Libro blanco

La nueva norma ISO/IEC 27031:2025

Cómo adaptar con éxito la planificación técnica de emergencias a la gestión estratégica de la resiliencia en toda la organización.

controllit
Business Continuity Management

Contenido

03
Introducción

04
Profundización en los cambios fundamentales

05
Reajuste estratégico e integración con la norma ISO 22301

08
Requisitos ampliados de gobernanza y gestión

11
Armonización con las normas/estándares existentes

15
Ampliación de las funciones del gestor del IRBC

18
Enfoque en la resiliencia digital y la ciberresiliencia

20
Enfoque tecnológico y relacionado con los datos

25
Requisitos empresariales y control basado en BIA

28
Planificación basada en el riesgo y MBCO final

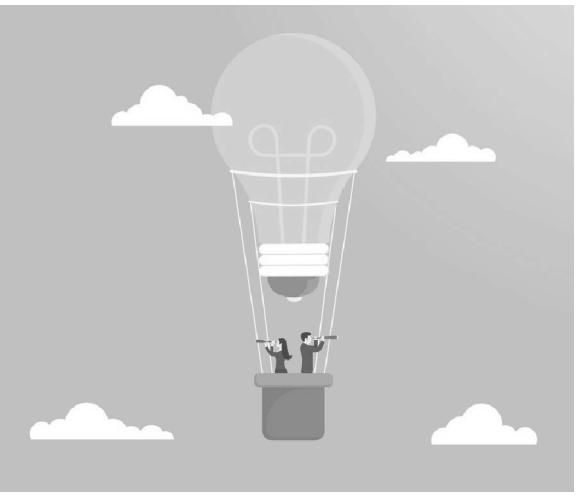
31
Planificación de la recuperación y requisitos de documentación

33
Estrategias IRBC y diseño de la recuperación

35
Recomendaciones de implementación para empresas

Introducción

La norma ISO/IEC 27031 se revisó en profundidad en mayo de 2025 y sustituye a la edición de 2011. En lugar de limitarse a la planificación puramente técnica de la recuperación de TI, la nueva norma adopta un enfoque integral de la resiliencia. ICT Readiness for Business Continuity (IRBC; la preparación de las TIC para la continuidad del negocio) se entiende como parte integrante de la estrategia corporativa y debe estar estrechamente vinculada a la continuidad del negocio, la seguridad de la información, la respuesta a incidentes y la gestión de riesgos.



Una nueva característica es el claro anclaje estratégico de la IRBC en las estructuras de gestión y control. Las funciones, responsabilidades y competencias deben definirse de manera vinculante. Los requisitos también se aplican en condiciones de ciberataques activos (por ejemplo, ransomware, APT), lo que amplía significativamente el papel del gestor de IRBC, que pasa a ser el de co-diseñador de arquitecturas TIC resilientes.

Las empresas deben proporcionar soluciones documentadas que tengan en cuenta la redundancia, la nube y las dependencias de la cadena de suministro, y que estén alineadas con el RTO, el RPO y el recién introducido MBCO final. La norma también exige un programa estructurado de pruebas, formación y auditoría con indicadores de rendimiento, evaluación sistemática y lecciones aprendidas.

Los sistemas ITSCM/IRBC existentes pueden seguir utilizándose siempre que cubran funcionalmente los nuevos requisitos. Estos incluyen vínculos claros de gobernanza, integración en los sistemas de gestión existentes, determinación del MBCO final y procesos de mejora continua. La norma no menciona explícitamente el ciclo PDCA, pero sigue el principio de mejora continua: desde la planificación hasta la implementación y las pruebas, pasando por la evaluación estratégica por parte de la dirección.

Este libro blanco presenta los cambios clave en comparación con la norma ISO/IEC 27031:2011, los clasifica estratégicamente y analiza su impacto en las empresas reguladas y los sistemas de gestión existentes en el ámbito de la gestión de la continuidad de los servicios de TI (ITSCM) y el IRBC. Tiene en cuenta elementos de normas relacionadas, como la ISO/IEC 22301 (gestión de la continuidad del negocio), la ISO/IEC 27001 (gestión de la seguridad de la información), el Marco de Ciberseguridad del NIST y métodos ITSCM probados.

Profundización de los cambios centrales

La nueva norma ISO/IEC 27031:2025 tiene un impacto notable en la práctica estratégica y operativa de la IRBC y la ITSCM. Se centra en una integración más estrecha con la BCM según la norma ISO 22301. Los objetivos de la IRBC se definen ahora junto con los resultados del BIA, de modo que el RTO, el RPO y el nuevo MBCO final están vinculados de forma trazable en todo momento.

Al mismo tiempo, la nueva norma amplía su enfoque para incluir normas relacionadas. La norma en sí misma se refiere exclusivamente a las normas ISO/IEC (por ejemplo, ISO 22301, 27002). Sin embargo, las empresas pueden asignar los controles a requisitos normativos como DORA o NIS-2 y marcos como NIST-CSF o NIST SP 800-61 para crear sinergias entre los procesos de seguridad de la información, continuidad y respuesta a incidentes. Por ejemplo, las empresas pueden incorporar controles como el control 5.30 de la norma ISO 27002 en su marco IRBC y documentarlos con fines normativos.

Un elemento clave es la gobernanza formalizada. La función del gestor de IRBC tiene competencias claramente definidas, depende de un comité directivo interdisciplinario de IRBC que se creará y gestiona un conjunto consolidado de indicadores clave de rendimiento (KPI). Estos indicadores abarcan desde el cumplimiento de los tiempos de recuperación de TI hasta las mediciones de pruebas y auditorías. Así, el gestor de IRBC actuará en el futuro como interfaz entre la implementación de TI y la alta dirección.

El BIA sigue siendo el eje central, pero se amplía para incluir un enfoque de trazabilidad coherente. El RTO técnico de las TIC y el RPO de las TIC derivan los valores técnicos objetivo de TI. Las brechas se cierran mediante inversiones o se aceptan como un riesgo y se documentan en el MBCO final (objetivo mínimo de continuidad del negocio). Este MBCO final define el nivel de rendimiento mínimo aceptable tras la finalización de la recuperación de TI, lo que aumenta la transparencia en situaciones en las que no se pueden alcanzar los objetivos ideales a corto plazo.

Reajuste estratégico e integración con la norma ISO 22301

La norma ISO/IEC 27031:2025 afianza la IRBC en el contexto estratégico mucho más firmemente que antes y destaca la relevancia de la resiliencia de TI como parte integral de un sistema de gestión de la continuidad del negocio (BCMS). La IRBC ya no se entiende como una respuesta puramente técnica a incidentes críticos de TI, sino como un instrumento de control estratégicamente afianzado dentro del BCMS de acuerdo con la norma ISO 22301. Esto incluye definiciones conjuntas de objetivos, análisis coordinados de riesgos (TI) e impacto empresarial (BIA), estructuras de gobernanza coordinadas y una estrategia coherente de pruebas y ejercicios (TI). Se destacan explícitamente las interfaces con la BCM, como el análisis de impacto empresarial (BIA), la evaluación de riesgos (TI), las estructuras de gobernanza coordinadas y una estrategia coherente de pruebas y ejercicios (TI).

Esta reorientación se manifiesta en la exigencia explícita de integración estratégica y dependencia mutua entre las disciplinas. El objetivo ya no es solo reiniciar la TI, sino garantizar la operatividad resiliente de los servicios de TI críticos en el tiempo, en consonancia con los requisitos de los procesos empresariales críticos en el tiempo. La TI se posiciona como un factor de valor añadido con altos requisitos de resiliencia.

La orientación estratégica se refleja en varios elementos:

- En el futuro, la IRBC debe configurarse estratégicamente e integrarse en la estrategia de resiliencia de la empresa.
- La integración con el BCMS es un elemento clave.
- La norma formula requisitos claros para el control, la coordinación y la derivación mutua de valores objetivo como RTO, RPO y MBCO final.
- Se está eliminando la separación entre las medidas de resiliencia técnicas y organizativas en favor de un enfoque integrado.
- La responsabilidad del IRBC ya no recae principalmente en el departamento de TI, sino que requiere una gobernanza interdisciplinaria.

Reajuste estratégico e integración con la norma ISO 22301

¿Qué exige específicamente la norma?

Mientras que la norma ISO/IEC 27031:2011 solo exigía indirectamente la integración en la gestión de la continuidad del negocio (BCM), la versión revisada de 2025 lo estipula ahora de forma explícita y vinculante. En concreto, la norma exige:

- la definición conjunta de objetivos en el BCMS
- análisis coordinados de riesgos (de TI) y de impacto en el negocio
- estructuras de gobernanza coordinadas
- estrategias integradas de pruebas y ejercicios de TI

¿Qué significa esto para la implementación?

Las empresas deben asegurarse de que las medidas de IRBC no se desarrollen y apliquen de forma aislada, sino como parte de la BCM. Esto incluye procesos de planificación conjunta, documentación integrada y coordinación periódica entre los responsables de IRBC y BCM. Los requisitos de continuidad de TI se derivan directamente de los resultados del BIA. La norma exige una gestión coordinada de ambas disciplinas. Esto incluye, entre otras cosas:

- valores objetivo acordados conjuntamente (RTO, RPO, MBCO final)
- procesos sincronizados de riesgo (TI) y BIA
- Estructuras de gobernanza y líneas jerárquicas interrelacionadas
- procesos coordinados de comunicación de emergencias (TI) y escalamiento
- documentación coherente y trazable (incluidas las interfaces entre IRBC y los planes de continuidad del negocio)

Las empresas que ya cuentan con sistemas de gestión IRBC/BCM interconectados suelen estar bien posicionadas. Sin embargo, los requisitos para lo siguiente son cada vez más estrictos:

- **Trazabilidad y metodología:** Las auditorías exigen cada vez más pruebas documentadas de cómo se han derivado las medidas de IRBC a partir de los resultados de BCM.
- **Gobernanza y estructura de funciones:** debe quedar claro quién es responsable de cada uno de los resultados del IRBC y cómo se organiza la cooperación con el BCM y el ISM.
- **Coherencia en las auditorías:** en el futuro, las auditorías se centrarán más específicamente en cómo se derivaron metódicamente las medidas IRBC a partir de los resultados de BCM, cómo se definen las funciones y cómo se organiza la interacción entre BCM, IRBC e ISM. La norma no solo exige una mayor cooperación entre estas disciplinas, sino que también aumenta las expectativas en cuanto a su coherencia documentada.

Reajuste estratégico e integración con la norma ISO 22301

Ejemplo práctico: Example Ltd – BIA e IRBC con documentación completa

En el futuro, las empresas deberán ser capaces de documentar y explicar cómo se tradujeron metódicamente los resultados del BIA en soluciones IRBC y cómo se organiza la cooperación entre BCM, IRBC e ISM.

Example Ltd. opera una plataforma en la nube de alta disponibilidad para las administraciones locales. Un BIA determinó que el fallo de la plataforma de autoservicio del cliente provocaría importantes retrasos administrativos y daños a la reputación tras un máximo de dos horas. Por lo tanto, el BCM define un RTO de dos horas. La planificación anterior preveía un escenario de espera activa con un tiempo de recuperación de TI de seis horas.

Como parte de la reorientación estratégica de acuerdo con la norma ISO/IEC 27031:2025, el IRBC se integró plenamente en el BCMS. Los objetivos de recuperación de TI (ICT-RTO, ICT-RPO) se derivaron de los resultados del BIA de forma trazable, se validaron técnicamente y se registraron en una documentación de planificación estructurada.

La arquitectura de la plataforma se convirtió a espera activa, el ICT-RTO se redujo a 90 minutos = objetivo alcanzado, documentación auditable.

La derivación se documentó de manera comprensible, incluyendo:

- Referencia al requisito respectivo del BIA (incluido el ID del proceso)
- la asignación de servicios TIC a procesos empresariales críticos
- la derivación de ICT-RTO/RPO basada en el BIA
- Opciones de soluciones técnicas, incluida la evaluación y consideración de los riesgos residuales
- Determinación del MBCO final en caso de desviaciones
- Fecha de revisión, evaluación y aprobación de la dirección

Para las auditorías internas, esta documentación sirve ahora como único punto de referencia para la lógica de derivación entre los requisitos empresariales y la solución IRBC implementada.

Requisitos ampliados de gobernanza y gestión

La nueva norma hace hincapié en la importancia de una gobernanza clara y estructurada para el IRBC. Anteriormente, muchos elementos de gobernanza (por ejemplo, políticas, manuales, informes anuales, etc.), mejores prácticas o interpretaciones estaban sujetos a interpretación. La propia norma ISO/IEC 27031:2011 se mantenía bastante vaga en su declaración sobre la gobernanza. Sin embargo, en la versión de 2025, la norma exige explícitamente la gobernanza, con requisitos mínimos definidos para las funciones, el control y la participación de la dirección.

¿Qué exige específicamente la norma?

Mientras que la norma ISO de 2011 se limitaba a mencionar elementos de gobernanza, la nueva norma exige la integración formal de la IRBC en las estructuras de gestión y control de la empresa. La IRBC se convierte en una tarea de gestión con participación de comités, obligaciones de información e interfaces con el BCMS, el ISMS y la gestión de riesgos (de TI).

La norma hace hincapié explícitamente en que la alta dirección no solo tiene la responsabilidad, sino que también debe tomar decisiones activas sobre la asignación de recursos, los objetivos, como el MBCO final, y la aceptación de riesgos basándose en los informes del IRBC.

Se refuerza el papel del responsable de IRBC, tanto a nivel estratégico como operativo.

Entre los requisitos clave se incluyen, entre otros:

- Nombramiento formal de un gestor de IRBC con tareas, adjuntos y poderes claros.
- Revisiones periódicas por parte de la alta dirección, incluyendo informes de KPI.
- Directrices y procesos documentados, así como canales de escalamiento y comunicación.
- Garantizar los recursos financieros y humanos adecuados para las actividades del IRBC.
- Ciclos fijos de auditoría y revisión para evaluar la eficacia de las estructuras de gobernanza.

¿Qué significa esto para la implementación?

El IRBC ya no debe considerarse una mera herramienta para la planificación de la recuperación de TI, sino un proceso de control integral que contribuye activamente a la estrategia de resiliencia de la empresa. La norma exige una integración sistemática en el modelo de gobernanza, incluyendo responsabilidades claramente documentadas, vías de escalamiento coordinadas e interfaces estructuradas con el BCMS, el ISMS y la gestión de crisis.

Requisitos ampliados de gobernanza y gestión

También se presta especial atención a la trazabilidad y auditabilidad de los modelos de referencia, las estructuras de comunicación y los procesos de toma de decisiones. Deben estar documentados de forma coherente y ser trazables en el contexto de las auditorías internas y externas.

La norma no especifica una forma concreta, pero exige un comité con la autoridad de control adecuada y con carácter interdisciplinario. En la práctica, podría tratarse, por ejemplo, de un consejo de resiliencia en el que el IRBC, el BCM, el ISM, la gestión de riesgos, las operaciones de TI y la dirección de la empresa coordinen periódicamente las cuestiones relacionadas con el IRBC. Las decisiones del IRBC no deben tomarse de forma aislada, sino que deben integrarse en la gestión global de la resiliencia corporativa.

Las empresas deben garantizar que:

- Las funciones del IRBC (propietario, gestor, etc.) con tareas, poderes y representación estén definidas por escrito.
- un comité directivo interdisciplinario (por ejemplo, el comité de resiliencia) realice revisiones de la gestión de forma periódica, por ejemplo, trimestralmente
- Los criterios de rendimiento se integren como KPI en los informes de gestión.
- Se tengan en cuenta los recursos necesarios para el IRBC en la planificación presupuestaria y de inversiones.
- Las estructuras de gobernanza, los canales de comunicación y escalamiento se revisen periódicamente y se gestionen de forma centralizada.
- El IRBC se incluye en un programa de auditoría y revisión interna y se puede demostrar su eficacia.

Requisitos ampliados de gobernanza y gestión

Ejemplo práctico: Example Ltd: establecimiento de una estructura de gobernanza del IRBC en un entorno regulado

Example Ltd es un proveedor de servicios financieros y está sujeto a los requisitos reglamentarios de NIS-2 y DORA. Una auditoría interna de cumplimiento reveló que, aunque existía un ITSCM básico, no había una estructura de gobernanza formal para el IRBC. Las funciones, responsabilidades y vías de escalamiento solo se conocían en áreas de TI individuales y no estaban documentadas de forma centralizada.

Posibles medidas para implementar los requisitos de la norma:

1. **Establecimiento de un Consejo de Resiliencia**
   - Tareas: revisiones trimestrales, aprobación de los objetivos del IRBC, decisiones sobre recursos, decisiones sobre la aceptación de riesgos
   - Composición: director del IRBC, director de BC, CISO, operaciones de TI, gestión de riesgos, dirección
2. **Nombramiento formal de un gestor del IRBC**
   - Definición por escrito de las tareas, facultades y acuerdos de representación
   - Establecimiento de líneas jerárquicas
3. **Integración de los KPI en los informes de gestión**
   - Informes trimestrales al Consejo de Resiliencia y presentación anual al Consejo de Supervisión (si procede)
   - Definición de los KPI: por ejemplo, consecución de objetivos ICT-RTO/ICT-RPO/MBCO final, desviaciones en las pruebas, resultados de las auditorías, avances en la aplicación de medidas
4. **Auditabilidad**
   - Realización de revisiones anuales de eficacia
   - Auditorías periódicas (internas/externas)

Armonización con las normas/estándares existentes

La nueva norma se posiciona claramente como un complemento de las normas de gestión y los marcos normativos existentes. Exige una estrecha integración y coordinación con las normas relacionadas, con el fin de evitar incoherencias, minimizar redundancias y crear sinergias en el desarrollo y el funcionamiento de las estructuras de resiliencia.

Se presta especial atención a las interfaces con:

- ISO/IEC 22301 (BCM): análisis del impacto en el negocio, desarrollo de estrategias, gestión de riesgos, definición de objetivos
- ISO/IEC 27001 (ISMS): por ejemplo, los controles 5.30 (Preparación de las TIC para la continuidad del negocio) y 8.16 (Actividades de supervisión) de la norma ISO/IEC 27002:2022 o A 5.30 y A 8.16 de la norma ISO/IEC 27001:2022
- ISO/IEC 27005:2022 (gestión de riesgos): la derivación de la estrategia IRBC y los análisis de escenarios (por ejemplo, el anexo B - CFIA/FMEA) se basan en una situación de riesgo consolidada de conformidad con la norma ISO/IEC 27005
- ISO/IEC 27035 (gestión de incidentes): integración de los procesos de incidentes y recuperación
- NIST SP 800-61 r3: Ciclo de vida de la gestión de incidentes, lecciones aprendidas
- NIST CSF 2.0: Funciones de detección, respuesta y recuperación
- NIS-2, DORA, norma BSI 200-4: requisitos normativos de resiliencia y verificación

¿Qué exige específicamente la norma?

En el SGSI según la norma ISO 27002, el control 5.30 protege la disponibilidad de los servicios críticos de TIC. La nueva norma ISO 27031 proporciona las directrices de implementación para ello. La norma se refiere a los incidentes de seguridad de la información y exige un enfoque coordinado entre la respuesta a incidentes, el IRBC y el BCM:

- una base armonizada de riesgo y planificación entre el SGSI, el SGBC y el IRBC con una redacción clara como requisito obligatorio, lo que hace que la implementación esté sujeta a auditoría
- Objetivos comunes para ICT-RTO, ICT-RPO y MBCO final, documentados y controlados de forma coherente mediante un control uniforme de los documentos
- Una estrategia vinculante para pruebas, ejercicios y auditorías con criterios de rendimiento definidos
- Pruebas de auditoría uniformes y a prueba de auditorías para auditorías internas y externas

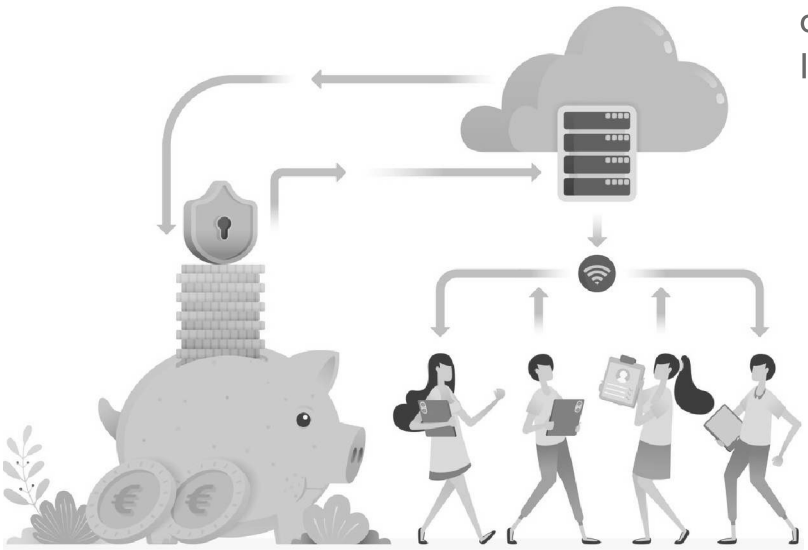
Armonización con las normas/estándares existentes

¿Qué significa esto para la implementación?

- **Armonización del ISMS/BCMS:** mapeo de controles y procesos
- **Informes de sinergia:** uso de cifras clave comunes y resultados de auditorías
- **Modelo GRC:** modelo integral de gobernanza, riesgo y cumplimiento que integra la resiliencia como una cuestión transversal

Ejemplo práctico: Example Ltd: control armonizado normativamente

Como operador de servicios en la nube para clientes financieros y administrativos, Beispiel GmbH está regulado tanto por DORA como por NIS-2. Hasta ahora, ISMS, ITSCM y BCM han funcionado sin una gestión integral de riesgos (informáticos).



Se está estableciendo un marco integrado como parte de la introducción de la norma ISO/IEC 27031:2025. Sus componentes son:

- la consolidación de las evaluaciones de riesgos (de TI) basadas en la norma ISO/IEC 27005
- la correspondencia de la norma con DORA y NIS-2 (por ejemplo, la asignación de controles a ISO/IEC 27002 A 5.30)
- la armonización de los objetivos de recuperación ICT-RTO/RPO entre BIA, BCM e IRBC
- la definición de una estructura de auditoría uniforme

Todas las medidas se recopilan en un único documento y se complementan con el alcance, las personas de contacto, las fechas de control y los ciclos de lecciones aprendidas. Esto significa que ahora se pueden documentar completamente los requisitos de auditoría interna y externa, con una documentación coherente y a prueba de auditorías.

Interfaz con ITIL 4 y distinción con respecto a IRBC

ITIL 4 continúa la práctica de la gestión de la continuidad de los servicios de TI (ITSCM), que se originó en la década de 1990. En el pasado, los términos ITSCM e IRBC se utilizaban a menudo como sinónimos, ya que ambos se centraban en la recuperación de las TI.

Armonización con las normas/estándares existentes

Con la nueva norma, el enfoque está cambiando significativamente de una recuperación puramente orientada al servicio (ITIL) a un enfoque de resiliencia en toda la organización (IRBC). Por lo tanto, en el futuro será importante indicar claramente si se hace referencia a las prácticas operativas de ITIL o al marco estratégico de IRBC. Los cambios en la nueva norma significan que las disciplinas están divergiendo en algunas áreas, pero siguen requiriendo una interacción coordinada.

Repercusión en los requisitos reglamentarios

Para las empresas reguladas (por ejemplo, los sectores financiero o KRITIS) que deben cumplir los requisitos de la norma ISO/IEC 27031, ya no es suficiente una mera implementación de ITSCM según ITIL. ITIL sigue cubriendo los procesos operativos de continuidad de TI para los servicios de TI críticos en términos de tiempo, pero no cumple los nuevos requisitos estratégicos de gobernanza, riesgo y resiliencia de la norma revisada.

Es posible ampliar un ITSCM existente para cumplir los requisitos de la norma ISO/IEC 27031:2025. El ITSCM se mantiene para la recuperación de TI y se le dota de una superestructura estratégica. Esta superestructura requiere una gobernanza formalizada, revisiones periódicas de la gestión y un programa de pruebas y auditorías orientado al riesgo. Esto traslada algunas tareas de la recuperación técnica de TI al trabajo de los comités, la gestión de los indicadores clave de rendimiento y la evaluación de riesgos.

Una desventaja importante surge de la diferente lógica de los procesos de ambos mundos. ITIL sigue un ciclo de vida centrado en el servicio, mientras que la norma ISO 27031 hace hincapié en el control estratégico basado en el riesgo. Si los requisitos de la norma ISO solo se «acoplan» superficialmente a los procesos de ITIL, el resultado es un híbrido que no cumple plenamente ni con los requisitos de eficiencia de ITIL ni con las obligaciones de documentación de la norma ISO. También existe el riesgo de un doble mantenimiento permanente. Los resultados de las pruebas, las lecciones aprendidas y los informes de KPI fluyen simultáneamente hacia la mejora continua de ITIL y los informes de IRBC. Esto crea el riesgo de rupturas en los medios y de información incoherente.

En consecuencia, la ITSCM debe funcionar como un subproceso dentro de la IRBC. Esto significa que las empresas reguladas deben incorporar la ITSCM existente en la estructura de gobernanza y pruebas de la IRBC, de modo que se cumplan plenamente los requisitos de auditoría y verificación de la norma. La ITSCM sigue siendo fundamentalmente relevante para la recuperación operativa de los servicios de TI críticos en el tiempo, mientras que la IRBC constituye el marco estratégico para la resiliencia de las TI en toda la organización. Ambas disciplinas de gestión deben sincronizarse mediante una gobernanza vinculante y exhaustiva.

Armonización con las normas/estándares existentes

Incluso sin ITSCM, las empresas pueden cumplir la norma ISO 27031 si el propio IRBC asume las tareas de ITIL. La implementación de ITSM o ITIL facilita la implementación operativa, pero no es un requisito obligatorio. Sin embargo, la nueva norma espera que el IRBC sustituya funcionalmente todos los procesos que faltan.

	IRBC (ISO 27031:2025)	Práctica ITSCM según ITIL 4
Objetivo	Garantizar la resiliencia de los servicios TIC críticos en términos de tiempo (incluida la gobernanza y la estrategia)	Reiniciar los servicios de TI de acuerdo con los objetivos de tiempo acordados
Ámbito	Organización (BCMS) e infraestructura de TI, gobernanza, riesgo, proveedores de servicios de TI y proveedores, datos	Servicios de TI críticos en cuanto al tiempo
Planificación	Estrategias (competencias, instalaciones, tecnología, etc.)	Acuerdos de nivel de servicio (SLA), infraestructura de TI, centro de datos
Enfoque	Ciber, cadena de suministro, cumplimiento normativo, datos y resiliencia de los proveedores de servicios (informáticos)	Infraestructura de TI, acuerdos de nivel de servicio (SLA) de TI
Gobernanza	Matriz de funciones que incluye al director/propietario del IRBC y la revisión de la gestión Buenas prácticas: Comité de resiliencia	Propietario de la práctica, gestor de la práctica y propietario del servicio

La nueva norma ISO/IEC 27031:2025 establece claramente que IRBC e ITSCM no son sinónimos. Mientras que ITSCM es una práctica operativa de ITIL responsable de la recuperación de los servicios TIC, IRBC define un marco estratégico para la gestión de la resiliencia TIC en toda la empresa. Los requisitos normativos, en particular los de DORA y NIS-2, solo pueden cumplirse si se implementa IRBC. ITSCM puede integrarse en este, pero no puede utilizarse por sí solo.

Ampliación de las funciones del gestor del IRBC

La norma ISO/IEC 27031:2025 revisada cambia fundamentalmente el papel del gestor de IRBC. Mientras que antes se encargaba principalmente de planificar y aplicar medidas de recuperación de TI de acuerdo con los requisitos de continuidad de BCM, ahora sus funciones se han ampliado considerablemente. Ya no es principalmente un planificador de medidas de recuperación de TI, sino que desarrolla activamente estructuras de TI resilientes, analiza los riesgos de TI, planifica modelos operativos de TI alternativos y coordina las medidas y procesos adecuados con BCM, ISM, respuesta a incidentes y gestión de crisis.

Esto requiere la capacidad de diseñar estructuras de TI resilientes con previsión, proporcionar modelos operativos de TI alternativos y garantizar la funcionalidad de los servicios TIC críticos en términos de tiempo, incluso en caso de ciberataques complejos. En el futuro, no solo tendrán que planificar la recuperación de TI en caso de un incidente crítico de TI, sino también garantizar la operatividad continua de TI en estrecha coordinación con BCM, la gestión de incidentes, la planificación de la respuesta cibernética y la gestión de crisis, por ejemplo, en caso de un ciberataque.

Al hacerlo, actúan como integradores técnicos entre los requisitos técnicos, organizativos y estratégicos, y deben tener habilidades interfuncionales. Además de los conocimientos tecnológicos, esto incluye conocimientos de gestión de riesgos (informáticos), análisis de procesos empresariales, seguridad de la información, gestión de pruebas y comunicación.

Una nueva área de responsabilidad clave es la definición y el mantenimiento del MBCO definitivo en colaboración con el BCM, incluidos los estudios de viabilidad técnica y la derivación de estrategias de recuperación (informática) adecuadas. Entre sus tareas también se incluye la gestión de proveedores de servicios (informáticos) externos, incluida la especificación contractual de medidas de resiliencia para minimizar los riesgos de las cadenas de suministro.

Es responsable de la auditabilidad, controlabilidad y trazabilidad de todas las medidas del IRBC. Estos aspectos se especifican como requisitos sujetos a auditoría y se comprueban durante la misma.

Ampliación de las funciones del gestor del IRBC

¿Qué exige específicamente la norma?

- Responsabilidad estratégica para ayudar a definir los objetivos de resiliencia, la planificación presupuestaria y la presentación de informes a la alta dirección
- Experiencia arquitectónica para evaluar y diseñar entornos de TI resilientes (redundancia, confianza cero, conmutación por error en la nube).
- Coordinación con BCM y gestión de incidentes/respuesta a incidentes cibernéticos para garantizar que la recuperación de TI solo se lleve a cabo tras la aprobación forense, incluida la coordinación de las escaladas
- Responsabilidad del ciclo de vida en lo que respecta al desarrollo, mantenimiento, pruebas y auditoría de todos los planes de continuidad de TI
- Responsabilidad de las habilidades, la formación y los recursos necesarios para las medidas de resiliencia
- Planificación y control de pruebas, seguimiento de KPI y proceso de lecciones aprendidas para la medición y la mejora
- Gestión de proveedores de servicios externos (TI) y definición de los requisitos contractuales de resiliencia

¿Qué significa esto?

El responsable del IRBC es responsable de implementar todo el ciclo de vida del IRBC, desde el análisis y las opciones de solución hasta la gestión de ejercicios y auditorías. Además, en el futuro se convertirá en el planificador central de un entorno de TI resiliente que integra la ciberresiliencia y está diseñado para el mantenimiento robusto de los servicios de TI críticos en el tiempo. Esto incluye la capacidad de mantener y activar entornos operativos de TI alternativos para incidentes críticos de TI.

Especialmente en el contexto de las amenazas cibernéticas (por ejemplo, ransomware, APT), asumirá en el futuro la responsabilidad operativa y estratégica. Esto incluye:

- Desarrollo de arquitecturas (informáticas) resilientes: diseño multizona, conmutación automática por error, marco de copia de seguridad inmutable, estrategias de salida de la nube.
- Revisiones periódicas de la arquitectura de resiliencia (RAR) para sistemas nuevos o modificados
- Evaluación técnica del cumplimiento de ICT-RTO, ICT-RPO y MBCO final, especialmente en caso de incidentes cibernéticos
- Integración y coordinación de los procesos de respuesta y recuperación de TI para servicios de TI en los que el tiempo es un factor crítico

Ampliación de las funciones del gestor del IRBC

Ejemplo práctico: Example Ltd: control armonizado normativo

Originalmente, el responsable de ITSC de Example Ltd coordinaba la planificación de la recuperación de acuerdo con ITIL. Con la introducción de la norma ISO/IEC 27031:2025, se nombró a un responsable de IRBC dedicado con responsabilidad integral sobre el análisis, la planificación, la arquitectura de TI, las pruebas y la documentación.

El responsable de IRBC introdujo una revisión anual de la arquitectura de resiliencia (RAR), planificó una zona virtual de conmutación por error en la nube e implementó copias de seguridad inmutables. Para cada sistema informático crítico,

- las especificaciones del BIA (por ejemplo, RTO de dos horas),
- las opciones técnicas
- y los procesos organizativos

se coordinaron metódicamente.

La derivación de los objetivos de recuperación del IRBC a partir del BIA ahora se documenta en:

- el concepto de solución IRBC (con mapeo RTO/RPO)
- el registro de medidas con evaluación y aprobación
- el protocolo de lecciones aprendidas de las pruebas
- el protocolo de escalado para incidentes cibernéticos

La función del gestor del IRBC está firmemente arraigada en el Consejo de Resiliencia, con responsabilidad directa en la consecución de los objetivos, la eficacia y la trazabilidad de la arquitectura informática resiliente

Enfoque en la resiliencia digital y la ciberresiliencia

La norma ISO/IEC 27031:2025 marca un cambio significativo en el enfoque del IRBC. Mientras que anteriormente se centraba principalmente en la recuperación de los servicios informáticos críticos en términos de tiempo tras un incidente informático grave, ahora se centra en la capacidad de los sistemas y estructuras informáticos para seguir funcionando, responder de forma adaptativa y aprender de manera específica, incluso en condiciones dinámicas, inciertas y potencialmente destructivas, como los ciberataques. Esto sitúa el concepto de resiliencia en el centro del enfoque del IRBC. La resiliencia se entiende no solo como un objetivo técnico, sino como un principio de gestión estratégicamente arraigado en toda la organización.

Esta nueva orientación se refleja especialmente en los requisitos de planificación proactiva, mejora continua, organizaciones adaptables y desarrollo de sistemas robustos, pero también adaptables. La resiliencia afecta a los sistemas informáticos, así como a los procesos, los empleados, las cadenas de suministro y los mecanismos de control organizativo. Esto convierte al IRBC en un componente esencial de la gestión integral de la resiliencia, en la que se deben tener en cuenta por igual los aspectos técnicos, organizativos y culturales.

Además, la norma exige explícitamente medidas técnicas como la segmentación de la red, el almacenamiento redundante de datos, las arquitecturas de confianza cero, las comprobaciones de integridad de los datos y los mecanismos de recuperación que funcionen de forma fiable incluso en condiciones de ataque activo. Estas especificaciones están vinculadas a parámetros de control de tiempo y se asignan a un nivel mínimo de rendimiento definido (MBCO final).

¿Qué significa esto en términos concretos?
El IRBC se establece como parte de una estrategia de resiliencia para toda la empresa. El enfoque pasa de la mera planificación de la continuidad de las TI a la protección estratégica de la capacidad empresarial mediante una respuesta controlada, la adaptación, la solidez, la redundancia y la capacidad de aprendizaje. El enfoque ya no se centra en la recuperación de las TI, sino en mantener la capacidad de actuar y hacer frente a la incertidumbre de forma resiliente, de acuerdo con los siguientes principios:

- **Adaptación:** capacidad de adaptarse a situaciones de amenaza cambiantes
- **Robustez:** resistencia a incidentes o ataques críticos de TI
- **Redundancia:** disponibilidad de recursos y sistemas de TI alternativos
- **Capacidad de aprendizaje:** establecimiento de bucles de retroalimentación a partir de incidentes y ejercicios

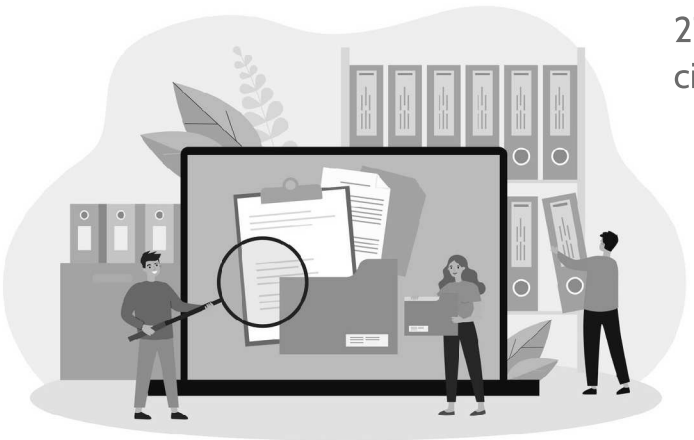
Enfoque en la resiliencia digital y la ciberresiliencia

La resiliencia digital se entiende como un objetivo estratégico que debe garantizarse mediante medidas técnicas, organizativas y estratégicas que van mucho más allá de la recuperación clásica de TI.

Implementación:

- Derivación de los requisitos de resiliencia (informática) a partir de los objetivos estratégicos de la empresa y los análisis de riesgos (informáticos)
- Integración de principios que promueven la resiliencia en la arquitectura de TI, los procesos y la cultura corporativa
- Establecimiento de bucles de retroalimentación y aprendizaje a partir de ejercicios, pruebas de TI e incidentes críticos de TI
- Desarrollo de KPI de resiliencia (informática) medibles y su evaluación periódica como parte de las revisiones de la dirección

Ejemplo práctico
Example Ltd. opera una plataforma para procesos de administración municipal. Una prueba del equipo rojo simuló un ataque de ransomware al DMS. Aunque se contaba con planes de recuperación de TI, se hizo evidente que no se había tomado ninguna decisión forensemente segura sobre la restauración de datos.



Durante la implementación de la norma ISO/IEC 27031:2025, se desarrolló una estrategia de ciberresiliencia:

- Se amplió la copia de seguridad de los datos para incluir copias de seguridad inmutables con redundancia geográfica.
- Se implementó técnicamente una red de emergencia segmentada como zona de recuperación independiente.
- Los procesos de recuperación de TI y restauración de datos se coordinaron con la gestión de respuesta a incidentes cibernéticos, incluyendo los pasos de liberación forense.

Ahora, la plataforma también se puede restaurar de forma controlada durante ataques activos, con un cumplimiento documentado de los RTO y RPO de las TIC y decisiones de gestión trazables.

Enfoque tecnológico y relacionado con los datos

La nueva norma hace especial hincapié en los fundamentos tecnológicos y los requisitos relacionados con los datos en el marco del IRBC. La resiliencia ya no se considera únicamente a nivel de procesos, sino también de forma explícita a nivel de los recursos informáticos necesarios, es decir, las infraestructuras, los sistemas y las aplicaciones informáticas.

La norma exige que se identifiquen sistemáticamente las dependencias tecnológicas, se definan canales alternativos de suministro y provisión, y se garantice la integridad de los datos incluso en caso de incidentes informáticos críticos, como ciberataques.

Se hace hincapié en la capacidad de poner a disposición servicios informáticos urgentes en plazos de recuperación aceptables. Esto incluye la copia de seguridad y la restauración de configuraciones de sistemas, bases de datos, infraestructuras de comunicación y acceso a aplicaciones basadas en la nube. También se abordan explícitamente aspectos como la redundancia geográfica, la segmentación de las conexiones de datos, la seguridad de las plataformas SaaS y la resiliencia de las interfaces.

¿Qué exige específicamente la norma?

La resiliencia de los entornos informáticos y la integridad de los datos críticos para el negocio se están convirtiendo en el centro de la planificación de la IRBC. La norma exige un conocimiento detallado de las dependencias técnicas y una planificación adecuada y apropiada de la recuperación informática, especialmente para las infraestructuras informáticas físicas y virtuales, las aplicaciones, los datos y el uso de la nube.

Técnicamente, esto significa que las arquitecturas de TI deben diseñarse y operarse para ser resilientes desde el principio, mediante el uso de redundancias, sistemas distribuidos, mecanismos de conmutación por error automatizados, microsegmentación o estrategias de alta disponibilidad basadas en la nube. En términos organizativos, la norma exige el establecimiento de responsabilidades claras, procesos de supervisión y escalamiento continuos, y la participación de personal con conocimientos específicos para mantener los servicios de TIC críticos en condiciones difíciles.

Enfoque tecnológico y relacionado con los datos

La norma ISO/IEC 27031:2025 destaca los siguientes requisitos en varias secciones:

- Documentación de todos los servicios TIC críticos en términos de tiempo, incluidos los valores de tiempo de recuperación asignados (ICT-RTO, ICT-RPO, MBCO final) y su función en el proceso empresarial.
- Los componentes de TI (por ejemplo, la infraestructura de TI, los sistemas de TI, las aplicaciones y las interfaces) deben documentarse tanto para el funcionamiento normal como para los entornos operativos de TI alternativos, incluida su configuración.
- La norma exige el uso de tecnologías de TI adecuadas para garantizar la resiliencia, por ejemplo, diseño de redundancia, conmutación automática por error, clústeres en la nube y procedimientos de copia de seguridad que cumplan con el RPO con ubicaciones de almacenamiento y rutas de acceso definidas.
- Para cada servicio TIC crítico en el tiempo, debe demostrarse claramente qué proceso crítico para el negocio soporta y cómo se ha diseñado la tecnología y la estructura de la arquitectura de TI asociadas.
- Las desviaciones entre el rendimiento técnico de TI (por ejemplo, el RTO de TIC alcanzable) y los valores objetivo definidos por el BCM deben identificarse, evaluarse en cuanto a riesgos, abordarse en el informe de gestión y aprobarse.

Implementación (medidas recomendadas)

Resiliencia por diseño:

- Planificación de arquitecturas de sistemas informáticos resilientes con redundancia, segmentación, mecanismos de conmutación por error automatizados y estrategias de alta disponibilidad basadas en la nube.

Resilient Data Management:

- Proteger, aislar y garantizar la disponibilidad de los datos a pesar de los riesgos.

Detektion und Kontrolle:

- Integración de componentes forenses, detectivos y preventivos para la detección temprana y el aislamiento.

Enfoque tecnológico y relacionado con los datos

Además, la norma ISO/IEC 27031:2025 IRBC también aborda las amenazas digitales y cibernéticas. De este modo, la norma contribuye al desarrollo de una comprensión integral de la resiliencia, tal y como se describe también en

- **DORA**
  - Art. 10: Marco de gestión de riesgos de las TIC
  - Art. 11: Política de continuidad del negocio de las TIC y planes de respuesta y recuperación
- **Marco de ciberseguridad del NIST**
  - Función «Recuperar» (RC.IM-1 a RC.IM-3)
  - Funciones «Responder» (RS) e «Identificar» (ID)

Esto convierte al IRBC en una parte integral de la gestión de riesgos de TI y de la resiliencia estructural y operativa de TI frente a escenarios de amenazas complejos, incluidos los causados por ciberataques.

La tabla ofrece una visión general de los temas clave:

Área temática	Contenidos principales
Arquitectura de TI resiliente	Diseño multizona y multirregional, mecanismos de conmutación automática por error, «defensa en profundidad»
Gestión de datos resiliente	Copias de seguridad inmutables/aisladas, protección contra el cifrado, ejercicios de restauración periódicos
Detección y control	Herramientas forenses, detección de anomalías, mecanismos de alerta temprana
Confianza cero y microsegmentación	Aplicación del privilegio mínimo, autenticación continua, aislamiento de segmentos comprometidos
Dependencias de la nube y SaaS	Estrategias de salida, agrupación multicloud, garantías RTO/RPO vinculantes por contrato
Observabilidad y telemetría	Canalización unificada de registros, detección de anomalías basada en IA, indicadores de alerta temprana para la corrupción de datos
Cumplimiento normativo, cifrado y gestión de claves	Políticas conformes con el RGPD/DORA, control del ciclo de vida de las claves, uso de HSM

Enfoque tecnológico y relacionado con los datos

Para las empresas, esto significa que no solo deben contar con planes de contingencia de TI para la recuperación de TI, sino que también deben garantizar el funcionamiento continuo de sus servicios TIC e infraestructuras de TI críticos en términos de tiempo, incluso en situaciones de estrés, y demostrar permanentemente esta capacidad mediante medidas y documentación adecuadas. La resiliencia se convierte así en un objetivo estratégico y el IRBC en un elemento central de la resiliencia empresarial digital.

¿Qué significa esto para la implementación?

- Identificación de las dependencias críticas de la tecnología y los datos de TI como parte del análisis de riesgos (de TI)
- Definición de rutas de datos redundantes y conceptos de recuperación de TI para entornos de TI híbridos
- Planificación de escenarios para la recuperación de datos y aplicaciones, incluida una estrategia de pruebas de TI
- Garantía de la integridad y disponibilidad de los datos incluso en escenarios de ataque

Ya no basta con disponer de planes de recuperación de TI y/o scripts de copia de seguridad. Las empresas deben alinear constantemente sus tecnologías de TI con sus objetivos de resiliencia.

Los pasos típicos incluyen:

- Revisión de la arquitectura de resiliencia (RAR) para cada proyecto importante de TI/TO, incluyendo la comprobación de la redundancia geográfica, el diseño de la segmentación y el mapeo de dependencias.
- Marco de copias de seguridad inmutable y credenciales separadas, política de escritura única, pruebas de restauración automatizadas periódicas en un entorno aislado.
- Fortalecimiento continuo y canalización de parches, infraestructura como código.
- Simulacros de salida de la nube a un proveedor alternativo/clúster local, incluida la medición documentada del RTO.
- Alerta temprana basada en telemetría: retraso de datos, puntuación de estado de la instantánea, tasa media de éxito de la conmutación por error; informe directo al Consejo de Resiliencia.

Enfoque tecnológico y relacionado con los datos

Ejemplo práctico: Example Ltd: la tecnología de resiliencia como principio de arquitectura de TI

Example Ltd opera un centro de datos híbrido con servicios SaaS y de plataforma. Una auditoría reveló que los objetivos de recuperación del archivo de datos no se ajustaban al BIA. RPO requerido según el BCM: dos horas; técnicamente factible: ocho horas

Como resultado, se estableció una revisión de la arquitectura de resiliencia (RAR):

- Segmentación de la conexión de la base de datos para su aislamiento en caso de ataque.
- Introducción de copias de seguridad inmutables, almacenamiento separado de credenciales, prueba de restauración automatizada
- Simulacro de salida de la nube, incluida la medición y documentación del RTO
- Análisis de deficiencias en una matriz tecnológica IRBC; informe al Consejo de Resiliencia

Las medidas se registraron como un marco de resiliencia tecnológica en el sistema de documentación del IRBC, incluyendo el estado de las deficiencias para BIA-RTO/BIA-RPO y las lecciones aprendidas de los escenarios de los ejercicios.

Requisitos empresariales y control basado en BIA

Aunque no es una novedad en la práctica, un requisito clave de la norma ISO/IEC 27031:2025 es la derivación coherente de todas las medidas IRBC a partir de los requisitos empresariales. En lugar de limitarse a especificar los tiempos de recuperación de las TI, la norma exige que el análisis del impacto empresarial (BIA), la evaluación de riesgos y los objetivos de recuperación de las TIC estén estrechamente interrelacionados.

Lo nuevo es la clara separación entre los objetivos de continuidad del negocio (BIA-RTO/RPO) y los objetivos técnicos de TI (ICT-RTO/RPO). Se aplica lo siguiente: ICT-RTO/RPO ≤ BIA-RTO/RPO. Las desviaciones deben subsanarse mediante inversiones o documentarse como un riesgo en el proceso final de MBCO.

La nueva norma exige una trazabilidad completa (cadena de pruebas) desde el proceso empresarial hasta las pruebas de TI. Cada asignación debe documentarse y revisarse anualmente o en caso de cambios significativos.

Esto crea una cadena cerrada de:

Proceso empresarial → Evaluación de la criticidad/BIA → BIA-RTO/RPO → MBCO → ICT-RTO/RPO → MBCO final → Estrategia y plan

¿Qué exige exactamente la norma?

Los servicios TIC deben analizarse en función de la dependencia de los procesos, la criticidad y la prioridad de recuperación. A partir de ahí se derivan los valores objetivo (RTO, RPO, MBCO), las estrategias de recuperación y los recursos, teniendo en cuenta los requisitos externos.

Las organizaciones deben garantizar que cada activo de TI esté configurado de manera demostrable para que se cumpla con el BIA RTO/RPO definido por el departamento especializado. Los pasajes más importantes del texto de la norma se pueden agrupar de la siguiente manera:

Capítulo	Requisito básico
Expectativas empresariales para el IRBC	• Identificación de los procesos empresariales críticos y sus dependencias de las TIC • Determinación de los MBCO iniciales y las prioridades • Documentación de los requisitos externos/normativos
Definición de los requisitos previos para el IRBC	• Derivación de los RTO/RPO de las TIC a partir de los resultados del BIA • Determinación del MBCO definitivo tras la comprobación de riesgos y viabilidad • Validación de los objetivos por parte de la dirección
Plan de continuidad de TI	• Los planes deben reflejar el RTO/RPO, las soluciones alternativas y la transición de una emergencia de TI a un funcionamiento normal de TI (MBCO final → recuperación completa)

Requisitos empresariales y control basado en BIA

La norma también exige lo siguiente:

- Cada asignación de proceso → activo de TI → RTO/RPO debe almacenarse en una matriz de trazabilidad rastreable.
- Al menos una vez al año, o en caso de cambios significativos, se deben verificar conjuntamente el BIA-RTO/RPO, el MBCO y el ICT-RTO/RPO.
- Si existen deficiencias, se deben documentar y aprobar por parte de la alta dirección medidas técnicas, estrategias alternativas o la aceptación formal del riesgo (MBCO final).
- Cada ICT-RTO debe verificarse mediante ejercicios programados o pruebas de conmutación por error; los resultados se incorporan a las lecciones aprendidas.

¿Qué significa esto para la implementación?

La separación coherente de BIA-RTO/RPO e ICT-RTO/RPO desplaza el enfoque de la planificación de la recuperación de TI puramente técnica a la gestión de la resiliencia impulsada por el negocio. Por encima de todo, la norma exige un principio de cadena de pruebas coherente. Esto significa que cada requisito técnico debe ser trazable hasta la configuración final del sistema de TI y las pruebas finales.

Por lo tanto, las empresas deben alinear su gobernanza de la continuidad de tal manera que

- los departamentos especializados especifiquen tiempos de tolerancia de proceso vinculantes,
- el equipo IRBC traduzca estos valores directamente en objetivos de TI viables,
- todos los pasos intermedios (MBCO → ICT-RTO/RPO → MBCO final) se documenten de forma transparente, versionada y auditable.

Esto requiere no solo una estrecha coordinación entre la gestión de la continuidad del negocio (BCM), la gestión de la continuidad del negocio y la recuperación (IRBC) y la gestión de riesgos (TI), sino también una planificación de las inversiones para subsanar las deficiencias técnicas o aceptar formalmente los riesgos. Solo cuando esta cadena de trazabilidad esté completamente documentada se considerará que se cumple el requisito de la norma.

Deben establecerse métodos estructurados para la evaluación de la criticidad, el análisis de dependencias y la derivación de objetivos. De este modo, el IRBC se convierte en parte integrante de la evaluación operativa del riesgo y la resiliencia (TI).

Requisitos empresariales y control basado en BIA

Ejemplo práctico: Example Ltd

Example Ltd opera servicios en la nube para portales fiscales municipales. La BIA determinó que los departamentos responsables del portal de auditoría fiscal aceptan una interrupción máxima de cuatro horas (BIA-RTO). Sin embargo, el análisis de deficiencias reveló que, en caso de fallo total, la restauración de la infraestructura en la nube lleva alrededor de seis horas (ICT-RTO).

Como resultado, se decidieron las siguientes medidas:

- Actualización técnica de la capa de almacenamiento con replicación de instantáneas
- Adaptación de la opción de solución IRBC (por ejemplo, conmutación por error)
- Aceptación formal del riesgo por parte de la alta dirección hasta su implementación

Todos los pasos se documentaron en una matriz de trazabilidad:

- Proceso empresarial → BIA-RTO/RPO → MBCO → ICT-RTO/RPO → MBCO final → Estrategia y plan de recuperación
- Además, el nuevo valor se verificó en la prueba de la función de TI y se integró en el informe de pruebas IRBC.

Esto significa que el enlace BIA se verifica desde el punto de vista técnico, organizativo y documental.

Planificación basada en el riesgo y MBCO final

El MBCO (objetivo mínimo de continuidad del negocio) no es una novedad en la norma actual. Sin embargo, lo que sí es nuevo es el enfoque ampliado de la norma ISO/IEC 27031:2025, que introduce el denominado MBCO final. El MBCO describe el nivel mínimo de rendimiento requerido de un proceso empresarial crítico en el tiempo o del servicio TIC de apoyo que debe mantenerse en un incidente crítico (de TI) o alcanzarse dentro del RTO para evitar consecuencias graves. El MBCO se deriva del BIA.

El MBCO final es el resultado validado de un proceso de planificación en el que no solo se deriva el resultado puro del BIA, sino que también se derivan los resultados del BIA sobre una base basada en el riesgo, teniendo en cuenta:

- la viabilidad técnica y organizativa
- las dependencias técnicas y organizativas (por ejemplo, cadenas de suministro, proveedores de servicios (informáticos))
- escenarios de amenazas y vulnerabilidades
- los resultados de pruebas, ejercicios y auditorías

El MBCO final sirve como variable de planificación y control para todas las medidas (informáticas) y organizativas que van más allá de las operaciones de emergencia informática inmediatas y que tienen por objeto garantizar la estabilidad de las operaciones comerciales. Además, se requiere la derivación y validación basada en el riesgo de los objetivos de continuidad.

Esto significa que los valores de RTO, RPO y MBCO no deben fijarse de forma estática, sino que deben revisarse y ajustarse periódicamente en el contexto de posibles escenarios de amenaza, probabilidades de ocurrencia y efectos de los daños.

El MBCO final debe documentarse formalmente, validarse sobre la base del riesgo y ser aprobado por la dirección. Por lo tanto, es vinculante para la planificación de incidentes críticos de TI y la estrategia de recuperación de TI. El MBCO final no es, por lo tanto, solo un resultado de análisis, sino un objetivo especificado y documentado.

Planificación basada en el riesgo y MBCO final

¿Qué exige específicamente la norma?

La norma exige una distinción explícita entre el funcionamiento temporal de emergencia de TI (MBCO) y el objetivo operativo final (de TI) (MBCO final). Este valor objetivo es crucial para la planificación de la recuperación (de TI), la priorización de recursos y el diseño de estrategias de recuperación (de TI). El MBCO final sirve como variable de planificación y control para todas las medidas que van más allá de la provisión de emergencia inmediata y tienen por objeto restablecer el funcionamiento estable de la empresa. De un vistazo:

- Separación explícita entre MBCO y MBCO final
- Validación basada en el riesgo: viabilidad técnica, dependencias, proveedores, personal
- Aprobación por parte de la dirección del MBCO final, incluida la aceptación documentada de los riesgos
- Derivación del plan y la estrategia: las medidas de recuperación deben mostrar cómo se llevará a cabo la transición de la MBCO de emergencia a la MBCO final.
- Revisión al menos una vez al año o en caso de cambios significativos; verificación en la revisión de la dirección

Los objetivos de recuperación no se definen de forma aislada, sino que se analizan y validan en el contexto de un escenario global realista y basado en el riesgo. El objetivo es aumentar el compromiso estratégico con los objetivos de recuperación de TI y minimizar las inconsistencias entre las perspectivas empresariales y de TI. La validación del MBCO final tiene por objeto garantizar que todos los planes de recuperación de TI sean viables desde el punto de vista organizativo, técnico y contractual.

¿Qué significa esto para la implementación?

La implementación de la planificación basada en el riesgo comienza con un análisis ampliado basado en el BIA que se ha llevado a cabo. También deben tenerse en cuenta las probabilidades de ocurrencia, las dependencias de los proveedores y los escenarios de amenaza. Este nivel de detalle tiene por objeto dejar claro dónde no son suficientes las capacidades de recuperación de TI puramente técnicas.

- Planificación basada en el riesgo = BIA + factores de riesgo y dependencia (IT) (escenarios de amenaza, proveedores de servicios de TI, viabilidad)

La norma describe esto en «Aportaciones del análisis del impacto en el negocio» y exige que la alta dirección confirme formalmente los resultados y requisitos determinados de esta manera.

Planificación basada en el riesgo y MBCO final

Los pasos de implementación en detalle:

1. **Análisis ampliado**
Las amenazas, las probabilidades de ocurrencia y las dependencias se registran sobre la base del BIA.

2. **Análisis de viabilidad**
Se identifican las diferencias entre el objetivo (BIA-RTO/RPO) y las capacidades técnicas/organizativas reales (ICT-RTO/RPO).

3. **Decisión basada en el riesgo**
Inversión o aceptación formal del riesgo mediante la aprobación de un MBCO final más alto por parte del Consejo de Resiliencia.

4. **Dokumentation und Versionierung**
Actualización del MBCO final en la matriz de trazabilidad, el plan de recuperación de TI, el registro de riesgos y la documentación de auditoría.

5. **Pruebas y revisión**
Realizar pruebas de escenarios y validar la transición del MBCO al MBCO final. Incorporar los resultados al panel de indicadores clave de rendimiento (KPI) y a las lecciones aprendidas.

Ejemplo práctico: Example Ltd – MBCO frente a MBCO final

Example Ltd opera un sistema central de tramitación de reclamaciones para clientes del sector de los seguros. El BIA especifica el MBCO de la siguiente manera: funcionamien-to de emergencia mediante procesamiento manual, recuperación limitada de datos durante un máximo de 48 horas.

El análisis de deficiencias muestra que la recuperación completa del servicio de TIC (con portal de clientes, replicación de bases de datos e integración de CRM) solo es posible después de 72 horas.

Esto da como resultado un MBCO final: funcionamiento del sistema con un 80 % de funcionalidad después de 72 horas, incluido el estado actual de los datos

La Junta de Resiliencia acepta la brecha mediante una resolución formal. El MBCO final se documenta, se prueba y se tiene en cuenta en la planificación de la recuperación de TI.

Planificación de la recuperación y requisitos de documentación

Los planes IRBC deben abarcar no solo los procesos técnicos de recuperación de TI, sino también los procedimientos organizativos, las soluciones alternativas y los canales de comunicación. En la edición de 2011, se recomendaban planes de continuidad, pero se consideraban principalmente artefactos técnicos auxiliares de los proyectos de recuperación ante desastres. La revisión de 2025 los eleva a un «control de eficacia» central. Un plan solo cumple con la norma si

- refleja claramente la separación entre el RTO/RPO empresarial y el RTO/RPO de las TIC,
- hace referencia al MBCO final como valor objetivo vinculante,
- se mantiene actualizado de forma demostrable mediante un ciclo de vida controlado con control de versiones, pruebas y revisiones.

Los manuales estáticos deben convertirse en documentos controlados, versionados y auditables, independientemente del medio. Es fundamental la vinculación verificable entre el contenido, la aprobación, las pruebas y las lecciones aprendidas.
Los planes deben estar basados en funciones, relacionados con escenarios, completamente documentados, probados periódicamente, actualizados e integrados en la documentación de BCM. Los procesos de comunicación, escalamiento y toma de decisiones deben estar regulados de manera vinculante. La norma define siete bloques de contenido obligatorios.

Sección	Contenido
Propósito y alcance	Vínculo con el BIA, servicios críticos, criterios de activación
Organización de la recuperación	Funciones, vías de escalamiento, datos de contacto, suplentes
Matriz de objetivos	Prueba de que el RTO/RPO de las TIC es ≤ al RTO/RPO del BIA, incluida la referencia final del MBCO
Manuales de procedimientos paso a paso	Procedimientos técnicos, soluciones alternativas, transición al funcionamiento de emergencia
Canales de comunicación	Flujo de aprobación, coordinación con la respuesta a incidentes y BCM
Proveedores y dependencias	Contactos, SLA, informes de pruebas, cláusulas de salida
Verificación del ciclo de vida	Versiones, pruebas, revisiones, lecciones aprendidas

Es fundamental que toda la información se almacene de forma que pueda ser auditada y esté rápidamente disponible incluso en caso de fallo informático.

Planificación de la recuperación y requisitos de documentación

¿Qué significa esto para la implementación?

En términos prácticos, este requisito se traduce en un **proceso de control de documentos** independiente y auditable dentro del IRBC. Las empresas deben definir una plantilla de plan uniforme, establecer una lógica de versiones y aprobación, y fijar un calendario de pruebas vinculante. Es secundario si utilizan un DMS, un repositorio Git a prueba de auditorías o una carpeta de emergencia gestionada físicamente. Lo importante es que los cambios, las pruebas y las revisiones se registren de forma trazable y que siempre haya una **copia disponible fuera de línea**. Además, tiene mucho sentido establecer un vínculo automático con la gestión de cambios e incidentes, de modo que cada cambio relevante en los sistemas o procesos informáticos active automáticamente una revisión del plan y los resultados de las pruebas se incorporen a un panel de control de KPI de resiliencia.

Pasos de implementación

1. Definir la plantilla del plan: estructura uniforme para las pruebas de auditoría
2. Configurar el control de documentos, incluido el flujo de trabajo de aprobación
3. Vincular los desencadenantes de cambios: los cambios relevantes desencadenan automáticamente revisiones del plan
4. Garantizar la disponibilidad sin conexión: copias en salas de emergencia y/o crisis de TI, ordenadores portátiles de emergencia o entorno seguro en la nube

Ciclo de vida del plan

Creación → Control de versiones → Prueba → Revisión → Lecciones aprendidas → Actualización

- Control de versiones: cada cambio con nota de lanzamiento (propietario y fecha)
- Realizar pruebas periódicas a intervalos regulares o cuando se realicen cambios en el sistema
- Incorporar los resultados de la revisión en el informe de gestión
- Lecciones aprendidas: documentar las mejoras y las comparaciones de los KPI

Estrategias IRBC y diseño de recuperación

La norma ISO 27031:2025 estructura la selección de estrategias IRBC en seis categorías de impacto. El objetivo es lograr un diseño de resiliencia holístico que integre aspectos técnicos, organizativos y relacionados con los proveedores. Las estrategias no deben considerarse de forma aislada, sino en su interacción entre sí, con el fin de crear soluciones coherentes y económicamente viables.

Las estrategias o soluciones deben derivarse de las categorías de habilidades, instalaciones, tecnología, datos, procesos y proveedores. La selección debe basarse en el riesgo, ser económicamente viable y estar coordinada. Las interacciones deben analizarse y las estrategias deben documentarse de manera comprensible.

¿Qué exige específicamente la norma?

Se deben desarrollar, evaluar y documentar estrategias o conceptos de solución para cada una de las seis categorías:

Categoría	Opciones típicas	Criterios de selección
Habilidades y conocimientos	Formación cruzada, redundancia de habilidades, certificaciones	Habilidades críticas, disponibilidad de expertos
Instalaciones	Segunda ubicación, centro de datos independiente del operador, centro de datos móvil	Riesgos geográficos y climáticos, conectividad
Tecnología	Clúster activo-activo, conmutación automática por error, segmentos de confianza cero	RTO/RPO, complejidad, modelos de licencia
Datos	Copias de seguridad inmutables, separación física, replicación en tiempo real	Requisitos de RPO, volumen de datos, latencia
Procesos	Libros de ejecución automatizados, guías SOAR, matriz de escalamiento	Criticidad de los procesos, madurez de la automatización
Proveedores	Estrategias multicloud, conmutación por error del proveedor, cláusulas de salida	Riesgos de dependencia, calidad del SLA, sanciones contractuales

Estrategias IRBC y diseño de recuperación

¿Qué significa esto para la implementación?

- Las estrategias deben seleccionarse en función del riesgo y la viabilidad económica.
- Las interacciones y dependencias deben analizarse y documentarse.
- Cada estrategia debe estar alineada con los objetivos definidos de RTO/RPO/MBCO.
- La implementación debe revisarse y ajustarse periódicamente.

Las empresas deben establecer un proceso estructurado para el desarrollo de estrategias. Esto incluye, como mínimo:

- Esquema de evaluación de riesgos, costes, complejidad y viabilidad
- Comparaciones de escenarios (por ejemplo, diseño de recuperación técnica frente a organizativa)
- Análisis económicos (CAPEX, OPEX, costes del ciclo de vida)
- Un documento central de estrategia de resiliencia que sirva de referencia para la planificación, las pruebas y las auditorías

Ejemplo práctico

Se desarrolla una combinación de conmutación por error en la nube, operaciones de emergencia de TI descentralizadas y soluciones manuales para una plataforma crítica de servicio al cliente. La estrategia se valida y documenta periódicamente con las partes interesadas.

Recomendaciones de implementación para empresas

Transición de la norma ISO 27031:2011 a la versión de 2025

Para las empresas que anteriormente han trabajado según la norma ISO/IEC 27031:2011 o un marco clásico de recuperación ante desastres de TI, se recomienda un modelo de migración en tres etapas. El objetivo es integrar gradualmente los nuevos requisitos de gobernanza, las obligaciones de documentación ampliadas y el concepto de MBCO final sin sobrecargar las operaciones de TI en curso.

Paso 1: análisis de deficiencias

Objetivo: registrar la situación actual e identificar las deficiencias en comparación con la norma ISO/IEC 27031:2025

Procedimiento:

- Recopilar todos los documentos pertinentes: planes de continuidad de las TIC, manuales de emergencia, informes de pruebas, resultados del BIA, informes de auditoría.
- Comparar los documentos con los 13 capítulos de la norma.
- Deficiencias comunes:
  - Falta de política IRBC
  - Trazabilidad incompleta de los objetivos del BIA con respecto al RTO/RPO de las TIC
  - Ausencia de un comité de resiliencia
  - Falta de KPI para la medición de RTO/RPO
- Creación de una visión general de la madurez (0-5) y obtención de resultados rápidos:
  - Nombramiento de un gestor de IRBC
  - Panel de control de KPI sencillo
  - Primera versión de la matriz de trazabilidad

Recomendaciones de implementación para empresas

Paso 2: cierre de las brechas prioritarias

Gobernanza:

- Publicación de la política del IRBC con la aprobación de la dirección
- Creación del Consejo de Resiliencia (BCM, IRBC, ISMS, gestión de riesgos, operaciones TIC)
- Aprobación del marco presupuestario para las medidas IRBC

Documentación:

- Completar la matriz de trazabilidad: Proceso empresarial → BIA-RTO/RPO → MBCO → RTO/RPO de TIC → MBCO final → verificación de pruebas
- Integración en el control de documentos

Medidas técnicas:

- Control de versiones de todos los planes de continuidad de las TIC
- Suministro fuera de línea (sala de crisis, ordenadores portátiles de emergencia, nube segura)
- Calendario de pruebas (al menos un simulacro de conmutación por error o restauración en vivo al año)
- Estrategias iniciales de copia de seguridad inmutable y aislamiento físico

Paso 3: Optimización y preparación para la auditoría

Optimización:

- Cuadros de mando de KPI en funcionamiento regular
- Proceso sistemático de lecciones aprendidas
- Ejercicios de simulación (por ejemplo, ransomware, fallo de un proveedor, fallo de la región principal de la nube)
- Prueba de la capacidad de transición MBCO → MBCO final

Preparación para la auditoría:

- Cadena de pruebas completa
- Repositorio de auditoría con política IRBC, matriz de trazabilidad, planes, informes de pruebas, protocolos de revisión de la gestión

Recomendaciones de implementación para empresas

Tabla de implementación

Acción	Responsable
Crear y aprobar la política IRBC	Gerente de IRBC, dirección
Crear la Junta de Resiliencia	Dirección
Implementar la matriz de trazabilidad	Gerente de IRBC, BCM
Definir calendario de pruebas	Gerente de IRBC, Operaciones de TIC
Implementar copias de seguridad inmutables	Operaciones TIC
Ejercicio de simulación de ransomware	Gerente de IRBC, ISMS
Documentar y aprobar el MBCO final	Gerente de IRBC, dirección
Realizar la comprobación de preparación para la auditoría	Gerente de IRBC, auditoría interna

Recomendaciones de implementación para empresas

Transición del ITSCM clásico a la norma ISO/IEC 27031:2025

Las empresas que anteriormente han aplicado la gestión clásica de la continuidad de los servicios de TI (ITSCM) según los principios de ITIL deben ampliar estratégicamente su enfoque. Mientras que la ITSCM se centra en la recuperación técnica de los servicios TIC individuales, la norma ISO 27031 integra el IRBC en el BCMS como un componente estratégico de resiliencia.

1. **Gobernanza**
   - Creación de un Consejo de Resiliencia
   - Adaptación de la función de gestor de ITSCM a la de gestor de IRBC
   - Introducción de revisiones trimestrales de la gestión
2. **Documentación**
   - Conversión de los planes de recuperación ante desastres en planes completos de continuidad de las TIC
   - Introducción de una matriz de trazabilidad
   - Control de versiones y almacenamiento a prueba de auditorías
3. **Integración**
   - Integración de ITSCM con BCM, ISMS y respuesta a incidentes
   - Alineación con ISO 27002 A.5.30 y A.8.16
   - Procesos uniformes de escalado y aprobación
4. **Adaptación de la estrategia de pruebas**
   - Mantener las pruebas técnicas de conmutación por error
   - Adición de ejercicios basados en escenarios (ciberataque, fallo de la nube, fallo del proveedor)
   - Integrar las lecciones aprendidas en los planes y los KPI

Perspectivas

La norma ISO/IEC 27031:2025 representa la transición de la planificación técnica de contingencias a la gestión estratégica de la resiliencia en toda la organización. Las empresas deben adaptar sus estructuras, procesos y funciones en consecuencia para cumplir con los requisitos ampliados.

¿Tiene alguna pregunta sobre este tema? ¡No dude en ponerse en contacto con nosotros!

Controllit AG
Kühnehöfe 20
22761 Hamburg
Alemania
www.controll-it.de

A partir de septiembre de 2025

Controllit AG es su socio para la gestión de la continuidad del negocio (BCM). Desde nuestra fundación, hemos desarrollado conceptos y productos integradores para la gestión de la continuidad del negocio, la gestión de la continuidad de los servicios de TI y la gestión de crisis. Le ayudamos con conceptos estratégicos, organizativos y técnicos para proteger sus procesos empresariales contra amenazas y prepararse para emergencias.

Créditos de las fotos/gráficos: Portada: iStock.com/treety ; S. 3: iStock.com/pishit; S. 7: iStock.com/TCmake_photo; S. 10: iStock.com/BRO Vector; S. 12: iStock.com/Imam Fathoni; S. 17: iStock.com/Alexey Yaremenko; S. 20: iStock.com/BRO Vector; S. 25: iStock.com/BRO Vector; S. 28: iStock.com/TCmake_photo; S. 31: iStock.com/TCmake_photo; S. 35: iStock.com/Iryna Spodarenko