



1 Identificación de riesgos

- Análisis del impacto en el negocio
- Evaluación de amenazas
- Calificación del riesgo inherente

2 Evaluación de controles clave

- Evaluación de controles de proveedores
- Evaluación de controles de servicios

3 Evaluación de riesgos

- Evaluación detallada de riesgos
- Calificación del riesgo residual

4 Toma de decisiones sobre riesgos

- Apetito de riesgo
- Toma de decisiones sobre riesgos

5 Contratación y adquisición

- Cláusulas contractuales
- Gestión de la conectividad de los usuarios
- Acuerdos de nivel de servicio (SLA)

6 Supervisión y notificación de riesgos

- Seguimiento de indicadores clave de ciberseguridad
- Participación del CSIRT: Inteligencia sobre amenazas

7 Actualización continua de los riesgos (auditoría)

- Recálculo del riesgo residual
- Gestión continua de los riesgos

8 Rescisión del contrato y salida

- Rescisión del riesgo
- Eliminación segura de los datos y devolución de los activos
- Transición del servicio y del proveedor
- Acceso a los sistemas/redes desactivado