interhost_
grupo satec

Servicio de recuperación ante desastres

Introducción al DRP

Félix Díez Sacristán

A quién pueda interesar

Proyecto: Introducción al DRP
Nivel de seguridad: N0 – Público
Fecha: 02/01/2020, **Versión**: 10.1

Registro de cambios

Versión	Fecha	Revisor	Resumen de los cambios producidos
1 a 09.0	Hasta 2019	FDS	Diferentes versiones antiguas del documento
10.0	Noviembre de 2019	FDS	Cambios en varios apartados
10.1	Diciembre de 2019	FDS	Inclusión de figuras y cambios varios
11.0	Enero de 2020	FDS	Varias modificaciones y cambios de orden. Añadido el Anexo III

Índice

Índice de ilustraciones

Estas notas tienen como objetivo esbozar las diferentes fases de un plan de recuperación ante desastres (DRP). El DRP se enmarca dentro de la más amplia actividad de **protección de datos** la cual asegura la no corrupción ni pérdida de datos, su disponibilidad y accesibilidad para tareas autorizadas y el cumplimiento con la legislación y normativa vigente. *Grosso modo* el DRP se centra en la **disponibilidad del dato** (*data availability*) entendida como el tiempo en que la información es accesible por aplicaciones y usuarios durante los períodos en que se espera que lo esté (idealmente el 100% del tiempo en cualquier período); la disponibilidad abarca por tanto la **accesibilidad, la integridad, la oportunidad y la usabilidad**. Cabe resaltar que una merma apreciable del rendimiento o de la seguridad hacen a la postre inaccesibles (o inusables) los datos por lo que hay que considerar que la protección abarca aspectos más generales.

En los primeros apartados se definen los conceptos básicos, los parámetros a tener en cuenta en el diseño del plan, y se detallan las tareas a ejecutar. A continuación el documento explora diversos métodos o **niveles de solución** (categorías) a incluir en un **plan técnico** de recuperación siguiendo un esquema de clasificación o caracterización en *tiers* de complejidad –y coste– crecientes. Por fin se sugiere asimismo un modelo de **plan de gobernanza** con la inclusión de tareas, roles y la incorporación de equipos de dirección y de coordinación de continuidad, tanto propios como del cliente. Finalmente y en sendos anexos se recoge información sobre la **oferta comercial de interhost_** (y del grupo SATEC) para la puesta en marcha de los servicios objeto del documento.

1_ Introducción

1.1. Conceptos básicos

El plan de continuidad de negocio (BCP) está constituido por el conjunto de **medios, estrategias y procedimientos** que preparan a una Compañía para afrontar un desastre sea cual sea la naturaleza e intensidad de éste. Los preparativos específicos implantados por el departamento de IT para garantizar el acceso a los sistemas de información corporativos (datos y aplicaciones) es lo que denominamos plan de recuperación ante desastres (PRD o **DRP** por *Disaster Recovery Plan* o a veces **IT DRP**). En este sentido el **BCP** aborda problemas, como por ejemplo dónde continuar con la actividad en caso de desastre (e.g. oficinas alternativas), que están fuera del alcance del DRP y por tanto de estas notas.[1]

Son muchas y muy variadas las pérdidas que puede acarrear un incidente o desastre. Sin ánimo de exhaustividad ilustramos las más comunes.

Ilustración 1: Potenciales pérdidas sobrevenidas tras un desastre

Con más precisión podemos definir el DRP como el conjunto de **sistemas** (hardware), **aplicaciones** (software), **comunicaciones** y **procedimientos** que permiten ante un desastre o pérdida de servicio en el Centro de Proceso de Datos (CPD) principal, restablecer el uso del sistema de información, con el mínimo tiempo de indisponibilidad, la menor pérdida de datos, y lo más completamente posible en términos funcionales y de rendimiento. Un buen

[1] Recogemos algunas definiciones comúnmente aceptadas de estos conceptos: ***Disaster recovery plan (DRP)****: The management approved document that defines the resources, actions, tasks and data required to manage the technology recovery effort. The process, policies and procedures related to preparing for recovery or continuation of technology infrastructure, systems and applications which are vital to an organization after a disaster or outage. (Disaster Recovery focuses on the information or technology systems that support business functions, as opposed to Business Continuity which involves planning for keeping all aspects of a business functioning in the midst of disruptive events. Disaster recovery is a subset of Business Continuity). The strategies and plans for recovering and restoring the organizations technological infra-structure and capabilities after a serious interruption (BCI)* ***Disaster recovery planning****: The process of developing and maintaining recovery strategies for information technology (IT) systems, applications and data. This includes networks, servers, desktops, laptops, wireless devices, data and connectivity.* ***Business continuity plan (BCP).*** *Documented procedures that guide organizations to respond, recover, resume and restore to a pre-defined level of operation following disruption.* Fuente*: Business Continuity Glossary* publicado por *DRJournal International* y *Business Institute (BCI)*. Marzo de 2018.

DRP es una condición necesaria (junto a otras medidas como: uso de plataformas fiables, ejecución sistemática de pruebas, gestión del cambio, arquitecturas de alta disponibilidad, personal cualificado, ciberseguridad y procedimientos de emergencia) para garantizar la fiabilidad, disponibilidad y capacidad de servicio de cualquier sistemas de información (condiciones que determinan **la robustez** del sitema y son conocidas como **RAS** por ***Reliability, Availability,* y *Serviceability*). Es comúnmente aceptado que el DRP contempla la recuperación en un CPD alternativo por lo que cabe distinguirlo de las tecnologías de alta disponibilidad (***High Availability*, HA**[2]) que garantizan el acceso a las aplicaciones ante **fallos locales**, o de las soluciones para **operaciones continuas** (mantenimiento en servicio, backup no disruptivo, etc.).

En la siguiente ilustración se muestran esquemáticamente los mecanismos más empleados para protección de datos. Huelga decir que estos mecanismos no son incompatibles sino complementarios y habitualmente coexisten.

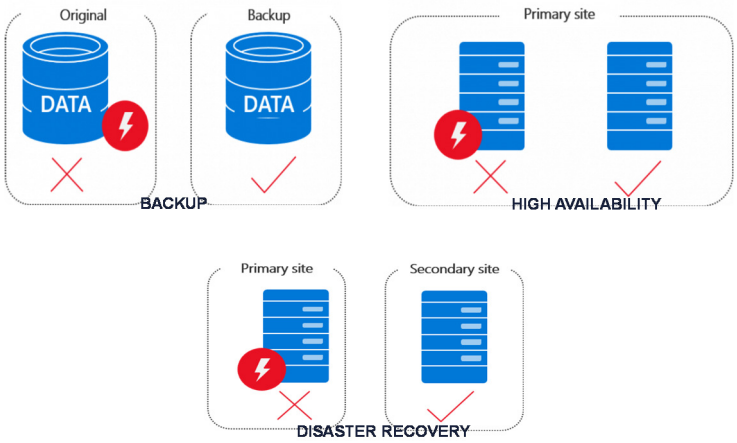

Ilustración 2: Diferentes mecanismos de protección de datos y aplicaciones

Los parámetros denominados **RTO y RPO**[3] son los principales objetivos del Plan de Recuperación ante Desastre que se diseña y concibe con el objeto de **minimizarlos** para todas y cada una de las aplicaciones y servicios protegidos. Como es habitual los objetivos no sólo están condicionados técnicamente, sino que en muchas ocasiones son restricciones económicas las que priman. RTO es el tiempo de recuperación, es decir el tiempo en que los sistemas están indisponibles por un desastre y se mide desde la pérdida de servicio hasta su efectiva recuperación (cómo definir la recuperación –sistema recuperado, usuarios productivos, u otra condición– dependerá del servicio); y el punto de recuperación (RPO), es el tiempo más próximo al desastre para el que se dispone de información que permite recuperar una imagen consistente y operativa de los datos y sistemas. Por tanto en un tiempo inferior a RTO no se podrá garantizar "la vuelta a la normalidad", y para tiempos inferiores a RPO los datos almacenados (registros, transacciones, *updates*, etc.) se perderán o no se garantiza su **integridad**.

[2] *High availability systems typically operate 24x7 and usually require built-in redundancy to minimize the risk of downtime due to hardware and/or telecommunication failures.* Fuente*: DRJournal International* y *Business Institute (BCI).* Marzo de 2018

[3] **RTO**: *The period of time within which systems, applications, or functions must be recovered after an outage. RTO includes the time required for: assessment, execution and verification.* **RPO:** *The point in time to which data is restored and/or systems are recovered after an outage.* Fuente*: DRJournal International* y *Business Institute (BCI).* Marzo de 2018

La suma del RTO y del RPO se puede interpretar como el **riesgo total para el negocio** (tiempo en sombra o tiempo de anormalidad, período durante el cual no existe información o bien porque no se genera, o bien porque se perdió irremediablemente) que se está dispuesto a asumir.

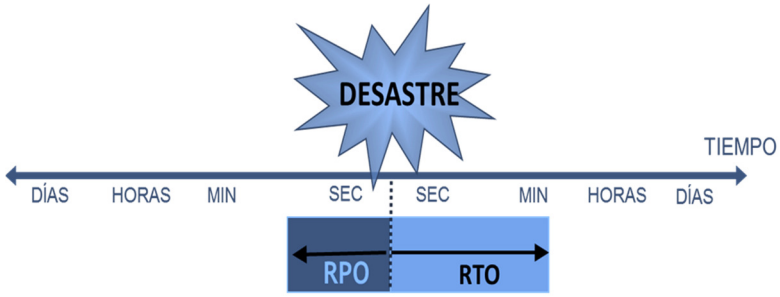

Ilustración 3: Objetivos de tiempo y punto de recuperación

Los parámetros RTO y RPO deben establecerse en función de las necesidades comerciales individuales de cada aplicación y antes de realizar cualquier tipo de planificación para la recuperación ante desastres. De hecho, estas métricas deberían definir la metodología y las actividades para copias de seguridad y replicación. Aunque es obvio que el óptimo y lo más tentador es establecer que todas las aplicaciones tengan un RTO y RPO de cero, ello requeriría inversiones desorbitadas; recíprocamente el exceso de austeridad puede poner en riesgo datos y negocio: se impone por tanto un balance entre lo asequible y lo deseable, considerando siempre –a la hora de definir el RTO/RPO– que las averías suceden en el peor momento y que las pérdidas crecen exponencialmente (no linealmente) con el tiempo de indisponibilidad.

Como es obvio que el tratamiento extremo a extremo es muy beneficioso en el DRP deberían incluirse también los procedimientos y comunicados necesarios para que no quede dañada la imagen del cliente ante hechos graves o se pueda mitigar de forma práctica el **riesgo reputacional** inherente a una situación de crisis.

Cabe señalar en este sentido que muchas empresas han contado sólo con planes de recuperación técnicos que no han sido suficientes para evitarles una mala percepción por parte de los clientes cuando han sufrido una contingencia. Las soluciones que contemplan una respuesta organizada, con mensajes claros y rápidos a los usuarios logran mantener e incluso aumentar y mejorar la percepción de la empresa por parte de empleados y terceros, no sólo reduciendo las pérdidas directas por la falta de servicio, sino mitigando las indirectas provocadas por la pérdida de imagen. Estos aspectos –relacionados con la reputación– no se abordarán aquí. Ha de tenerse en cuenta que un buen **diseño técnico** del DRP es una condición necesaria para salvaguardar una buena imagen pública, pero no siempre suficiente si su supuesta excelencia no se acompaña del relato adecuado.

Recapitulando, los objetivos principales perseguidos en el DRP son: minimizar y **limitar** el alcance de la interrupción y el daño (es decir el RTO y RPO o el tiempo en sombra); **minimizar** el impacto económico de la interrupción; establecer **medios alternativos** de operación por adelantado; disponer de **personal formado** en procedimientos de emergencia; **restaurar el servicio rápidamente y con eficiencia** (sin merma de capacidad y/o rendimiento) y finalmente **salvaguardar la reputación** y la imagen de aquí se deduce que los determinantes (o *drivers*) que guían la elaboración son tanto técnicos, como económicos o de negocio.

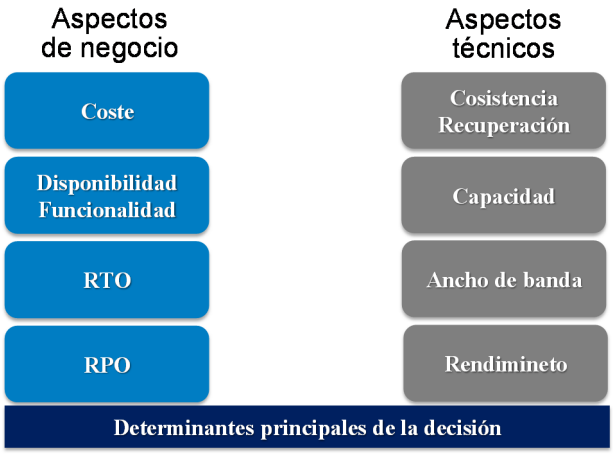

Ilustración 4: *Drivers* técnicos y de negocio condicionantes del DRP

Disponer de un plan de recuperación ante desastres conlleva las siguientes ventajas: garantiza la **continuidad** de los negocios; facilita la conformidad con las regulaciones vigentes (**compliance**), reduce los costes de gestión del riesgo; fortalece la **seguridad**, privacidad y protección del datos; mejora **la formación** y el acervo tecnológico de la compañía; aumenta el **atractivo de la empresa** como *partner* y la mantiene en el mercado de forma sólida incrementando su **competitividad**.

1.2. Alcance

Localmente las tecnologías para garantizar la disponibilidad se pueden jerarquizar en **un continuo** que implica a equipos y a grupos humanos capaces de alcanzar objetivos cada vez más ambiciosos próximos a un **servicio continuo con disponibilidad del 100%** (o al menos 99,999% que es el denominado "*five nines, five minutes*"–es decir cinco minutos de parada anual para una disponibilidad de cinco nueves–), estadio en el que de facto el DRP no sería en teoría activado. Dicho de otra forma si la alta disponibilidad en el estado inicial, llamémosle A, es tan robusta como para cubrir las necesidades del escenario B de DR, es decir A=B, entonces el DRP (que por definición establece las condiciones para B) no sería necesario, pero este no suele ser el caso.

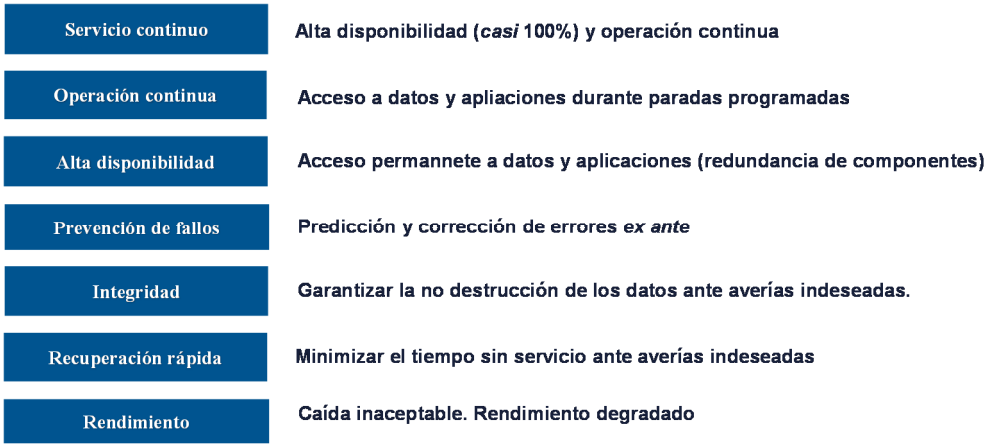

Ilustración 5: Diferentes hitos en el "continuo de disponibilidad"

Estas notas se centran y recogen fundamentalmente aspectos relacionados con la recuperación técnica de datos, sistemas y comunicaciones y con la restauración del servicio después de un desastre que no puede mitigar la alta disponibilidad local. Huelga decir que un DRP incluye más actividades que podemos enumerar genéricamente en la siguiente lista:

- **Activación**: Cuándo y cómo declarar una emergencia o desastre
- **Evaluación**: Determinación de la causa (raíz) del desastre y evaluación de impacto
- **Contención y control**: Medidas para evitar la propagación
- **Recuperación *express***: Restauración de al menos los sistemas críticos
- **Operación de emergencia**: Cómo operar durante la recuperación y hasta la vuelta a la normalidad
- **Restauración**: Vuelta a la operación normal eventualmente con los SS.II. en otro CPD.
- **Pruebas**: Cómo y cuándo se ha de testear el DRP.

El diagrama que sigue ilustra diferentes elementos sustantivos de un BCP/DRP

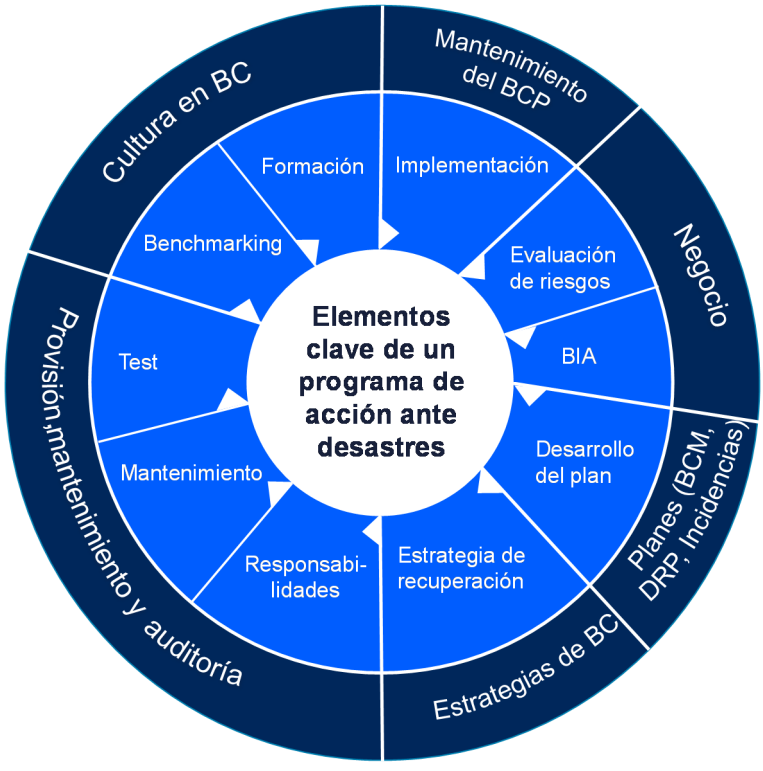

Ilustración 6: Elementos clave para actuación ante incidentes

En el siguiente apartado describimos con más detalle algunas de estas tareas.

2_ Tareas a ejecutar

Se recogen a continuación las tareas a ejecutar (y **buenas prácticas**) que con carácter general habrán de llevarse a cabo (y tenerse en cuenta) en la elaboración del DRP.

1. Realización y convalidación del **análisis de activos de información y riesgos (BIA-RA[4]:** *Business Impact Analysis and Risk Assessment***)**, así como su impacto en el negocio, las operaciones internes, la imagen, etc.
2. Identificación y clasificación de **situaciones de riesgo** hipotéticas: leves, menos graves y críticas.
3. Nivel y **alcance del desastre** en términos de incidencia sobre el "parque" de equipos de producción:
   - Afecta a una sola máquina o sistema de información o entorno. En este caso la alta disponibilidad local (HA) o redundancia puede ser suficiente para alcanzar un RTO cero.
   - Afecta a varias máquinas, varios sistemas de información o varios entornos
   - Afecta a todo el CPD o todo el edificio
4. Las aplicaciones y sistemas informáticos del cliente **se clasificarán de acuerdo a su nivel de criticidad**, estableciéndose claramente los RTO (Recovery Time Objetive) y RPO (Recovery Point Objetive) de cada aplicación y entorno funcional.
5. **Análisis coste-beneficio**: Después del BIA y del RA el análisis coste-beneficio es un proceso técnico-económico que permite establecer un balance de tipo financiero entre el coste –inversión– necesario para establecer cada opción y el ahorro que supone. A priori **son puntos ideales** (RPO y RTO) aquellos dónde el coste compensa la pérdida. Es decir aquellos en que recuperar más datos (menor RPO) o más rápidamente (menor RTO) resultaría antieconómico por implicar una inversión superior al valor de las transacciones/datos perdidas o al coste del negocio cesante.

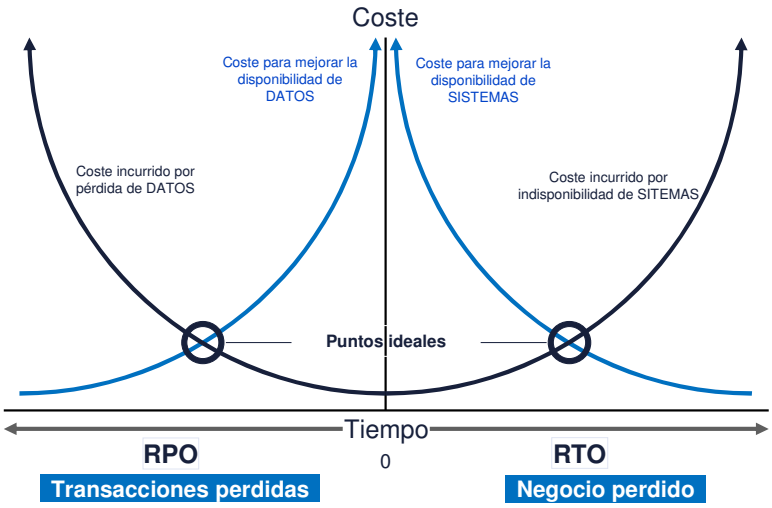

Ilustración 7: Análisis coste-beneficio

[4] **BIA**: *Process of analyzing activities and the effect that a business disruption might have on them.* (ISO 22300:2012). **RA**: *Overall process of risk identification, risk analysis, and risk evaluation.* (ISO Guide 73)

6. **Identificación de los responsables** de la activación y puesta en marcha del DRP. Los equipos han de estar preconstituidos, formados y motivados.
7. Señalización en su caso de un **centro de recuperación alternativo** (normalmente el CPD secundario o de respaldo). No siempre es necesario restaurar los SS.II. de un centro alternativo o secundario si es posible **restablecer la normalidad**, en un tiempo inferior al RTO, desde el centro de producción. (Qué significa en este contexto "restablecer la normalidad" es parte del contenido del DRP). En este punto conviene también caracterizar el *site* alternativo (si lo hubiere) como *cold*, *warm*, *hot* o *mobile* porque ello determina los procesos de recuperación de forma notable. Igualmente ha de tenerse en cuenta que la existencia de un centro secundario obliga a analizar con detalle los aspectos de la **WAN** (arquitectura, redundancia, **latencia, ancho de banda**) así como su optimización. (Las **herramientas de optimización**, deduplicación[5] y aceleración WAN pueden agilizar el tráfico de red *site to site* a un coste menor que el de usar redes más capaces o más rápidas).
8. Cuando se externaliza el CPD de recuperación alternativo y además los servicios asociados al DRP son efectuados por un tercero como un servicio recurrente de alto valor añadido hablamos de **DRaaS**.

   Asimismo conviene tener en cuenta que la recuperación puede hacerse **sin la necesidad de espacio físico** para servidores, sistemas periféricos o incluso conectividad de red. Todo "el respaldo" puede residir en un servicio de almacenamiento y proceso basado en la nube, listo para funcionar cuando sea necesario. Idealmente, las soluciones basadas en la nube pueden proporcionar otra línea de defensa para respaldar las operaciones de TI existentes (en este sentido es cada vez más importante la presencia de servicios de DR *cloud based*). Frente a un sitio de DR tradicional (CPD secundario, *on-premise* o externalizado) con un servicio de tipo **DRaaS *cloud based*** no se necesitan mantener una instalación remota para DR (y se obvian los gastos asociados al mantenimiento hardware de aquellos servidores inactivos provisionados para reflejar estrechamente el entorno *on-premises*). Además con el servicio *DRaaS cloud based*, la infraestructura para DR y las cargas de trabajo existen en la nube **sólo el tiempo que sea necesario**. En el momento en que no se necesiten podrán eliminarse y no supondrán ningún gasto (*cloud elasticity*)

   En definitiva, DRaaS *cloud based* aprovecha la copia en la nube para una recuperación rápida cuando una copia de seguridad local no está disponible. Esencialmente, DRaaS proporciona una capa adicional de recuperación más flexible al **combinar una copia basada en la nube** (BaaS, *Backup as a Service*) **con computación basada en la nube**, **automatización** basada en la nube y **orquestación** basada en la nube; todo ello con el objetivo de alojar los sistemas de información críticos de la organización[6].
9. **Procedimientos** a seguir según el nivel/alcance del plan y de la incidencia del desastre. De forma general estos procedimientos (correctamente documentados y accesibles) son del tipo: invocación del plan, acceso a interlocutores, constitución del gabinete de crisis, ejecución de acciones singulares, comunicaciones a terceros o internas, calendario de recuperación, proceso de reversión y similares. En la medida de lo posible se han de **minimizar las interdependencias** entre procesos lo que facilitará su solapamiento en el tiempo y por ende la disminución del RTO.

   Es importante asimismo que los procedimientos específicos del DRP se alineen con las políticas corporativas de **GRC** (*Governance, Risk and Compliance*): hay que pensar en la continuidad del negocio como parte esencial de la actividad general de GRC. Piénsese por ejemplo que los aspectos legales relacionados con la propiedad, custodia, acceso, retención, localización y uso de los datos pueden incidir en la implantación del DRP en un centro secundario de un tercero.

[5] **Deduplication***: The replacement of multiple copies of data—at variable levels of granularity—with references to a shared copy in order to save storage space and/or bandwidth.* The Storage Networking Industry Association (SNIA). SNIA Dictionary | 18th Edition.

[6] Aun siendo restrictivo, normalmente se usa **DRaaS** como sinónimo de DRaaS *cloud based*, mercado con un crecimiento compuesto anual (CAGR) estimado en más de un 40% (datos de 2016 a 2022).

10. Elaboración de un plan de **recuperación de servidores, comunicaciones y aplicaciones**, detallando recursos disponibles en activo, recursos reservados en *standby* pero comprometidos, configuración de los mismos, plan de trabajo, tiempo estimado de activación, dependencia entre subsistemas, comentarios, etc. Técnicamente esta es la fase determinante y más compleja, máxime si implica la intervención de terceros (operadores de telecomunicaciones, proveedores de servicio externos, desarrolladores, etc.).
11. **Basculación entre *sites***. El proceso de descargar/conmutar las cargas de trabajo (*workload*) desde el *site* principal de producción al *site* secundario de DR (ya sea por una avería, un desastre, un ataque, una prueba, etc.), de manera que la producción y la experiencia de los usuarios sean perturbadas lo menos posible, se denomina ***failover***. Un *failover* implica la restauración de aplicaciones, bases de datos, ficheros, configuración del sistema operativo, y estado[7].

    En sistemas complejos y/o distribuidos la activación de los diferentes subsistemas ha de seguir un riguroso orden debido a las dependencias existentes entre ellos, por lo que se ha acuñado un nuevo parámetro relacionado con las actividades de DR denominado **RCO (Recovery Consistency Objective)** que es una medida cuantitativa del **porcentaje de usabilidad** de los datos después de un *failover*.

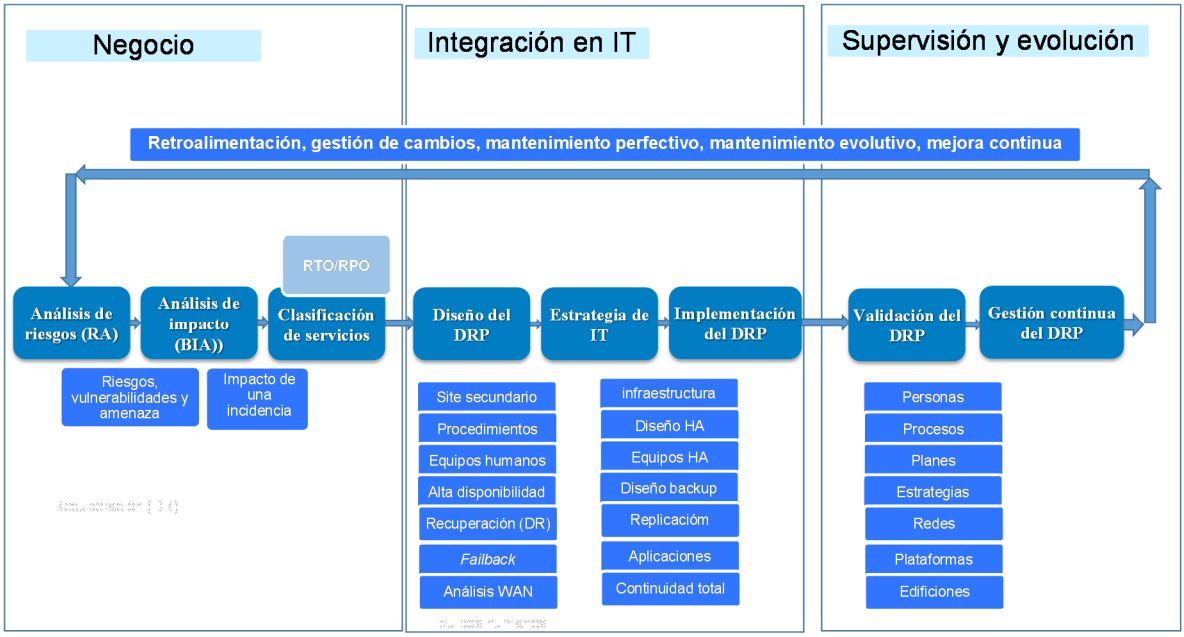

Ilustración 8: Flujo de actividades para abordar el DRP

12. **Reversión**. Se trata del proceso de diseño y planificación del ***failback***[8]**.** Téngase en cuenta que el *failover* es una conmutación al secundario que se debe considerar un **estado temporal**, por lo que el *failback* es un transición a un nuevo **estado permanente**.
13. Diseño de las **pruebas** de los procesos de recuperación del negocio. En caso de establecerse la ejecución de un simulacro de desastre la coordinación del mismo será competencia del responsable del DRP, que

[7] **Failover**: *The automatic substitution of a functionally equivalent system component for a failed one.* The Storage Networking Industry Association (SNIA). SNIA Dictionary | 18th Edition.

[8] A **failback** *operation is the process of returning production to its original location after a disaster or a scheduled maintenance period.* IBM Knowledge Center

comunicará (a propios y a terceros, como SP) la realización de las pruebas con la antelación pactada y suficiente.

14. Establecimiento de una metodología de **mantenimiento evolutivo** del plan que permita incorporar al mismo nuevos servicios a medida que estos son provisionados.

3_ Niveles de DR

Con un conocimiento preciso y exhaustivo de la plataforma de explotación, de su parametrización, de los mecanismos de acceso a la misma, de las medidas de seguridad, de las políticas de salvaguarda, etc.; después de un análisis de riesgos e impactos en el negocio de los potenciales incidentes; y tras una clasificación de aplicaciones y subsistemas se estará en condiciones de diseñar una **solución completa e integral** de Disaster Recovery. En este apartado abordamos esta cuestión que se corresponde, *grosso modo*, con las tareas de los últimos puntos de la enumeración del epígrafe anterior.

Suponemos que los sistemas de información del cliente se encuentran **totalmente operativos y eventualmente externalizados** (bajo el control del proveedor de alojamiento o proveedor de nube pública o privada), con los equipos y datos ubicados en los centros de proceso de datos de producción (*on premise*, externos o en la nube) y suponemos asimismo que se ha elegido –obedeciendo a criterios técnicos, operativos y regulatorios que aquí no se discuten– el/los centro/s de respaldo (del cliente, del proveedor o de ambos; físico o en la nube).

Como norma general hay que tener en cuenta que cualquier solución de BC/DR ha de ser capaz de **integrar** diferentes piezas en un solo producto aunque se puede implantar optando por **diferentes categorías o niveles (*tier*)**, con diferentes alcances, siendo el objeto del diseño del plan determinar qué *tier* es necesario para cada entorno funcional o sistema de información (en función de su criticidad para el negocio y por ende del RTO/RPO preestablecido). La suposición de que todas las cargas de trabajo se pueden proteger bajo un solo esquema de DR sin consideración a diferentes categorías o *tiers* conduce inevitablemente a soluciones subóptimas o directamente inservibles.

Los posibles planes para DR normalmente se ubican en los siguientes tres segmentos (que de hecho se sustancian en un continuo de soluciones):

- **Copias de seguridad y restauración**: es la solución más simple y básica para proteger y recuperar datos ante fallos. El proceso de copia de seguridad copia los datos en otro sistema de almacenamiento administrado por un servidor de backup. El servidor retiene las versiones copiadas de acuerdo con políticas predefinidas y reemplaza las versiones anteriores del archivo con versiones más nuevas. La política incluye el número de versiones y el tiempo de retención. Un cliente puede restaurar la versión más reciente de un archivo o puede restaurar versiones de un momento anterior. Los datos restaurados pueden reemplazar (sobrescribir) el original, o –y este es el caso que nos ocupa– **restaurarse en una ubicación alternativa** (para DR).

- **Recuperación rápida de datos**: Manteniendo una segunda copia de datos en disco, consistente en un punto en el tiempo (***snapshot***) lo más cercano posible al momento del fallo, se pueden reiniciar los sistemas y las aplicaciones sin tener que restaurar los datos y eventualmente volver a aplicar las actualizaciones que se han producido desde el momento del *snapshot* al objeto de minimizar la posible pérdida de un número mínimo de transacciones en vuelo. La recuperación rápida de datos se distingue de la disponibilidad continua principalmente por el nivel de automatización en la conmutación, *failover* y *failback*. (La tecnología de *snapshots* para backup y DR es muy empleada en entornos de cloud computing. Originalmente los *snapshots* proporcionan copias de seguridad *on-line* a las que se puede acceder rápidamente, a través de directorios especiales ocultos en el sistema de archivos, lo que permite recuperar archivos que se han eliminado o modificado accidentalmente. Conviene en todo caso tener presentes las diferencias entre snapshot y backup a nivel de seguridad, ocupación, coste, administración, consistencia de los aplicativos, tiempo de retención, granularidad de la recuperación, etc. De hecho cabría considerar los snapshot como la “fase inicial” del backup y no su alternativa *sensu strictu*).

  Conviene señalar también que aunque en las ciertas tecnologías de DR la operación de *failover* es automática (e.g. clústering local o remoto), en general esta tarea ha de ser preprogramada (con *scripting* manual o bien usando las herramientas de automatización u orquestación que suministran ciertas soluciones comerciales);

en ocasiones incluso es recomendable una intervención manual para evitar riesgos en la conmutación entre *sites* y su reversión.

- **Disponibilidad continua**: Las soluciones de disponibilidad continua integran servidores, almacenamiento, redes y software de automatización. Una agrupación especializada de servidores (*clúster)* ubicados en CPD diferentes realiza un conjunto predefinido de tareas necesarias para reiniciar la aplicación en caso de fallo en otro nodo del mismo CPD (fallo local) o **conmutar y ejecutar en otro CPD**. Todas las tareas están automatizadas y predefinidas.

De la segmentación esbozada se sigue que en todo plan de recuperación ante desastres se impone disponer de una copia de los datos fuera de las instalaciones principales susceptibles de sufrir el desastre. Existen dos mecanismos principales para la copia de datos: **el backup/snapshot y la replicación**[9]. La diferencia fundamental entre estas dos tecnologías es clara: la copia de seguridad o backup copia la totalidad de la imagen de un servidor, de un archivo, o de una base de datos (o los cambios incrementales desde la última copia de seguridad) en una **única operación que se repite periódicamente** mientras que la replicación implica la transferencia (si es entre *sites* a través de una red) continua o casi continua de bloques/lotes de disco; *ergo*, de información; la periodicidad de estas **transferencias por lotes** determinará la **sincronía** o **asincronía** de la réplica (obsérvese además que –contrariamente a lo que sucede con el backup– con la réplica no se necesita una operación de *restore* para acceder a los datos *salvados*) . La replicación sería por tanto la condición necesaria para implementar soluciones en el segmento de recuperación rápida o de disponibilidad continua. Actualmente una buena estrategia de DR implica backup (por ejemplo de VM) y réplica (por ejemplo de datos).

Existen tecnologías generales para estos grandes segmentos de DR con escalas crecientes de complejidad por lo que –aun siendo independientes– las clasificamos en categorías o niveles (a.k.a. *tiers*). La razón por la que existen múltiples niveles de DR es porque a medida que disminuye el objetivo de RTO las tecnologías óptimas de DR deben cambiar. O alternativamente: para un RTO dado siempre hay un conjunto particular de tecnologías de DR/BC de **precio y rendimiento óptimos** (ver ilustración 5). Además la categorización en niveles permite segmentar las soluciones factibles de DR en función de los SS.II. a proteger y su criticidad. En conjunto las diferentes soluciones/niveles de DR entran dentro de los tres grandes segmentos: copias de seguridad; recuperación rápida de datos y operación continua (total disponibilidad). En la siguiente tabla se da una idea de objetivos y coste relativo (a la inversión en el centro de producción principal) de los diferentes segmentos.

Nivel/segmento	Recovery Point Objetive (RPO)	Recovery Time Objetive (RTO)	Coste relativo (%)
Backup/Recovery	8 horas a más de 24 horas	12 horas a más de 48 horas	5 a 50
Recuperación rápida	10 minutos a 8 horas	1 horas a 12 horas	50 a 90
Disponibilidad continua	segundos a 10 minutos	menos de 2 horas	90 a 100

3.1. Primer nivel: copias de seguridad con almacenamineto fuera del CPD

El primer paso de un DRP son las **copias de seguridad**. Mediante la ejecución sistemática de copias de seguridad se garantiza la recuperación de la información con un RPO de como máximo 24 horas, si suponemos una política

[9] **Data replication**: *Continuously maintaining a secondary copy of data—possibly at a remote site—from a primary volume for the purposes of providing high availability and redundancy.* The Storage Networking Industry Association (SNIA). SNIA Dictionary | 18th Edition

de copias incremental diaria y total semanal o similar. Evidentemente el tiempo de recuperación dependerá mucho de la interdependencia de las aplicaciones y del tipo de desastre (virus, alimentación, avería fatal, etc.), dado que la mera restauración de datos no garantiza la operatividad. También la modalidad de backup (***file level*** o ***image level backup***) puede determinar el compromiso de RTO. Comoquiera que un backup permite la recuperación de datos, pero no evita el costoso tiempo de inactividad debido a los –en principio– largos tiempos de recuperación integral y operativa de los sistemas de información, en entornos virtuales se ha impuesto la modalidad de *image level backup*, frente a la más convencional en entornos físicos de f*ile level backup*, porque permite una rápida recuperación de un servidor virtual de forma integral (datos, sistema y aplicaciones).

Es evidente que el backup ha de almacenarse fuera del CPD principal para garantizar que en caso de desastre fatal los datos se encuentran íntegros y operativos (deben existir al menos dos **copias completas** –**full**– de los datos *on-site* y al menos una copia full ha de permanecer fuera –*off-site*– pero en formato "backup"). Es por ello que como primer estadio se propone en esta fase un traslado de copias de seguridad desde el CPD principal a un búnker seguro de almacenamiento pasivo (e.g. armario ignífugo). El mecanismo de recuperación –ya muy en desuso– suele denominarse **PTAM** por *Pickup Truck Access Method*. Hoy en día los requerimientos de almacenamiento se miden en TB o incluso PB –petabytes– por lo que resulta obvio que las soluciones PTAM resultan inmanejables. En principio y a este nivel sólo se exige el almacenamiento *off-site* del backup pero no se requiere necesariamente de *site* alternativo para la recuperación lo que puede alargar de forma intolerable el RTO, dado que la recuperación de un desastre implica buscar un *site* de recuperación alternativo al original (inoperativo a causa del desastre), instalar nuevos equipos de TI, transportar copias de seguridad de respaldo desde la instalación segura hasta el sitio de recuperación elegido, restaurar el sistema, los subsistemas y la infraestructura de la aplicación junto con los datos relacionados, y reiniciar la carga de trabajo (por lo general estas tareas pueden demorar varios días).

Algunas consideraciones sobre el backup[10] y virtualización

Las copias de seguridad (backup) o archivo (backup con tiempo de retención ilimitado) se llevan a cabo precisamente para sortear problemas de paradas, averías o desastres (DR) o –en el caso del archivo– por motivos regulatorios, legales o litigiosos. Los pasos para establecer un **buen plan de backup** pasan por: agrupar y tipificar los datos en función de su criticidad para el negocio; para cada tipo establecer los objetivos RTO y RPO; identificar la mejor infraestructura para las copias (cinta, disco); definir las políticas de backup en función del tipo de datos y la infraestructura de backup seleccionada; probar el correcto funcionamiento del servicio; y finalmente llevar a cabo un mantenimiento perfectivo y evolutivo de la/s solución/es.

Asimismo, y como se ha señalado, el servicio de copias de seguridad podrá ser prestado tanto para máquinas físicas a nivel de fichero (mediante agentes específicos), como para servidores virtuales (con la posibilidad del denominado *image level backup*). La tecnología *image level backup* es óptima para situaciones de *disaster recovery* al permitir restaurar un VM de forma íntegra en el punto de "toma del backup" (incluyendo ficheros específicos de aplicación, registro, etc.). Incluso, para minimizar el RTO en caso de desastre, se puede implementar una funcionalidad de recuperación instantánea o recovery in place (RIP). Un backup a nivel de imagen no es más que un *snapshot* (instantánea o copia en un punto del tiempo) que debe ser montado y restaurado antes de proceder a la recuperación de un fichero, por lo que para esta operación (restaurar un fichero dañado y/o borrado) es más eficiente el sistema tradicional de backup de ficheros; por contra recuperar un VM íntegro de un *file level backup* obliga a instalar el sistema operativo, las aplicaciones y el agente de backup y proceder a la restauración de los ficheros de datos, lo que consume mucho tiempo (más RTO).

La virtualización y la administración inteligente de máquinas virtuales han contribuido significativamente a mejorar y potenciar los servicios DRaaS. En entornos virtuales los sistemas operativos individuales (que residen dentro de máquinas virtuales) son "imágenes", es decir que son grandes archivos planos que se pueden **copiar/mover al sitio de recuperación** para una restauración rápida y completa de los servidores. De hecho se puede utilizar las

[10] Ver el Anexo I de este documento dónde se describe brevemente la oferta de **interhost_** para el servicio de copias de seguridad

imágenes migradas de los VM a un proveedor de cloud computing para "botar" (iniciar) desde ellas los hosts virtuales provisionados en la nube pública de dicho proveedor.

3.2. Segundo nivel: *Hot site* y *bare metal restore*

Una segunda categoría o nivel de DR implica disponer de un *site* secundario dónde llevar a cabo la recuperación. Se trata de un centro alternativo (***hot site***[11]) dónde se dispone de equipamiento (hardware y software) para recuperar los SS.II. afectados por el fallo. En el *site* alternativo se manejan los mismos procesos de datos que en el *site* principal. Si ocurre un desastre las copias de seguridad se emplean para la restauración en el *hot site*. Con este enfoque la restauración es más rápida ya que solo los datos, y no el sistema en sí, tienen que ser restaurados (como sucedería en la categoría anterior basada en *cold site*)

Como una mejora en este segundo nivel se puede optar –para equipamiento físico– por el denominado *bare metal restore* (se salvaguardan **datos y una imagen** del servidor de producción) al objeto de minimizar el RTO. Recuperar un servidor de producción en una ubicación alternativa puede ser extremadamente laborioso a nivel de sistema operativo, parches, aplicaciones básicas, etc. Con la tecnología *bare metal restore* (restauración completa) se crea una imagen del servidor de producción junto con la copia de los datos. Esta imagen es almacenada fuera (junto con los datos) y es el punto de partida para la rápida recuperación de los servidores de producción.

Comoquiera que la recuperación de un servidor desde una imagen no es evidente salvo que el hardware de origen y el de destino sean similares el mantenimiento de esta solución es complejo (compárese por ejemplo con la simplicidad y facilidad del *image level backup* de entornos virtuales donde la consistencia es necesaria sólo entre gestores de máquinas virtuales o **hipervisores** al objeto de evitar conversiones de VM). Cabe señalar que actualmente la tecnología *bare metal restore* permite restauración en hardware distinto (cambiando ajustes e incluyendo y activando controladores –*drivers*– para garantizar que el sistema operativo arranque de forma adecuada).

3.3. Tercer nivel: backup remoto en el CPD secundario (*electronic vaulting*)

Para evitar el trasiego de medios entre los CPD (*shipping*) y al objeto de mejorar el RTO/RPO la siguiente categoría de soluciones lleva a cabo la ejecución de copias de seguridad en el CPD secundario a través de una WAN o red de área extensa (***electronic vaulting***). Para ello es necesario habilitar un canal de comunicación entre *sites* de suficiente ancho de banda y configurar adecuadamente la aplicación de backup (incluyendo técnicas de optimización de la capacidad como comprensión, deduplicación, etc.). La solución implica además provisionar equipos (al menos los críticos) para la recuperación de los SS.II. en el CPD secundario/*hot site* (como en nivel previo) en el menor tiempo posible. Normalmente el *vaulting* remoto se efectúa entre servidores de backup (*server to server*) y las copias remotas se efectuarán sobre un array de discos (o sobre **VTL, virtual tape library,** sistema de backup basado en disco que emula una librería de cintas).

En algunos escenarios sólo ciertos sistemas de información, considerados críticos, son respaldados a través de la línea de comunicación (además con políticas de backup más exigentes), de manera que la solución de DR es un híbrido entre este nivel y los anteriores (siempre existe la opción de almacenar manualmente tanto la base de datos de backup –catálogo– como las copias de seguridad siguiendo esquemas similares a los de los niveles anteriores).

[11] Un CPD *hot site* mimetiza el CPD de producción y dispone de hardware y software operativo y disponible 24x7 para retomar en el mínimo tiempo –RTO– las operaciones. Por el contrario en un CPD *cold site* lo que hay disponible es básicamente espacio técnico (servicios básicos de energía, comunicación y controles ambientales) pero ningún equipo operativo, que habrá que configurar, junto con las conexiones, el software etc. en caso de desastre.

3.4. Cuarto nivel: Recuperacón rápida

Para mejorar los parámetros RPO Y RTO el segmento que hemos catalogado como de recuperación rápida incorpora varias categorías/niveles (*tier*) que comparten soluciones de **réplica** generalmente utilizando copia a disco en un punto en el tiempo (**PIT copy**[12]) o ***snapshots*** (ver la introducción de este epígrafe). Se trata de una imagen instantánea de un dispositivo de almacenamiento que se puede preservar como guía para su restauración, por lo que es una tecnología muy versátil para protección de datos.

Además de los *backups* basados en *snapshots* para la recuperación rápida se impone el uso de tecnología de **replicación síncrona o asíncrona** de datos en un segundo CPD, junto con la garantía de **integridad transaccional** provista a nivel de aplicación

Para poder abordar con éxito un proyecto de replicación es fundamental conocer la carga de trabajo y la **volatilidad de la información** (o frecuencia de cambios) al objeto de dimensionar la capacidad (en términos de ancho de banda y latencia) de la línea de datos entre *sites* necesaria para poder efectuar la réplica, que es más exigente en este aspecto que le backup remoto o *electronic vaulting* de la categoría anterior. (Ver la introducción de este epígrafe y la nota 9).

La réplica puede ser **síncrona o asíncrona**[13]. Aunque el primer mecanismo asegura que no existe pérdida de ningún dato (cualquier operación de i/o no finaliza hasta recibir el OK de ambas localizaciones) es muy sensible a la latencia de red y puede ser inaceptable por motivos de rendimiento (o precio). La réplica asíncrona no afecta al rendimiento pero implica que los datos de los *sites* pueden estar **desfasados unos segundos**.

Por fin el mecanismo de replicación se favorece en muchos casos mediante el empleo de herramientas ligadas o propias del hardware de almacenamiento. El disponer de dos cabinas (*a.k.a. arrays*) de discos de tecnología similar permite emplear herramientas propias del fabricante para réplicas de datos, lo que de nuevo redunda en una mejora notable del RPO. De hecho la replicación tradicional está basada en hardware y **redes de área de almacenamiento (SAN to SAN)** y es una solución eficiente y robusta (aunque dependiente de fabricante) pero extremadamente costosa. Con la tecnología de replicación hardware (entre cabinas o SAN to SAN) una misma solución simple –única– permite proteger diferentes plataformas software y de aplicación. Esta versatilidad la hace muy útil cuando coexisten sistemas críticos basados en diferentes aplicativos. Por el contrario la solución adolece de falta de soporte para entornos heterogéneos, es decir con cabinas diferentes. Habida cuenta de lo anterior muchas empresas están interesadas en la actualidad en soluciones de **replicación basadas en software** de mucho menor coste y especialmente apropiadas para entornos de virtualización.

Otra tecnología de replicación es la réplica continua o CDP (*Continous Data Protection*[14]) que proporciona en tiempo real replicación asíncrona a nivel de bloque y se usa tanto para soluciones de migración como recuperación ante desastres. La tecnología CDP se diferencia del backup en que no requiere un calendario de copias planificado

[12] ***Point-in-Time copy (PIT)***: *A fully usable copy of a defined collection of data that contains an image of the data as it appeared at a single point-in-time. A PIT copy is considered to have logically occurred at that point in time, but implementations may perform part or all of the copy at other times (e.g., via database log replay or rollback) as long as the result is a consistent copy of the data as it appeared at that point in time. Implementations may restrict point in time copies to be read-only or may permit subsequent writes to the copy. Three important classes of point in time copies are split **mirror**, changed **block**, and concurrent. **Pointer remapping** and **copy on write** are implementation techniques often used for the latter two classes.* The Storage Networking Industry Association (SNIA). SNIA Dictionary | 18th Edition

[13] **Asynchronous replication:** *A replication technique in which data must be committed to storage at only the primary site and not the secondary site before the write is acknowledged to the host. Data is then forwarded to the secondary site as the network capabilities permit.* **Synchronous replication:** *A replication technique in which data must be committed to stable storage at both the primary site and the secondary site before the write is acknowledged to the host.* The Storage Networking Industry Association (SNIA). SNIA Dictionary | 18th Edition

[14] ***CDP***: *A class of mechanisms that continuously capture or track data modifications enabling recovery to previous points in time.* SNIA Dictionary | 18th Edition

(*schedule*) por eso a la tecnología de *sanpshots* se la conoce a como ***near CDP***. La replicación CDP se realiza a nivel del sistema operativo, en lugar de hipervisor o SAN lo que permite el soporte de servidores físicos y virtuales.

Atendiendo a la aplicación, para bases de datos y en general sistemas transaccionales, y si el objetivo es disminuir el RPO, otra tecnología empleada es el denominado **remote journaling** (también *log shipping*) que copia el registro o diario de transacciones con periodicidad muy corta (en lugar de hacer una copia completa de la DB como en el caso de *electronic vaulting*) permitiendo restaurar copias coherentes de la información con mínima pérdida de datos (consistencia e integridad).

Para poder implementar la estrategia anterior se requiere aplicar las últimas transacciones/actualizaciones sobre el último backup válido de forma automática lo que reduce el RTO. Además se puede combinar la copia instantánea de la base de datos (*Point in Time Copy*) con el *remote jounaling* aplicando periódicamente los cambios en el *site* secundario sobre una base de datos sombra de la principal (***shadow***). En todos los casos estos mecanismos de disaster recovery dependen fuertemente de la aplicación (e.g. del sistema gestor de base de datos en uso) y hacen un uso exhaustivo de sus capacidades y herramientas propias (e.g. MS SQLserver Always on, Oracle RAC u otras). Asimismo requieren, en el sitio secundario, una infraestructura similar a la del sitio principal.

De hecho suelen considerarse niveles diferentes de DR aquellas réplicas dónde la **integridad transaccional** depende totalmente de la aplicación (que eventualmente hay que modificar y mantener para agregar la lógica de confirmación en dos *sites*), frente a aquellas dónde es el hardware de almacenamiento el que garantiza la consistencia, en este caso las empresas no tienen ninguna tolerancia a la pérdida de datos y necesitan restaurar los datos y las aplicaciones muy rápidamente.

3.5. Quinto nivel: *mirroring* y clúster geográfico

Si lo que se desea es minimizar tanto el RPO como el RTO y automatizar la operativa ante averías o desastres la tecnología de **clúster entre *sites*** es la más adecuada y constituye el estadio último de las denominadas arquitecturas de alta disponibilidad para DR. El clúster exige disponer de nodos similares en ambos *sites* y automatiza las operaciones de conmutación entre *sites*: *failover* y *failback*.

En este escenario se efectuará una replicación de datos síncrona y en tiempo real entre *sites*. Es lo que se denomina **mirroring**. La tecnología y mecanismos de la réplica dependerán de lo establecido en el nivel anterior, así como de la naturaleza de las aplicaciones (el clúster implemente una suerte de *software mirroring*, aunque también se puede emplear a este nivel un *storage mirroring* con automatización)

En un clúster los dos nodos pueden estar activos y procesando peticiones o transacciones o bien la configuración puede ser activo/pasivo. En todo caso es fundamental analizar y determinar los mecanismos de **distribución de carga y su balance global** (caso activo/activo) o de **conmutación** entre *sites* (activo/pasivo) y para ello es esencial conocer la naturaleza de las conexiones, los protocolos de acceso, los mecanismos de sincronización y acoplamiento entre nodos y en general es fundamental contar con un conocimiento "fino" de la aplicación de negocio a configurar en clúster (lo que permitirá por ejemplo emplear scripting *ad hoc* para automatizar las operaciones y garantizar la continua disponibilidad)

3.6. Prescripciones generales comunes

Una vez diseñado el plan de recuperación ante desastres (con las categorías que sean pertinentes dependiendo de la criticidad de los sistemas a proteger), se definirán y especificarán las **prescripciones técnicas** para:

- La supervisión, monitorización y administración del servicio

- La integración del grupo de soporte del cliente con el personal encargado de poner en marcha el DRP (si fueran distintos).
- La interlocución con los desarrolladores de las aplicaciones para integrar las mismas y nuevas funcionalidades dentro del DRP (definiéndose asimismo el modelo de relación).
- La ejecución con la periodicidad convenida, de un simulacro de desastre con la subsiguiente puesta en marcha del plan de crisis elaborado y documentado de forma precisa.

4_ Procedimientos organizativos y operativos

El **objetivo global** de un plan contingencias es dotar a la plataforma respaldada (entendida en sentido extenso), de los elementos necesarios para conocer qué hacer, cómo actuar y a quién o quienes responsabilizar durante una crisis o contingencia para mitigar y reducir los tiempos objetivos (RTO y RPO) de recuperación de los sistemas respaldados.

Anteriormente hemos esbozado diferentes categorías de soluciones cuya implantación y ejecución debe garantizar la continuidad de negocio y de los servicios TIC que el cliente pone a disposición de sus administrados y/o de sus propios empleados.

Una **consultoría** centrada en aspectos operacionales complementará el DRP con el objeto de acometer la definición de procedimientos organizativos y operativos extendidos a la capa de negocio/servicio, **definición de equipos** de dirección/coordinación, logística, recuperación y comunicación. Estos procedimientos han de abordar la ejecución de las tareas que siguen:

- Desarrollar los **procedimientos técnicos** de recuperación que llevarán a cabo los equipos técnicos de sistemas para la recuperación de los mismos, y documentarlos.
- Dimensionamiento de **equipos humanos**, definición de roles, responsabilidades y disponibilidad.
- Conformar los procedimientos operativos para la **logística, comunicados y plan de crisis** (o de respuesta a incidentes).
- Definición de las necesidades de **ubicación** de usuarios integrantes del equipo, espacios y salas alternativas.
- Definición de plantillas y **documentación** adicional necesaria para la ejecución del plan.
- Definición, diseño y documentación del plan de **pruebas** abordando:
  - Tipología de pruebas (extremo a extremo, parcial, global).
  - Calendarios periódicos y tentativos de realización de las mismas.
  - Establecimiento de criterios, necesidades y requerimientos para las pruebas según tipología.
  - Establecimiento de los escenarios de las pruebas según tipologías.
  - Establecimiento de objetivos y actividades preparatorias de las pruebas.
  - Información exhaustiva sobre las incidencias registradas en la ejecución de las pruebas.
- **Revisión recurrente** anual (u otra periodicidad) de procedimientos, con la modificación e inclusión/corrección pertinente de los procedimientos del plan afectados por los cambios de la solución de respaldo. Mantenimiento **perfectivo y evolutivo** del DRP
- Establecimiento de las dependencias con el proceso de **gestión de cambios**.
- Establecimiento de las dependencias con el plan de pruebas.

Como resultado se dispondrá de la documentación complementaria del **plan director de continuidad** incluido el Plan de Contingencia (DRP), así como el Plan de Pruebas necesario, las plantillas, comunicados y definiciones previas, así como la organización y responsabilidades concurrentes para la ejecución de dicho plan director.

5_ Roles y equipos

El **equipo de trabajo** y colaboradores necesarios para acometer exitosamente la elaboración del plan de continuidad global de negocio se esboza a continuación:

Por parte del proveedor del servicio de recuperación ante desastres:

- **Consultor** especialista BCRS (***Business Continuity and Recovery Specialist***). Participación en la etapa de definición del Plan Global como coordinador especialista y consultor de proyecto.
- Personal **técnico** especialista en BC/DR. Participación en la definición de los procedimientos técnicos de recuperación y participación en el diseño de las pruebas anuales.

Por parte del cliente

- **Responsable del servicio**. Dirección y Control. Colaboración en revisiones, diseño y toma de decisiones
- Personal de los **grupos de servicio** actuales del cliente. Participación en los procesos de revisión y definición de la organización, responsabilidades y procedimientos. Participación en las revisiones anuales. Integrantes de equipos de continuidad
- Responsables de las diferentes **áreas de negocio**. Colaboración parcial en revisiones y pruebas en lo que afecte a su área de actividad.

Aunque el plan de recuperación ante desastres y continuidad ha de enfocarse con una **metodología holística** cada departamento o área de actividad concernida ha de hacer su aportación tanto en el análisis de riesgo y criticidad como en la parametrización y metodología de recuperación. Un buen servicio es el que es capaz de **sumar e integrar** todas estas necesidades heterogéneas en un proyecto común.

6_ Anexo I. Servicio de copias de seguridad

El servicio de backup tiene la función de realizar copias de seguridad periódicas de aquella información de los servidores y sistemas de almacenamiento que se considera importante, vital, o crítica y que no debe ser borrada de forma inadvertida. Si un equipo en producción pierde la antedicha información, ésta ha de poder ser recuperada desde la copia de seguridad en el menor tiempo posible (**mínimo RTO**) y con la versión más actualizada o coherente posible (**mínimo RPO** y mínima pérdida de datos). No se trata por tanto de un servicio de provisión de un equipamiento de contingencia que pueda ser utilizado cuando sea necesario y/o en cualquier condición (*disaster recovery, business continuity, metrocluster,* etc.). Tampoco se trata de un servicio de archivo definitivo (período de retención infinito) de información consolidada (*read only*) que deba ser salvaguardada en el tiempo.

Servidores dedicados (físicos)

Para equipamiento físico dedicado el servicio de backup se implementa mediante el **modelo cliente/servidor**. El servicio se implementa en un **servidor de backup** principal y dedicado (con el **software de backup** adecuado) que "tomará" los equipos (servidores, aplicaciones, subsistemas de almacenamiento) del equipamiento alojado objeto del servicio como clientes. En estos clientes se instalarán **agentes específicos** (para sistema operativo, aplicación, etc. según la oferta contenida en el **catálogo de compatibilidad** del fabricante del software de backup) que son los que permiten el volcado de información sobre el dispositivo de backup, que es un array o *appliance* de discos integrado con la solución de backup.

La misma aproximación podría ser empleada en entornos virtualizados, pero la proliferación de máquinas virtuales y su movilidad conllevarían una carga extraordinaria sobre el hipervisor en términos de proceso, memoria, I/O, e incluso licenciamiento.

Servidores virtuales

Un servicio de backup diferenciado para máquinas virtuales está basado en la ejecución de una copia íntegra de la imagen de la VM (*virtual machine*), es el denominado ***image level backup*** (en contraposición al ***file level backup***). Comoquiera que un VM es simplemente un fichero con este método se procede a inmovilizar momentáneamente el VM (congelación o ***quiescing***) y efectuar una copia instantánea del mismo o *snapshot*. Es finalmente este *snapshot* el que se salvaguarda. El método ignora la naturaleza de los datos dentro del VM por lo que para minimizar el volumen de datos a copiar se emplean técnicas de deduplicación, reconocimiento de bloques pertenecientes a ficheros borrados y seguimiento de bloques cambiados, CBT, lo que permite copias incrementales y en definitiva reducir las ventanas de backup.

Cabe decir que un backup a nivel de imagen no es más que un *snapshot* que debe ser montado y restaurado antes de proceder a la recuperación de un fichero, por lo que para esta operación (recuperar un fichero) es más eficiente el sistema tradicional que mantiene una base de datos (**catálogo**) que permite el acceso directo y rápido a cada fichero salvaguardo; por contra recuperar un VM íntegro de un *file level backup* obliga a instalar el sistema operativo, las aplicaciones y el agente de backup y proceder a la restauración de los ficheros de datos, lo que consume mucho tiempo.

Filers

Para *appliances* servidores de ficheros en red se emplea el protocolo **NDMP** (*Network Data Management Protocol*) para efectuar backup de dispositivos **NAS (*Network Attached Storage*)** que no permiten la instalación de agentes de backup. Con este método además se descarga de trabajo al servidor de backup dado que el *stream* de datos a salvaguardar fluye directamente del *filer* (NAS) al repositorio (cinta u otro *filer* en configuración ***three-way backup***)

7_ Anexo II. Oferta comercial de servicios

Como proveedor de servicios gestionados en la nube y en CPD físico, **interhost_** brinda soluciones que permiten a las organizaciones implementar un programa/servicio de protección y replicación de datos, o contratar un servicio para implementar y operar un **programa completo de recuperación ante desastres** (vía *site* secundario o DraaS *on cloud*) que respalde y garantice la continuidad de sus negocios y permita cumplir con los requisitos comerciales (SLA, reputación, etc.) y regulatorios.

Para el servicio de recuperación ante desastres **interhost_** ofrece un portfolio de soluciones tanto comerciales como de ingeniería y puesta en marcha que abarcan los aspectos técnicos y operativos del proyecto. La oferta se complementa con los productos y servicios de **SATEC**, empresa matriz de **interhost_** e integrador de sistemas y soluciones con una dilatada experiencia en servicios TIC, servicios de protección de datos y específicamente en todos los aspectos – prospectivos, operativos, técnicos, legales, normativos– de un DRP.

Aspectos generales.

- **interhost_** dispone de dos CPD operativos (en la Comunidad Autónoma de Madrid y Principado de Asturias)
- De forma general **interhost_** ofrece tres posibles escenarios para ubicar los datos y aplicaciones a proteger:
  - **Secundario**: Un CPD de **interhost_** se constituye como **centro de secundario** del principal que se mantiene en las dependencias del cliente (*on premise*).
  - **Principal y secundario**: Un CPD de **interhost_** aloja el nodo de producción y un segundo CPD de **interhost_** constituye el secundario.
  - ***DRaaS on cloud***: La nube pública de **interhost_** almacena los datos de copias de seguridad (***BaaS***) y las réplicas de sistemas y aplicaciones contempladas en el DRP.
- Si es responsabilidad de **interhost_**, la **infraestructura de producción**:
  - Usa hardware de máxima calidad de vendedores reconocidos
  - Emplea elementos redundantes
  - Se **diseña y ofrece** con redundancia local y HA
- Infraestructura igual o similar en el sitio de recuperación secundario.
- Se dispone de una MMR (***Meet Me Room***) para proponer líneas de comunicación entre *sites* de alto ancho de banda y baja latencia (con amplia oferta de tecnologías y operadores).

Replicación

- *Log shipping*, *remote jounaling* u otros mecanismos, dependiendo de la aplicación (empleado cuando se exige el ACK de secundario para validar una transacción)
- Herramientas propietarias del vendedor
- Ejemplos de **aplicaciones más extendidas** para implantar replica entre *sites*:
  - Oracle: RAC
  - MSSQL: *always on*

- Archivos de Windows: DFS
- MS Exchange: DAG
- **Site Recovery Manager** (VMWare) integrado con *storage mirror* (SAN to SAN u otra tecnología)
- Otros

- **Almacenamiento en espejo síncrono**
  - Escritura en Y (ACK válido en ambos *sites*)
  - Metrocluster de NetApp
  - Solución de equilibrio de carga global (varios fabricantes)
  - Fronteras sin estado y replicación sincrónica para bases de datos
- Scripting *ad hoc* para automatizar siempre que sea posible cualquier operación necesaria para mantener los servicios.

Solución de software de respaldo y recuperación

- **Veritas Netbackup** como solución general de backup en entornos físicos y virtuales
- VM y sistemas Windows y Linux modernos: Veeam Availability Suite
- Para equipamiento físico, heredado (*legacy*) y DDBB: CommVault Simpana
- Copia de seguridad en disco
- Replicación a sitio secundario
- Integración de instantáneas (*snapshots*) con almacenamiento local
  - RPO de pocas horas o incluso minutos
  - RTO: recuperación de datos en minutos, recuperación de la aplicación según tareas automatizadas previas, herramientas de orquestación, etc.

Destino/media para hardware de respaldo y recuperación

- Sistemas de cintas para períodos de retención largos (archivo) (D2T)
- Sistemas de discos (NetApp) (D2D)
- Copia de seguridad en cascada en sistemas de disco y luego en sistemas de cinta (D2D2T)
- Copia de seguridad en cascada en sistemas de disco (primario) y réplica en disco (D2D2D)
- Instalación fuera del sitio principal para el sistema de almacenamiento de copias de seguridad: en disco (secundario, NetApp) y en cinta (secundario, VTL, *off site*/PTAM)
- Contrato de servicios de *vaulting* con terceros

8_ Anexo III. Radiografía de los servicios para DR

Al objeto de cualificar la importancia del servicio de recuperación ante desastres (DRS) recogemos a continuación las principales conclusiones de una reciente encuesta sobre el estado de la cuestión[15].

- Más de la mitad (50,4%) de los encuestados indicaron que su organización ha experimentado un **"evento desastroso"** en los últimos 24 meses.
- En los últimos 24 meses el **ransomware**, con un 36% de respuestas, fue seleccionado como la principal causa de "eventos desastrosos".
- El 89,4% de los encuestados asegura estar preocupado por el ransomware.
- La mayoría (55,3%) de aquellos que han experimentado un "evento desastroso" en los últimos 24 meses declararon que el **failover** al *site* secundario fue problemático o falló.
- La principal preocupación ante un desastre (es así para el 74,2% de las organizaciones encuestadas) es la pérdida de **productividad**.
- El 89,6% de los CIO y responsables de TI aseguran que la capacidad de su empresa para responder rápidamente ante un desastre es cada año más importante para su organización.
- El 88,1% de los encuestados usarían la/s nube/s pública/s como su *site* secundario si únicamente tuvieran que pagar cuando la/s necesiten, es decir cuando se activa el DRP (por desastre, test u otras causas).
- Las tres cuartas partes (74,9%) de las organizaciones declararon que su **presupuesto para DRS** ha aumentado en los últimos 12 meses.
- Además, en los próximos 24 meses, el 67,3% de los CIO esperan que aumente su presupuesto para DRS.
- El objetivo prioritario a la hora de contratar DRS es **minimizar el RTO**.

[15] The State of Enterprise Data Resiliency and Disaster Recovery 2019. Datrium