TEMA 128. LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. PLANES DE CONTINUIDAD Y CONTINGENCIA DEL NEGOCIO

Actualizado a 10/01/2022

1. La Gestión de la Continuidad del Negocio

La gestión de la continuidad del negocio **ayuda a disminuir la posibilidad de ocurrencia de un incidente**, y en caso de producirse, ofrece a la empresa los medios para responder, reducir el daño causado y recuperarse lo antes posible.

Las normas que aplican en relación con los planes de continuidad de negocio son principalmente:

ISO 22301

- La ISO 22301:2019 (en España UNE-EN ISO 22301:2020) es una norma basada en la BS 25999-2 que define los requisitos para implementar, mantener y mejorar un sistema de gestión de la continuidad del negocio (**SGCN**) para proteger y reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de disrupciones cuando éstas surjan.
- Está estructurada en 10 capítulos, entre los que destacan el ámbito de aplicación, contexto de la organización, liderazgo, planificación, apoyo, operación, evaluación del desempeño y mejora. Todo ello en línea con el enfoque de mejora continua Plan-Do-Check-Act.
- Todo SGCN debe contener una **Política de Continuidad del Negocio**. Esta política:
    - Implica el compromiso de la Dirección con la Continuidad del Negocio.
    - Estará alineada con el propósito de la organización (alineada con objetivos)
    - Proporcionará un marco para establecer los objetivos de continuidad del negocio.
    - Incluye un compromiso de mejora continua y de satisfacción de requisitos
    - Deberá estar disponible como información documentada
    - Será comunicada dentro de la organización y puesta a disposición de las partes interesadas.
    - Será revisada para su continua adecuación.
- Entre la documentación que forma el SGCN se encuentra:
    - El contexto de la organización (alcance, partes interesadas, requisitos legales, reglamentarios, normativos…)
    - Política de la continuidad de negocio.
    - Objetivos de la continuidad del negocio.
    - Análisis del impacto en el negocio (BIA).
    - Evaluación de los riesgos.
    - Estrategias y soluciones de continuidad del negocio para antes, durante y después de la disrupción (planes de continuidad, procedimientos de recuperación …)
    - Programas de pruebas
    - Evaluación del desempeño (seguimiento, auditoría interna, revisión por la dirección)
    - Mejora continua (oportunidades de mejora, no conformidades y acciones correctiva
- Este estándar es certificable y auditable según la norma ISO 22301.

NOTA: Algunas definiciones indicadas en la UNE-EN-ISO 22301:2020:

- Continuidad del Negocio: capacidad de una organización para continuar suministrando productos y servicios en plazos aceptables con una capacidad predefinida durante una disrupción

- Plan de continuidad del negocio: Información documentado que orienta a una organización para responder a una disrupción y reanudar, recuperar y restablecer la entrega de productos y servicios en consonancia con sus objetivos de continuidad de negocio
- Análisis de impacto en el negocio (BIA): Proceso de análisis del impacto de una disrupción en la organización a lo largo del tiempo
- Disrupción: incidente, ya sea previsto o imprevisto, que causa una desviación negativa no planificada de la provisión prevista de productos y servicios acorde con los objetivos de una organización
- Incidente: evento que puede ser, o podría conducir a una disrupción, pérdida, emergencia o crisis
- Sistema de Gestión: conjunto de elementos de una organización interrelacionados o que actúan entre sí para establecer políticas y objetivos y procesos para alcanzar esos objetivos.

ENS: PLAN DE CONTINUIDAD DE NEGOCIO

- El Esquema Nacional de Seguridad establece una de sus medidas operativas para determinar los criterios necesarios a cumplir en este punto en base a la categoría de su dimensión de disponibilidad.
    - Artículo 25 RD 3/2010, Continuidad de la actividad: "*Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo*".
    - La medida operativa del **Plan de Continuidad de Negocio** se incluye dentro del marco operacional que está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin, dentro de este es la segunda medida del apartado de Continuidad del Servicio [op.cont.2].
    - Es una medida que en la versión actual del ENS solo aplica a las valoraciones de la **dimensión de Disponibilidad de nivel alto**, no aplicando ni a las de nivel medio, ni bajo.
    - Para el nivel ALTO la medida exige que se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Este plan contemplará los siguientes aspectos:
        - Se identificarán funciones, responsabilidades y actividades a realizar.
        - Existirá una previsión de los medios alternativos que se va a conjugar para poder seguir prestando los servicios.
        - Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.
        - Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
        - El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.

¡Importante!: A fecha de actualización de este documento, el ENS vigente es el RD 3/2010, no obstante, se encuentra un borrador de un nuevo ENS con fecha prevista de aprobación a principios del 2022

ISO 270001: SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- La ISO 27001:2013 (en España UNE-EN ISO/IEC 27001:2017) especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información que preserve la confidencialidad, integridad y disponibilidad de dicha información.
- Como parte fundamental para asegurar la disponibilidad de la información, la norma incluye en su anexo, objetivos y controles relacionados con la continuidad de negocio (se encuentran detallados en la ISO 27002), como, por ejemplo, el objetivo 17.1: *"La continuidad de la seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización",* incluyendo controles para si planificación, implementación y verificación, revisión y evaluación.

2. PLAN DE CONTINUIDAD Y CONTINGENCIA DE NEGOCIO

En el Plan de Contingencia y Continuidad de Negocio se regulará los mecanismos a poner en marcha en caso de un incidente grave de seguridad con el objeto de ser capaces de reaccionar a la interrupción de la actividad o un fallo de los procesos críticos de negocio, de dar una respuesta rápida y eficaz ante cualquier contingencia grave, de proteger al personal y los activos, de manera que podamos recuperar la actividad normal en un plazo de tiempo tal que no se vea comprometido nuestro negocio, minimizando el proceso de la toma de decisiones durante la contingencia.

BENEFICIOS	*OBJETIVOS*
● Previene o minimiza las pérdidas ● Clasifica los activos para priorizar su protección ● Conocer los tiempos críticos de recuperación ● Mejora imagen y revalorización de la confianza en la organización	● Análisis crítico de la organización y detección de puntos débiles. ● Identificación y evaluación de riesgos. ● Establecimiento medidas preventivas y de recuperación. ● Disponer de guía para el personal.
PRIORIDADES	*AYUDA A*
● Evitar pérdidas humanas ● Reanudar las operaciones lo antes posible ● Lograr conexiones con los principales clientes y proveedores ● Mantener la confianza en la organización ● Proteger el medio ambiente	● Mantener el nivel de servicios en los límites definidos ● Establecer el punto de recuperación mínimo ● Recuperar la situación antes del incidente ● Analizar resultados y motivos del incidente ● Evitar que la actividad se interrumpa

El Plan de Contingencia es la herramienta clave para garantizar la continuidad del negocio. Se deben definir todos los protocolos y acciones a realizar, incluyendo formación del personal implicado, las adquisiciones necesarias, y la realización de pruebas y simulacros para su mejora continua.

INCIBE establece en su metodología para la elaboración de su plan de continuidad tres tipos de plan:

- **Plan de Continuidad de Negocio (PCN o BCP en inglés)** que establece la continuidad de una organización desde múltiples perspectivas: infraestructura **TIC**, recursos humanos, mobiliario, sistemas de comunicación, logística, sistemas industriales, infraestructuras físicas, etc. Cada uno de estos ámbitos tendrá a su vez un plan de continuidad más específico, ya que no es lo mismo la inundación de un almacén de logística que el corte del suministro eléctrico en una sala de servidores.
- **Plan de Continuidad TIC** (**PCTIC**), es uno de los planes que forman el plan de continuidad de negocio de nuestra organización, pero restringido al ámbito TIC. Mientras que un PCN sirve de disparador para los diferentes planes de contingencia, un **PCTIC** se limita al ámbito tecnológico. Aunque el alcance de un PCN es por lo general superior al de un PCTIC, ya que hay otros procesos y activos no tecnológicos implicados, las fases de su elaboración son básicamente las mismas. Suele componerse de 3 subplanes:
    - **Plan de Respaldo**: contempla las medidas preventivas ANTES de la materialización de la amenaza.
    - **Plan de Emergencia**: contempla las medidas paliativas o minimizadoras DURANTE la materialización de la amenaza, o justo después. Mediante uso de árboles de decisión como procedimiento de toma de decisiones y hojas de contactos con los responsables de las salvaguardias.
    - **Plan de Recuperación**: contempla las medidas necesarias DESPUÉS de la materialización de la amenaza y haberla controlado. Incluye las acciones:
        - Preparación: inicio de actividades
        - Movilización: activación y puesta en marcha de recursos necesarios
        - Recuperación: puesta en marcha de medidas recuperación
        - Verificación: validación de las medidas recuperación por cada responsable.
- **Plan de Recuperación ante Desastres (PRD).** En este caso, su fase de análisis es menos profunda y se enfoca al ámbito más técnico, de modo que es un plan reactivo ante una posible catástrofe.

FASES DEL PCN (SEGÚN INCIBE)

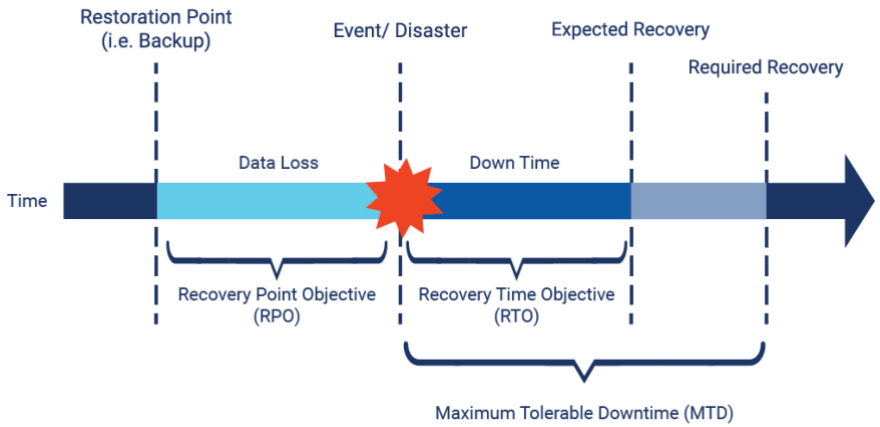
FASE 0: DETERMINACIÓN DEL ALCANCE.

- Lo que determinará el coste del proyecto y su viabilidad.
- Se determinarán los elementos que van a ser el foco del plan de continuidad.
- Enfoques:
    - por activo: más apropiado cuando el proyecto lo dirige el equipo Informático
    - por proceso: más apropiado cuando el proyecto es liderado por el Negocio.

FASE 1: ANÁLISIS DE LA ORGANIZACIÓN

- Será iniciado con un conjunto de entrevistas con los usuarios finales a partir del cual se elaborará un **Análisis de impacto sobre el Negocio o BIA,** siempre elaborado desde el punto de vista del negocio. En esta fase se deben determinar:
    - **RPO**: Punto de recuperación Objetivo o la cantidad de perdida de dato durante un desastre que la empresa considera tolerable. Esto determinará la política de backup que se considera necesario.
    - **RTO**: Tiempo de recuperación objetivo o el tiempo máximo que se acepta que este el negocio no operativo.

- El Tiempo máximo tolerable de caída o **MTD** antes de que se produzcan consecuencias desastrosas. El MTD está relacionado con el negocio, mientras que el RTO será determinado por personal técnico.
- Niveles mínimos de recuperación de servicio o **ROL** aunque este no sea óptimo.
- Dependencia de otros procesos internos o proveedores externos.



- Una vez analizada y recogida toda esta información, se llevará a cabo un **análisis de riesgos** determinando:
  - Las amenazas que impliquen una indisponibilidad de los procesos en el alcance.
  - La probabilidad y el impacto de cada una de esas amenazas.
  - El producto de la probabilidad por el impacto de cada amenaza.
- De esta manera, se obtiene un listado de riesgos y un **plan de tratamiento de riesgos** que incluya las medidas para tratarlos (transferir, eliminar, asumir o mitigar), la fecha límite de implantación, el responsable de este y los recursos necesarios.

Fase 2: Determinación de la Estrategia de Continuidad.

- Mediante la cual se debe determinar si los recursos actuales y sus estrategias de recuperación permitirán cubrir el MTD establecido para cada proceso. Los recursos afectables serán: personal, locales, tecnología, información y proveedores.
- Se deberá definir el **conjunto de roles y responsabilidades del equipo** que deberán conformar el equipo de crisis. Este equipo deberá ser multidisciplinar.
- Se deberá determinar el **plan de comunicación** en caso de contingencia, determinando un único interlocutor.
- Se deberá valorar el **coste y viabilidad de su implantación y mantenimiento**.

Fase 3: Respuesta a la contingencia.

- Determina el flujo en la toma de decisiones, según las particularidades de la interrupción.
- Se implementan las iniciativas de la estrategia, y se elabora la documentación, en especial:
  - El **Plan de Crisis o de incidentes**.
  - Los **planes operativos de recuperación de entornos**.
  - Los **procedimientos técnicos de trabajo**.

Fase 4: Prueba, mantenimiento y revisión.

- Se deberá llevar a cabo en base a una **planificación previa** y siempre al menos una vez al año. Se deberá tener en cuenta:
    - El personal técnico implicado en la prueba.
    - El usuario del aplicativo.
    - El personal externo implicado.
    - La descripción de la prueba.
    - Descripción del resultado esperado.
    - Hora y fecha de realización teniendo en cuenta que puede suponer una pérdida de servicio por lo que deberá hacer en horario de mínimo impacto.
- Es importante determinar que fallos podrían producirse, para tenerlos en cuenta en la planificación de las pruebas, y **como mínimo deberá tenerse en cuenta las siguientes**:
    - Fallo eléctrico.
    - Tiempos de recuperación de repositorios documentales.
    - Recuperación de aplicaciones críticas de negocio.
    - Acceso remoto a la infraestructura desde una ubicación externa.
    - Aseguramiento de que funcionan los entornos replicados en cluster.
- Adicionalmente, debe de existir un **plan de mantenimiento** que tendrá que ser actualizado cada vez que se produzca un cambio significativo en la organización, así como **un Plan de pruebas** que garantice que la información del plan se mantenga actualizada, que la empresa puede recuperarse, asegure la cohesión del personal implicado, mejore el conocimiento de los usuarios en relación con las pruebas e incremente la confianza de los usuarios en la organización.

FASE 5. PLAN DE CONCIENCIACIÓN.

- Aplicado para todo el personal, en especial el responsable, técnico y participantes en el equipo de crisis. Es necesario que tanto el personal técnico como los responsables de la empresa conozcan qué es y qué supone en Plan de Continuidad de Negocio así como qué se espera de ellos.