Plan de Continuidad del Negocio (BCP)

Sede Barcelona

1. Introducción

Este Plan de Continuidad del Negocio tiene como objetivo garantizar que los **procesos críticos de la sede de Barcelona** —principalmente **consultoría y atención al cliente**— puedan mantenerse operativos o ser restaurados rápidamente ante incidentes disruptivos como ciberataques, caídas de servicios, fallos eléctricos, incendios, entre otros.

Este documento forma parte del SGSI y está alineado con la estrategia global de TechSys.

---

2. Alcance

Aplica a:

- Procesos clave de atención al cliente, consultoría, soporte técnico.
- Recursos humanos en modalidad presencial y teletrabajo.
- Sistemas utilizados en la sede y servicios en la nube.
- Dependencias con otras sedes (Madrid, Sevilla) y proveedores comunes.

---

3. Normativa de referencia

- ISO 22301, ISO/IEC 27001 y 27031
- Esquema Nacional de Seguridad (ENS)
- LOPDGDD y RGPD

---

4. Análisis de Impacto al Negocio (BIA)

ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA)							
ACTIVIDAD O	**ÁREA O**	**DEPENDENCIA**	**REQUISITOS NEGOCIO**		**CAPACIDAD SISTEMAS**		**¿LA CAPACIDAD DE SISTEMAS CUBRE LOS REQUISITOS DEL NEGOCIO?**
PROCESO	**DEPARTAMENTO**	**SERVICIOS TIC**	**RTO**	**RPO**	**RTO**	**RPO**	
Gestión de consultas y reclamaciones	Atención al Cliente	CRM / Plataforma de tickets (como Zendesk, Freshdesk, HubSpot, etc.)	3	3	3	2	✅SÍ
Atención telefónica y soporte en tiempo real		Centralita VoIP / Software de atención en vivo	2	2	2	2	✅SÍ
Análisis de la empresa	*Consultoría*	Herramientas de análisis. Herramientas de gestión documental.	3	3	2	2	✅SÍ
Gestión de proyectos		Herramienta de gestión de proyectos. Herramientas de gestión documental	2	3	2	2	✅SÍ

---

5. Evaluación de riesgos

Amenazas relevantes para la sede:

- Corte eléctrico o fallo de red.
- Fallo en proveedor cloud.
- Infección por malware/ransomware.
- Ataque DDoS a herramientas de comunicación.

- Problemas físicos en oficina (inundación/incendio).

---

6. Estrategias de continuidad

- Teletrabajo habilitado para todo el personal.
- Herramientas SaaS redundantes (CRM, soporte, correo).
- Respaldos automáticos en servidores cloud (UE).
- Comité mixto de crisis (Barcelona + Madrid).
- Contacto inmediato con proveedor de conectividad en caso de corte.
- Redundancia eléctrica (con SAIS)

---

7. Plan de respuesta y recuperación

- Activación del BCP tras notificación por parte del Comité.
- Comunicación inmediata al personal.
- Restauración prioritaria de acceso a CRM y plataforma de soporte.
- Comunicación a clientes si hay afectación superior a 1h.

---

8. Roles y responsabilidades

Rol	Función
Comité de crisis (mixto)	Evaluar incidentes y activar el plan.
Responsable local Barcelona	Coordinar respuesta operativa y comunicación interna.
Soporte técnico central	Restaurar servicios, evaluar backups.
DPD	Garantizar cumplimiento con normativa de datos.

---

9. Comunicación en crisis

- Canales: email alternativo, WhatsApp corporativo, teléfono directo.
- Plantillas predefinidas para clientes y proveedores.
- Comunicación con autoridades solo si se ve afectada la seguridad de datos.

---

10. Recursos necesarios

- Conexión VPN y portátiles preparados para teletrabajo.
- Acceso remoto a CRM y sistema de tickets.
- Documentación crítica almacenada en sistema cloud.

---

11. Pruebas y ejercicios

- **Pruebas anuales** de restauración de servicios en todas las sedes.
- Ejercicios parciales por procesos críticos.
- Registro de cada prueba con hallazgos y mejoras propuestas.

---

12. Mantenimiento del plan

- Revisión anual o tras cambios organizativos.
- Responsable: Comité de Seguridad + Coordinador sede Barcelona.

---

13. Anexos

- Árbol de dependencias (ver archivo PDF).
- Lista de contactos clave (internos y externos).
- Formularios de activación del plan.
- Registro de simulacros.