



# T10 : Resiliencia

## Introducción

• pilares de la Seguridad de la Info:



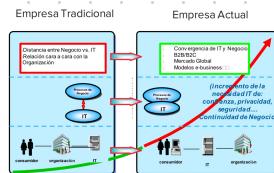
Causas disponibilidad de los sist. Info

Riesgos Crecientes

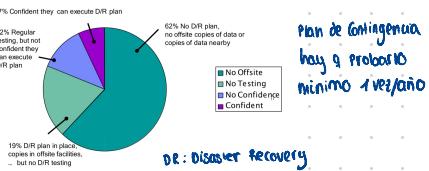
- Catástrofes atmosféricas
- Terrorismo
- Ciberataques

Riesgos Decrecientes

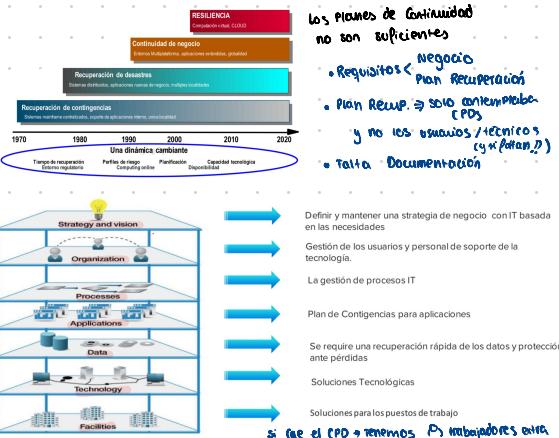
- Incendios
- Fallo infraestruct. edificios
- Falta de servicios



¿Dónde están la mayoría de hoy en día?  
soluciones disponibilidad

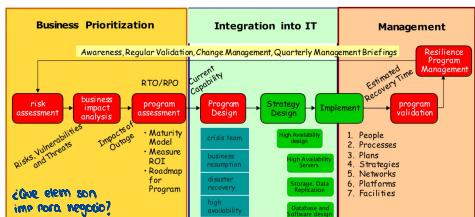


## Evolución de la soluciones



Antes: "Experimenta y Reacciona" Ahora: "Anticiparse y Ajustar"  
Resiliencia  $\Rightarrow$  que se note lo menos posible que ha habido un impacto

## Requisitos de Resiliencia en un Plan de Continuidad de Negocio (PCN)

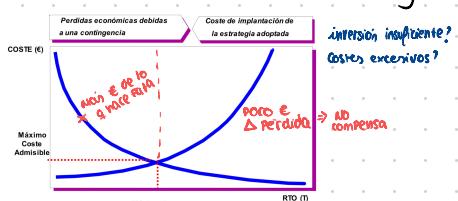


Protección de datos IT  Alta disponibilidad operaciones continuas Recuperación ante desastre

RPO : Recovery Point Objective  
RTO : Recovery time objective

 <b>desigualdad</b> <b>RTO</b> depende de lo que tenemos	<b>RPO</b> depende de los términos de la ecuación
<b>Planteado</b> <b>premiso ente</b>	<b>copia</b> $\leftrightarrow$ <b>cada</b> <b>RPO</b> $\leftrightarrow$ <b>únic</b> <b>Juan</b>

Balance coste solución ↔ pérdidas por contingencia



# T10 : Resiliencia

## Normativa y Mejores Prácticas

### Ley de Resiliencia Operativa Digital (DORA) de la UE

Digital Operational Resilience Act - Nueva ley de la UE (10/2020) para codificar la forma en que las entidades financieras gestionan el riesgo digital.

- La resiliencia operativa digital es la capacidad de las empresas de garantizar que pueden soportar perturbaciones y amenazas relacionadas con el entorno TIC.

- Ambitos de la gestión de riesgos de las TIC sobre la Ley DORA
  - Gestión de riesgos
  - Notificación de incidentes
  - Prueba de resiliencia operativa digital
  - Riesgo de terceros en materia de TIC
  - Intercambio de inteligencia



### Convenios de Gestión de la Continuidad de Negocio exigidos por el Banco de España:

- Análisis del impacto sobre el negocio:
- Estrategia de recuperación
- Planes de continuidad del negocio:
- Programas de comprobación de la eficacia de los planes
- Programas de divulgación
- Programas de comunicación y gestión de crisis.



## Normas ISO y Estándares

### BS 25999 / ISO 22301

① Prácticas y Soluciones para Gestión Continuidad Negocio

② Desarrollo + Implementación SGCN

Sist. de Gestión cont. Negocio

④ ISO 22301 → § 3 Fases

#### Fase Inicial

- Identif. requisitos
- Obj. & Alcance
- Tratamiento Riesgos

#### Implement. Sistema

- Analisis impacto riesgos
- Estrategia
- Implement. PCN
- Sensibilización Promoción
- Documentación

#### Revisión & Mantenimiento

- Ejercitación PCN
- Analisis resultado
- Planes Comunicación
- Acciones correctivas
- Revisión & Mantenimiento

ANALISIS DE RIESGOS ⇒ cada vez es más difícil PREDICIR riesgo

¿ES IMPORTANTE?

IMP Hacer BIA: Business Impact Analysis

### ISO 22316: 2017

#### seguridad y Resiliencia

- Resiliencia Organizacional
- Norma → Mayor capacidad <sup>anticipar</sup> abordar riesgos/vulnerab.
- Mayor <sup>Coordinación</sup> Integración disciplinas de gestión para mejorar coherencia de actuación
- Recomendación: hacer **BIA** Análisis de Impacto al Negocio
- Guía para seguir proceso + documentar

### ISO 22316: 2020

#### seguridad y Resiliencia

capacidad de una empresa para <sup>absorber</sup> adaptarse a los imprevistos, sin dejar de cumplir su obj. a alcanzar

1 Compromiso de los órganos de Dirección

2 Estructura de gobierno

3 Asegurar inversión en actividades de resiliencia organizacional

4 Sistema de soporte a la gestión

5 Evaluación continua

6 Comunicación