cyber zaintza
BASQUE CYBERSECURITY AGENCY

# Guía de apoyo para la elaboración de un Plan de Continuidad en materia de Ciberseguridad

Noviembre 2025

EUSKO JAURLARITZA
GOBIERNO VASCO

# Índice

# 1 Control del documento

CONTROL DE FIRMAS

| | Nombre y Apellidos/ Cargo | Fecha | Firma |
|---|---|---|---|
| Elaborado por: | | | |
| Aprobado por: | | | |

CONTROL DE VERSIONES

| Versión | Fecha aprobación | Control de cambios |
|---|---|---|
| 1.0 | Noviembre 2025 | 1ª versión del documento |
| | | |
| | | |

# 2 Introducción

En una sociedad tan interconectada, cada vez es más habitual la dependencia sobre las nuevas tecnologías y los sistemas de información. Esta dependencia, a su vez, expone a un mayor crecimiento de las ciberamenazas, que pueden variar desde incidentes menores hasta ataques sofisticados que comprometen la disponibilidad, integridad y confidencialidad de la información.

Frente a este panorama, contar con un Plan de Continuidad en materia de Ciberseguridad se torna esencial como una estrategia integral para garantizar la resiliencia operativa y reducir el impacto sobre posibles incidentes que afecten a los servicios esenciales y, consecuentemente, a la sociedad y población de Euskadi.

Los poderes públicos están comprometidos con la protección de la vida y la seguridad, no solo reaccionando ante emergencias, sino anticipándose a ellas. Además, es clave que la ciudadanía conozca los riesgos de la ciberseguridad y entienda que la seguridad es un derecho y una responsabilidad compartida.

La normativa y regulación relativa a la gestión de Emergencias y Protección Civil obliga a ciertos sectores a tener planes de autoprotección, especialmente si las actividades que las entidades prestan pueden causar o verse afectadas por emergencias, por lo que resulta imprescindible que dispongan de planes que permitan proteger la vida y la seguridad de las personas.

Es por ello, que la implementación de un Plan de Continuidad de Ciberseguridad sólido refleja el compromiso proactivo de las entidades frente a la seguridad y la gestión de riesgos, permitiendo reaccionar de manera rápida y coordinada ante eventuales ataques, interrupciones o fallos tecnológicos. Además, promueve la identificación y priorización de activos críticos, la asignación clara de responsabilidades y la preparación efectiva de los equipos involucrados.

En el territorio de la CAPV, el Gobierno Vasco ha desarrollado y aprobado una Orden por la que se regula la necesidad de elaborar planes de continuidad en materia de ciberseguridad para ciertas actividades sujetas a la norma vasca de autoprotección.

Esta guía está diseñada para facilitar a cualquier entidad la elaboración, implementación y mantenimiento de su Plan de Continuidad en materia de Ciberseguridad de forma clara, sencilla y efectiva, y cuyo contenido esencial deberá incluir los siguientes aspectos:

- Planificación y control operacional.
- Análisis de impacto y evaluación de riesgos.
- Estrategias de continuidad de negocio.
- Procedimientos de emergencias.
- Simulacros y ejercicios.

# 3 Normativa de referencia

La normativa de referencia aplicable se detalla a continuación:

- Orden de 7 de junio de 2024, del Vicelehendakari Primero y Consejero de Seguridad, por la que se regula la elaboración de planes de continuidad en materia de ciberseguridad para ciertas actividades sujetas a la norma vasca de autoprotección.
- Decreto Legislativo 1/2017, de 27 de abril, por el que se aprueba el texto refundido de la Ley de Gestión de Emergencias.
- Decreto 277/2010, de 2 de noviembre, por el que se regulan las obligaciones de autoprotección exigibles a determinadas actividades, centros o establecimientos para hacer frente a situaciones de emergencia.
- Decreto 21/2019, de 12 de febrero, de segunda modificación del Decreto por el que se regulan las obligaciones de autoprotección exigibles a determinadas actividades, centros o establecimientos para hacer frente a situaciones de emergencia.
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

# 4 Objetivo

La guía tiene como objetivo establecer un marco de referencia integral que facilite a las entidades la identificación, estructuración y aplicación de las directrices y los criterios mínimos necesarios para la elaboración, implementación y mantenimiento efectivo de sus Planes de Continuidad en materia de ciberseguridad, garantizando de este modo la resiliencia operativa ante incidentes de ciberseguridad y el cumplimiento de la normativa vigente.

# 5 Alcance

Esta guía está dirigida a todas aquellas entidades que prestan actividades comprendidas en el ámbito de aplicación de las siguientes normas:

- Decreto 277/2010, de 2 de noviembre, por el que se regulan las obligaciones de autoprotección exigibles a determinadas actividades, centros o establecimientos para hacer frente a situaciones de emergencia.
- Orden de 7 de junio de 2024, del Vicelehendakari Primero y Consejero de Seguridad, por la que se regula la elaboración de planes de continuidad en materia de ciberseguridad para ciertas actividades sujetas a la norma vasca de autoprotección.

# 6 Contenido del Plan

De acuerdo con lo establecido en la Orden de 7 de junio de 2024, el contenido mínimo de un Plan de Continuidad de ciberseguridad, recogido en su Anexo II, es el siguiente:

1. Una planificación y un control operacional: se debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos propios de la actividad e implementar las acciones destinadas a abordar los riesgos y oportunidades.

2. Un análisis de impacto del negocio y evaluación de los riesgos: se debe implementar y mantener un proceso para analizar el impacto comercial y evaluar los riesgos de interrupción que establezca el contexto, defina criterios y evalúe el impacto potencial de una interrupción.

3. Estrategias y soluciones de continuidad del negocio: se debe identificar y seleccionar estrategias de continuidad del negocio basadas en los resultados del análisis de impacto del negocio y la evaluación de riesgos. Las estrategias de continuidad del negocio podrán estar compuestas por una o más soluciones.

4. Planes y procedimientos de continuidad del negocio: se debe implementar y mantener una estructura que permita la advertencia y la comunicación oportunas a las partes interesadas relevantes, y proporcionar planes y procedimientos para administrar la entidad durante una interrupción. Los planes y procedimientos se utilizarán cuando sea necesario para ejecutar soluciones de continuidad del negocio.

5. Programa de ejercicios: se debe implementar y mantener un programa de ejercicios y pruebas para validar con el tiempo la efectividad de las estrategias y soluciones de continuidad del negocio.

A continuación, se incluye la estructura e información detallada que debe contener el Plan de Continuidad en materia de ciberseguridad según lo requerido por la normativa:

## 6.1 Planificación y control operacional

Esta primera fase, la entidad debe identificar todas las actividades y procesos de negocio cuya operativa es necesaria para el mantenimiento de sus funciones, siempre dentro del ámbito de aplicación de la norma vasca de autoprotección (Decreto 277/2010). Una vez realizadas estas identificaciones, la organización deberá determinar los procesos o subprocesos sobre los cuales se desarrollará el Plan de Continuidad, asegurando así una respuesta eficaz ante posibles interrupciones.

## 6.2 Análisis de Impacto al Negocio y Evaluación de Riesgos

Identificado el mapa de procesos y actividades, la entidad deberá elaborar un análisis de impacto al negocio o BIA (por sus siglas en inglés, *Business Impact Analysis*) por cada actividad o proceso que contenga, al menos, la siguiente información:

- Inventario de activos necesarios para la operación de cada una de las actividades / procesos de negocio identificados:
  - Relación de los sistemas de información, aplicaciones y plataformas necesarias que soportan el proceso o actividad de negocio.

- Datos e información necesaria que se requiere recopilar, procesar y almacenar para llevar a cabo las actividades, incluyendo tanto datos internos como externos.
- Proveedores externos o terceros que suministran productos o servicios necesarios para la operación.
- Personal interno, es decir, recursos humanos que participan en la realización de la actividad o proceso de negocio.
- Establecimiento/s donde se presta la operación.
- Otras ubicaciones necesarias para la operación, como oficinas, plantas, CPDs, etc.
- Otro equipamiento TIC, es decir, equipos tecnológicos necesarios que no entran directamente en la categoría de sistemas de información, pero que son vitales para la operación como, por ejemplo, servidores, routers, switches, dispositivos móviles, dispositivos IoT, …

- Determinación de los tiempos críticos ante una posible interrupción. En concreto, se deberá identificar:
  - Tiempo Objetivo de Recuperación (RTO, por sus siglas en inglés) que es el plazo máximo tolerable que una entidad puede permitirse para restaurar un proceso, sistema o servicio tras una interrupción antes de que el impacto en el negocio sea inaceptable.

    En otras palabras, es el tiempo que debe transcurrir desde la ocurrencia de un incidente hasta la recuperación total o parcial del servicio.
  - Punto Objetivo de Recuperación (RPO, por sus siglas en inglés) que determina la cantidad máxima de datos que una entidad está dispuesta a perder, expresada en tiempo, en caso de una interrupción o desastre. Representa el punto en el tiempo hasta el cual los datos deben recuperarse para que la entidad continúe operando sin afectar significativamente sus actividades.
  - Tiempo Máximo Tolerable de Interrupción (MTPD, por sus siglas en inglés) que es el período máximo durante el cual un proceso puede permanecer interrumpido sin ocasionar daños irreparables a la entidad.

    Se diferencia del RTO en que el MTPD considera el tiempo total durante el cual la interrupción puede ser soportada, incluyendo no solo la recuperación técnica, sino también el período de impacto en el negocio y la capacidad de respuesta global.
  - Identificación de las principales amenazas y vulnerabilidades de ciberseguridad que pueden afectar a los procesos críticos identificados y puedan comprometer la confidencialidad, integridad y disponibilidad de los procesos de negocio críticos.

    A través de esta identificación, la entidad podrá tomar medidas preventivas y mitigadoras adecuadas para proteger los activos esenciales de la entidad.

## 6.3 Estrategias y soluciones de continuidad de negocio

Realizado el análisis de impacto y análisis de riesgos de cada una de las diferentes actividades y procesos de negocio, la entidad deberá identificar y definir las estrategias y soluciones de continuidad necesarias para garantizar que los procesos que se hayan determinado como críticos en función a los tiempos de respuesta puedan continuar operando o recuperarse de manera efectiva ante cualquier eventualidad que interrumpa su funcionamiento normal.

Estas estrategias y soluciones deben estar alineadas con los tiempos de recuperación establecidos en el análisis. Para ello, la entidad deberá evaluar y seleccionar un conjunto de medidas que pueden incluir acciones preventivas, contingencias de operación y protocolos de recuperación, que aseguren la disponibilidad y resiliencia de las actividades críticas.

La identificación de estas soluciones implica considerar aspectos claves como la infraestructura técnica requerida, el soporte humano, la redundancia de sistemas, los acuerdos con proveedores externos, y los métodos alternativos de operación ante fallos. También es importante que estas estrategias permitan una rápida adaptación ante diferentes escenarios de riesgo y sean económicamente viables, con el fin de optimizar los recursos y minimizar el impacto en el negocio.

En definitiva, mediante esta fase la entidad establece un marco integral de continuidad operacional que no solo protege sus activos y procesos esenciales, sino que también fortalece su capacidad para responder, adaptarse y recuperarse frente a incidentes, manteniendo así la confianza de sus clientes, socios y demás partes interesadas.

## 6.4 Planes y procedimientos de continuidad de negocio

Una vez que la entidad haya seleccionado o determinado las soluciones o estrategias para cada uno de los diferentes procesos, deberá diseñar y elaborar planes operativos y procedimientos de recuperación específicos que den respuesta a las estrategias seleccionadas.

Estos planes constituyen el conjunto detallado de instrucciones, protocolos y acciones que guiarán a los equipos responsables durante la activación de la respuesta ante incidentes o interrupciones, garantizando que se lleven a cabo las actividades operativas necesarias para restablecer la continuidad del negocio en los tiempos estipulados.

Estos planes deberán definir de manera clara y precisa cuáles son los pasos a seguir, quiénes son los responsables de cada tarea y qué recursos se requieren para ejecutar cada actividad. Asimismo, deben contemplar las condiciones bajo las cuales se deben activar, los mecanismos de comunicación interna y externa, así como los criterios para evaluar la efectividad de la recuperación.

## 6.5 Programa de ejercicios

Elaborados los planes operativos y procedimientos de recuperación específicos, la entidad deberá verificar y asegurarse de que dichos planes y procedimientos de continuidad de negocio son eficaces mediante la implementación de un programa de ejercicios y pruebas.

Para garantizar el programa de ejercicios, la entidad deberá:

- Determinar los objetivos y alcance de las pruebas, es decir, conocer qué es lo que se quiere probar y el alcance de las pruebas a realizar, para definir los diferentes escenarios.

- Determinar el calendario de pruebas, planificando cuándo se deben realizar las pruebas. Para ello, la entidad deberá establecer un calendario tentativo y actualizable del conjunto de pruebas a realizar, así como de su periodicidad.

- Documentar previamente de forma precisa y secuencial (a modo de checklists) todas las actividades y tareas a llevar a cabo en cada prueba, para su correcto desarrollo.

Los planes y procedimientos se pueden probar de manera independiente, sin necesidad de realizar un simulacro de gestión de crisis para verificar su efectividad. En los niveles de madurez inicial del Plan de Continuidad de Negocio, es conveniente probar ciertas alternativas de continuidad de manera aislada, para poder incorporarlas a los simulacros de gestión de crisis cuando dispongan del nivel de madurez adecuado.

# 7 Anexo

**Ejemplos de ficha de prueba:**

| **Título de prueba:** | **Ejercicio activo de acceso a aplicaciones y tecnología del centro alternativo.** |
|---|---|
| **Propósito:** | Ejercitar de forma activa los planes de recuperación de desastres tecnológicos. |
| **Áreas afectadas:** | Dpto. Infraestructuras y Dpto. Sistemas. |
| **Áreas de soporte a la prueba:** | Dpto. Telecomunicaciones. |
| **Documento de referencia:** | Plan de Contingencias Informáticas. |

**Descripción:**

- ✓ Determinar el grado de conocimiento, entendimiento y aplicación práctica de los procesos de continuidad tecnológica.
- ✓ Determinar la disponibilidad de los recursos requeridos para garantizar la continuidad.
- ✓ Determinar si los procedimientos se encuentran actualizados.
- ✓ Determinar el grado de cumplimiento de las expectativas de los intervinientes en el proceso.

**Procedimiento de prueba:**

Los responsables deberán reunir al resto del equipo que se verá afectado por el escenario de crisis simulado sin comunicarles el propósito en forma previa.

Una vez reunidos, cada responsable describirá la situación de crisis a simular y cada integrante deberá ejecutar las responsabilidades que tendrá a su cargo. Asimismo, cada vez que se detecte la necesidad de utilizar algún recurso en particular, se deberá verificar la disponibilidad de este.

**Elementos a probar:**

| | | |
|---|---|---|
| ☒ Procedimientos | ☒ Telecomunicaciones | ☐ Gestión de Crisis |
| ☒ Capacitación | ☒ Aplicaciones | ☐ Traslado del Personal |
| ☐ Acceso al centro alternativo | ☐ Recursos humanos | ☐ Vuelta a la Normalidad |
| ☐ Procesos de Negocio | ☐ Comunicación | |

**Indicadores:**

- ✓ Tiempo transcurrido hasta la recuperación de la continuidad de la tecnología.
- ✓ Porcentaje de recursos requeridos para la continuidad disponibles.
- ✓ Porcentaje de conocimiento de los procedimientos (nº personas con conocimiento / personas involucradas).
- ✓ Cantidad de errores en los procedimientos (grado de actualización).

EUSKO JAURLARITZA
GOBIERNO VASCO

cyber zaintza
BASQUE CYBERSECURITY AGENCY

# ¡Muchas gracias!

www.ciberseguridad.eus