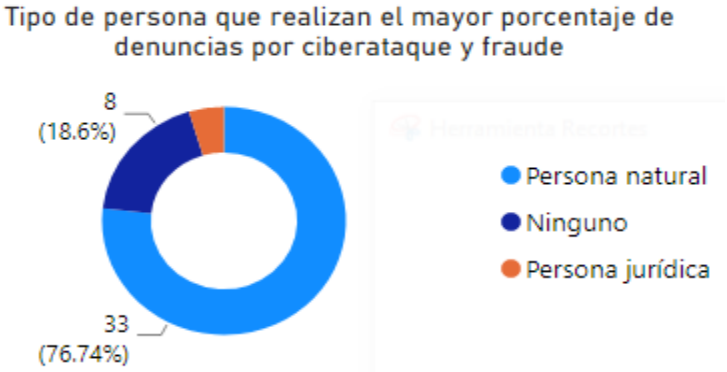


Gráfico 13:Tipo de persona que realiza el mayor porcentaje de denuncias por Ciberataque y Fraude

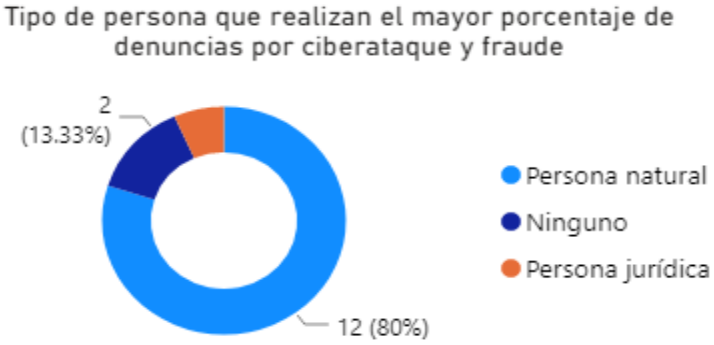


Gráfico N°1: Bancos Comerciales

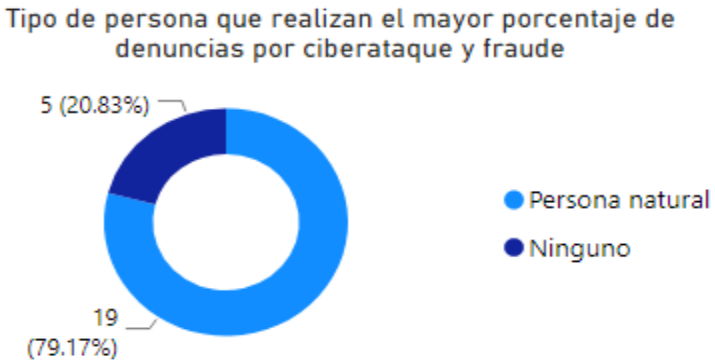


Gráfico N°2: Cooperativas de Ahorro y Crédito

Gráfico N°3: Bancos Estatales

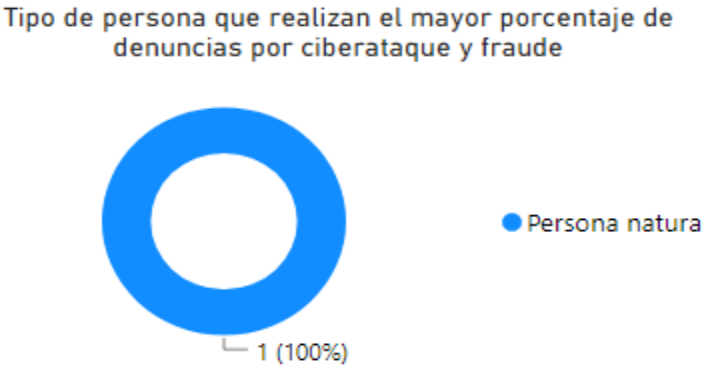


Gráfico N°4: INDEL

Ilustración 20:Tipo de persona que realiza el mayor porcentaje de denuncias por Ciberataque y Fraude

Cuáles son los medios por los que se puede detectar un posible evento de ciberataque o fraude

Los medios por los cuales se recibe una denuncia por ciberdelito o fraude en su conjunto son; de manera presencial, correo electrónico y llamada telefónica como se presenta en el gráfico N°14.

Al igual por cada sector en la ilustración N°21 (gráfico N°1-gráfico N°4) se visualiza sobre todo en los Bancos, Cooperativas de Ahorro y Crédito y en la INDEL los mismos medios que se presentaron en la gráfica anterior, en cuanto a los Bancos Estatales inicialmente se realiza comunicación interna al oficial de atención al usuario financiero. Cabe destacar que en un menor porcentaje se presenta instituciones en las cuales no se ha dado denuncias por ciberdelito o fraude ya que no se ha recibido ataques de este tipo.

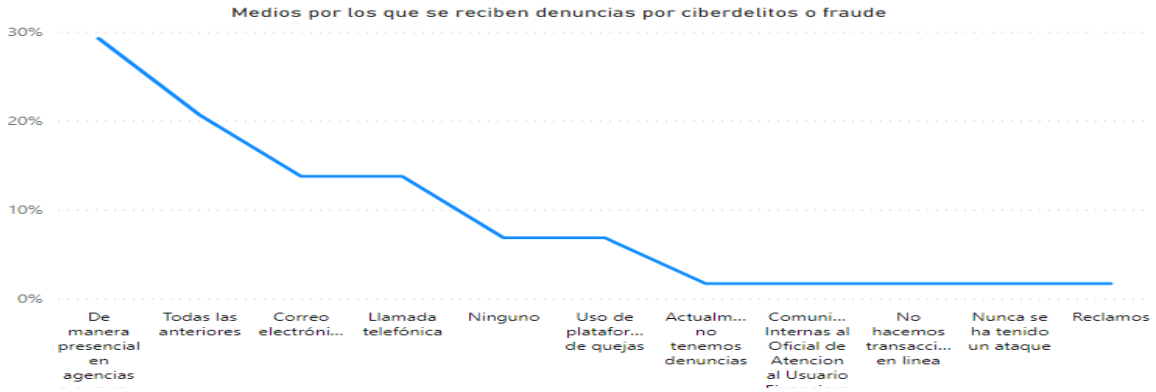


Gráfico 14:Medios por los que se detectan eventos de Ciberataque o Fraude

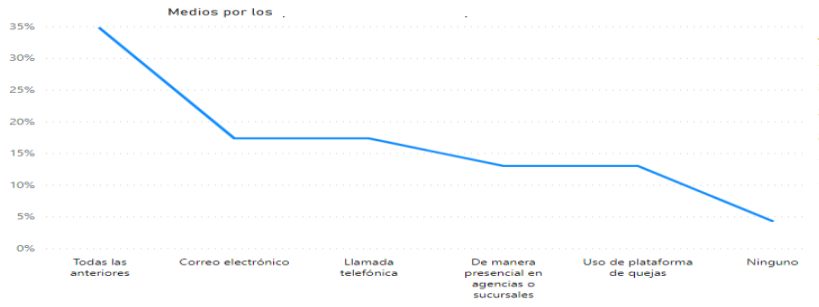


Gráfico N°1: Bancos Comerciales

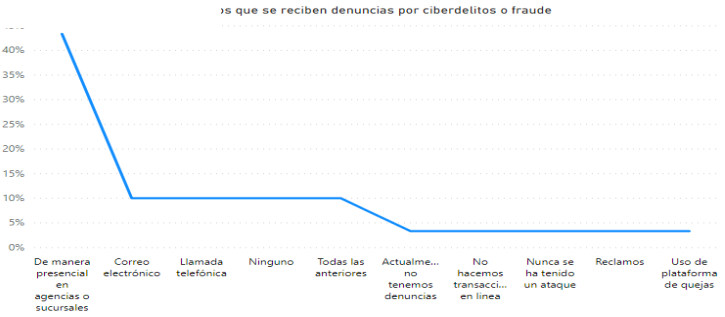


Gráfico N°2: Cooperativas de Ahorro y Crédito

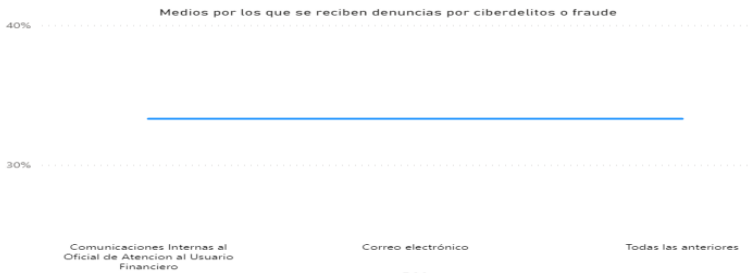


Gráfico N°3: Bancos Estatales

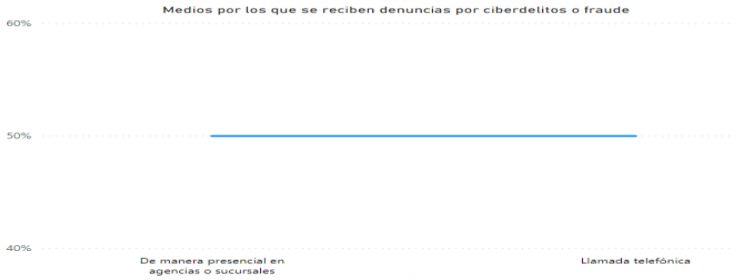


Gráfico N°4: INDEL

Ilustración 21:Medios por los que se detectan eventos de Ciberataque o Fraude

Si la detección por Ciberdelito o Fraude fue por parte de la institución, porque medio le informa al cliente

De acuerdo con los datos presentados en los gráficos una vez que las instituciones identifican Ciberdelito o Fraude la comunicación con el cliente es mediante vía telefónica y presencial, siendo el primero el mayor rango de porcentaje.

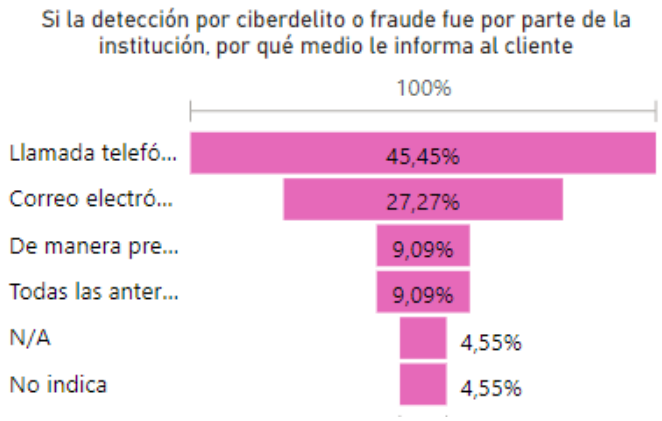


Gráfico N°1: Bancos Comerciales

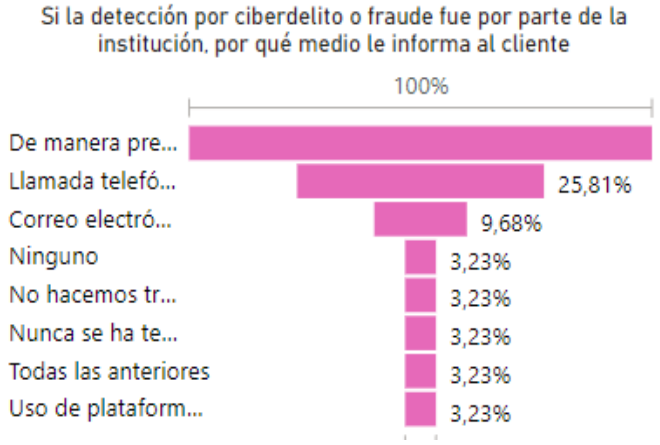


Gráfico N°2: Cooperativas de Ahorro y Crédito

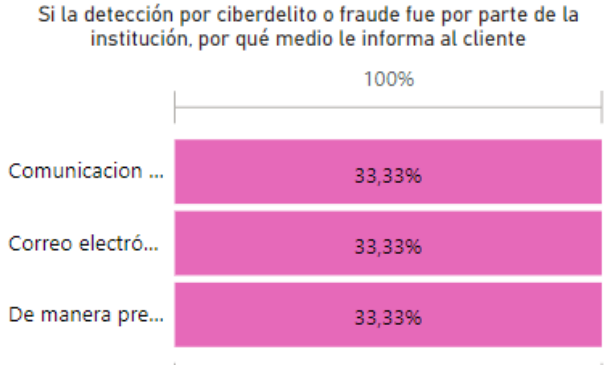


Gráfico N°3: Bancos Estatales

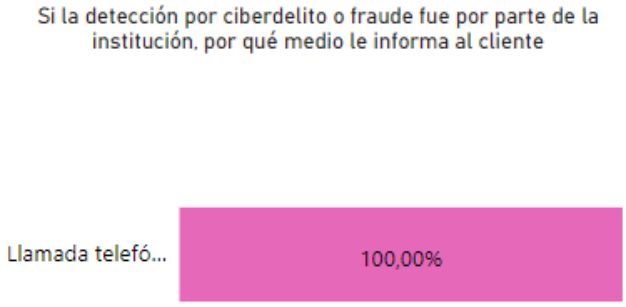


Gráfico N°4: INDEL

Qué cantidad de reclamos relacionado a ciberdelito y fraude recibe al año

La materialización de un ciberataque o fraude siempre es una amenaza latente ya que los infractores siempre están en la búsqueda de víctimas y creando nuevos métodos para llevar a cabo sus fechorías, en ese sentido, en el gráfico N°15 se refleja la cantidad de reclamos por ciberdelito o fraude que se han presentado, concentrándose en 53.49% de reclamos en un rango de 1-25 reclamos de manera global, seguido por 16.28% de reclamos en un rango mayor a 100 reclamos, es importante recalcar que destaca con 18.60% “ninguno” reclamo, esto se debe a que en ciertas instituciones no se han presentado ningún tipo de reclamo referente a estos delitos.

De forma específica por cada sector, se aprecia que los Bancos Comerciales (gráfico N°1) y la INDEL (gráfico N°4) son las que presenta el mayor porcentaje en cantidad de quejas, siendo de un 40%-100% en un rango de reclamos de 100 en adelante, el cual es consecuente debido a la cantidad de operaciones que llevan a cabo estos dos sectores y por el tipo de productos y servicios brindados.

En cuanto a las Cooperativas de Ahorro y Crédito (gráfico N°2) y los Bancos Estatales (gráfico N°3), se obtienen porcentaje de 33%-70% en el cual la concentración de quejas oscila entre 1-25 reclamos, rangos que están acorde al tamaños, giro y cantidad de transacciones de estos sectores.

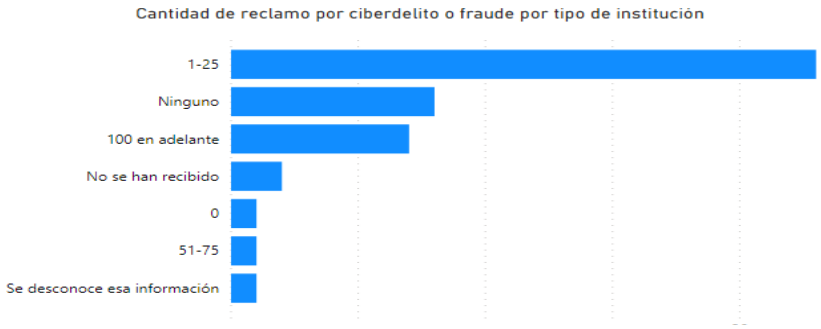


Gráfico 15:Cantidad de reclamos por Ciberdelito o Fraude

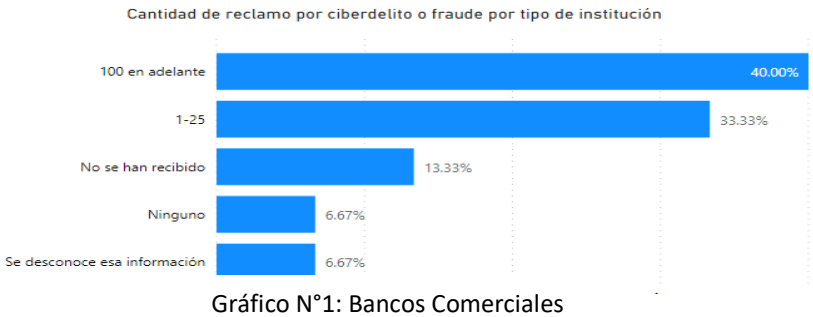


Gráfico N°1: Bancos Comerciales

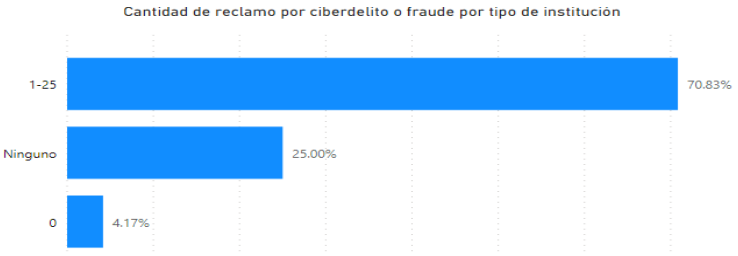


Gráfico N°2: Cooperativas de Ahorro y Crédito

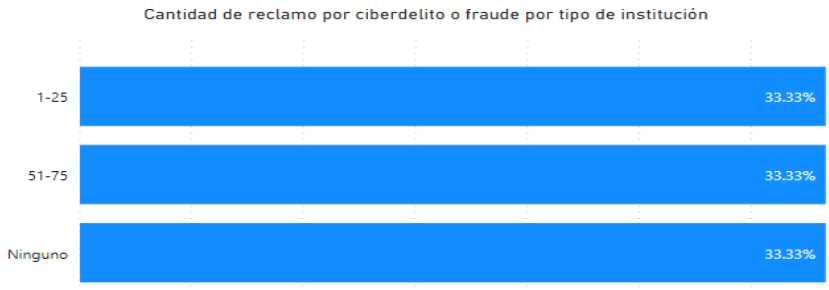


Gráfico N°3: Bancos Estatales

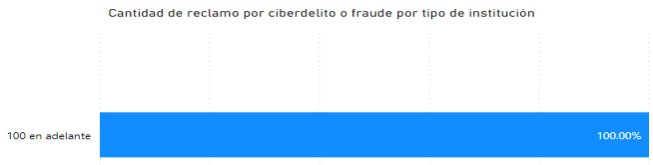


Gráfico N°4: INDEL

Ilustración 22:Cantidad de reclamos por Ciberdelito o Fraude

Rangos monetarios (lempiras) estima el impacto o pérdida operativa de estos delitos para su institución

Las instituciones consideran en un rango mayor de L 1,000,000.00 las pérdidas estimadas por delitos cibernéticos y/o fraude, exceptuando a las Cooperativas con un monto menor de L10,000.00.

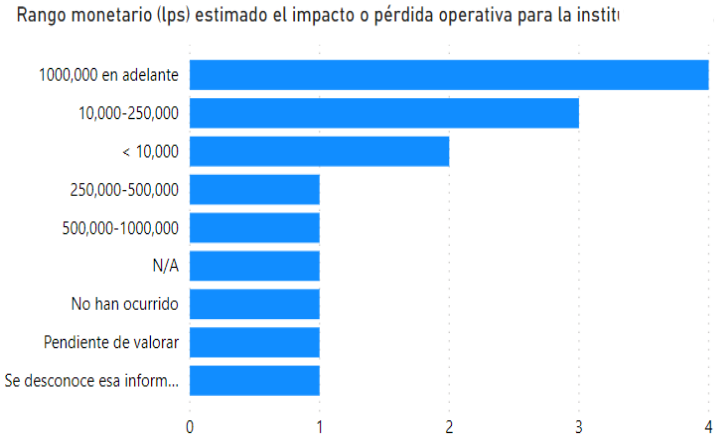


Gráfico N°1: Bancos Comerciales

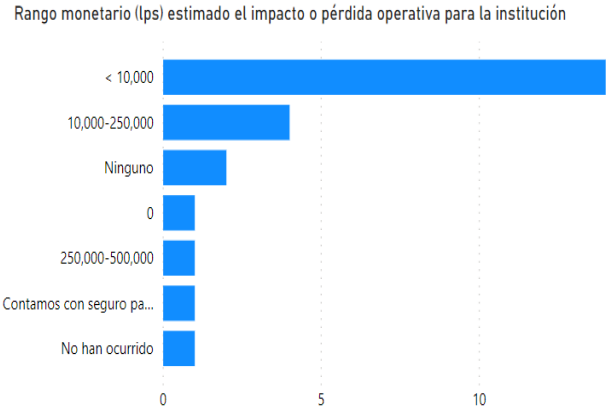


Gráfico N°2: Cooperativas de Ahorro y Crédito

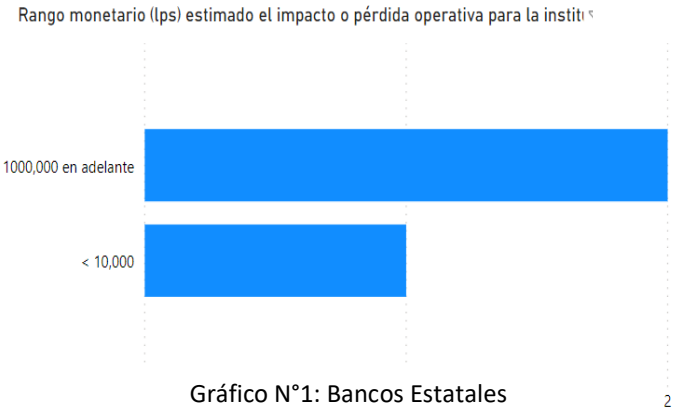


Gráfico N°1: Bancos Estatales

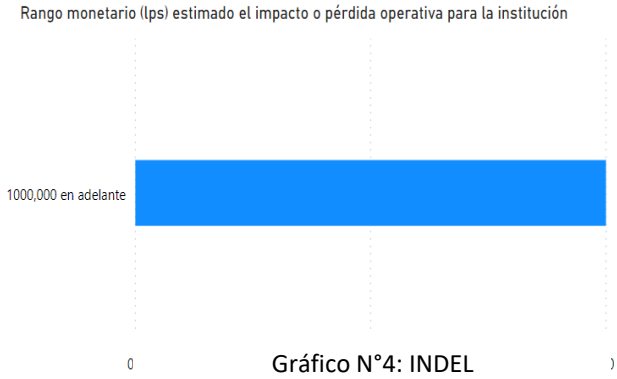


Gráfico N°4: INDEL

Zona geográfica del país en donde se presentan más denuncias y quejas

Según lo manifestado por las instituciones la zona Norte y Centro es donde reciben la mayor cantidad de denuncias sobre delitos cibernéticos y/o fraude.

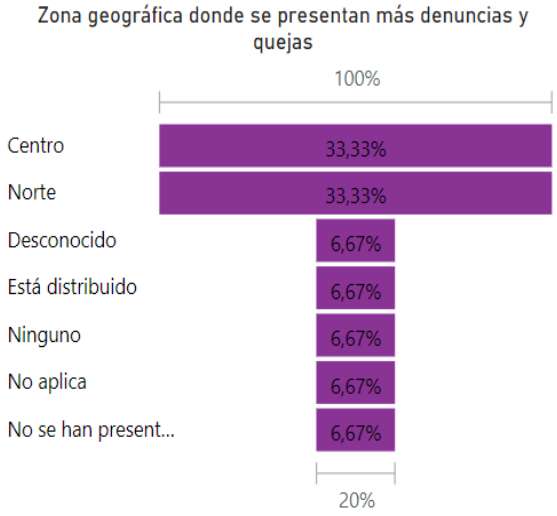


Gráfico N°1: Bancos Comerciales

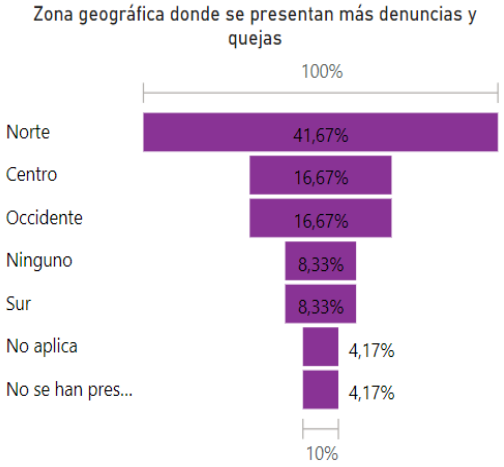


Gráfico N°2: Cooperativas de Ahorro y Crédito

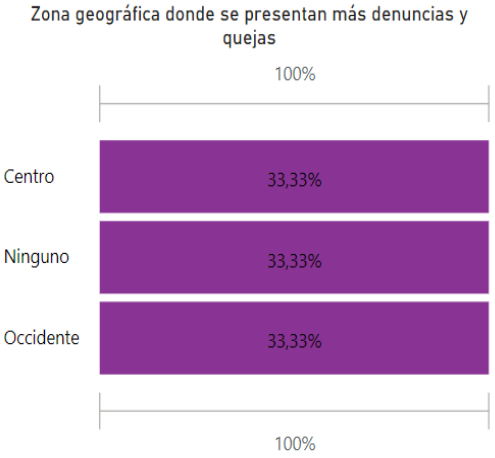


Gráfico N°1: Bancos Estatales

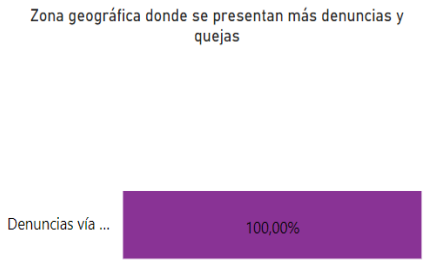


Gráfico N°4: INDEL

Las Instituciones han realizado reportes de operaciones sospechosas asociados al ciberdelito o fraude

De todas las instituciones solo la INDEL (gráfico N°4) ha enviado ROS a la UIF asociados al Ciberdelito o Fraude.

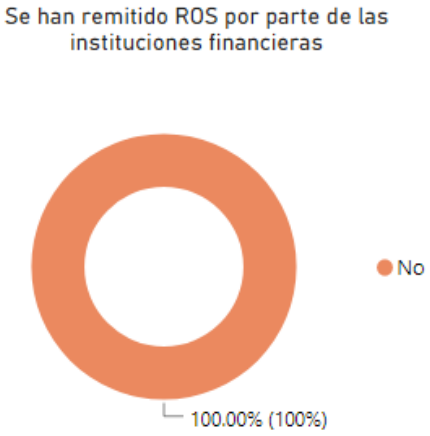


Gráfico N°1: Bancos Comerciales

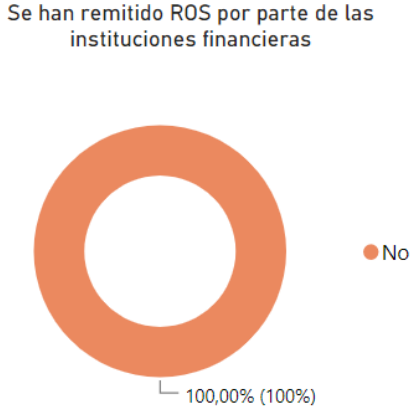


Gráfico N°2: Cooperativas de Ahorro y Crédito

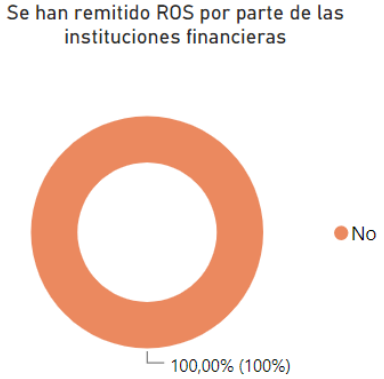


Gráfico N°1: Bancos Estatales

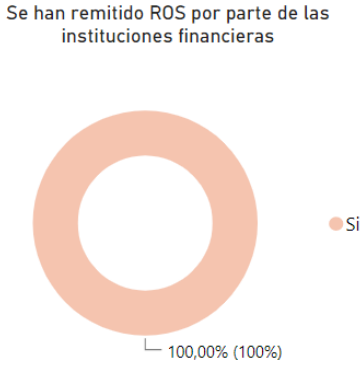


Gráfico N°4: INDEL

Motivos o razones que justifican el no realizar reportes de operaciones sospechosas a la UIF

Las instituciones manifestaron que no han realizado ROS a UIF porque la detección no reúne los requisitos para hacer un ROS debido que han encontrado que el cliente es la víctima de un tercero no relacionado con la institución y por falta de capacitación para tratar estos tipos de reportes. Exceptuando la INDEL la cual si realizó Reportes de Operaciones Sospechosas.

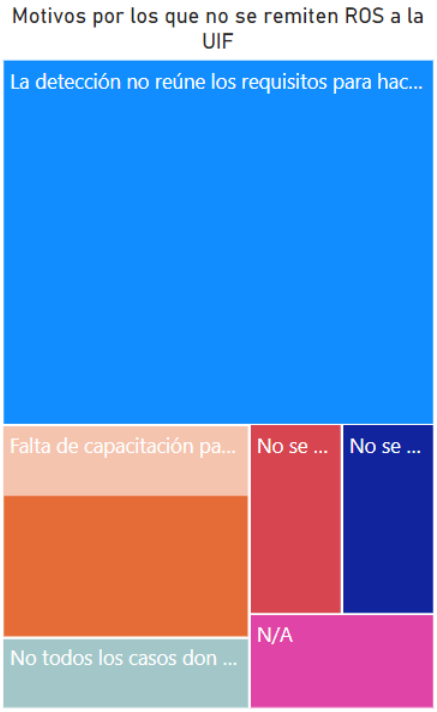


Gráfico N°1: Bancos Comerciales

Gráfico N°2: Cooperativas de Ahorro y Crédito

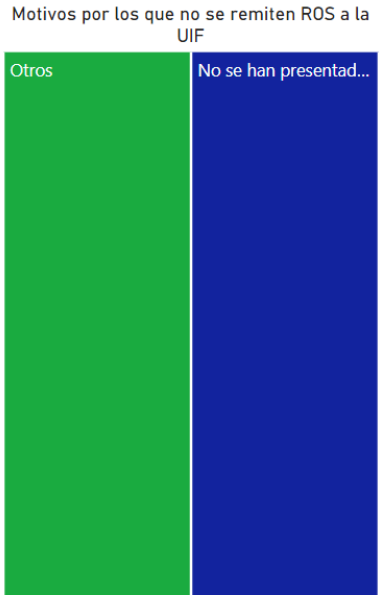


Gráfico N°1: Bancos Estatales

Reclamos y Zona Geográfica

Como se ha mencionado en otras secciones de este análisis los sujetos obligados consultados pertenecen a los siguientes sectores:

En la consulta relacionada a la zona geográfica para determinar desde donde las instituciones reciben la mayor cantidad de denuncias o reclamos vinculados a prácticas como el robo de identidad, fraude y/o la suplantación de identidad se ha logrado establecer que la zona del ***norte*** (ver ilustración 1) del país es la región con mayor número de reclamos o denuncias por este tipo de prácticas delincuenciales, este hecho es aplicable en su mayoría para las instituciones que forman parte de los sectores de **Bancos comerciales y Cooperativas de ahorro y crédito**, mientras que en el caso de Bancos Estatales hay una distribución equitativa entre la zona *Norte, Centro y Sur* lo anterior en vista de que el sector no tiene un número significativo de transacciones por canales digitales o medios magnéticos a diferencia de los antes mencionados.

Zonas del Pais	Reclamos Recibido
⊞ Norte	34.88%
⊞ Centro	23.26%
⊞ Occidente	11.63%
⊞ Ninguno	9.30%
⊞ No aplica	4.65%
⊞ Sur	4.65%
⊞ No se han presentado	4.65%
⊞ Desconocido	2.33%
⊞ Denuncias vía Contact Center (Llamadas)	2.33%
⊞ Está distribuido	2.33%
Total general	100.00%

Ilustración 23: Distribución geográfica de reclamos o denuncias

Cuando se vincula el número de denuncias recibidas en el periodo analizado con la zona geográfica se puede determinar

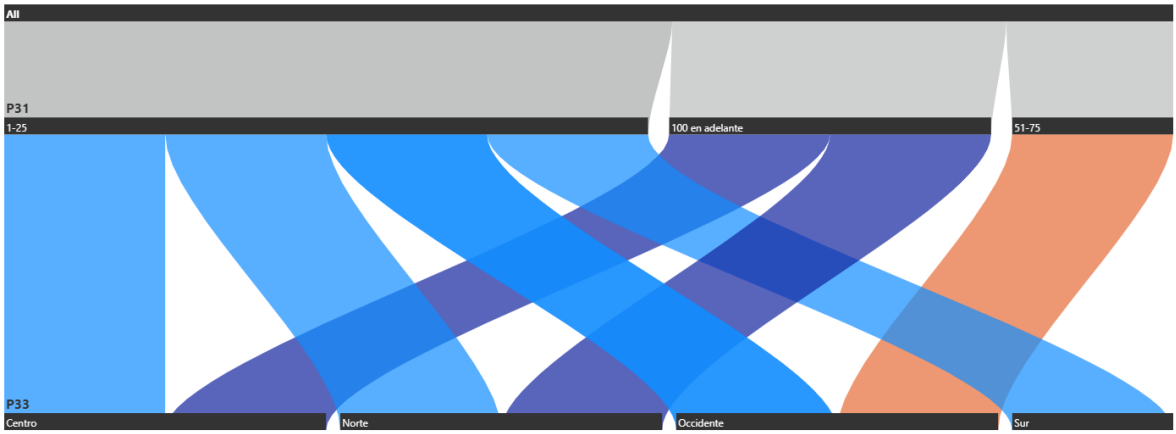


Ilustración 24 Zona de origen de los reclamos y rangos en el periodo de estudio

Las instituciones declaran que en su mayoría recibieron reclamos o denuncias entre 1 – 25 en el término de 1 año de manera global y que estas se origen en 4 zonas del país (norte, centro, sur y occidente), de manera particular deberemos dejar planteada la pregunta de qué sucede con la zona oriental del país compuesta por lo departamento de El Paraíso, Olancho y Gracias a Dios que no presenta reclamos asociados a fraude o ciberdelitos lo cual invita a pensar que:

1. Existe mayor movilización de efectivo en la zona.
2. No se han promovido muchos los servicios digitales.
3. En su mayoría la actividad comercial de la zona es agrícola lo que motiva más el uso del efectivo.

Estas son solo conclusiones a priori dado el fenómeno de no recibir reportes de dicho sector o zona del país; entre otros hallazgos del análisis se debe resaltar que en el rango de reclamos recibido entre 100 en adelante son solo parte de los bancos comerciales los que se encuentran en dicha categoría, ya que al día de hoy son los que presentan un desarrollo mayor en el campo de la innovación de servicios financieros lo que también los deja mayormente expuestos a prácticas de fraude y ciberdelitos, sin embargo también resulta significativo que dicho sector presenta mayor madurez en la adopción de esquemas de seguridad de datos.

En cuanto las Cooperativas de ahorro y crédito el mayor número de reclamos son recibidos de la zona norte y occidente que es donde se puede ver mayor presencia de estas instituciones y teniendo una distribución de los reclamos casi equitativa entre las clases de 1 – 25 reclamos y en mayor volumen entre 51 – 75 desde la zona occidental compuesta por los departamentos de Ocotepeque, Copán, Lempira y Santa Barbara. Estas instituciones en la consulta realizada representan el 56% del total de sujetos obligados participantes, la

siguiente grafica involucra todos los sectores consultados y la distribución de zona y detalle de rangos de reclamos excluyendo aquellas categorías que no son significativas para el análisis como campos nulos, no aplica y otras categorías menores al 2% de representatividad en la colección de datos.

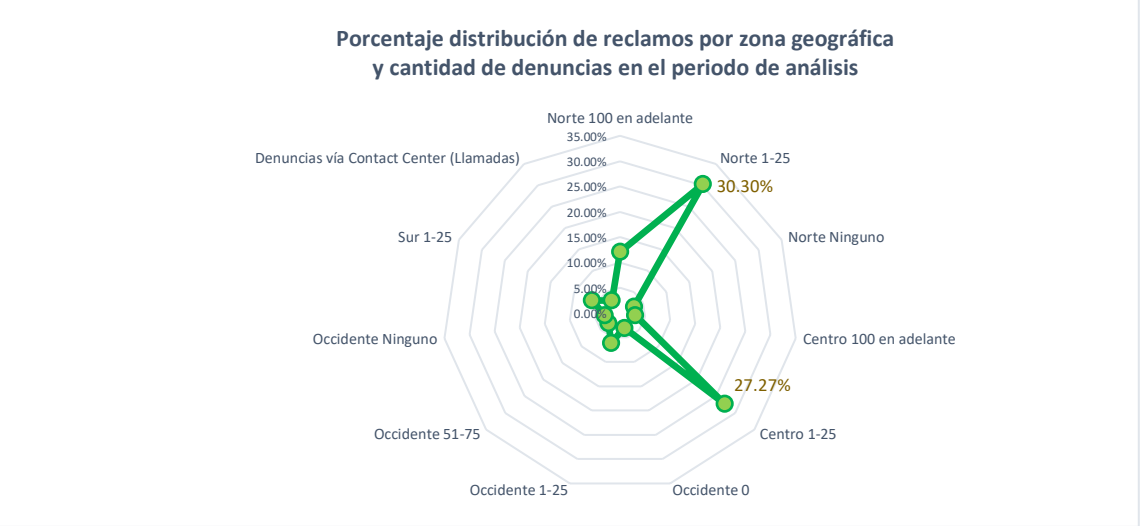


Ilustración 25 Distribución de reclamos por zona

Como se mencionó anteriormente las categorías más significativas como se puede observar en la ilustración están en cantidades casi equivalentes (30%) en zona norte y centro las demás categorías se concentran en valores entre el 3 y 6 % de la colección de datos.

No resulta extraño que la concentración de este tipo de reclamos se de en las zonas más significativas a nivel nacional debido a que ellas también se encuentra la mayor presencia de instituciones financieras por lo que el número de transacciones es mayor, se debe resaltar que en esos territorios también se encuentra una alta presencia de crimen organizado por lo que se deben tomar mayores y mejores medidas de control y prevención de los delitos asociados al lavado de activos.

Número de transacciones por zona durante el periodo de marzo a noviembre 2020

Esta sección tiene como objetivo mostrar de manera cualitativa, si en realidad existió un incremento durante el periodo de marzo a noviembre del año 2020 con respecto al año 2019. A nivel de país ya desde los meses de junio del 2020 se comenzaba a experimentar una flexibilización de las medidas de circulación de personas en las diferentes ciudades, sin embargo la habilitación de nuevos canales digitales para la realización de diferentes tipos de gestiones durante este periodo y de manera positiva logró acelerar la adopción de nuevas tecnología y modelos de negocios innovadores ofreciendo a los usuarios y clientes alternativas para efectuar gestiones financieras sin presentarse a una ventanilla.

Tal como se puede observar en las siguientes graficas por zona geográfica para los mismos periodos de los años 2019 y 2020 no hay cambios significativos de un año a otro, pero si es importante mencionar que al observar el comportamiento de los rangos de transacciones se puede percibir un incremento de una clase a otra por ejemplo, si observamos el rango de transacciones de 1 – 1000 para el periodo del año 2019(Ilustración 26) en la zona norte este representaba el 25% de los Sujetos Obligados consultados seguido de 12.5% en las transacciones mayores a 5,000. Para el mismo espacio temporal en el año 2020 se da una variación entre las clases disminuyendo el rango de 1 – 1,000 de 25% a 21.88% y aumentando a 18.75% el rango de transacciones de mayores a 5,000 (Ilustración 27). ¿Cómo puede interpretarse este cambio entre clases para esta zona?, claramente este movimiento es el que evidencia el incremento en el uso nuevos medios para realizar gestiones financieras. Un cambio porcentual de aproximadamente 6 puntos en la clase mayores a 5,000 en términos reales significa miles sino es que millones de transacciones ejecutadas por medios digitales en las instituciones consultadas.

Caso similar ocurre en la zona sur donde para el año 2019 existía la categoría de 4,001 a 5,000 misma que para el siguiente año se encuentra concentrada en la clase de transacciones mayores a 5,000; lo anterior puede interpretarse como un efecto migratorio de una clase a otra pudiendo inferir que si se han dado aumentos importantes en el uso de canales digitales durante los primeros 8 meses de la emergencia sanitaria mundial, acelerando las iniciativas de innovación tecnológica y disruptiva en el mercado financiero nacional y en ciertos casos despertar la necesidad de estos nuevos esquemas de negocios

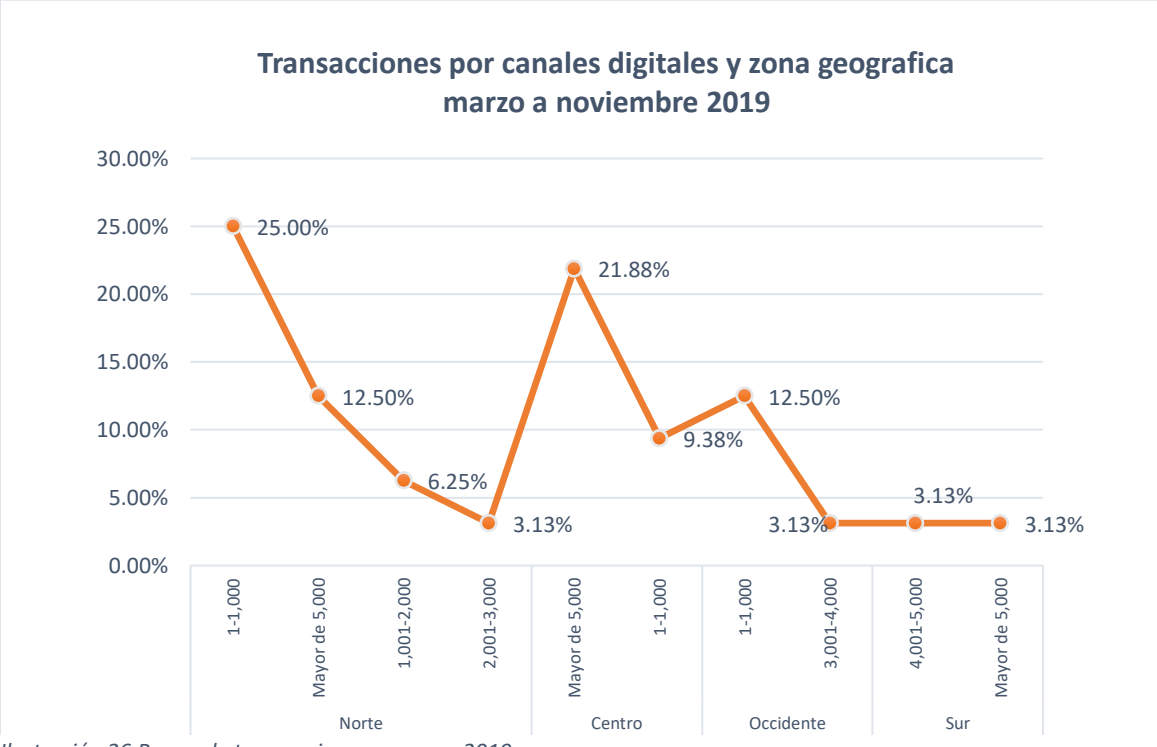


Ilustración 26 Rango de transacciones por zona 2019

que hagan aportes significativos en temas de inclusión financiera, medios de pago, servicios financieros en línea entre otros.

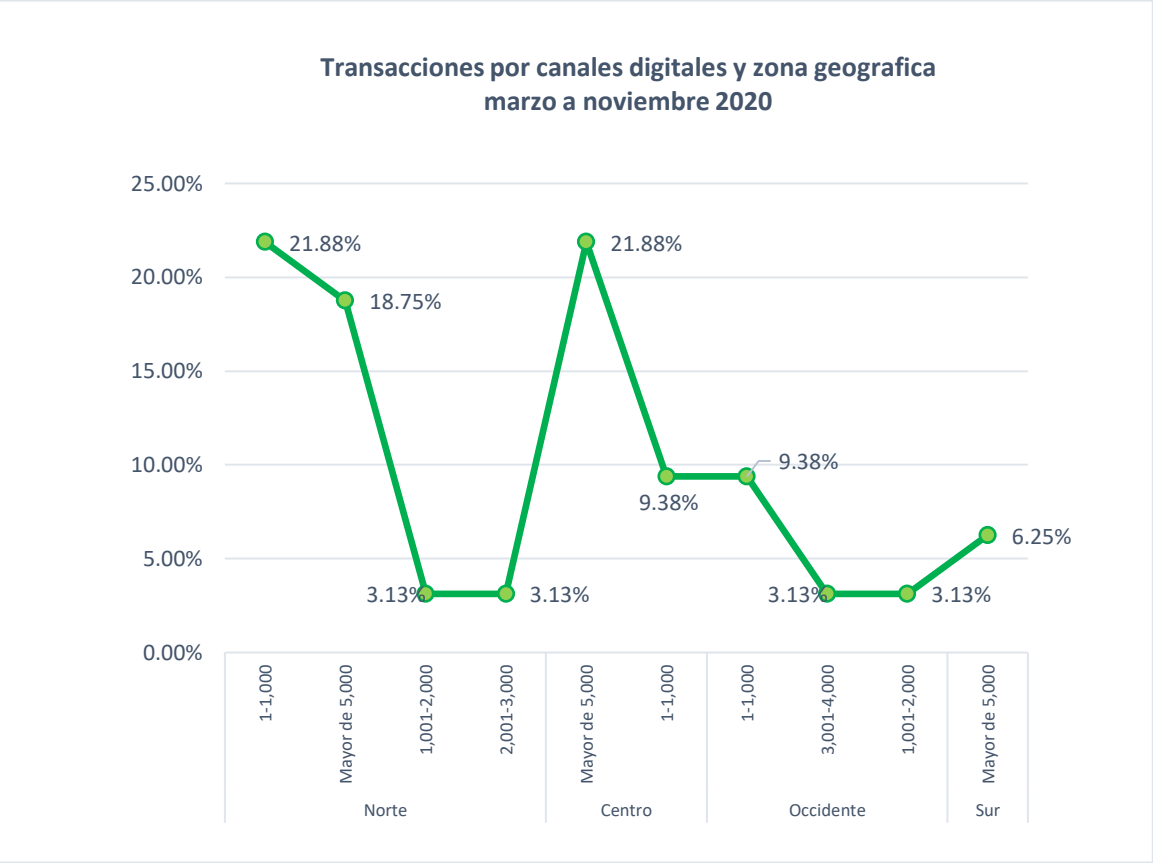


Ilustración 27 Rango de transacciones por zona año 2020

Canales o servicios financieros creados durante la pandemia.

En la consulta general realizada a las instituciones si había creado nuevos canales o servicios financieros para la atención de sus clientes, aproximadamente el 75% contestaron que si lo habían hecho; comprobando con esto, que como efecto derivado de la pandemia la aceleración de la transformación digital durante los primeros 3 meses ha sido significativa, tal ha sido el efecto que de acuerdo con el Reporte de Ciberseguridad 2020 (BID - OEA, 2020)[19] esta transformación estaba prevista que ocurriera en tres años más.

[19] Página 28 Nayia Barmpaliou, Jefa de Políticas e Iniciativas Públicas Centro para la Ciberseguridad, Foro económico Mundial

Lo anterior permite establecer el contexto en que las instituciones financieras del país realizaron esfuerzos de acercar sus servicios a la población siendo los más significativos de acuerdo con la consulta realizada los siguientes:

Servicios o Canales	Porcentaje
Apertura de productos financieros no presencial	29.63%
Aplicaciones móviles	24.07%
Banca en línea	12.96%
Métodos de pago sin contacto o pasarelas de pago	5.56%

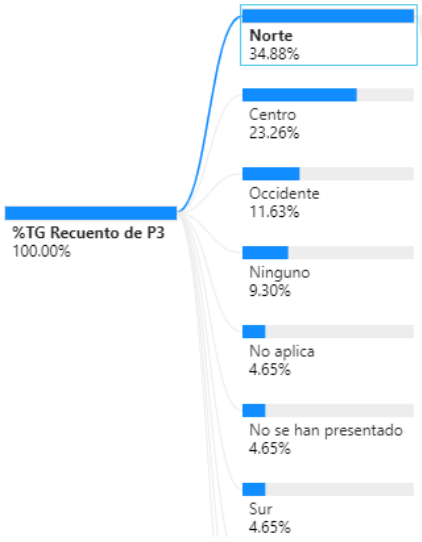
Tabla 1 Servicios y canales implementados

Si hacemos diferencias por los sectores a los que pertenecen los sujetos obligados participantes del estudio en el caso de los Bancos Comerciales e INDEL los canales como aplicaciones móviles y banca en línea ya estaban implementados tiempo atrás, pero durante el periodo de la pandemia se han agregados nuevos servicios como:

- Depósitos de cheques de manera no presencial.
- Pago de remesas con deposito en cuentas de banco o en monedero electrónico.
- Solicitud de tarjetas de crédito y débito en línea.
- Activación de servicios de banca en línea.
- Apertura de cuentas.

Con respecto al sector de Cooperativas de Ahorro y Crédito algunas de las consultadas mencionaron que se han dado incrementos en las transferencias realizadas por la institución a cuentas de ahorros de clientes en bancos comerciales, también se han incorporado servicios de cobranza y pago de préstamos de manera digital.

En términos generales y en los sectores donde aplique el aumento del uso de tarjetas de débito y crédito ha sido mayor, esto a razón de que muchas de las actividades económicas como la venta de alimentos de consumo masivo, servicios de restaurantes y otros también implementaron servicios de entrega en la puerta de la casa lo que motivaba registro de las tarjetas de crédito y débito en estas aplicaciones o portales de compra explicando de esta manera el incremento en el uso de tarjetas.



Si segmentamos estos canales o servicios por las zonas geográficas desde donde más se reciben reclamos por delitos de fraude y ciberdelitos, la región con más apertura de servicios como en párrafos anteriores sigue siendo la zona norte del país seguida del centro y occidente, como se observa en el gráfico.

De manera preliminar dado que la zona geográfica referida no indica el origen de donde se apertura el servicio, se podría también aseverar con una precisión media que el

número de reclamos futuros seguirán teniendo la misma distribución en cuanto a las zonas, por lo que lo mecanismos de vigilancia y monitoreo deben ser más exhaustivos en dichas regiones.

Evaluación de riesgos LAFT previo a lanzamiento de canales, productos y servicios financieros.

En cumplimiento a lo establecido en los artículos 47 y 48 del Régimen de obligaciones, medidas de control y deberes de las instituciones supervisadas en relación con la ley especial contra el lavado de activos, insta a los sujetos obligados a realizar identificación de riesgos para la prevención de lavado de activos (art. 47) a través de diferentes factores (art. 48) en el inciso b establece:

> **Productos y Servicios**. Conocer el riesgo asociado a los productos y servicios, existentes o nuevos e innovadores que se ofrecen por cuenta propia o por terceros, ya que pueden ser utilizados por clientes o usuarios para el delito de lavado de activos. Asimismo, realizar análisis cuantitativos y cualitativos utilizando variables que permitan identificar los productos y servicios de mayor riesgo.

Parte de la consulta dirigida a los sujetos obligados comprueba que en su mayoría 68% realizan una evaluación de riesgos previo al lanzamiento de un producto o servicio, el otro 32% no lo realiza ya sea porque no han lanzado ningún servicio digital o los ya existentes cuentan con una evaluación posterior a la realización de este análisis.

Estimación de Impacto

Los reclamos realizados por los clientes al haber sido víctimas de alguna practica relacionada a fraude o ciberdelito provocan que los sujetos obligados deban resarcir ese daño ocasionado por las bandas delincuenciales a sus clientes, lo que puede provocar perdidas en los modelos de negocios que involucren canales digitales como es obvio este impacto también debe ser medido de acuerdo al tamaño del sector y número de operaciones que tienen durante cierto periodo de tiempo, este análisis no pretende realizar una cuantificación monetaria del impacto de estas prácticas delictivas sino más bien establecer una valoración cualitativa a través de la consulta realizada a los sujetos obligados en los siguientes rangos en lempiras:

- 0.00
- < 10,000.00
- 10,000-250,000.00
- 250,000-500,000.00

- 500,000-1,000,000
- 1,000,000 en adelante

Tres (3) de los sectores (Bancos Comerciales, INDEL y Bancos Estatales) consideran que el impacto económico derivado de transacciones va más allá de 1,000,000.00 de lempiras al año en costos por reparar el perjuicio ocasionado a los clientes por estos grupos criminales, lo cual se estima como una pérdida operativa del negocio; se debe destacar que la mayoría de estas instituciones tiene inversiones importantes en la detección de operaciones fraudulentas pero aun así este tipo de prácticas siguen afectando significativamente la operación del negocios evidenciando que el crimen organizado siempre busca nuevas formas de evadir controles y generar ganancias ilícitas.

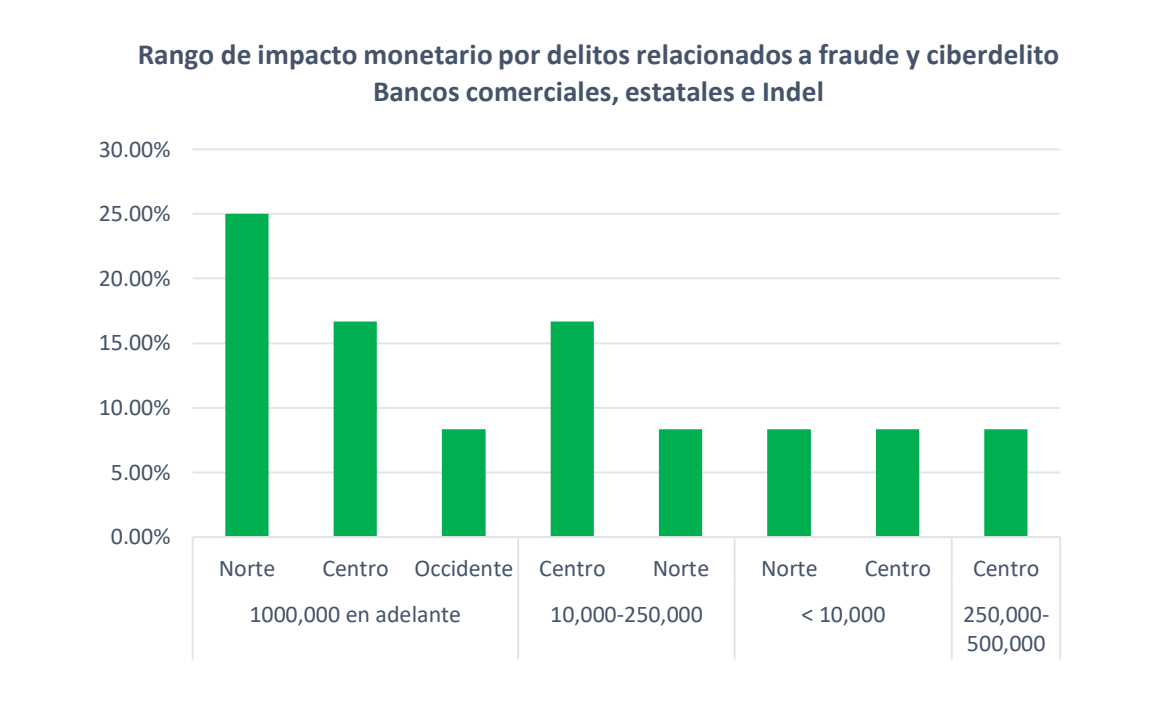


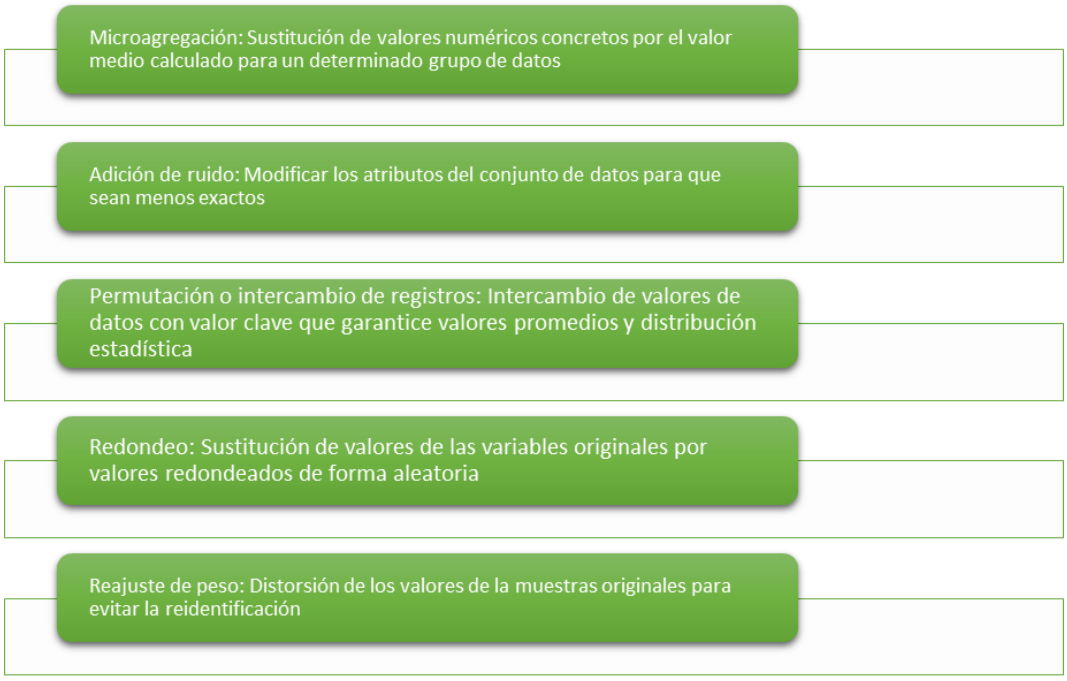
Ilustración 28 Distribución por zona geográfica de rango de impacto económico para 3 sectores

Para el sector cooperativo los impactos son menores en donde el 42% de los consultados pertenecientes a ese sector consideran que su percepción de perdida está en valores menores a L. 10,000.00 en las zonas Norte, Centro, Sur y Occidente del país tal como lo muestra la siguiente ilustración.

Ilustración 29 Distribución por zona geográfica de rango de impacto económico cooperativas de ahorro y crédito

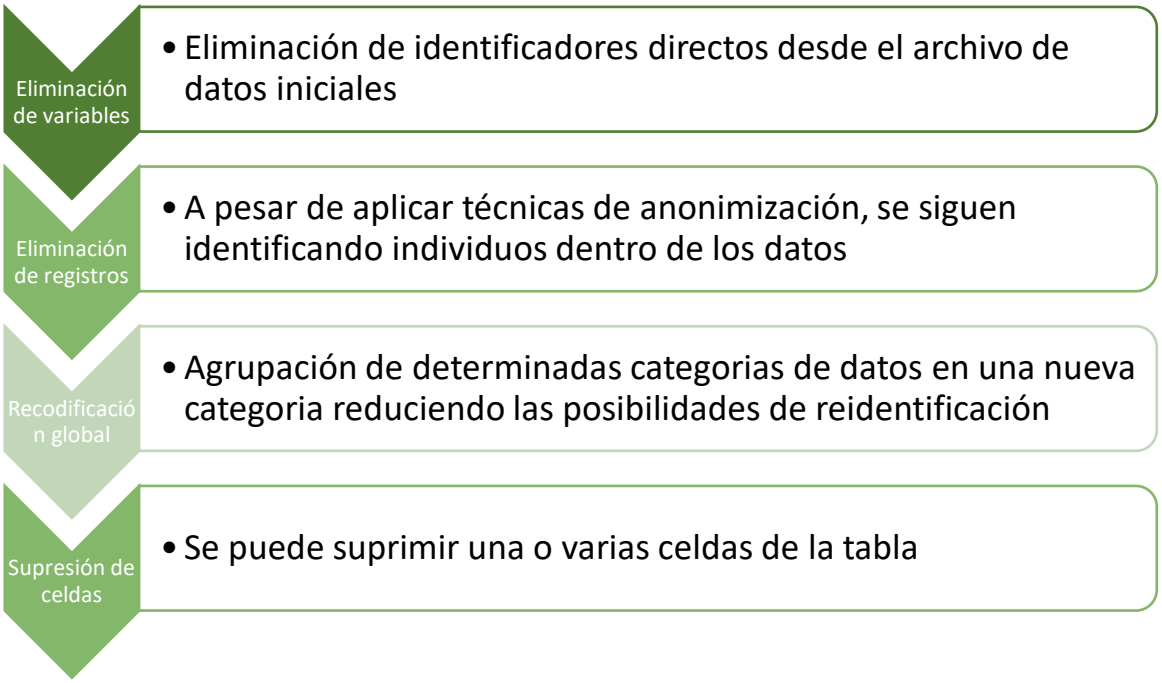
Observaciones

- Con el fin de mantener los datos personales seguros, se debe se hacer uso de métodos de anonimización como, por ejemplo:



- **Métodos de aleatorización o perturbación**: Modificación sistemática de datos (pequeñas cantidades aleatorias) de tal manera que las cifras no sean lo suficientemente precisas como para revelar información para casos individuales.

- **Método de reducción o generalización**: No se alteran los datos, sino que se producen supresiones parciales o reducciones del nivel de detalle del conjunto original.



- **Método o técnica de preanonimación**: Requiere tener claridad sobre la clasificación de datos. Se deben identificar las variables que no se pueden anonimizarse y se eliminan de forma directa
  - Seudoanonimización: Se asignan seudónimos a las variables. Deben evaluarse especialmente los riesgos de reidentificación indirecta

- Contar con más datos en relación con el mundo cibernético permitirá introducir la cultura de gestión del riesgo cibernético, que es preciso extender tanto en el sector público como en el privado.

Conclusiones

-*Los esfuerzos por reducir los impactos derivados de los delitos de Fraude y el Ciberdelito benefician no solo a las instituciones financieras sino también a los clientes, haciéndolos sentir más seguros y respaldados por las instituciones, resulta fundamental fortalecer el conocimiento de los clientes y empleados acerca de los métodos y prácticas que las estructuras criminales utilizan para llevar a cabo los delitos antes mencionados, en ese sentido, como hemos visto en los resultados del análisis; las campañas de sensibilización y concientización para mantener una sana interacción financiera por medios digitales se convierte en una estrategia de carácter preventivo para reducir la exposición de los clientes y las instituciones a estos delitos precedentes de Lavado de Activos y Financiación del Terrorismo.

-*La clonación de tarjetas, uso de tarjetas en páginas web y fraude, son métodos análogos al delito de estafa, de igual manera, los delitos cibernéticos relacionados al ransomware (secuestro de archivos a cambio de un rescate) y extorsión, tienen características similares en cuanto a la complejidad para identificar a quienes cometen este tipo de delitos, luego de los resultados del estudio se ha comprobado que los clientes de las instituciones financieras resultan ser víctimas de estas prácticas delincuenciales afectando el patrimonio económico de los mismos, dificultando el poder realizar un Reporte de Operación Sospechosa, en este sentido, y aprovechando las campañas de sensibilización sobre este tipo de crímenes, en paralelo se debe promover una cultura de denuncia que permita obtener más datos o elementos que motiven el análisis exhaustivo por parte de las áreas de cumplimiento para la detección temprana de este tipo de métodos que afectan los activos financieros de los clientes; es necesario también mejorar las políticas de debida diligencia relacionadas a los empleados [20](KYE) de las instituciones financieras en aquellos puestos en donde se percibe una mayor actividad en lo relacionado a la manipulación de datos, manejo de los cajeros automáticos como una buena práctica y aplicación de un enfoque basado en riesgos.

-*La aceleración en la implementación de productos y servicios financieros en el mercado nacional hoy más que nunca requiere de un marco regulatorio que ayude a generar los mecanismos suficientes y eficientes para permitir el desarrollo de negocios digitales asegurando la protección de la información y la confiabilidad de las transacciones. Los avances en esta temática según el informe de Ciberseguridad 2020 (BID - OEA, 2020) para nuestro país no han sido significativos, aunado a los resultados de este estudio y de acuerdo

[20] Know your employee (conozca a su empleado)

a la opinión de la instituciones participantes del mismo, podemos deducir que el riesgo por ciberdelitos puede categorizarse en una escala media, lo anterior puede generar impactos adversos en el crecimiento y madurez de los productos y servicios; en vista que no solo se necesita crecer en el ámbito tecnológico sino también en la percepción de confiabilidad de los usuarios y adopción de nuevas tecnologías que impulsen la inclusión financiera, el ambiente FINTECH adoptando desde etapas tempranas un enfoque basado en riesgo.

Recomendaciones

- Fortalecer el conocimiento de los clientes y empleados acerca de los métodos y prácticas que se utilizan para llevar a cabo delitos cibernéticos y/o fraude.

- Promover una cultura de denuncia por parte del cliente o usuario, ya sea comunicándolo directamente al cajero de la ventanilla o a través del llenado de una hoja de reclamo, con el fin de obtener datos que ayuden a identificar las diferentes operativas o modus operandi de los delincuentes y de esta forma generar Reportes de Operaciones Sospechosas (ROS) orientados al ciberdelito y/o fraude.

- Realizar campañas de educación financiera por medio de anuncios o publicaciones sobre ciberdelito, ciberseguridad, fraude, en los correos electrónicos de los clientes o en las páginas web de las instituciones deben ser de fácil visualización.

- Dar seguimiento continuo a los empleados aplicando la debida diligencia sobre todo en aquellos casos en los cuales estos tienen acceso a las diversas bases de datos e información de los clientes y técnicos que dan soporte a las máquinas ATM.

- Fomentar la construcción de un marco regulatorio que permita de acuerdo a la realidad del país dar confiabilidad a los usuarios de la protección de su información y garantice la transparencia de las operaciones financieras realizadas desde las diferentes plataformas o medios, en este sentido los diferentes sectores que componen el sistema financiero nacional en conjunto con el ente regulador deberán realizar esfuerzo para impulsar proyectos de ley que permitan espacios de crecimiento de nuevos modelos de negocios financieros seguros, confiables y competitivos que tengan con fin asegurar la privacidad y uso correcto de la información de los usuarios; adoptando un enfoque basado en riesgo y alineado con la legislación vigente y los estándares de lucha contra el Lavado de Activos y la Financiación del Terrorismo.

Glosario

CMM: Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones

NCS: Estrategia Nacional de Ciberseguridad

(APP): Asociaciones público-privadas.

ACTIVO VIRTUAL: De acuerdo con el glosario de términos del GAFI lo define como una representación digital de valor que puede ser comerciada o transferida digitalmente y que puede ser usada para realizar pagos o inversiones

ROS: Reporte de Operaciones Sospechosas

KNOW YOUR EMPLOYEE: (conozca a su empleado)

Anexos

Anexo N°1: Dimensiones del Modelo de Madurez de la Capacidad de Ciberseguridad

Dimensión 1 Política y Estrategia de Ciberseguridad (Diseño de estrategia y resiliencia de ciberseguridad)	**D1.1** Estrategia Nacional de Ciberseguridad **D1.2** Respuesta a Incidentes **D1.3** Protección de Infraestructura Crítica (IC) **D1.4** Gestión de Crisis **D1.5** Defensa Cibernética **D1.6** Redundancia de Comunicaciones
Dimensión 2 Cultura Cibernética y Sociedad (Fomentar una cultura de ciberseguridad responsable en la sociedad)	**D2.1** Mentalidad de Ciberseguridad **D2.2** Confianza y Seguridad en Internet **D2.3** Comprensión del Usuario de la Protección de Información Personal en Línea **D2.4** Mecanismos de Presentación de Informes **D2.5** Medios y Redes Sociales
Dimensión 3 Educación, Capacitación y Habilidades en Ciberseguridad (Desarrollo del conocimiento de ciberseguridad)	**D3.1** Sensibilización **D3.2** Marco para la Educación **D3.3** Marco para la Formación Profesional

Dimensión 4 Marcos Legales y Regulatorios (Creación de marcos legales y regulatorios efectivos)	**D4.1** Marcos Legales **D4.2** Sistema de Justicia Penal **D4.3** Marcos de Cooperación Formal e Informal para Combatir el Delito Cibernético
Dimensión 5 Estándares, Organizaciones y Tecnologías (Control de riesgos a través de estándares, organizaciones y tecnologías)	**D5.1** Adhesión a los Estándares **D5.2** Resiliencia de Infraestructura de Internet **D5.3** Calidad del Software **D5.4** Controles Técnicos de Seguridad **D5.5** Controles Criptográficos **D5.6** Mercado de Ciberseguridad **D5.7** Divulgación Responsable

Anexo N°2: Indicadores Honduras


D3
2016
2020
Formación, Capacitación y Habilidades de Seguridad Cibernética
3-1 Sensibilización
Programas de Sensibilización
Sensibilización Ejecutiva
3-2 Marco para la Formación
Provisión
Administración
3-3 Marco para la Capacitación Profesional
Provisión
Apropiación
D4
2016
2020
Marcos Legales y Regulatorios
4-1 Marcos Legales
Marcos Legislativos para la Seguridad de las TIC
Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
Legislación Sobre Protección de Datos
Protección Infantil en Línea
Legislación de Protección al Consumidor
Legislación de Propiedad Intelectual
Legislación Sustantiva Contra el Delito Cibernético
Legislación Procesal Contra el Delito Cibernético
4-2 Sistema de Justicia Penal
Fuerzas del Orden
Enjuiciamiento
Tribunales
4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético
Cooperación Formal
Cooperación Informal
D5
2016
2020
Estándares, Organizaciones y Tecnologías
5-1 Cumplimiento de los Estándares
Estándares de Seguridad de las TIC
Estándares en Adquisiciones
Estándares en el Desarrollo de Software
5-2 Resiliencia de la Infraestructura de Internet
Resiliencia de la Infraestructura de Internet
5-3 Calidad del Software
Calidad del Software
5-4 Controles Técnicos de Seguridad
Controles Técnicos de Seguridad
5-5 Controles Criptográficos
Controles Criptográficos
5-6 Mercado de Seguridad Cibernética
Tecnologías de Seguridad Cibernética
Seguro Cibernético
5-7 Divulgación Responsable
Divulgación Responsable

Anexo N°3: Enlaces páginas web de los Sujetos Obligados y Cooperativas en tema de seguridad

1. Banco Ficohsa: https://www.ficohsa.com/tus-finanzas/usuario-financiero/honduras/protejase-contra-codigo-malicioso/
2. BAC Credomatic: https://www.baccredomatic.com/es-hn/seguridad
3. Banco Promerica: https://www.bancopromerica.com/informacion-financiera/notificaciones-importantes/
4. Banco Atlántida: https://www.bancatlan.hn/efa/
5. Banco de Occidente: https://www.bancodeoccidente.com.co/wps/portal/banco-de-occidente/bancodeoccidente/canales-servicios/seguridad-en-canales/seguridad-digital
6. Banco Azteca: http://www.aprendeycrece.hn/Articulos/TusFinanzas/22/421; http://www.aprendeycrece.hn/Articulos/TusFinanzas/55/3468
7. Banco Davivienda: https://comunicaciones.davivienda.com/la-tia-segura?utm_source=dominio-principal&utm_medium=redirected&utm_campaign=tia-segura_slf&utm_content=latiasegura.davivienda_link_na&utm_term=na
8. Banpaís: No se encontró o era muy difícil de visualizar
9. Banrural: No se encontró o era muy difícil de visualizar
10. Lafise: No se encontró o era muy difícil de visualizar
11. Ficensa: No se encontró o era muy difícil de visualizar
12. BANHCAFE: No se encontró o era muy difícil de visualizar
13. Banco de los Trabajadores: No se encontró o era muy difícil de visualizar
14. Banco Popular: No se encontró o era muy difícil de visualizar
15. Cooperativa Elga: No se encontró o era muy difícil de visualizar
16. Cooperativa Sagrada Familia: No se encontró o era muy difícil de visualizar
17. Cooperativa Chorotega: No se encontró o era muy difícil de visualizar