Capítulo extraído del libro "**Análisis funcional de sistemas y tecnologías de la información**" de Aníbal Mario Mazza Fraquelli (2025) **ISBN 978-987-26981-3-3**.

Business Continuity Plan y Disaster Recovery Plan

Presentación del tema

En las organizaciones contemporáneas, los Sistemas de Información (SI) se han convertido en la columna vertebral de los procesos operativos, financieros, comerciales y de gestión. En este contexto, la resiliencia organizacional depende de la capacidad de sostener servicios críticos frente a eventos adversos. Dos instrumentos centrales son el BCP (Business Continuity Plan, Plan de Continuidad del Negocio) y el DRP (Disaster Recovery Plan, Plan de Recuperación ante Desastres).

Ambos forman parte de un enfoque integral de gestión del riesgo y continuidad, pero no son equivalentes: el BCP se orienta a asegurar que la organización continúe funcionando ante una interrupción significativa, mientras que el DRP se concentra en la recuperación tecnológica de infraestructura, aplicaciones y datos. Comprender esta diferencia es crítico para la administración, porque define responsabilidades, prioridades, inversiones y tiempos de respuesta frente a un incidente.

Concepto de incidente

Un incidente es un evento —o serie de eventos— que interrumpe, degrada o amenaza el funcionamiento normal de un servicio, proceso o activo crítico, pudiendo afectar la confidencialidad, integridad o disponibilidad de la información. En el ámbito de TI, los incidentes pueden incluir fallas de infraestructura, cortes de energía, ciberataques, errores humanos, fallas de proveedores o eventos físicos.

Desde la administración, un incidente se define por su impacto en el negocio, no solo por su naturaleza técnica. Un evento "pequeño" tecnológicamente puede ser "crítico" si afecta un proceso esencial en un momento determinado.

El BCP: Plan de Continuidad del Negocio

El BCP es el conjunto de estrategias, procedimientos, roles y recursos que permiten a la organización mantener o reanudar operaciones críticas ante un incidente. Su objetivo es minimizar el tiempo de interrupción, la pérdida de ingresos, el daño reputacional y los incumplimientos regulatorios.

El BCP actúa cuando el incidente afecta la capacidad de operar normalmente y requiere activar procesos alternativos: derivar llamadas a otra sede, procesar transacciones manualmente, activar proveedores de respaldo o comunicar a clientes los tiempos de recuperación. Es un plan organizacional que involucra áreas operativas, finanzas, recursos humanos, comunicación, legal y TI.

Los componentes principales del BCP incluyen el análisis de impacto en el negocio (BIA), la identificación de procesos críticos, las estrategias de continuidad para cada proceso, los protocolos de comunicación de crisis y los criterios de activación y desactivación del plan.

El DRP: Plan de Recuperación ante Desastres

El DRP define los procedimientos técnicos y operativos para restaurar sistemas de información, datos e infraestructura tecnológica tras un incidente grave. Se activa cuando el BCP requiere disponibilidad tecnológica para garantizar la continuidad, o cuando la interrupción es exclusivamente tecnológica y el negocio puede continuar en un modo degradado.

Sus componentes clave incluyen los objetivos RPO y RTO, el inventario de sistemas críticos con sus prioridades de recuperación, los procedimientos de recuperación paso a paso, la definición de sitios alternativos (hot site, warm site, cold site) y las pruebas periódicas. El hot site es una instalación completamente equipada y disponible de inmediato; el warm site requiere configuración parcial; el cold site requiere instalación completa antes de operar.

Articulación entre BCP y DRP

El BCP y el DRP se complementan de manera sistémica: el BCP garantiza que el negocio pueda operar; el DRP garantiza que la tecnología esté disponible para soportarlo. Sin DRP, el BCP carece de la infraestructura tecnológica necesaria; sin BCP, el DRP recupera sistemas que no pueden ser utilizados de manera organizada. Las pruebas periódicas conjuntas son la condición de efectividad de ambos planes.

Conceptos clave

- BCP: continuidad de los procesos de negocio ante interrupciones.
- DRP: recuperación tecnológica de sistemas, datos e infraestructura.
- BIA como análisis previo que identifica procesos críticos y sus requisitos.
- RPO y RTO como objetivos de diseño del DRP.
- Hot site, warm site y cold site como opciones de sitio alternativo.
- Pruebas periódicas como condición de efectividad de ambos planes.

Preguntas de repaso del tema

1. ¿Cuál es la diferencia principal entre BCP y DRP?
2. ¿Cómo se define un incidente desde la perspectiva del negocio?
3. ¿Qué es el BIA y qué informa al diseño del BCP?
4. ¿Cuál es la diferencia entre un hot site, warm site y cold site?
5. ¿Cómo se relacionan RPO y RTO con el DRP?
6. ¿Por qué BCP y DRP deben diseñarse y probarse de manera conjunta?
7. ¿Qué áreas de la organización deben participar en la elaboración del BCP?

8. ¿Por qué las pruebas periódicas son condición de efectividad de ambos planes?
9. ¿Qué consecuencias puede tener una organización que tiene DRP pero no BCP?
10. ¿Cómo se relacionan BCP y DRP con la gestión del riesgo tecnológico?