Universidad de Buenos Aires
Facultad de Ciencias Económicas

Business Continuity Plan y Disaster Recovery Plan

AR Tema extractado del libro "**Análisis Funcional de Sistemas y Tecnologías de la Información**" de Aníbal M. Mazza Fraquelli - ISBN 978-987-26981-3-3

Presentación del Tema

En las organizaciones contemporáneas, los Sistemas de Información (SI – *Information Systems*) 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 para lograrlo son el **BCP (Business Continuity Plan / Plan de Continuidad del Negocio)** y el **DRP (Disaster Recovery Plan / Plan de Recuperación ante Desastres)**.

Ambos planes 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. La diferencia es crítica para la administración, porque define responsabilidades, prioridades, inversiones y tiempos de respuesta frente a un **incidente (Incident / Incidente)**.

En términos académicos y prácticos, comprender qué es un incidente, cuándo se activa cada plan y cómo se articulan BCP y DRP permite a los futuros

administradores diseñar estrategias de continuidad alineadas con la gobernanza de TI, la gestión del riesgo y los objetivos del negocio.

Desarrollo

1. Concepto de Incidente

> ➡ Un **incidente (Incident / Incidente)** es un evento —o una 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 y/o la continuidad operativa.

En el ámbito de TI, los incidentes pueden incluir:

- Fallas de infraestructura (servidores, almacenamiento, red).
- Cortes de energía o fallas de climatización en centros de datos.
- Ciberataques (ransomware, DDoS, intrusión).
- Errores humanos (borrado accidental, configuración errónea).
- Fallas de proveedores o servicios en la nube.
- Eventos físicos (incendio, inundación).

Desde la administración, el concepto clave es que 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 (por ejemplo, el sistema de cobranzas en horario de cierre).

---

2. BCP: Business Continuity Plan

2.1 Definición y objetivo

El **BCP (Business Continuity Plan / Plan de Continuidad del Negocio)** es el conjunto de estrategias, procedimientos, roles y recursos que permiten a la

organización **mantener o reanudar operaciones críticas** ante un incidente que interrumpe parcial o totalmente su funcionamiento.

Su objetivo central es asegurar la continuidad de los procesos esenciales del negocio, minimizando:

- Tiempo de interrupción.
- Pérdida de ingresos.
- Daño reputacional.
- Incumplimientos regulatorios o contractuales.

El BCP es, por definición, un plan **organizacional**: involucra áreas operativas, finanzas, recursos humanos, comunicación, legal, proveedores y TI.

2.2 ¿Cuándo actúa el BCP?

El BCP actúa cuando un incidente afecta la capacidad de la organización de operar "como siempre" y se requiere:

- Continuar el servicio con modos alternativos (workarounds).
- Reducir el impacto al cliente.
- Repriorizar procesos.
- Reasignar recursos.
- Habilitar operaciones temporales (manuales o en sedes alternativas).

Ejemplos de activación:

- Caída del sistema de facturación en plena operación diaria.
- Indisponibilidad del edificio principal (incendio, evacuación).
- Corte prolongado de conectividad que impide operar servicios centrales.
- Ciberincidente que obliga a aislar sistemas preventivamente.

2.3 Componentes típicos del BCP

1. **BIA (Business Impact Analysis / Análisis de Impacto en el Negocio)**

   Identifica procesos críticos, dependencias y consecuencias de interrupción.

2. **Definición de criticidad y prioridades**

   Determina qué debe sostenerse primero y bajo qué umbrales.

3. **RTO y RPO**

   - **RTO (Recovery Time Objective / Objetivo de Tiempo de Recuperación):** tiempo máximo tolerable para restablecer un proceso/servicio.
   - **RPO (Recovery Point Objective / Objetivo de Punto de Recuperación):** máxima pérdida de datos tolerable medida en tiempo (por ejemplo, "no más de 4 horas de datos").

4. **Estrategias de continuidad**

   - Procesos manuales temporales.
   - Reubicación de equipos (sitio alternativo).
   - Trabajo remoto controlado.
   - Proveedores alternativos.

5. **Plan de comunicación de crisis**

   Mensajes internos y externos (clientes, reguladores, prensa), roles autorizados para comunicar.

6. **Roles, responsabilidades y escalamiento**

   Comité de crisis, líderes por proceso, y cadenas de decisión.

7. **Pruebas y simulacros**

   Validación periódica del plan para asegurar que sea ejecutable.

2.4 Ejemplo de BCP (en clave de administración y TI)

Una empresa con plataforma de e-commerce sufre una caída del gateway de pagos. El BCP puede disponer:

- Activación inmediata de un proveedor de pagos alternativo (si existe contrato).
- Habilitación de transferencias bancarias con conciliación posterior.

- Priorización de atención a clientes y comunicaciones para minimizar reputación negativa.
- Registro manual de pedidos críticos.

Obsérvese que el BCP no “repara servidores”; mantiene el negocio operando.

---

3. DRP: Disaster Recovery Plan

3.1 Definición y objetivo

El **DRP (Disaster Recovery Plan / Plan de Recuperación ante Desastres)** es el conjunto de procedimientos y recursos destinados a **restaurar la infraestructura tecnológica, aplicaciones, servicios y datos** luego de un incidente grave que genera indisponibilidad o degradación significativa.

Su objetivo central es recuperar la capacidad tecnológica necesaria para volver a operar con normalidad, en línea con los RTO y RPO definidos.

El DRP es, por naturaleza, más **técnico-operativo**, liderado por TI, pero debe estar alineado con prioridades del negocio establecidas por el BCP.

3.2 ¿Cuándo actúa el DRP?

El DRP actúa cuando se requiere:

- Restaurar servidores o servicios críticos.
- Recuperar bases de datos desde backups.
- Habilitar un sitio alternativo (disaster recovery site).
- Migrar cargas a la nube o entorno secundario.
- Reconstituir redes y comunicaciones.
- Remediar daños causados por malware (por ejemplo, ransomware).

Ejemplos:

- Pérdida total o parcial del data center.
- Corrupción masiva de bases de datos.
- Ataque de ransomware que obliga a reconstruir entornos.

- Fallo crítico de infraestructura sin posibilidad de reparación rápida.

3.3 Componentes típicos del DRP

1. **Inventario de activos tecnológicos críticos**

   Aplicaciones, servidores, redes, bases de datos, dependencias.

2. **Arquitectura de recuperación**
   - Sitio secundario (hot site / warm site / cold site).
   - Replicación de datos.
   - Backups (copias) con estrategia 3-2-1 (concepto común).
   - Infraestructura como código (cuando aplica).

3. **Procedimientos de restauración**

   Pasos detallados para reconstruir servicios: orden de arranque, validaciones, pruebas.

4. **Backups y restauración comprobada**

   No basta con "tener backups"; se exige prueba periódica de restauración.

5. **Seguridad en la recuperación**

   Verificación de que los entornos restaurados no reintroduzcan la amenaza (por ejemplo, restaurar un backup contaminado).

6. **Monitoreo y validación post-recuperación**

   Confirmar integridad de datos, performance y disponibilidad.

3.4 Ejemplo de DRP

Ante ransomware, el DRP puede indicar:

- Aislamiento inmediato de red (contención).
- Reinstalación de servidores comprometidos.
- Restauración de bases desde backups inmutables.
- Revisión de credenciales y rotación de claves.

- Verificación de integridad antes de reponer servicios.

Aquí el foco está en la **recuperación técnica**.

---

4. Relación y Diferencias entre BCP y DRP

Aunque se complementan, difieren en propósito y foco:

- **BCP:** continuidad de procesos del negocio (personas, operación, comunicación, alternativas).
- **DRP:** recuperación de TI (infraestructura, datos, aplicaciones, redes).

En la práctica:

1. Ocurre un incidente.
2. Se evalúa impacto y se activa el **BCP** para sostener lo crítico.
3. Paralelamente se ejecuta el **DRP** para recuperar la plataforma tecnológica.
4. Se retorna a operación normal y se cierra el incidente con revisión y mejoras.

El BCP define "qué no puede parar"; el DRP define "cómo se restablece la tecnología para que eso vuelva a funcionar".

---

5. Indicadores esenciales para administración y TI

- **RTO** y **RPO** deben definirse por proceso (negocio) y traducirse a requerimientos de TI.
- **MTTR (Mean Time To Repair / Tiempo Medio de Reparación)** puede utilizarse como indicador de eficiencia operativa de recuperación.
- **Pruebas**: un plan no probado es un plan no confiable.

---

6. Dimensión de Gobernanza y Responsabilidad

Desde la perspectiva de la administración:

- El BCP es responsabilidad de la alta dirección y dueños de proceso.
- El DRP es responsabilidad primaria de TI, con soporte de seguridad y proveedores.

- Ambos requieren patrocinio ejecutivo, presupuesto y auditoría periódica.

La ausencia de BCP/DRP maduros incrementa riesgo operacional y riesgo reputacional, además de posibles incumplimientos regulatorios en sectores críticos.

Conclusión

El **BCP (Plan de Continuidad del Negocio)** y el **DRP (Plan de Recuperación ante Desastres)** son instrumentos complementarios y esenciales para la resiliencia de organizaciones dependientes de sistemas de información. El BCP se activa para sostener o reanudar procesos críticos del negocio ante un incidente, mediante estrategias organizacionales y operativas; el DRP se activa para recuperar la plataforma tecnológica —infraestructura, aplicaciones y datos — que permite volver al funcionamiento normal.

El concepto de **incidente** debe entenderse como un evento con impacto sobre la operación, no meramente como una falla técnica. En términos de gobernanza, la eficacia de BCP y DRP depende de su alineación con prioridades de negocio, la definición clara de RTO y RPO, la asignación de responsabilidades, la coordinación inter-áreas y la realización de pruebas periódicas. En un contexto digital, estos planes no son accesorios: son condiciones estructurales para la continuidad, el cumplimiento y la sostenibilidad organizacional.

Preguntas de autoevaluación

1. ¿Cuál es la diferencia principal entre BCP y DRP en términos de objetivo y alcance?
2. ¿Qué es un incidente y por qué se define por su impacto en el negocio?
3. ¿Cómo se relacionan los conceptos RTO y RPO con la planificación de BCP/DRP?
4. ¿Qué componentes organizacionales incluye el BCP que el DRP normalmente no cubre?
5. ¿Por qué la prueba periódica de backups y simulacros es indispensable para validar un DRP y un BCP?

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos),** los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.
La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.
Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.
Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.
Queda expresamente excluido cualquier uso con fines comerciales.