					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P32S					Título del documento: **Política de Continuidad del Negocio y Recuperación ante Desastres**							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025			Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro	

Historial de revisiones				
Número de revisión	**Fecha de revisión**	**Cambios**	**Revisado por**	**Propietario del proceso**

Aprobaciones			
Nombre	**Cargo**	**Fecha**	**Firma**

Alineación con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 6.1, 6.3, 8	
ISO/IEC 27002:2022	Controles 5.29, 5.30	
NIST SP 800-53 Rev. 5	CP-2, CP-4, CP-6, CP-7	
RGPD de la UE	Artículos 32, 33	
Directiva NIS2 de la UE	Artículo 21(2)(f)	
DORA de la UE	Artículo 10	
COBIT 2019	DSS04	

1. Finalidad

1.1 Esta política garantiza que la organización pueda mantener sus operaciones y recuperar los servicios de TI esenciales durante y después de eventos disruptivos, como cortes de suministro eléctrico, ciberataques, infecciones por ransomware o fallos de sistemas.

1.2 Establece un marco claro para la planificación de la continuidad del negocio y la recuperación ante desastres (BC/DR), adaptado a pymes sin equipos de TI dedicados.

1.3 Esta política ayuda a la organización a cumplir los requisitos aplicables de ISO/IEC 27001:2022, el RGPD de la UE, la Directiva NIS2 de la UE, DORA de la UE y COBIT 2019, al tiempo que refuerza la resiliencia operativa y la confianza de los clientes.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todos los sistemas y servicios críticos para las operaciones de la organización (p. ej., correo electrónico, almacenamiento en la nube, plataformas de facturación, registros de clientes)

2.1.2 Todos los empleados y proveedores externos de servicios de TI responsables de la preparación y ejecución de BC/DR

2.1.3 Todo tipo de interrupciones, incluidos incidentes cibernéticos, fallos de hardware, pérdida de suministro eléctrico, inundaciones e inaccesibilidad de la oficina

2.2 Esta política abarca:

2.2.1 la gestión de copias de seguridad

2.2.2 la planificación de la continuidad del negocio (BCP)

2.2.3 las operaciones de recuperación ante desastres

2.2.4 la formación del personal y las pruebas

2.2.5 los procedimientos de respuesta legal y regulatoria

3. Objetivos

3.1 Proteger la capacidad de la organización para prestar servicios clave pese a interrupciones no planificadas.

3.2 Garantizar la recuperación oportuna de sistemas y datos con Objetivos de Tiempo de Recuperación (RTO) predefinidos.

3.3 Permitir que todo el personal siga los procedimientos de continuidad durante las crisis con la mínima confusión posible.

3.4 Mantener el cumplimiento de la normativa sobre protección de datos y resiliencia operativa, incluido el artículo 32 del RGPD de la UE y el artículo 21 de la Directiva NIS2 de la UE.

3.5 Establecer una estrategia práctica y verificable de continuidad y recuperación adecuada para pymes.

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Es responsable del proceso de BC/DR y de esta política

4.1.2 Aprueba los Planes de Continuidad del Negocio (BCP/DRP)

4.1.3 Coordina la respuesta a incidentes y la comunicación interna durante las interrupciones

4.1.4 Realiza las notificaciones regulatorias cuando sea necesario (p. ej., notificaciones de violaciones de seguridad de los datos personales en virtud del RGPD de la UE)

4.2 Proveedor externo de TI / Administrador de sistemas

4.2.1 Mantiene y prueba las copias de seguridad

4.2.2 Ejecuta los procedimientos de recuperación ante desastres cuando se activen

4.2.3 Documenta todas las acciones de recuperación y los eventos de restauración de sistemas

4.2.4 Notifica inmediatamente al DG cualquier incidente de TI crítico

[... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ...]

9. Requisitos de revisión y actualización

9.1 Revisión anual de la política y del plan

9.1.1 El Director General (DG) debe garantizar que esta política y su correspondiente Plan de Continuidad del Negocio (BCP) se revisen formalmente al menos una vez al año.

9.1.2 La revisión debe incluir:

9.1.2.1 evaluación de riesgos nuevos o emergentes

9.1.2.2 revalidación de los RTO/RPO

9.1.2.3 verificación de la información de proveedores y contactos

9.1.2.4 alineación con cambios en los sistemas de TI, las obligaciones legales o las operaciones

9.2 Actualizaciones basadas en desencadenantes

9.2.1 Esta política también debe actualizarse en respuesta a:

9.2.1.1 incidentes o interrupciones graves, especialmente si no se cumplieron los objetivos

9.2.1.2 nuevas obligaciones legales o regulatorias (p. ej., modificaciones de DORA de la UE)

9.2.1.3 cambios en sistemas críticos, plataformas en la nube o personal

9.2.1.4 hallazgos de las pruebas anuales de BCP/DR

9.3 Proceso de control de cambios

9.3.1 Todos los cambios deben ser aprobados por el DG

9.3.2 Debe mantenerse un historial de versiones, incluyendo la fecha, la descripción del cambio y el aprobador

9.3.3 La política actualizada debe redistribuirse a todo el personal pertinente, incluido el proveedor de TI y los responsables de departamento

9.4 Documentación de lecciones aprendidas

9.4.1 Tras las pruebas o las interrupciones reales, las lecciones aprendidas documentadas deben incorporarse a futuras revisiones

9.4.2 Estas revisiones también deben incluir evaluaciones del desempeño de los proveedores y comprobaciones de la adecuación de la respuesta

10. Políticas relacionadas y vinculaciones

10.1 Esta política está estrechamente integrada con las siguientes políticas para pymes:

10.1.1 P1S – Política de Seguridad de la Información: define los objetivos de seguridad de alto nivel que deben respaldar las prácticas de continuidad y recuperación.

10.1.2 P4S – Política de Control de Acceso: permite la revocación o restauración de emergencia del acceso de los usuarios durante escenarios de interrupción de la actividad.

10.1.3 P6S – Política de Gestión de Riesgos: constituye la base para identificar, evaluar y priorizar los riesgos relacionados con la continuidad.

10.1.4 P8S – Política de Concienciación y Formación en Seguridad de la Información: garantiza que los empleados estén preparados para actuar durante interrupciones y comprendan el BCP.

10.1.5 P15S – Política de Copias de Seguridad y Restauración: proporciona procedimientos técnicos específicos para salvaguardar la disponibilidad y recuperación de los datos.

10.1.6 P17S – Política de Protección de Datos y Privacidad: garantiza que la planificación de la continuidad respete la protección de los datos personales y cumpla el RGPD de la UE durante y después de los incidentes.

10.1.7 P22S – Política de Registro y Supervisión: respalda la detección de eventos que puedan activar procesos de BC/DR y proporciona trazas de auditoría forense tras una interrupción.

10.1.8 P30S – Política de Respuesta a Incidentes: precede directamente a la activación del proceso de recuperación en caso de incidentes cibernéticos u operativos.

10.1.9 P31S – Política de Recopilación de Evidencias y Análisis Forense: garantiza que se recopilen evidencias digitales durante escenarios de continuidad para fines de cumplimiento, seguro o investigación.

10.2 Estas políticas conforman un marco cohesionado, preparado para auditorías, para la resiliencia, la responsabilidad proactiva y la continuidad de los controles en todas las operaciones de la organización.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001:

11.1.1 cláusula 6.1: exige planificación y tratamiento basados en riesgos, incluida la continuidad del negocio y la recuperación.

11.1.2 cláusula 6.3: hace hincapié en la mejora continua tras las interrupciones.

11.1.3 cláusula 8.1: exige controles operativos, incluidos controles documentados de continuidad.

11.2 ISO/IEC 27002:

11.2.1 control 5.29: exige el establecimiento y mantenimiento de disposiciones de continuidad del negocio.

11.2.2 control 5.30: exige pruebas y revisión de dichas disposiciones.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 CP-2: define requisitos para la planificación de contingencias.

11.3.2 CP-4: exige formación en contingencias para el personal de la organización.

11.3.3 CP-6: cubre los requisitos del emplazamiento alternativo de almacenamiento.

11.3.4 CP-7: regula las expectativas sobre el emplazamiento alternativo de procesamiento.

11.4 RGPD de la UE:

11.4.1 artículo 32: exige medidas para garantizar la disponibilidad y resiliencia continuas de los sistemas y servicios de tratamiento.

11.4.2 artículo 33: activa obligaciones de notificación de violaciones de seguridad cuando un fallo de continuidad da lugar al compromiso de datos personales.

11.5 Directiva NIS2 de la UE (2022/2555):

11.5.1 artículo 21(2)(f): exige capacidades de planificación de la continuidad y gestión de crisis como condición de preparación frente al riesgo cibernético.

11.6 DORA de la UE (2022/2554):

11.6.1 artículo 10: exige la implantación de pruebas de resiliencia operativa digital y capacidades de recuperación, especialmente para pymes del sector financiero.

11.7 COBIT 2019:

11.7.1 DSS04 – Gestionar la continuidad: proporciona directrices de gobernanza empresarial para mantener y validar la resiliencia operativa, incluida la asignación de responsabilidades, las pruebas, la integración de proveedores y las revisiones posteriores al evento.