EVALUACIÓN DEL ESTADO ACTUAL DEL FRAUDE TELEFÓNICO REALIZADO A TRONCALES SIP Y/O PBX CONTRA USUARIOS Y PROVEEDORES DEL SERVICIO EN COLOMBIA

ANDRÉS FELIPE ECHEVERRY MORALES

TECNOLOGÍA EN TELECOMUNICACIONES

DIRECTOR(ES) DEL TRABAJO DE GRADO: ANDRÉS FELIPE BETANCUR

INSTITUTO TECNOLÓGICO METROPOLITANO

16 de Agosto de 2016

RESUMEN

Este documento contiene información teórica acerca de los fraudes cometidos a empresas que utilizan PBX o Troncales SIP; en el cual, se recopila información acerca de las modalidades de fraudes cometidos a las empresas y a los proveedores de servicio; se hace una aproximación a las cifras de incidencia, modalidades, intención del fraude y hábitos de seguridad de los usuarios.

La información se recolectó mediante una encuesta dirigida a usuarios de PBX y/o troncales SIP empresarial, residentes en Colombia, para el caso de los proveedores de servicio, se realizó una encuesta telefónica.

Los resultados demuestran que los fraudes realizados a troncales SIP y/o PBX empresariales en Colombia, no son un fenómeno aislado sino frecuente, y la mayoría se realizan cuando se activan las funciones de DISA. Generalmente, los actos fraudulentos se dan luego de haber realizado un mantenimiento. En muchas de las ocasiones, estos fraudes se realizan por infidelidad de los mismos empleados; la mayoría de las ocasiones se hacen con el fin de realizar llamadas de larga distancia nacional e internacional. Respecto a los hábitos de seguridad de los usuarios, se puede decir que, aunque existe una cultura de seguridad, aún hay muchos aspectos relevantes que fortalecer para garantizar un mayor nivel de seguridad, especialmente en el control de las personas que configuran o realizan mantenimiento al sistema. En cuanto a los proveedores de servicios, se pudo obtener poca información; sin embargo afirmaron que es un problema de importancia y que han sido víctimas especialmente de By Pass y Call back.

*Palabras clave***:** fraude telefónico, PBX, Trocales SIP, seguridad telefónica.

RECONOCIMIENTOS

Se agradece en primer lugar a la familia que siempre creyó en que este sueño se hiciera realidad y por su incondicional apoyo. A todos los docentes del ITM por sus asesorías y paciencia, especialmente al asesor **Andrés Felipe Betancur**, se agradece a todas las personas que participaron voluntariamente en esta encuesta y a la empresa UNE, Claro y Movistar por acceder a realizar la entrevista.

ACRÓNIMOS

CDR: Call Detail Record, o Registro Detallado de Llamadas.

IP: protocolo de internet.

ITSP: proveedor de Servicio de Telefonía por Internet.

LDI: llamadas a larga distancia internacional.

LDN: llamadas a larga distancia nacional.

RDSI: red digital de servicios integrados.

RTC: red de telefonía pública.

TABLA DE CONTENIDO

LISTA DE FIGURAS

1. INTRODUCCIÓN

Es importante hacer estudios acerca de los fraudes telefónicos realizados a empresas y a proveedores de servicio; pues, es una modalidad de robo que está en aumento, no sólo en el país sino en el mundo. Esto con el fin de identificar el *modus-operandi* de los delincuentes, y los hábitos de seguridad que adoptan los usuarios; para poder proponer estrategias de prevención y mitigar las pérdidas económicas que esto genera.

Por lo tanto, el objetivo general de este proyecto es evaluar el estado actual del fraude telefónico realizado a troncales SIP y/o PBX contra usuarios y proveedores del servicio en Colombia.

Esta evaluación, se propuso realizar a través de los siguientes objetivos específicos:

- Identificar la incidencia y tipologías de fraudes más usados contra usuarios y proveedores de servicio de troncales SIP y/o PBX.
- Determinar los hábitos de seguridad adoptados por los usuarios para evitar estos fraudes.
- Identificar las debilidades de seguridad que poseen las empresas prestadoras del servicio de SIP y/o PBX.
- Proponer estrategias de prevención para el usuario y a las empresas de telecomunicaciones que sirvan para mitigar el riesgo de estos delitos.

En este informe, se encontrará entonces el desarrollo, los resultados y las propuestas generadas en esta investigación.

En primer lugar se encuentra el marco teórico, donde se recopila información teórica acerca de los PBX, Troncales SIP, como qué son, cómo funcionan, cuáles son sus ventajas y sus vulnerabilidades principales. Además, se hará una contextualización acerca de los fraudes

realizados en estas tecnologías, tanto en Colombia como en el mundo; finalmente, en este capítulo, se encontrarán algunas recomendaciones teóricas para disminuir el índice de fraudes de este tipo.

Posteriormente, se encuentra el capítulo de metodología, donde se explica con precisión qué se hizo y a través de cuáles medios se recopiló la información. A continuación, en el capítulo de resultados y discusión, se presentarán gráficamente los resultados obtenidos en la encuesta, con su respectivo análisis; además se hará una descripción de los datos más relevantes aportados por las empresas prestadoras de este tipo de servicio y finalmente, se hará un listado de actividades que sirven para prevenir futuros fraudes, basados en los hábitos de seguridad de los usuarios y los datos aportados por los proveedores.

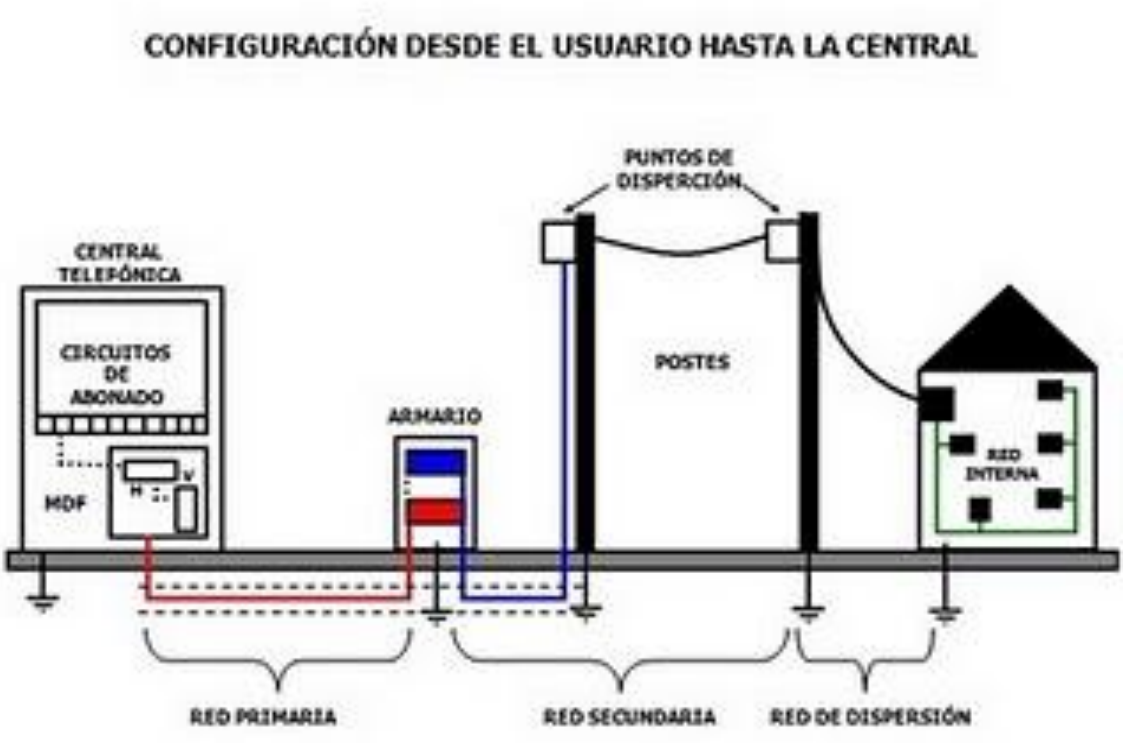
Para finalizar, se encontrarán las recomendaciones y conclusiones, donde se resumen los hallazgos de esta investigación y se proponen ideas para futuras investigaciones.

2. MARCO TEÓRICO

La telefonía es el medio de telecomunicación más antiguo y vigente; consiste en un servicio, que permite la transmisión de señales acústicas, (generalmente la voz), a través de señales eléctricas. Esta trasmisión de señales es posible debido a una línea telefónica, la cual consta de un circuito eléctrico, generalmente un cable físico que conecta el teléfono del usuario con la red de telecomunicaciones del proveedor de servicio; comúnmente, el usuario posee un número único, que funciona como una identificación, la cual sirve para recibir las llamadas y el cobro de factura, (Roca, 2000).

Desde su invención, a mediados del siglo XIX hasta la actualidad, el teléfono y su forma de funcionamiento ha evolucionado sucesivamente; en la actualidad se puede hablar de telefonía fija o convencional, telefonía móvil, telefonía satelital, RDSI o a través de banda ancha (ADSL, DDSL), entre otros, que han permitido una transmisión de datos con mayor velocidad, (Henríquez, 2012).

Figura 1. Línea telefónica.



Fuente: (Borbón, 2013).

En la figura anterior se muestra el funcionamiento y elementos necesarios para la conexión telefónica. Esta inicia en la central telefónica de alguna compañía, la cual conecta con un armario ubicado generalmente en un lugar público. Esta conexión del armario se dirige hacia diferentes puntos de dispersión, los cuales permiten enviar el servicio a un hogar o empresa del usuario final.

2.1. Telefonía PBX

El PBX o *Private Branch Exchange*, por sus siglas en inglés, traduce Central Secundaria Privada, o Ramal privado de conmutación, (Gomara, 2015). El autor, lo define como un sistema de telefonía que sirve para comunicarse vía telefónica dentro de una organización. Según explican Cascante y Guadamuz (2005) esta plataforma es una central telefónica conectada directamente a la red de telefonía pública, mediante líneas troncales, que permite

gestionar llamadas entrantes, salientes e internas, por lo que posee autonomía sobre otra central telefónica y de allí proviene el término privado.

En la actualidad El PBAX se convirtió en sinónimo de PBX, pues es la misma plataforma sólo que no necesita de un operador, sino que es automático y por su masificación, se adopta el término a esta última tecnología, (Gomara, 2015).

El PBX es entonces un ordenador físico dentro de una organización y el usuario es quien configura los parámetros de las llamadas entrantes, salientes e internas.

Actualmente, los PBX también pueden conmutarse a través de internet, (Redes LAN – WLAN), lo cual es denominado PBX IP, VoIP PBX o Voz IP, (Cascante y Guadamuz, 2005).

2.2. Troncales SIP (Protocolo de Inicio de Sesiones)

Es un protocolo diseñado para cumplir con las funciones de iniciación, modificación y finalización de sesiones interactivas de carácter multimedia; inicialmente se diseñó para que la telefonía fuera un servicio más prestado a través de internet; es decir, es un protocolo de señalización de IP, (Caramillo, 2002).

Según un informe presentado por IPCOM Network (2010), las troncales SIP son un servicio ofrecido por un proveedor de ITSP, que le permite a las organizaciones que tienen instalado un PBX, usar servicios VoIP por fuera del network de la compañía a través de la misma conexión a Internet.

2.3. Problemas de seguridad y fraudes

Los sistemas telefónicos en la actualidad, se han convertido en el objetivo de delincuentes informáticos; por lo cual, su vulnerabilidad a ataques delictivos, es alta. Estos delincuentes buscan errores en los sistemas para acceder a información, robar consumo telefónico e incluso realizar llamadas fraudulentas o extorsivas. En muchas ocasiones, los actos ilegales

son llevados a cabo por técnicos externos contratados por el usuario, que, al carecer de conocimientos básicos de los procedimientos no se percatan de lo que éstos realizan, (Sandoval, 2008).

Según el autor, las estadísticas señalan que por cuenta de la actividad ilegal de la manipulación del fraude telefónico, las empresas de telecomunicaciones colombianas han perdido 974.880 millones de pesos entre el año 2000 y 2007, mientras que Medellín, Cali y Bogotá son las ciudades con mayor índice de fraudes.

Un fraude puede definirse como un engaño que se realiza eludiendo obligaciones legales o usurpando derechos con el fin de obtener un beneficio; afectando a los operadores de telecomunicaciones, usuarios y prestadores de servicio; el cual genera una pérdida de ingresos e imagen para las empresas, tanto para el comprador como proveedor, (UNE, 2010).

El fraude reduce las ganancias, afecta a los clientes y a la eficiencia operacional y el impacto real escasamente se cuantifica, por lo cual, reduce la visibilidad de la eficiencia de las medidas y acciones de seguridad y prevención, principalmente, porque compromete la imagen de las compañías que ofrecen los servicios de telecomunicaciones, (Gallardo, 2006).

Los fraudes pueden clasificarse de diferentes formas; sin embargo, se tomará la clasificación presentada por Gallardo (2006) para el caso de fraudes en la telefonía:

I. ***Fraudes realizados por terceras personas donde la víctima es el usuario o cliente final:***

- Manipulación de armarios y robo de líneas telefónicas: acceso ilegal al armario o a los cables físicos de la línea para realizar llamadas.
- Manipulación de PBX: acceso remoto o local sin autorización para acceder a información confidencial o realizar llamadas fraudulentas.

• Llamadas no autorizadas mediante el uso de tarjetas: uso de códigos de tarjetas públicas o privadas para realizar llamadas fraudulentas.

• Generación de llamadas mediante engaños: generalmente son llamadas internacionales realizadas engañosamente, que no son aclaradas a quien se le cobrará posteriormente.

II. Fraudes realizados por terceras personas donde la víctima es el proveedor del servicio:

• Fraude en teléfonos públicos: dañar, alterar técnicamente o eludir el pago de llamadas en estos teléfonos.

• Pagos fraudulentos: pagos de facturas y/o consumo del defraudador de manera fraudulenta.

• Fraude de suscripción: solicitud de servicios con identidades y/o información falsa y así evitar el pago de la factura.

• Ingeniería social: engaño a personas para que cometan el acto fraudulento sin que lo sepan.

III. Fraude donde intervienen otros operadores (legalmente establecidos o no) donde las víctimas son las empresas de telefonía:

• Callback o re-origen: generalmente, mediante un ordenador, los delincuentes hacen que la llamada se re-origine; es decir, ellos son los que llaman inicialmente, sin embargo, la llamada se devuelve como si se hubiera originado en el verdadero lugar de destino, a quien será cobrada la llamada internacional.

• Refilling o re-enrutamiento: la llamada internacional es enrutada hacia un tercer país, donde se re-enruta hacia el destino final.

• By pass.

Según varios autores como UNE (2010) y Gallardo (2006), la modalidad de Bypass es la más frecuente en el sector de la telefonía y consiste en encaminar el tráfico de una llamada entrante de un país externo directamente a las centrales telefónicas locales, (generalmente sin licencia de operación); por lo cual, no pasan por la central telefónica internacional; esto se traduce en el cobro de la llamada como si fuera local.

A continuación, se muestra una figura con el funcionamiento de esta modalidad.

Figura 2. Funcionamiento de fraude By Pass internacional.

Fuente: (Hinojosa y Béjar, 2012, pág. 3)

En la figura anterior se observa el funcionamiento del fraude By pass internacional, en el cual se aprecia que un usuario A en un país X realiza una llamada, la señal pasa por el operador telefónico de ese país, luego a internet y llega a una central telefónica no autorizada que la convierte en una llamada local en el país Y y el operador de telefonía local transfiere la llamada al usuario B siendo entonces cobrada como llamada nacional.

Así como el tráfico de llamadas, la demanda de telefonía también está en aumento y en conjunto con esto, los actos fraudulentos y aunque existen protocolos de seguridad como se verán a continuación, y las empresas han tomado medidas, las fallas de seguridad son tanto de los proveedores del servicio como de los usuarios finales.

2.3.1. Los proveedores:

Las compañías de telecomunicaciones ofrecen un protocolo de seguridad básico, el cual se basa en detecciones automáticas de anomalías y configuración de los servicios, los cuales se pautan y fijan para cada servicio, mediante un contrato escrito. Internamente poseen seguridad para garantizar eficacia y eficiencia en el servicio y posee a su vez, autoridad para restringir y/o bloquear un servicio si considera algún riesgo o un mal uso y debe notificar a los operadores del riesgo y al cliente para que verifique su planta o central, si es el caso. Igualmente, en caso de ser necesario, puede disponer de visitas técnicas acordadas con el cliente para supervisar el uso y adecuado funcionamiento del servicio, (Lozoya, 2013).

Aunque las Troncales, PBX y demás servicios de telefonía posean un plan ilimitado, se pueden evidenciar riesgos de fraudes por el desmesurado flujo en llamadas, marcaciones a destinos considerados alto riesgo (tarificación), o altos consumos; a través de CDR. Cada proveedor posee sistemas de pruebas automáticos y manuales que monitorean y controlan el tráfico para identificar fallas fraudulentas. Se determina entonces el tipo de falla de seguridad y si es por parte del usuario se les notifica para que revise su configuración.
En el caso de troncales SIP, se bloquean preventivamente, se informa al usuario y se procede a realizar las acciones necesarias; para el caso de PBX, es el usuario el responsable de su seguridad; sin embargo, las empresas deben responsabilizarse en caso de tarificación y violación de sus sistemas de seguridad, (Lozoya, 2013). Según afirma el autor, en cualquier caso, es responsabilidad de la empresa, informar al usuario sobre posibles fraudes y tráficos o consumos sospechosos.

2.3.2. Los usuarios:

El error más común de los usuarios es el acceso y uso indebido de sus plataformas debido a sus desconocimientos, por lo que se ven obligados a contratar técnicos para su manipulación. Los fraudes son generados por fallas en su programación y en ocasiones por desconocimiento de las funciones del sistema, que facilitan al defraudador acceder remotamente y realizar llamadas de larga distancia (LDN, LDI) o a teléfonos móviles, (UNE, 2010).

Los fraudes son realizados para obtener beneficios a través de la reventa de minutos, el enrutamiento y terminación de Tráfico LDN o LDI; la utilización del servicio de telefonía local, el acceso a las líneas 900 y 901 (Premium) y llamadas a móviles, (Hinojosa y Béjar, 2012).

Aunque existen pocas cifras y un alto sub registro sobre este tipo de fraudes, Flórez (2004) publica que, en Colombia, anualmente se pierden 300.000.000 de pesos por fraudes en las telecomunicaciones.

Por su parte, Gallardo (2006) afirma que, se reporta la existencia de empresas ilegales; las cuales, mediante la implementación de un centro de atención telefónica falso demuestran a un operador de telefonía fija su necesidad de líneas telefónicas, presentando documentación falsa, como datos de contacto, identificaciones y certificados de Cámara de Comercio.

2.4. Recomendaciones para prevenir fraudes en sus sistemas telefónicos:

Funcionalidad DISA (Direct Inward System Access): esta opción permite realizar llamadas desde el sistema telefónico accediendo desde una línea externa de la empresa. Esta funcionalidad puede ser muy riesgosa si no se tiene una buena programación y políticas de seguridad para su uso, sino se cuenta con esto es muy probable que se presenten problemas

de fraude, dado que queda abierta la posibilidad que cualquier persona que conozca el manejo o los códigos de acceso a troncales del sistema, puede realizar llamadas que serán cobradas a la empresa.

Para poder utilizar esta funcionalidad, los sistemas tienen códigos por defecto, que deben ser cerrados o habilitarse con códigos personalizadas para que los usuarios autorizados por la compañía puedan realizar este tipo de llamadas, por lo que las posibilidades del fraude están dadas por inadecuada definición de políticas de códigos secretos sobre el sistema:

- No obligación de cambio de clave cada determinado tiempo, claves genéricas, fuga de Información por parte de los empleados, administradores del sistema y/o personal de manteniendo de la misma, que realizan un mal uso de la información compartiendo las claves y accesos.

- Ingeniería social: es la práctica de obtener información confidencial a través de la manipulación de usuarios. Es el arte de sacar información de fuentes humanas.

- Buzones de Voz (Voice Mail) la herramienta de habilitar casilleros para mensajes de voz, ofrece, además de eficiencia en las comunicaciones de una empresa, servicio para sus clientes. Desafortunadamente, los buzones son usualmente atacados por los defraudadores, debido a que esta funcionalidad permite en algunos casos realizar llamadas de regreso (call back) al número telefónico que dejó el mensaje. Estas llamadas pueden ser locales, de larga distancia nacional o internacional o a teléfonos móviles. Sin una correcta programación, alguien se podría apoderar de los buzones de voz cambiándoles las claves de acceso originales.

- 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.

Algunos de las opciones más utilizadas por los defraudadores son:
0, * 0, # 9, * 9, * 90 #, # 1234 #, * 83.

- Re-direccionamiento de extensiones de empleados a destinos móviles, larga distancia nacional e internacional con cargo a la empresa. Este fraude, por lo general se hace con complicidad de personal que tiene acceso a los recursos de la empresa, direccionando su teléfono a un destino de larga distancia nacional, internacional o móvil para la realización de llamadas de terceros a estos destinos.

- Mantenimientos remotos. Algunos proveedores realizan la configuración del sistema por vía telefónica o remota. Este es un procedimiento normal, pero en algunos casos el modem que se activa para este fin no es apagado en el momento de finalizar la programación quedando el riesgo de que el personal técnico, con este conocimiento, continúa entrando a la planta y realiza llamadas o cambios en la configuración para su beneficio. Este tipo de casos también se presentan a través de mantenimiento o soporte virtual (acceso a través de las redes de Internet o corporativas, VPN, etc.)

IVR (Interactive Voice Response). Es una poderosa plataforma de desarrollo de aplicaciones telefónicas, que permite diseñar, integrar, implementar y administrar sistemas de respuesta interactiva de voz. Viene preparada para manejo de voz, fax, acceso y escritura a bases de datos vía ODBC o sockets, reconocimiento de voz, texto a voz y aplicaciones CTI entre otras. Así mismo, soporta E1/T1/ISDN, VoIP, entre otros. Es utilizado en empresas corporativas, bancos, casas de bolsa, universidades y gobierno entre otros, para automatizar la atención

telefónica. Tiene capacidad para atender miles de llamadas al día, permitiendo a sus clientes recibir información, consultar y modificar bases de datos, vía telefónica y transferirse con una persona, cuando así lo requieran.

- Para este tipo de sistema el fraude requiere de un grado de experticia mayor.

- Existen otros sistemas como las Automatic Attendant, el cual recibe las llamadas de manera automática con un mensaje pregrabado y dirige la llamada a la extensión solicitada. los IVM, que son equipos básicamente iguales a los descritos.

2.5. Actividades para prevenir fraudes:

- No active funciones del PBX que no vaya a utilizar, por ejemplo, DISA, buzones de voz, desvío de llamadas y acceso a servicio de operadoras.

- Defina categorías, políticas internas y niveles de acceso para cierto tipo de llamadas (LDN, LDI, móviles).

- Configure su sistema para no permitir acceder a tono de discado bajo ninguna circunstancia (marcación en 2 etapas).

- Elimine o bloquee los buzones de voz que no estén en funcionamiento.

- Recomiende a sus empleados cambiar la clave de los buzones de voz.

- Cuelgue cuando reciba llamadas con anuncios en un lenguaje extranjero.

- Tenga precaución con cualquier sistema de recepción automática de llamadas incluyendo aquellas que han estado integradas a su red de datos (consola automática, IVR, IVM, correo de voz con mensajería unificada).

- No conecte llamadas entrantes solicitando las extensiones 151-159, 171-179 y 191-199.

- Antes de aceptar asesoría y soporte para probar o configurar su sistema telefónico por parte de personas que dicen pertenecer a las compañías telefónicas, solicite una identificación, indague por el número de la orden de servicio o valide con la compañía telefónica respectiva.

- Pregunte a su proveedor por el modo nocturno de su planta para evitar llamadas fuera del horario laboral.

- Maneje los manuales de configuración del PBX como documentos a los que solo debe tener acceso personal autorizado.

- Establezca con su proveedor fecha y horas específicas para el mantenimiento remoto de su sistema y confirme que el modem utilizado para el mantenimiento a distancia o remoto sea apagado o bloqueado en el momento de finalizar el trabajo.

- Incluya en los contratos de instalación y mantenimiento del sistema con terceros, cláusulas de responsabilidad por casos de fraude o cambios no acordados.

- Vigile y compruebe el trabajo de los técnicos durante y después de los trabajos de mantenimiento.

- Realice un control y seguimiento de los mantenimientos, reprogramaciones o cambios al sistema, llevando fecha, hora y detalle de las modificaciones.

- Revise la facturación periódicamente apoyándose en los reportes internos del sistema y comparándolos con la facturación de las empresas telefónicas.

- Pida a su proveedor orientación sobre lo que deben conocer sus empleados y lo que no deben conocer del funcionamiento del PBX.

3. METODOLOGÍA

Inicialmente, se realizó una búsqueda y selección de fuentes secundarias sobre el tema, y aspectos técnicos de la telefonía SIP como informes, artículos, publicaciones, estadísticas, entre otros; entre los que se destacan informes presentados por UNE y Supertel. Posteriormente, se diseñó una encuesta en la herramienta Formularios de Google Drive, dirigida a organizaciones que hacen uso de PBX y/o troncales SIP, a quienes se les interrogó acerca de hábitos de seguridad, incidencia de fraudes o intento de ellos, los medios usados y formas en que éstos han logrado evitar un fraude; igualmente, se diseñó otra encuesta, en la misma herramienta, dirigida a empresas proveedoras de estos servicios, donde se les interrogó acerca de incidencia de fraudes, tipologías, estimación de pérdidas, medidas que toman para evitarlos o afrontarlos, entre otros. Estos datos se compararon con los estudios publicados con el fin de caracterizar a Colombia en el contexto global y posteriormente, proponer estrategias de prevención basándose en los resultados de los hábitos de seguridad de los usuarios y debilidades de las empresas. Las encuestas se realizaron mediante correo electrónico y los resultados se tabularon y graficaron en Microsoft Office Excel 2013. Se realizaron 210 encuestas a usuarios y 3 a empresas proveedoras del servicio por vía telefónica.

4. RESULTADOS Y DISCUSIÓN

A continuación, se presentan los resultados de las encuestas realizadas a 210 empresas que utilizan troncales SIP y/o PBX como telefonía empresarial.

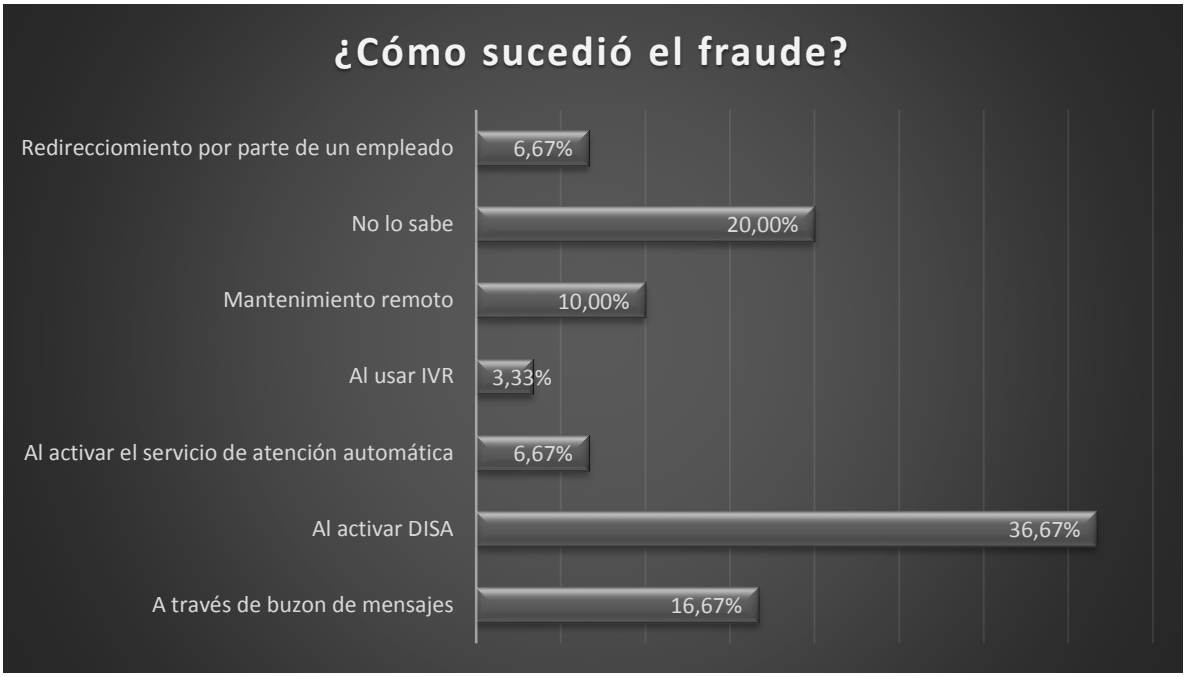
4.1. Incidencia y tipología de fraudes ocurridos a usuarios

Figura 3. Incidencia de fraude telefónico en empresas

Fuente: propia

El 55,55% del total de empresas encuestadas, afirma que no ha sido víctima de ningún tipo de fraude telefónico; por su parte, el 21,21% asegura no saber o no tener certeza, lo cual es un nivel alto y es necesario ponerle atención y el 24,24% afirma haber sido víctima al menos una vez.

Figura 4. Modalidades de fraude telefónico en empresas



Fuente: propia

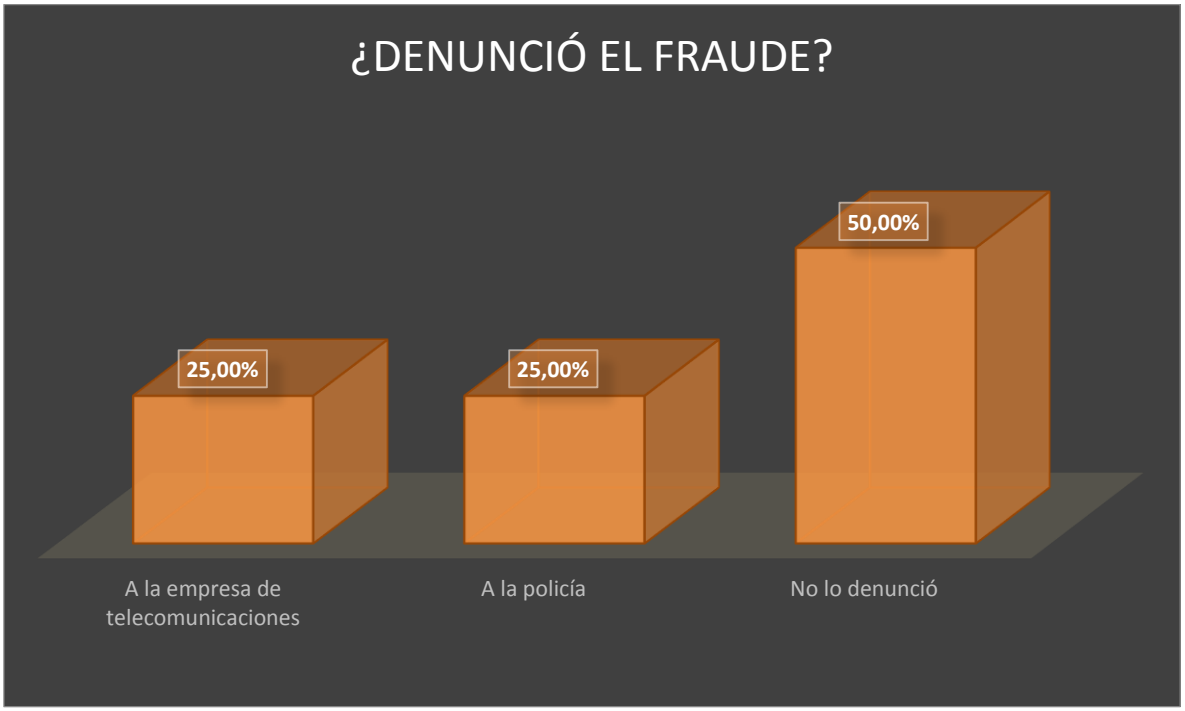
Del 24,24% del total que afirmó haber sido víctima, el 36,67% dijo que el fraude se cometió a través de DISA y el 20% no lo sabe, lo cual nos indica que existe un alto nivel de desconocimiento de cómo funciona la telefonía empresarial por parte de los usuarios. El 16,67% afirmó que fue a través del buzón, y en menor medida se encuentra el re-direccionamiento por parte de un empleado o al activar la atención automática, (6,67% cada uno). Finalmente, con un 3,33% los fraudes se realizaron al usar IVR.

Figura 5. Proveedores de las víctimas

Fuente: propia

Respecto a las empresas proveedoras, UNE es la proveedora con mayores casos de fraude, (64,52%), seguida por la empresa Movistar, con un 19,35% de incidencia de los casos de fraude. El resto pertenece a otras empresas.

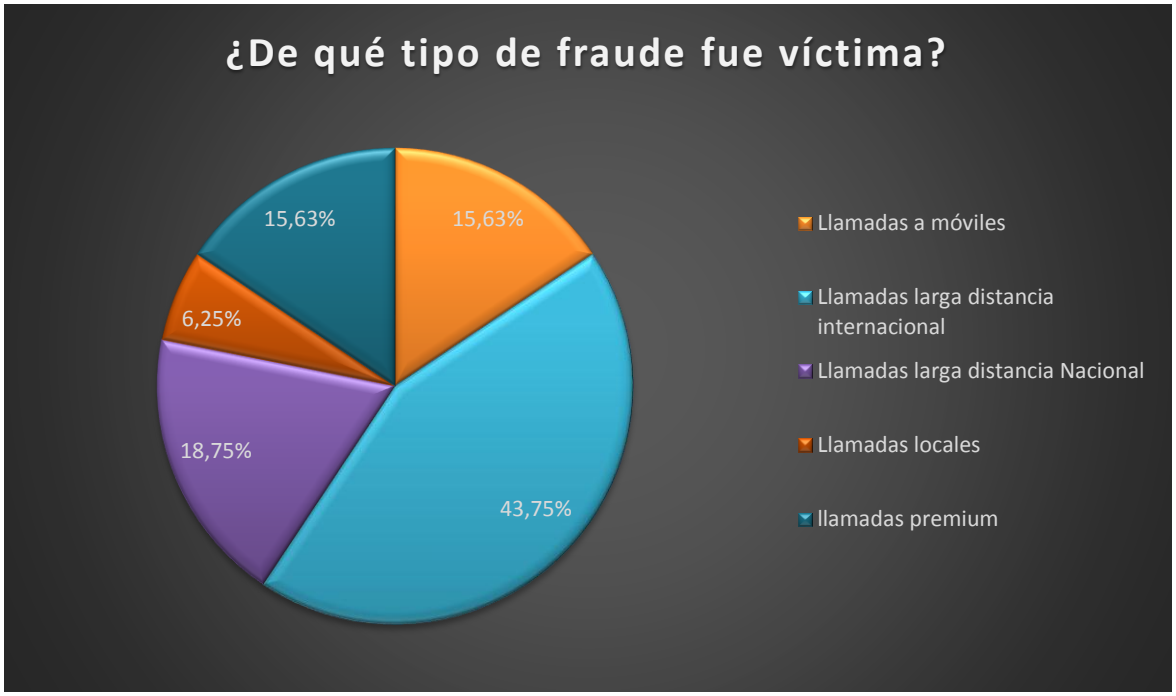
Figura 6. Denuncias de fraude



Fuente: propia

Se evidencia y es alarmante que el 50% de las personas víctimas de fraude no lo denunciaron; mientras que la mitad de las personas que sí lo hicieron fue a la empresa proveedora del servicio y el otro 25% a la policía. Esto demuestra que no existe una cultura de denuncia, lo que facilita el accionar delictivo a causa de la impunidad y genera sub-registros.

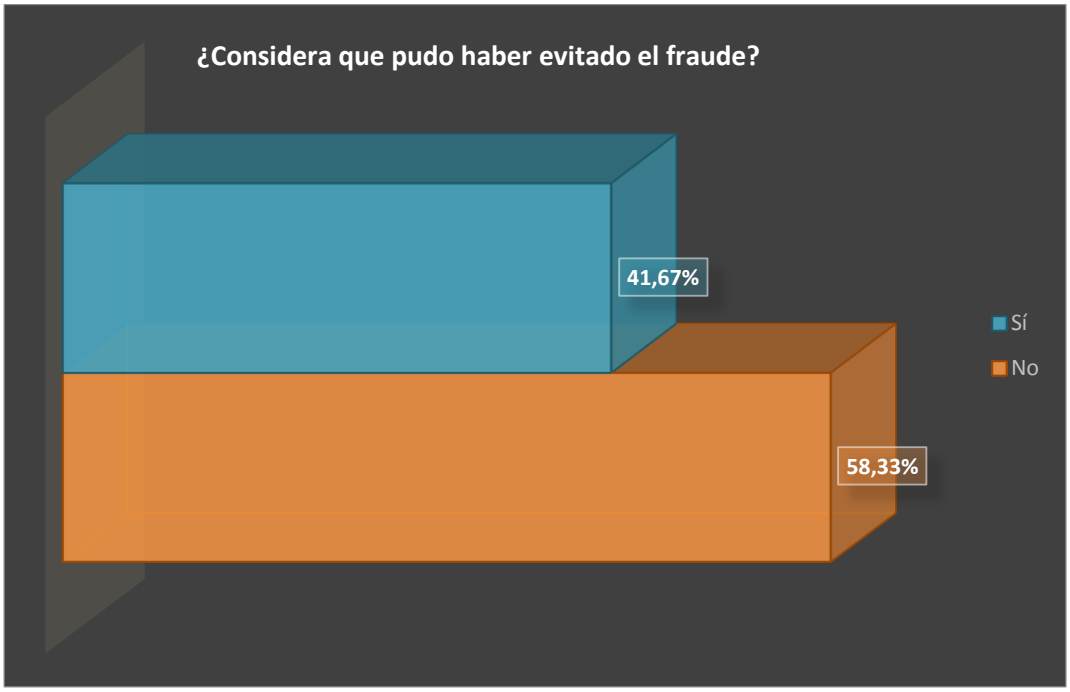
Figura 7. Tipo de fraude



Fuente: propia

En cuanto al tipo de fraude, la mayoría fueron víctimas de llamadas a larga distancia internacional, con un 43,75% de participación; seguida por llamadas a larga distancia nacional, (18,75%); posteriormente con un 15,63% cada uno se encuentran las llamadas Premium y a móviles y finalmente las llamadas locales. Por lo anterior, se infiere que, la mayoría de los delincuentes buscan satisfacer necesidades de llamadas LD.

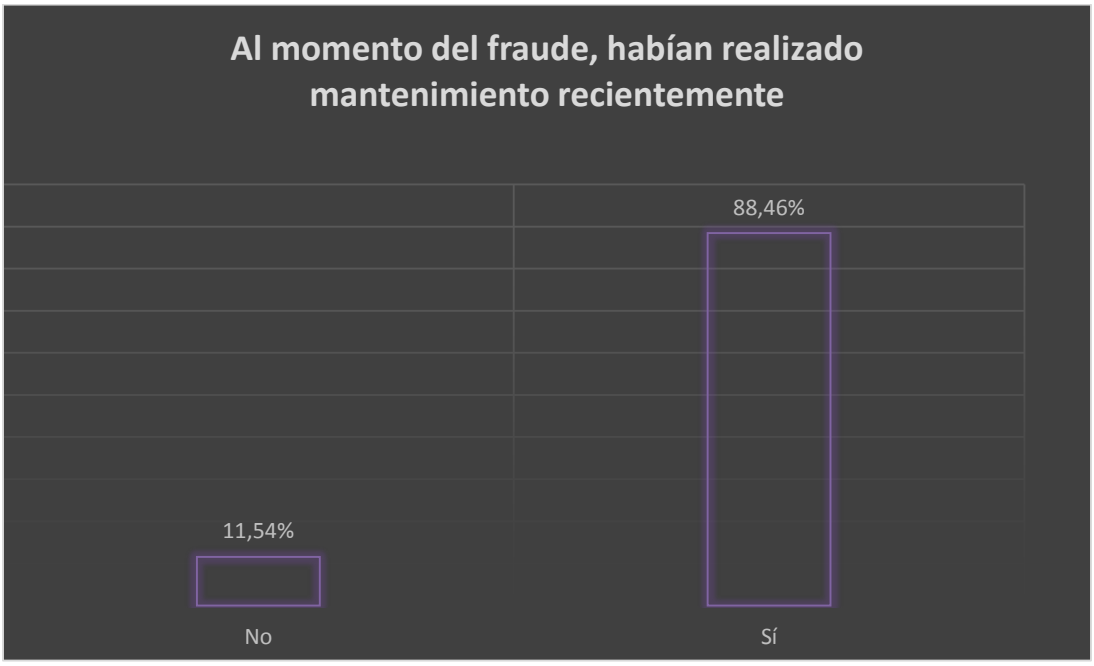
Figura 8. Percepción sobre evitar el fraude



Fuente: propia

El 58% de las víctimas considera que bajo ninguna circunstancia pudo haber evitado el fraude, mientras que el 41,67% considera que sí, mediante hábitos o medidas de seguridad que no adoptaron; lo que demuestra que, existe un alto nivel de conciencia en la importancia de implementar hábitos de seguridad, sin embargo, los esfuerzos no son suficientes.

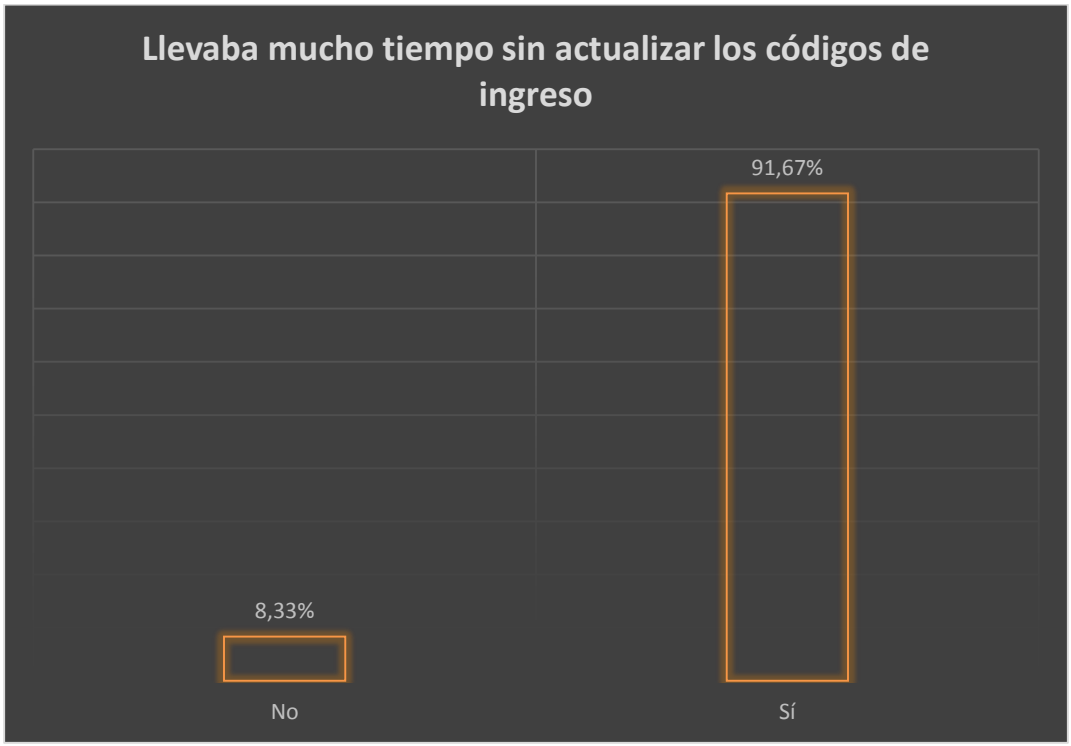
Figura 9. Circunstancias al momento del fraude: mantenimiento



Fuente: propia

En el 88,46% de los casos de fraude, se había realizado mantenimiento recientemente, lo cual demuestra que, o el técnico está involucrado en el fraude, o luego del mantenimiento no se configuran adecuadamente las medidas de seguridad; por lo cual, es un momento al que es necesario poner especial atención.

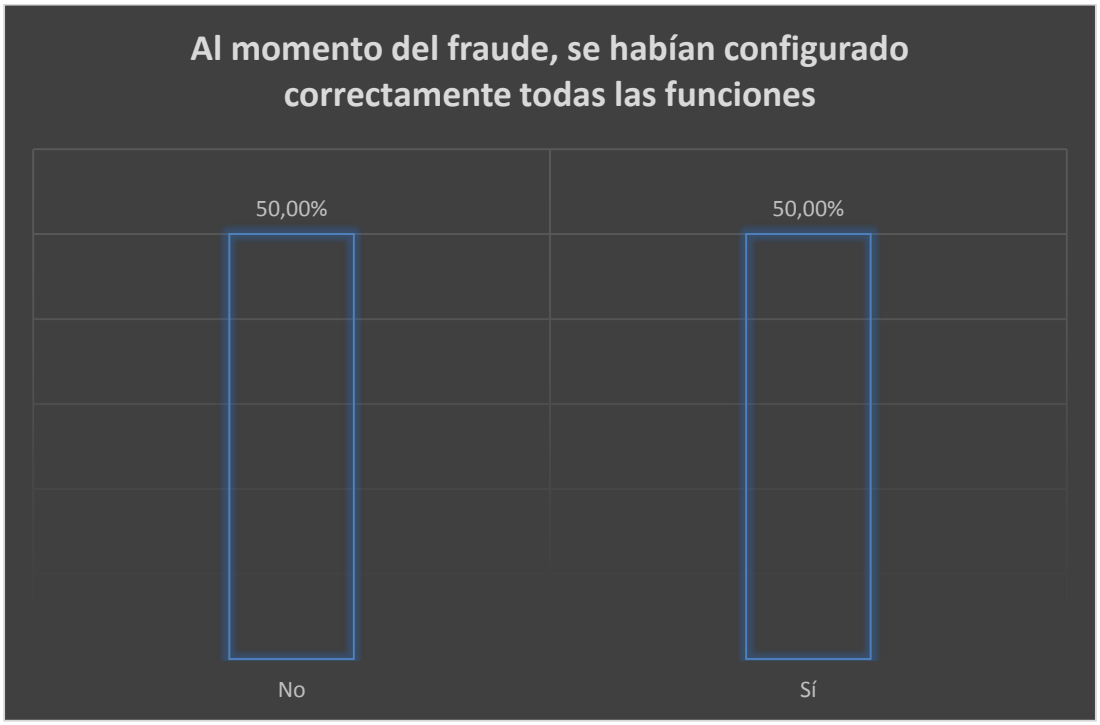
Figura 10. Circunstancias al momento del fraude: códigos de ingreso



Fuente: propia

Otra de las medidas no adoptadas por los usuarios víctimas de fraude es la actualización constante de las claves de acceso; pues el 91,67% afirma no haberlas cambiado durante mucho tiempo en el momento del fraude; lo que demuestra la importancia de este hábito de seguridad.

Figura 11. Circunstancias al momento del fraude: configuración

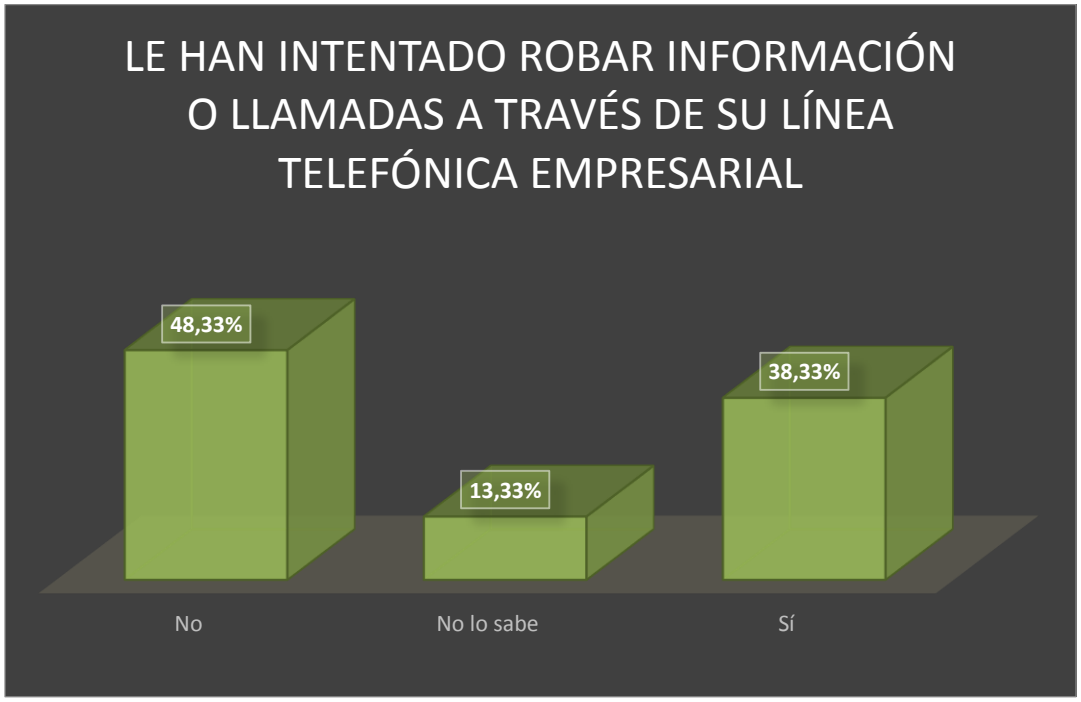


Fuente: propia

El 50% de los usuarios, aseguró haber tenido correctamente las configuraciones de seguridad de su servicio telefónico al momento del fraude; en funciones como buzón de mensajes, IVR, modo nocturno, DISA, etc; por su parte, el otro 50% aseguró no haberlo hecho.

4.2. Incidencia de intentos de fraude a usuarios

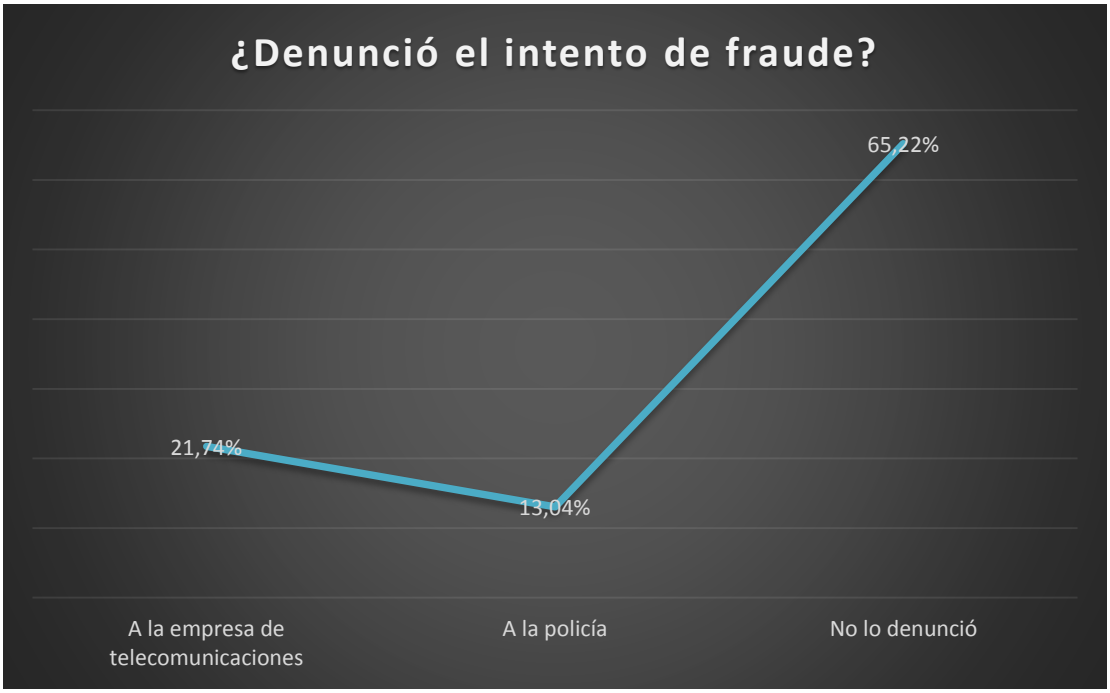
Figura 12. Incidencia de intento de fraude



Fuente: propia

Al 41,22% de las personas encuestadas que aseguraron no haber sido víctimas o no estar seguros, se les preguntó si les habían intentado realizar un fraude; a lo cual el 48,33% afirma que no, el 13,33% no lo sabe y el 38%33 afirma que sí le han intentado robar a través de sus líneas telefónicas.

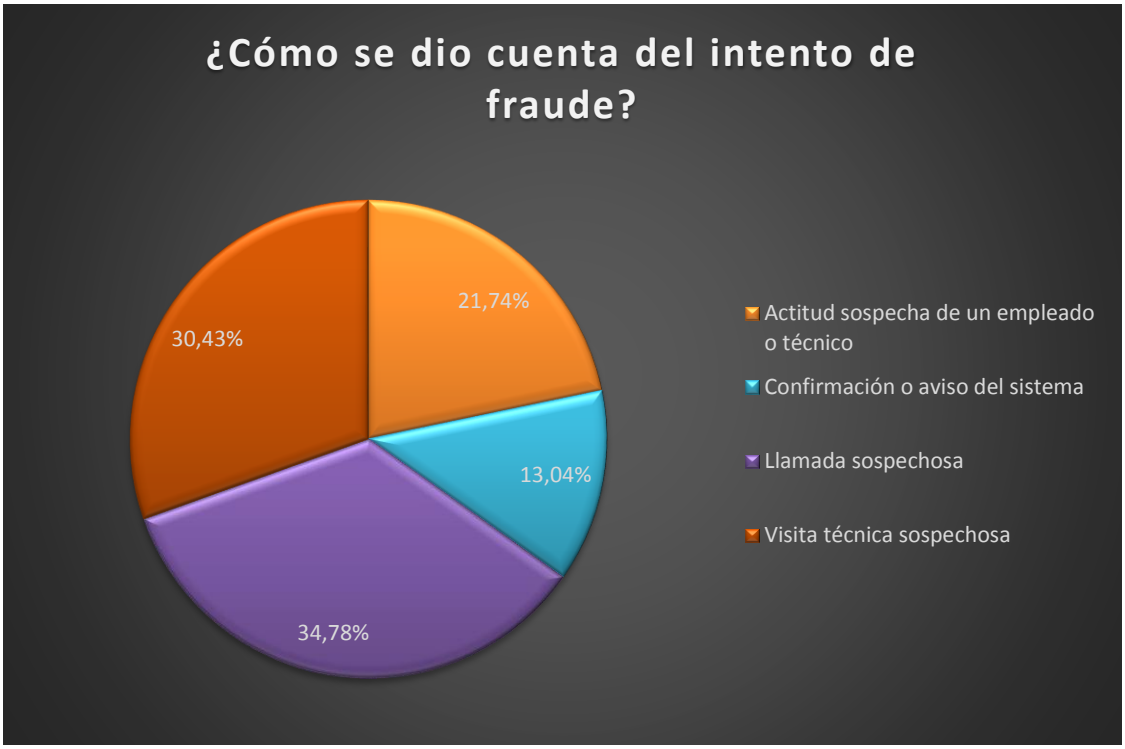
Figura 13. Denuncias de intento de fraude



Fuente: propia

El 62,22% de las personas que afirmaron que les habían intentado hacer un acto fraudulento, no denunciaron; mientras que el 13,04% lo denunció a la policía y el 21,74% lo reportó en la empresa proveedora del servicio. Es evidente que las personas no poseen un hábito de denuncia.

Figura 14. Advertencia de intento de fraude

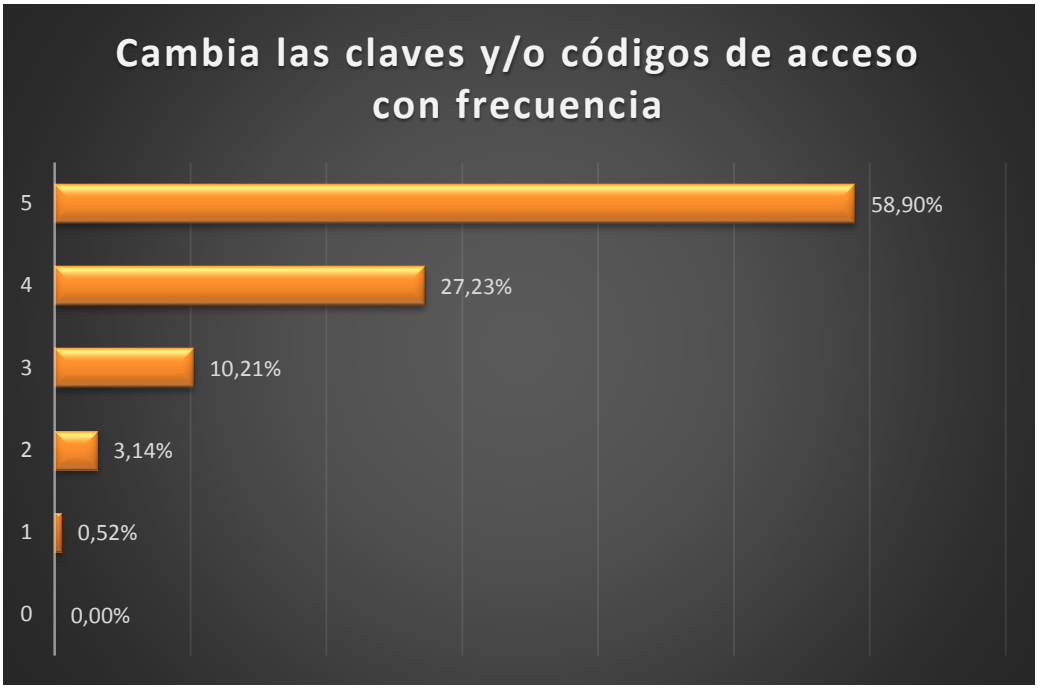


Fuente: propia

El 34,78% de las personas que evitaron el fraude, se percataron de esto por medio de una llamada sospechosa; mientras que el 30,43% lo hizo a través de una visita o asistencia técnica. Por su parte, el 21,74% se dio cuenta por la actitud sospechosa de un técnico y/o empleado y sólo el 13,04% fue por el mismo sistema de seguridad; estos datos sugieren que las llamadas sospechosas son un método usado frecuentemente pero no necesariamente exitoso; mientras que el sistema de seguridad propio del servicio no detecta gran cantidad de fraudes, lo que traduce que los delincuentes lo realizan suplantando identidades o a través de ingeniería social para pasar desapercibidos ante el sistema.

4.3. Hábitos de seguridad de los usuarios

Figura 15. Hábitos de seguridad: claves y códigos



Fuente: propia

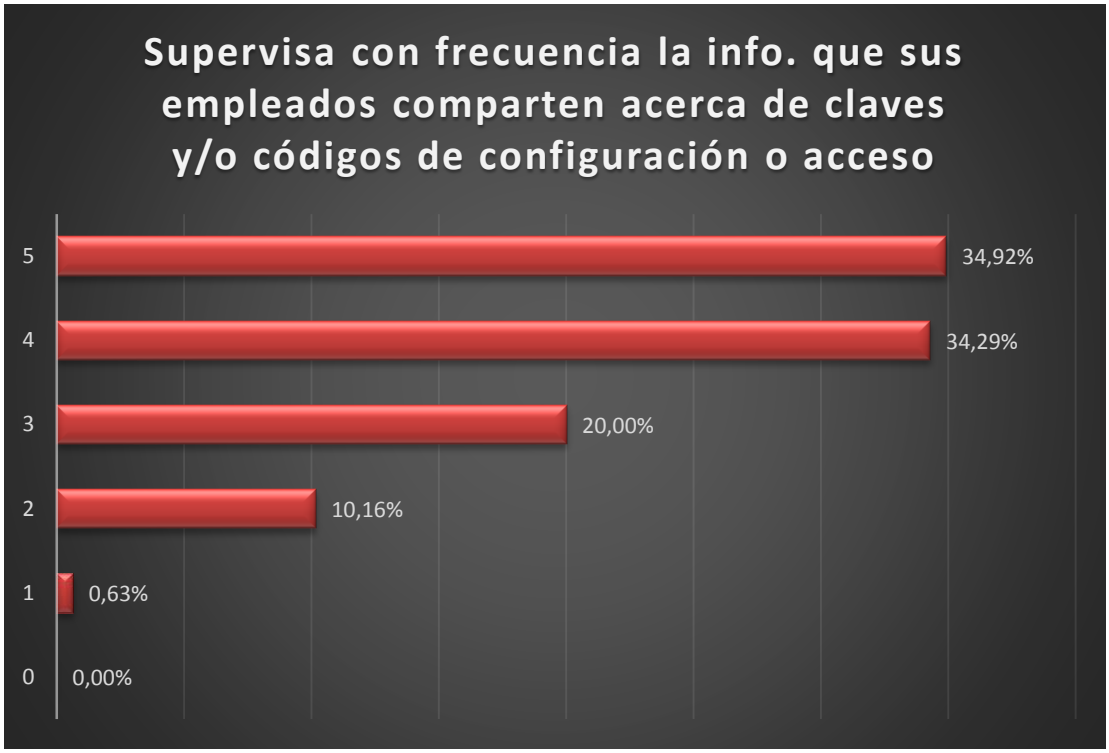
Respecto a los hábitos de seguridad, se encuentra que el 58,90% de los encuestados, dio una calificación de 5 (muy frecuentemente) frente al cambio de códigos de acceso; el 27,23% dio una calificación de 4 (frecuentemente); el 10,21% con calificación de 3 afirma hacerlo de vez en cuando y el 3,66% afirmó hacerlo escasamente y casi nunca. Esto demuestra que aunque no todas las empresas realizan este importante hábito de seguridad con la frecuencia adecuada, existe un alto nivel de adopción de cambio regular de claves.

Figura 16. Hábitos de seguridad: visitas o asistencias técnicas

Fuente: propia

Respecto a las visitas y/o asistencias técnicas, el 31,91% afirmó validar la identificación y autorización del proveedor del servicio siempre, (calificación 5); seguida por casi siempre (26,60%); sin embargo, el 19,15% lo hace escasamente, el 2,13% nunca lo confirma y el 8,51% casi nunca. Estos datos demuestran que falta mucha adopción de este hábito de seguridad, pues sólo algunas empresas se preocupan realmente de quién es la persona que le brinda asistencia técnica y tiene acceso a su información y configuración.

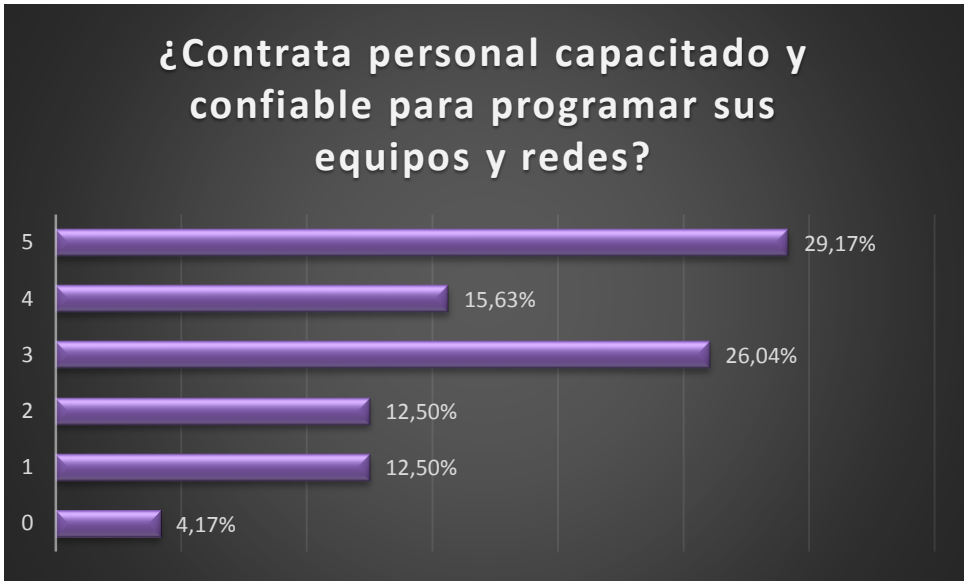
Figura 17. Hábitos de seguridad: supervisión de fuga de información interna



Fuente: propia

Se evidencia que la mayoría de los usuarios poseen un hábito alto en cuanto a la supervisión de la información que sus empleados comparten, (34,92% muy frecuentemente y 34,29% frecuentemente). Esto es un buen indicador ya que la fuga de información tanto entre la misma organización como fuera de ella es determinante en cuanto al nivel de seguridad que ésta posee.

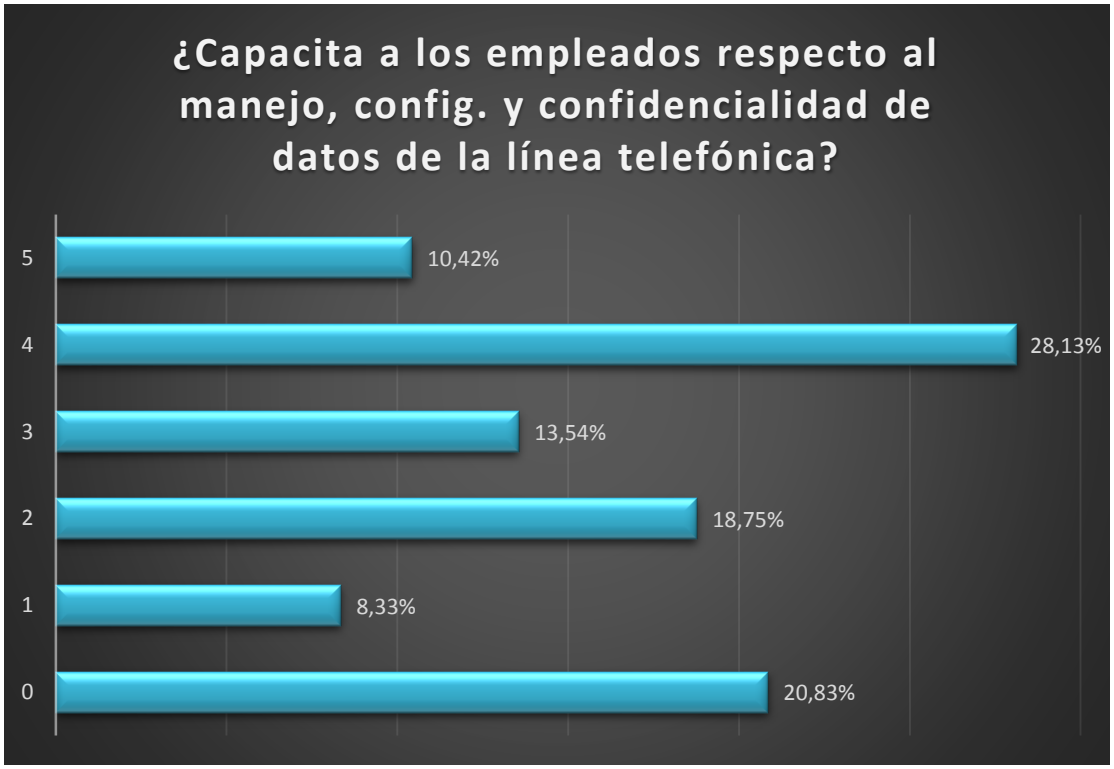
Figura 18. Hábitos de seguridad: personal de programación y revisión



Fuente: propia

Aunque el 29,17% de las empresas afirmó contratar personal capacitado y confiable para programar sus equipos y redes, hay muchas empresas que dieron una calificación baja a este nivel, un total de 29,17% entre 0 y 2. Por su parte, el 26,04% afirmó hacerlo en un nivel medio (3). Esto traduce que hace falta un fortalecimiento en este tipo de hábito de seguridad, el cual es sumamente importante ya que mediante la programación es como se fuga fácilmente la información y se puede programar el nivel de acceso de los usuarios.

Figura 19. Hábitos de seguridad: capacitación a los empleados



Fuente: propia

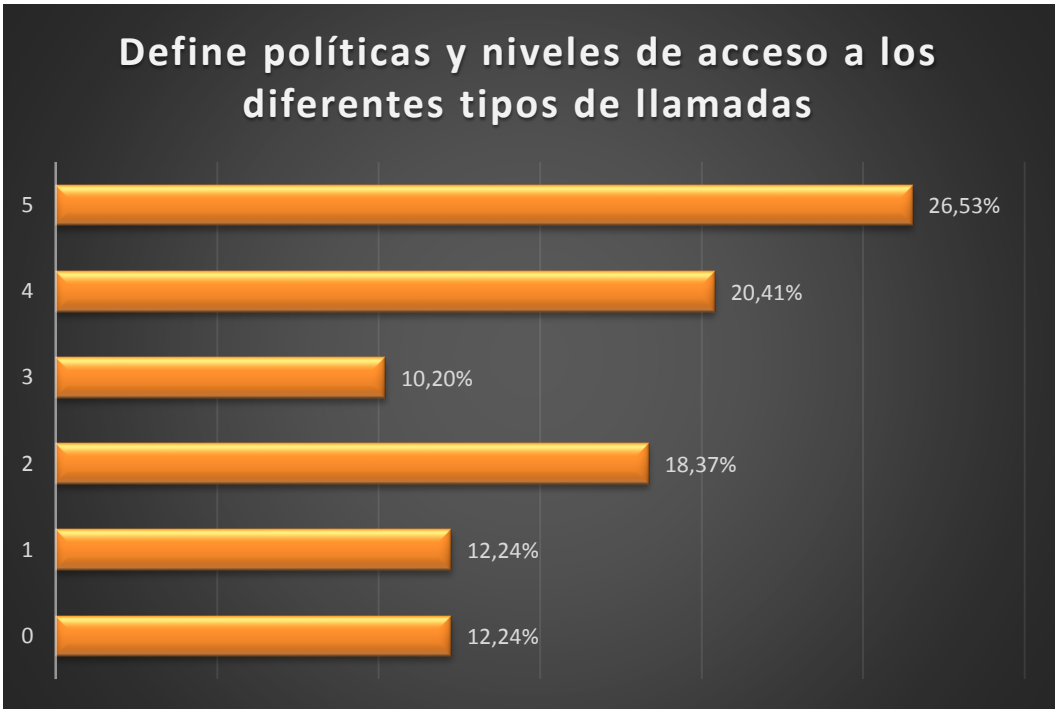
El 28,13% de las empresas, afirmó que brindaba capacitación concerniente a la seguridad, configuración y manejo de la línea telefónica acorde a sus funciones de manera frecuente; sin embargo el 28,83% nunca lo hace, y alrededor del 49% lo hace en un nivel medio - bajo, entre 3 y 1. Este tipo de hábito, según los datos obtenidos, es necesario fortalecerlo en las políticas de seguridad empresarial, ya que no se presenta en el grado que debería para garantizar la seguridad necesaria.

Figura 20. Hábitos de seguridad: revisión de facturación

Fuente: propia

En general, se evidencia que existe una cultura de revisión de facturas telefónicas, lo que permite conocer detalladamente el consumo y uso de éstas; además de comparar con meses anteriores lo que puede ayudar a identificar irregularidades y posibles fraudes. Más de la mitad de las organizaciones afirmaron hacer esta práctica todos los meses o casi todos los meses (calificación de 5 y 4); por su parte, el 12,24% no lo hace y el 8,16% ocasionalmente.

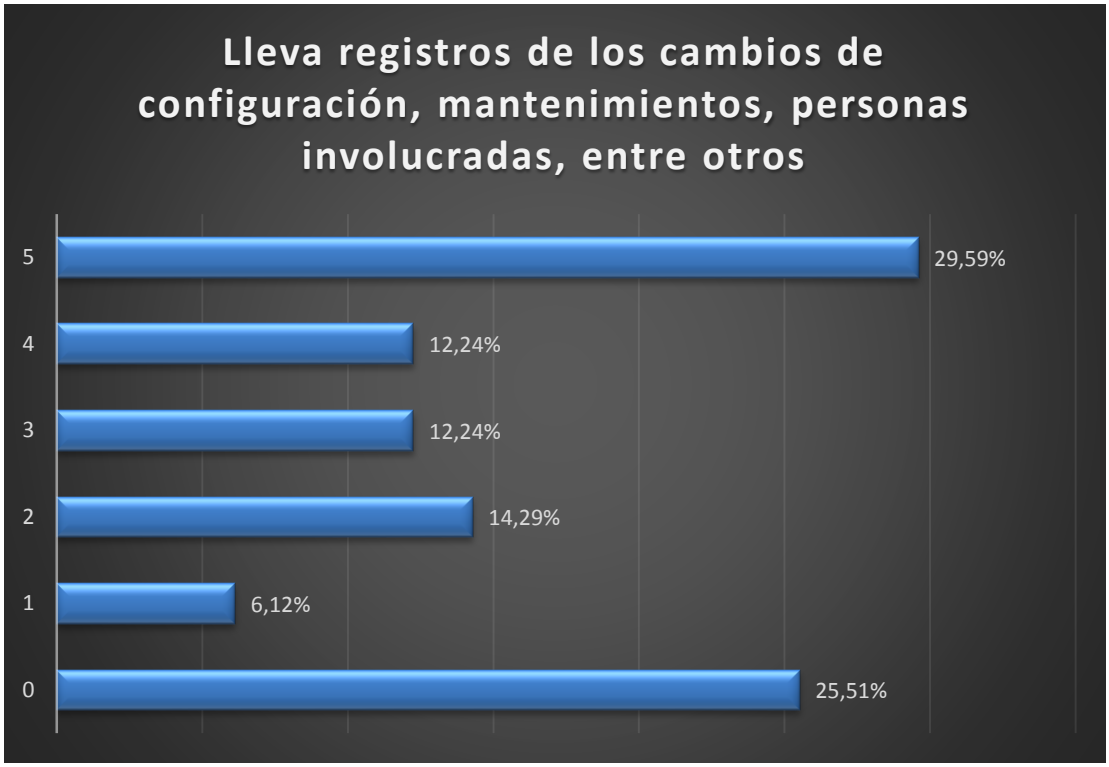
Figura 21. Hábitos de seguridad: políticas internas y niveles de acceso a diferentes tipos de llamadas



Fuente: propia

Sólo el 26,53% de las empresas encuestadas asegura que posee un sistema claro en la definición de políticas internas y niveles de acceso a diferentes tipos de llamadas con una calificación de 5, seguido por una calificación de 4 con un 20,41%. Por su parte el 24,48% nunca las ha definido o son muy incipientes, con calificaciones entre 0 y 1. Definir los niveles de acceso no sólo garantiza un nivel de seguridad máximo, sino que implica ahorro y un uso adecuado del teléfono.

Figura 22. Hábitos de seguridad: registros de configuración, asistencia, empleados, facturas.



Fuente: propia

Mientras que el 29,59% de las empresas aseguró llevar estrictamente los registros referentes a la manipulación de las líneas telefónicas (mantenimientos, configuraciones, empleado que la realiza, entre otros). El 25,5% de las empresas aseguró no implementar esta práctica. Llevar registros es sumamente importante, porque permite identificar el error o fraude realizado de acuerdo a la fecha, manipulación y persona que lo realizó, en caso tal de que el fraude haya ocurrido desde un empelado interno o por medio de una asistencia técnica que lo propiciara.

Figura 23. Hábitos de seguridad: reporte de situaciones sospechosas

Fuente: propia

Se evidencia que la mayoría de las empresas posee el hábito de seguridad de informar al proveedor de servicios situaciones sospechosas referentes a seguridad de sus líneas telefónicas; que aunque no todas las empresas afirmaron reportar toda situación sospechosa, sí todas informaron hacerlo al menos una vez en su haber. Esto demuestra que existe un alto conocimiento de la importancia de informar; sin embargo, se puede mejorar aun más este aspecto.

4.4. Índices de fraudes y pérdidas económicas de las empresas proveedoras del servicio

Se realizaron tres (3) entrevistas telefónicas a diferentes proveedores de servicio de este tipo de telefonía; a UNE, CLARO y a Movistar. Ninguna de las empresas quiso aportar información respecto a pérdidas económicas; sin embargo UNE informó que recibe alrededor de 600 quejas o denuncias al mes por parte de usuarios, por fraudes o irregularidades relacionados con la facturación y seguridad de las líneas telefónicas empresariales.

UNE y CLARO afirmaron que los fraudes más frecuentes son los de las modalidades By Pass y Call Back, especialmente para llamadas a teléfonos móviles. Por su parte, Movistar informó que han sido víctimas frecuentes de Call Back y asegura que en muchas ocasiones, el fraude proviene de algún empleado de la compañía o una empresa de servicios contratada.

4.5. Recomendaciones de seguridad a los usuarios

- Cambio de claves mensualmente.
- Generar políticas internas y niveles de acceso a los diferentes tipos de llamadas según la necesidad del cargo.
- Implementar registros que abarquen fecha, nombre del empleado o empleado externo, labor que realizó al sistema y otros factores dependiendo de la circunstancia y/o necesidad.
- Contratar personal capacitado y de confianza para la configuración de las diferentes funciones del servicio.
- Solicitar al proveedor del servicio habilitar sólo las funciones que en realidad necesita y sabe usar.

- Capacitar a los empleados, según el cargo acerca del uso, configuración y confidencialidad de los datos de la troncal.
- Confirmar la identidad del personal de la empresa prestadora de servicio cada vez que reciba o solicite una llamada o visita técnica.
- Revisar y comparar siempre las facturas.
- Generar cultura de seguridad entre todos los empleados
- Reportar situaciones sospechosas e irregularidades, ante el proveedor de servicio y la autoridad pertinente.

4.6. Recomendaciones a los proveedores de servicio

- Invertir en investigación y cultura de seguridad encaminada a disminuir este tipo de fraudes.
- Implementar políticas internas y estrategias de supervisión de personal técnico.
- Capacitar empleados de la misma compañía en lugar de contratar empleados externos para las actividades de manipulación y configuración de estos servicios.
- Implementar y revisar frecuentemente los registros de mantenimientos e intervenciones técnicas a las troncales SIP y/o PBX.

5. CONCLUSIONES, RECOMENDACIONES Y TRABAJO FUTURO

- El fraude telefónico realizado a troncales SIP y/o PBX contra usuarios y proveedores del servicio en Colombia no es un fenómeno aislado; se evidencia que, los principales factores que lo propician son el desconocimiento y falta de hábitos de seguridad por parte de los usuarios; la gran mayoría de este tipo de fraudes se realiza con el fin de realizar llamadas de larga distancia, internacional y nacional y en la mayoría de ocasiones, los fraudes ocurren luego de un mantenimiento del sistema, lo que demuestra que no se hacen las configuraciones de seguridad adecuadas y que probablemente, en muchos de estos casos, los técnicos están relacionados con este crimen; para los proveedores de servicio, se infiere que es mediante ingeniería social y deslealtad de parte de sus empleados; sin embargo, fue poca la información que pudo obtenerse por parte de estas empresas debido a políticas internas de seguridad. Los resultados obtenidos son de una proporción pequeña del total de empresas con este tipo de sistema en Colombia; sin embargo, son concluyentes y demuestran que es necesario intervenir en mejoras de seguridad de estos sistemas.

- Se concluye que existe un alto índice de fraudes a usuarios, con un resultado de 24,24% y así mismo existe un alto porcentaje de usuarios que no saben con certeza si han sufrido un fraude o no (21,21%); lo que demuestra que, la cultura de seguridad respecto al tema, es muy bajo. La mayoría de los fraudes ocurridos se reportan con la funcionalidad DISA activado, por lo cual, es necesario prestar atención a mitigar sus riesgos. Otro aspecto relevante es que la mitad de los usuarios, después de haber sufrido un fraude no lo reportan ni al proveedor de servicio ni lo denuncian ante la policía o alguna autoridad, lo que dificulta realizar procesos de investigación y de seguridad y genera un alto subregistro.

- Respecto a los hábitos de seguridad que poseen las empresas, se evidencia que hay una baja uniformidad entre los diferentes factores y las empresas; puede decirse que existe un nivel medio de cultura de seguridad de las líneas telefónicas, por lo que se hace necesario impulsar esfuerzos para este fin. Se encuentra que, en general, existe un nivel alto de cambiar las claves y códigos de acceso, supervisión de la información que los empleados comparten, revisión frecuente de facturas e informar al proveedor de servicio situaciones sospechosas. Por su parte, existe u nivel medio de adopción de hábitos de seguridad referentes a la contratación de personal calificado y confiable para programar sus equipos y redes, definición de políticas internas y niveles de acceso a los diferentes tipos de llamadas y registros de la manipulación del sistema, Y en general, existe un nivel bajo del hábito de seguridad referente a la capacitación del personal respecto al manejo, configuración y confidencialidad de datos de la línea telefónica respecto al cargo.

- Aunque la información aportada por las empresas fue muy escasa, se pudo evidenciar que existe un alto número de denuncias o quejas por parte de los usuarios, referentes a problemas de seguridad o irregularidades en la facturación por consumos anormales en su servicio de telefonía y que estos proveedores de servicio son víctimas sobretodo de By Pass y Call back y que la mayoría de fraudes se debe aparentemente por ingeniería social; es decir, por engaño, puesto que gran parte de estos crímenes han ocurrido por parte de algún empleado de la misma compañía o de alguna empresa externa en la que el proveedor del servicio ha confiado.

- Los usuarios, mediante las estrategias de seguridad pueden disminuir el riesgo de ser víctimas de algún tipo de fraude telefónico. Para ello sólo se requiere conocerlas y generar hábitos y cultura de seguridad entre los empleados.

- Se recomienda obtener resultados de un mayor número de empresas con el fin de generar una mayor precisión en los resultados; así mismo conocer el cargo específico que posee la persona que responde a la encuesta y el nombre de la empresa.

- Para un trabajo futuro, es conveniente medir las vulnerabilidades de una central SIP y/o PBX organizacional; con el fin de encontrar las vulnerabilidades y determinar qué tan sencillo es o no realizar este tipo de fraudes para implementar sistemas de seguridad con base en los resultados; igualmente, si se desean conocer datos de los proveedores de servicio, se recomienda a la Institución Educativa intervenir, con el fin de generar seguridad y garantizar al representante de la empresa la finalidad y buen uso de los datos proporcionados.

REFERENCIAS

Borbón, P. (2010). Red de telefonía: configuración desde el usuario hasta la central. 01/03/2010. Recuperado de internet el 08/11/2015 en http://pabloborbon.com/2010/03/introduccion-a-la-red-de-telefonia-publica-basica-conmutada-tpbc/

Caramillo, G. (2002). Desmitificando el SIP. Mc Graw Hill. México. ISBN 0-07-137340-3.

Cascante R, A. y Guadamuz A, E. (2005). Desarrollo de un sistema para la supervisión de fallas de centrales telefónicas PBX Meridian a través de Internet. Universidad de Costa Rica. 91 p.

Flórez, J.C. (2014). Fraude en las Telecomunicaciones en Bogotá- Colombia. Universidad Distrital Francisco José de Caldas. 9(1). 26-31 p.

Gallardo Y, C. M. (2006). Análisis de estrategias para el control de fraude en la telefonía fija como mecanismo para asegurar los ingresos de las empresas de telecomunicaciones. Escuela politécnica nacional. Quito: Ecuador. 296 p.

Gomara P, C. (2015). Gestión e implementación de funcionalidades en el sistema PBX VOIP en la empresa Nasertic. Universidad de Navarra, España. 39 p.

Henríquez, A. (2012). La evolución del teléfono. 19 de agosto de 2012. Recuperado de internet el 08/12/2015 en http://es.slideshare.net/alejandrita1998/evolucin-telfono

Hinojosa C, X. A. y Béjar A, J. G. (2012). Desarrollo de un sistema basado en ASTERISK que permita investigar situaciones anómalas (bypass) en el Ecuador para la SUPERTEL. Escuela Politécnica Nacional. Quito: Ecuador. 6 p.

IPCOM Network. (2010). Troncales SIP. Recuperado de internet el 10/12/2015 en http://www.ipcomnetwork.com/Troncales-SIP.htm

Lozoya, J. (2013). Estafas telefónicas: tipos, clases de timos y fraudes telefónicos. Publicado el 15/07/2013. Recuperado de internet el 11/12/2015 de http://suite101.net/article/estafas-telefonicas-tipos-clases-de-timos-y-fraudes-telefonicos-a25796#.VmrJJXYvfIV

Roca C, J.M. (2000). El teléfono como medio de comunicación. *Revista Telos.* 29 (2). Madrid, España. 6-10 p.

Sandoval, Á. (2008). Fraude camuflado en telefonía. Portafolio. Publicado el 10 de septiembre de 2008. Recuperado de internet el 10/12/2015 de http://www.portafolio.co/archivo/documento/MAM-3086379

UNE. (2010). Funcionalidades más vulnerables al fraude de telefonía. Publicado el 3 de marzo de 2010. Recuperado de internet el 09/12/2015 de http://troncalsip.une.net.co/doc_pdf/funcionalidades_vulnerables.pdf

APÉNDICE

Apéndice A.

Cuestionario

1. ¿Ha sido usted víctima de algún fraude telefónico en su empresa?
    - Sí
    - No (salte a pregunta 10)
    - No Sabe (salte a pregunta 10)

2. ¿Cómo sucedió el fraude?
    - Redireccionamiento por parte de un empleado
    - No lo sabe
    - Mantenimiento remoto
    - Al usar IVR
    - Al activar servicio de atención automática
    - Al activar DISA
    - A través de buzón de mensajes

3. ¿A cuál empresa pertenecía el servicio contratado?
    - UNE
    - Claro
    - Movistar
    - Otra

4. ¿Denunció el fraude?
    - No
    - A la policía

- Al proveedor de servicio

5. ¿De qué tipo de fraude fue víctima?
   - Llamadas móviles
   - Llamadas larga distancia internacional
   - Llamadas larga distancia nacional
   - Llamadas locales
   - Llamadas Premium

6. ¿Considera que pudo haber evitado el fraude?
   - Sí
   - No

7. ¿Al momento del fraude había realizado mantenimiento recientemente?
   - Sí
   - No

8. Al momento del fraude llevaba mucho tiempo sin actualizar los códigos de ingreso?
   - Sí
   - No

9. Al momento del fraude se habían configurado correctamente todas las funciones?
   - Sí
   - No

10. ¿Le han intentado robar información o llamadas a través de su línea telefónica empresarial?
    - Sí
    - No sabe (pase a la pregunta 13)
    - No

11. ¿Denunció el intento de fraude? (pase a la pregunta 13)
    - A la empresa de telecomunicaciones
    - A la policía
    - No lo denunció

12. ¿Cómo se dio cuenta del intento de fraude?
    - Actitud sospechosa de un empleado o técnico
    - Confirmación o aviso del sistema
    - Llamada sospechosa
    - Visita técnica sospechosa

13. Indique por favor, en la siguiente escala siendo 0 nunca y 5 siempre los siguientes hábitos de seguridad que se implementan en su empresa

	0	1	2	3	4	5
Cambia las claves y/o códigos de acceso con frecuencia						
Permite sólo visitas y/o asistencias técnicas autorizadas y validadas por el proveedor del servicio						
Supervisa con frecuencia la info. que sus empleados comparten acerca de claves y/o códigos de configuración o acceso						
¿Contrata personal capacitado y confiable para programar sus equipos y redes?						
¿Capacita a los empleados respecto al manejo, configuración y confidencialidad de datos de la línea telefónica?						
Revisa sus facturas telefónicas						
Define políticas internas y niveles de acceso a los diferentes tipos de llamadas según el cargo						
Implementa registros de los cambios de configuración y mantenimiento con las personas involucradas en el proceso						
Informa al proveedor de servicio situaciones sospechosas						

FIRMA ESTUDIANTES

ANDRES F. ECHEVERRI M.

FIRMA ASESOR

FECHA ENTREGA: 26-08-2016

FIRMA COMITÉ TRABAJO DE GRADO DE LA FACULTAD _____

RECHAZADO_____ ACEPTADO____ ACEPTADO CON MODIFICACIONES_____

ACTA NO._____

FECHA ENTREGA: _____

FIRMA CONSEJO DE FACULTAD_____

ACTA NO._____

FECHA ENTREGA: _____