
# *Ingeniería Informática*
# *Diseño de Auditoría a la Ciberseguridad*

## *Control de Lectura Unidad 2*
## *Planes de Contingencia y Continuidad de Negocio*
## *Basado en INCIBE*

***Alumnos:***
***Aldo Hernandez, Johan Suarez, Fernando Ureta***

***Profesor:***
***Miguel Angel Castillo***

Octubre 2025

A partir del documento Plan de Contingencia y Continuidad de Negocio de INCIBE, responder las siguientes preguntas, citando el texto.

1. Diferencia de Alcance y Rol de los Planes.

**Pregunta:** Como auditor, explique la diferencia fundamental en el **alcance** (perspectivas que abarca) y el **enfoque** (técnico vs. negocio) de los tres planes. Además, indique cuál de estos planes sirve como el "**disparador**" para la puesta en marcha de los diferentes planes de contingencia.

**R: El Plan de Continuidad de Negocio (PCN)** se enfoca en la continuidad de la organización en múltiples perspectivas, como la infraestructura TIC, recursos humanos, mobiliario, sistemas de comunicación, etc. Tiene un enfoque más general sobre el negocio y sirve como "disparador" para poner en marcha planes de continuidad más concretos según el caso. El Plan de Continuidad TIC (PCTIC) se restringe al ámbito de las Tecnologías de la Información, teniendo así un enfoque más técnico. Finalmente, **el Plan de Recuperación ante Desastres (PRD)** mantiene un alcance reactivo ante catástrofes, de manera que tiene un enfoque más técnico.

2. Análisis de Impacto y Métricas Críticas (RTO, MTD, RPO)
   El Análisis de Impacto sobre el Negocio (BIA) es uno de los ejes principales del Plan de Continuidad TIC, ya que contiene las necesidades de los procesos críticos.

**Pregunta**: Describa y diferencie conceptualmente los siguientes parámetros críticos que se definen en el BIA: RTO (Recovery Time Objective), MTD (Maximum Tolerable Downtime) y RPO (Recovery Point Objective). Indique, además, la relación matemática o lógica que debe existir obligatoriamente entre el RTO y el MTD para que un proceso sea recuperable.
**R:**
- **RTO (Tiempo de recuperación)** es el tiempo que un proceso estará detenido antes de que su funcionamiento sea restaurado.
- **MTD (Tiempo máximo tolerable de caída)** es el tiempo que un proceso puede permanecer caído antes de que existan consecuencias desastrosas para la empresa.
- **ROL (Niveles mínimos de recuperación de servicio)** es el nivel mínimo de recuperación que debe tener una actividad para que la consideremos recuperada, incluso si su servicio no es el óptimo.
- **RPO (Grado de dependencia de la actualidad de los datos)** es un valor que determina el impacto que se tiene sobre la actividad la pérdida de datos.

De forma intuitiva, el tiempo de recuperación (RTO) siempre debe ser menor al tiempo máximo tolerable de caída (MTD) ya que debemos poder recuperar el proceso hasta cumplir el nivel mínimo (ROL) antes de generar consecuencias para la organización.

3. Fases de Análisis y Estrategias de Riesgo

La Fase 1: Análisis de la Organización incluye la recopilación de información y el Análisis de Riesgos.

**Pregunta:** Explique la finalidad principal del Análisis de Riesgos en el contexto de un Plan de Continuidad de Negocio (PCN) e identifique las cuatro (4) estrategias para el tratamiento de los riesgos con mayor impacto que el documento sugiere. Proporcione un ejemplo práctico de la estrategia.

**R:**La finalidad principal del **Análisis de riesgos** en el contexto de un Plan de Continuidad de Negocio es estudiar qué amenazas pueden materializarse afectando a los procesos dentro del alcance, con qué probabilidad, qué impacto tendrían en éstos y qué activos involucrados se verían afectados.

El propósito central es **identificar aquellos riesgos que pueden poner en peligro la continuidad o la información de los procesos críticos** de la organización. Esto permite identificar los riesgos que se deben tratar con mayor prioridad.

**Estrategias para el tratamiento de los riesgos**

Una vez establecidos los principales riesgos (aquellos con mayor impacto), el documento sugiere tratarlos mediante una de las siguientes cuatro (4) estrategias:

1. **Transferir el riesgo a un tercero**.
2. **Eliminar el riesgo**.
3. **Asumir el riesgo**.
4. **Implantar medidas para mitigarlo**.

**Ejemplo para "Transferir el riesgo a un tercero":** Una empresa transfiere el riesgo financiero de una caída catastrófica de sus servidores o un ciberataque al **contratar una póliza de seguro de ciber-riesgo o continuidad de negocio**. De esta forma, si el evento se materializa, el costo de la recuperación (daños, multas, interrupción de negocio) es asumido por la aseguradora.

4. Determinación de la Estrategia y la Brecha de Continuidad

La Fase 2: Determinación de la Estrategia de Continuidad es vital para el diseño del Plan.

**Pregunta:** ¿Cuál es el principal objetivo de la Fase 2? Explique cómo se identifica la brecha de continuidad al utilizar la información clave obtenida en la Fase 1. Utilice el ejemplo del proceso de contratación de personal del documento para ilustrar un caso donde el RTO de un activo supera el MTD del proceso, creando dicha brecha.

**R:**El **principal objetivo de la Fase 2: Determinación de la estrategia de continuidad** es determinar si, en caso de desastre, la organización será capaz de recuperar los activos que soportan los procesos críticos en el tiempo necesario. En los casos en que esto no sea posible, se deben establecer las diversas estrategias de recuperación.

**Identificación de la brecha de continuidad**

La brecha de continuidad se identifica al determinar la **diferencia entre las necesidades de los procesos de negocio** (obtenidas en la Fase 1: Análisis de la organización) y las **capacidades de los recursos que utilizan**. Es decir, se compara lo que el negocio exige con lo que la infraestructura tecnológica puede garantizar. De este modo, se identifica si los recursos actuales y sus estrategias de recuperación permitirían cubrir el **MTD** (tiempo máximo tolerable de caída) establecido para cada proceso.

**Ilustración con el ejemplo del proceso de contratación**

El documento ilustra la brecha de continuidad con el siguiente ejemplo:

**Necesidad del proceso (MTD):** El proceso de contratación tiene un **MTD de 24 horas**.

**Capacidad de un activo (RTO):** El proceso utiliza el correo electrónico, un directorio departamental y una aplicación específica de contabilidad.

- El email y el directorio departamental tienen un RTO (Tiempo de Recuperación) de **8 horas** (cumplen con el MTD).
- La **aplicación específica de contabilidad** tiene un RTO de **48 horas**.

**La brecha de continuidad:** En este caso, el RTO del activo (aplicación de contabilidad = **48 horas**) es **superior al MTD del proceso** (proceso de contratación = **24 horas**). Esto significa que si dicha aplicación falla, el proceso se interrumpirá durante 48 horas, lo que implica un **deterioro grave de la actividad de la empresa**.

**Estrategia a seguir:** El propósito de la Fase 2 es implantar medidas que **reduzcan este RTO de 48 horas por debajo del MTD de 24 horas**.

5. Enfoques para la Determinación del Alcance (Fase 0)

La Fase 0: Determinación del Alcance establece la magnitud y el coste del proyecto de continuidad.

**Pregunta:** Como líder de un proyecto PCTIC, ¿cuáles son los dos enfoques principales para determinar el alcance del proyecto (según activo o según proceso)? Describa las características de cada enfoque e indique cuál es el más recomendado en el documento para el desarrollo de un Plan de Continuidad de Negocio TIC (PCTIC) y por qué.

**R:** El documento de INCIBE señala que existen dos enfoques principales para determinar el alcance de un plan de continuidad:

1. **Enfoque por activo:**

Se centra en mejorar la continuidad de un conjunto de activos tecnológicos (servidores, equipos, bases de datos, etc.) y a partir de ellos se determinan los procesos que dependen de esos activos.

Este enfoque es más propio de un Plan de Recuperación ante Desastres (PRD) o de proyectos liderados por el departamento técnico.

2. **Enfoque por proceso:**

Se orienta a la continuidad de un proceso de negocio crítico, independientemente de los activos que lo soporten. Busca mejorar la capacidad del proceso para continuar operando ante una contingencia.

Este enfoque es más propio del negocio y permite abordar las necesidades reales de la organización.

El enfoque recomendado por el documento para un **Plan de Continuidad de Negocio TIC (PCTIC)** es el enfoque por proceso, ya que según INCIBE "vamos a coger nuestro proceso más crítico y vamos a mejorar su continuidad" y puede aplicarse a distintos entornos (tecnología, logística, producción, etc.) con pocas modificaciones.

Cita INCIBE: "Dado que nuestra idea es hacer un Plan de Continuidad de Negocio TIC, vamos a centrar nuestro proyecto en un enfoque por proceso. Es decir, vamos a coger nuestro proceso más crítico y vamos a mejorar su continuidad."

6. Prueba y Concienciación (Verificación y Cultura)

Las últimas fases del Plan de Continuidad se enfocan en la verificación y la cultura organizacional.

**Pregunta:** Desde la perspectiva de un auditor, justifique la importancia de la Fase 4 (Prueba, Mantenimiento y Revisión) y la Fase 5 (Concienciación). Específicamente, mencione los dos (2) planes o documentos clave que deben elaborarse e implantarse en la Fase 4 para verificar la efectividad del PCN/PCTIC.

**R:** Desde la visión de auditoría, ambas fases son críticas para garantizar la eficacia y vigencia del **Plan de Continuidad de Negocio (PCN/PCTIC):**

- **Fase 4: Prueba, Mantenimiento y Revisión**

Su propósito es mantener actualizado el plan y comprobar que funciona correctamente ante una contingencia real.

Un plan no probado puede contener información desactualizada (personal que ya no trabaja, versiones obsoletas, teléfonos erróneos, etc.), lo que podría ser catastrófico durante una crisis.

En esta fase se deben elaborar e implantar dos documentos fundamentales:

1. **Plan de mantenimiento**, que asegura que la documentación del plan se mantenga actualizada ante cualquier cambio significativo en infraestructura, personal o procesos.
2. **Plan de pruebas**, que verifica mediante ejercicios y simulaciones que la organización puede recuperarse en los tiempos definidos (RTO, MTD) y que el personal sabe actuar ante una contingencia.

**Cita INCIBE:**
"*El propósito es mantener actualizada toda la documentación cada vez que se produzca un cambio significativo… Esto permitirá que la documentación refleje fielmente la información de los distintos actores involucrados.*"
*"El objetivo es mostrar los distintos tipos de pruebas de contingencia que debemos llevar a cabo… para garantizar la salud del PCTIC."*

- **Fase 5: Concienciación**

Se orienta a fortalecer la cultura organizacional de continuidad, asegurando que todo el personal —técnico y de negocio— conozca sus responsabilidades, los planes existentes y cómo actuar en una contingencia.
Un personal concienciado reduce el error humano y mejora la respuesta ante incidentes.
**Cita INCIBE:** "*Debemos llevar a cabo aquellas tareas que incrementen la concienciación del personal en relación con la continuidad… tanto del personal implicado en los procesos de negocio, como del personal de TI.*"