# ATAQUES A CENTRALES IP-PBX

## 1. INTRODUCCIÓN

Una Central PBX (Private Branch Exchange), es una red telefónica privada utilizada por ejemplo dentro de una empresa, que constituye una puerta de entrada, distribución y salida de las llamadas telefónicas dentro de una compañía.

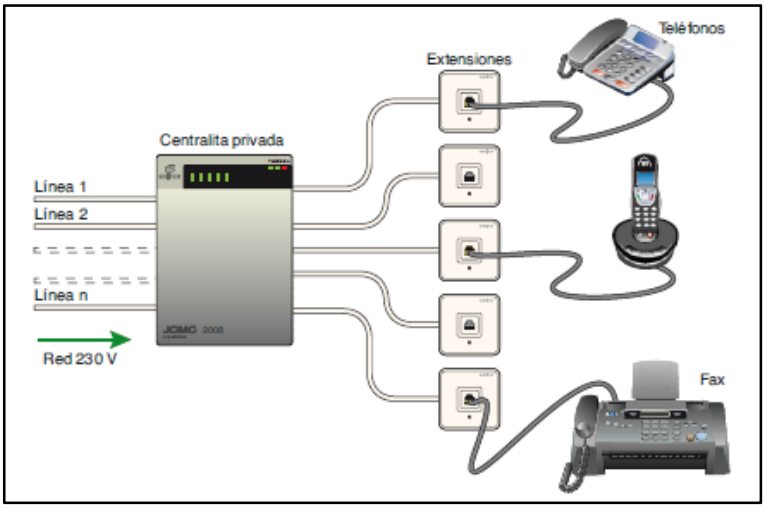


**Figura No. 1 Central PBX**

Una PBX se encarga de establecer conexiones entre terminales de una misma empresa, o de hacer que se cursen llamadas al exterior. Hace que las extensiones tengan acceso desde el exterior, desde el interior, y ellas a su vez tengan acceso también a otras extensiones y a una línea externa.

Una central telefónica IP, es un equipo telefónico diseñado para ofrecer servicios de comunicación a través de las redes de datos. A esta tecnología se le conoce como voz por IP (VoIP), donde el IP es el llamado protocolo de Internet y la dirección IP, es la dirección por la cual se identifican los dispositivos dentro de la web. Con los componentes adecuados se puede manejar un número ilimitado de extensiones en sitio o remotos vía Internet, añadir video, conectar troncales digitales. Los aparatos telefónicos que se usa son conocidos como teléfonos IP o SIP y se conectan directamente a la red.



**Dirección:** Av. Diego de Almagro N31-95 entre Whymper y Alpallana.
**Código postal:** 170518 / Quito - Ecuador
**Teléfono:** 593-2 2947-800 - www.arcotel.gob.ec

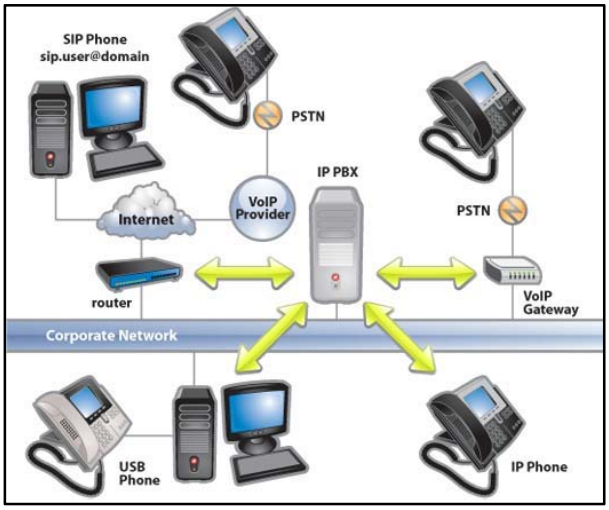


**Figura No. 2 Central IP-PBX**

## 2. RIESGO

El uso de centrales IP-PBX crece incluso en medianas y pequeñas empresas, debido las facilidades que ofrecen así como por sus bajos costos de implementación, ya que en muchos casos no requieren de un hardware especializado e incluso se han liberado los códigos para su descarga y uso en forma gratuita, sin embargo al momento de implementar estas centrales no se toman en cuenta configuraciones básicas de seguridad.

Por las facilidades de movilidad y por las soluciones en la nube, las centrales telefónicas están expuestas directamente a Internet con una IP Pública o un dominio, sin embargo, con poca o ninguna protección la central queda expuesta a que sea atacada. Uno de los principales ataques es el de “Fuerza Bruta”, que consiste en averiguar una contraseña probando todas las combinaciones posibles hasta dar con la correcta.

Una vez que los atacantes han logrado ingresar a la central telefónica crean nuevas extensiones y rutas para así poder hacer llamadas fraudulentas a destinos sumamente caros, como Cuba, Afganistán, Lituania, destinos satelitales entre otros. En poco tiempo pueden realizar una gran cantidad de llamadas las cuales son facturadas a la empresa. Además, borrar los log’s que genera la central a fin de que no quede rastro de evidencia que podría ayudar a identificar el origen y como se realizó el acceso no autorizado la central telefónica.

## 3. ACCIONES RECOMENDADAS

Al momento de configurar una central telefónica se debe tener en consideración las siguientes recomendaciones:



**Dirección:** Av. Diego de Almagro N31-95 entre Whymper y Alpallana.
**Código postal:** 170518 / Quito - Ecuador
**Teléfono:** 593-2 2947-800 - www.arcotel.gob.ec

- Se debe cambiar la contraseña de administración por defecto y colocar una contraseña con al menos 8 dígitos, donde se combinen mayúsculas, minúsculas, números y caracteres especiales.
- Cada extensión debe tener una contraseña. Se debe evitar poner la misma contraseña a todas las extensiones.
- Para las líneas troncales, a cada ruta saliente, se le debe asignar un nivel de privilegio (Interno, Local, Nacional o Internacional), y a cada uno de ellos se le debe asignar a cada extensión. No es necesario que todas las extensiones tengan todos los niveles de privilegio, es decir no todas las extensiones deben tener salida Internacional.
- Se debe asignar a cada ruta una contraseña.
- Monitorear los registros de los sistemas de telefonía para, detectar cualquier intento, o vulneración de la seguridad, lo antes posible y responder ante ésta.
- Por defecto desactivar la opción DISA (*Direct Inward Access System*), y en caso de que se deba activarla, habilitar la opción para solicitar una contraseña.
- Activar la función de firewall de la central telefónica, en sus dos opciones de defensa, tanto estática como dinámica.
- Habilitar la opción FAIL TO BAN, a fin de que se rechace peticiones de direcciones IP cuando haya alcanzado un cierto número de peticiones fallidas. También puede definir el tiempo que durara antes de volver a aceptar nuevas peticiones.
- Para acceder a la central mediante web, activar el protocolo HTTPS.
- Publicar al internet los servicios mínimos necesarios.
- No permitir el uso de la extensión fuera de la red LAN cuando realmente no es necesario.
- Solicitar a la operadora telefónica el bloqueo de llamadas internacionales, si no se utiliza.
- Realizar auditorías periódicas del sistema para garantizar que los controles de seguridad (actualizaciones del sistema o parches, control de acceso, revisiones…) funcionan correctamente.

## 4. REFERENCIAS


- https://www.zettaelectronics.com/10-ajustes-de-seguridad-para-centrales-ucm6100/
- https://www.optical.pe/seguridad-de-la-telefonia-ip/
- http://elastixtech.com/fundamentos-de-telefonia/pbx-central-telefonica/
- https://www.3cx.es/voip-sip/central-telefonica-pbx/




**Dirección:** Av. Diego de Almagro N31-95 entre Whymper y Alpallana.
**Código postal:** 170518 / Quito - Ecuador
**Teléfono:** 593-2 2947-800 - www.arcotel.gob.ec