

Política de seguridad de la información y continuidad del negocio

Ecosistema Telecom, S.A. de C.V. (CIISTEC®) · Versión 1.0 · Vigente desde el 22 de octubre de 2026

1. Compromiso

En Ecosistema Telecom, S.A. de C.V. (CIISTEC®) protegemos la confidencialidad, integridad y disponibilidad de la información de nuestros clientes y de nuestra operación, y mantenemos los servicios funcionando ante fallas, incidentes o desastres.

2. Alcance

Personas, procesos, plataformas en la nube, red, interconexiones con otros operadores y proveedores que intervienen en nuestros servicios.

3. Principios de seguridad

- **Acceso mínimo:** cada persona accede solo a lo que necesita, con cuentas individuales y verificación en dos pasos.
- **Proveedores evaluados:** trabajamos con plataformas de clase mundial y exigimos medidas equivalentes a las nuestras.
- **Cifrado:** la información viaja y se guarda cifrada en las plataformas que lo permiten.
- **Monitoreo 24/7:** vigilamos red y servicios para detectar fallas y actividad anómala.
- **Gestión de incidentes:** registramos, contenemos, resolvemos y notificamos al cliente afectado y, cuando la ley lo exija, a la autoridad.
- **Datos personales:** conforme a la legislación de protección de datos personales y a nuestro aviso de privacidad.
- **Capacitación:** el equipo se capacita en seguridad y confidencialidad al ingresar y al menos una vez al año.

4. Continuidad del negocio

- **Redundancia:** servicios en la nube con centros de datos redundantes; en enlaces de alta disponibilidad, un enlace principal y uno de respaldo por rutas físicas distintas, con cambio automático.
- **Interconexión diversificada:** rutas con distintos operadores para evitar un punto único de falla.
- **Plan de recuperación:** procedimientos documentados para restablecer el servicio con los tiempos objetivo de la tabla siguiente.
- **Respaldos:** configuraciones y datos críticos respaldados periódicamente y probados.
- **Pruebas:** al menos un simulacro de continuidad al año.

- **Comunicación en crisis:** avisamos a los clientes afectados por los canales registrados, con estimación de restauración.

5. Tiempos objetivo ante incidentes críticos

Medidos desde la correcta apertura del ticket. El detalle por nivel de severidad está en el anexo de niveles de servicio de cada contrato.

Servicio	Primera respuesta	Solución o restauración
Enlaces dedicados a internet	10 minutos	40 minutos
Telefonía en la nube (UCaaS)	10 minutos	110 minutos
Centro de contacto (CCaaS)	15 minutos	4.5 horas
Mensajería (SMS, RCS y voz)	90 minutos	Según el anexo de niveles de servicio

Atención de incidentes críticos las 24 horas, los 365 días: +52 55 9020 7176 (opción 1) y servicioalcliente@ciistec.com. Los plazos pueden variar cuando dependen de terceros (operadores, agregadores o plataformas externas).

6. Niveles de servicio

Los niveles de disponibilidad comprometidos (por ejemplo, 99.9% en enlaces de alta disponibilidad) quedan estipulados en cada contrato.

7. Revisión

La Dirección General revisa esta política cada año y después de cualquier incidente relevante.

Rubén Medina Zarazúa

Director General, CIISTEC®