# RECOMENDACIONES DE SEGURIDAD PARA SU RED INTERNA DE TRABAJO

En **PBX Hosting** contamos con estándares de seguridad a nivel servidor, para que usted este despreocupado al momento de contratar nuestros servicios, sin sufrir ninguna interrupción o preparados para proteger nuestros servidores de cualquier atacante.

Sin embargo, es muy **IMPORTANTE** que a nivel **USUARIO** usted también siga las siguientes recomendaciones de seguridad, dentro de la red donde se trabajara con el servicio de VoIP, ya que de no hacerlo puede verse afectado por un **hackeo**, generando llamadas no deseadas y consumo de saldo incluso dejando su troncal con saldo negativo.

## TRONCAL SIP

Por la parte de la Troncal SIP de voz IP pueden implementarse medidas de seguridad para minimizar los riesgos de hacking telefónico en toda la plataforma, pero para habilitarlas necesitamos su autorización:

- **Limitación de la duración de las llamadas:** Se puede configurar que las llamadas se corten automáticamente tras un tiempo razonable, evitando que llamadas se hagan sin limitación. si esto lo quiere habilitar debe solicitarlo a soporte@pbxhosting.com.mx
- **Bloqueo mediante lista de países de riesgo:** Disponemos de una lista de países y destinos potencialmente peligrosos que se bloquean para no poder llamar. Para hacer este bloqueo necesitamos que usted lo solicite en ticket a tarifas@pbxhosting.com.mx
- **Limitación de llamadas simultáneas:** Es recomendable permitir un límite máximo de 10 canales o llamadas simultáneas por cliente, si esto lo quiere habilitar debe solicitarlo a soporte@pbxhosting.com.mx

### ¿Por dónde entran los hackers?

Regularmente atacan los teléfonos y los usuarios de sistemas de Voz IP instalados en equipos de cómputo los cuales regularmente tienen contraseñas muy fáciles de descifrar, tales como 1, 2, 3, 4, el mismo número de extensión, o un nombre sencillo. Recordemos que una contraseña debe ser FUERTE para considerarse segura y tener mayúsculas, minúsculas, números y algún carácter especial.

**IMPORTANTE:** Estas recomendaciones deben ejecutarse por parte del CLIENTE en su red interna de trabajo.

- Revisar agujeros de IPs y puertos abiertos, usados habitualmente en este tipo de ataques. La mayoría de ataques son a través de agujeros en la red informática del cliente.
- Contraseñas WiFi. Debemos tener en cuenta que la telefonía VoIP es accesible, si se cuelan a la red informática y eso incluye el acceso por wifi. Deben de tener mucho cuidado cuando se conectan a su servicio deVoIP especialmente en redes wifi públicas.
- Mantener una IP fija con el operador VoIP. Es una medida de protección adicional si la telefonía sólo la tenemos disponible desde la IP fija de la oficina. Sin embargo, esto dificulta un despliegue en múltiples sedes, el teletrabajo, y usuarios remotos.
- Cambiar cada 1 o 2 meses las claves de configuración en terminales. Los teléfonos SIP tienen una clave de fábrica para la configuración. Es recomendable cambiarlo por una clave secreta.
- Los correos electrónicos pueden estar infectados con algún virus y si se ejecuta puede infectar la red de trabajo y obtener los accesos a la troncal sip, es importante vacunar y proteger con antivirus TODOS los equipos de trabajo, más si ahí se tiene instalado el softphone o se tiene acceso a la troncal sip o conmutador.
- Tener solamente los puertos en su conmutador o dialer que se utilizan en la telefonía IP como 5060, 10000 a 20000 en udp.
- Tener un bloqueador de IPs como “Fail2ban” que bloquea los intentos de registro fallidos de extensiones o acceso al servidor.
- Si se cuenta con una IP publica en el conmutador registrar su troncal mediante IP y no utilizar la opción por registro.
- Solicitar vía ticket a tarifas@pbxhosting.com.mx el bloqueo de destinos que no utilice.
- Utilizar prefijos para la salida a llamadas internacionales desde su conmutador.
- Bloquear el acceso web a Países en los cuales no tengan agentes.
- Si cuentan con un conmutador utilizar Doble autentificación para el acceso web.
- Verificar que en los equipos donde se registran las extensiones de su conmutador o dealer no se encuentran infectados con malware.

**¿Qué sucede si hago caso OMISO a las recomendaciones anteriores?**

Corre el riesgo de que en cualquier momento **hacken** su servicio de telefonía VoIP, sacando llamadas desde su conmutador propio, conmutador alojado con nosotros, teléfono IP, softphone, etc. sacando llamadas no deseadas a destinos que usted no conoce, generando consumo de su saldo, vaciando su cuenta o hasta dejando un saldo negativo que tendrá que cubrir con **PBX Hosting.**

**¿Qué sucede con el saldo que me llegara a consumir un hacker?**

No es rembolsable por parte de PBX Hosting ya que es parte de las obligaciones de nuestro cliente ejecutar medidas de seguridad en su red interna de trabajo y es por eso que le estamos enviando estas recomendaciones cuando contrata nuestros servicios.