



**LA SEGURIDAD  
DE SU PBX**

un compromiso que nos une

**Nos une  
la gente**

UNE, el mejor aliado de quienes  
trabajan por Colombia



<b>1. Definiciones – generalidades sobre fraudes telefónicos</b>	<b>5</b>
<b>1.1.</b> ¿Qué es un sistema telefónico y para qué sirve?	6
<b>1.2.</b> ¿Qué es un IP PBX?	7
<b>1.3.</b> ¿Qué es Asterisk?	7
<b>2. ¿Cómo se hacen los fraudes a través de un PBX?</b>	<b>8</b>
<b>2.1</b> Objetivo de los fraudes	8
<b>3. Funcionalidades más vulnerables de los PBX y fraudes más comunes</b>	<b>9</b>
<b>3.1</b> Funcionalidad DISA (Direct Inward System Access)	10
<b>3.2</b> Servicio de atención automática	10
<b>3.3</b> Buzones de voz	11
<b>3.4</b> Redireccionamiento de extensiones	12
<b>3.5</b> Mantenimientos remotos	12
<b>3.6</b> Transferencia de llamadas a los números de operadoras	12
<b>4. Ataques más comunes en sistemas IP PBX</b>	<b>13</b>
<b>4.1</b> Negación de servicio	14
<b>4.2</b> Los ataques cuya finalidad es el daño	14
<b>4.3</b> Robo	14
<b>4.4</b> Escucha	15
<b>4.5</b> Llamadas no solicitadas	16
<b>4.6</b> Autenticación de usuarios no autorizados	16
<b>4.7</b> Fuga de información	17
<b>4.8</b> Ingeniería social	17
<b>4.9</b> Otros riesgos	17
<b>5. Recomendaciones para evitar fraudes telefónicos en su compañía</b>	<b>18</b>
<b>6. Recomendaciones para prevenir ataques en sistemas Asterisk</b>	<b>21</b>



# CONOZCA ESTA COMPLETA GUÍA QUE LE PERMITIRÁ INFORMARSE

sobre el riesgo de fraudes en su sistema telefónico

Como su aliado en Telecomunicaciones, y en cumplimiento con lo establecido por la Comisión de Regulación de Comunicaciones en la Resolución 3066 de 2011, es nuestro deber informarle sobre los riesgos relativos a la seguridad de la red y de los servicios contratados, y sobre las acciones a su cargo para preservar la seguridad y evitar fraudes telefónicos en su compañía que le pueden costar más que una llamada de atención.

**Conozca la vulnerabilidad de los sistemas telefónicos para que mitigue los riesgos de posibles ataques, que generan un alto impacto económico para su compañía.**



## GENERALIDADES sobre fraudes telefónicos

Los PBX o plantas telefónicas que la mayoría de compañías utilizan para comunicarse con sus clientes y proveedores, y la facilidad de comunicarse al interior de la misma, son constantemente objeto de ataques realizados por defraudadores, quienes utilizando puntos débiles en la programación y conociendo algunas de sus funcionalidades básicas acceden remotamente al sistema y realizan todo tipo de llamadas para beneficio propio sin ninguna autorización. Estos ataques generan altos consumos, que luego son cobrados por los operadores de telecomunicaciones a su compañía.

**Todas las plantas telefónicas pueden ser blancos de estos defraudadores, pero si usted cuenta con una buena programación en su sistema telefónico, con estrictos cuidados en la seguridad y un continuo seguimiento, podrá prevenir este riesgo para su compañía.**



## ¿Qué es un **SISTEMA TELEFÓNICO** y **PARA QUÉ SIRVE?**

1.1

**PBX son las siglas en inglés de “Private Branch Exchange”,** la cual es la red telefónica privada utilizada dentro de una compañía. Los usuarios del sistema telefónico comparten un número definido de líneas telefónicas para poder realizar llamadas externas.

El sistema telefónico conecta las extensiones dentro de una compañía y al mismo tiempo las conecta con la red pública conmutada, conocida también como PSTN (Public Switched Telephone Network).

**Su función principal** es gestionar, además de llamadas internas, las entrantes y/o salientes, con autonomía sobre cualquier otra central telefónica. Este dispositivo generalmente pertenece a la compañía que lo tiene instalado y no a la compañía que suministra el servicio de telefonía pública, de aquí el adjetivo privado a su denominación.

Una de las tendencias más recientes es el desarrollo de sistemas telefónicos que transmiten la voz por medio de la red de Internet. Estos llevan el nombre de VoIP PBX ó IP PBX. También el uso de aplicaciones abiertas de software libre como Asterisk que proporciona funcionalidades de una central telefónica.



**Un IP PBX** combina las ventajas del mundo IP con las funciones de los sistemas **PBX**. Con respecto a **IP**, esta es la abreviatura de Internet Protocol, que sumado a **PBX** resulta Internet Protocol Private Branch Exchange. La función de este sistema es la misma, sólo que en lugar de utilizar telefonía convencional, es un sistema que soporta Voz sobre IP. La ventaja de la Voz sobre IP es que es una tecnología que utiliza Internet (redes LAN o WAN) como vía para llevar a cabo la llamada, por lo que la información se digitaliza y transmite en forma de paquetes de datos digitales. Con estas plataformas se pueden usar teléfonos IP, softphones o teléfonos convencionales (depende del fabricante) y funciona igual que un PBX convencional.

**Un IP PBX, al ser totalmente digital, no sólo puede trabajar con voz, sino también con video y otra serie de herramientas de colaboración como mensajería y conferencias, entre otras.**

**Asterisk es** una aplicación para controlar y gestionar comunicaciones de cualquier tipo, ya sean **analógicas, digitales o VoIP** mediante todos los protocolos VoIP que implementa.

Asterisk es una aplicación de software libre (OpenSource) basada en licencia GPL (General Public License), que proporciona funcionalidades de una central telefónica. Como cualquier PBX, se puede conectar un número determinado de teléfonos para hacer llamadas entre sí. Asterisk es un sistema híbrido que permite gestionar comunicaciones telefónicas tradicionales (analógicas, digitales, móviles) como comunicaciones IP mediante el uso de los protocolos estándar de VoIP.



## ¿Cómo **SE HACEN LOS FRAUDES** a través **DE UN PBX?**

2.

Los fraudes a través de los PBX son generados por fallas en la programación, en la seguridad y, en ocasiones, por desconocimiento de las funciones del sistema, que le facilitan al defraudador acceder remotamente y realizar llamadas de larga distancia (nacional e internacional) o hacia teléfonos móviles que terminan siendo cobradas a la empresa dueña del sistema.

**En los sistemas IP PBX y Asterisk, cuando la voz entró al mundo de los datos, heredó todas las implicaciones de seguridad de las redes de datos. En especial se volvió susceptible a los ataques que sufren los demás servicios que se prestan en Internet.**

### Objetivo **DE LOS FRAUDES**

2.1

Estos fraudes son realizados para obtener beneficios económicos a través de la reventa de minutos, el enrutamiento y terminación de tráfico nacional e internacional, la utilización del servicio de telefonía local, larga distancia nacional e internacional, el acceso a las líneas 900 y 901 (premium) y llamadas a teléfonos móviles.





# FUNCIONALIDADES MÁS VULNERABLES

de los PBX y fraudes más comunes

## **FUNCIONALIDAD DISA** (Direct Inward System Access)

3.1

**También conocida como acceso remoto.** Esta opción permite realizar llamadas desde el PBX accediendo desde una línea externa de la compañía. Este servicio para la telefonía de la compañía y de sus empleados, puede ser muy riesgosa si no se tiene una buena programación y políticas de seguridad para su uso.

Por medio de una línea externa y utilizando esta funcionalidad, cualquier persona que conozca el manejo o los códigos de acceso a troncales del PBX, puede realizar llamadas que serán cobradas a la compañía. Estas llamadas suelen realizarse en las noches y fines de semana, y se pueden evitar configurando correctamente el PBX, definiendo políticas internas para el uso de esta funcionalidad y programando el sistema para que bloquee las llamadas en horarios no laborales.

## Servicio de **ATENCIÓN AUTOMÁTICA**

3.2

**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

Estos varían de acuerdo al tipo de PBX  
o sistema de llamadas y a la programación  
de los mismos.

## BUZONES de voz

3.3

La herramienta de habilitar casilleros para mensajes de voz ofrece eficiencia en las comunicaciones de su compañía y un mejor 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. Además, sin una correcta programación, alguien podría apoderarse de los buzones de voz cambiándoles las claves de acceso originales.



## **REDIRECCIONAMIENTO** de extensiones 3.4

Este fraude se hace direccionando el teléfono a un destino de larga distancia nacional, internacional o móvil para la realización de llamadas de terceros a estos destinos. Para hacer esta configuración, se debe acceder a la planta telefónica.

## **MANTENIMIENTOS** remotos 3.5

Algunos proveedores realizan la configuración del sistema por vía telefónica o remota. Este es un procedimiento normal, pero en algunos casos el módem que se activa para este fin, no es apagado en el momento de finalizar la programación quedando abierto el sistema para que alguien pueda ingresar a la planta y realice 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, VPNs, etc).

## **TRANSFERENCIA DE LLAMADAS** a los números de operadoras 3.6

Ocurre cuando alguien de la compañía recibe una llamada y le solicitan transferirla a las extensiones de llamadas asistidas por operadora de las compañías de larga distancia (Ejemplo: 151-159, 171-179, 191-199). Al transferirse la llamada, el defraudador accede al servicio de larga distancia nacional o internacional y esa llamada es cobrada a la compañía propietaria del PBX.



# ATAQUES MÁS COMUNES

en sistemas **IP PBX**

## Negación **DE SERVICIO**

4.1

Los ataques de negación de servicio, se basan en la mayoría de los casos en ataques de **“fuerza bruta”** que buscan saturar el software y hardware haciendo que se presente lentitud , que no haya respuesta en el sistema y no se pueda utilizar el servicio.

### **Las dos formas más comunes son:**

- Generar una gran cantidad de falsos requerimientos de servicio para que el sistema y la máquina no tenga suficientes recursos para atender los verdaderos requerimientos.
- Enviar requerimientos que generen fallas en los protocolos, bloqueando u obligando a reiniciar el sistema para recuperar su funcionalidad.

## Los ataques cuya finalidad **ES EL DAÑO**

4.2

Son ataques que **buscan introducirse en sistemas de información o prestación de servicios** y modificar o suprimir algunas de sus partes de manera que no puedan volver a operar. Estos ataques se diferencian de los ataques de negación de servicio, en que en éstos últimos no hay destrucción, y al reiniciar la máquina se recupera la funcionalidad.

## **ROBO** de información

4.3

**La finalidad de este tipo de ataques** es buscar vulnerabilidades del sistema que permitan acceder a información, en especial a claves de acceso para luego manipularlas y venderlas en el mercado negro. Con la obtención de estas claves, se da acceso al sistema para poder realizar todo tipo de llamadas.

**En sistemas IP la voz se convierte en datos**, y la inversión en seguridad que se hagan en los datos, se hereda para la voz. Así que el uso de VPN, redes MPLS, equipos de inscripción de datos y tecnologías similares, que son necesarios para proteger el mundo de los datos, nos ayudan en este nuevo medio de transporte de la voz. El costo que pagamos es que todas estas tecnologías generan encabezados adicionales, generando un mayor consumo de ancho de banda y el proceso de encriptación y desencriptación genera latencia lo cual afecta las comunicaciones en tiempo real.

Los protocolos de comunicaciones **buscan identificar plenamente al interlocutor** para entregarle la voz, pero existen viejas técnicas de ataque *Man in the middle* que se utilizan para engañar a un equipo activo para que nos entregue una copia de los datos, y a diferencia de la voz convencional, en VoIP no es posible detectar si nos están espiando, porque no ocurren cosas como que se baje el volumen o se escuchen ruidos de fondo al grabar las llamadas.

## Llamadas **NO SOLICITADAS**

4.5

El protocolo SIP puede aceptar llamadas en los *endpoints* o terminales sin autenticación y con la facilidad de acceder a ellos solo conociendo su dirección IP, lo cual facilita que se hagan barridos de direcciones buscando los puertos de SIP o h323 abiertos para enviar tráfico sin tener ninguna identificación del origen. A diferencia de la voz convencional, en el mundo IP no es necesario ser usuarios de la misma red o de una central interconectada para enviar tráfico, esto se puede hacer utilizando un servidor que haga esta labor sin dejar rastro.

**Para defenderse de esto se pueden implementar listas negras o listas blancas en los equipos, e implementar sistemas seguros de autenticación y claves.**

## Autenticación de **USUARIOS NO AUTORIZADOS**

4.6

Esto se da por una inadecuada definición de políticas de *password* sobre las plataformas, por ejemplo, el uso de clave de longitud corta, con baja complejidad, o genéricas. También se presenta porque no hay un control y obligación del sistema para que los usuarios renueven sus claves en un tiempo definido.

## 4.7

## FUGA de información

Ocurre cuando un sistema diseñado para realizar tareas que no deben ser observadas por un atacante revela parte de esa información debido a errores en los procedimientos de trabajo. Por ejemplo, al diseñarse una red de mensajería instantánea cifrada, un experto en telecomunicaciones puede saber en qué momento se emiten los mensajes. Si en el proceso de generación de números pseudo aleatorios se utilizó la hora como semilla se podría deducir la clave secreta estimando el tiempo que tarda la mensajería instantánea en cifrar el mensaje antes de transmitirla.

## 4.8

## INGENIERÍA social

En el campo de la seguridad informática, ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos, fuentes humanas. Es una técnica que pueden usar ciertas personas, para obtener claves y acceder al sistema telefónico para cometer los fraudes.

## 4.9

## OTROS riesgos

- No bloqueo del usuario después de un número de intentos fallidos.
- Sesiones abiertas simultáneamente para un mismo usuario.
- Mal uso del acceso remoto.
- Falta de políticas y conciencia en seguridad dentro de la compañía.
- Configuración por defecto de los equipos de la solución.



# RECOMENDACIONES PARA EVITAR

fraudes telefónicos **en su compañía**

- 1.** 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.
- 2.** Compruebe periódicamente si la funcionalidad DISA (perfeccionamiento del sistema de acceso directo) ha sido activada.
- 3.** Cambie las contraseñas por defecto que son suministradas por el proveedor para la administración de la planta telefónica.
- 4.** Configure su sistema para no permitir acceder a tono de discado bajo ninguna circunstancia (marcación en 2 etapas).
- 5.** Mantenga seguros los buzones de correo, para ello es necesario que cambie periódicamente las contraseñas y elimine o bloquee los buzones de correo no utilizados.
- 6.** Configure el sistema para que los usuarios, obligatoriamente, cambien las contraseñas en el primer inicio de sesión a su buzón de correo. No permita disponer de las contraseñas que estén relacionados con su número de extensión o contraseñas débiles como 0000 ó 1234.
- 7.** Cuelgue cuando reciba llamadas no identificadas con anuncios en un lenguaje extranjero.
- 8.** 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).
- 9.** No conecte llamadas entrantes de personas desconocidas, solicitando las extensiones 151-159, 171-179, 191-199 y otros códigos de los operadores de larga distancia para llamadas asistidas.
- 10.** Defina categorías, políticas internas y niveles de acceso de larga distancia para cierto tipo de llamadas (LDN, LDI, móviles).
- 11.** 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.

- 12.** Pregunte al proveedor de su planta telefónica por el modo nocturno del sistema para evitar llamadas fuera del horario laboral.
- 13.** Maneje los manuales de configuración del PBX como documentos a los que solo debe tener acceso personal autorizado.
- 14.** Establezca con su proveedor fecha y horas específicas para el mantenimiento remoto de su sistema y confirme que el módem utilizado para el mantenimiento a distancia o remoto sea apagado o bloqueado en el momento de finalizar el trabajo.
- 15.** Incluya en los contratos de instalación y mantenimiento del sistema con terceros, cláusulas de responsabilidad por cambios no acordados.
- 16.** Vigile y compruebe el trabajo de los técnicos durante y después de los trabajos de mantenimiento.
- 17.** Realice un control y seguimiento de los mantenimientos, reprogramaciones o cambios al sistema, llevando fecha, hora y detalle de las modificaciones.
- 18.** Revise la facturación periódicamente apoyándose en los reportes internos del sistema y comparándolos con la facturación de las compañías telefónicas.
- 19.** Realice un monitoreo permanente de los destinos entrantes y salientes, hacia y desde la planta telefónica. Si se detecta algún tráfico irregular o sospecha del mismo, comuníquese inmediatamente con el operador de Telecomunicaciones.
- 20.** Audite periódicamente el sistema PBX para comprobar la seguridad, puntos débiles y la forma en que la programación se ajuste a las necesidades de la compañía.
- 21.** Haga uso de la facilidad de código secreto ofrecida por su operador de telefonía local. Esto le permitirá activar y desactivar la restricción de llamadas de larga distancia desde su línea, así como llamadas hacia teléfonos móviles. Los servicios de Telefonía de UNE ya tienen incluido el servicio de código secreto sin costo adicional. Para conocer cómo activar y desactivar este servicio, comuníquese con nuestra línea gratuita 01 8000 41 01 41. Para líneas de otros operadores, póngase en contacto con su proveedor.



# RECOMENDACIONES PARA PREVENIR

ataques en **Sistemas Asterisk**

- 1.** Durante la instalación, con el apoyo de un experto, programe y configure el sistema adecuadamente para cerrar vulnerabilidades y prevenir ataques desde la red.
- 2.** Manténgase al día en actualizaciones, vulnerabilidades y soluciones sobre esta aplicación de software libre.
- 3.** Haga un mantenimiento continuo de la aplicación. Lleve un control exhaustivo del sistema: versiones de paquetes, nuevas actualizaciones.
- 4.** Compruebe en los logs del Asterisk los intentos fallidos de autenticación y en el caso de varios intentos, bloquee de manera automática el supuesto atacante añadiendo la dirección IP al firewall para denegar el acceso a la red desde ésta.
- 5.** Evite utilizar puertos estándares (5060, 4569, 80, 22, etc.)
- 6.** Implemente herramientas que le den seguridad y protejan su red como un firewall y el PortSentry para evitar escaneos y ataques DoS.
- 7.** Deniegue peticiones al 5060/4569 UDP desde el exterior siempre que no tenga usuarios SIP/IAX externos.
- 8.** Deshabilite el "allowquest=yes", algunas interfaces lo traen habilitado por defecto.
- 9.** Siempre configure el "realm", "defaultuser" y el parámetro "secret".
- 10.** Realice una correcta configuración del dialplan. Si las extensiones no son configuradas con estrictas medidas de seguridad, los usuarios maliciosos se pueden autenticar y registrar en nuestro sistema para hacerse pasar por una extensión con permisos y hacer llamadas como un usuario normal. Ante esto debe configurar contraseñas robustas difíciles de identificar.



# IMPORTANTE

Si su empresa cuenta con servicios de comunicaciones como E1s, RDSIBRI, RDSI PRI, Troncales SIP, Líneas análogas o Líneas IP conectadas a su planta telefónica, PBX, Asterisk o Call manager para sus comunicaciones empresariales, usted debe tener en cuenta que existen riesgos de seguridad que pueden afectar estos últimos equipos o sistemas de comunicaciones y que **es su obligación conocer y aplicar estrictos controles de seguridad, mantenimiento y manejo de los equipos** cuya infraestructura y uso son de su entera responsabilidad.

Nos une  
la gente

UNE, el mejor aliado de quienes  
trabajan por Colombia



Conozca los riesgos y las medidas de seguridad  
que debe implementar para **evitar**  
**fraudes telefónicos en su compañía.**

Trabajar por Colombia, **mejor juntos**  
**018000 41 01 41**  
[www.une.com.co/corporativo](http://www.une.com.co/corporativo)

