

# Continuidad en las operaciones de negocio

ADR - UTN - FRBA - 2020

# **Plan de contingencia y recuperación ante desastres**

# Plan de contingencia y recuperación ante desastres

Existen una variedad de riesgos que pueden afectar significativamente las operaciones de IT:

- ▶ Desastres naturales
- ▶ Pérdida del suministro eléctrico
- ▶ Fallas de hardware/software
- ▶ Errores humanos

Un Plan de Contingencia incluye las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una compañía ante un desastre.

# Plan de contingencia y recuperación ante desastres

## Recovery Time Objective (RTO)

**Tiempo que pasará una infraestructura antes de estar disponible.**

Para reducir el RTO, se requiere que la Infraestructura (Servidores, Redes, Almacenamiento, Base de Datos, Aplicaciones, etc) esté disponible en el menor tiempo posible pasado el evento de interrupción.

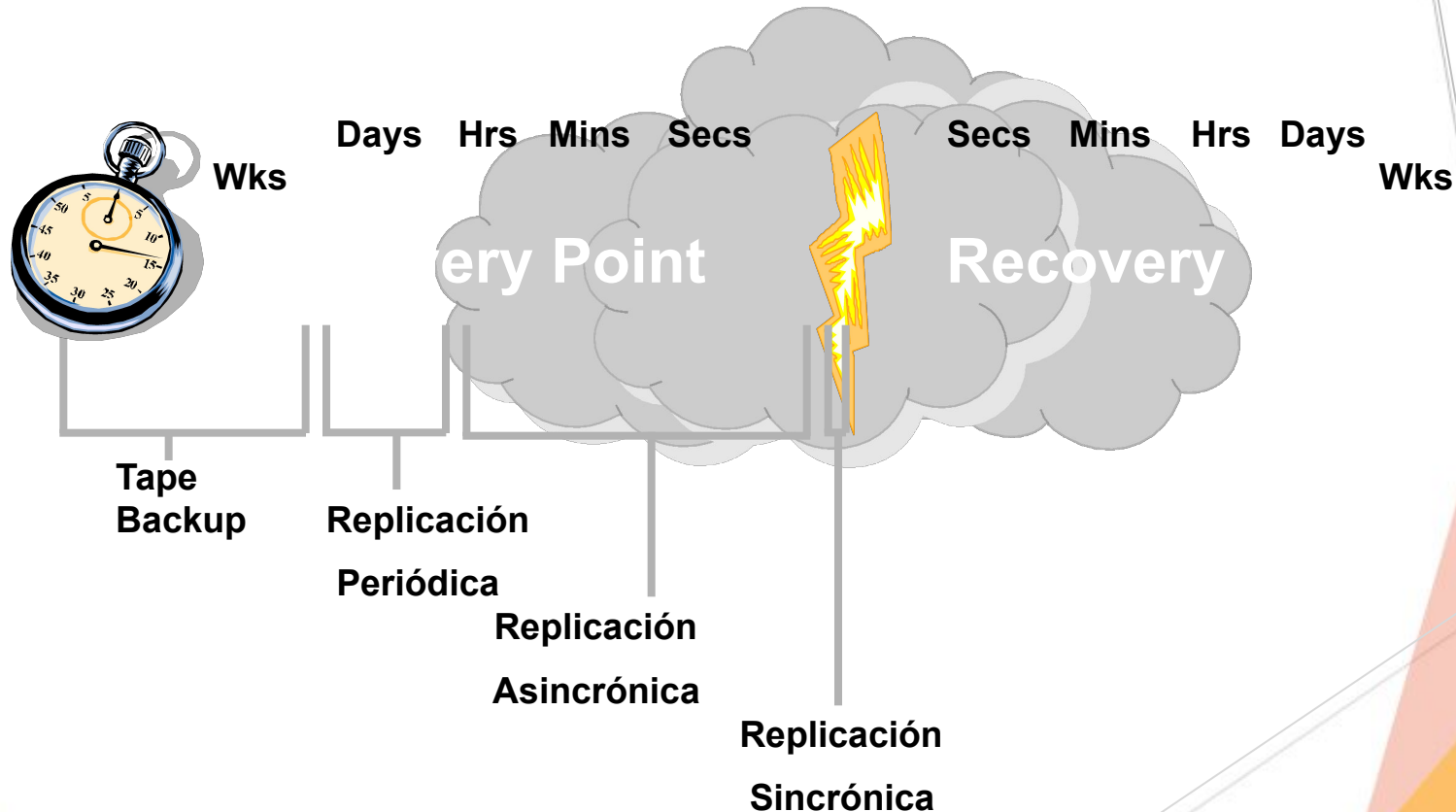
## Recovery Point Objective (RPO)

**Representa cuantos datos está dispuesta a perder la organización ante la ocurrencia de un incidente.**

Para reducir un RPO es necesario aumentar el sincronismo de réplica de datos.

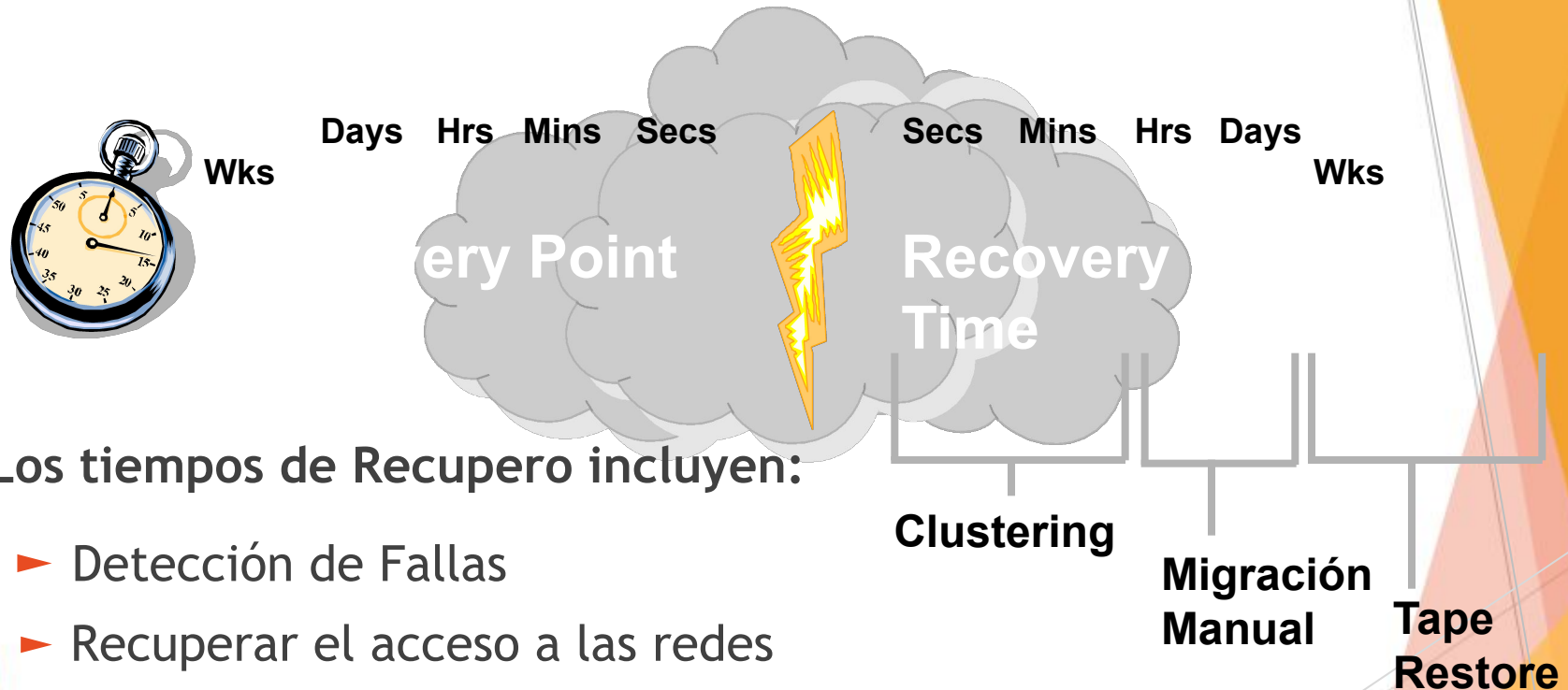
# Plan de contingencia y recuperación ante desastres

## Tecnologías de Replicación - RPO



# Plan de contingencia y recuperación ante desastres

## Tecnologías de Recuperación - RTO

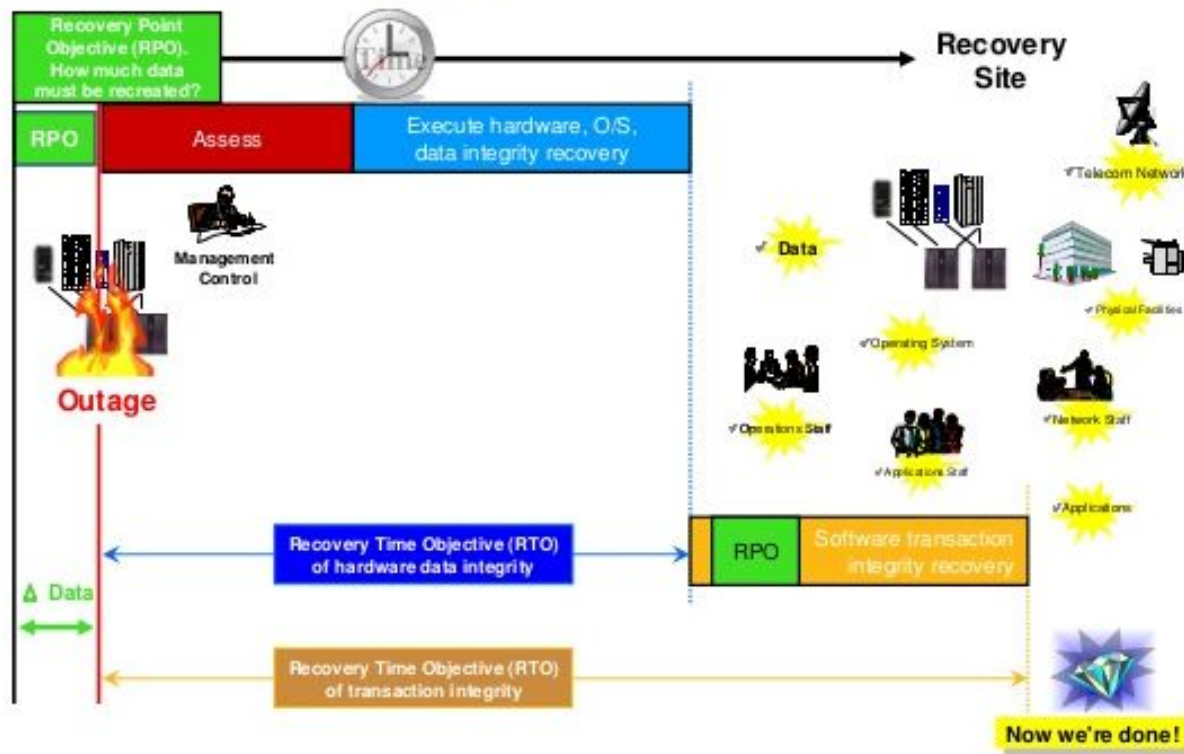


Los tiempos de Recupero incluyen:

- ▶ Detección de Fallas
- ▶ Recuperar el acceso a las redes
- ▶ Recuperar los datos
- ▶ Restaurar las Aplicaciones

# Plan de contingencia y recuperación ante desastres

Timeline of a Disaster Recovery



# Plan de contingencia y recuperación ante desastres

## Estrategias de protección de datos

Copias de resguardo en discos locales y externos:

### **Ventajas:**

- ▶ Rápido acceso
- ▶ Integración con aplicaciones y bases de datos

### **Desventajas:**

- ▶ Costo alto
- ▶ No es transportable a otro datacenter
- ▶ Si la falla se produce en el datacenter no puedo recuperar el dato

Copias de resguardo periódicas en cinta, sin y con almacenamiento de manera externa en discos locales y externos:

### **Ventajas:**

- ▶ Costo bajo
- ▶ Transportable a otro datacenter

### **Desventajas:**

- ▶ Requieren mayor tiempo de recupero



# Plan de contingencia y recuperación ante desastres

## Estrategias de protección de datos

Replicación de datos en sitio externo:

### **Ventajas:**

- ▶ Permite tener un resguardo de los datos fuera del datacenter principal

### **Desventajas:**

- ▶ Implica un costo en licencias de replicación
- ▶ No me permite continuar la operación ante una contingencia en el datacenter principal

# Plan de contingencia y recuperación ante desastres

## Estrategias de protección de datos

Replicación de datos en centro de datos externo implementado como sitio de contingencia. (Para garantizar continuidad de negocio offsite)

### **Ventajas:**

- ▶ Ante una contingencia en el datacenter principal se puede continuar la operación en el datacenter de contingencia
- ▶ Permite volver a operar rápidamente (depende del RTO) y de forma más sencilla (comparado con backup y restore de cintas)

### **Desventajas:**

- ▶ Representa un costo alto dado que se debe duplicar la infraestructura necesaria para operar
- ▶ Implica un costo en licencias de replicación

# Plan de contingencia y recuperación ante desastres

## Medidas para la recuperación ante desastres:

### **Medidas Preventivas:**

- ▶ Acciones para evitar la ocurrencia de eventos no deseados

### **Medidas de detección:**

- ▶ Controles para la detección de eventos no deseados

### **Medidas correctivas:**

- ▶ Acciones para recuperar la operatoria de los sistemas

**Consultas...**