INVESTIGACIÓN

Comportamiento del fraude internacional y su impacto en operadores de telecomunicaciones

International Fraud Behavior and How It A ects Telcos

Ydelsi Vielza Caraballo[1*], Dianelys Álvarez González[2]

Recibido: 06/2023 | Aceptado: 08/2023 | Publicado: 12/2023

Resumen

El desarrollo de las nuevas Tecnologías de la Información y las Comunicaciones ha fomentado la proliferación de maniobras delictivas como el fraude, mediante el uso de las vías telemáticas. Debido al aumento existente del fraude en las empresas de telecomunicaciones, se deben proteger a los clientes de los diferentes ataques a los servicios y la aparición de aplicaciones ilícitas. El presente trabajo tiene como objetivo analizar el comportamiento del fraude en el contexto internacional, así como su repercusión en este sector. Se presentan varios casos de estudio con los métodos y técnicas de fraude que inciden en los operadores de las telecomunicaciones, además del marco jurídico para combatirlo. Para la realización del estudio se utilizó el análisis documental para contar con los criterios teóricos que abordan la temática estudiada, se empleó el criterio de expertos y la entrevista como método para la validación de elementos identificados por parte de los investigadores y especialistas en el área. Como resultado de este análisis se presenta el comportamiento de los fraudes más recurrentes en los operadores seleccionados, las estrategias y técnicas adoptadas por los

1* Empresa de Telecomunicaciones de Cuba S.A., ETECSA. La Habana 11300. Cuba. ydelsi.vielza@etecsa.cu

2 Empresa de Telecomunicaciones de Cuba S.A., ETECSA. La Habana 11300. Cuba. dianelys.alvarez@etecsa.cu

mismos, con el fin de identificar aquellos que pueden afectar al país en aras de adoptar medidas en la lucha contra estos. De la misma forma, se incluyen algunas recomendaciones como solución para contrarrestar este tipo de actividades delictivas en el ambiente digital cubano.

Palabras clave: Fraude Internacional; Operadores; Telecomunicaciones; TIC, Ciberseguridad

Abstract

The development of new Information and Communication Technologies has encouraged the proliferation of criminal activities such as fraud through the use of telematics channels. Due to the current increase in fraud in telecommunications operators, customers must be protected from different service attacks and the emergence of illegal applications. The purpose of this paper is to analyze the fraud behavior in an international context, as well as its impact on this sector. The methods and fraud techniques impacting on Telcos and the legal framework for combating it are presented through several case studies. For the study, not only documentary analysis was used to obtain the theoretical criteria that address the subject matter studied, interviews expert judgment as a method to validate the elements identified by researchers and specialists in the field. As a result of this analysis, the behavior of the most recurrent frauds in the selected Telcos, the strategies and techniques adopted by them are presented in order to identify those that may negative impact on the country with the purpose of implementing measures to fight against them. Likewise, to neutralize this type of criminal activities in the Cuban digital environment, some recommendations are included as a solution.

Keywords: *International Fraud; Telcos; Telecommunications; ICT; Cybersecurity*

Introducción

En los años setenta, a partir de la aparición de infracciones asociadas al desarrollo de las TIC, es creada por primera vez la categoría de delitos informáticos. De esta categoría formaban parte tanto los comportamientos delictivos realizados a través de procesos electrónicos,

como aquellos otros delitos tradicionales que recaían bien sobre bienes que presentaban una configuración específica en la actividad informática o bien sobre nuevos objetos como el hardware y el software.

En la actualidad el sector de las Tecnologías de la Información y las Comunicaciones (TIC) siguen siendo uno de los espacios de mayor oportunidad criminal, trayendo consigo disímiles maneras de cometer fraude. Este fenómeno de la criminalidad relacionada con el uso de las tecnologías no pierde la novedad, y en particular, por las empresas que tienen que afrontar la prevención de esta amenaza, como es el caso de los operadores de telecomunicaciones.

Al respecto, estas compañías están cada vez más inclinadas a enfrentar sus desafíos únicos por los fraudes venideros, puesto que el fraude se ha incrementado rápidamente por la evolución de sus métodos y recursos. Situación que también ha afectado directamente a todos los sectores empresariales que desarrollan sus negocios, principalmente, sobre canales digitales. En este sentido, la industria de las telecomunicaciones nunca dejará de ser el escenario donde se desarrollen los más complejos y diversos tipos de fraudes que se comenten hoy día (Cruz Vivar, 2021).

Es por ello que el principal objetivo de la investigación es justamente identificar los disímiles casos que han afectado económicamente tanto a las empresas como a los clientes de las mismas. En este sentido, resultando de gran interés abordar los diferentes tipos de fraude que se pueden presentar en los operadores de telecomunicaciones. Esto con el fin de identificar su modus-operandi para así prevenir la mayor cantidad de eventos desfavorables en este entorno. Además, con la identificación de buenas prácticas y la propuesta de estrategias se puede reducir al máximo las pérdidas ocasionadas por dichos actos en este sector tan dinámico y cambiante.

Materiales y métodos de investigación

Esta investigación es de carácter mixto con preponderancia cualitativa, se utilizó el método inductivo-deductivo y analítico-sintético. Se realizó el análisis documental, para determinar las fuentes bibliográficas y profundizar en el tema de objeto de estudio.

Se emplearon además, las técnicas de análisis de casos para profundizar mejor en la investigación, donde se ejemplifica el accionar de actos delictivos de ciberfraude en los operadores de telecomunicaciones analizados como son ENTEL CHILE, VODAFONE ESPAÑA, ORANGE ESPAÑA, VERIZON WIRELESS, CNT ECUADOR.

Asimismo, se empleó la entrevista y criterios de expertos especialistas e investigadores en el área de antifraude de este sector en Cuba, para validar la tipología de términos empleados en el estudio.

Resultados y discusión

Comportamiento del fraude internacional: Impacto en las Telecomunicaciones

1. Visión general del mercado TIC

Es una realidad que la pandemia Covid-19 trajo aparejado una serie de efectos que no solo se reflejaron en el sector de la Salud sino también en el de las TIC. En este sentido, esta situación al ocasionar que se ajustaran los modos de realizar las actividades laborales como por ejemplo el cambio al trabajo híbrido o remoto, provocó que los controles existentes con respecto al fraude fueran poco efectivos.

Tal es el caso que, en el 2021 la mayoría de las empresas radicadas en la región de América Latina y el Caribe informaron que sufrieron pérdidas por fraude, infracciones de cumplimiento o ciberataques, cuyos hechos no solo trajeron pérdidas financieras para las empresas sino también que ocasionaron daños a la reputación y credibilidad de la misma, así como a su marca comercial. Los fraudes, estafas o engaños por internet representaron más del 80% de los ciberdelitos cometidos en ese año.

2. Marco jurídico del sector

La regulación, la gestión y el establecimiento de mecanismos que aseguren los derechos y deberes de los usuarios es una labor fundamental para caminar con seguridad hacia una era más digital. Respecto del compromiso con el tema, a nivel mundial se han producido iniciativas con distintos alcances como es el caso de Naciones Unidas a través de la Unión Internacional de Telecomunicaciones1 (UIT). Al

1 Organismo especializado para las tecnologías de la información y la comunicación, encargado de regular las telecomunicaciones a nivel internacional entre los Estados miembros y las empresas operadoras

respecto, la UIT estableció en el 2015 la Recomendación UIT-T X.1157 que describe las capacidades necesarias para el servicio de detección y respuesta al fraude de servicios basados en aplicaciones de tecnologías de la información y la comunicación (TIC) sensibles a la seguridad. Utilizada por lo general, en áreas verticales de gestión económica del cliente, como ciberfinanzas, acceso a distancia en la empresa pero también se utiliza a menudo para detectar fraudes internos y otros tipos de actividades no autorizadas.

Esta recomendación aunque sirve de referencia normativa para muchas empresas tanto por su alcance global como por garantizar las interconectivdad de sus redes, sigue siendo insuficiente para este sector que se caracteriza por la rapidez del cambio. Por ello, la UIT en cada espacio de análisis sobre el tema incide en que los gobiernos junto a los órganos reguladores deben avanzar en esta materia a lo interno del país y desarrollar estrategias nacionales robustas y coordinadas para poder proteger los activos de las organizaciones y los usuarios.

Para ello, es necesario que se desarrollen evaluaciones regulares de sus compromisos de seguridad, incluidas métricas, así como que monitoreen y actualicen las estrategias de seguridad con planes de implementación claros. Asimismo, que promuevan la participación regular en actividades internacionales para compartir buenas prácticas, estudios de casos y mejorar la capacidad de preparación y respuesta.

3. Tipología de Fraudes en el sector de las Telecomunicaciones

Las telecomunicaciones se enfrentan constantemente a nuevos retos y cambios debido al crecimiento significativo del avance tecnológico, lo que propicia un aumento en los riesgos de fraude en este sector. Tal es el caso que el fraude de telecomunicaciones, también conocido como fraude telco, o fraude de telecom, incluye cualquier tipo de actividad diseñada para abusar o ganar ventaja sobre las compañías de telecomunicaciones utilizando el engaño (Nebrada, 2022). Existen varios criterios para clasificar los tipos de fraude que se cometen en los diferentes servicios y redes de telecomunicaciones, por ello, en la siguiente tabla se expone un resumen de los mismos, teniendo en cuenta lo abordado por García Carral, 2017 y otros referentes:

TIPOLOGÍAS DE FRAUDE	DESCRIPCIÓN
Secuestro de llamadas	Denomina blueboxing o manipulación del plan de numeración. En este escenario el operador de tránsito B decide maliciosamente redireccionar un porcentaje de estas llamadas a algún equipamiento propio que atienda dichas llamadas con alguna locución pregrabada. Con este accionar el operador B cobra al operador A por llamadas que nunca llegan a su destino verdadero y que, por lo general, no poseen costo alguno para él. Además, se puede presentar el caso donde el operador B puede generar la llamada haciéndose pasar por el operador A manipulando el prefijo o numeración del operador principal.
Falso establecimiento de llamadas	Denominado FAS (False Answer Supervision). Una llamada telefónica comienza su tarifación desde el momento en que el destinatario de la misma la atiende. Toda la etapa anterior al establecimiento no genera cargos para el usuario que inició la llamada ni tampoco para los operadores de telefonía intermediarios. En este sentido, el establecimiento prematuro de la llamada por alguno de los operadores de telefonía (intermedios) y la generación de una falsa señal sonora de progreso de llamada hacia el origen. De esta forma la llamada es tarifada por un período mayor al verdadero tanto al Operador A como al abonado originante. En esencia, es posible que existan llamadas que finalmente nunca son atendidas por ausencia del destinatario y que también son tarifadas.
Secuestro o *hacking* de la central telefónica de un usuario	En esta situación un atacante realiza una intrusión remota a una central telefónica de un usuario o abonado final. Las técnicas para lograr este objetivo son diversas, entre estas están las siguientes modalidades: 1. Utilización de técnicas de fuerza bruta para adivinar contraseñas de la central telefónica del usuario. 2. Explotación de malas configuraciones que permiten a intrusos generar llamadas a través de la central telefónica del usuario. 3. Explotación de configuraciones de fábrica que permiten tener acceso la central telefónica del usuario.
Fraude Internacional de Ingresos Compartidos (IRSF)	Las tarifas de llamadas telefónicas a las distintas regiones o países del mundo no son todas iguales. Existen países que por su situación geográfica o regulatoria poseen valores muy altos. La existencia de destinos de tan alto valor genera la aparición de este escenario de fraude debido a las elevadas sumas que el defraudador puede generar en cortos intervalos de tiempo. De esta manera el defraudador renta números a uno de los operadores telefónicos locales en alguno de los países que presentan valores elevados en el precio de sus llamadas. El defraudador posee un acuerdo de participación en los ingresos con el operador, también denominado en inglés “revenue share”. Mediante este acuerdo el defraudador recibirá parte de las ganancias que el operador local cobra por recibir llamadas desde el exterior a los números rentados. El escenario de fraude se completa con el defraudador generando tráfico telefónico internacional a estos números mediante alguno de los siguientes métodos: 1. Secuestro o hacking de la central telefónica de un usuario. 2. Robo o falsificación de tarjetas SIM de teléfonos móviles locales. 3. Robo de tarjetas SIM de teléfonos móviles de extranjeros que posean itinerancia (roaming). 4. Engaño a usuarios. 5. Redirección de llamadas. En este sentido, la modalidad de robo que se ha extendido a diferentes partes del mundo es la llamada Wangiri. La misma es un fraude que se produce con un sistema informático que origina múltiples llamadas por minuto y las corta al instante para incitar a las víctimas a devolverlas. Los ataques de tipo “Wangiri” lanzan entre 200k y 300k llamadas, teniendo como objetivo recaudar dinero justo cuando la víctima realiza la devolución de la llamada con el coste del minuto telefónico internacional.

Arbitraje	Existencia de planes residenciales con tarifas planas. Dichos planes ofrecen al usuario una tarifa fija a cambio de llamadas ilimitados. Los planes de tarifas planas son generados y calculados teniendo en cuenta patrones normales de llamados telefónicos de usuarios promedio, tanto en volumen de llamadas como en sus destinos. Los defraudadores suelen investigar activamente el mercado residencial para encontrar estas ofertas comerciales. Cuando estos productos ofrecen deficiencias en su armado que los exponen a un arbitraje, los defraudadores los utilizan para generar llamadas por volumen o a destinos que exceden el racional comercial con el que fueron diseñados.
Secuestro o hacking de teléfonos VoIP	El objetivo de este ardid es generar llamadas perdidas a celulares mostrando como origen números premium o internacionales. El receptor de la llamada es engañado en devolver el llamado a números que le generan una alta facturación. Por lo general el defraudador engaña por más tiempo a su víctima imponiendo una música que simula ser el tono de llamada al número discado.
Fraude de suscripción	Se refiere a eludir los controles de crédito y riesgo para obtener productos y servicios de telecomunicaciones sin la intención de pagar. Los estafadores generan información de identificación sintética, la obtienen a través de medios ilegítimos o la extraen de clientes existentes utilizando métodos como la ingeniería social. Estos datos se utilizan para manipular el proceso de incorporación, y cada evento de fraude de suscripción puede someter a un operador a una pérdida significativa (Subex Limited, 2021).
Suplantación de identidad (Spoofing)	Se suplanta no solo la identidad de un cliente para disfrutar de forma ilegal de los servicios y productos que ha contratado el usuario legítimo (llamadas, internet, servicios de contenidos en streaming, hacer pedidos en las divisiones de renting o venta de dispositivos de las propias teleoperadoras), sino también de hacerse pasar por ellos a través de estos para cometer actos delictivos en otras partes (Sacristán, 2023). ejemplo de estos son: **1. Phising:** los delincuentes utilizan el correo electrónico y envían emails suplantando la identidad de alguna empresa. Esos correos suelen tener una apariencia similar a la que enviaría la empresa en cuestión, incluyendo su logotipo, diseño y hasta la tipografía. El contenido del email suele estar relacionado con el pago de una factura pendiente, la devolución de un dinero, el abono de un premio. Transmiten cierta urgencia para que cliques en un enlace que lleva a la página donde te solicitan información sensible como datos personales y bancarios. **2. Smishing:** se intenta llevar a cabo la estafa mediante un mensaje, ya sea a través de un SMS o desde las diferentes plataformas de mensajería instantánea, especialmente Whatsapp. Te piden que hagas clic en un enlace o que llames a un número de teléfono para verificar o actualizar los datos personales o incluso reactivar la cuenta. Esta técnica es más simple, pues un mensaje es más sencillo y corto que un correo electrónico, no hace falta imitar la apariencia. Lo que no cambia es el carácter de urgencia y el objetivo: obtener los datos personales. El enlace conduce a una página falsa o a la descarga de una app maliciosa que puede acabar tomando el control de tu teléfono. **3. Vishing:** es también conocido como “el timo de doble llamada". En este caso, los estafadores realizan dos llamadas haciéndose pasar por operadoras de telecomunicaciones o empresas de servicios. En la primera llamada, se identifican como tu actual compañía móvil o de suministros para informarte de una falsa subida de precios inminente sobre la tarifa contratada. Y en la segunda, se hacen pasar por otra compañía que te propone una mejor oferta comercial o una tarifa más ventajosa. El objetivo es obtener información personal o empujarte a cambiar de compañía.
SIM Swapping	Es conocido también como “**suplantación de SIM**" o “**clonado/duplicado de SIM**", es un fraude que consiste en obtener un duplicado o clon de una tarjeta SIM asociada a una línea telefónica para suplantar la identidad del titular de la línea y poder acceder a sus cuentas bancarias a través del envío de un mensaje SMS (código OTP) utilizado como doble factor de autenticación (Campillo, s.f.)

Fraude de derivación de interconec-ción o Bypass	Conocido también como **fraude de caja SIM o SIMBox**, empleando las tarjetas SIM del operador local. El estafador enruta las llamadas a través de la VoIP y conecta las llamadas como tráfico local, lo que permite al usuario fraudulen-to evitar las altas tarifas internacionales y reducir los precios cobrados por los operadores locales. En las comunicaciones de voz, normalmente se utiliza una central privada para recibir tráfico de un área local y las llamadas se enrutan a través de Internet a una caja SIM en una región remota. Este modelo de negocio de operación se utiliza comúnmente para evitar peajes más altos para llamadas de larga distancia no móviles, particularmente aquellas asociadas con países menos desarrollados.
Fraude de PBX	Uso no autorizado de un sistema de comunicación por atacantes externos y cada vez más usado por hackers debido al poco refuerzo que se hace en la se-guridad de los sistemas de comunicaciones. Permite al defraudador aprove-charse y lucrarse a través de la generación de alto tráfico de llamadas locales, móviles y de larga distancia nacional o internacional, dado que la facturación será recibida por la empresa dueña del sistema. Estas llamas se realizan a tra-vés del sistema telefónico privado para obtener beneficios económicos por me-dio de reventa de minutos, reoriginamiento y el enrutamiento de tráfico dentro y fuera del país, de manera ilegal. Se pueden encontrar diferentes modalidades de este tipo de fraude, entre ellas están: **1. Funcionalidad DISA (Direct Inward Systey fram Access) o acceso remoto:** esta opción se habilita para realizar llamadas desde el PBX, accediendo desde una línea externa de la compañía. **2. Servicio de atención automática-activación marcación en dos etapas:** Existen algunos sistemas de atención automática en los cuales, a través de ciertas opciones, se accede al tono de marcado y se activa la funcionalidad de marcación en dos etapas. Si el sistema no está apropiadamente configurado, el servicio de atención automática pasa la llamada de regreso al PBX como una solicitud de tono de marcado y deja al defraudador en posibilidad de realizar llamadas a cualquier lugar y con cargo a la compañía propietaria del PBX.
Bombeo de tráfico	También conocido como **estimulación de acceso**. Es una práctica en la que las centrales locales sin escrúpulos manipulan el número de llamadas a sus redes para beneficiarse con las tasas de compensación establecidas por la Comisión Federal de Comunicaciones de EE. UU.

Tabla 1: Tipologías de fraude en operadores de telecomunicaciones.

4. Estudio de casos de fraude más recurrentes en operadores de Telecomunicaciones

VERIZON WIRELESS

Verizon Wireless es el mayor operador de telefonía móvil de Esta-dos Unidos con más de 80 millones de clientes. Ofrece servicios de acceso a internet de banda ancha móvil para smartphones, teléfonos básicos, tablets, netbooks, módems USB o fijos, hotspots móviles, smartwatches, autos conectados y otros dispositivos móviles a tra-vés de nuestras redes 5G Ultra Wideband, 5G o 4G LTE. Esta com-pañía reporta indistintamente que se ha enfrentado a actividades fraudulentas relacionadas con su estatus de proveedor de servicios inalambricos.

Las estafas de mensajes de texto no son nada nuevo para Verizon. Como parte de un esquema de fraude reciente, los malhechores han estado enviando mensajes de texto a algunos de sus clientes. Estos mensajes provenían del propio nombre y número del cliente y decía que era un mensaje gratuito que ofrecía información sobre la factura ya pagada. Junto con ello aparecía un pequeño regalo con un enlace que al acceder a el busca información de la tarjeta de crédito del cliente. Al respecto, algunos clientes que recibieron el texto de ellos mismos, informaron que el enlace en el mensaje los enviaba a una red de medios estatales rusa. Los mensajes surgen luego de que el presidente Joe Biden advirtiera a las empresas estadounidenses sobre posibles ataques cibernéticos rusos. Sin embargo, no se comprobó indicios de ninguna participación rusa en esa estafa. Posteriormente a ese suceso, Verizon anunció nuevos esfuerzos para impedir que los mensajes de texto no deseados lleguen a los teléfonos de los clientes. En este sentido recomendó que si se recibía un mensaje de texto no deseado, el cliente podía copiar el mensaje y reenviarlo a un código que daban (SPAM) para denunciarlo.

Otro hecho fraudulento está relacionado con llamadas y envío de textos por WhatsApp a sus consumidores. Al respecto, los estafadores llaman y envían textos por esta vía anunciándole a las víctimas que ganaron un “sorteo internacional” de dinero en efectivo y vehículos de último modelo y les piden llamar a números de teléfono en Guatemala y otros países para retirar el premio. Algunos mensajes provenían supuestamente de la propia empresa de telefonía. El mensaje incluye un número telefónico de Maryland y otro de Guatemala que, presuntamente, es la “línea directa” de un “gerente” de la empresa que coordinará la entrega de los premios. Estos sorteos **son un intento de estafa** para robarle a las personas su dinero. Es una práctica criminal que ha venido en aumento en los últimos dos años contra inmigrantes centroamericanos que viven en Estados Unidos. El primero en desmentir la existencia de un “sorteo internacional” fue Verizon, recomendando a sus clientes no hacer clic ni interactuar con ningún enlace incluido en esos mensajes.

Un tercer tipo de fraude identificado por Verizon fue el phishing donde **suplantaron la identidad de la empresa**. Esta suplantación de identidad la están utilizando para engañar a los usuarios de un sitio web de aspecto similar al de Verizon Wireless. Este fraude consiste en que se recibe una llamada que parece provenir de la asistencia técnica y afirma ser el operador, mediante un mensaje grabado diciendo que el cliente es elegible para recibir un vale para su cuenta. En este sentido, indica que es necesario visitar un sitio web para reclamarlo, cuya dirección web determinada tiene Verizon y el valor del bono. Dicha página web parece oficial, tiene los colores de Verizon Wireless, los gráficos y la navegación. El sitio pide verificar la cuenta del cliente mediante la introducción de su número de teléfono celular, Verizon ID y contraseña, así como los últimos cuatro dígitos del número de Seguro Social. Al ingresar esa información no se recibe un vale, sin embargo, ya se abrió al riesgo de robo de identidad.

Recomendaciones para detectar una estafa de phishing:

- Estar atento a las direcciones URL de semejanza. Tener cuidado con los sitios que tienen Verizon como un sub-dominio de otra URL (es decir, » verizon.scamwebsite.com » o parte de un URL más largo (es decir, » verizonvoucher105.com «).
- Ponerse en contacto con el negocio: En caso de duda, llamar a la línea de atención al cliente de la empresa para comprobar la legitimidad de la oferta. Asegurarse de averiguar el número de teléfono en su cuenta o por una búsqueda en la web – no es el sitio web de los estafadores que te dieron.
- No creer lo que se ve. La página web que los estafadores crean para esta estafa parece increíblemente similar al real sitio de la empresa. Pero arrancando logotipos, colores y gráficos en línea es fácil para los estafadores.
- Se aconseja no abrir un mensaje de texto o correo electrónico que no sea familiar o parezca sospechoso, simplemente proceder a eliminar algo que es incierto.

ENTEL CHILE

Entel es una de las empresas de telecomunicaciones más grandes de Chile. Considerada como líder de este sector, presta servicios de

conectividad móvil y fija, así como una amplia gama de servicios TI y digitales para los segmentos de personas, empresas y grandes corporaciones. Igualmente ofrece servicios mayoristas y de call center en todo Chile.

Entel identificó una inédita estafa sobre acceso fraudulento a su sistema de llamadas por internet. La firma señala que "desconocidos" generaron desde su red, en un día, 130.740 llamadas al extranjero vía internet. Esta acción legal tiene por objeto acreditar el fraude, que se detenga la cadena de cobros y pagos entre los carriers involucrados en el tráfico y, así, evitar un lucro ilegal. Se accedió de manera fraudulenta a su sistema de centralita en la nube, a través de la cual se gestionan las llamadas entrantes y salientes de su servicio para empresas. Gran parte de estas llamadas se realizaron a números inexistentes y utilizando dos direcciones IP. La estimación de este hecho roza los $ 100 millones, cifra que Entel exigió que debe ser abonada a los principales proveedores siguientes en la cadena de pago por conceptos de terminación internacional. Dicho fraude fue detectado oportunamente por el monitoreo permanente que Entel realiza de los comportamientos de tráfico de voz internacional.

Otro de los fraudes a los que se enfrenta la compañía esta relacionado con el llamado SIM Swapping, que no es más que la apropiación de claves o engaños telefónicos. Este es un un ciberdelito que se caracteriza por la suplantación de la identidad de los usuarios de telefonía móvil. Generalmente, la persona que es víctima queda automáticamente sin servicio en su teléfono, por lo que no puede realizar ni recibir llamadas, ni mensajes de textos. Además, queda sin cobertura e internet de forma repentina. La realidad es que, debido a la creciente digitalización, este tipo de fraudes ha aumentado considerablemente en los últimos años.

Los hechos comenzaron en la compañía en el 2019 cuando una consumidora, quien contaba con un plan de teléfono hogar y celular prepago, se acercó a una sucursal de la empresa, con el objetivo de solicitar su cuenta mensual, a lo que la ejecutiva se negó, argumentándole que no estaba a su nombre y que el Rut asociado tenía una

deuda pendiente. Meses después, y pese a pagar su cuenta de forma regular, sus servicios de telefonía eran constantemente suspendidos, así como su deuda había aumentado. En este hecho le habían suplantado su identidad, usado su número de carnet (SERNAC, 2022). A pesar de los diversos reclamos, la compañía no respetó los derechos básicos de la consumidora. Asimismo, actuó de forma negligente al no tomar las medidas de seguridad y de resguardo para evitar la suplantación de identidad.

Para prevenir y reducir el SIM Swapping, Entel recomienda:

- En caso de tener guardada información confidencial (contraseñas o credenciales de acceso) en equipos móviles, es necesario revisar constantemente y cuidar el uso que se le está dando a este tipo de datos.
- Si descargas aplicaciones que tengan atributos transaccionales, debe estar pendiente de revisarlas periódicamente.
- Evitar compartir información personal a través de redes sociales de forma abierta y, en caso de hacerlo, tener conocimiento de que la persona es de confianza y es quien dice ser.
- No es recomendable abrir mensajes, anuncios o links sospechosos. En esos casos, es necesario comprobar primero si esa oferta y empresa son reales.

CNT ECUADOR

La Corporación Nacional de Telecomunicaciones (CNT EP), es la entidad relacionada al Ministerio de Telecomunicaciones y de la Sociedad de la Información de Ecuador. La empresa pública tiene presencia en las cinco líneas de negocios del país donde ofrece servicios de telefonía fija local, regional e internacional, acceso a internet, televisión satelital y telefonía móvil en el territorio ecuatoriano.

El inicio de 2022 para la compañía estatal estuvo marcado por denuncias de robo de identidad y cobros injustificados, donde se vio envuelta en un escándalo de hackeo a sus sistemas y una declaratoria de emergencia institucional. Hasta ese momento se habían detectado 2.107 casos de suplantación de identidad. En esos casos, personas son notificadas con cuentas pendientes por líneas de telefonía fija o

celular, internet, y otros servicios, que no contrataron ni sabían de su existencia hasta ahora. La mayoría de esas denuncias ocurriendo en una provincia específica, donde miles de usuarios se quejaron de que, de un momento a otro, no pueden mover dinero de sus cuentas bancarias y se ven involucrados en procesos de coactiva sin tener nada que ver (DPL News, 2022).

Ante el creciente descontento, CNT emitió un comunicado en donde reconoció que existían irregularidades en su cartera vencida, y aseguró revisar todos los procesos. Habilitó números para que los ciudadanos denuncien robos de identidad. El monto total de la cartera vencida, que estuvo en procesos coactivos, fue de más de $116,4 millones. Eso representó el 20% de los 579 millones de la cartera total de CNT.

ORANGE ESPAÑA

Orange es el operador alternativo de referencia del mercado español y uno de los principales inversores extranjeros en la industria de telecomunicaciones, con más de 13.000 millones de euros de inversión en los últimos años. Ofrece servicios de telefonía móvil, fija, Internet de banda ancha y TV por ADSL en todo el país.

Orange notificó un gravísimo hackeo, ocasionando la filtración de datos personales de sus clientes. Algunos de los datos filtrados fueron: nombre y apellidos, fecha de nacimiento, número de documento de identificación (DNI/NIE/pasaporte), dirección postal física, dirección de email, número de teléfono y número de cuenta corriente (IBAN). Los usuarios afectados recibirían un aviso por email o SMS con detalles de los datos filtrados, pues no son los mismos en todos los casos. Orange España habla de un “número limitado de clientes”, pero por ahora no ha hecho públicas las cifras. El número acabará trascendiendo, puesto que Orange ha informado a la Policía Nacional y a la Agencia Española de Protección de Datos, algo obligatorio por ley ante un hackeo así. Resulta muy probable que esta última inicie una investigación, que derivaría en una cuantiosa multa si se detecta que la seguridad no era la adecuada. Se ha indicado que todos los datos son de personas con las que ha tenido una relación comercial, pero no queda del todo claro si eso incluye clientes dados de baja antes del hackeo. El hackeo a

Orange apunta a ser uno de los más graves en España por lo delicado de los datos personales robados.

Recomendaciones para no caer en la trampa:

Estar atentos a posibles estafas que aprovechen los datos filtrados, pues los ciberdelincuentes pueden usar la información para ganarse la confianza de las potenciales víctimas en fraudes más o menos elaborados.

Además, quienes hayan visto filtrada la cuenta bancaria deberían estar pendientes de posibles cargos no autorizados, y contactar con el banco si encontraran algo que no se reconoce.

Existen servicios especializados en comprobar si se ha filtrado la contraseña u otros datos personales, por lo que está bien revisar de vez en cuando, y es probable que añadan el hackeo de Orange a los registros.

VODAFONE ESPAÑA

Vodafone es una empresa líder de comunicaciones tecnológicas que ofrece servicios de telefonía móvil, telefonía fija, banda ancha y televisión digital en España. Esta empresa fue víctima de una campaña de phishing por un SMS que se encuentran recibiendo algunas personas, y en el cual se dice que pueden proceder ya a retirar una tasa de devolución anual y adjuntan un enlace para ello. El modus operandi es similar al de otros casos, solo que con "vestido" nuevo.

La compañía asegura que los estafadores se hacen pasar por sus operadores, y en caso de no querer facilitar la información que solicitan, amenazan con incluir los datos del cliente en "un fichero" para que la OCU se encargue de que le llamen otras operadoras. Al entrar a la URL se abre una plataforma de pago con tarjeta, siendo llamativo dado que esto es lo propio cuando el pago lo va a realizar el cliente y no en sentido contrario. Lo que se pretende es que la víctima introduzca los datos de su tarjeta y con ello cobrarles el dinero que presuntamente le iban a devolver. Este método es conocido como "vishing" donde los estafadores buscan la facilidad de adquirir los datos, especialmente los bancarios. Para efectuar dicho método se burlaron los sistemas de identificación del móvil, para figurar el nombre de la empresa a la que usurparon con siglas "VDFN".

Recomendaciones de Vodafone a seguir para no caer en la trampa:

Si se reciben dos llamadas en el mismo día o muy seguidas, desconfiar y estar alertas.

No se comunica la subida de la tarifa por teléfono. Generalmente se anuncia por escrito, junto con la factura mensual.

Si se anunciara una subida inminente. La compañía debe avisar del incremento en la tarifa con, al menos, 30 días de antelación.

Si la compañía que hace la nueva oferta no se identifica o dice que la tarifa está avalada por la OCU, desconfiar de las llamadas desde números ocultos o desconocidos.

Verificar con la compañía si las subidas son reales. No se debe devolver la llamada al número en cuestión, sino contactar con la empresa a través de los canales oficiales.

Si se ofrece una buena oferta por vía telefónica, pedir siempre que la envíen por escrito o por correo electrónico.

Tanto si se contrata una nueva tarifa por teléfono como en la tienda física, se dispone de 14 días naturales para desistir del contrato.

5. Propuestas de estrategias a adoptar para combatir el fraude en el contexto cubano

Las estrategias más recomendadas como solución para contrarrestar este tipo de actividades delictivas se enfocan en la implementación de sistemas de gestión que permitan la detección y mitigación del fraude. Las mismas se resumen en la siguiente imagen:

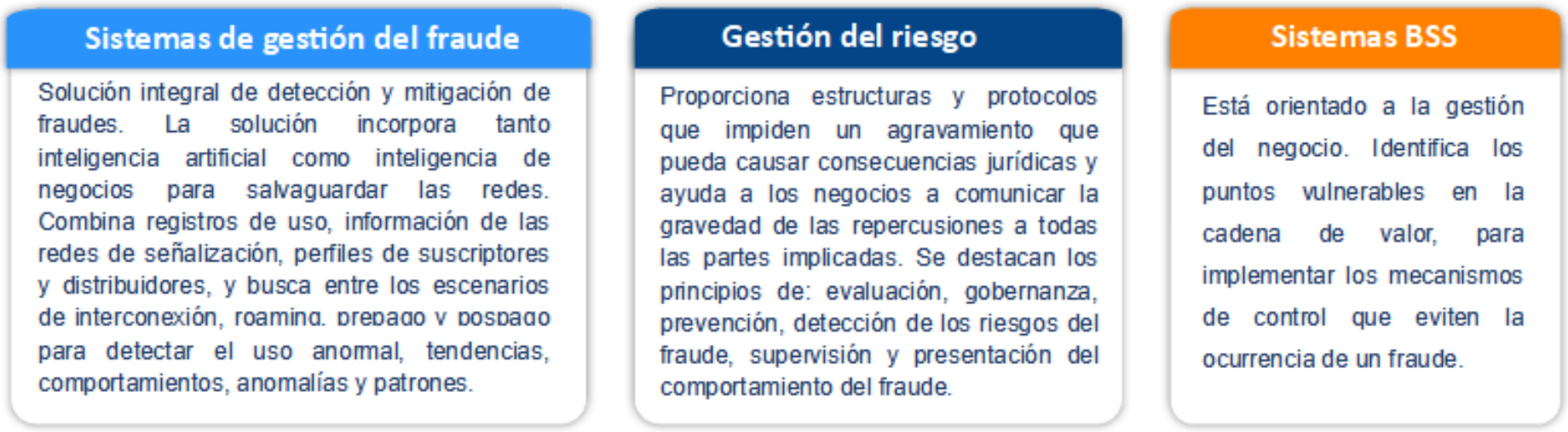

Figura 1: Elaboración propia a partir de la información proporcionada por los operadores analizados.

5.1 Técnicas que se deben aplicar para la detección del fraude en el sector

Técnicas de análisis absoluto: con este tipo de técnica se determinan los comportamientos fraudulentos basados en reglas, que se

definen teniendo en cuenta el comportamiento previo de cada fraude. Son eficientes porque tienen conocimiento de cómo se realizan estos procedimientos por parte de los delincuentes. Pueden fallar cuando haya cambios sutiles o existan nuevos tipos de engaño.

Técnicas de análisis diferencial: permiten detectar cambios en el comportamiento de los clientes sobre el uso de los servicios o llamadas. Funciona almacenando un historial a corto y largo plazo para calcular su comportamiento y captar un cambio. Los datos fundamentales para hacer el análisis son los registros de llamadas, que incluyen la fecha, tiempo de duración, número de origen y destino.

Inteligencia Artificial (IA) y Big Data: la Inteligencia Artificial es un facilitador de mejoras dentro de las tecnologías y servicios de comunicación. La inteligencia artificial es esencial para la optimización y mantenimiento predictivo de las redes de las compañías de telecomunicaciones a través de asistentes virtuales y chatbots para mejorar el servicio, crear la fidelización de clientes, detectar actividades fraudulentas y facilitar la toma de decisiones a partir del análisis de grandes cantidades de datos.

Internet de las cosas (IoT): permitirá un mayor intercambio de información, monitorización de estaciones base, captación de datos, control remoto y automatización en la toma de decisiones para prevenir y descubrir a tiempo violaciones potenciales de seguridad.

La telefonía fija da paso a la nube y chatbots: las tecnologías en la nube permiten sustituir la centralita tradicional y los sistemas de call center por software de telefonía que pueden ofrecer funciones más avanzadas por menos costo. Además, gracias a la inteligencia artificial (IA), es posible ofrecer atención 24/7 y recoger una gran cantidad de datos en tiempo real.

Ciberseguridad: los sistemas cada vez se hacen más vulnerables a las amenazas y fraudes en línea. Por lo que se debe prestar atención a las falsas noticias, propagadas en las redes sociales, que causan daños en la reputación de personas, empresas e instituciones ocasionando pérdidas millonarias. También, a las smart cities donde los servicios públicos y los hogares estarán controlados por IoT.

6. Buenas prácticas en materias de procesos

1. Existencia de validaciones extensivas sobre la identidad del abonado al menos durante las siguientes interacciones entre este y la empresa de servicios:

Alta de un nuevo cliente. Es el momento más sensible y donde mayor foco debe ponerse en verificar la verdadera identidad del potencial nuevo usuario de servicio.

Consultas técnicas sobre el servicio. La información técnica sobre el servicio puede ser peligrosa en manos de estafadores profesionales. El brindarla debe estar precedido de la validación de la identidad cliente.

Modificación de datos personales y/o de facturación. Los cambios de datos básicos del cliente deben ser cuidadosamente alterados y solo valiéndose de buenas pruebas de acreditación de la veracidad del cliente.

La validación debe intentar agrupar la mayor cantidad de datos que permitan validar la identidad real del cliente. Datos clásicos como número de documento, identificador tributario, nombre/apellido, edad, dirección de residencia y otros, pueden no ser suficientes por encontrarse fácilmente online mediante exploración sencilla en un motor de búsqueda (Google, Bing, Yahoo, otros).

Un dato de importancia a ser considerado es el incremento de la gestión de trámites remotos. La autogestión o gestión no presencial pueden ser variados: a través de Internet, mediante mensajes SMS, terminales de autoservicio en lugares públicos o semipúblicos, llamadas telefónicas, otros. En todos ellos el usuario no interactúa físicamente con un representante de la empresa, sino que lo hace a través de alguna tecnología de comunicación. Entendiendo que este paradigma es una tendencia general, los procesos de validación de identidad deben ser ajustados para poder interactuar con clientes que tal vez nunca visiten presencialmente oficinas del operador.

2. Investigación de la capacidad crediticia del cliente. En un proceso comercial, la validación crediticia de la persona física o empresa es clave para contratar los servicios. Por lo general existen servicios

privados que brindan esa información (quebrantos, cheques rechazados) y estos deben ser incorporados como un paso dentro del camino crítico del proceso. Es de vital importancia poder mesurar el riesgo de incobrabilidad que posee cada cliente, y este deberá tener una relación con el máximo crédito en servicios que se le permita consumir dentro de un periodo de facturación.

3. Implementación de una mesa de operaciones destinada a la gestión de fraudes. Se recomienda la existencia de una mesa de operaciones que atienda las alertas generadas por las herramientas que controlan el tráfico de llamadas y predicen la probabilidad de fraude. El proceso de gestión debe incluir, indefectiblemente, un equipo que tenga asignada esta tarea. Es posible que la empresa no posea la envergadura para solventar un equipo de operaciones destinado a dicho fin, por ende, esta función deberá ser sumada a otra mesa de operaciones ya existente. Esta función puede ser agregada a las funciones del SOC32, el NOC33, o del centro de atención al cliente.

Los intentos de fraude pueden ocurrir en cualquier momento, aunque existe predilección por horarios no convencionales. Dado que poseen conocimiento que las empresas poseen menos personal en horarios de fines de semana o madrugadas, suelen concentrar sus ataques en esos momentos. Por lo tanto, es imprescindible que el área que posea delegada la función de recepción de alertas posea operadores 7x24.

4. Auditoria internas y controles. Muchos escenarios de fraude requieren acuerdos de sectores internos en las empresas de telefonía.

Los sectores técnicos poseen acceso a las plataformas de servicio. Estos pueden brindar servicios que nunca serán facturados, alterar registros, generar altas fraudulentas, reasignar cobros de un cliente a otro y otra variedad de acciones que de no mediar su acción un defraudador externo no podría acceder.

Los sectores de producto o compra de destinos telefónicos. Estos habitualmente arreglan con otros operadores interconexiones por las cuales enviar llamadas. En sus manos recae la autoridad para arreglar precios, cantidades, tiempos, calidades y condiciones.

Dentro de esta área bien pueden generarse arreglos que perjudican a la organización.

7. Buenas prácticas en materias informáticas

1. Resguardo de los registros de comunicaciones (CDR). En su nivel más básico toda llamada genera un registro con información que puede variar según la tecnología subyacente que utiliza el operador. Estos registros deben poseer la máxima información posible y deben ser guardados por el mayor tiempo posible. Los registros de las llamadas son un activo valioso para las empresas y es recomendable la generación de resguardos redundantes.

2. Generación de un data warehouse que contenga toda la información de los clientes. No solamente los CDR son información valiosa para la prevención del fraude sino que todo dato estructurado proveniente de todos los sistemas de información de la empresa. Entre los posibles sistemas de interés se encuentran:

Sistemas de atención al cliente o de incidencias.

Comunicaciones de clientes mediante redes sociales de la empresa.

Registros de comunicaciones de clientes mediante llamadas telefónicas o correos electrónicos.

CRM (Customer Relationship Manager).

Bitácoras de equipamiento de comunicaciones y telefonía.

Sistemas de facturación, software de gestión.

Cuentas de crédito o balances de clientes.

Implementación de modelos probabilísticos.

3. Implementación de modelos probabilísticos. La herramienta de reclamos debe contribuir con sus datos estructurados al sistema de antifraude para poder construir la detección de ese modelo de comportamiento anómalo y de esa forma lograr una descripción amplia del comportamiento del cliente o del proveedor. De igual forma puede prevenirse el escenario de Falso establecimiento de llamadas (FAS), también originado por proveedores fraudulentos y también de difícil detección por mecanismos manuales.

Los datos recolectados desde todos los sistemas de la organización deben ser utilizados en conjunción para entender cuales son los patro-

nes de conducta de un defraudador y en base a ellos definir sistemas de detección, tanto basados en métodos probabilísticos predefinidos o basados en sistemas de autoaprendizaje.

4. Análisis financiero. El análisis financiero de la unidad de negocios de telefonía debe hacerse agrupando o cortando el universo de datos por distintas características. Se recomiendan algunas básicas, pero es necesario ampliarse a otras que reflejen la realidad de la empresa. Por lo tanto, es indispensable generar un tablero de comando o reportes periódicos que muestren la rentabilidad a los siguientes niveles.

Unidad de negocios. Considerando la facturación total de los clientes versus los costos directos de la unidad comercial (costos de llamadas, personal directo involucrado, infraestructura directa asociada, costos fijos directos de enlaces de datos, costos fijos directos de interconexiones de telefonía, otros).

Producto comercial. Realizando la agrupación de la facturación por cada producto. La asignación de costos por productos puede ser compleja y necesitar un exhaustivo análisis, pero permite entender que productos son rentables y cuales no lo son.

Destino. Este reporte es uno de los más importantes debido a que numerosas pérdidas se dan por motivos de precios mal asignados a ciertos destinos del mundo. El escenario de fraude derivado de un arbitraje de precios puede ser detectado mediante reportes que incorporen la facturación directa de tráfico telefónico agrupado por destino versus los costos directos asociados.

Cliente. Muestra la rentabilidad de cada cliente. Para empresas grandes verificar la rentabilidad de cada cliente de forma individual es imposible, pero si es posible ver la rentabilidad de aquellos que posean los mayores volúmenes de facturación o los mayores volúmenes de tráfico de llamadas telefónicas.

5. Realimentación a sistemas comerciales y operativos. La integración de todos los sistemas de información y el desarrollo de una herramienta de software automatizada para la detección del fraude, debe permitir la retroalimentación con los sistemas de originales.

Retroalimentación a sistemas comerciales o de relacionamiento con el cliente.

Retroalimentación a sistemas técnicos.

Retroalimentación a sistemas de validación crediticia.

Registros de actividades.

Conclusiones

En el sector de las TIC se identificó que los operadores de telecomunicaciones son las entidades más vulnerables y propensas a los ataques de fraude. Conducido por el hecho de que estos generalmente poseen una extensa base de clientes y por ende manipulan un cúmulo de información confidencial sobre los mismos, convirtiéndose en un gran atractivo para los delincuentes.

El estudio realizado arrojó además, que en el periodo comprendido del 2020 al 2023 los fraudes más comunes se basaron en el robo de dinero y/o datos personales por parte de los ciberdelincuentes. En este sentido, los más representativos se relacionan con el envío de correos electrónicos o SMS que se hacen pasar por correos y/u otras empresas de mensajería; falsos emails de la Agencia Tributaria y otros organismos oficiales y códigos falsos de verificación de WhatsApp. Asimismo, como fue en el periodo de la pandemia, se agudizaron los comunicados falsos sobre el Covid donde los estafadores aprovecharon la angustia de la población para difundir links o enlaces a páginas web fraudulentas y de este modo, robar o sustraer datos personales. Igualmente confirmaciones de compra de plataformas e-commerce; incrementos de la técnica del Phishing de bancos y servicios de pago, así como de plataformas de streaming (Netflix, Amazon Prime, HBO o Disney Plus); robo de cuentas en Instagram y/u otras RRSS; estafas con criptomonedas y cupones de descuento de grandes empresas.

Los operadores están implementando cada vez más estrategias que integran la inteligencia artificial (IA), Big Data e Internet de las Cosas (IoT) como soluciones para contrarrestar este tipo de actividades delictivas en función de optimizar sus operaciones y ofrecer un mejor servicio a sus clientes.

El conjunto de buenas prácticas analizadas, así como las propuestas de estrategias a adoptar para combatir el fraude permite mejorar la capacidad de preparación y respuesta ante estos hechos delictivos que tienen actualmente implementadas las empresas.

Referencias

Arica: Justicia condena a Entel a indemnizar a consumidora por suplantación de identidad. (2022). SERNAC. Disponible en: https://www.sernac.cl/portal/604/w3-article-65892.html

Campillo, R. (s.f.). ¿Qué es el SIM Swapping y cómo evitar el fraude?. Mobbeel. Disponible en: https://www.mobbeel.com/blog/que-es-el-sim-swapping-y-como-evitar-el-fraude/

Cruz Vivar, B. S. (2021). Desarrollo De Un Sistema De Control Para Prevenir El Fraude Comercial Realizado Por Tramitadores, Aplicando Estrategias De Inteligencia De Negocios En Una Empresa De Telecomunicaciones. Disponible en: https://repositorio.untels.edu.pe/jspui/bitstream/123456789/749/1/CRUZ%20VIVAR%2c%20BENJI%20STEVEN.pdf

DPL News (2022). Ecuador | Denuncias de robo de identidad y cobros injustificados crecen contra CNT. DPL NEWS. Disponible en. https://dplnews.com/ecuador-denuncias-de-robo-de-identidad-y-cobros-injustificados-crecen-contra-cnt/

García Carral, J. M. (2017). La gestión del fraude en empresas de telefonía Propuesta de mejoras. Universidad de Palermo. Disponible en: https://dspace.palermo.edu/dspace/bitstream/handle/10226/2076/TESIS%20MBA%20GARC%c3%8dA%20CARRAL%20FINAL.pdf?sequence=1&isAllowed=y

Nebrada, P. (2022). El fraude en la industria telco. Alice. Disponible en: https://alicebiometrics.com/el-fraude-en-la-industria-telco/

Sacristán, L. (2023). El diccionario de las estafas telefónicas: qué son Phishing, Smishing, Vishing y Spoofing. Xataka móvil. Disponible en: https://www.xatakamovil.com/seguridad/diccionario-estafas-telefonicas-que-phishing-smishing-vishing-spoofing

Subex Limited (2021). ¿Qué es el fraude de suscripción? ¿Cómo abordar el fraude en las suscripciones de telecomunicaciones?. SUBEX. Disponible en: https://www.subex.com/article/que-es-el-fraude-de-suscripcion-como-abordar-el-fraude-en-las-suscripciones-de-telecomunicaciones/

Unión Internacional de Telecomunicaciones (2015). Aplicaciones y servicios con seguridad – Protocolos de seguridad. Capacidades técnicas de detección y respuesta al fraude para servicios con requisitos de alto nivel de seguridad. (Serie X). Sector de Normalización de las Telecomunicaciones UIT. Disponible en: https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1157-201509-I!!PDF-S&type=items