Junio 2026

CHIEF RESILIENCE OFFICER

Libro Blanco

Una iniciativa de:

CRC
CYBER RESILIENCE CENTRE

isms forum

AUTORES

COORDINADORES
Cristina Pereira Gestoso
Carlos Fernández de la Reguera

PARTICIPANTES
Álvaro Fuentes
Amelia Torres
Araceli González
Félix Rodríguez
Gema Brihuega
Jesús Valverde
José Márquez
Juan Caubet
Óscar López
Patricia Nieto
Rodrigo Esteban
Tomás Ávila
Trina De Miguel

REVISORES
Angel Pérez
Carlos Fernández de la Reguera
Cristina Pereira
Gema Brihuega
Gonzalo Sánchez
Javier Ordúñez

GESTIÓN DE PROYECTO
Beatriz García

DISEÑO Y MAQUETACIÓN
Susana Marín

ÍNDICE

INTRODUCCIÓN Y CONTEXTO DE ACTUACIÓN

1

1.1. Contexto de evolución contingencia TI (continuidad de negocio, resiliencia digital, resiliencia operativa y organizacional)

En los últimos años hemos vivido una profunda evolución en los conceptos de continuidad de negocio y resiliencia que tuvieron su origen en la gestión de contingencias tecnológicas. Tradicionalmente, las organizaciones se centraban en la preparación de planes de recuperación ante desastres (DRP) con un enfoque reactivo: restaurar sistemas y procesos tras una interrupción (incendios, inundaciones, fallos hardware, etc.). En estos casos, la estrategia de solución consistía en tener unos procedimientos completos, actualizados y entrenados, así como un plan de copias de seguridad y de redundancia entre centros alternativos. No se consideraba (al menos de forma integral) el impacto en el negocio ni en la organización, aunque evidentemente estaba ahí y en muchas ocasiones superando al coste de la recuperación técnica.

A finales de los 90 el enfoque deja de ser puramente técnico y comienzan a utilizarse metodologías estructuradas, basadas en mejora continua y que son la base de la continuidad de negocio. La digitalización, globalización y complejidad de riesgos emergentes hacen necesario empezar a incluir procesos críticos y servicios integrales[1] en estos planes de recuperación. Empiezan a utilizarse en las organizaciones conceptos como el ***RTO (Recovery Time Objective)***, ***RPO (Recovery Point Objective); MTPD (Maximum Tolerable Period of Disruption)*** y muchos otros términos que ayudan en la definición de análisis de impactos y de planes completos para la recuperación de las operaciones después de un incidente grave.

Parte de la evolución histórica se debe a un cambio de contexto relevante, que se inició a partir de 2015 y que se materializó con una sucesión de incidentes relevantes, entre ellos el ataque WannaCry en 2017, así como otros eventos de distinta naturaleza como la borrasca Filomena, la pandemia o incidentes graves que afectaron a proveedores tecnológicos críticos.

Desde la materialización de estos eventos, existe un entendimiento generalizado de que estos planes ya no sólo abarcan los sistemas y/o aplicaciones, sino que deben tener en cuenta todos los departamentos de la organización incluyendo las áreas de negocio y departamentos de soporte como recursos humanos o finanzas. Podemos decir que pasamos a un modelo de continuidad operativa que empieza a considerarse un pilar estratégico en los modelos de negocio.

[1] A efectos del presente documento, los términos procesos críticos y servicios esenciales se emplean de forma equivalente para referirse a aquellos procesos, funciones o servicios cuya interrupción, degradación o indisponibilidad tendría un impacto significativo en la continuidad del negocio, el cumplimiento normativo, la estabilidad operativa o la sostenibilidad de la organización. No obstante, desde un punto de vista técnico y normativo, el concepto de servicios esenciales se encuentra vinculado a la Directiva (UE) 2022/2555 (NIS2), a la Directiva (UE) 2022/2557 (CER) y al Reglamento (UE) 2022/2554 de Resiliencia Digital Operativa (DORA); mientras que procesos críticos responde principalmente al ámbito de la continuidad de negocio y la resiliencia operativa.

Podemos definir esta resiliencia operativa como la capacidad de una organización para mantener la continuidad de sus procesos críticos y servicios esenciales ante eventos disruptivos, adaptándose rápidamente a condiciones cambiantes y minimizando el impacto en clientes, empleados y socios.

El entorno en el que las organizaciones actuales operan es cada vez más complejo y es absolutamente necesario integrar una gestión adecuada de los riesgos incluso en escenarios adversos que no eran tenidos en cuenta por su baja probabilidad de suceder. Hay una serie de aspectos clave, de pilares que sustentan esta continuidad o resiliencia operativa y que podemos resumir en:

- **Flexibilidad:** capacidad para reorganizar recursos, proveedores y flujos operativos ante interrupciones.

- **Integración transversal:** conexión entre áreas de negocio, tecnología, gestión de riesgos y crisis.

- **Cumplimiento normativo:** alineación con marcos regulatorios como DORA, NIS2, CER, ISO 22301, etc. Las organizaciones deben entender el marco normativo como un activo de valor que aporta seguridad de cara a los clientes, evita pago de sanciones y multas y fortalece la confianza y el valor en el mercado.

- **Gestión de la cadena de suministro:** las organizaciones dependen de proveedores que son también, a su vez, vulnerables a crisis geopolíticas, desastres naturales, ciberataques y fallos logísticos, entre otros. Es necesario tener planes de continuidad asociados a estos proveedores e involucrarles en la realización de ejercicios y auditorías para asegurar una correcta continuidad del servicio ante casuísticas de fallo de estos terceros

- **Concienciación y formación** a todos los niveles lo que permite desarrollar una cultura basada en la gestión de riesgos proactiva, antes de que estos se materialicen y reforzando la resiliencia como parte del ADN corporativo.

Pasar de resiliencia operativa a resiliencia organizacional significa ir un paso más allá, integrar a personas, proveedores, departamentos, procesos, clientes, etc., en la cultura de flexibilidad y adaptación al cambio, de supervivencia, de mejora continua, buscando que la empresa no solo sobreviva a las crisis, sino que salga reforzada.

Podemos citar algunos elementos que contribuyen en el camino de la resiliencia organizacional:

- **Liderazgo y compromiso de la alta dirección:** si desde este nivel de gestión se considera la resiliencia como un pilar corporativo y se integra en la estrategia, ésta no queda relegada a un área técnica, y se asegura que los planes de continuidad estén alineados con los objetivos de negocio.

  La dirección debe asegurar que se asignan recursos en formación, ejercicios y personal especializado, fomentando la concienciación, responsabilidad y comunicación entre los distintos equipos de trabajo y áreas corporativas. Asimismo, debe facilitar la gobernanza y toma de decisiones impulsando la creación de comités de seguimiento, políticas y procedimientos, reporte periódico, etc. Por último, pero no menos importante, asegurar que la organización cumpla con sus compromisos regulatorios y normativos reforzando así la confianza del mercado.

- **Formación y concienciación que fomenta los comportamientos proactivos ante riesgos.** Un programa completo de formación asegura que los empleados conozcan protocolos, roles y responsabilidades en situaciones críticas asegurando una respuesta ágil en dichas situaciones y, además, que se puedan identificar e incorporar lecciones aprendidas en los procedimientos.

- **Monitorización** a través de indicadores y/o métricas clave de desempeño (KPIs).

- **Mejora continua.**

- **Integración tecnológica y cultural:** herramientas digitales y evolución organizacional.

1.2. Concepto de resiliencia

El concepto ***resiliencia*** se entiende como la capacidad de un material de recuperar su forma o posición original después de ser sometido a una fuerza de doblado, estiramiento o compresión. Es un término ampliamente estudiado en física e ingeniería y tiene multitud de aplicaciones en el diseño de materiales de alta capacidad para mitigar oscilaciones por viento (rascacielos), absorber energía de impactos en vehículos y proteger así a los ocupantes, diseño de materiales deportivos, suspensiones y amortiguadores y muchísimos ejemplos más que podemos encontrar en entornos industriales y en nuestra vida cotidiana.

Esta capacidad de adaptación es directamente aplicable al entorno empresarial y el concepto ha pasado a ser ampliamente utilizado debido en gran parte al entorno complejo e incierto en el que operan las organizaciones hoy en día. Acontecimientos de impacto inimaginable hace unos años como pandemias, guerras en Europa, tensiones geopolíticas con impacto en la cadena de suministro, etc., han puesto sobre la mesa el término resiliencia para empezar a hablar de resiliencia en el negocio, resiliencia organizativa o resiliencia operacional.

En esta línea podemos definir la resiliencia empresarial y/u organizacional como la capacidad de una organización para anticipar, resistir, adaptarse y recuperarse frente a eventos disruptivos, manteniendo la prestación de sus servicios críticos y/o esenciales protegiendo a sus grupos de interés. No se trata solo de disponer de planes de continuidad; es un modelo de gestión integral que combina cultura, procesos, tecnología y gobernanza para sostener el desempeño en escenarios adversos.

En el contexto normativo europeo, especialmente con la Directiva y Reglamento CER (Resiliencia de Entidades Críticas), la resiliencia se define como la ***capacidad de una entidad para anticipar, resistir, absorber, adaptarse y recuperarse de incidentes, fallos o ataques (naturales, humanos, cibernéticos, híbridos, etc.), asegurando la continuidad de servicios esenciales y transformando la adversidad en aprendizaje para mejorar su funcionamiento futuro.*** No es solo resistir, sino poder volver a la normalidad y mejorar tras la crisis, algo crucial no sólo para infraestructuras críticas sino para cualquier organización que quiera garantizar su supervivencia y continuidad. Se trata de una definición amplia que integra todos los conceptos que debemos tener en cuenta cuando hablamos de resiliencia organizacional desde un punto de vista integral.

La resiliencia entendida de forma integral está basada en unas capacidades o disciplinas entrelazadas que permiten a las organizaciones transformar las vulnerabilidades en ventajas competitivas y garantizar su sostenibilidad a largo plazo. La resiliencia se transforma entonces en un valor estratégico que supone una ventaja competitiva en los mercados y aporta confianza y reputación ante los clientes.

Y, ¿cuáles son estas capacidades? a continuación, citamos algunas de ellas:

- ***Modelo de gestión de riesgos basado en la anticipación.*** Identificar riesgos, dependencias y vulnerabilidades antes de que se materialicen, a todos los niveles, desde los riesgos estratégicos hasta los operativos y en todas las áreas críticas de la organización. Es fundamental disponer de un mapa de riesgos actualizado con frecuencia y que contempla escenarios complejos que ponen a prueba la continuidad en la prestación de los servicios esenciales.
- ***Resistencia:*** diseñar arquitecturas, procesos y servicios con capacidad de recuperación en los tiempos de tolerancia máxima identificados. Revisión especial de los puntos únicos de fallo.
- ***Cultura y liderazgo*** (roles claros, entrenamiento y comunicación eficaz).
- ***Planes enfocados de forma integral.***
- ***Cumplimiento normativo y regulatorio.***
- ***Asignación de recursos.***
- ***Pruebas:*** la planificación es importante, pero lo es más poder poner en práctica y testar lo establecido a nivel documental. Relevancia otorgada a la realización de pruebas y ejecución de Ejercicios de Simulación.

La resiliencia no es un destino, sino ***un proceso continuo que exige coherencia entre estrategia, cultura, operaciones y tecnología.*** Las organizaciones que invierten en resiliencia protegen su misión, aceleran su recuperación y fortalecen su reputación ante clientes y reguladores.

MARCO NORMATIVO NACIONAL Y EUROPEO

2

2.1. DORA / NIS2 / Directiva CER / Otros

Reglamento DORA (UE) 2022/2554

DORA es el Reglamento de Resiliencia Operativa Digital, un marco único y obligatorio para todo el sector financiero, específicamente en relación con los riesgos relacionados con las tecnologías de la información y las comunicaciones (TIC), y está en vigor desde enero de 2025. Nació con el objetivo de asegurar que el sector financiero europeo pueda mantenerse resiliente en caso de perturbaciones operativas graves, y establece unos requisitos y obligaciones específicos para la gestión del riesgo de las TIC, la notificación de incidentes, la realización de pruebas de resiliencia operativa, el establecimiento de acuerdos de intercambio de información sobre ciberamenazas y la monitorización del riesgo de la cadena de suministro en las entidades financieras. A diferencia de otras Directivas, Reglamentos o Estándares, que exigen y/o persiguen una "buena ciberseguridad", DORA obliga a bancos, aseguradoras, fintech, proveedores TIC críticos, etc., a que vayan más allá, que puedan resistir, continuar operando y recuperarse ante cualquier incidente digital grave. Es por ello que hace hincapié en la realización de pruebas de resiliencia operativa digital. Las instituciones financieras deben probar regularmente sus sistemas TIC para evaluar su fortaleza y detectar vulnerabilidades, así como realizar simulacros de crisis en escenarios de alto impacto. Las pruebas incluyen evaluaciones de vulnerabilidades, ejercicios de continuidad, pruebas de recuperación, y pruebas de penetración con amenazas específicas dirigidas a entidades financieras (TLPT).

Directiva NIS2 (UE) 2022/2555

Directiva europea que busca garantizar la resiliencia de las organizaciones, concretamente de las redes y los sistemas de información, y sustituye a la Directiva NIS1 (2016/1148) ampliando sectores, obligaciones y el régimen sancionador. La NIS2 debe ser transpuesta por los diferentes Estados miembros; algunos ya lo han hecho, y otros, como España, se encuentran en proceso de transposición. Aplica a medianas y grandes empresas, ya sean públicas o privadas, y su cobertura abarca a los sectores y servicios de mayor relevancia social y económica, considerando a las entidades esenciales o importantes, en función del grado de criticidad de sus sectores, de su tamaño o del tipo de servicio que prestan. La NIS2 define un nuevo régimen de seguridad poniendo especial atención en la gobernanza del riesgo digital, la seguridad de la cadena de suministro, la gestión de incidentes, la continuidad del negocio y, la cultura y la formación. Para ello recoge un listado mínimo de medidas técnicas, operativas y de organización para gestionar los riesgos de seguridad de los sistemas y redes de información, así como del entorno físico de dichos sistemas.

Directiva CER (UE) 2022/2557

CER es la Directiva de Resiliencia de Entidades Críticas y establece obligaciones para reforzar la resiliencia física y operativa de las entidades críticas que prestan servicios esenciales en la UE. Es la sucesora de la antigua Directiva de Infraestructuras Críticas Europeas (ECI).

Al igual que la NIS2, la Directiva CER debe ser transpuesta por los diferentes Estados miembros; algunos ya lo han hecho, y otros, como España, tienen la transposición en proceso.

Aunque no se trata de una directiva puramente de ciberseguridad, incluye la resiliencia frente a riesgos tanto físicos como organizativos, y se complementa con la Directiva NIS2. En el marco europeo actual, la NIS2 y la CER establecen una separación clara entre ámbitos: todo lo relativo a la ciberseguridad recae en la NIS2, independientemente de si el origen del incidente es físico o digital, mientras que la CER se centra en la resiliencia de las entidades frente a disrupciones de carácter no cibernético.

Este enfoque supone una evolución respecto al concepto tradicional de seguridad integral aplicado en España, y resulta clave para comprender la relación entre ciberseguridad y resiliencia, donde la dimensión digital adquiere un papel predominante.

CER cubre 11 sectores esenciales, como energía, transporte, salud o agua, la mayoría en común con NIS2. Además, obliga a los Estados miembros a identificar a las entidades que consideren críticas, a elaborar estrategias nacionales de resiliencia y a realizar evaluaciones de riesgos a nivel país.

Las principales obligaciones para las entidades que sean identificadas como críticas son: realizar evaluaciones de riesgos (incluyendo amenazas cibernéticas), implementar medidas de resiliencia (físicas, organizativas, tecnológicas, etc.), notificar incidentes significativos, elaborar planes de resiliencia, someterse a supervisión y auditorías por parte de los Estados miembros.

Reglamento CRA (UE) 2024/2847

El CRA es el Reglamento de Ciberresiliencia de los productos con elementos digitales y obliga a los fabricantes a garantizar la seguridad durante todo el ciclo de vida de los productos: seguridad por diseño y por defecto, actualizaciones de seguridad, gestión de vulnerabilidades y reporte de incidentes. Está en vigor desde diciembre de 2024; aplicable plenamente en 2027. El CRA permitirá reforzar la cadena de suministro que NIS2 o DORA exigen controlar, reducirá el riesgo sistémico de la cadena de suministro.

Esquema Nacional de Seguridad (ENS) – RD 311/2022

El ENS es un marco regulatorio nacional para el sector público y los proveedores tecnológicos de éste, que tiene como objetivo garantizar que los sistemas públicos sean seguros, confiables y resilientes, obligando a que las organizaciones puedan resistir, recuperarse y seguir prestando servicios incluso ante incidentes graves. El ENS incluye controles de continuidad, disponibilidad, robustez y resiliencia de los servicios esenciales, establece unos principios básicos de seguridad, los requisitos mínimos y las medidas organizativas, operativas y técnicas que deben cumplir las administraciones públicas y los proveedores que trabajan para ellas. A diferencia de otros estándares de seguridad, como la ISO 27001, complementa las tres dimensiones clásicas de la seguridad (confidencialidad, integridad y disponibilidad) con dos dimensiones adicionales, que son la trazabilidad y la autenticidad.

Solvencia II

Marco normativo de la Unión Europea que regula el sector asegurador con el objetivo de garantizar su estabilidad financiera y proteger a los asegurados.

Aunque no constituye un marco específico de resiliencia operativa u organizacional en el sentido de NIS2, DORA o CER, Solvencia II resulta relevante desde una perspectiva indirecta, en tanto incorpora exigencias de gobierno, gestión de riesgos, solvencia financiera y pruebas de resistencia que condicionan la capacidad de las entidades aseguradoras para absorber impactos severos y mantener la continuidad de su actividad.

2.2. Estándares

Las normas de gestión de riesgos se han consolidado como un pilar estratégico para asegurar la estabilidad, la resiliencia y el crecimiento sostenible de cualquier organización. En un mundo cada vez más globalizado y expuesto a tantas amenazas (económicas, tecnológicas, operativas o reputacionales), disponer de un enfoque estructurado y basado en estándares internacionales se vuelve imprescindible.

Las normas ISO en el ámbito de la Gestión de Riesgos ofrecen un marco sólido y reconocido que permite a los profesionales tomar decisiones informadas, anticiparse a escenarios adversos y fortalecer la capacidad de respuesta empresarial. A continuación, analizamos las normas más relevantes que todo CRO debería dominar para liderar con eficacia en estos entornos tan complejos.

Principales estándares relacionados con Resiliencia

ISO 22301 – Sistema de Gestión de la Continuidad de Negocio (SGCN)

Esta norma establece los requisitos para un Sistema de Gestión de la Continuidad del Negocio (SGCN), enfocándose en garantizar que las organizaciones puedan mantener activas sus operaciones ante eventos disruptivos severos, como desastres naturales, fallos tecnológicos o crisis económicas. Esta norma permite a las empresas identificar y gestionar riesgos que podrían afectar su continuidad, asegurando una recuperación rápida y eficiente.

Si integramos la ISO 22301 con otras normas de gestión de riesgos, fortaleceremos la resiliencia organizacional, optimizaremos la toma de decisiones durante situaciones críticas y aseguraremos el uso eficiente de los recursos en momentos de crisis. Es esencial para organizaciones que dependen de la estabilidad operativa y buscan minimizar el impacto de eventos disruptivos.

ISO 22316 – Resiliencia Organizacional

Proporciona un enfoque estructurado para mejorar la capacidad de recuperación de una organización y lo hace mediante principios que proponen atributos y actividades que contribuyen a las organizaciones a ser más resistentes. Actúa como un paraguas que cubre un rango de disciplinas de gestión, las cuales deben ser lo suficientemente maduras y capaces de interactuar entre sí de una manera sinérgica.

ISO 22317 – Análisis de Impacto en el Negocio (BIA)

Proporciona directrices específicas para la identificación de impactos, dependencias y tiempos de recuperación, siendo un estándar clave para fundamentar decisiones de resiliencia y continuidad.

ISO 27001 – Sistema de Gestión de la Seguridad de la Información (SGSI)

Es una norma que establece los requisitos para implementar un Sistema de Gestión de la Seguridad de la Información (SGSI), que ayuda a las organizaciones a proteger la confidencialidad, integridad y disponibilidad de sus datos mediante la gestión sistemática de riesgos, siendo aplicable a cualquier empresa de cualquier tamaño y sector para mejorar su ciberseguridad y reputación. Se basa en un ciclo de mejora continua (Planificar-Hacer-Verificar-Actuar) y se complementa con controles definidos en la ISO 27002.

ISO 27031 – Continuidad de los servicios TIC

Ofrece directrices para preparar y mantener la continuidad de los servicios tecnológicos que soportan procesos críticos de negocio.

ISO 22398 – Ejercicios y pruebas de continuidad y resiliencia

Define buenas prácticas para el diseño, ejecución y evaluación de ejercicios y simulacros, asegurando la eficacia operativa de los planes definidos.

Otros estándares indirectamente relacionados con resiliencia

ISO 22320 – Gestión de emergencias e incidentes

Es una norma esencial para aquellas organizaciones que operan en zonas propensas a desastres naturales y situaciones de emergencia. Esta norma proporciona directrices sobre cómo organizar una respuesta efectiva a emergencias, como inundaciones, terremotos o incendios. También establece cómo coordinar las actividades de respuesta ante un desastre, cómo evaluar los recursos necesarios y cómo garantizar la comunicación entre todos los involucrados. A través de esta norma, las organizaciones pueden minimizar el impacto de desastres y mejorar sus tiempos de recuperación.

ISO 31000 – Gestión del riesgo

Es una norma internacional de gestión de riesgos que ofrece principios y directrices para ayudar a cualquier organización a identificar, analizar, evaluar, tratar, monitorear y comunicar sus riesgos de forma sistemática, integrando este proceso en sus actividades para mejorar la toma de decisiones, la resiliencia y el cumplimiento de objetivos, sin ser específica de un sector concreto.

ISO 9001– Sistemas de gestión de la calidad

Es una de las normas más conocidas y utilizadas en todo el mundo, ya que establece los requisitos para un Sistema de Gestión de Calidad (SGC). En su versión más reciente, la norma incorpora el concepto de «pensamiento basado en riesgos», lo que significa que la gestión de riesgos se integra dentro del proceso de gestión de calidad. Aunque esta norma no está enfocada exclusivamente en la gestión de riesgos, sí establece directrices clave para la identificación, evaluación y gestión de los riesgos dentro de los sistemas de calidad de las organizaciones.

ISO 21500 – Gestión de proyectos

Es una guía internacional para la gestión de proyectos que incluye la gestión de riesgos como un componente clave, proporcionando directrices para identificar, analizar, tratar y monitorear obstáculos potenciales y oportunidades durante el ciclo de vida del proyecto, buscando mejorar el éxito y la efectividad. Aunque no es una norma certificable y se enfoca en un marco conceptual para estandarizar procesos y mejorar la comunicación global, ve la gestión de riesgos como una práctica esencial para el éxito del proyecto, integrándola en un marco global de dirección y gestión para mejorar el rendimiento y la consistencia.

ISO 55000 – Gestión de activos

Es un conjunto de tres normas de gestión de riesgos que permiten establecer un Sistema de Gestión de Activos en las organizaciones. Esta norma es especialmente útil en sectores como la industria, el transporte y la energía, donde la gestión eficaz de activos es clave para garantizar el rendimiento de la empresa.

Este estándar no solo ayuda a gestionar los activos físicos, sino que también se aplica a activos intangibles, como la información, el conocimiento y la reputación.

ISO 19011 – Auditoría de sistemas de gestión

Esta norma, es fundamental para quienes pretendan ser auditores internos o quieran trabajar para entidades certificadoras. Esta regulación brinda las claves para realizar una auditoría de sistemas de gestión. Es decir, sirve para evaluar si una organización está cumpliendo o no con una determinada norma ISO. Se trata por tanto de una norma clave para la Gestión de Riesgos Empresariales.

ISO 37301 – Sistemas de gestión de compliance

Esta norma establece los requisitos para implementar un Sistema de Gestión de Compliance o Cumplimiento Normativo, enfocado en asegurar que las organizaciones cumplan con las leyes y regulaciones pertinentes, evitando sanciones, daños reputacionales o litigios. Esta norma ayuda a identificar los riesgos legales y regulatorios y a crear mecanismos efectivos para mitigarlos.

ISO 37000 – Gobierno corporativo

Es una norma clave en el ámbito del cumplimiento corporativo que ayuda a las empresas a prevenir sobornos y prácticas corruptas. La corrupción representa un riesgo significativo en muchas organizaciones, especialmente en sectores de alta regulación como el financiero.

La implementación de esta norma ayuda a las empresas a demostrar su compromiso con la ética empresarial y las buenas prácticas, lo que fortalece la confianza de sus clientes y socios.

PCI DSS – Seguridad de datos en entornos de pago

El Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago es un conjunto de normas de seguridad creado por las principales marcas de tarjetas (Visa, MasterCard, etc.) para proteger los datos sensibles de los titulares de tarjetas durante el procesamiento, almacenamiento y transmisión, aplicable a cualquier empresa que acepte pagos con tarjeta. Su objetivo es prevenir el fraude y garantizar transacciones seguras.

LA FUNCIÓN DE LA RESILIENCIA

3

3.1. Objetivos y pilares de la función de resiliencia

La función de resiliencia se configura como un elemento estructural del gobierno corporativo y del sistema de gestión de la organización. Su objetivo es fortalecer la capacidad de anticipar, absorber, responder, recuperarse y adaptarse frente a interrupciones que pueden comprometer la prestación de servicios esenciales. Esta capacidad requiere una visión holística que considere amenazas emergentes, interdependencias críticas, cambios regulatorios, exigencias tecnológicas y escenarios operativos complejos.

La resiliencia no se articula como un sistema de gestión independiente, sino como un componente integrado del sistema global de gestión de la organización. Este enfoque evita la duplicidad de estructuras, favorece la coherencia entre disciplinas y facilita que la resiliencia utilice los mismos mecanismos de gobernanza, supervisión y mejora continua que el resto de los sistemas ya implantados. La estructura de alto nivel de las normas ISO (International Organization for Standardization) permite alinear los principios de resiliencia y sus estándares asociados (como ISO 22316, ISO 22301 o ISO 22398) con sistemas de gestión de calidad, medio ambiente, seguridad de la información o seguridad y salud en el trabajo.

Desde esta perspectiva, la resiliencia adquiere un carácter transversal que conecta funciones, procesos, activos y personas en un marco común. Su propósito no es solo asegurar la recuperación tras un incidente, sino favorecer que la organización opere con estabilidad en entornos adversos y evolucione en función de la experiencia y los cambios del entorno.

Objetivos de la función de resiliencia

1. Alinear la resiliencia con la estrategia corporativa e integrarla en el sistema de gestión

El primer objetivo de la función de resiliencia es asegurar que sus principios se alinean con los objetivos estratégicos y se integran dentro del sistema de gestión de la organización. Esta integración permite que la resiliencia utilice estructuras ya establecidas, comités, roles, indicadores, auditorías internas, procesos de revisión por la dirección, garantizando una visión unificada del desempeño organizativo. Dicha integración con el sistema de gestión permite que la resiliencia no dependa de áreas aisladas ni se convierta en un conjunto de actividades desconectadas. Por el contrario, sus objetivos, roles y procesos se articulan bajo los mismos principios de gestión, liderazgo, evaluación del desempeño y mejora continua que el resto de los sistemas certificados de la organización.

La resiliencia contribuye a la toma de decisiones estratégicas mediante la identificación de riesgos que pueden afectar al modelo de negocio, la valoración de vulnerabilidades que derivan de dependencias internas y externas, y el establecimiento de prioridades que orientan las inversiones necesarias para proteger los servicios esenciales.

2. Proteger y sostener los servicios esenciales mediante un enfoque basado en dependencias

La función de resiliencia debe identificar los servicios críticos y/o esenciales y analizar sus dependencias críticas para comprender su vulnerabilidad ante escenarios disruptivos. Para dichos servicios críticos, este enfoque abarca identificar:

- Procesos de negocio críticos de los que dependen dichos servicios.
- Personas con funciones clave en los procesos críticos.
- Infraestructuras físicas y tecnológicas.
- Sistemas de información (aplicaciones, bases de datos, etc.).
- Proveedores estratégicos y servicios externalizados críticos.
- Relaciones funcionales entre procesos (interdependencias cruzadas).

La protección de los servicios esenciales requiere comprender cómo una interrupción en cualquiera de estos elementos puede desencadenar efectos en cascada en otros, especialmente en organizaciones con elevada interdependencia operativa. Pero no solo hay que tener en cuenta las interdependencias internas, sino también las externas; bien sea a través de la gestión de riesgos de terceros o hacia otras entidades consideradas críticas o esenciales por el Estado o en la prestación de servicios esenciales para la sociedad.

3. Favorecer una respuesta ante incidentes integrada y escalada

La respuesta a un incidente grave que pueda poner en riesgo la continuidad de una organización requiere coordinación entre múltiples áreas: seguridad (física y ciberseguridad), operaciones, recursos humanos, tecnología, comunicación y proveedores. La función de resiliencia proporciona la estructura necesaria para asegurar que esta coordinación se produce de manera ordenada, proporcional a la magnitud del incidente y con roles claramente definidos en los tres niveles de la organización: **Estratégico (Crisis), Táctico (Continuidad de Negocio) y Operativo (gestión de incidentes y emergencias).**

Planes de respuesta de Resiliencia

Gráfica 1. Modelo de Resiliencia: Gestión de Crisis, Continuidad y Respuesta Operativa

Los marcos profesionales consolidados, como los difundidos por el BCI (Business Continuity Institute), destacan la importancia de un modelo de activación escalado, con criterios claros de umbrales, responsabilidades predefinidas y mecanismos para consolidar información en tiempo real. Estos principios se integran en el marco de resiliencia para asegurar una actuación coherente y eficiente.

La respuesta incluye la comunicación interna y externa, la toma de decisiones informada y la coordinación con autoridades o reguladores cuando sea necesario.

4. Impulsar la recuperación y el restablecimiento progresivo

La recuperación tiene como objetivo restablecer la actividad dentro de los niveles aceptables definidos por la organización. Este proceso incluye:

- Validación técnica y de seguridad de los sistemas restaurados.
- Reconstrucción de capacidades afectadas.
- Coordinación con proveedores.
- Monitorización del restablecimiento.
- Comunicación con grupos de interés.
- Documentación de decisiones y acciones.

En sectores regulados o entidades críticas, la recuperación también exige trazabilidad y transparencia para asegurar la confianza de clientes, autoridades y sociedad.

5. Favorecer el aprendizaje organizacional y la adaptación continua

La adaptación es un componente esencial de la resiliencia y actúa como motor de evolución para el sistema de gestión. Tras ejercicios, pruebas o incidentes reales, la función de resiliencia lidera con una visión holística ejercicios de lecciones aprendidas que permiten identificar oportunidades de mejora, actualizar procedimientos, optimizar capacidades y ajustar políticas o roles.

Este proceso de aprendizaje se integra en el sistema de gestión, lo que facilita:

- Su revisión por la dirección.
- Su consideración en auditorías internas y/o externas.
- La actualización coordinada de procesos.
- La alineación con objetivos estratégicos.

Así, la resiliencia se fortalece como un mecanismo vivo, capaz de evolucionar con la organización y con su entorno operativo.

Pilares de la función de resiliencia

1. Anticipación

Permite comprender riesgos, vulnerabilidades e interdependencias con antelación suficiente para orientar la planificación estratégica. Incluye análisis de escenarios de contingencia, vigilancia del entorno y consideración de impactos sistémicos que puedan comprometer servicios esenciales.

2. Preparación

Desarrolla capacidades, roles, procedimientos y recursos para prevenir y actuar de forma eficaz ante incidentes. Incluye la formación, la definición de equipos de respuesta, la planificación de recursos y la realización de pruebas y simulaciones reconocidas por las buenas prácticas, como parte fundamental de la preparación operativa.

3. Respuesta

Activa mecanismos de reacción, coordinación y toma de decisiones durante un incidente. Abarca la actuación técnica y operativa, pero también la gestión estratégica y reputacional del incidente, la comunicación y la coordinación con terceros.

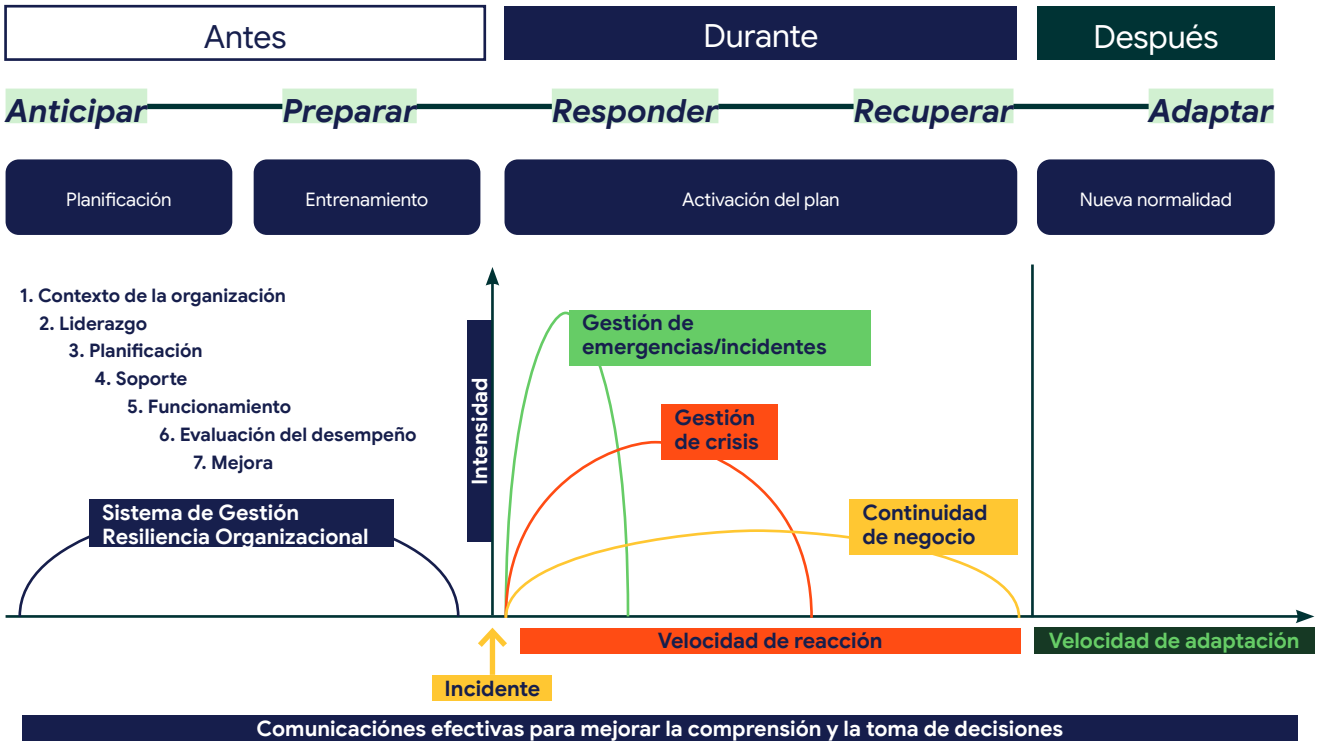
4. Recuperación

Restaura la actividad dentro de los niveles aceptables definidos por la organización, asegurando estabilidad operativa, transparencia y retorno seguro al desempeño habitual.

5. Adaptación

Integra la resiliencia dentro del ciclo de mejora continua del sistema de gestión, promoviendo un aprendizaje constante que ajusta procesos y capacidades a la evolución del entorno.

Pilares de la función de Resiliencia



Gráfica 2. Ciclo de la Resiliencia Organizacional: de la Anticipación a la Adaptación

Definir roles, responsabilidades, autoridad y suplencias, y asegurar su competencia y disponibilidad, convierte la respuesta en algo estructurado y efectivo, capaz de proteger realmente los servicios esenciales y la reputación de la organización, así como la confianza de las partes interesadas.

Las organizaciones de referencia ya no hablan de planes separados, sino de resiliencia operativa integrada, donde las tecnologías de la información (TI) y las tecnologías operacionales propias de los sistemas de control industrial (OT-SCI), negocio y gestión de crisis se diseñan como un único ecosistema, coordinados por la función del CRO.

3.2. Funciones del responsable de resiliencia y gobernanza

El CRO es un perfil que debe unir una visión de seguridad, riesgo, continuidad, cumplimiento y gobernanza, ya que debe hacer de puente entre tecnología, negocio y cumplimiento. Las funciones que tiene se pueden clasificar en siete ámbitos: estrategia, riesgo y cumplimiento, continuidad y recuperación, incidentes y crisis, terceros, cultura y liderazgo, con capacidad de interactuar, a su vez, con las distintas áreas expertas dentro de su organización.

Se listan a continuación las funciones que un CRO debe supervisar. En función del modelo organizativo de cada entidad, el CRO podrá ejecutar en primera instancia todas o parte de ellas, o bien actuar como integrador de estas, interactuando con otras áreas (ver **Sección 5. Modelos Organizativos y Relacionales**).

Funciones estratégicas:

Definir la estrategia de resiliencia corporativa.

Un CRO define la estrategia de resiliencia corporativa, estableciendo un marco global que cubre los ámbitos digital, operativo y organizativo. Conecta esa resiliencia con los objetivos de negocio y el apetito de riesgo, unificando aspectos de continuidad, gestión de terceros, ciberseguridad, gestión de crisis y recuperación para asegurar una respuesta coherente y sólida ante cualquier disrupción.

Asesorar a la alta dirección.

Un CRO asesora al órgano de dirección proporcionando una visión clara y actualizada sobre los riesgos, el contexto interno y externo, los incidentes relevantes y el nivel de madurez de la organización en materia de resiliencia. También vela por que la alta dirección cumpla sus responsabilidades de supervisión, especialmente las exigidas por marcos normativos aplicables a la tipología de la organización, como los identificados en el **apartado 2**. A partir de esta información, impulsa que las decisiones estratégicas se fundamenten en criterios de riesgo y capacidad de recuperación, ayudando a que la compañía actúe con anticipación, coherencia y solidez frente a posibles disrupciones graves.

Funciones de gestión del riesgo y cumplimiento

Supervisar la gestión del riesgo digital y operativo.

El CRO supervisa los riesgos relacionados con la resiliencia operativa y organizacional, entendidos como aquellos que pueden comprometer la continuidad de los servicios críticos o esenciales, la capacidad de recuperación de la organización y su estabilidad ante escenarios disruptivos.

Esta supervisión se centra, de forma específica, en riesgos de continuidad, riesgos operativos, riesgos digitales, riesgos asociados a dependencias críticas y riesgos derivados de terceros, incluyendo la identificación de interdependencias y puntos únicos de fallo que puedan generar impactos en cascada.

La función del CRO en este ámbito no sustituye ni duplica la función corporativa de gestión de riesgos, cuando esta exista, ni las responsabilidades formales atribuidas por la normativa a otras figuras con competencias específicas en materia de resiliencia y seguridad (como el RSI en el marco NIS/NIS2 o el RSR en el ámbito CER). Se ejerce de forma coordinada con la función de Riesgos o de ***Enterprise Risk Management (ERM)***, alineando criterios, metodologías y prioridades, y asegurando que los escenarios de disrupción y continuidad se integran adecuadamente en el marco global de gestión de riesgos de la organización.

Asegurar el cumplimiento normativo en materia de resiliencia.

Asegura el cumplimiento normativo actuando como eje coordinador de marcos como NIS2, ENS, DORA, CER o las normas ISO 27001 y 22301, garantizando una aplicación coherente en toda la organización. Supervisa qué políticas, procedimientos y evidencias de control se mantengan actualizados y alineados con los requisitos regulatorios. Además, prepara a la compañía para auditorías internas y externas, impulsando una cultura de rigor y mejora continua que refuerza la confianza de clientes, reguladores y socios.

Funciones de continuidad y recuperación.

Un CRO asegura la resiliencia operativa garantizando que los servicios esenciales puedan mantenerse o recuperarse con rapidez ante cualquier disrupción. Para ello, impulsa una visión integral que incorpora la resiliencia en los procesos y servicios críticos, en las capacidades tecnológicas y resto de dependencias de activos críticos y en la preparación de las personas. Esta integración permite identificar y corregir vulnerabilidades, reforzar la continuidad y asegurar que la organización opere con solidez incluso en escenarios adversos.

Para ello vela por que exista una adecuada gestión y liderazgo de la continuidad del negocio asegurando así una comprensión precisa de los impactos potenciales mediante la dirección del BIA (Business Impact Analysis). A partir de ese diagnóstico, le corresponde la definición de estrategias de continuidad y recuperación que permitan mantener las funciones críticas ante cualquier disrupción. Además, debe promover la realización de pruebas periódicas y simulacros para validar la eficacia de los planes, identificar posibles mejoras y fortalecer la preparación organizativa. Con ello, se garantiza que la organización pueda responder y recuperarse con rapidez y coherencia.

Funciones de gestión de incidentes y crisis

Supervisar la gestión de incidentes.

Un CRO supervisa la gestión de incidentes asegurando una coordinación eficaz de la detección, la respuesta, el escalado y la notificación para minimizar el impacto operativo. También vela por que la organización cumpla los plazos regulatorios establecidos por los marcos normativos aplicables (NIS2, DORA o ENS), evitando sanciones y reforzando la confianza institucional. Además, garantiza la realización de un análisis post-incidente y la implantación de acciones correctoras, impulsando un aprendizaje continuo que fortalece la resiliencia global de la compañía.

Dirigir la gestión de crisis.

Un CRO vela por la existencia de una adecuada gestión de crisis asegurando una activación oportuna y eficaz del comité de crisis cuando la situación lo requiere. Con este liderazgo, la organización puede responder con control, minimizar impactos y recuperar la normalidad con mayor rapidez.

Funciones relacionadas con terceros y la cadena de suministro

Supervisa la gobernanza de proveedores y la resiliencia de la cadena de suministro.

El CRO impulsa que los respectivos responsables gestionen adecuadamente los riesgos asociados a proveedores críticos y a la cadena de suministro, evitando que se conviertan en un punto débil para la organización. Promueve que los contratos y los procesos de compra incorporen requisitos claros de cumplimiento, y que los proveedores dispongan de planes de continuidad adecuados y probados. De este modo, se anticipan riesgos, se reducen dependencias críticas y se refuerza la capacidad de respuesta ante posibles disrupciones externas.

Funciones de cultura, formación y concienciación

Impulsar una cultura de resiliencia.

Dentro de sus funciones, está la de impulsar una cultura de resiliencia diseñando programas de formación y concienciación que fortalezcan las capacidades de toda la organización. Además, prepara a la dirección y a los equipos clave para que comprendan su papel en la prevención, respuesta y recuperación ante disrupciones. También promueve una responsabilidad compartida, asegurando que cada área asuma su parte en la protección y continuidad del negocio. Con este enfoque, la resiliencia deja de ser un esfuerzo aislado y se convierte en un valor integrado en el día a día corporativo.

Funciones de coordinación y liderazgo

Conectar negocio y tecnología.

Un CRO conecta negocio y tecnología traduciendo los riesgos técnicos en impactos claros y comprensibles para toda la organización, facilitando decisiones informadas. Actúa como puente entre áreas clave (Seguridad, Tecnología, Operaciones, Riesgos y Cumplimiento) para alinear prioridades y evitar visiones aisladas. Gracias a esta coordinación, la organización puede equilibrar innovación, seguridad y continuidad, asegurando que la tecnología apoye de forma coherente los objetivos estratégicos.

Liderar la mejora continua.

Lidera la mejora continua, impulsando proyectos que eleven la madurez de la organización en materia de resiliencia, asegurando avances sostenidos y medibles. Supervisa indicadores de desempeño y/o riesgo clave (KRIs/KPIs de resiliencia) para evaluar el desempeño y detectar áreas de preocupación o mejora. Además, mantiene un ciclo constante de revisión, aprendizaje y ajuste que permite adaptar procesos, capacidades y controles a un entorno cambiante. Con este enfoque, la resiliencia se convierte en un proceso vivo que evoluciona junto al negocio.

3.3. Principales Stakeholders

Tal y como venimos hablando en el presente documento el contexto en el que operan las organizaciones, marcado por la volatilidad, la incertidumbre, la interdependencia operativa, las amenazas tecnológicas, la presión regulatoria y la complejidad de las cadenas de suministro globales, hace que el rol del CRO haya evolucionado significativamente en los últimos años.

La alta exposición a riesgos regulatorios, operativos, reputacionales y tecnológicos, convierten a la función del CRO en estratégica para asegurar la continuidad de negocio, la resiliencia organizativa y la robustez frente a escenarios disruptivos.

En la preparación de estas capacidades de respuesta integrada y la activación de las mismas es un factor decisivo la identificación de las partes interesadas clave (o stakeholders) para la organización que pueden ser internas o externas.

El CRO debe orquestar a estas figuras o partes interesadas para que la resiliencia deje de ser un concepto aspiracional y se convierta en un mecanismo operativo integrado en toda la organización y en el entorno en el que la organización opera.

Los stakeholders del CRO se pueden clasificar en dos grandes categorías:

Stakeholders internos, que participan directamente en la operativa corporativa, la toma de decisiones o el soporte funcional.

Stakeholders externos, que tienen intereses compartidos con la organización y por tanto forman parte del sistema, pudiendo afectar al comportamiento, estabilidad o cumplimiento de la organización.

Los stakeholders cumplen diferentes roles o funciones: expertos técnicos, responsables de activos críticos, agentes de regulación, clientes, proveedores críticos o esenciales, socios estratégicos y, en última instancia, las personas que definen la “cultura” organizativa.

Las funciones de los stakeholders quedan claramente diferenciadas según el momento temporal en que se produzcan, y desde este punto de vista, su involucración y coordinación por parte del CRO, tiene en cuenta si la organización se encuentra:

En momentos de paz o business as usual (BAU): para integrarlos en las tareas de identificación, análisis, gestión del riesgo, elaboración de planes y estrategias, entrenamiento y formación, entre otras, como tareas dirigidas a la mejora continua y a la adquisición de un grado cada vez mayor de madurez en la resiliencia dentro de las organizaciones.

En momentos de contingencia o crisis: para involucrarles en la gestión de la respuesta, coordinar su participación, facilitar que la información fluya de manera segura y oportuna a aquellas áreas donde es necesaria para la toma de decisiones y se consiga generar una respuesta integrada y eficaz a la crisis.

En esta función de coordinación, el CRO necesita mantener una visión sistémica, acorde a las dependencias críticas identificadas de antemano y garantizando que se establecen los canales de comunicación eficaces con todos los stakeholders. Esto implica coordinar múltiples equipos, entender sus motivaciones, gestionar expectativas y asegurar que las responsabilidades se alinean con el marco de resiliencia corporativa.

Para ello debe asegurar que exista un inventariado claro de todos los stakeholders a considerar y los responsables de interlocución con los mismos, conforme a los distintos criterios aplicables y las instrucciones que correspondan tanto en momentos de paz como en momentos de contingencia.

La correcta gestión de estos actores determina la madurez del programa de resiliencia y el grado de preparación de la organización ante eventos disruptivos.

Stakeholders internos

Los stakeholders internos representan el punto más relevante de interlocución para el CRO, ya que gran parte de los procesos críticos, controles, capacidades y decisiones de riesgo se alojan dentro de la estructura organizativa.

Entre los principales destacan:

Alta Dirección y Comité Ejecutivo

Los ejecutivos son los principales sponsors de la estrategia de resiliencia en las organizaciones. Sus funciones principales:

Asignación de recursos suficientes.

Integración de criterios de resiliencia en la estrategia.

Toma de decisiones informada sobre los principales riesgos, tanto en momentos de paz para el tratamiento y gestión de estos, como en momentos de contingencia o crisis, para tomar decisiones en la gestión de las mismas.

El CRO debe mantener un canal fluido con el grupo de stakeholders para presentar análisis, métricas clave, propuesta y resultados de simulaciones, escenarios de estrés y recomendaciones.

Consejo de Administración y Comisiones Delegadas

En sectores regulados, el Consejo demanda garantías sobre:

Solidez de la continuidad de negocio y resiliencia.

Adecuación a las normativas a las que está sujeta la organización (por ejemplo, DORA, EIOPA, NIS2, Solvencia II).

Evaluación integral de riesgos estratégicos.

El CRO actúa como enlace técnico, introduciendo una visión integrada del riesgo operacional y de resiliencia.

Tecnología en su sentido amplio (CIO, CISO, áreas de TI)

Este es uno de los grupos más críticos, derivado de la dependencia tecnológica que hoy en día tienen todas las organizaciones, ya que concentra:

- Ciberseguridad.
- Infraestructura tecnológica.
- Sistemas de información.
- Continuidad tecnológica.
- Gestión de incidentes tecnológicos.
- Arquitecturas de recuperación.

La capacidad de la organización para responder y continuar con su operativa depende, en gran medida, de la disponibilidad de sistemas y la protección frente a amenazas digitales.

Operaciones y unidades de negocio

Son quienes conocen en profundidad los procesos críticos y las dependencias funcionales.

Funciones de aportación al rol de CRO:

- Representan la fuente primaria de información sobre riesgos reales.
- Disponen de la visión potencial de impacto en clientes.
- Son responsables de activar parte de los protocolos en crisis.
- Necesitan formación y acompañamiento para integrar la resiliencia en su actividad diaria.

Riesgos, cumplimiento y auditoría interna

Este triángulo marca el marco normativo y de control:

- Riesgos: propone los escenarios y el apetito de riesgo.
- Cumplimiento: verifica alineación con normativa y requisitos de supervisión.
- Auditoría interna: evalúa la eficacia del sistema de resiliencia.

La coordinación entre estas áreas evita silos y crea una visión uniforme del riesgo.

Dirección de Personas, Talento y cultura (o Recursos Humanos)

El factor humano es esencial en la operativa pero también el principal agente a proteger en situaciones de crisis cuando su integridad pueda verse afectada, por ello las acciones en relación con ellos son principalmente:

- Planes de protección y gestión de emergencias.
- Planes de sustitución y/o sucesión.
- Programas de comunicación interna.
- Cultura de resiliencia y capacitación.

Este grupo constituye una palanca fundamental para impulsar una cultura organizacional resiliente.

Comunicación corporativa.

La narrativa durante una crisis determina el impacto reputacional:

Prepara mensajes clave.

- Gestiona medios.
- Coordina la comunicación interna y externa durante incidentes.

El CRO debe trabajar estrechamente para asegurar mensajes consistentes y alineados con la realidad operativa, mediante la involucración y coordinación entre todos los equipos y grupos donde la información se genera y la dirección responsable de la generación y transmisión de dichos mensajes, como se refleja en el apartado relativo a Comunicación interna y externa.

No solo en momentos de crisis esta función de la comunicación es clave, sino que también lo es en momentos de paz fomentando una cultura de resiliencia basada en la colaboración, transparencia y alineación estratégica. Todo ello clave tanto en la comunicación interna como en la comunicación externa, ofreciendo al ecosistema exterior aquella información que robustezca la imagen de resiliencia sobre la organización.

Stakeholders externos

Los stakeholders externos representan el ecosistema que rodea a la organización y que influye directamente en su estabilidad. En resiliencia, comprender estas dependencias es fundamental para identificar riesgos emergentes y puntos de bloqueo.

- Reguladores y supervisores.
- Reguladores sectoriales.
- Reguladores horizontales.
- Reguladores especializados según actividad.

Su papel es definir obligaciones, supervisar cumplimiento y evaluar la robustez del modelo operativo.

Clientes

Son la razón de ser de la compañía, los destinatarios de su objeto social.

Aspectos a considerar por parte del CRO:

- El impacto en los mismos en una contingencia debe ser mitigado conforme a los criterios de tolerancia preestablecidos de antemano (tipo de cliente, volumen, servicios esenciales, etc.) deben ser protegidos frente a disrupciones que afecten a servicios esenciales.
- Su percepción de la gestión realizada por parte de la organización en escenarios críticos influye en la reputación corporativa y puede marcar la relación futura entre ambos.
- Reclaman transparencia, y por tanto información, sobre disponibilidad y tiempos de recuperación.

Por todo lo anterior, son el stakeholder clave para cualquier organización y es de máxima relevancia tener bien predefinidos y probados los canales y contenidos de comunicación con los mismos, para distintos escenarios de contingencia.

Proveedores y terceros críticos

La gestión del riesgo de terceros es un aspecto fundamental en la estrategia de resiliencia de las organizaciones y el CRO es responsable de asegurar que proveedores críticos y/o esenciales (por ejemplo, de infraestructuras clave TI, centros de atención de llamadas, plataformas externalizadas de gestión de clientes, proveedores cloud, etc.).

Operan alineados con los requisitos de resiliencia definidos por la organización y que, en caso de incidente, sus actuaciones se integran correctamente dentro de los mecanismos de gestión de crisis de la entidad, en coordinación con los organismos competentes cuando resulte de aplicación.

- Cumplen con los niveles de resiliencia requeridos.
- Cuentan con plan de continuidad respecto a los servicios críticos externalizados por la organización y los prueban con regularidad.
- Mantienen capacidades de recuperación alineadas con los RTO/RPO internos.
- Se definen estrategias de salida siempre que sea necesario.

Fuerzas y cuerpos de seguridad, servicios de emergencia y protección civil

En situaciones de crisis:

- Facilitan información crítica.
- Colaboran en la respuesta.
- Actúan como soporte operativo en incidentes de seguridad física, ciberataques, desastres u otras emergencias nacionales.
- Toman el mando de la gestión de la crisis en determinadas situaciones, y en este caso el rol del CRO es fundamental en la coordinación.

En situación de normalidad, su involucración y participación en la elaboración de planes y estrategias de respuesta y en la ejecución de simulaciones, se convierte en factor de éxito en los supuestos de respuesta real.

Medios de comunicación

El CRO deberá asegurar que existe una coordinación con los medios, ya que su papel es clave porque:

- Influyen en la percepción pública.
- Ayudan a comunicar información clave en crisis.
- Los mensajes que transmiten llegan a un gran colectivo en muy poco tiempo, por lo que pueden ser claves para agravar o minimizar el impacto mediático del incidente.

Buenas prácticas en la gestión de stakeholders del CRO

Ejemplo de caso de uso

A continuación, ofrecemos un escenario como ejemplo de buenas prácticas en la actuación de un CRO que asume el rol de coordinador de crisis. Escenario: Una caída inesperada de los sistemas de atención al cliente afecta la operativa de la compañía.

Escenario: El CRO es informado de una caída de los sistemas de comunicación de call center, lo que está suponiendo una ralentización de la operativa.

1. Identificación de aquellas áreas en la organización afectadas para recabar toda la información necesaria para llevar a cabo una evaluación del impacto actual y anticipando los posibles escenarios adversos futuros.

2. Identificación y priorización de stakeholders.

El CRO identifica en paralelo, y tras una primera evaluación del incidente y valorando los posibles impactos, a los grupos clave implicados: TI, Operaciones, Atención al Cliente, Comunicación (Interna y Externa) y Alta Dirección.

Identifica los diferentes planes de acción de cada uno de estos grupos y hace seguimiento de los resultados que se van consiguiendo con los diferentes planes de respuesta, asegurando que están cubiertos todos los roles necesarios para hacer frente al incidente y, en caso contrario, identificando las personas suplentes correspondientes.

Adicionalmente, verifica que todos los involucrados conocen claramente qué se espera de ellos en este escenario.

Todo ello considerando el nivel de influencia, dependencia del servicio afectado, necesidades de información y sinergias en la actuación entre todos ellos.

3.Activación de canales de comunicación.

El CRO convoca un comité de crisis extraordinario e instaura un canal de comunicación directo con TI para recibir actualizaciones cada 15 minutos, mientras Comunicación Corporativa prepara mensajes para los empleados y, si fuera necesario, para clientes, accionistas y terceros interesados.

Como aspecto clave que debe tener en cuenta el CRO es atender a las necesidades de comunicación e información a las autoridades u órganos de supervisión, reguladores y socios clave en aquellas compañías que formen parte de un Grupo y en sectores regulados que imponen unos tiempos de comunicación pautados y definidos.

4. Toma de decisiones y coordinación.

A partir de la información recopilada, el CRO coordina la priorización de acciones: seguimiento de las labores de restauración progresiva del sistema, identificación de alternativas manuales y activación de medidas de continuidad previamente definidas.

Entre las funciones de coordinación es fundamental llevar a cabo puntos de situación específicos con las áreas que están participando en la respuesta, así como puntos de situación en el Comité de crisis, para conocer el estado en que se encuentra la gestión del incidente, pero también para el análisis y la toma de decisiones teniendo en cuenta los impactos colaterales de dichas decisiones.

La coordinación implica la elaboración de actas, bitácora y documentación de análisis que serán de utilidad no solo para el seguimiento y actuación en la respuesta sino también en las fases post-crisis para analizar la gestión y sacar lecciones aprendidas.

5. Seguimiento y cierre.

Una vez restablecido el servicio, el CRO documenta las lecciones aprendidas junto con cada stakeholder, actualiza los planes de resiliencia y revisa los umbrales de notificación y los protocolos utilizados. Convoca al comité de crisis para realizar un ejercicio conjunto de análisis de situación tras el incidente, identificar acciones de recuperación que llevarán un periodo de tiempo más largo. Esta fase es fundamental si se persigue una mejora continua y un aumento de la madurez en resiliencia dentro de la compañía.

3.4. Cómo establecer la función de resiliencia desde cero

La función de resiliencia y la continuidad de negocio no son lo mismo. Si bien la continuidad de negocio se puede considerar como la semilla de la función de resiliencia, esta va más allá interconectándose con los procesos de gobernanza y sistemas de gestión existentes en la organización.

Teniendo en cuenta lo anterior, en este apartado se tratará de ofrecer una guía de implantación de la función de resiliencia a todos los niveles y suficientemente amplia para que sea aplicable a distintos tipos de organizaciones, partiendo desde la tarea básica de establecer la continuidad de negocio y evolucionándola hacia una función de resiliencia integrada de forma sistemática con los procesos de gestión y gobierno de la organización.

Aspectos clave para establecer la función de resiliencia

1. Alineación estratégica

La decisión de establecer la función de resiliencia en una organización tiene que ser el resultado de alinear las necesidades de continuidad con la misión de la organización en términos de crecimiento, cumplimiento normativo y confianza de los clientes y los organismos reguladores. En los casos donde estos aspectos no formen parte de la misión de la organización los esfuerzos por implantar la función de resiliencia pueden ser en vano.

2. Delimitar la función

Es necesario acotar/definir la función antes de abordar el proyecto de implantación: misión, alcance, responsabilidades, indicadores y autoridad que va a ostentar sobre los distintos interlocutores (órganos de gobierno, unidades de negocio, TI, gestión de terceros y ciberseguridad, entre otros). Si bien la función de resiliencia no sustituye a ninguna de estas funciones, debe estar perfectamente coordinada con todas ellas.

3. Patrocinio del Comité de Dirección

Más allá de la alineación estratégica, antes de iniciar el proyecto de implantación es esencial disponer del respaldo del Comité de Dirección. Este Comité será el responsable de la fijación del apetito de riesgo, la fuente de empoderamiento para la función y quien debe aprobar las delimitaciones de la función.

4. Definición del modelo de gobierno

En la fase inicial del proyecto de implantación de la función se debe definir los distintos comités que constituyen la función, así como una matriz de responsabilidades RACI (Responsable, Aprobador, Consultado, Informado) sobre las funciones y procesos que soportan la resiliencia operativa, y el modelo de relación con los interlocutores.

Un aspecto clave para establecer una función de resiliencia que vaya más allá de la continuidad de negocio habitual es la integración sistemática con procesos y estructuras existentes en la organización, es decir, tratar de reaprovechar los procesos y foros ya establecidos. Algunos ejemplos:

- Cuando se definen procesos de resiliencia, los procesos de gestión de incidentes o emergencias se deben modificar para incluir la evaluación del impacto en la organización de forma natural, para que estos puedan desencadenar la respuesta apropiada para garantizar la resiliencia sin que esto se haga en procesos separados.
- Los comités de continuidad y de crisis no tienen que estar circunscritos a la función de resiliencia o bajo el CRO, sino que se pueden integrar en los comités de gobierno y cumplimiento ya existentes en la organización.
- La identificación de riesgos de continuidad y escenarios de desastre no debe ser un proceso aislado que se lleve a cabo por la función de resiliencia, sino que debe estar integrado con otras funciones (por ejemplo, la función de gestión de riesgos corporativos o control interno).

5. Identificación de procesos críticos y requerimientos de continuidad

Como ya se ha comentado, una parte esencial de la implantación de la función de resiliencia es una implantación previa de la continuidad de negocio más tradicional. En este sentido, será necesario llevar a cabo un análisis de impacto en negocio BIA que permita identificar los activos críticos de la compañía (servicios, sistemas, proveedores, personas, instalaciones, información, etc.).

Típicamente esto se lleva a cabo identificando y analizando los procesos de negocio más críticos, determinando el tiempo de disrupción aceptable en cada uno en base a su impacto (económico, reputacional, legal o de otra índole) e identificando los activos críticos que se requieren para recuperarlos en caso de disrupción. Para ello se puede seguir alguna de las múltiples metodologías o estándares citados a lo largo de la guía.

El resultado de este ejercicio es la identificación de las necesidades de recuperación en tiempo (RTO) y forma (RPO) de los procesos y activos críticos para garantizar la resiliencia operativa. Estos requerimientos deben completarse con los requerimientos regulatorios y contractuales a los que este sometida la organización.

Esta información será clave para construir el plan de mejora continua de las capacidades de resiliencia de la organización.

6. Integración de la cadena de suministro

Como parte de la identificación de activos y servicios críticos se obtiene, entre otros, el inventario de servicios y proveedores críticos y/o de alto riesgo.

Se entiende por proveedores críticos aquellos que resultan imprescindibles para mantener activo un servicio y/o proceso crítico de negocio y por proveedores de alto riesgo aquellos que, en caso de sufrir un incidente, pueden causar la disrupción de un servicio crítico de negocio, pudiendo cada proveedor estar en una o ambas categorías a la vez. Un ejemplo práctico: en un proceso de expediciones de mercancías donde el operador logístico está externalizado, dicho proveedor sería crítico puesto que sin él no se puede mantener operativo el proceso de distribución de mercancías a los clientes. Si además, para una ubicación concreta, dicho proveedor logístico es el único que opera y además es pequeño y no puede garantizar la continuidad de su servicio, entonces es también un proveedor de alto riesgo por ser de difícil o imposible sustitución.

En la gestión de la continuidad de negocio se deben gestionar los riesgos asociados a proveedores críticos y proveedores de alto riesgo, por ejemplo, mediante transferencia de riesgo a nivel contractual o mitigando mediante diversificación de proveedores. Para ir más allá e implantar la función de resiliencia se deben integrar en los procesos de la organización, y como mínimo:

- Evaluar el riesgo de los proveedores críticos en el alta del servicio y de forma recurrente.
- Incorporarlos en los planes de comunicación y gestión de crisis, donde formarán parte de la matriz de contactos.
- Establecer canales de cooperación para la detección y notificación de incidentes.
- Hacerles partícipes de los planes de prueba y recuperación.
- Invitarles a formar parte de los procesos de mejora continua.

7. Situación actual y hoja de ruta

Uno de los objetivos básicos de la implantación de la función de resiliencia es conocer las capacidades de resiliencia de la organización, identificar los requerimientos de continuidad de los servicios de negocio y en base a ello generar un plan de mejora continua que permita alcanzar capacidades de resiliencia alineadas con el apetito de riesgo de la organización.

Para lograr este objetivo la forma ideal sería identificar los requerimientos de continuidad de todos los activos que soportan los servicios de negocio y establecer medidas de control y redundancia que garanticen su continuidad ante cualquier incidente, pero ello requeriría un presupuesto ilimitado.

Por ello lo más práctico es definir una serie de escenarios de riesgo. Se parte de un catálogo de amenazas estándar sobre los activos críticos para identificar supuestos de contingencia factibles que puedan causar interrupciones en los servicios críticos de la organización. Después se evalúan los controles existentes para mitigar estos riesgos y como resultado se obtienen las principales carencias priorizadas que deben remediarse para alcanzar los objetivos de resiliencia de la organización.

El seguimiento y la actualización regular de este plan de mejora continua constituirá la mayor parte del trabajo diario de la función de resiliencia.

8. Definición de capacidades necesarias

Tras disponer de funciones claramente definidas, un modelo de gobierno sobre el que trabajar, un alcance de activos que proteger y conjunto de requerimientos y capacidades que satisfacer, será necesario dotar a la función de resiliencia de las capacidades necesarias para ejecutar todas sus funciones. A lo largo de la guía se citan numerosas funciones y capacidades, destacando las siguientes como las más básicas en el momento de constituir la función:

- Reporte regular a dirección para el alineamiento estratégico.
- Garante de ejecución de procesos de análisis de riesgos y controles periódicos.

- Supervisor de los planes de recuperación, gestión de incidentes y crisis.
- Asegurador de servicios de evaluación de riesgos de terceras partes y cadena de suministros.
- Garante de la existencia y prueba de planes de gestión de comunicación.
- Garante de la definición y ejecución de planes de capacitación y concienciación.

9. Definición de indicadores

Finalmente, se puede considerar que la función de resiliencia está establecida cuando puede generar indicadores que permitan medir las capacidades de la organización y la propia evolución de la función.

Teniendo en cuenta todos los aspectos clave citados hasta el momento se puede definir un proyecto u hoja de ruta de implantación que permita acometer todos ellos. Más adelante se discute sobre recomendaciones para la implantación en función del tamaño de la organización y el grado de centralización entre otros factores, las cuales se centran en el faseado y la necesidad de realizar una implantación iterativa, pero de forma general se puede hablar ahora de las siguientes fases:

Fases de la implantación

i. Constitución

Esta fase es la más crítica, se centra en definir el ámbito de actuación de la función y entender cómo se integra con la organización. Las principales actividades que acometer son:

- **Fundación y gobierno básico:** definición y formalización del apetito de riesgo con el comité de dirección y del modelo de relación con los órganos de gobierno de la organización.
- **Ejecución del BIA:** como se indica más adelante, se puede acometer una ejecución total o parcial centrada en las áreas más críticas de la organización, pero resulta esencial obtener un primer inventario de activos y servicios críticos sobre el que empezar a desplegar las capacidades de la función.
- **Definición de políticas:** la función de resiliencia debe formar parte de las funciones de gobierno de la organización, para ello es necesario formalizar su ámbito de actuación y sus atribuciones en las políticas de la organización.
- **Creación de primeros indicadores:** deben definirse los indicadores objetivos que permitirán medir las capacidades de la organización. Cuando la organización sea capaz de generar sistemáticamente estos indicadores se habrá logrado el hito de establecer formalmente la función en la organización.

ii. Despliegue

Esta fase se focaliza en la construcción de las capacidades básicas que dan respuesta a la atribución de responsabilidades de la función. Para ello debe llevarse a cabo la implantación de procesos, la integración con terceros y las primeras pruebas. Las principales actividades que acometer son:

- **Implantación del plan de continuidad de negocio:** definición y formalización del plan de planes que gobernará la continuidad de los servicios de negocio críticos de la organización, incluyendo el plan de gestión de crisis, los planes de recuperación ante desastres, el plan de comunicación y el plan de formación, entre otros.

- **Implantación del proceso de gestión de riesgos de terceros:** bien sea directamente dentro de la función o a través de la supervisión de procesos en otros departamentos, será necesario definir e implantar un plan de gestión de riesgos de continuidad de servicios prestados por terceras partes que abarque el proceso de gestión de alta e incorporación en la organización (onboarding) y la revisión paulatina de los terceros ya existentes en función de su nivel de riesgo.

- **Ejecución de un plan de formación y concienciación:** si bien el plan de capacitación regular forma parte de los procesos regulares de la función, en esta fase es necesario llevar a cabo una campaña exhaustiva de concienciación y formación a toda la organización que permita dar a conocer la función, sus objetivos y el valor que aporta.

- **Ejecución de los primeros planes de pruebas:** como colofón a la fase de despliegue es muy recomendable llevar a cabo un plan de pruebas que involucre al mayor número de empleados posible (simulaciones de emergencia, pruebas del plan de recuperación de desastres, simulaciones con terceros, etc.). Esto permitirá, por un lado, validar los resultados teóricos obtenidos hasta el momento, y por otro, reforzará notablemente el impacto en la organización del plan de formación y concienciación.

iii. Maduración

El objetivo de esta última etapa de la implantación es la mejora de la propia función de resiliencia. Se pretende implantar capacidades de resiliencia predictiva, automatización de procesos establecidos, ejecución de simulaciones específicas para validar la efectividad de los controles implantados y generar un reporte sistemático a dirección que permita garantizar la madurez y consistencia de la función de resiliencia dentro de la organización.

Para esta última etapa se pueden encontrar multitud de herramientas de mercado, proveedores especializados y servicios gestionados. Su idoneidad variará significativamente en función del tamaño de la organización, su complejidad y el presupuesto disponible, con lo que no se entrará a mayor detalle en el contexto de esta guía.

3.5. Beneficios de una organización resiliente

Podemos entender como una organización resiliente aquella que tiene la capacidad de anticipar, resistir, adaptarse y recuperarse ante situaciones adversas, producidas por factores externos y/o internos a la propia organización.

Es una organización capaz de establecer mecanismos que le permiten mantener la continuidad de sus operaciones esenciales, reducir el impacto económico y reputacional, y garantizar la confianza de todas las partes interesadas.

En el contexto actual en el que nos movemos, marcado por factores como las ciber amenazas, interrupciones de servicio en las cadenas de suministro, y los cambios regulatorios, la resiliencia debe considerarse como una inversión estratégica.

Las organizaciones que adoptan este enfoque son las que logran adaptarse con mayor rapidez, optimizar sus recursos y fortalecer su posición competitiva, indistintamente del presupuesto disponible.

Se puede asegurar que una organización ha alcanzado el grado óptimo de resiliencia cuando no solo sobrevive a la crisis sobrevenida en una situación gravemente adversa, sino que aprende, se adapta y sale fortalecida, de modo que convierte su resiliencia en un activo estratégico que impacta en todas las dimensiones del negocio, permite obtener una serie de beneficios y genera confianza en sus stakeholders externos:

- Garantiza que los servicios críticos se mantengan operativos ante interrupciones, minimizando pérdidas económicas y reputacionales (continuidad de negocio).
- Identifica vulnerabilidades antes de que se conviertan en incidentes, pudiendo prevenir impactos financieros, legales y/o reputacionales (reducción del riesgo).
- Facilita la alineación con normativas y estándares internacionales, evitando sanciones y fortaleciendo la gobernanza (cumplimiento normativo).
- Ofrece una respuesta eficaz ante situaciones de crisis, lo que genera credibilidad frente a sus clientes, socios y reguladores (reputación y confianza).
- Permite responder con rapidez a cambios regulatorios, tecnológicos o del mercado, sin comprometer la estabilidad (adaptación ágil).
- Fomenta la colaboración, responsabilidad compartida y la conciencia de riesgo en todos los niveles (genera cultura de resiliencia).
- Recupera su operativa rápidamente, en comparación con sus competidores, tiene mejor preparación para innovar (ventaja competitiva).

La resiliencia es claridad en lo crítico, hábitos repetibles y controles básicos bien ejecutados. Empezar por lo que “más duele si falla” (continuidad), reducir las causas más comunes (riesgos), asegurar el “mínimo legal” (cumplimiento) y convertir todo en práctica sostenida (cultura). La ventaja competitiva llegará como consecuencia de todo lo anterior.

1. Continuidad de negocio.

Utilizando un símil, fácil de entender, si se imagina la resiliencia como una casa, la continuidad serían sus cimientos. No se habla de manuales complejos, técnicos, sino de claridad operativa:

- Qué es crítico.
- Cuanto tiempo puede estar inoperativo.
- Y cómo volver a estar operativos lo más pronto posible, sin improvisar.

Cuando se definen RTO y RPO realistas, se realizan pruebas de continuidad y se alinean los requerimientos de servicio de los proveedores con los objetivos de negocio, se convierte un posible caos en una interrupción controlada.

La fortaleza reside en lo simple: roles y responsabilidades definidas, planes de continuidad, realización de pruebas, evaluación de sus resultados, mejora continua, y un "plan B" conocido por quien debe y tiene que conocerlo, de esta forma un incidente deja de ser un caos, paralizando la organización y se convierte en una situación que se puede manejar y controlar.

El ejercicio de la continuidad de negocio obliga a ordenar todos los procesos y servicios, especialmente los críticos, y sus dependencias, lo que permite reducir riesgos futuros y envía un mensaje potente a clientes, socios y reguladores: "podemos tropezar y caernos, pero nos levantamos y continuamos".

2. Reducción del riesgo

Se podría explicar cómo diseñar un plan para que lo que puede fallar haciendo el mayor daño, falle lo menos posible, y si falla, duela lo menos posible.

Disponer de un inventario de riesgos, identificando los más críticos para el negocio, con un respectivo dueño y un entorno de control adecuado, reducirá la probabilidad de que se materialicen, mitigará el impacto que el incidente pudiera producir, y como valor añadido permitirá mejorar la toma de decisiones:

- Priorizando inversiones con criterio.
- Eligiendo proveedores óptimos.
- Eliminando el síndrome de "todo es urgente".

No se debe evitar hablar de riesgos, al contrario, es beneficioso para una organización que el análisis de riesgos sea la base para la toma de decisiones conscientes, que forme parte de la cultura de gobierno, todo ello muestra un alto grado de madurez interna. Los beneficios son menos sobresaltos, más previsibilidad y equipos proactivos en lugar de reactivos.

3. Cumplimiento normativo y gobernanza

El cumplimiento no debe verse como un mero trámite burocrático, o para evitar sanciones, debe servir como esqueleto que da orden, define responsabilidades y agiliza la ejecución.

Marcos como las diferentes ISO, DORA, ENS o RGPD deben ser vistas como herramientas, guías, en las que las que la organización puede apoyarse para:

- Definir políticas, procedimientos, protocolos.
- Establecer quién decide y quién responde.
- Evidenciar que se hace lo que se dice.

Los beneficios obtenidos son: menos sorpresas regulatorias, mayor garantía de cara a los clientes y socios y anticipación de mejores resultados en auditorías.

Un incidente deja de gestionarse de manera improvisada, convirtiéndose en un proceso definido con roles y umbrales temporales. En resiliencia, la gobernanza es la columna vertebral; garantizando que la organización se mueve de manera coordinada y eficaz en momentos de máxima complejidad e incertidumbre.

4. Confianza y reputación

La confianza se obtiene con todo el trabajo previo ante la previsión de un incidente que ponga a la organización en riesgo, y se demuestra cuando éste se produce. Cuando una organización es resiliente actúa con rapidez, sin improvisación, aprende y comparte lo aprendido, comunica en tiempo y forma.

Este comportamiento genera lealtad en clientes, socios, y compromiso interno en los equipos, así como mayor confianza por parte de proveedores y agilidad en la toma decisiones por parte de los órganos de gobierno. Sin olvidar unas mayores garantías y transparencia para organismos reguladores o supervisores, que a su vez obtienen evidencias de cumplimiento y control.

Convertir un incidente en credibilidad acumulada es un sello de calidad en organizaciones que invierten en la función de resiliencia.

5. Adaptación ágil

La resiliencia es elástica, permite ajustar el rumbo sin perder estabilidad cuando llega una nueva norma, cuando cambia la tecnología, cuando se introducen nuevos sistemas, cuando algo falla, o cuando un proveedor crítico no responde según lo esperado.

También es beneficioso porque se reducen los costes en fases de cambio, cuando se afrontan esas etapas, si la organización ya está entrenada, no depende de improvisación, sino de procesos conocidos y repetidos. En mercados cambiantes y que premian la eficacia y la rapidez, esta agilidad es una ventaja respecto a otros.

6. Cultura sólida

Es el sistema operativo de la resiliencia. Si la cultura forma parte del ADN, todo funciona mejor, se trata de hábitos tales como reportar un incidente en el momento adecuado, reportar errores sin miedo, revisar accesos como rutina e incluir el riesgo como parte del diseño.

Si las personas entienden por qué (proteger al cliente, sostener el negocio), los controles dejan de sentirse como un obstáculo y se integran de forma natural. La cultura reparte responsabilidad, la seguridad deja de ser responsabilidad de un subconjunto para formar parte de la cultura de todos, cada incidente se convierte en una lección aprendida.

Invertir en cultura ofrece el mejor retorno de inversión a medio plazo, traduciéndose en menor número de incidentes, mayor eficiencia, y por tanto en una organización robusta y mejor preparada.

7. Ventaja competitiva

Los 6 puntos vistos anteriormente se cristalizan en este. La resiliencia se traduce en un mayor tiempo con el servicio operativo, menor tiempo en recuperaciones después de incidentes, decisiones mejor tomadas y auditorías más sencillas de gestionar con mejores resultados.

Se obtienen beneficios frente a la competencia dado que se transmite seguridad al cliente. Una organización resiliente trasmite seguridad, confianza, robustez, es más fiable dado que demuestra que es capaz de retomar la normalidad con agilidad.

Todo ello repercute en que sea vista como un referente por su valor añadido, lo que le permite destacar en el mercado frente a sus competidores.

ACTIVIDADES DE RESILIENCIA EN LA EMPRESA

4

4.1. Responsable de resiliencia vs CISO vs Responsable de Continuidad

La resiliencia organizacional requiere coordinar de manera coherente diferentes funciones que, históricamente, han operado con marcos y responsabilidades independientes: Tecnología, Seguridad de la información, Continuidad de negocio y la Gestión de crisis.

El CRO emerge como figura transversal cuya misión es integrar estas capacidades dentro del sistema consolidado de gestión de la organización, evitando silos y facilitando una respuesta coherente ante interrupciones complejas.

La resiliencia forma parte del sistema integrado de gestión (SIG) y se apoya en los mismos principios de planificación, supervisión, control y mejora continua que rigen otros sistemas basados en normas ISO. Esta integración permite evitar estructuras paralelas, garantizar una visión unificada de riesgos y capacidades, y asegurar que tecnología, seguridad, continuidad y crisis se gestionan bajo un marco común. El CRO no sustituye a funciones especializadas como el CIO, el CISO, el Responsable de Continuidad o el Responsable de Gestión de crisis, sino que articula sus resultados para aportar coherencia y alinear todas estas funciones con la protección del servicio esencial.

Relación entre el CRO y el CIO

El CIO (Chief Information Officer) lidera la gestión de la tecnología. Su función consiste en asegurar que la tecnología soporta de manera adecuada las necesidades del negocio. Entre otras, debe gestionar los incidentes tecnológicos y los planes de recuperación ante desastres (DRP por sus siglas en inglés).

El CRO debe recibir información completa de los planes de recuperación ante desastres definidos en la organización, las pruebas de los mismos, debilidades identificadas y planes de mejora para solventar las debilidades detectadas. También debe recibir información precisa de cualquier incidente tecnológico que pueda comprometer la prestación de los servicios esenciales, de su gestión y participar en el ejercicio de lecciones aprendidas.

Relación entre el CRO y el CISO

El CISO lidera la seguridad de la información y la ciberseguridad. Su función se orienta a prevenir, detectar y responder a incidentes digitales, así como contribuir al cumplimiento de marcos regulatorios como NIS2, ENS y DORA cuando apliquen.

El CRO complementa esta visión con una aproximación más amplia que evalúa:

- El impacto de incidentes digitales en procesos y servicios esenciales.
- La posibilidad de operar en modo degradado.
- La coordinación táctica y estratégica durante incidentes graves.
- Y la integración de la dimensión digital en el sistema global de resiliencia.

Ambas figuras colaboran especialmente en escenarios híbridos, donde incidentes tecnológicos y operativos se solapan.

Relación entre el CRO y el Responsable de Continuidad

El Responsable de Continuidad desarrolla, mantiene y prueba los planes de continuidad. Su perspectiva es principalmente operativa y se centra en restaurar procesos críticos/esenciales en tiempos aceptables. La continuidad de negocio constituye un componente esencial del sistema de resiliencia, pero no su totalidad. El CRO integra estos resultados dentro de una visión más amplia que combina:

- Interdependencias.
- Impacto en servicios esenciales.
- Escalado operativo y estratégico.
- Coordinación con el CISO, el Responsable de Seguridad de la información (RSI) del marco ENS y/o, cuando aplique, con el Responsable de Seguridad y Resiliencia (RSR) del marco CER. También con otras figuras que puedan existir en la organización (gestión de terceros, asesoría jurídica o recursos humanos).

Relación entre el CRO y el Responsable de Riesgos

La relación entre el CRO y el Responsable de Riesgos resulta especialmente relevante para garantizar una gestión integral y coherente del ciclo del riesgo dentro de la organización. Ambas funciones comparten un objetivo común: reducir la probabilidad y el impacto de eventos que puedan comprometer la consecución de los objetivos estratégicos y, en particular, la prestación de los servicios esenciales.

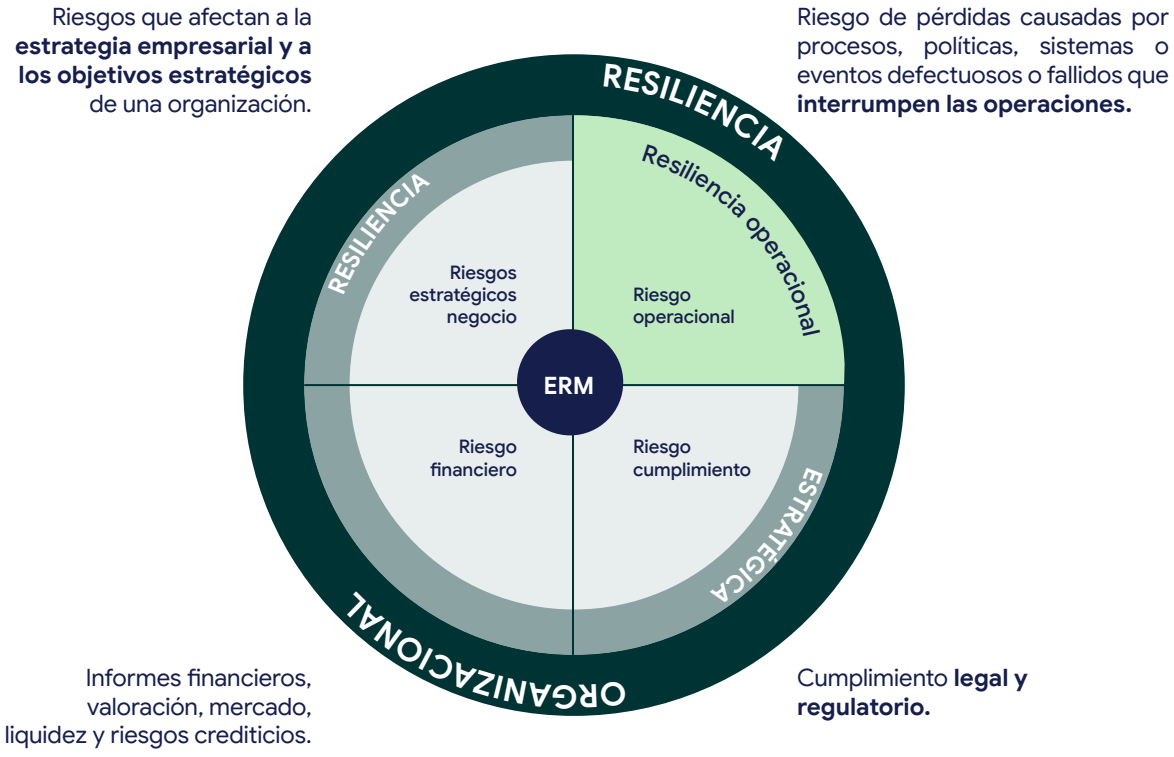
El Responsable de Riesgos se centra tradicionalmente en la identificación, análisis y evaluación de los riesgos, así como en la supervisión de controles preventivos y mitigadores, de acuerdo con los marcos de gestión de riesgos adoptados por la organización (ERM, ISO 31000 u otros modelos corporativos). El CRO complementa esta labor asegurando que, para los servicios esenciales, cuando dichos controles resultan insuficientes o fallan, la organización dispone de capacidades efectivas de respuesta, continuidad, recuperación y adaptación.

Desde esta perspectiva, la colaboración entre ambas funciones permite cerrar el ciclo completo del riesgo, desde su evaluación inicial hasta la activación de los planes de respuesta operativa. En particular, esta coordinación facilita:

- La utilización de los análisis de riesgos y los de impacto en negocio, como base para priorizar servicios esenciales, escenarios de interrupción y capacidades de resiliencia.
- La alineación entre los controles de riesgo definidos y los planes de continuidad, crisis y resiliencia.
- La detección temprana de fallos en los controles y la activación oportuna de los mecanismos de respuesta.
- Y la retroalimentación del sistema de gestión de riesgos a partir de las lecciones aprendidas tras incidentes reales o ejercicios.

En determinados modelos organizativos, las funciones de Responsable de Riesgos y CRO pueden confluir en una misma persona. Esta confluencia puede aportar ventajas en términos de coherencia, agilidad en la toma de decisiones y visión transversal.

Enterprise Risk Management (ERM) y Resiliencia



Gráfica 3. Visión 360º del Riesgo y la Resiliencia en la Organización

Evolución del CISO en el contexto NIS2, ENS, DORA y CER

La evolución regulatoria en seguridad y resiliencia, incluyendo NIS2, ENS, DORA y el futuro marco CER, está impulsando modelos en los que la interacción entre el CISO, el Responsable de Seguridad de la Información (RSI), el Responsable de Seguridad y Resiliencia (RSR) y el CRO debe ser cada vez más integrada.

A nivel conceptual:

- El **CISO/RSI** mantiene el liderazgo técnico en seguridad digital y cumplimiento de marcos de ciberseguridad.
- El **Responsable de Seguridad y Resiliencia** del marco CER tendrá responsabilidad sobre la seguridad física y la resiliencia.
- El **CRO** garantiza la coherencia global del sistema de resiliencia dentro del SIG, con un enfoque más estratégico.
- En **organizaciones pequeñas o medianas,** estas figuras **pueden coincidir en una misma persona,** siempre que cumplan con los requisitos regulatorios, y sus responsabilidades estén claramente documentadas y supervisadas.

El detalle sobre cómo estas funciones interactúan, se coordinan y reportan, tanto interna como externamente, se desarrolla más adelante, en el apartado **dedicado a los modelos organizativos y líneas de reporte.**

4.2. El responsable de resiliencia como directivo

Los ámbitos que hoy conforman la resiliencia organizacional, como la continuidad de negocio, la seguridad, la tecnología o la gestión de crisis, han sido tratados tradicionalmente como disciplinas especializadas e independientes, habitualmente ubicadas en áreas técnicas u operativas. Esta aproximación ha favorecido una gestión por silos, en la que cada función desarrollaba sus propias prioridades, metodologías y marcos de actuación.

No obstante, la experiencia acumulada en la gestión de incidentes y disrupciones pone de manifiesto que los eventos significativos rara vez afectan de manera aislada a una única área. Por el contrario, suelen generar impactos simultáneos en personas, procesos, infraestructuras tecnológicas, proveedores, clientes y reputación. La respuesta eficaz ante este tipo de situaciones exige una visión integral y una coordinación transversal que trascienda los límites organizativos tradicionales.

En este contexto, la figura del CRO surge como responsable de integrar las distintas dimensiones de la resiliencia bajo un marco común de gobierno. Sin embargo, para que esta función cumpla su propósito de manera efectiva, no es suficiente con contar con conocimientos técnicos o capacidad de coordinación operativa. Es imprescindible que el CRO disponga de autoridad directiva. La resiliencia no constituye únicamente un ámbito técnico, sino una responsabilidad estratégica que debe ser asumida al más alto nivel.

La resiliencia como ámbito de decisión estratégica

Una de las principales razones para situar al CRO en el nivel directivo es que las decisiones fundamentales en materia de resiliencia son, en esencia, decisiones de negocio.

Entre ellas cabe destacar:

- La identificación de los servicios esenciales cuya interrupción comprometería la continuidad y viabilidad de la organización.
- La definición de niveles aceptables de impacto y prioridades de recuperación, de manera consciente y alineada con los objetivos estratégicos.
- La determinación de inversiones destinadas a reforzar la capacidad de resistencia y recuperación, priorizando aquellas que aporten mayor protección al negocio.
- La incorporación de criterios de resiliencia desde el diseño de procesos y servicios.
- La evaluación y aceptación, en su caso, de dependencias estructurales respecto de terceros o tecnologías críticas.
- La decisión de mantener o interrumpir operaciones en condiciones adversas, ponderando los riesgos y consecuencias para la organización y sus grupos de interés.

Estas decisiones inciden directamente en la rentabilidad, la experiencia de cliente, el posicionamiento competitivo y la reputación corporativa. En consecuencia, no pueden abordarse desde una perspectiva exclusivamente técnica ni delegarse en niveles carentes de capacidad real de decisión.

Cuando la resiliencia no cuenta con una representación clara en el ámbito directivo, los riesgos asociados no desaparecen, sino que se asumen de forma implícita, sin un debate estratégico explícito ni una responsabilidad claramente asignada. Resulta, por tanto, esencial que el CRO disponga de legitimidad organizativa para participar e influir en las decisiones estructurales del negocio.

Autoridad y liderazgo en situaciones de crisis

El CRO, en su condición de directivo, debe contar con la facultad de activar y liderar los mecanismos de gestión de crisis de la organización. Su posición le permite integrar información procedente de múltiples áreas y ofrecer a la Alta Dirección una visión consolidada de los impactos y de las alternativas disponibles. De este modo, contribuye a una toma de decisiones informada y coherente en escenarios complejos.

Sin un posicionamiento en el nivel directivo, la función de resiliencia quedaría limitada a un papel consultivo, dependiente de la voluntad y colaboración de otras áreas. Con rango ejecutivo, en cambio, el CRO se configura como un referente organizativo capaz de alinear esfuerzos, establecer prioridades y garantizar una respuesta coordinada ante situaciones críticas.

Compromiso estratégico ante el entorno

La gestión de la resiliencia es objeto de creciente atención por parte de reguladores, inversores y clientes. Los marcos normativos y de supervisión refuerzan la necesidad de implicación activa del órgano de dirección, de asignación clara de responsabilidades ejecutivas y de mecanismos efectivos de rendición de cuentas.

Más allá de las exigencias regulatorias, situar al CRO en el nivel directivo constituye una declaración inequívoca de compromiso estratégico. Implica reconocer que la capacidad de mantener la prestación de servicios esenciales en condiciones adversas forma parte del núcleo de responsabilidades del negocio, y no de un mero cumplimiento formal.

De la formalidad a la capacidad efectiva

Numerosas organizaciones disponen de políticas y planes de resiliencia formalmente definidos. Sin embargo, la diferencia entre una resiliencia declarativa y una capacidad real reside en el liderazgo ejercido desde la alta dirección.

Cuando el CRO forma parte del equipo directivo, la resiliencia se integra de manera efectiva en la toma de decisiones estratégicas, en la asignación de recursos, en el diseño de procesos y servicios y en el desarrollo de la cultura organizativa. De este modo, deja de ser una función fragmentada para convertirse en una capacidad estructural del negocio.

En definitiva, la resiliencia organizacional no debe entenderse como una función de soporte ni como una disciplina técnica adicional. Se trata de una capacidad estratégica que condiciona la sostenibilidad, la legitimidad y la confianza en la organización. Por ello, el CRO debe ocupar un cargo directivo, con autoridad transversal, acceso al máximo órgano de gobierno y capacidad real para influir en las decisiones que garantizan la continuidad y el desarrollo del negocio en el largo plazo.

4.3. Actuaciones en tiempo de paz / momento de crisis

La resiliencia no es un estado estático, sino una capacidad que se desarrolla según el nivel de alerta de la organización. La función de resiliencia y la de gestión de crisis lideran la transición entre estas dos fases para garantizar que la empresa mantenga su total operatividad.

1. Fase A: actuaciones en tiempo de paz

También denominada fase de construcción y vigilancia, esta fase destaca por estar dentro del periodo de estabilidad, donde la actividad se centra en la preparación, la prevención y el fortalecimiento de la cultura de riesgos. El enfoque es proactivo y analítico, destacando los siguientes puntos:

Identificar los roles y personas clave necesarias para situaciones de crisis, así como sus suplentes en periodos de ausencia, asegurando que conocen claramente su misión y responsabilidades en este ámbito:

- **Monitorización de indicadores (KRI):** el equipo de riesgos supervisa de forma continua los umbrales de tolerancia definidos en la matriz de apetito de riesgo y se analizan las desviaciones para corregirlas.
- **Simulacros y pruebas de resiliencia:** según lo recomendado por las buenas prácticas, y también exigido por normativas como DORA o NIS2, se realizan evaluaciones de vulnerabilidades, pruebas de penetración dirigidas por amenazas (TLPT), simulacros basados en escenarios y ejercicios de intercambio de información.
- **Formación y sensibilización:** se ejecutan los planes de comunicación interna. Se capacita tanto a la Alta Dirección como al resto del personal para que identifiquen señales tempranas de riesgo, cómo identificar vulnerabilidades y entender el rol individual en la continuidad operativa, para asegurar la resiliencia de la organización ante disrupciones digitales.
- **Actualización del mapa de riesgos:** se revisan las amenazas emergentes (geopolíticas, tecnológicas o competitivas) y se ajustan los planes de continuidad y respuesta para reflejar el contexto actual, adaptando en consecuencia los requisitos y mecanismos de control aplicables a terceros.

2. Fase B: actuaciones en momentos de crisis

También denominada fase de respuesta y recuperación, en esta fase un riesgo se materializa (un ciberataque masivo, una sanción regulatoria inesperada o una interrupción de la cadena de suministro) y la función de resiliencia y la de gestión de crisis activan los protocolos de gestión de crisis, destacando los siguientes puntos:

- **Convocatoria del comité de crisis:** se convoca de inmediato al comité de crisis que corresponda según la magnitud del incidente para centralizar y agilizar la toma de decisiones, incluyendo la activación de los suplentes cuando no se disponga de los titulares.
- **Activación de planes de continuidad de negocio (PCN):** se ponen en marcha las medidas de contingencia para asegurar que las funciones esenciales de la empresa sigan operativas, respetando el tiempo de recuperación fijado como límite estratégico.
- **Comunicación regulatoria y externa:** en cumplimiento con el ENS, RGPD, DORA y la normativa aplicable en materia de ciberseguridad (incluyendo NIS2 y el Real Decreto-ley 12/2018), deben coordinarse las comunicaciones oficiales a las autoridades competentes y a las partes interesadas según lo establecido en el Plan de Comunicación.
- **Contención de daños y triaje:** se prioriza la protección de los activos críticos y servicios esenciales sobre las operaciones no esenciales.

4.4. Comunicación interna y externa

Durante una crisis es imprescindible llevar a cabo diferentes tipos de comunicaciones y notificaciones que emanarán desde el círculo de confianza que lidera la crisis. Deberá existir un plan específico de Comunicación en el cual se establezcan los grupos o partes interesadas destinatarios de dichas comunicaciones, así como quiénes deben ser las funciones responsables de ejecutar dichas comunicaciones.

Como se comentaba en el apartado anterior, las actividades a realizar por parte del CRO variarán en función de la situación (tiempo de paz / situación de crisis), siendo un buen ejemplo las relacionadas con la comunicación interna y externa, que serán clave para garantizar la coordinación y la protección de la reputación de la organización.

Durante la fase más aguda de la crisis, diferentes partes interesadas van a intervenir de una u otra forma, bien para colaborar en labores de contención, erradicación y recuperación, bien para interesarse por la situación, algunos de ellos velando por sus propios intereses.

Mientras los equipos de respuesta a incidentes se focalizan en actividades de contención, investigación, erradicación y recuperación, otro conjunto de especialistas debe dedicarse a la realización de actividades de comunicación.

Es fundamental, por tanto, tener correctamente identificados a todos estos grupos de interés por los que se dispersará la información del incidente acaecido y controlar el mensaje, evitando caer en cualquier tipo de contradicciones y proporcionando a cada uno de ellos la información pertinente, en tiempo adecuado, por el canal más propicio del que se disponga y en la secuencia óptima, de acuerdo con las legislaciones existentes.

Dada la diversidad de partes interesadas, se suele distinguir entre Comunicación interna (interna a la propia organización, empleados, sindicatos) y Comunicación externa, que incluiría el resto de las partes interesadas.

Es de extraordinaria utilidad contar con un Plan de Comunicación en el que se detalle con toda precisión la secuencia, así como quién será el emisor y quién el receptor. Se pueden definir plantillas tipo como base a comunicaciones finales que deberán ser revisadas, partiendo de las verdades oficiales sobre hechos confirmados, por los miembros del equipo de crisis de las funciones de Servicios jurídicos, Comunicación, Cumplimiento y la propia Dirección del negocio afectado.

Específicamente, es recomendable contar con un Manual de Comunicación de Crisis que, además de poder ayudar a calibrar la gravedad de la situación en función de algunos parámetros de entrada (repercusión en medios de comunicación y redes sociales, duración, contexto, impacto en el entorno), contenga un argumentario para cada tipo de incidente.

Otra buena práctica recomendada es la de disponer de una lista predefinida (o checklist) que sirva de guía para secuenciar las comunicaciones y para que todas y cada una de las partes interesadas sea debidamente informada, guardando registro de fecha, hora y contenido de la comunicación.

En este contexto, dicha checklist debe contemplar tanto a los organismos de respuesta técnica (INCIBE, CCN-CERT) como a las autoridades competentes en materia de ciberseguridad, incluyendo la Oficina de Coordinación de Ciberseguridad (OCC) en el caso de operadores de servicios esenciales con carácter crítico, así como otros organismos sectoriales o regulatorios que resulten de aplicación.

Parte Interesada	Ejecutor
Servicios Externos de primera respuesta (Emergency Incident Response)	Coordinador Comité Operativo
Aseguradora (por ejemplo, Ciberseguro)	Coordinador Comité Operativo
INCIBE / CNPIC / CCN-CERT	CISO; Seguridad Corporativa
Organismos supervisores y autoridades competentes (CNMV / SEC / AEPD / Banco de España, DGSFP)	Gobierno Corporativo; Relaciones con inversores; Compliance; Apoderado Negocio
Empleados	RRHH/RRLL
Sindicatos	RRHH/RRLL
Accionistas	Relación con Inversores
Clientes finales	Atención al Cliente del Negocio
Proveedores	Responsables de Contratos
Auditoría	Coordinador Comité Táctico
Prensa, Medios de comunicación y RRSS	Comunicación, Marca y Reputación

Gráfica 4. Modelo Integrado ERM–Resiliencia

Comunicación Interna

La norma ISO 22316 de Resiliencia Organizacional establece que la organización debe priorizar y dotar de recursos suficientes para mejorar la comunicación, la coordinación y la cooperación entre disciplinas de gestión de la organización.

Así pues, en tiempo de paz, la comunicación interna debe fomentar una cultura de resiliencia basada en la colaboración, transparencia y alineación estratégica. Es crucial romper silos organizacionales para integrar planes y políticas entre departamentos y promover sinergias que fortalezcan la capacidad de adaptación y recuperación ante cualquier crisis. El CRO debe actuar como facilitador y coordinador de equipos transversales, promoviendo la conciencia sobre la resiliencia mediante sesiones de concienciación y entrenamiento en todos los niveles, así como asegurando una comunicación clara y oportuna durante disrupciones para evitar desinformación.

El CRO, junto a la función de Comunicación en caso de existir, se ocupa de la gobernanza en comunicación interna en tiempo de crisis, definiendo roles claros, mecanismos de alerta y escalado, formando parte del Comité de Crisis.

El flujo de información debe ser transparente, evitando zonas de silencio que generen ansiedad, y promoviendo la cultura "informar pronto, actualizar con frecuencia". La formación constante y simulacros son esenciales para preparar a los líderes en mensajes breves y comunicación efectiva.

La comunicación interna, entendiéndose como la que se hace a personas o equipos pertenecientes a la propia organización, tiene características diferenciales. En función del tamaño de la organización se establecen varios grupos de interés:

- Conjunto global de empleados.
- Subconjunto formado por los equipos de respuesta a incidentes y de gestión de crisis, incluidos miembros de los Comités de Crisis (equipo de decisión, equipo de evaluación, equipo de coordinación, equipo de recuperación).
- Subconjunto formado por personal cuya función, para una determinada situación, resulte clave para mantener la continuidad de las operaciones.
- Resto de empleados cuya función, en la situación dada, no requiere de un restablecimiento con carácter urgente.
- Sindicatos.
- Accionistas.

Dados estos colectivos, las buenas prácticas coinciden en un punto esencial: se debe identificar claramente a las personas clave que sostienen los procesos críticos, ya que en caso contrario no puede haber una gestión eficaz de incidentes, de fallos operacionales ni de situaciones de crisis.

También se debe tener en consideración que la documentación y manuales de respuesta (o playbooks), por ejemplo, todos los relacionados con el proceso de Comunicación, deben estar accesibles en medios alternativos (por ejemplo, papel, aplicaciones en la nube) incluso ante fallos de los sistemas críticos de la organización.

En esta línea, se debe poder asegurar la contactabilidad de todo el personal, así como de los colectivos específicos de empleados. Como facilitador se recomienda el uso de listas de distribución dinámicas, así como el uso de herramientas especializadas de comunicación masiva de emergencias que integra múltiples canales (llamada telefónica, SMS, correo electrónico, notificación "push" en aplicaciones móviles, complementando a la tradicional cartelería digital o megafonía del edificio.

Para grupos como los empleados, una solución eficaz es ofrecer una línea telefónica informativa. El Comité de Crisis actualizará el mensaje para que cubra las necesidades generales de quienes no pueden recibir atención individualizada. Este servicio se diseña para proporcionar información masiva y desatendida durante una situación crítica o de emergencia. Su objetivo principal es optimizar la comunicación y reducir la carga de los equipos de respuesta, ofreciendo un canal único donde las personas pueden llamar y escuchar un mensaje pregrabado con instrucciones o actualizaciones.

Alternativamente, se pueden establecer otros canales de comunicación como por ejemplo una página web en la que se publique el estado del incidente (landing web) donde las partes interesadas puedan obtener la próxima actualización o información.

Comunicación Externa

El CRO, y la función de comunicación en caso de existir, deben asegurarse de que se gestiona la comunicación externa con un enfoque en proteger la reputación y generar confianza. Esto implica colaboración estrecha con la función de Comunicación para asegurar una narrativa corporativa proactiva que integre la resiliencia como valor central, asegurando coherencia con los mensajes internos. La gestión de partes interesadas y alianzas es clave, cultivando relaciones sólidas con clientes, proveedores, reguladores, medios y comunidades para poder contar con su apoyo durante la crisis.

Para conseguir esto, lo primero será identificar y mapear partes interesadas clave, evaluando relaciones y desarrollando estrategias de comunicación que la organización considere óptima, teniendo en cuenta que durante las situaciones de crisis se ha de convivir con la incertidumbre.

La estrategia de comunicación de crisis distingue entre comunicación proactiva y reactiva. La comunicación proactiva se aplica cuando las consecuencias del incidente tienen una influencia severa o grave en la salud, la seguridad, la reputación o la solvencia económica de la organización. La comunicación reactiva se aplica cuando el incidente no tiene consecuencias severas o graves. Es importante, por tanto, establecer el umbral en función de la situación para la activación formal del protocolo.

Durante la crisis, la comunicación externa debe ser rápida, precisa y empática, reconociendo el impacto en las partes afectadas y asumiendo responsabilidades para mitigar daños reputacionales, así como indicar claramente lo que la organización está haciendo para abordar la situación.

Para evitar la desinformación también es muy importante delimitar las personas o funciones que tienen atribuciones para emitir mensajes en nombre de la organización. Debe existir una política de comunicación externa que determine estos aspectos y concienciar a los empleados de que, en caso de incidente disruptivo, deben abstenerse de proporcionar a prensa o medios de comunicación ningún tipo de información y remitirse siempre a la función de comunicación o a quien tenga atribuida esta función en la organización (por ejemplo, el CRO si no hay función de comunicación).

Se recomienda la preparación de mensajes preaprobados para distintos escenarios y la coordinación legal para asegurar cumplimiento regulatorio y contractual. La gestión de redes sociales y la supervisión de rumorología son fundamentales para controlar la narrativa digital y evitar desinformación.

En el Plan de Comunicación de Crisis mencionado antes, de forma complementaria a las partes interesadas internas, han de ser contempladas todas las siguientes que se engloban dentro de la Comunicación Externa, incluyendo a las autoridades y organismos competentes en función del ámbito del incidente, tales como INCIBE, CCN, AEPD, Banco de España, CNMV o SEC, así como la Secretaría de Estado de Seguridad, a través de la Oficina de Coordinación de Ciberseguridad (OCC), en aquellos supuestos vinculados a operadores de servicios esenciales con carácter crítico o incidentes con impacto en la seguridad pública.

- Prensa.
- Redes Sociales.
- Relaciones Institucionales.
- Relaciones con inversores.
- Socios.
- Proveedores.
- Autoridades competentes y organismos de referencia en función del tipo de incidente.
- Clientes.
- Público en general.

Estos aspectos se alinean con estándares de buenas prácticas, que enfatizan la comunicación como capacidad central para la resiliencia organizacional. El CRO y la función de comunicación, si existe, en coordinación con las áreas internas deben adaptar estos elementos al contexto específico de la organización.

Desde el punto de vista de la comunicación con las partes interesadas, el seguimiento post-crisis es fundamental para documentar decisiones, realizar análisis de lecciones aprendidas y comunicar las medidas adoptadas para prevenir recurrencias, fortaleciendo así la confianza y la resiliencia organizacional. Las organizaciones deben poner en valor los esfuerzos realizados por sus equipos internos, mostrar agradecimiento por los actores externos que han ayudado a superar la disrupción, y premiar la fidelidad de los clientes por mantener la confianza en la organización.

Aspectos Transversales y Buenas Prácticas

Es fundamental garantizar la veracidad, coherencia y control temporal de los mensajes, evitando tecnicismos innecesarios y equilibrando empatía con rigor para conectar con las audiencias y transmitir control. La comunicación es vista como una herramienta clave que sostiene la cultura en tiempos de paz, la continuidad durante crisis y la reputación tras ellas.

La comunicación interna y externa deben hacerse de forma coordinada, evitando de esta forma que los empleados se enteren de las novedades por los medios de comunicación. De igual manera, se debe concienciar a los empleados de que deben abstenerse de realizar declaraciones ante los medios, evitar especulaciones y remitir cualquier consulta a los portavoces oficiales.

Se presenta un decálogo de comunicación en crisis que enfatiza la importancia de comunicar temprano, mantener coherencia, hablar claro, controlar la narrativa, mostrar empatía, validar jurídicamente los mensajes, priorizar la frecuencia sobre la perfección y comunicar aprendizajes post-crisis para consolidar la confianza:

- Protocolos claros: asegurar que todos conozcan su rol y las líneas de comunicación a seguir en caso de crisis. El protocolo debe establecer quién recibe qué, cómo y cuándo.
- Información oportuna: proporcionar actualizaciones precisas y en tiempo real al equipo interno durante una crisis para evitar rumores y estrés innecesarios.
- La comunicación externa debe estar alineada con las obligaciones regulatorias, cláusulas contractuales y consideraciones legales (responsabilidades, confidencialidad, GDPR, sanciones).
- Moral y motivación: transmitir un mensaje de fortaleza, aprendizaje y motivación para afrontar la adversidad, lo cual incrementa el compromiso y la productividad de los equipos en situaciones de gran exigencia.
- Colaboración: establecer alianzas que permitan contar con apoyo externo durante las disrupciones, comunicando la capacidad de la empresa para trabajar en red.
- “Bancos de Mensajes” preaprobados: tener plantillas de comunicados internos y externos para escenarios comunes de crisis (ciberseguridad, desastres naturales, etc.) que puedan ser adaptados rápidamente.
- Evitar las zonas de silencio donde la falta de información genera ansiedad o rumores.
- Establecer canales rápidos para notificaciones regulatorias obligatorias.
- Realizar una revisión exhaustiva para identificar qué funcionó, qué falló y dónde deben ajustarse los protocolos, los planes de respuesta y las capacidades de comunicación.
- Informar a todas las partes interesadas que la crisis se ha resuelto y describir las medidas correctivas implementadas para prevenir una recurrencia (esto refuerza la confianza y la capacidad de aprendizaje).

En resumen, el CRO es el eje central que asegura que la organización no solo sobreviva a las adversidades, sino que aprenda y se fortalezca mediante una comunicación estratégica, transparente, coordinada y proactiva tanto interna como externamente, con protocolos claros y adaptados al contexto específico de la organización.

Los protocolos de comunicación de crisis son la herramienta más crítica bajo la supervisión del CRO para proteger a la organización cuando el riesgo se materializa.

MODELOS ORGANIZATIVOS Y RELACIONALES

5

El modelo organizativo idóneo para la función de resiliencia no es único, sino que estará condicionado por diversos factores estructurales y operativos de la organización, tales como el sector de actividad, el grado de dispersión geográfica, el nivel de regulación aplicable, el grado de dependencia tecnológica, el volumen de la organización o la complejidad de sus operaciones.

En función de estos parámetros, cada organización deberá identificar el mejor encaje organizativo para el contexto específico de la compañía, equilibrando eficiencia operativa, independencia en la supervisión y capacidad de respuesta ante incidentes.

5.1. Modelo 1: el Responsable de Resiliencia dentro de una subárea de tecnología

Las organizaciones pueden tomar la decisión de incluir a la figura del responsable de resiliencia dentro del área de tecnología. La Dirección de Riesgos no puede supervisar cada proceso técnico de forma aislada, por ello, se establece la figura del Responsable de Resiliencia que actúa como nodo crítico de articulación entre los equipos de tecnología y la dirección de riesgos.

Ventajas del modelo de responsable de resiliencia dentro del área tecnológica

Este enfoque prioriza la agilidad técnica y la integración del riesgo en el día a día de todos los desarrollos y operaciones tecnológicas.

Al pertenecer al área de tecnología tiene un conocimiento técnico profundo, por ello el responsable de resiliencia comprende la arquitectura real de los sistemas. Esto evita que los planes de resiliencia sean “documentos teóricos” y garantiza que sean factibles desde un punto de vista técnico.

La proximidad física y jerárquica permite que el control de riesgos se aplique en las fases iniciales de cualquier proyecto tomando la “Resiliencia desde el Diseño”. Se detectan vulnerabilidades antes de que lleguen a producción, lo que reduce costes de corrección.

En caso de incidente, hay una respuesta inmediata. La persona responsable ya forma parte del equipo técnico. No existe una “curva de aprendizaje” sobre lo que está fallando; la comunicación con los administradores de sistemas es directa y en su mismo lenguaje.

El personal de tecnología suele percibir a las figuras de riesgos externas como “frenos” burocráticos. Un responsable de resiliencia interno se ve como un facilitador que ayuda a construir sistemas más robustos, mejorando la aceptación de los controles y reduciendo la resistencia al cambio.

Desventajas del modelo de responsable de resiliencia dentro del área tecnológica

El principal problema de este modelo es la posible pérdida de objetividad y la dilución de la autoridad de control frente a las necesidades de entrega rápida.

Si el área de tecnología tiene presión por cumplir plazos de entrega, el responsable de resiliencia en este modelo puede verse tentado (o presionado por su superior jerárquico) a relajar los controles de seguridad para no retrasar un lanzamiento, generándose de esta forma un conflicto de intereses.

Al estar dentro de una subárea, existe el riesgo de que la persona se enfoque exclusivamente en la resiliencia técnica, perdiendo de vista el impacto de negocio o los riesgos legales y reputacionales (visión holística) que el CRO sí supervisa.

Si la relación entre el responsable de resiliencia y el equipo técnico es demasiado estrecha se puede generar debilidad, pues la función de control puede volverse complaciente, dificultando la detección de errores críticos que una auditoría externa sí encontraría.

Es frecuente que, al estar dentro de tecnología, este perfil acabe asumiendo tareas de desarrollo o mantenimiento que no le corresponden, descuidando su función principal de vigilancia y cumplimiento normativo.

Para mitigar estas desventajas, se podría optar por un Modelo de Doble Reporte: ubicar al responsable de resiliencia físicamente en tecnología (para mantener la agilidad), pero manteniendo también un reporte funcional directo hacia el Responsable de Riesgos. Esto garantizaría que, ante cualquier conflicto entre “rapidez de entrega” y “seguridad”, la dirección de riesgos tenga la última palabra.

5.2. Modelo 2: el Responsable de Resiliencia en un área específica de seguridad.

La función de Resiliencia se puede ubicar también dentro de un área específica de Seguridad. Este modelo puede responder a la creciente necesidad de integrar la gestión de la resiliencia operativa con las capacidades de protección, detección y respuesta ante incidentes de seguridad.

Ventajas del Modelo de responsable de resiliencia dentro del área de Seguridad

La integración de la función de Resiliencia en el área de Seguridad permite aprovechar sinergias entre la gestión de riesgos tecnológicos, la continuidad de negocio y la ciberseguridad.

En este modelo, la persona responsable de Resiliencia (CRO) suele reportar de forma directa a la Dirección de Seguridad, lo que facilita la coordinación de políticas, procedimientos y controles orientados a la protección de los activos críticos de la organización y que formarían parte del Marco Normativo de la Seguridad de la Información.

En este modelo la función de Resiliencia compartiría recursos, herramientas y metodologías con el área de Seguridad, lo que favorece la detección temprana de amenazas y la respuesta coordinada ante posibles incidentes de seguridad. La ubicación en el área de Seguridad facilita la integración de la resiliencia en los procesos de gestión de incidentes, pruebas de recuperación y simulacros, así como en la formación y concienciación del personal interno de la organización.

Entre los beneficios de este modelo se encuentran la optimización de recursos, la mejora en la comunicación interna y la capacidad de respuesta ante incidentes complejos que afectan tanto a la seguridad como a la continuidad de las operaciones.

Desventajas del Modelo del responsable de resiliencia dentro del área de Seguridad

La dirección de Seguridad TI tiene una gran cantidad de responsabilidades (proteger contra ciberataques, cumplir normativas de seguridad, gestionar identidades, etc.), muchas de ellas son de naturaleza inmediata y reactiva. Si a estas responsabilidades se le suma la responsabilidad de resiliencia operativa existe el riesgo de que, en la práctica, los temas de resiliencia queden relegados frente a “lo urgente” de ciberseguridad.

Uno de los principales retos de la función de Resiliencia consiste en garantizar que dicha función tenga una visión transversal y estratégica, evitando que su alcance se limite únicamente a los aspectos tecnológicos o de ciberseguridad.

Una de las responsabilidades adquiridas por el CRO es el Marco de riesgos TIC y, dentro de dicho Marco, se encuentra la Estrategia de Resiliencia Operativa. Esta estrategia, que en la mayoría de las organizaciones se aprueba en el Consejo, tiene como uno de sus objetivos analizar la situación de resiliencia operativa de la entidad. Para ello, el CRO debe de analizar y controlar cómo están implementados los controles, tanto de seguridad como técnicos, propios de áreas como infraestructuras o tecnología. Para realizar este tipo de controles es recomendable que sea independiente tanto del CISO como del CIO y así evitar un posible conflicto de interés.

5.3. Modelo 3: el Responsable de Resiliencia en el área de Continuidad de Negocio / Riesgos

La función de resiliencia en el área de Continuidad de Negocio y Riesgos puede ser una opción especialmente para aquellas organizaciones que conciben la resiliencia como una extensión natural del gobierno del riesgo y de la protección de los procesos críticos.

Ventajas del Modelo de responsable de resiliencia dentro de Continuidad de Negocio / Riesgos

En este enfoque, la resiliencia se apoya en disciplinas ya consolidadas como el análisis de impacto en negocio (BIA), la gestión de riesgos corporativos y la planificación de la continuidad, integrándolas bajo una visión común orientada a asegurar la prestación sostenida de los servicios esenciales. La cercanía con la función de riesgos permite que la resiliencia se fundamente en una identificación estructurada de amenazas, vulnerabilidades y dependencias, facilitando una priorización objetiva de escenarios de disrupción y una asignación más eficiente de recursos. Asimismo, la integración con continuidad de negocio garantiza que las capacidades de respuesta y recuperación no se limiten a ejercicios teóricos, sino que se traduzcan en planes operativos probados, alineados con los niveles de tolerancia al impacto definidos por la Alta Dirección. Este modelo favorece una visión menos reactiva y más preventiva de la resiliencia, en la que los riesgos no se gestionan únicamente desde la probabilidad de ocurrencia, sino también desde la capacidad real de la organización para absorber y recuperarse de los impactos.

Desventajas del Modelo del responsable de resiliencia dentro de Continuidad de Negocio / Riesgos

No obstante, este modelo puede no ser efectivo si la función de resiliencia no mantiene una posición transversal y queda circunscrita a un enfoque excesivamente documental o metodológico. La resiliencia debe conservar su capacidad de influencia estratégica, participando en la toma de decisiones relevantes y coordinándose estrechamente con seguridad, tecnología y negocio.

Cuando se gobierna adecuadamente, este modelo permite cerrar el ciclo completo del riesgo: anticipación, mitigación, respuesta y aprendizaje y convierte la continuidad de negocio en un pilar vivo de la resiliencia organizacional, más allá del cumplimiento normativo.

5.4. Modelo de las 3 Líneas

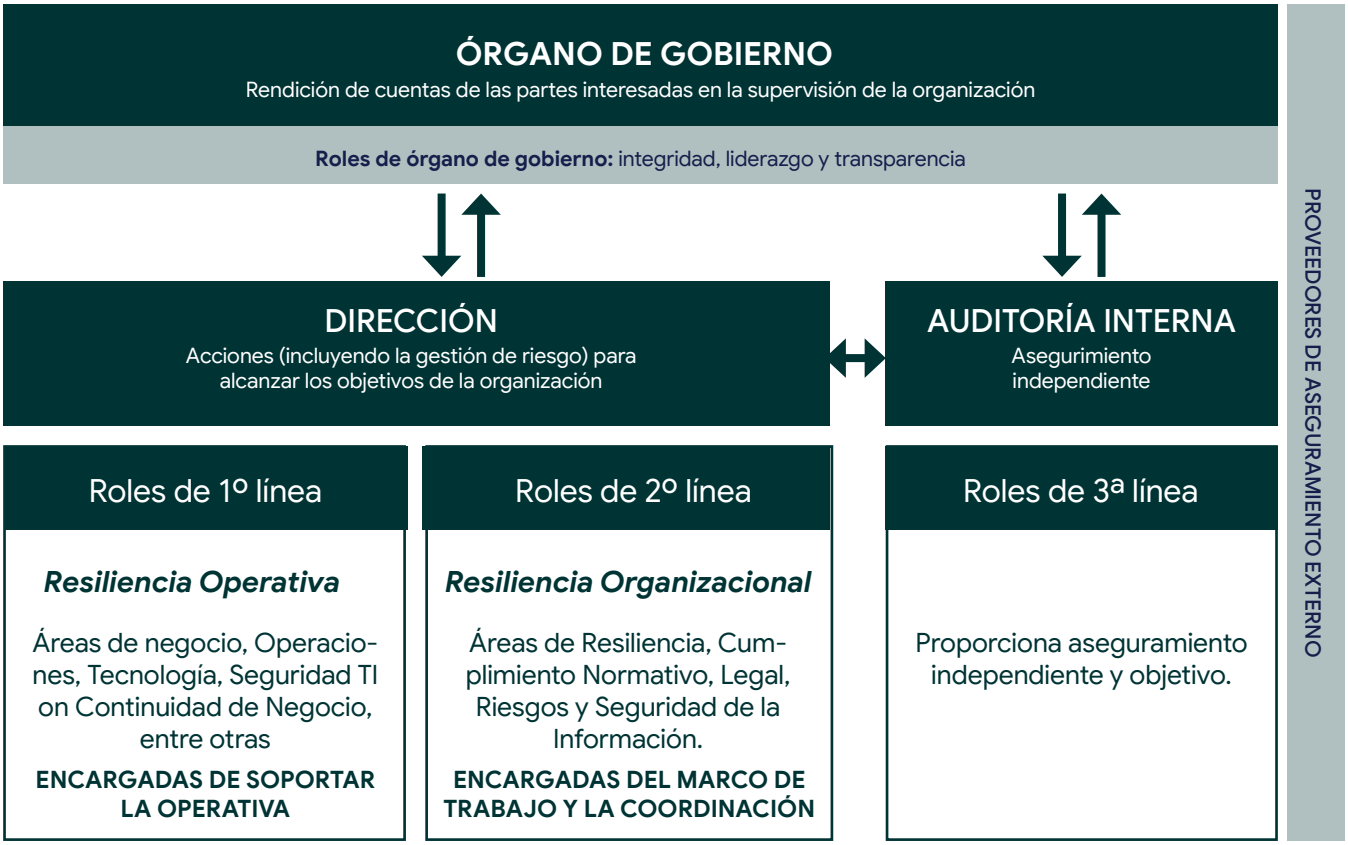
Para aquellas organizaciones enfocadas en los modelos de líneas de defensa, se adjuntan también ciertas propuestas de implantación. Esta sección puede no ser de interés para entidades que no utilicen este enfoque y terminología en su día a día.

El Modelo de las 3 líneas de defensa, o 3LoD según su acrónimo en inglés, fue presentado en 2013 por el Instituto de Auditores Internos, estableciendo un modelo operativo para la gestión de riesgos en el que se diferenciaban las funciones de las áreas operativas o de negocio (primera línea de defensa), las áreas de riesgos y cumplimiento (segunda línea de defensa), y auditoría interna (tercera línea de defensa).

En el año 2020, se presentó la nueva versión del modelo, que pasaba a denominarse simplemente 3 líneas, dado que la separación de roles en lo referente a Operación, Riesgos y Cumplimiento normativo, y Supervisión y Aseguramiento, se aplica a numerosas áreas y procesos dentro de las organizaciones.

A continuación, se muestra una posible adaptación del Modelo de las 3 líneas a la Función de Resiliencia:

Adaptación del Modelo de las 3 líneas a la función de resiliencia



Gráfica 5. Gobernanza de la Resiliencia basada en el Modelo de las Tres Líneas

En este modelo, el CRO está ubicado en la 2LoD, formando parte de los roles que garantizan la resiliencia organizacional. También puede ser una función de control dentro de la 1LoD, es decir, una especie de línea 1.5, o incluso coexistir en ambos niveles.

Ventajas del Modelo de las 3 líneas

El modelo de 3 líneas permite la existencia de una función de Resiliencia tanto en la 1LoD como en la 2LoD y que ambas coexistan, siendo la de 1LoD una especie de línea 1.5 que combina gestión y control. En este caso el CRO probablemente sería la figura 1.5 y la 2LoD estaría ubicada en Riesgos.

Este modelo tendría ventajas similares a las vistas para los modelos que ubican la función de Resiliencia dentro de Tecnología, pero las desventajas quedarían muy mitigadas por la existencia de una 2LoD independiente.

Desventajas del Modelo de las 3 líneas

La principal desventaja del Modelo de las 3 líneas es que tiene un coste económico mayor.

5.5. Gobernanza y líneas de reporte interna y a Alta Dirección

La resiliencia organizacional exige una arquitectura de gobernanza que garantice coherencia entre seguridad, continuidad, tecnología, operaciones y riesgos.

A diferencia de los modelos organizativos descritos en los apartados anteriores, este enfoque no define la ubicación de la función, sino las líneas de reporte y los mecanismos de integración necesarios para asegurar su correcta gobernanza.

Más allá de las funciones individuales descritas anteriormente, las organizaciones deben disponer de líneas de reporte claras, tanto internas como hacia organismos reguladores, con el fin de:

- Asegurar una visión integrada del riesgo,
- Facilitar la toma de decisiones estratégicas en momentos críticos,
- Cumplir con requisitos regulatorios en materia de resiliencia operativa, ciberseguridad y protección del servicio esencial.

Este modelo de gobernanza debe integrarse dentro del Sistema integrado de gestión (SIG), evitando estructuras paralelas, duplicidades y solapamientos funcionales.

Principios generales del modelo de reporte

1. Coherencia dentro del sistema integrado de gestión (SIG)

Las funciones de seguridad, continuidad, resiliencia, riesgos y tecnología deben operar bajo un marco común de planificación, supervisión y mejora continua, aprovechando la estructura de alto nivel de las normas ISO.

2. Visión única de riesgo y resiliencia para la Alta Dirección

El Comité de Dirección debe recibir información consolidada que integre:

- Riesgo digital (CISO/RSI),
- Capacidad operativa (Continuidad),
- Impacto en servicios esenciales (RSR/CRO),
- Dependencias críticas internas y externas (CISO/RSI/Continuidad/RSR).

3. Posibilidad de coincidencia de roles

En organizaciones pequeñas o medianas, los roles de CISO, RSI, RSR y CRO pueden coincidir en la misma persona, siempre que el SIG documente responsabilidades y controles que garanticen una supervisión adecuada.

4. Alineación regulatoria

El modelo de gobernanza debe dar respuesta simultáneamente a:

- DORA → resiliencia operativa digital y gobernanza TIC.
- NIS2 → ciberseguridad y notificación de incidentes graves.
- ENS → responsabilidad formal del RSI.
- CER → protección del servicio esencial y figura del Responsable de Seguridad y Resiliencia (RSR).

Modelos de gobernanza interna según el tamaño de la organización

Organizaciones pequeñas o medianas

- CISO, RSI, RSR y CRO **pueden coincidir en una misma persona**, siempre que las responsabilidades estén documentadas.
- El SIG toma un papel esencial para asegurar independencia en la supervisión.
- El comité de resiliencia puede cubrir seguridad, continuidad y riesgos.

Organizaciones grandes o complejas

- **Roles diferenciados:**
  - CISO (seguridad digital)
  - RSI (cumplimiento ENS)
  - RSR (servicio esencial)
  - CRO (resiliencia global)
  - Responsable de Continuidad (continuidad operativa)
- **Comités específicos:**
  - Comité de seguridad corporativa
  - Comité de ciberseguridad (si no está integrada en seguridad corporativa)
  - Comité de continuidad
  - Comité de resiliencia o de operaciones críticas
  - Comité de riesgos
- **Flujos de reporte bidireccionales:**
  - Técnico ⟶ Estratégico
  - Operativo ⟶ Alta Dirección

5.6. Recomendaciones en función del tipo de empresa

Tal como se ha mencionado a lo largo de la guía, la elección sobre dónde ubicar las responsabilidades de resiliencia dentro de la organización, sobre cómo estructurar el modelo de relación con otras funciones y sobre cómo establecer el modelo de reporting dependerán en gran medida del tipo de organización en la que se desea implantar la función.

Estas decisiones van a determinar, o como mínimo condicionar, la estrategia y el enfoque que se le dé a la función de resiliencia, y por ende, van a marcar diferencias significativas en el proceso de definición y despliegue de la misma.

En este apartado sería perfecto poder desglosar las tipologías de empresa que existen y dar recomendaciones concretas para cada una, no obstante, las casuísticas son prácticamente infinitas y abarcarlas todas resultaría imposible. Por ello se van a dar recomendaciones en función de diversas características que son más relevantes para una organización:

1. Tamaño de la organización

El tamaño y la complejidad de la organización influirán tanto en la segregación de funciones como en el alcance de la función.

Pequeñas y medianas empresas

Organización: en este tipo de organizaciones las figuras del responsable de continuidad, el responsable de seguridad, el responsable de resiliencia y el responsable de riesgos pueden coincidir en una misma persona.

En este contexto resulta esencial que las responsabilidades estén debidamente documentadas, acotando el ámbito de actuación, estableciendo líneas de reporting claras y asegurando la independencia en la supervisión. Asimismo, siempre que surjan conflictos de interés entre la gestión de riesgos de resiliencia y la agilidad en la implantación tecnológica, deberían resolverse por un área de gestión de riesgos independiente o una jerarquía superior. La toma de decisiones informada debería quedar perfectamente documentada para delimitar responsabilidades sobre la aceptación de un riesgo o del retraso de un proyecto que impacte en negocio.

Implantación: realizar una implantación integral, cubriendo todas las áreas y todos los procesos de negocio, puede resultar factible y económicamente viable; no obstante, la carga excesiva de trabajo acumulada sobre una misma figura que desempeña demasiadas funciones puede ser traicionera, y embarcarse en una implantación integral demasiado optimista suele desembocar en un proyecto fallido.

Un indicador útil para determinar si una implantación integral es realmente viable es el tiempo transcurrido entre el inicio del proyecto y la ejecución de las primeras pruebas. No deberían pasar más de 8-9 meses desde el inicio del proyecto hasta el inicio de la fase de pruebas, de lo contrario será recomendable fasear la implantación por áreas o procesos de negocio.

Maduración / mantenimiento: es habitual que en pequeñas y medianas empresas se descuide el proceso continuo o el mantenimiento y la implantación quede como un proyecto desfasado. Programar con antelación reuniones para los comités periódicos, con agendas concretas, planificar los hitos anuales del ciclo continuo y formalizar los procesos de revisión y mantenimiento son las herramientas que permitirán evitar que figuras con múltiples roles descuiden estas responsabilidades.

Grandes empresas

Organización: en este tipo de organizaciones existen múltiples configuraciones de distribución de responsabilidades entre distintos roles, que además pueden estar ubicados en distintas áreas, cada una de ellas con ventajas e inconvenientes, tal como se ha discutido ampliamente en secciones anteriores.

En este contexto puede ser muy recomendable establecer un HUB organizativo que gestione la función de resiliencia operativa. Un HUB organizativo es una unidad de trabajo paralela a la estructura organizativa formal que coordina, integra y conecta diferentes áreas, funciones, procesos o equipos dentro de una empresa. Su propósito es centralizar información, facilitar la colaboración, armonizar prácticas y acelerar la toma de decisiones, especialmente en contextos complejos o de transformación.

Crear un equipo de proyecto multidisciplinar para la implantación, y que más adelante evolucione a un HUB organizativo de resiliencia con responsables del área tecnológica, el área de riesgos y cumplimiento, las áreas de operaciones y las áreas de backoffice, con dedicación asignada, presupuesto, capacidad de gobierno propio y capacidad de reporting al comité de dirección puede ser la forma ideal de romper los silos organizativos sin necesidad de crear un área dedicada, especialmente en las fases iniciales de la función.

Implantación: el alcance de esta fase de implantación debe ser limitado en el tiempo. Lo más aconsejable es que los procesos recurrentes de la función de resiliencia se implanten con periodicidad anual, para lo que es esencial realizar un despliegue iterativo incorporando procesos de negocio o áreas de la organización en ciclos de despliegue inferiores a 8-9 meses, desde la definición inicial de la función hasta la ejecución de pruebas, de forma que puedan pasar a formar parte del proceso periódico sin alterar su ejecución.

Cómo se delimita el alcance de cada iteración dependerá de cada organización. Debe realizarse una segmentación del alcance que resulte natural a la operación normal de la compañía y sus dependencias, bien sea por unidades organizativas, áreas, zonas geográficas o procesos de negocio.

Maduración / mantenimiento: el mayor riesgo para que la función de resiliencia pueda entrar en la etapa de maduración y mejora continua es la naturaleza iterativa de la implantación, sobre todo si la gestión del proyecto de implantación y la operación de los procesos resultantes la realizan las mismas personas. En estos casos suele ser recomendable establecer equipos dedicados a la implantación y la operación, o como mínimo fijar dedicaciones mínimas a cada caso tras el primer ciclo de implantación, evitando así que parte de la función quede desfasada durante los primeros años.

2. Nivel de centralización de las operaciones de negocio

Para establecer la función de resiliencia es esencial un modelo de relación robusto con los responsables de las operaciones de negocio, por lo que su organización va a ser un factor clave para el establecimiento y la operación de la función.

Organizaciones centralizadas

Organización: en organizaciones centralizadas donde se dispone de un COO (Chief Operations Officer) o una figura similar que controla y coordina las operaciones, el CRO podrá articular comités y líneas de reporting menos complejas. Tratar de mantener la simplicidad en el modelo de gobierno de la función, alineado con el de la propia organización, es lo más recomendable en estos casos.

Implantación: en estructuras centralizadas la implantación debe llevarse a cabo top-down, no solo en el alineamiento estratégico inicial, sino acompañando toda la toma de decisiones en la definición y el despliegue. En los casos donde el volumen o la complejidad de la organización aconsejen una implantación iterativa, el COO global será un aliado clave para determinar cuál es la forma más natural de segmentar y qué área o proceso de negocio es el más crítico para empezar la implantación por ahí.

Maduración / mantenimiento: de nuevo, mantener una estructura de procesos central, alineada con las operaciones, en un ciclo único anual permitirá ser eficiente en el mantenimiento de la función.

Organizaciones con centros de operaciones regionales o locales

Organización: independientemente del modelo organizativo escogido para la función de resiliencia y del área en que estén ubicados sus responsables, debe alinearse con la estructura regional / local de las operaciones de la organización donde pretende implantarse. En estos casos es recomendable incorporar a responsables regionales / locales en el gobierno de la función para llegar a todas las áreas de negocio, aunque no se corresponda por su nivel de reporting.

En los casos donde no sea posible incorporar responsables locales / regionales, bien sea por el volumen de personas o el cambio horario, puede optarse por replicar la estructura de gobierno de la función de resiliencia a nivel local/regional, organizando comités acotados.

Implantación: se tendrá en consideración una implantación iterativa definiendo alcances vinculados a la segmentación territorial. Este enfoque es muy arriesgado ya que será habitual pasar por alto dependencias que resultarán críticas durante la implantación, generando retrabajo o incluso llegando a puntos de bloqueo. Un estudio previo de interdependencias entre funciones y activos críticos compartidos previo a la toma de decisión sobre la estrategia de implantación es muy recomendable en este caso.

Adicionalmente, aunque se realice una implantación iterativa vinculada a un criterio territorial, es muy recomendable presentar el proyecto a toda la organización, justificando de forma clara y objetiva la priorización de regiones / áreas para poder gestionar el factor humano que puede entorpecer la relación con áreas relegadas a etapas menos prioritarias.

Maduración / mantenimiento: es recomendable establecer equipos dedicados a la implantación y la operación. Cuando haya sido posible llevar a cabo una implantación integral, cubriendo todos los procesos de negocio y áreas para una región o localidad concreta, resultará esencial iniciar los procesos de maduración de la función de forma sostenida para evitar perder el trabajo realizado, además que permitirá obtener lecciones aprendidas y mejoras continuas que resultarán de gran valor no solo cuando otras ubicaciones se incorporen a la función sino también en los propios ciclos de implantación.

Este apartado se ha centrado en dos características clave que tendrán un gran impacto en el modelo organizativo y la estrategia de implantación, y pueden ser de aplicación de manera general.

No obstante, existen otras características, de carácter más técnico y específico, que también se deben tener en cuenta para la toma de decisiones sobre la función de resiliencia, como son el nivel de centralización de funciones relacionadas con la continuidad (por ejemplo, Tecnología), el nivel de dependencia tecnológica en la cadena de valor o el nivel de presión regulatoria sobre el sector.

Estas variables deben analizarse de forma complementaria en función del contexto específico de cada organización.

PERFIL DEL RESPONSABLE DE RESILIENCIA

6

6.1. Características de un Responsable de Resiliencia (Chief Resilience Officer)

El papel del CRO ha adquirido una relevancia estratégica en las organizaciones sujetas a regulaciones como DORA. La creciente complejidad de los riesgos tecnológicos, la dependencia de terceros y la necesidad de garantizar la continuidad de los servicios críticos o esenciales exigen un perfil profesional con competencias multidisciplinares, visión transversal y capacidad de liderazgo en entornos de alta exigencia.

Esta visión estratégica le permitirá comprender a la organización en su conjunto y de este modo identificar las interdependencias de los procesos, las personas, la tecnología y los proveedores. Con esta visión y conociendo los procesos de negocio en profundidad será capaz de definir posibles escenarios de disrupción atendiendo a las amenazas tecnológicas que tenga su organización. De esta forma, con esa visión transversal será capaz de alinear los objetivos de resiliencia que deben ir de la mano con los objetivos de negocio o de estrategia.

6.2. Formación y capacitación

La capacitación del CRO debe considerarse como un proceso continuo, estratégico y transversal. Un CRO adecuadamente formado fortalece la resiliencia corporativa, asegura el cumplimiento regulatorio, incrementa la preparación organizativa y mejora la capacidad de respuesta ante un entorno incierto y cambiante.

Los **objetivos** que debe perseguir esta formación o capacitación, entre otros, son los siguientes:

- Desarrollar una visión holística de todos los riesgos corporativos que afectan a los servicios críticos y/o esenciales, integrando continuidad, ciberseguridad, riesgo tecnológico, riesgo de terceros y riesgo operacional.
- Ejercer una supervisión activa de la resiliencia operativa, en línea con los requerimientos de las normativas aplicables a la Alta Dirección.
- Coordinar eficazmente los equipos multidisciplinares, incluyendo TI, Seguridad de la Información, Riesgos, Cumplimiento, Capital Humano y áreas de negocio.
- Tomar decisiones estratégicas durante crisis, basadas en marcos de gobierno, análisis situacional y capacidad para priorizar de manera ágil.
- Impulsar una cultura corporativa resiliente, orientada a la anticipación, la prevención y la respuesta eficaz.

La formación deberá abordarse desde estas tres **perspectivas:**

Competencias técnicas:

- Continuidad de negocio y gestión de crisis: comprensión profunda del Sistema de Gestión de Continuidad de Negocio (SGCN), procedimientos, pruebas, reporte y escalado.
- Resiliencia operativa digital: identificación de activos críticos, dependencias tecnológicas, pruebas técnicas, evaluación de ciberincidentes y mecanismos de respuesta.
- Gestión del riesgo tecnológico, operacional y de terceros: gobernanza TI, metodologías de evaluación de riesgos, matrices multidimensionales y criterios de criticidad.
- Gobierno y cumplimiento normativo: alineamiento con requisitos regulatorios (normativa sectorial, modelos de prevención, políticas de seguridad, etc.).

Competencias estratégicas:

- Toma de decisiones en situaciones de alta presión y sin contar con la información necesaria.
- Modelos de gobernanza y liderazgo transversal.
- Evaluación de impactos y priorización de servicios esenciales.
- Visión integral del negocio, ecosistema corporativo y de terceros.

Competencias personales:

- Comunicación clara y efectiva con Alta Dirección, equipos técnicos y grupos de interés.
- Capacidades de facilitación en crisis y gestión de stakeholders.
- Mentalidad de aprendizaje continuo y enfoque proactivo.

La capacitación del CRO deberá estructurarse en un **plan** anual, robusto, medible y conectado a las necesidades reales de la organización. Este plan deberá estar basado en buenas prácticas extraídas de los programas formativos de continuidad, seguridad, riesgo penal, ciberseguridad y cultura corporativa, entre otros.

El plan de formación del CRO ***debe incluir:***

1. Formación inicial.
2. Formación continua obligatoria.
3. Formación para especialización del CRO.
4. Formación de todos los grupos que operan desarrollando la resiliencia en la organización (equipos de crisis, miembros principales y alternativos, equipos de evaluación y respuesta, personal TIC, especialmente en reporte, pruebas técnicas y escalado, Alta Dirección, áreas de Seguridad, Cumplimiento y Personas).

Estos programas pueden ser: píldoras formativas, vídeos corporativos de alcance masivo, sesiones presenciales y virtuales, simulaciones y talleres prácticos.

Los programas de formación deberán evolucionar en las siguientes materias:

- Mayor integración entre resiliencia, ciberseguridad avanzada e Inteligencia Artificial (IA).
- Métricas más rigurosas de madurez operativa.
- Programas sectoriales compartidos entre entidades.
- Escenarios de crisis híbridas (ciber + operativa + reputacional).
- Competencias de gestión del riesgo de terceros.

El plan de formación y capacitación del CRO deberá ser ***medible*** para identificar fortalezas y puntos de mejora a incorporar en futuros planes. Para ello deberán elaborarse indicadores que permitan medir:

- Progreso individual del CRO y sus equipos.
- Cobertura formativa en los programas corporativos.
- Resultados de simulacros y pruebas técnicas.
- Indicadores de mejora continua (lecciones aprendidas).
- Madurez de cultura organizacional de resiliencia.

6.3. Soft Skills

Las habilidades no técnicas del Chief Resilience Officer: El factor humano de la resiliencia organizativa

La resiliencia organizativa no depende únicamente de planes, tecnologías o estructuras formales. En situaciones de crisis reales, caracterizadas por alta incertidumbre, presión temporal y escasez de información, la capacidad de una organización para absorber, adaptarse y recuperarse se manifiesta principalmente a través de las personas que toman decisiones y coordinan la respuesta.

En este apartado se analizan las ***habilidades no técnicas (soft skills)*** asociadas a la figura del CRO, entendidas como competencias prácticas, observables y entrenables, que resultan críticas para garantizar una gestión eficaz de crisis y disrupciones. Estas habilidades constituyen un factor determinante para transformar los marcos de resiliencia definidos en los planes en comportamientos efectivos durante eventos reales.

1. Contexto y marco de referencia

La norma **ISO 22316** define la resiliencia organizativa como la capacidad de una organización para ***anticipar, prepararse, responder y adaptarse*** a cambios y disrupciones, con el objetivo de sobrevivir y prosperar. Si bien este enfoque incorpora procesos, sistemas y gobernanza, su aplicación práctica depende en gran medida de la actuación humana bajo condiciones adversas.

En escenarios de crisis, los procedimientos establecidos rara vez cubren todas las variables. La toma de decisiones se produce con información incompleta y bajo presión, lo que **exige competencias que van más allá del conocimiento técnico**. En este contexto, el CRO actúa como figura integradora, responsable de estabilizar la organización y facilitar una respuesta coordinada.

2. Templanza y liderazgo bajo presión

Una de las competencias más críticas del CRO es la ***capacidad de mantener la calma y ejercer liderazgo bajo presión.*** La templanza permite reducir el ruido organizativo, evitar reacciones impulsivas y sostener un entorno de trabajo funcional en situaciones de estrés elevado.

El liderazgo efectivo en crisis no se basa en la imposición jerárquica, sino en una **autoridad funcional,** sustentada en la coherencia, la claridad y la consistencia en la toma de decisiones. Esta capacidad resulta esencial para evitar bloqueos decisionales derivados de la incertidumbre y para mantener el foco en los objetivos de recuperación.

La experiencia demuestra que esta competencia puede desarrollarse mediante entrenamientos específicos, como simulaciones y ejercicios de crisis, que permiten exponer a los equipos directivos a escenarios realistas y mejorar su capacidad de respuesta.

> "Una de las mejores lecciones que puedes aprender en la vida es mantener la calma. La calma es un superpoder".
>
> **Bruce Lee.**

3. Comunicación estratégica en situaciones de crisis

La comunicación constituye un elemento estructural de la gestión de crisis. En este ámbito, el CRO desempeña un papel clave como ***facilitador y coordinador de la comunicación estratégica,*** tanto interna como externa.

En contextos de disrupción, comunicar eficazmente implica:

- Reducir la incertidumbre mediante información clara y estructurada.
- Diferenciar hechos confirmados, hipótesis y líneas de investigación.
- Mantener coherencia en los mensajes a lo largo del tiempo.
- Evitar tanto el alarmismo como la generación de falsas certezas.

Aunque el CRO no siempre asuma el rol de portavoz, suele actuar como ***referente en la gestión de la narrativa***, asegurando que los mensajes contribuyan a la estabilidad organizativa, la alineación interna y la protección de la reputación corporativa.

4. Pensamiento sistémico y visión integral

El pensamiento sistémico es otra competencia esencial del CRO.

A diferencia de otros roles centrados en dominios específicos (tecnología, seguridad, operaciones, riesgos), el CRO debe ser capaz de ***ver la organización como un sistema vivo,*** compuesto por elementos interdependientes. Las disrupciones rara vez afectan a un único dominio; un incidente técnico puede escalar rápidamente hacia impactos operativos, regulatorios, financieros, reputacionales y humanos.

El CRO debe ser capaz de:

- Comprender la organización como un sistema interdependiente.
- Anticipar efectos en cascada y dependencias críticas.
- Ampliar el análisis más allá del incidente inicial.
- Identificar actores relevantes que deben incorporarse a la gestión de la crisis.

Esta visión integral permite evitar decisiones parciales que, aun resolviendo un problema local, generen impactos negativos a nivel global.

5. Gestión del ego y liderazgo adaptativo

La ISO 22316 subraya la importancia de un liderazgo y una gobernanza eficaces. En situaciones de crisis, los modelos de liderazgo tradicionales basados en jerarquías rígidas pierden eficacia. El CRO debe ejercer un ***liderazgo adaptativo***, ajustando su rol en función del contexto y del conocimiento disponible.

La **gestión del ego** es una competencia clave en este entorno. El CRO eficaz sabe cuándo liderar, cuándo delegar y cuándo ceder protagonismo a expertos técnicos. Esta actitud reduce conflictos internos, favorece la colaboración y refuerza la eficacia colectiva.

La humildad profesional y la orientación a objetivos comunes resultan determinantes para mantener equipos cohesionados y evitar dinámicas de competencia improductiva.

6. Gestión de personas e inteligencia emocional aplicada

La resiliencia organizativa está estrechamente vinculada al factor humano. En crisis prolongadas, el estrés continuado incrementa el riesgo de fatiga, errores humanos y deterioro del rendimiento.

El CRO debe aplicar una **inteligencia emocional orientada a la operación**, que incluya:

- Detección temprana de agotamiento.
- Gestión adecuada de turnos y descansos.
- Ajuste de ritmos y expectativas.
- Prevención del burnout en equipos críticos, dominando el arte de mantener a largo plazo la motivación y obtener lo mejor de las personas individuales y de los equipos.
- En ocasiones, el CRO deberá romper el hielo y ser transmisor de la importancia de mantener el sentido del humor, el ánimo y el optimismo realista de que “de esta vamos a salir”, relativizando la gravedad de las situaciones.

Cuidar a las personas no constituye únicamente una responsabilidad ética, sino una **medida directa de protección de la capacidad operativa y de la continuidad del negocio.** En este ámbito, emerge la figura complementaria del ***Chief Care Officer (CCaO)***, centrada en la resiliencia de los equipos de respuesta y continuidad claves.

7. Aprendizaje organizativo y mejora continua

La capacidad adaptativa, elemento central de la ISO 22316, se materializa cuando la organización aprende de la crisis. Aquí emerge otra soft skill esencial del CRO: **facilitar el aprendizaje sin culpabilización.**

Las revisiones post-incidentes solo generan resiliencia si se realizan en un entorno de seguridad psicológica. El CRO debe fomentar conversaciones honestas, centradas en sistemas y decisiones, no en personas. Esta es una responsabilidad clave del rol.

Como recurso útil para el desarrollo efectivo de esta habilidad, pueden encontrarse referencias en la literatura como la Guía Scrum, con fuerte foco en el aprendizaje derivado de las retrospectivas.

8. Conclusiones: el CRO como arquitecto de comportamientos

La resiliencia organizativa no se materializa únicamente a través de planes, tecnologías o estructuras formales, sino mediante comportamientos efectivos bajo presión. En este sentido, el Chief Resilience Officer actúa como un ***facilitador de decisiones, integrador de capacidades y estabilizador organizativo*** en contextos de alta incertidumbre.

Las habilidades no técnicas no deben considerarse un complemento del rol del CRO, sino su principal activo estratégico, ya que permiten transformar los marcos de resiliencia definidos sobre el papel en respuestas eficaces ante crisis reales.

6.4. Capacitación y habilidades directivas

La función del CRO requiere una capacitación que combine conocimiento normativo, experiencia práctica y habilidades directivas avanzadas.

Desde el punto de vista de la formación especializada, el CRO debe contar con una base sólida en estándares internacionales de gestión. Resulta especialmente relevante el dominio de normas ISO vinculadas a resiliencia y continuidad, como ISO 22301 (Sistemas de Gestión de la Continuidad de Negocio), ISO 22316 (Resiliencia Organizacional), ISO 22398 (Ejercicios y pruebas), así como su integración con ISO 31000 (Gestión del Riesgo) e ISO/IEC 27001 (Seguridad de la Información). Esta capacitación permite al CRO comprender la resiliencia como un sistema integrado, evitando enfoques fragmentados y facilitando la alineación con otros sistemas de gestión corporativos.

Las certificaciones profesionales refuerzan esta base y aportan reconocimiento y lenguaje común con el entorno regulado. En este sentido, se citan varias certificaciones de referencia que pueden contribuir a la adquisición de las capacidades requeridas para este rol: (Organización emisora / Certificación)

- ***ISMS:*** **CCSP (Certified Cyber Security Professional)** o **CPCC (Certified Professional Cyber Compliance)**. La formación y certificaciones promovidas por ISMS Forum y sus programas asociados en continuidad, resiliencia, ENS, NIS2 o DORA aportan un enfoque práctico y contextualizado al marco regulatorio europeo y nacional, reforzando la capacidad del CRO para operar en sectores críticos y altamente supervisados.
- ***ISACA:*** **CISM (Certified Information Security Manager), CRISC (Certified in Risk and Information Systems Control) o CGEIT (Certified in the Governance of Enterprise IT),** especialmente valiosas para el CRO, al fortalecer competencias en gobierno, gestión del riesgo, control y alineación con objetivos de negocio. Estas certificaciones facilitan además el diálogo con Consejos de Administración y comités de riesgos.

- ***BCI*: CBCI (Certificate of the Business Continuity Institute)**
- ***ISO 22301 Lead Implementer/Auditor***
- ***ISC2*: CISSP (Certified Information Systems Security Professional)**
- ***DRI*: CBCP (Certified Business Continuity Professional)**

No obstante, la capacitación técnica debe complementarse con habilidades directivas clave, como las explicadas en la sección anterior.

Finalmente, la orientación a la mejora continua y al aprendizaje organizacional constituye una competencia esencial. El CRO debe promover la revisión sistemática de incidentes, auditorías, ejercicios y simulaciones, integrando las lecciones aprendidas en la estrategia, los procesos y la cultura corporativa. Esta combinación de certificaciones reconocidas, dominio normativo y habilidades directivas convierte al CRO en un actor clave para la sostenibilidad, estabilidad y confianza de la organización.

CONCLUSIONES

7

La resiliencia organizacional ha dejado de ser un conjunto de prácticas aisladas, tradicionalmente asociadas a la continuidad de negocio o a la recuperación tecnológica, para consolidarse como una ***capacidad estratégica transversal*** que condiciona la sostenibilidad, la relevancia y la confianza en las organizaciones modernas. El contexto actual, marcado por la complejidad operativa, la dependencia tecnológica, la interconexión de cadenas de suministro y un marco regulatorio cada vez más exigente, exige una aproximación integral que combine cultura, gobernanza, procesos, personas y tecnología.

A lo largo de este documento se ha puesto de manifiesto que ***la resiliencia no consiste únicamente en resistir o recuperarse***, sino en ***anticipar, adaptarse y aprender***, transformando las disrupciones en una oportunidad de mejora continua. Este enfoque supera la visión reactiva de la contingencia y sitúa la protección de los servicios críticos o esenciales como un elemento central de la estrategia corporativa, alineado con los objetivos de negocio y el apetito de riesgo definido por la Alta Dirección.

Los marcos normativos europeos (por ejemplo, DORA, NIS2, CER, ENS y otros) refuerzan esta visión al exigir una implicación directa de los órganos de gobierno y una responsabilidad clara sobre la resiliencia operativa y organizacional. Sin embargo, más allá del cumplimiento, estos marcos deben entenderse como ***palancas para ordenar la gobernanza, clarificar responsabilidades y fortalecer la confianza de clientes***, reguladores y demás partes interesadas.

La creación y consolidación de la ***función de resiliencia***, independientemente de su modelo organizativo, emerge como un factor clave para integrar disciplinas tradicionalmente fragmentadas: continuidad de negocio, gestión de crisis, ciberseguridad, gestión de riesgos y dependencia de terceros. En este contexto, la figura del ***Chief Resilience Officer (CRO)*** se configura como un rol de carácter directivo, con autoridad transversal, visión sistémica y capacidad real de influir en la toma de decisiones estratégicas, tanto en situaciones de estabilidad como en escenarios de crisis.

Asimismo, el documento destaca que la efectividad de la resiliencia no depende exclusivamente de estructuras formales o planes documentados, sino del ***comportamiento organizativo bajo presión***. La cultura, la formación, la concienciación y las habilidades no técnicas, como el liderazgo, la comunicación, el pensamiento sistémico y la gestión del factor humano resultan determinantes para convertir los marcos de resiliencia definidos sobre el papel en respuestas eficaces frente a eventos reales.

En definitiva, ***invertir en resiliencia es invertir en continuidad, confianza y ventaja competitiva.*** Las organizaciones verdaderamente resilientes no son aquellas que evitan las disrupciones, sino las que están preparadas para gestionarlas con criterio, transparencia y coherencia, manteniendo la prestación de sus servicios esenciales y reforzando su legitimidad ante un entorno cada vez más exigente. La resiliencia, entendida de forma integral, se consolida como un activo estratégico y un elemento diferenciador clave para la sostenibilidad a largo plazo.

GLOSARIO DE TÉRMINOS

8

Alta Dirección

Órgano ejecutivo responsable de la definición de la estrategia, la asignación de recursos y la supervisión del desempeño global de la organización, incluyendo la resiliencia y la continuidad de los servicios esenciales.

Apetito de Riesgo

Nivel y tipo de riesgo que una organización está dispuesta a asumir para alcanzar sus objetivos estratégicos.

BAU (Business As Usual)

Situación de funcionamiento normal de la organización, sin incidentes o crisis activas.

BCI (Business Continuity Institute)

Organización internacional de referencia en continuidad de negocio y resiliencia, que establece buenas prácticas, marcos profesionales y certificaciones.

BIA (Business Impact Analysis)

Análisis de Impacto en el Negocio. Proceso sistemático para identificar procesos, servicios, recursos y dependencias críticas, así como los impactos derivados de su interrupción.

Cadena de suministro

Conjunto de proveedores, terceros y servicios externalizados de los que depende la organización para la prestación de sus servicios críticos o esenciales.

CER (Critical Entities Resilience Directive – Directiva (UE) 2022/2557)

Directiva europea sobre resiliencia de entidades críticas, orientada a garantizar la continuidad de los servicios esenciales frente a amenazas físicas, organizativas y operativas.

CIO (Chief Information Officer)

Responsable ejecutivo de la gestión y evolución de la tecnología de la información, asegurando que soporta adecuadamente las necesidades del negocio.

CISO (Chief Information Security Officer)

Responsable ejecutivo de la seguridad de la información y de la ciberseguridad de la organización.

Comité de Crisis

Órgano de decisión activado ante incidentes graves, encargado de la gestión estratégica de la crisis, la toma de decisiones críticas y la coordinación de la respuesta.

Continuidad de Negocio (BCM – Business Continuity Management)

Disciplina orientada a garantizar que la organización puede mantener o recuperar sus procesos críticos dentro de tiempos aceptables tras una disrupción.

Crisis

Situación excepcional que compromete de forma significativa la prestación de servicios esenciales, la seguridad de las personas, la reputación o la viabilidad de la organización.

CRO (Chief Resilience Officer)

Responsable de integrar, coordinar y supervisar la resiliencia organizacional, operativa y digital, unificando continuidad, gestión de crisis, riesgos y dependencias críticas.

DORA (Digital Operational Resilience Act – Reglamento (UE) 2022/2554)

Reglamento europeo que establece requisitos obligatorios de resiliencia operativa digital para entidades financieras y proveedores TIC críticos.

DRP (Disaster Recovery Plan)

Plan de Recuperación ante Desastres. Conjunto de procedimientos técnicos para restaurar sistemas y servicios tecnológicos tras un incidente grave.

ENS (Esquema Nacional de Seguridad)

Marco normativo español que establece principios y requisitos de seguridad y resiliencia para sistemas de información del sector público y sus proveedores.

ERM (Enterprise Risk Management)

Gestión Integral de Riesgos Empresariales. Enfoque estructurado para identificar, evaluar y gestionar los riesgos que afectan a la organización.

GDPR (General Data Protection Regulation – Reglamento (UE) 2016/679)

Reglamento europeo de protección de datos personales que establece las obligaciones para el tratamiento seguro y lícito de la información, garantizando los derechos de las personas físicas y exigiendo a las organizaciones la adopción de medidas técnicas y organizativas adecuadas para proteger la confidencialidad, integridad y disponibilidad de los datos.

Gobernanza

Conjunto de estructuras, responsabilidades, procesos y mecanismos de supervisión mediante los cuales se dirige y controla la organización.

IA (Inteligencia Artificial)

Tecnologías que permiten a sistemas informáticos realizar tareas que requieren capacidades cognitivas humanas, con impacto creciente en la resiliencia y gestión de riesgos.

ISO (International Organization for Standardization)

Organización internacional que desarrolla normas técnicas y de gestión ampliamente reconocidas.

KPI (Key Performance Indicator)

Indicador clave de desempeño utilizado para medir la eficacia de procesos o funciones.

KRI (Key Risk Indicator)

Indicador clave de riesgo empleado para anticipar desviaciones respecto al apetito de riesgo definido.

OT (Operational Technology)

Tecnologías utilizadas para controlar y supervisar procesos físicos y operativos, especialmente en entornos industriales.

Resiliencia Organizacional

Capacidad de una organización para anticipar, resistir, adaptarse y recuperarse de disrupciones, manteniendo la prestación de servicios críticos o esenciales.

Resiliencia Operativa

Capacidad de mantener operaciones y servicios esenciales dentro de niveles de impacto aceptables durante y después de una disrupción.

RSI (Responsable de Seguridad de la Información)

Figura establecida en el Esquema Nacional de Seguridad (ENS), responsable de garantizar la seguridad de la información y de los sistemas que la soportan, así como de coordinar el cumplimiento de los requisitos normativos en materia de seguridad y actuar como punto de interacción con los organismos competentes.

RSR (Responsable de Seguridad y Resiliencia)

Figura prevista en el marco de la Directiva CER, responsable de la protección y resiliencia de los servicios esenciales, incluyendo la gestión de riesgos físicos, operativos y organizativos, así como la coordinación de las medidas necesarias para garantizar la continuidad y recuperación ante disrupciones.

Resiliencia Operativa Digital

Capacidad de resistir y recuperarse de incidentes relacionados con las tecnologías de la información y las comunicaciones.

RPO (Recovery Point Objective)

Objetivo de Punto de Recuperación. Define la cantidad máxima de datos que la organización puede permitirse perder.

RTO (Recovery Time Objective)

Objetivo de Tiempo de Recuperación. Tiempo máximo aceptable para restablecer un servicio o proceso tras una interrupción.

RSR (Responsable de Seguridad y Resiliencia)

Figura prevista en el marco CER, responsable de la protección del servicio esencial y de la resiliencia frente a amenazas físicas y organizativas.

Servicios Críticos / Servicios Esenciales

Procesos, funciones o servicios cuya interrupción tendría un impacto significativo en la continuidad del negocio, el cumplimiento normativo, la estabilidad operativa o la sostenibilidad de la organización. (A efectos del documento, ambos términos se utilizan como equivalentes).

SIG (Sistema Integrado de Gestión)

Conjunto integrado de sistemas de gestión (riesgos, continuidad, seguridad, cumplimiento, etc.) bajo un marco común de gobernanza y mejora continua.

Terceros Críticos

Proveedores o entidades externas cuya indisponibilidad o fallo puede comprometer la prestación de servicios esenciales.

TI / TIC (Tecnologías de la Información / Tecnologías de la Información y las Comunicaciones)

Conjunto de sistemas, infraestructuras y servicios tecnológicos que soportan los procesos de negocio.

TLPT (Threat-Led Penetration Testing)

Pruebas de penetración avanzadas basadas en amenazas reales, exigidas por DORA para evaluar la resiliencia operativa digital.

Modelo de las 3 Líneas (3LoD)

Modelo de gobernanza que distingue entre funciones operativas (primera línea), funciones de supervisión y control (segunda línea) y aseguramiento independiente (tercera línea).

REFERENCIAS

9

- Agencia Estatal Boletín Oficial del Estado. (2018). Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. ***https://www.boe.es/buscar/act.php?id=BOE-A-2018-12257***
- Agencia Estatal Boletín Oficial del Estado. (2024). Real Decreto 207/2024, de 27 de febrero. ***https://www.boe.es/buscar/doc.php?id=BOE-A-2024-3793***
- Business Continuity Institute. (2019). Good Practice Guidelines (6th ed.). ***https://www.thebci.org***
- ENISA. (2023). NIS2 Directive: Technical guidance and implementation considerations. ***https://www.enisa.europa.eu***
- European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2). ***https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81965***
- European Parliament & Council of the European Union. (2022). Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities (CER). ***https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81965***
- European Parliament & Council of the European Union. (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). ***https://eur-lex.europa.eu***
- INCIBE-CERT. (2017). El ransomware WannaCry, responsable del ciberataque mundial. ***https://www.incibe.es/incibe-cert/blog/ransomware-wannacry-responsable-ciberataque-mundial***
- International Organization for Standardization. (2018). ISO 31000:2018 Risk management—Guidelines. ***https://www.iso.org/standard/65694.html***
- International Organization for Standardization. (2019). ISO 22301:2019 Security and resilience—Business continuity management systems—Requirements. ***https://www.iso.org/standard/75106.html***
- International Organization for Standardization. (2021). ISO 22316:2021 Security and resilience—Organizational resilience—Principles and attributes. ***https://www.iso.org/standard/50053.html***
- International Organization for Standardization. (2018). ISO 22398:2018 Security and resilience—Exercises and testing. ***https://www.iso.org/standard/50295.html***
- International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements. ***https://www.iso.org/standard/27001***
- Ministerio del Interior. (2024). El Gobierno aprueba una ley de protección y resiliencia de las entidades públicas y privadas que operan en los sectores estratégicos. ***https://www.interior.gob.es/opencms/es/detalle/articulo/El-Gobierno-aprueba-una-ley-de-proteccion-y-resiliencia-de-las-entidades-publicas-y-privadas-que-operan-en-los-sectores-estrategicos/***
- Oficina de Coordinación de Ciberseguridad (OCC). (s. f.). Portal público de la Oficina de Coordinación de Ciberseguridad. ***https://occ.ses.mir.es/publico/occ***

Junio 2026

CHIEF RESILIENCE OFFICER

Libro Blanco

Una iniciativa de:

CRC
CYBER RESILIENCE CENTRE

isms forum