					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P32					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**

Alineada con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 8	
ISO/IEC 27002:2022	Controles 5.29, 5.30	
NIST SP 800-53 Rev. 5	CP-1 a CP-11	
NIST SP 800-34 Rev. 1	Planificación de contingencias	Marco
ISO 22301:2019		Requisitos del Sistema de Gestión de la Continuidad del Negocio
RGPD de la UE	Artículo 32	
Directiva NIS2 de la UE	Artículo 21(2)(f)	
DORA de la UE	Artículo 10	
COBIT 2019	DSS	

1. Propósito

1.1. Esta política define los controles y las responsabilidades obligatorios para garantizar la capacidad de la organización de mantener o restablecer sus operaciones críticas y los servicios de TIC de soporte durante y después de un incidente disruptivo.

1.2. Su objetivo es proteger la vida, la estabilidad operativa, las obligaciones legales, los compromisos con los clientes y la reputación de la organización, incorporando resiliencia mediante una planificación proactiva y capacidades de recuperación validadas.

1.3. Esta política establece la base del marco de gestión de la continuidad del negocio (BCM) y recuperación ante desastres (DR) de la organización, garantizando el cumplimiento de los requisitos regulatorios, contractuales y sectoriales aplicables.

2. Alcance

2.1. Esta política se aplica a todas las unidades organizativas, sistemas de información, procesos de negocio, personal y servicios de terceros que se clasifiquen como críticos o esenciales sobre la base de los resultados del análisis de impacto en el negocio (BIA).

2.2. La política abarca:

2.2.1. Interrupciones de origen natural o humano, incluidos ciberataques, fallos de infraestructura, interrupciones de centros de datos, pandemias e interrupciones de los servicios de proveedores

2.2.2. La planificación, las pruebas y la mejora continua de los planes de continuidad del negocio (BCP) y de los planes de recuperación ante desastres (DRP)

2.2.3. Las funciones y responsabilidades relativas a la respuesta de emergencia, la coordinación de la recuperación y el escalado de incidentes

2.3. Todo el personal con responsabilidades de continuidad o recuperación, incluidos TI, responsables de negocio, responsables de crisis y proveedores, está sujeto a las disposiciones de esta política.

3. Objetivos

3.1. Garantizar la continuidad de las operaciones y los servicios de la organización mediante procedimientos predefinidos y probados, minimizando el impacto operativo, reputacional y legal.

3.2. Recuperar los servicios de TIC dentro de los objetivos de tiempo de recuperación (RTO) y los objetivos de punto de recuperación (RPO) definidos, alineados con los niveles de tolerancia al riesgo de la organización.

3.3. Asignar la titularidad de la planificación, la ejecución y la gobernanza de la continuidad del negocio y la recuperación ante desastres en toda la organización.

3.4. Garantizar que las capacidades de continuidad se prueben, mantengan y mejoren periódicamente sobre la base de escenarios realistas y hallazgos de auditoría.

3.5. Cumplir las obligaciones aplicables en materia de cumplimiento conforme a ISO, NIST, RGPD de la UE, DORA de la UE y la Directiva NIS2 de la UE, respaldando la diligencia debida en materia de resiliencia operativa y disponibilidad.

4. Funciones y responsabilidades

4.1. Alta Dirección

4.1.1. Aprueba la Política de Continuidad del Negocio y Recuperación ante Desastres y garantiza su alineación estratégica.

4.1.2. Asigna presupuesto y recursos para respaldar la continuidad del negocio, la respuesta de emergencia y los ejercicios de recuperación.

4.2. Responsable de Continuidad del Negocio

4.2.1. Es responsable del desarrollo y mantenimiento de los BCP de toda la organización y de la coordinación de las pruebas de continuidad.

4.2.2. Mantiene el calendario del BIA, facilita la formación y garantiza que la documentación cumpla los requisitos normativos aplicables.

[... 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. Esta política deberá revisarse anualmente por el Responsable de Continuidad del Negocio y el Director de Seguridad de la Información para garantizar su alineación con:

9.1.1. Cambios en las operaciones de la organización, los sistemas críticos o la infraestructura

9.1.2. Lecciones aprendidas de incidentes, auditorías, ejercicios de mesa o pruebas de DR

9.1.3. Obligaciones regulatorias o contractuales actualizadas (por ejemplo, DORA de la UE, RGPD de la UE o requisitos de RTO/RPO de clientes)

9.1.4. Modificaciones del apetito de riesgo o de la estrategia de continuidad de la organización

9.2. Las revisiones deberán incluir:

9.2.1. La validación de la vigencia de los planes y de los datos de contacto

9.2.2. La reevaluación de RTO, RPO y niveles de recuperación

9.2.3. La evaluación de la capacidad de los servicios de copia de seguridad y DR

9.2.4. La retroalimentación de las partes interesadas que hayan ejecutado planes o pruebas de recuperación recientes

9.3. Todos los cambios en la política deberán:

9.3.1. Mantenerse sujetos a control de versiones con justificación documentada y aprobación de las partes interesadas

9.3.2. Comunicarse al personal y a los equipos clave con responsabilidades actualizadas

9.3.3. Reflejarse en la formación, los materiales de concienciación y los procedimientos operativos actualizados

9.4. Deberán emitirse actualizaciones provisionales de emergencia cuando exista un cambio sustancial en la organización, un mandato legal o un hallazgo crítico que haga inviables los planes o la política vigente.

10. Políticas relacionadas y vínculos

10.1. Esta política funciona en coordinación con los siguientes documentos clave:

10.1.1. P1 – Política de Seguridad de la Información: establece el requisito de operaciones basadas en riesgos y resilientes en toda circunstancia.

10.1.2. P5 – Política de Gestión de Cambios: garantiza que cualquier cambio de configuración o infraestructura relacionado con la recuperación siga flujos documentados y aprobados.

10.1.3. P14 – Política de Conservación y Eliminación de Datos: rige el ciclo de vida de los soportes de copia de seguridad y de los datos recuperados utilizados en las operaciones de continuidad.

10.1.4. P15 – Política de Copias de Seguridad y Restauración: aplica controles sobre la frecuencia de las copias de seguridad, su seguridad y la verificación de la restauración.

10.1.5. P18 – Política de Controles Criptográficos: garantiza que los procesos de recuperación mantengan los estándares de cifrado y confidencialidad.

10.1.6. P22 – Política de Registro y Supervisión: respalda la detección y el escalado de eventos que afecten a la continuidad.

10.1.7. P30 – Política de Respuesta a Incidentes: define los procesos de contención, escalado y análisis de causa raíz alineados con los desencadenantes de continuidad.

10.1.8. P33 – Política de Auditoría y Supervisión del Cumplimiento: valida la integridad y eficacia de las prácticas de continuidad y recuperación en sistemas y procesos.

11. Normas y marcos de referencia

11.1. Esta política está alineada con normas internacionales reconocidas de continuidad del negocio y recuperación ante desastres, respaldando la auditabilidad, la resiliencia y el cumplimiento legal.

11.2. ISO/IEC 27002

11.2.1. Anexo A, control 5.29 – Seguridad de la información durante una interrupción: exige la continuidad de los controles de seguridad en condiciones adversas.

11.2.2. Anexo A, control 5.30 – Preparación de las TIC para la continuidad del negocio: exige la preparación, prueba y validación de las capacidades de recuperación de TIC.

11.3. ISO 22301:2019 – Sistemas de gestión de la continuidad del negocio

11.3.1. Proporciona el marco para establecer, implantar y mantener prácticas de BCM alineadas con los objetivos de la organización y los umbrales de riesgo.

11.4. NIST SP 800-34 Rev. 1 – Guía de planificación de contingencias

11.4.1. Establece buenas prácticas para planes de contingencia de sistemas de TI, incluido el desarrollo de la estrategia de continuidad, el análisis de impacto y las pruebas de los planes.

11.5. RGPD de la UE (2016/679)

11.5.1. Artículo 32 – Seguridad del tratamiento: exige la resiliencia de los sistemas de tratamiento y la restauración oportuna de la disponibilidad y del acceso a los datos personales tras un incidente.

11.6. Directiva NIS2 de la UE (2022/2555)

11.6.1. Artículo 21(2)(f): exige medidas de continuidad del negocio y gestión de crisis para respaldar la seguridad de las redes y los sistemas de información.

11.7. DORA de la UE (2022/2554)

11.7.1. Artículo 10 – Continuidad del negocio de las TIC: exige que las entidades financieras desarrollen y prueben planes de continuidad de las TIC, incluidos RTO/RPO basados en riesgos y capacidades de conmutación por error.

11.8. COBIT 2019

11.8.1. DSS04 – Gestionar la continuidad: cubre todos los aspectos de la planificación de la continuidad, incluida la identificación de amenazas, el análisis de impacto, la estrategia de recuperación y las pruebas periódicas.