Políticas de seguridad
Guía de prevención de fraudes

El actual documento es una guía de sugerencias que le ayudara a prevenir fraudes provenientes de atacantes externos o hackers dedicados a encontrar vulnerabilidades en sistemas de comunicaciones. No es obligación de El Reseller o cliente cumplir estas recomendaciones, pero si desea tener un nivel mínimo de protección debería cumplirlas.

1. Nunca usar el mismo password igual que el login, (ejemplo login: 12345 y password: 12345)
2. En lo posible crear usuarios alfabéticos, y contraseñas de mínimo 8 dígitos que incluyan: letras minúsculas, mayúsculas, números y caracteres.
3. Si usa el servicio desde un dispositivo VoIP como Teléfono IP, ATA o Gateway, cambie el usuario y contraseña administrador que viene por defecto en el equipo.
4. No publique en Internet un dispositivo VoIP, hágalo debajo de un router.
5. Si el usuario realiza llamadas a pocos destinos solo déjele activos esos. Inactive el resto.
6. De ser posible desactive los destinos costosos como África, Asia, Europa del este, etc..
7. No le deje canales ilimitados a la cuenta, establézcale limite 1 y solo active más canales siempre y cuando el cliente lo solicite.
8. Si un cliente usa Asterisk u otro PBX sugiérale que en las extensiones no deje el mismo password que el número de extensión, ejemplo: extensión: 105 y password: 105.