Tema

5

Administración de Sistemas

Plan de Recuperación de Desastres

Universidad Francisco de Vitoria
UFV Madrid

Grado en Ingeniería Informática
Escuela Politécnica Superior

Objetivos y resultados de aprendizaje

- Conocer los principios básicos de los planes de continuidad de negocio y de los planes de recuperación de datos.

- Los objetivos específicos consisten en:

  - ✓ Conocer los diversos aspecto del PCN.
  - ✓ Conocer los tipos básicos de Backup y Replicas
  - ✓ Definir estrategias de Respaldo

Evaluación del tema

- Los resultados de aprendizaje correspondiente a este tema se evaluarán con los siguientes tipos de pruebas:

  - ✓ Pruebas escritas de carácter teórico
  - ✓ Práctica
  - ✓ Trabajo Autónomo (“Estrategia de Restauración”)

Bibliografía

- Para obtener más información puedes consultar:

  - ✓ metad_plan_de_contingencia_y_continuidad_de_negocio.pdf (en Canvas)
  - ✓ https://www.stackscale.com/es/blog/plan-de-disaster-recovery/

Índice de contenidos

- ✓ PCN
  - ✓ Fases
  - ✓ Criterios de Criticidad
- ✓ PRD
  - ✓ Backup
  - ✓ Replica

PCN

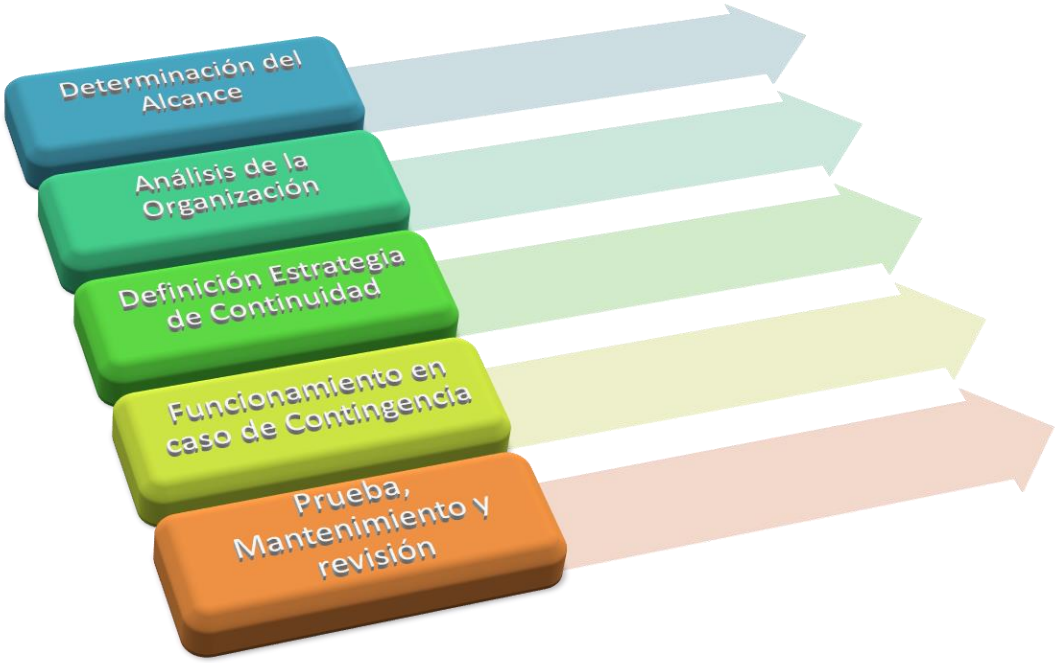
Universidad Francisco de Vitoria UFV Madrid

- El plan de continuidad de negocio está pensado y organizado para que el impacto que puede producir la interrupción del servicio informático sobre el resto de la compañía sea mínimo, restaurando sistemas y comunicaciones en el menor tiempo posible con todos nuestros empleados y colaboradores.

- *"…regularemos los mecanismos a poner en marcha en caso de un incidente grave de seguridad. Estos mecanismos nos ayudarán a mantener el nivel de servicio en unos límites predefinidos, establecerán un periodo de recuperación mínimo, recuperarán la situación inicial anterior al incidente, analizarán los resultados y los motivos del incidente, y evitarán la interrupción de las actividades corporativas.*
- *En caso de desastre, el hecho de tener definido y poder aplicar un Plan de Contingencia y Continuidad de Negocio repercutirá positivamente en nuestra imagen y reputación, además de mitigar el impacto financiero y de pérdida de información crítica ante estos incidentes."*(1)

PCN

- Fases



- ✓ ¿Qué activos se incluyen?.
  - ✓ Los de mayor Criticidad(*)
- ✓ Análisis de la Organización.
  - ✓ Reuniones
  - ✓ Análisis de Impacto
  - ✓ Análisis de Riesgo
- ✓ Para establecer la Estrategia de Continuidad, debemos disponer de la información siguiente:
  - ✓ Procesos afectados (tiempos y requisitos de recuperación).
  - ✓ Riesgos de la Infraestructura IT.
- ✓ (Funcionamiento: siguiente diapositiva)*
- ✓ Es primordial la realización de pruebas y adecuación a los cambios en la organización
  - ✓ Los cosos reales son, auqneu no deseados, la mejor batería de prueba y revisión

PCN

Universidad Francisco de Vitoria UFV Madrid

- Funcionamiento

PCN

Universidad Francisco de Vitoria UFV Madrid

- Niveles de Criticidad(*)

Críticos	Sus funciones no pueden ser ejecutadas a menos que sean reemplazados por recursos idénticos Costo de interrupción es muy alto
Vitales	Sus funciones pueden ser ejecutadas manualmente durante un periodo corto Mayor tolerancia a las interrupciones Costos de interrupción menores
Sensitivos	Sus funciones pueden ser ejecutadas manualmente durante un periodo relativamente largo Mientras se hace manualmente requiere plantilla adicional Costos de interrupción medios
No Críticos	Sus funciones pueden ser interrumpidas durante un periodo relativamente largo, con poco o ningún costo.

PRD

Universidad Francisco de Vitoria UFV Madrid

Tipos de Controles a Establecer

Preventivos

Tratan de evitar el hecho.

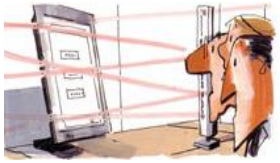
Amenaza

Plataforma Informática

Operatividad

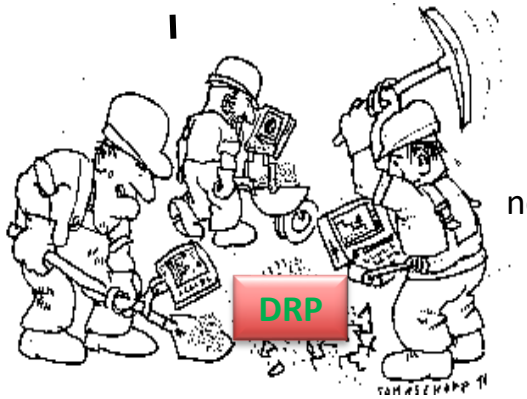
T_{min}

Disuasivos



Detectivos

Cuando fallan los preventivos, para tratar de conocer cuanto antes el evento.



Correctivos

Permiten la vuelta a la normalidad cuando se han producido incidencias.

PRD

Universidad Francisco de Vitoria UFV Madrid

- Un plan de recuperación ante desastres (del inglés Disaster Recovery Plan) es un proceso de recuperación que permite a las empresas recuperar los datos y aplicaciones de misión crítica en el menor tiempo posible.

- Los activos sobre los que se define un DRP son el hardware y el software crítico, natural o causado por humanos.

- El objetivo es que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre.

- Los conceptos clave a la hora de definir un DRP son “Alta Disponibilidad” (consiste en la capacidad de un sistema para asegurar la continuidad de los servicios) y Respaldo (Salvaguardas de la información crítica que permite su restauración en caso de perdida o fallos de su integridad).

PRD

Universidad Francisco de Vitoria UFV Madrid

- En el caso de un desastre que impacta sobre la continuidad de los servicios, debemos ser capaces de restaurar estos en el menor tiempo posible y con un rendimiento lo más cercano posible al instante previo al desastre.
- Es impórtate definir tres parámetros que nos permitirá definir y evaluar la corrección de nuestro DRP:

  - RTO: (Recovery Time Objetive) es el tiempo máximo durante el cual es aceptable que se interrumpa la actividad de la empresa. Es decir, el tiempo que podemos soportar que dure una interrupción antes de que empiece a perturbar la actividad normal del negocio.
  - RPO: (Recovery Point Objetive) es el punto previo en el tiempo al que podemos permitirnos volver para recuperar los datos y funcionalidades de la empresa. Es decir, representa la cantidad de datos que la empresa está dispuesta a perder entre la última copia de seguridad y una contingencia.
  - ROL (Revised Operating Level). Este sería el nivel mínimo de recuperación que debe tener una actividad para que se considere recuperada. Dependencias con otros procesos, ya sean internos o con proveedores externos.

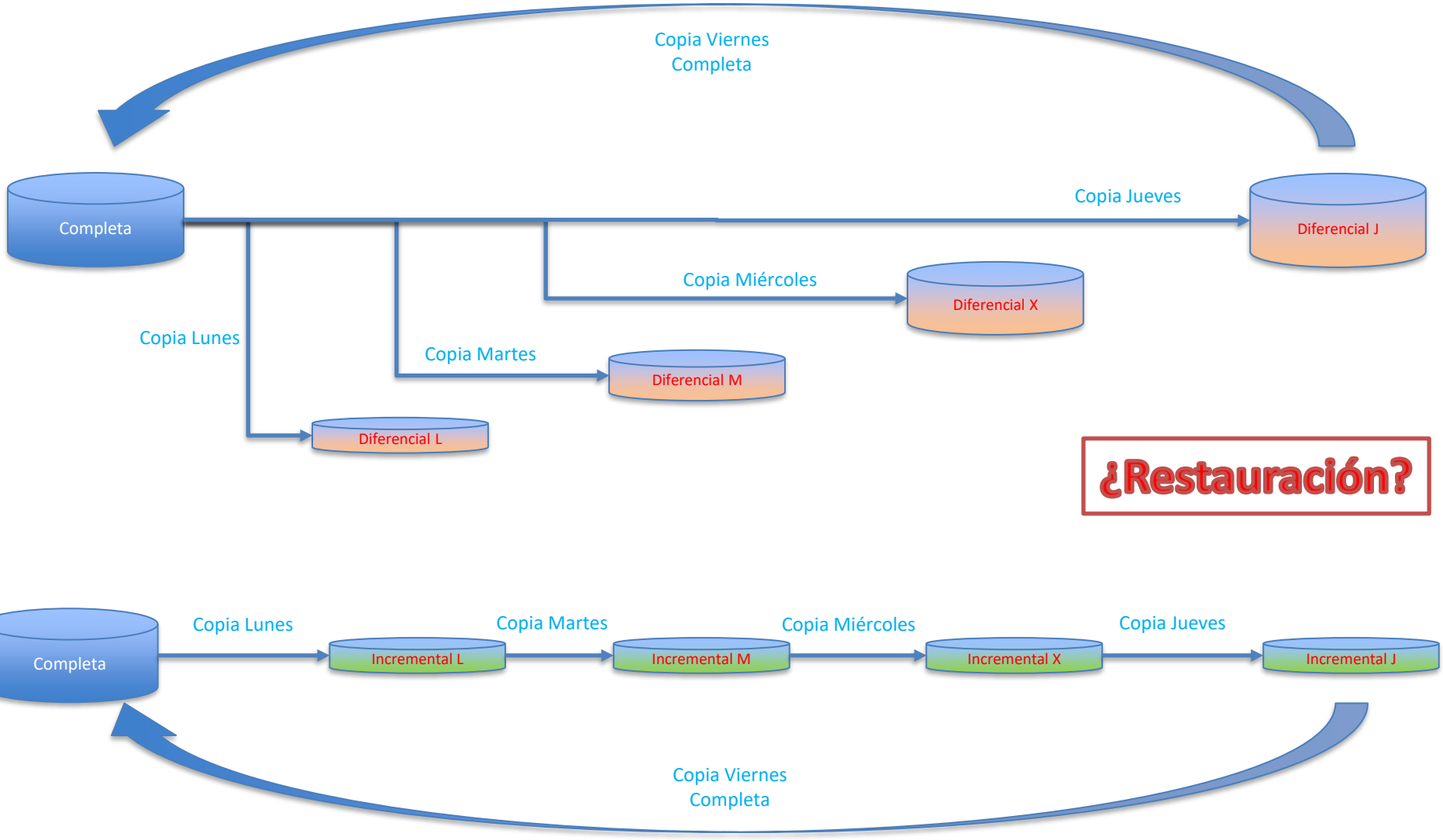
PRD

Universidad Francisco de Vitoria UFV Madrid

- Backup: Crea una cadena de respaldo independiente en la ubicación secundaria.
- Regla 3 2 1
  - La norma establece que debes tener al menos tres copias de tus datos
  - Dos de las copias de seguridad deben estar almacenadas en diferentes tipos de medios, y al menos una copia de seguridad debe estar almacenada fuera del sitio o en la nube.
- Tipos Básicos
  - Backup Completo
  - Backup Incrementales: hace una copia de seguridad de los cambios realizados desde el último backup (completo o incremental).
  - Backup Diferenciales: contiene todos los datos que han cambiado desde la última copia de seguridad completa.

PRD

Universidad Francisco de Vitoria UFV Madrid



PRD

Universidad Francisco de Vitoria UFV Madrid

- Replica: Permite tener otra copia a la que acceder en caso de desastre.

- Síncrona
  - ❖ Proporciona un RPO muy cercano a Cero para los datos. Dependerá del ancho de banda.
  - ❖ Requiere de mayores recurso.
  - ❖ Requiere ACK (ACKNOWLEDGEMENT /acuse de recibo) en ambos sitios. Retrasa el proceso
- Semi-Síncrona
  - ❖ Asíncrona: Se inicia la replica al sitio remoto después de que los datos están correctamente escritos en la fuente (ACK).
  - ❖ El RPO proporcionado depende de su configuración y recursos