voipstudio

White paper

Cómo proteger tu sistema telefónico empresarial en la nube

Comprender los riesgos

Los sistemas telefónicos basados en la nube han transformado la forma en que las empresas se comunican. Pero junto con una **mayor conectividad, también surgen nuevos desafíos de seguridad.**

Las pequeñas y medianas empresas son especialmente vulnerables, ya que los atacantes suelen asumir que cuentan con menos recursos para invertir en seguridad. Sin embargo, con las estrategias adecuadas, puedes proteger de forma proactiva tu infraestructura de comunicaciones y garantizar la confianza de tus clientes.

Principales riesgos a tener en cuenta

1. **Filtraciones de datos**: la información sensible de clientes y empresas puede ser interceptada si los sistemas no están protegidos.
2. **Fraude VoIP:** los delincuentes explotan vulnerabilidades para realizar llamadas internacionales no autorizadas o redirigir el tráfico, generando costes inesperados.
3. **Acceso no autorizado:** los protocolos de autenticación débiles facilitan que los atacantes secuestren cuentas o intercepten llamadas.
4. **Ataques de denegación de servicio (DoS):** los hackers saturan los sistemas, dejando inoperativos los servicios telefónicos.
5. **Phishing e ingeniería social:** los atacantes se dirigen a los empleados para obtener credenciales de administrador o información sensible.

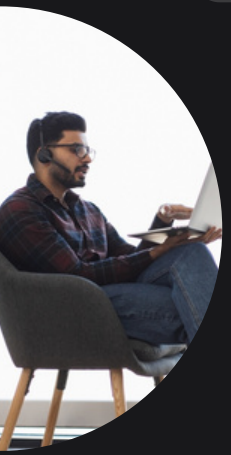
43%

de los ciberataques se dirigen a pymes, y los sistemas VoIP se están convirtiendo en un objetivo cada vez más frecuente para los hackers

Fuente: Verizon DBIR

voipstudio

Mejores prácticas para la protección



Proteger tu sistema telefónico en la nube no tiene por qué ser complicado, pero sí requiere un enfoque proactivo. **El objetivo es combinar políticas sólidas, autenticación robusta y supervisión continua.**

Mejores prácticas de seguridad

- **Activa la autenticación multifactor (MFA):** añade una capa adicional de seguridad para evitar accesos no autorizados a los paneles y cuentas.
- **Usa comunicaciones cifradas:** sistemas como VoIPstudio ofrecen cifrado de extremo a extremo para llamadas y mensajes, protegiendo los datos sensibles durante la transmisión.
- **Configura controles de acceso:** limita los permisos según los roles, asegurando que solo los miembros autorizados del equipo gestionen configuraciones clave.
- **Supervisa y audita la actividad:** realiza un seguimiento regular de los intentos de inicio de sesión, patrones de llamadas y actividad inusual de cuentas para detectar riesgos a tiempo.

99,2%

de reducción en el riesgo de accesos no autorizados a cuentas al usar MFA en comparación con depender únicamente de contraseñas.

Fuente: Microsoft Security

voipstudio

Construir una estrategia de seguridad preparada para el futuro

voipstudio

Proteger tu sistema VoIP no es una tarea puntual, sino un proceso continuo. **Las amenazas evolucionan constantemente y las empresas necesitan una estrategia de seguridad con visión de futuro que crezca junto con la tecnología y las demandas de los clientes.**

Integra la seguridad en los flujos de trabajo

Incorpora medidas de seguridad en la incorporación de personal, el acceso remoto y las operaciones diarias.

Forma a los empleados de manera continua

Educa al personal sobre phishing, gestión segura de contraseñas y prácticas de comunicación segura.

Colabora con proveedores de confianza

Proveedores como VoIPstudio ofrecen sólidas certificaciones de seguridad, políticas transparentes y protecciones integradas.

Planifica la respuesta ante incidentes

Prepara un plan de acción detallado ante posibles brechas para minimizar el tiempo de inactividad y el daño reputacional.

75%

de las organizaciones que utilizan comunicaciones en la nube considera que la seguridad a nivel del proveedor es esencial para la protección continua y el cumplimiento normativo.

Fuente: Gartner

Checklist: evalúa la seguridad de tu sistema telefónico

voipstudio

Paso 1: Verifica la MFA y el cifrado

- [ ] Activa la autenticación multifactor (MFA) en todos los paneles de administración y cuentas de usuario para bloquear accesos no autorizados.
- [ ] Asegúrate de que tu sistema telefónico utilice cifrado de extremo a extremo en llamadas y mensajes para proteger los datos sensibles.

Paso 2: Configura controles de acceso basados en roles

- [ ] Asigna permisos según las funciones del puesto para que los empleados solo accedan a lo que necesitan.
- [ ] Usa cuentas separadas para administradores y usuarios a fin de minimizar el impacto de credenciales comprometidas.

Paso 3: Supervisa la actividad

- [ ] Monitorea los análisis en tiempo real e históricos para detectar patrones de llamadas inusuales, intentos fallidos de inicio de sesión o comportamientos sospechosos de cuentas.
- [ ] Revisa con frecuencia los registros de auditoría detallados para identificar anomalías antes de que se conviertan en brechas de seguridad.

Paso 4: Forma a tu equipo

- [ ] Realiza sesiones de formación continuas sobre phishing, buenas prácticas de contraseñas y acceso remoto seguro.
- [ ] Lleva a cabo simulacros de ataque para evaluar la preparación de los empleados y reforzar la conciencia en seguridad.

95%

de las brechas de seguridad son causadas por error humano. La formación continua y la supervisión proactiva son tu mejor defensa.

Fuente: IBM

Conclusión y próximos pasos

voipstudio

Proteger tu sistema telefónico empresarial en la nube también significa salvaguardar a tus clientes, tu reputación y la continuidad de tu negocio. A medida que las empresas y los equipos crecen, el riesgo se amplía, por lo que las prácticas de seguridad sólidas son indispensables.

VoIPstudio te proporciona funciones de seguridad de alto nivel empresarial para mantener tus comunicaciones seguras y en cumplimiento de la normativa, sin añadir complejidad.

- **Cifrado de extremo a extremo:** protege llamadas, mensajes y datos frente a interceptaciones.
- **Autenticación multifactor (MFA):** añade una capa extra de seguridad en el inicio de sesión.
- **Control de acceso basado en roles (RBAC):** restringe los permisos a lo estrictamente necesario.
- **Paneles en tiempo real:** detecta patrones de llamadas inusuales y posibles amenazas al instante.
- **Centros de datos seguros:** infraestructura con redundancia integrada y supervisión 24/7.
- **Registros completos:** visibilidad total de la actividad del sistema para facilitar el cumplimiento normativo.

Descubre el poder de un call center de alto nivel a precios asequibles.

- Empieza una prueba gratuita de 30 días
- Contáctanos