

Continuidad de Negocio

José A. Mañas < <http://www.dit.upm.es/~pepe/> >
Dep. de Ingeniería de Sistemas Telemáticos
E.T.S. Ingenieros de Telecomunicación
Universidad Politécnica de Madrid

24.2.2018

- Es improbable un desastre; pero somos muy vulnerables
 1. dependencia creciente de la tecnología
 2. interdependencia de los proveedores
 - su problema es mi problema
 3. un acto individual puede tener consecuencias planetarias
 4. la competencia [feroz] no perdona detenciones prolongadas o, simplemente, apreciables por los usuarios
REPUTACIÓN
 5. por obligación legal
o por regulación sectorial
sectores regulados | operan con licencia administrativa

dit

windsor – 13.2.2005



incident

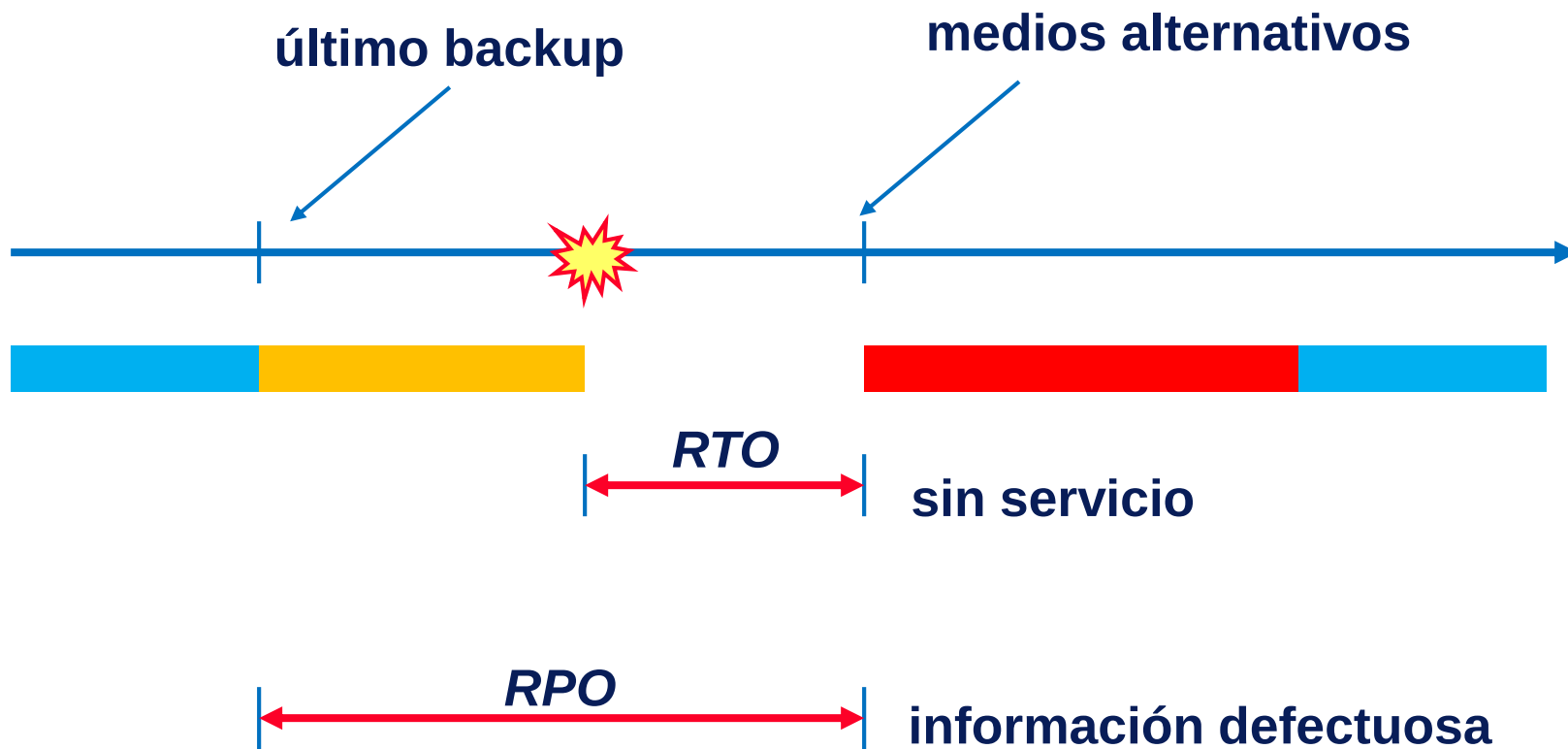
- situation that might be, or could lead to, a disruption, loss, emergency or crisis

disaster

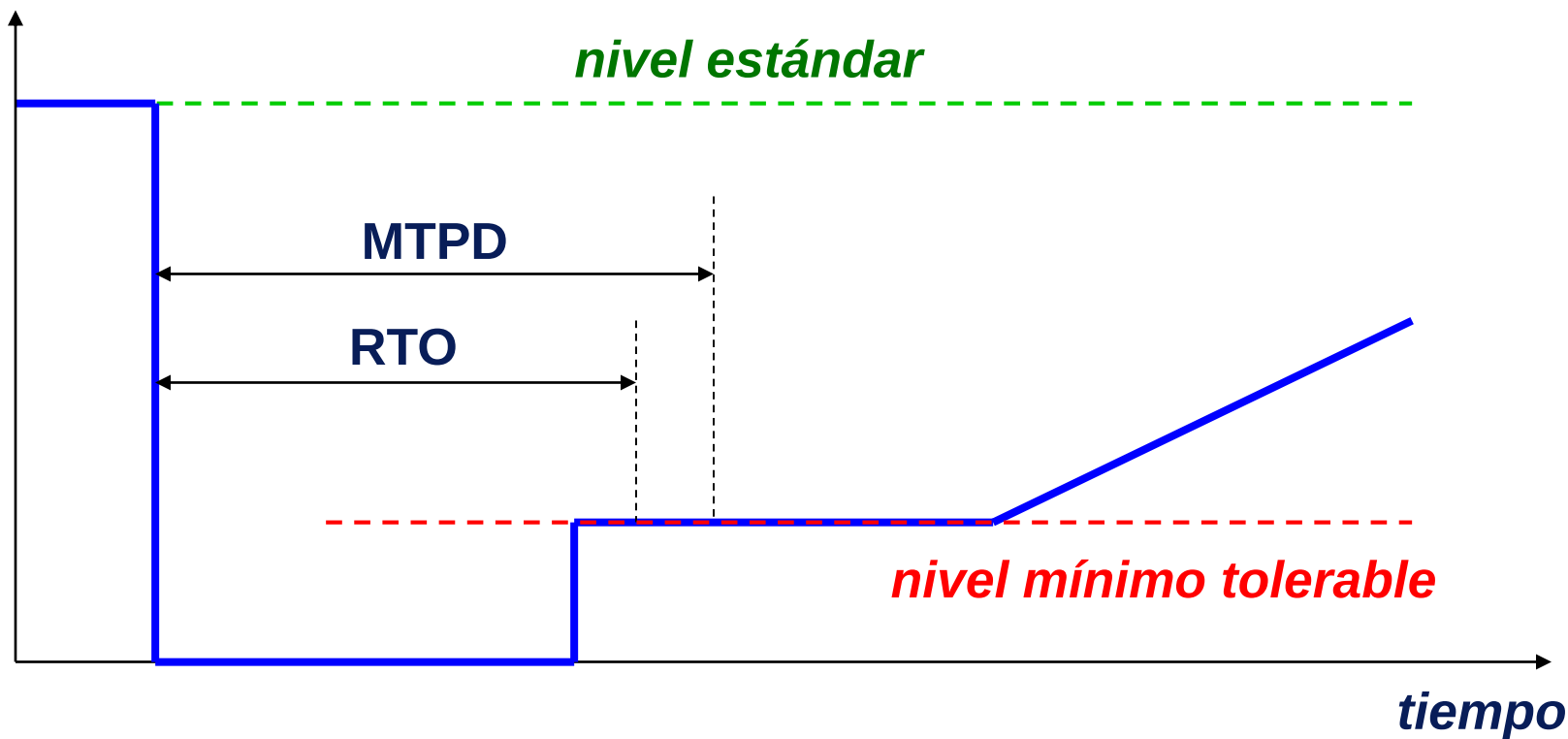
- situation where widespread human, material, economic or environmental losses have occurred which exceeded the ability of the affected organization, community or society to respond and recover using its own resources

dit

tiempos



nivel de servicio



MTPD - maximum tolerable period of disruption

- time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable

RTO - recovery time objective

- period of time following an incident within which product or service must be resumed, or activity must be resumed, or resources must be recovered.

RPO - recovery point objective

- point to which information used by an activity must be restored to enable the activity to operate on resumption
- NOTE Can also be referred to as “maximum data loss”.

resiliencia

- Capacidad de los sistemas para seguir operando pese a estar sometidos a un ciberataque, aunque sea en un estado degradado o debilitado. Así mismo, incluye la capacidad de restaurar con presteza sus funciones esenciales después de un ataque.

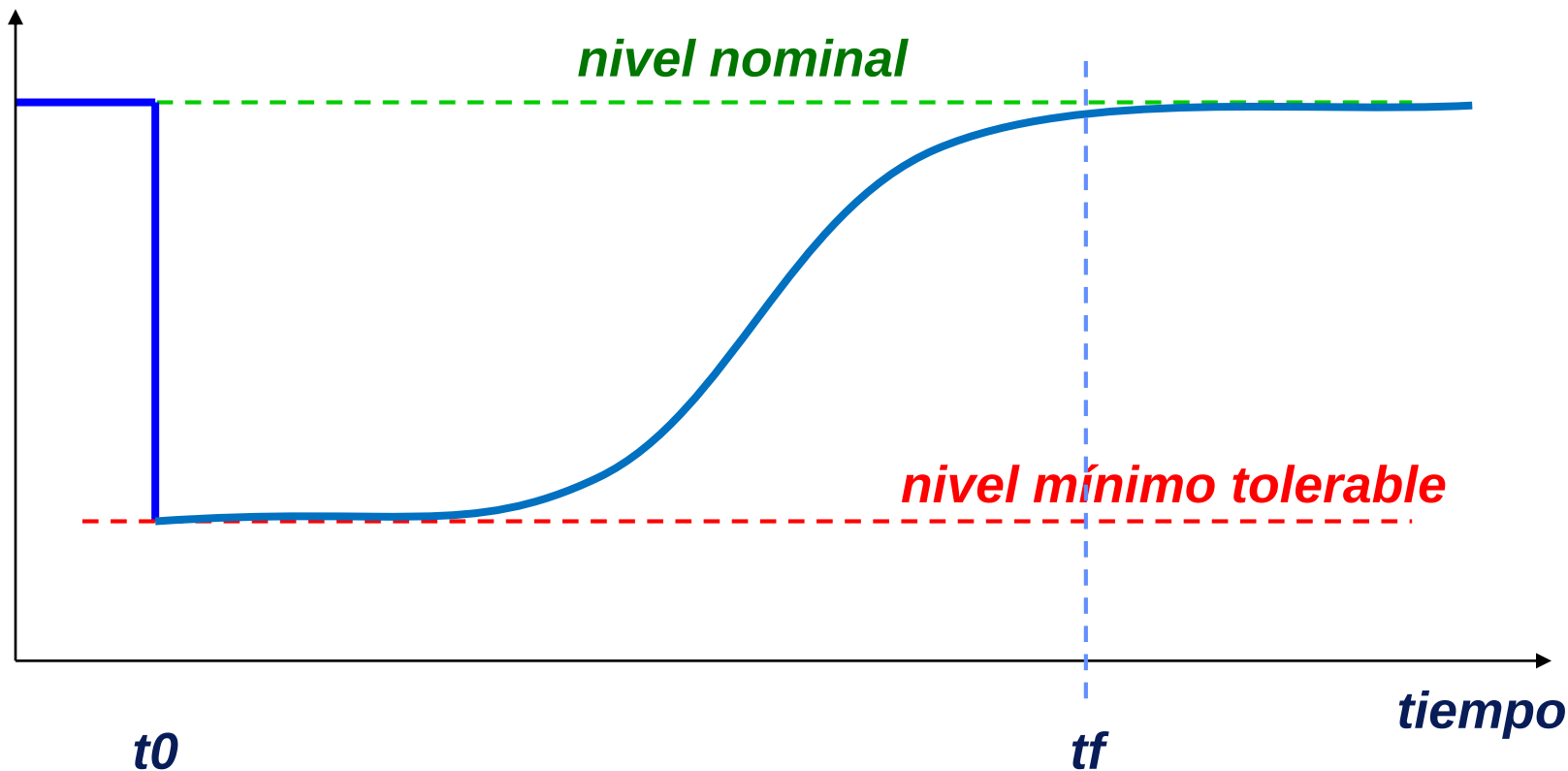
resiliencia

- Capacidad de adaptación de una organización en un entorno complejo y cambiante.[UNE Guía 73:2010]

dit

métricas de impacto

nivel de servicio



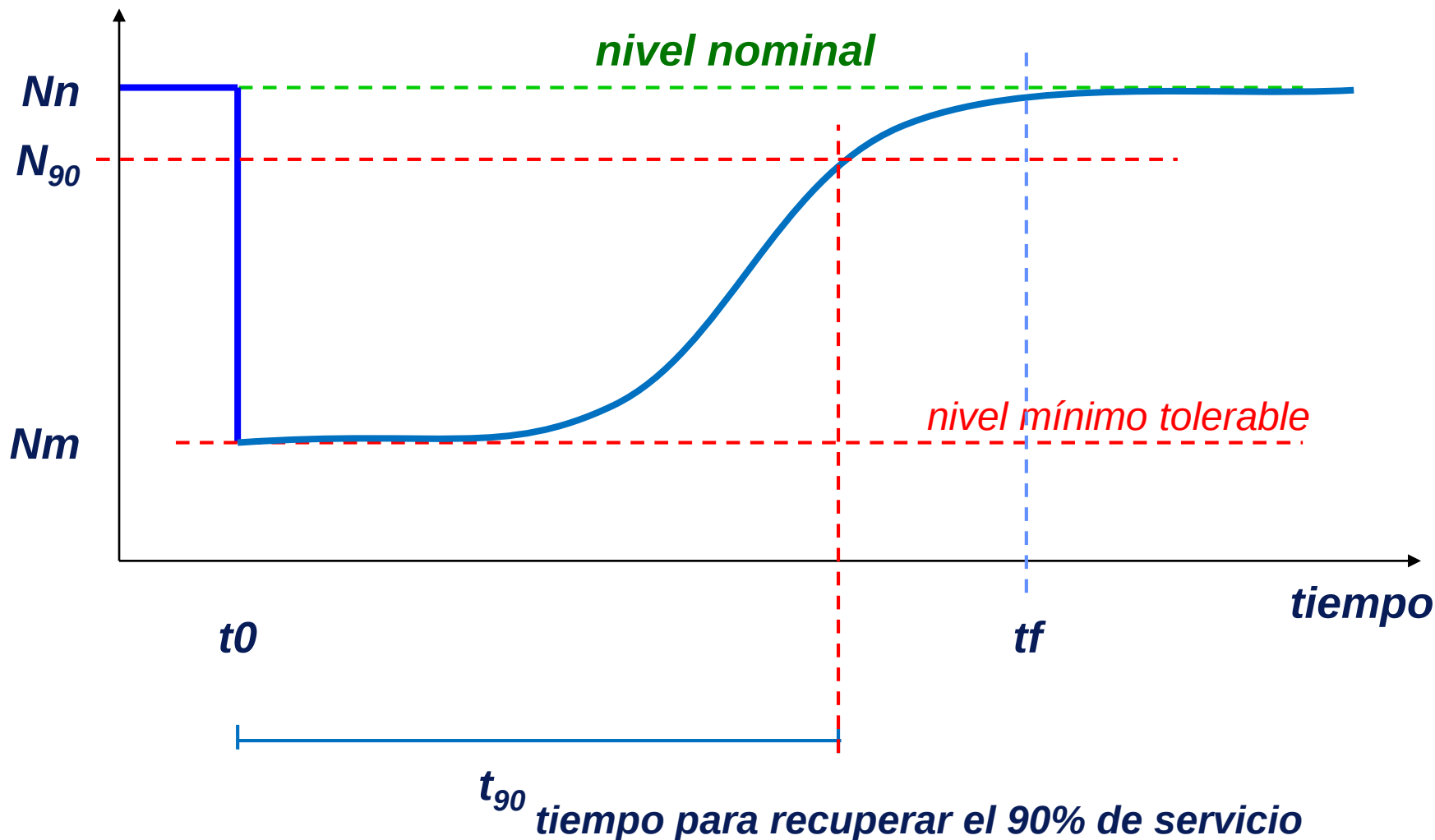
$$\text{resiliencia} = \int_{t_0}^{t_f} \text{nivel} \times dt$$

target: 1

dit

métricas de resolución

nivel de servicio



BC - business continuity

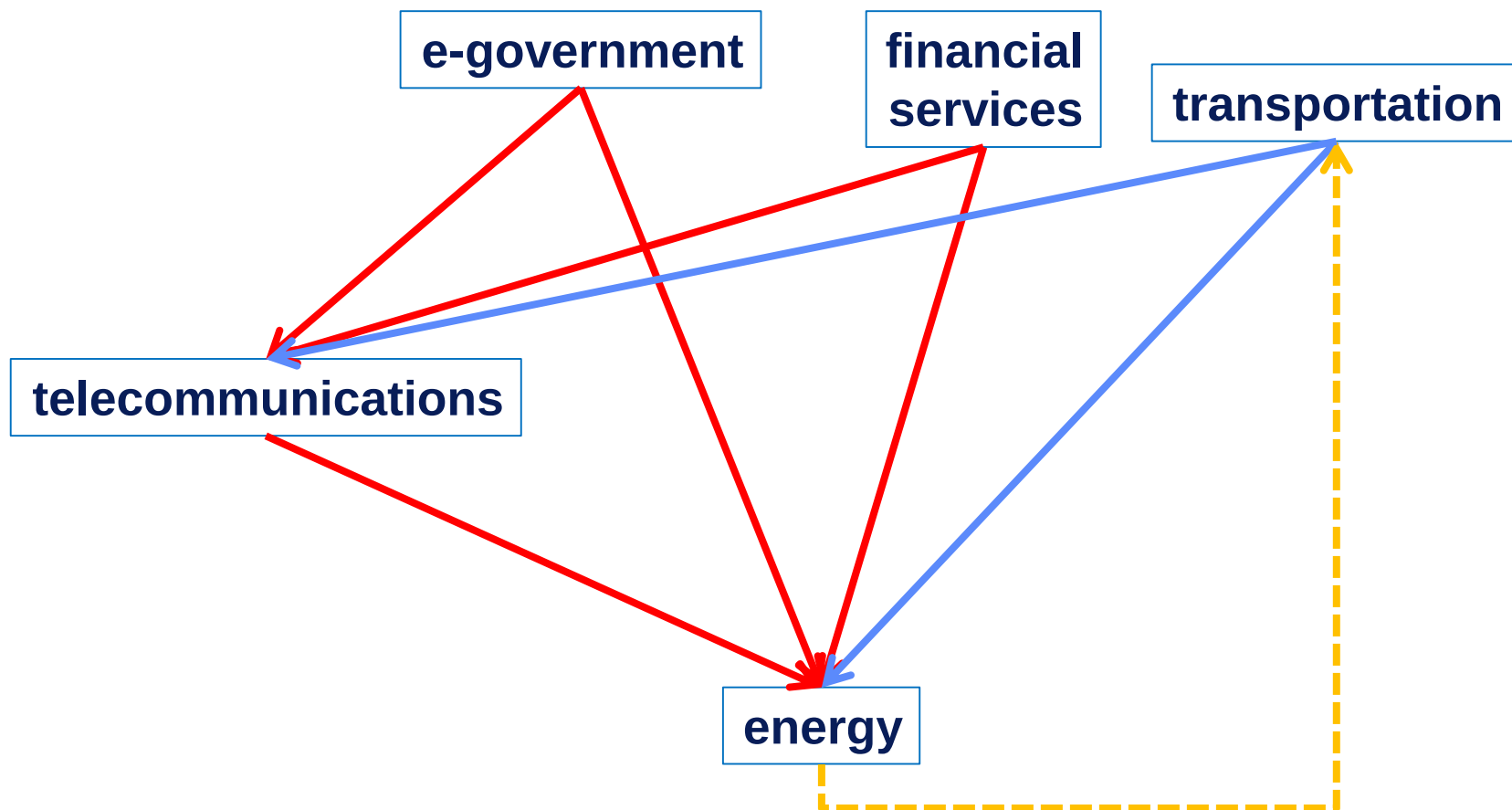
- capability of the *organization* to continue delivery of products or services at acceptable predefined levels following disruptive *incident*

BCM - business continuity management

- holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities

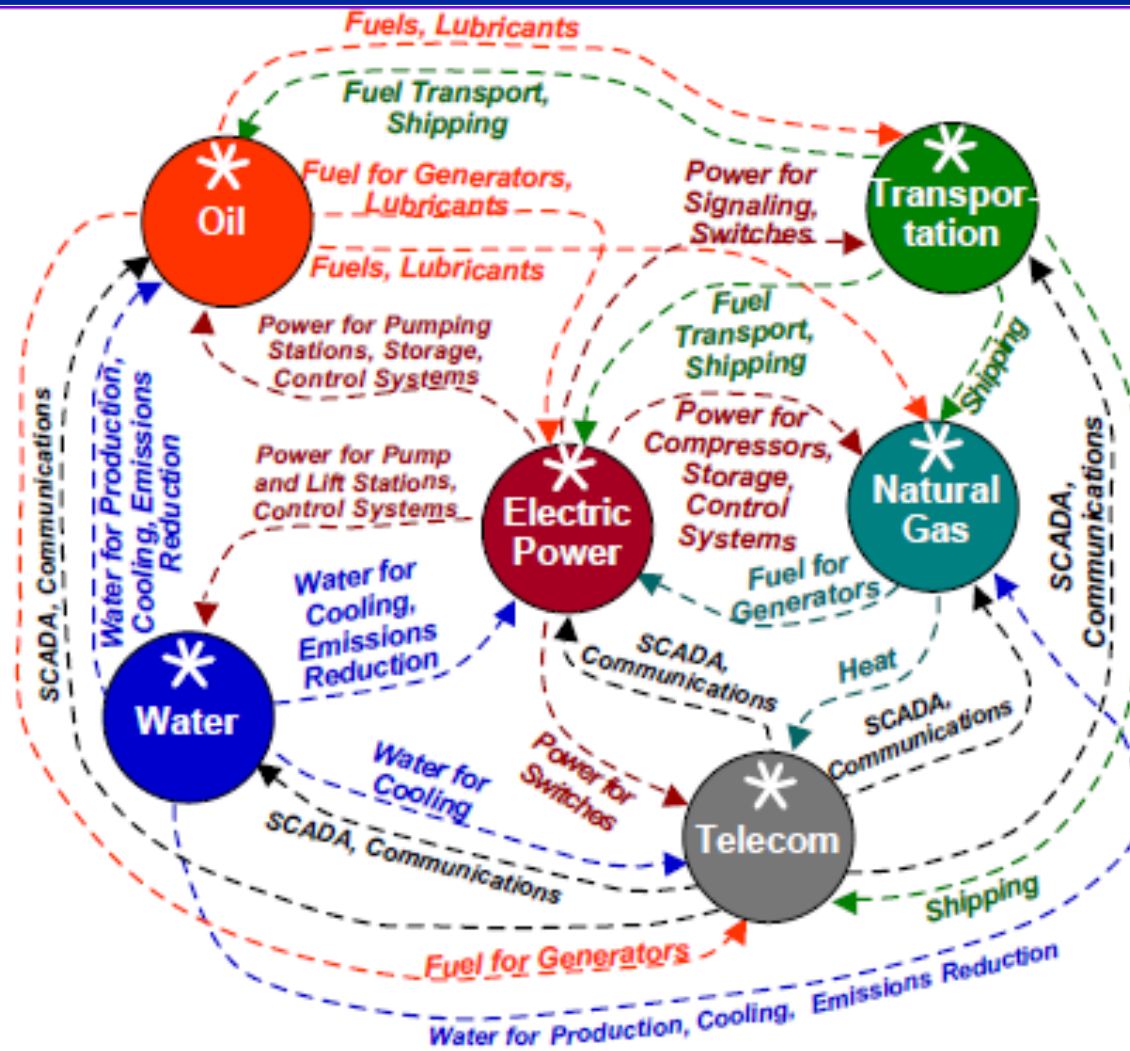
dit

interdependencias



dit

interdependencias



BCP - business continuity plan

- documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption

invocation

- act of declaring that an organization's business continuity arrangements need to be put into effect in order to continue delivery of key products or services

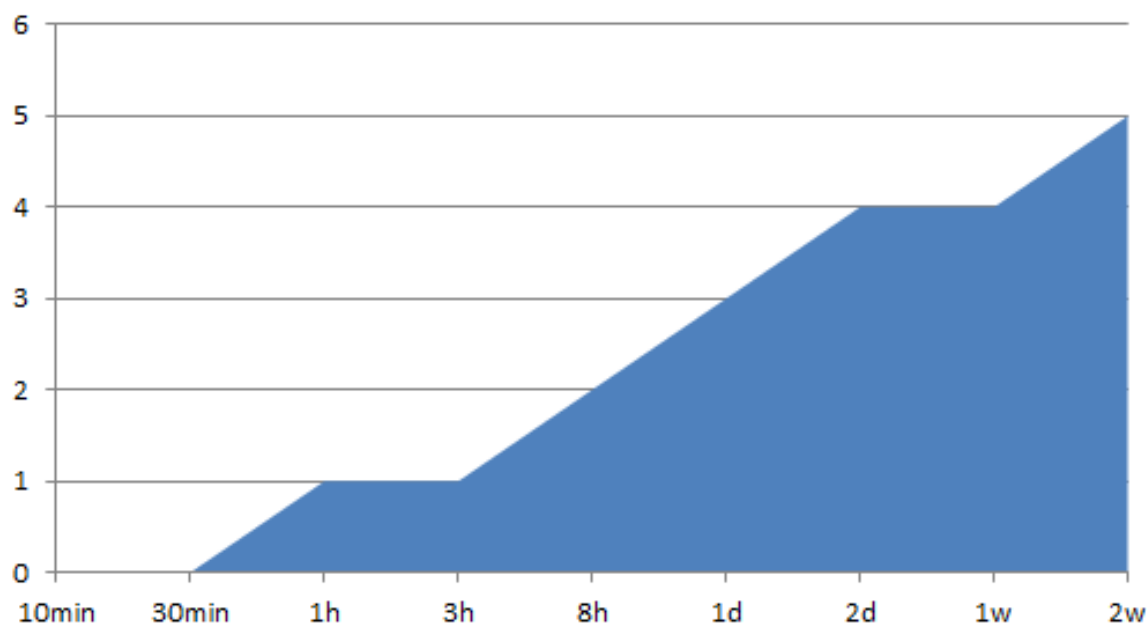
DRP - Disaster Recovery Plan

- A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.
[NIST-SP800-34:2002]

BIA - business impact analysis

- process of analyzing activities and the effect that a business disruption might have upon them

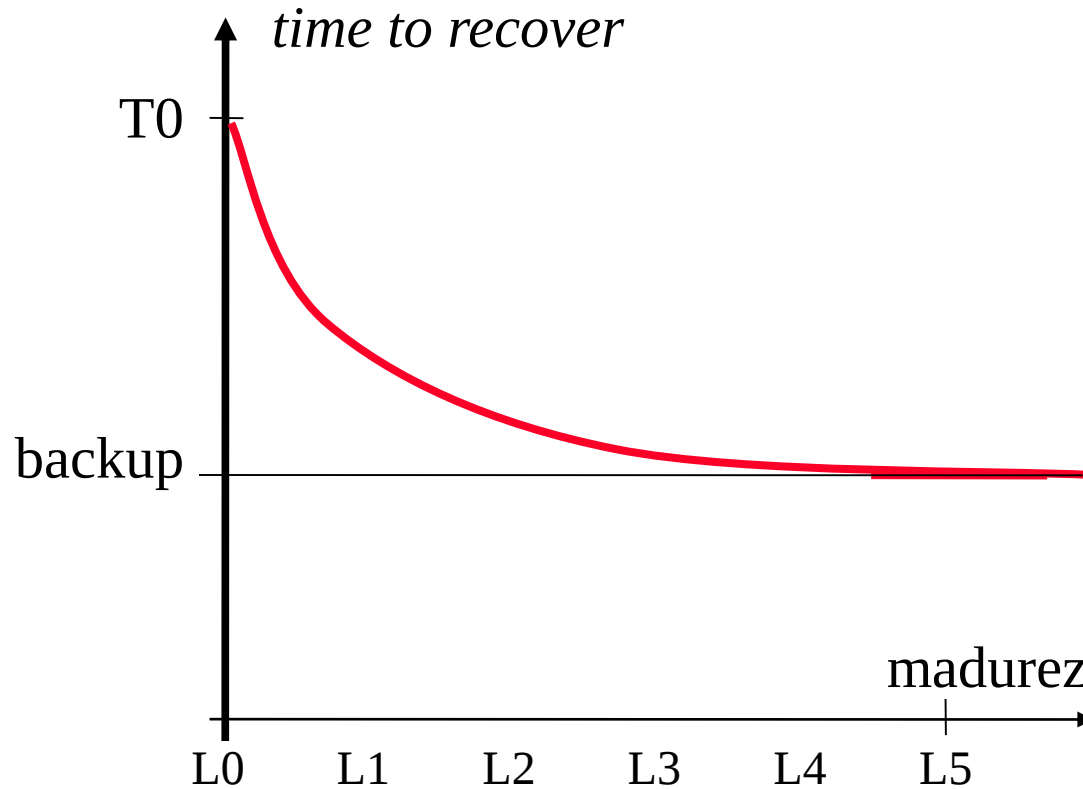
coste de la interrupción

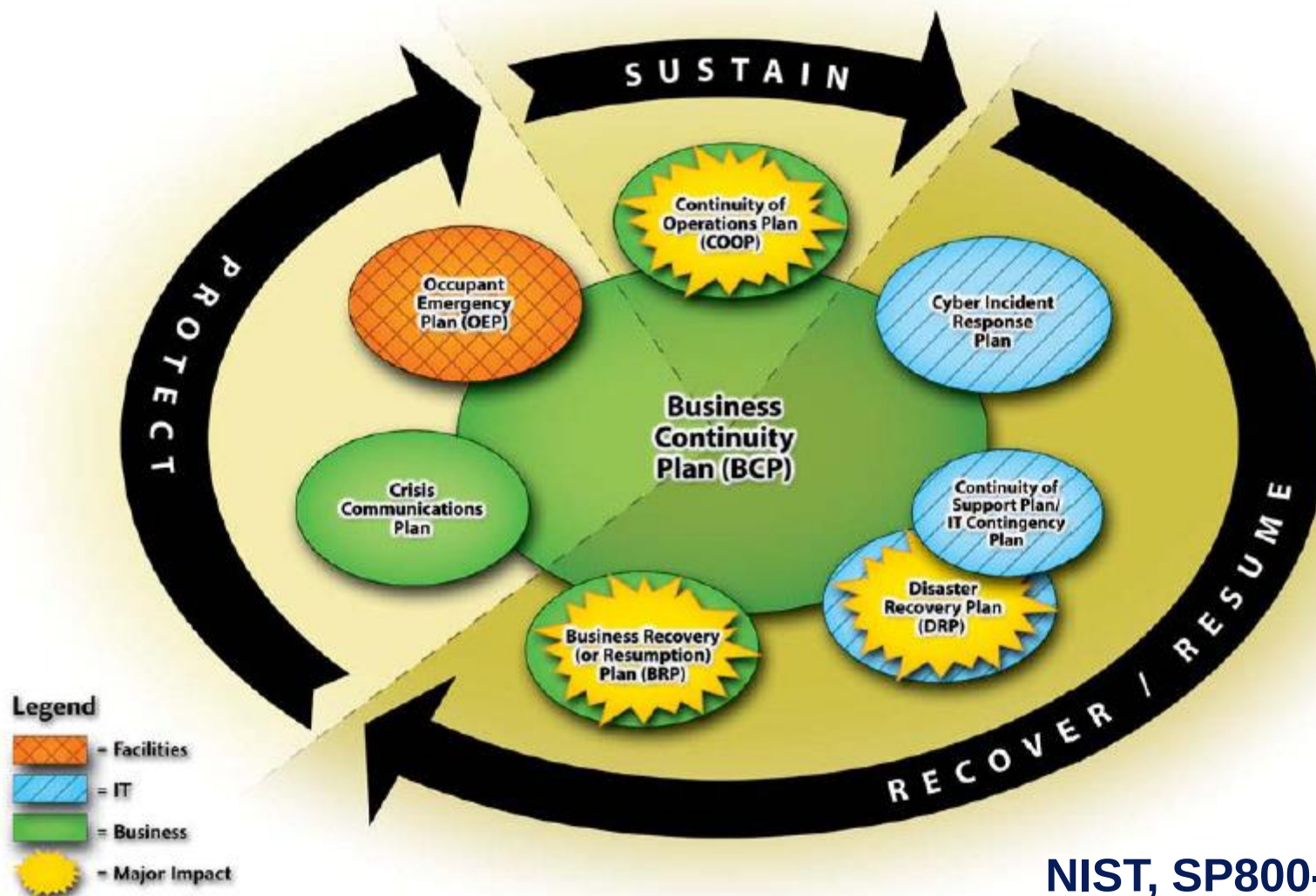


duración de la interrupción

dit

impacto residual





- Puede tenerse miedo de diferentes desastres
 - incendio del CPD
 - incendio de las instalaciones
 - accidente que afecta al parque empresarial
 - indisponibilidad de las personas
 - huelga, epidemia, amenaza de bomba, ...
 - indisponibilidad de las comunicaciones
 - ...
- ante cada supuesto hay que tener un plan de actuación

crítico

- ... de emergencia (OEP)
 - salvar a las personas
 - frenar el incidente
 - hacer acopio de información
 - **informar (personal, prensa, familias, ...)**
- ... de continuidad de operaciones (COOP)
 - alternativas para seguir trabajando pese a no disponer de los medios habituales

crítico

- ... de recuperación tras el desastre (DRP)
 - equipamiento alternativo
 - informática
 - comunicaciones
 - instalaciones
 - personal
- ... de retorno a la normalidad (BRP)
 - para regresar a las condiciones anteriores



- sin edificios
- sin personal
- sin transporte
- sin comunicaciones
- acceso restringido



Equipo humano de emergencia

- personal, personal de guardia, director(es) y proveedores
 - turnos, equipos rotatorios, ...
- medios de localización y entrada en juego: escalado
 - teléfonos de contacto
empleados, medios de comunicación, servicios de emergencia

Precauciones técnicas

- información: copias de respaldo
 - periodicidad, ubicación, ...
 - procedimiento de recuperación: transporte, claves, ...
- equipamiento alternativo: hw + sw + com + local + personas
 - ubicación, pre-configuración, activación, ...

Medios

- informáticos: back up
 - información, ¿al día? ¿consistente?
 - sw: programas y configuraciones
- tradicionales: papel
- personal técnico y directivo
 - ¿dónde se sienta? ¿cómo habla?

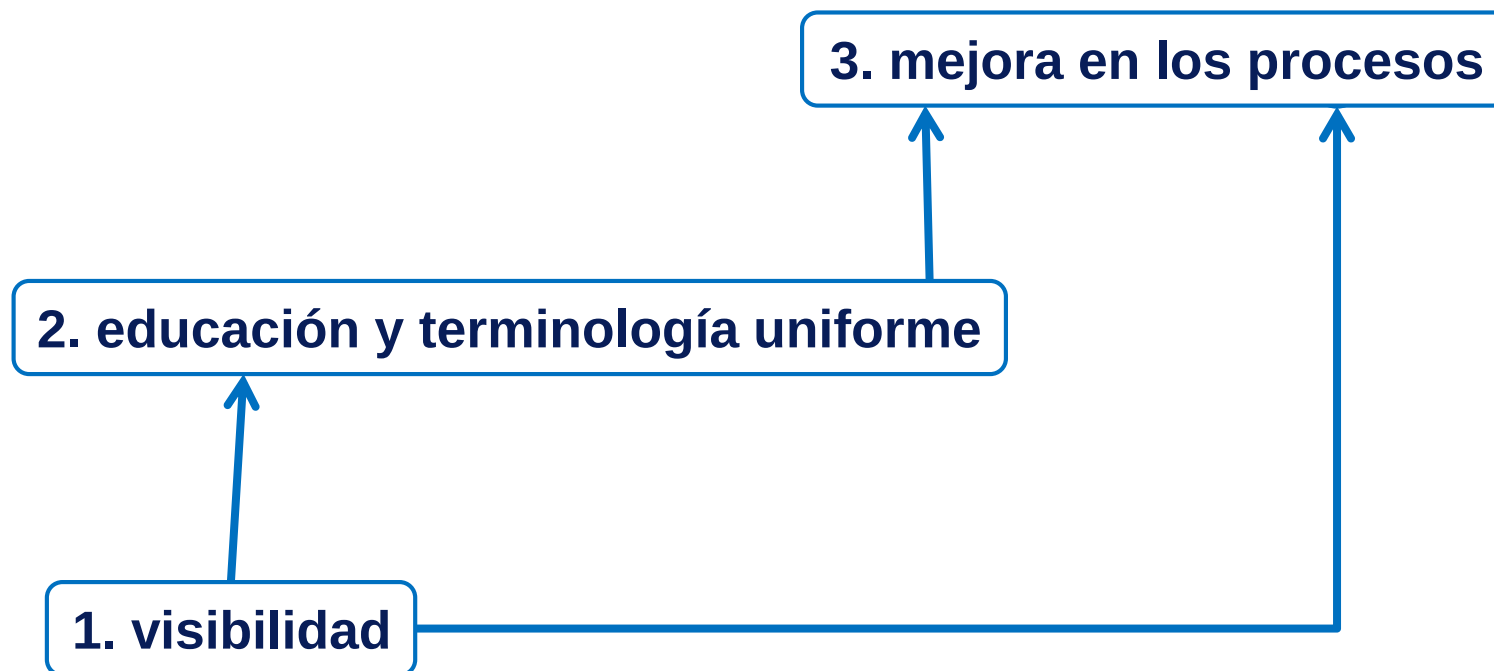
Procedimientos

- Pruebas regulares y mantenimiento

- COMPROBAR, COMPROBAR y COMPROBAR
 - en una emergencia no hay tiempo para experimentar
- Verificar
 - que funciona la comunicación de activación
 - que se entienden los planes (corto y claro)
 - que cada uno sabe lo que tiene que hacer, sin dudar
 - que no hay puntos de dependencia crítica
 - que no nos pisamos unos a otros
 - que no quedan tareas sin asignar
 - que los proveedores responden
- Tras cada prueba
 - evaluar cualitativa y cuantitativamente
 - actualizar los planes

- exercise
 - process to train for, assess, practice, and improve performance in an organization
 - NOTE 1 Exercises can be used for: validating policies, plans, procedures, training, equipment, and inter-organizational agreements; clarifying and training personnel in roles and responsibilities; improving inter-organizational coordination and communications; identifying gaps in resources; improving individual performance; and identifying opportunities for improvement, and controlled opportunity to practice improvisation.
 - NOTE 2 A test is a unique and particular type of exercise, which incorporates an expectation of a pass or fail element within the goal or objectives of the exercise being planned.

**Cuando no hay incidentes,
hay que provocarlos**

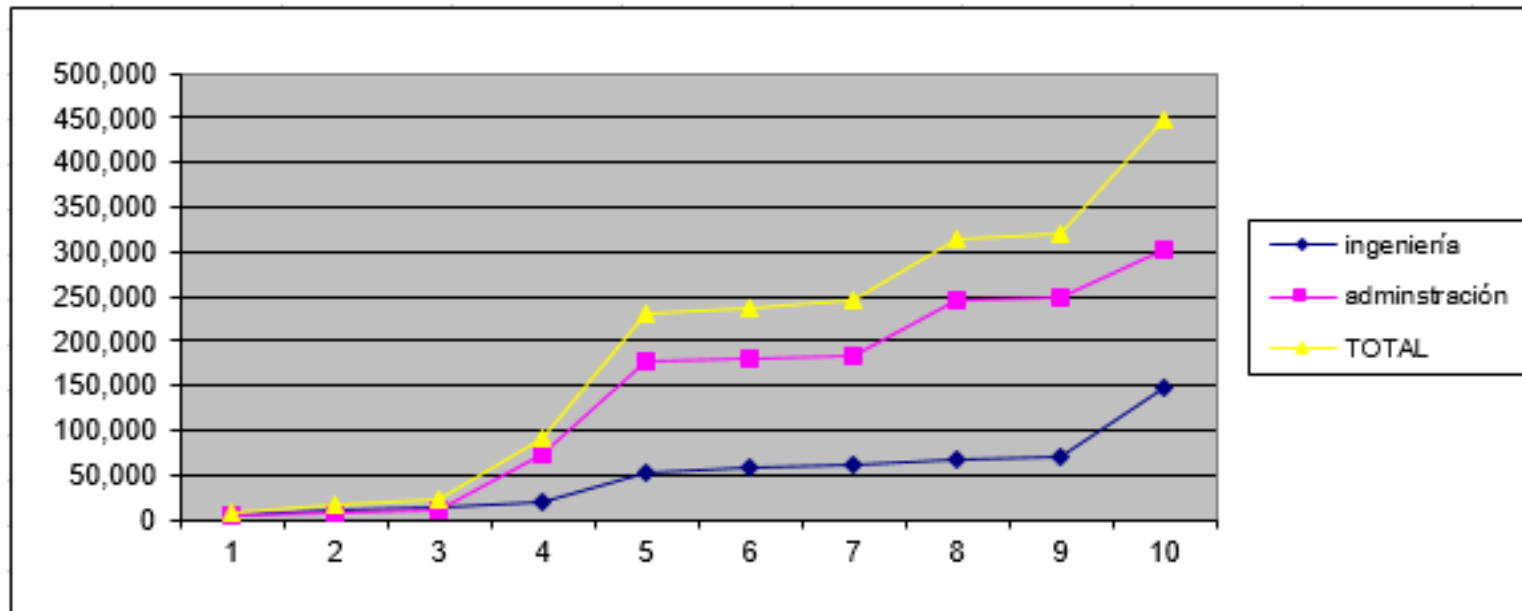


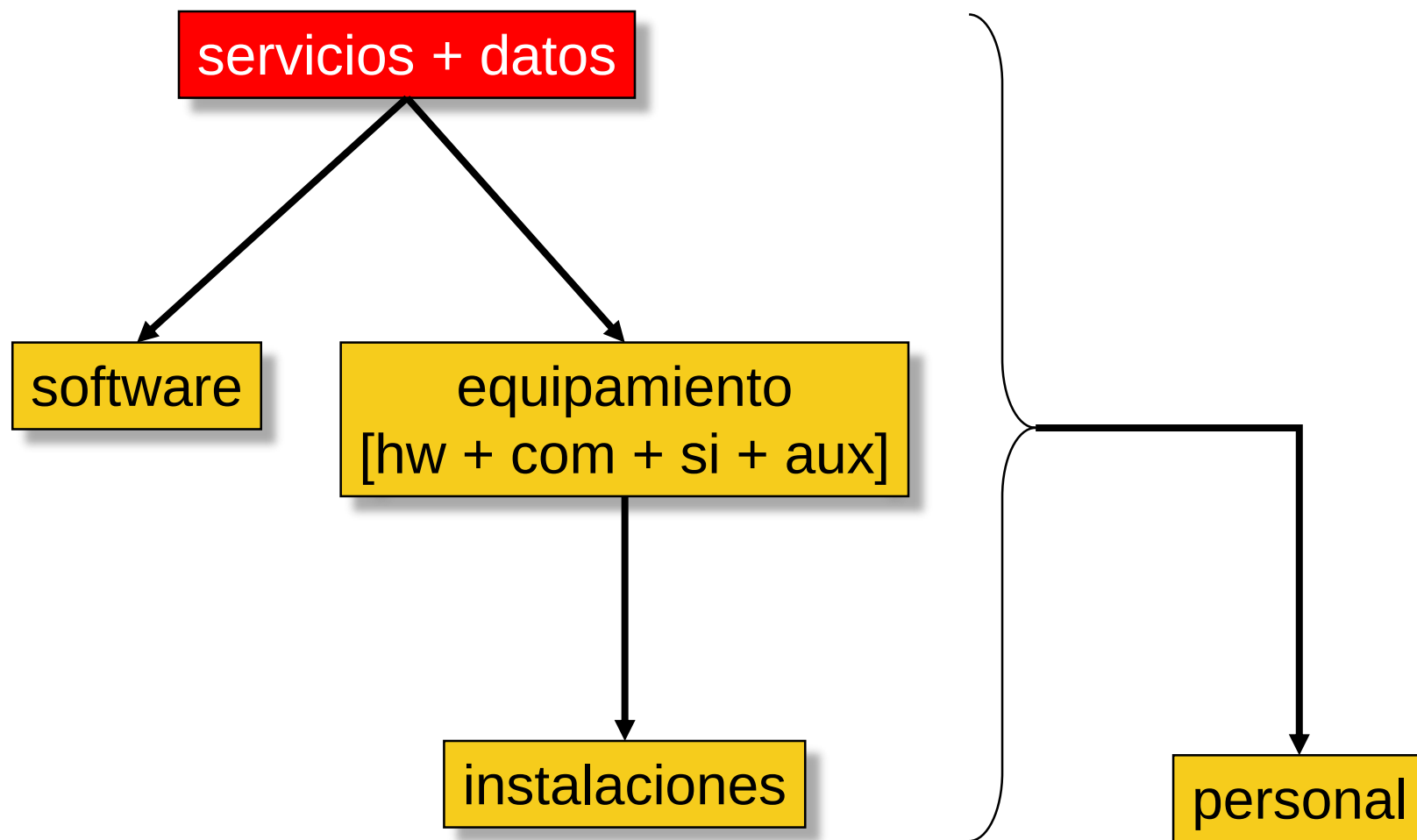
- Configuración del sistema recuperado
- Traslado de información
- Conmutación
- Terminación de los medios alternativos
 - borrado, destrucción, devolución, ...
- Informes
 - PDCA: consecuencias sobre los planes preparatorios

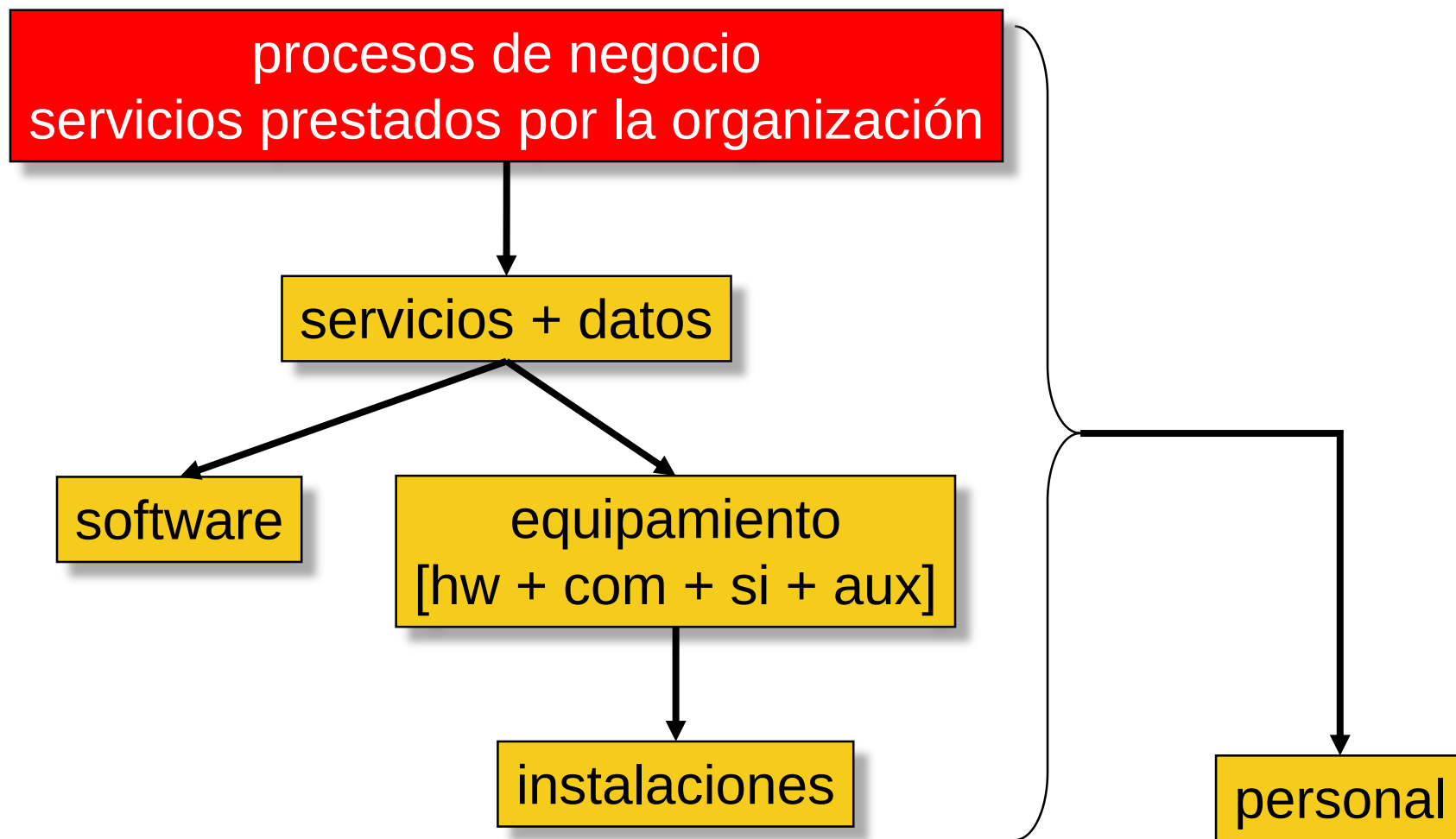
1. Definir una política (formal)
2. BIA – análisis del impacto en el negocio
3. Identificación de medidas preventivas (agr)
4. Selección de medios alternativos
5. Escribir un plan
6. Auditoría, pruebas, entrenamiento
7. Mantenimiento regular
 - tenemos más
 - sabemos más

1. Determinación de las funciones críticas
 - de producción
 - de responsabilidad legal y contractual
2. Determinación de recursos críticos para funciones críticas
3. Determinación del coste por hora de indisponibilidad
4. Identificación de
 - activos que requieren una alternativa
 - tiempo crítico de puesta en marcha

						días									
			diario			1	2	3	4	5	6	7	8	9	10
ingeniería			personas	€/ p / día	/ día										
desarrollo															
	puesta al día	8	400	3,200	3,200	6,400	9,600	12,800	16,000	19,200	22,400	25,600	28,800	32,000	
	retrasos								30,000	30,000	30,000	30,000	30,000	30,000	100,000
mantenimiento															
	puesta al día	2	200	400	400	800	1,200	1,600	2,000	2,400	2,800	3,200	3,600	4,000	
	SLA			1,000	1,000	2,000	3,000	4,000	5,000	6,000	7,000	8,000	9,000	10,000	
TOTAL						4,600	9,200	13,800	18,400	53,000	57,600	62,200	66,800	71,400	146,000
adminstración															
comercial															
	puesta al día	10	300	3,000	3,000	6,000	9,000	12,000	15,000	18,000	21,000	24,000	27,000	30,000	
	ventas								50,000	50,000	50,000	50,000	50,000	50,000	100,000
administración															
	puesta al día	3	100	300	300	600	900	1,200	1,500	1,800	2,100	2,400	2,700	3,000	
	bancos							60,000	60,000	60,000	60,000	120,000	120,000	120,000	
	legal								50,000	50,000	50,000	50,000	50,000	50,000	
TOTAL						3,300	6,600	9,900	73,200	176,500	179,800	183,100	246,400	249,700	303,000
TOTAL						7,900	15,800	23,700	91,600	229,500	237,400	245,300	313,200	321,100	449,000







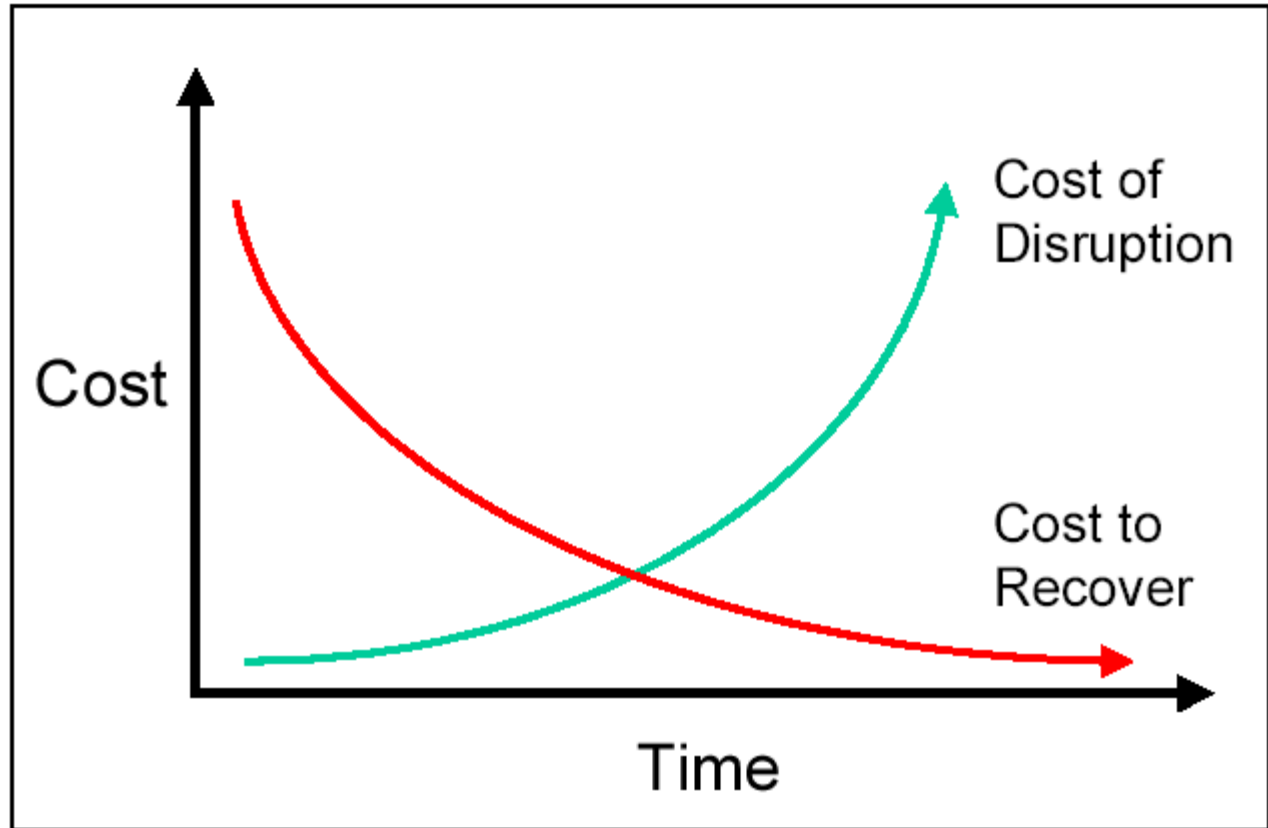
- ... de los servicios
- ... de la información
- ... de las aplicaciones
- ... de los equipos
- ... de las instalaciones
- ... del personal

criterios

- impacto a tratar
- coste
- tiempo de entrada en acción
- localización

dit

una decisión política



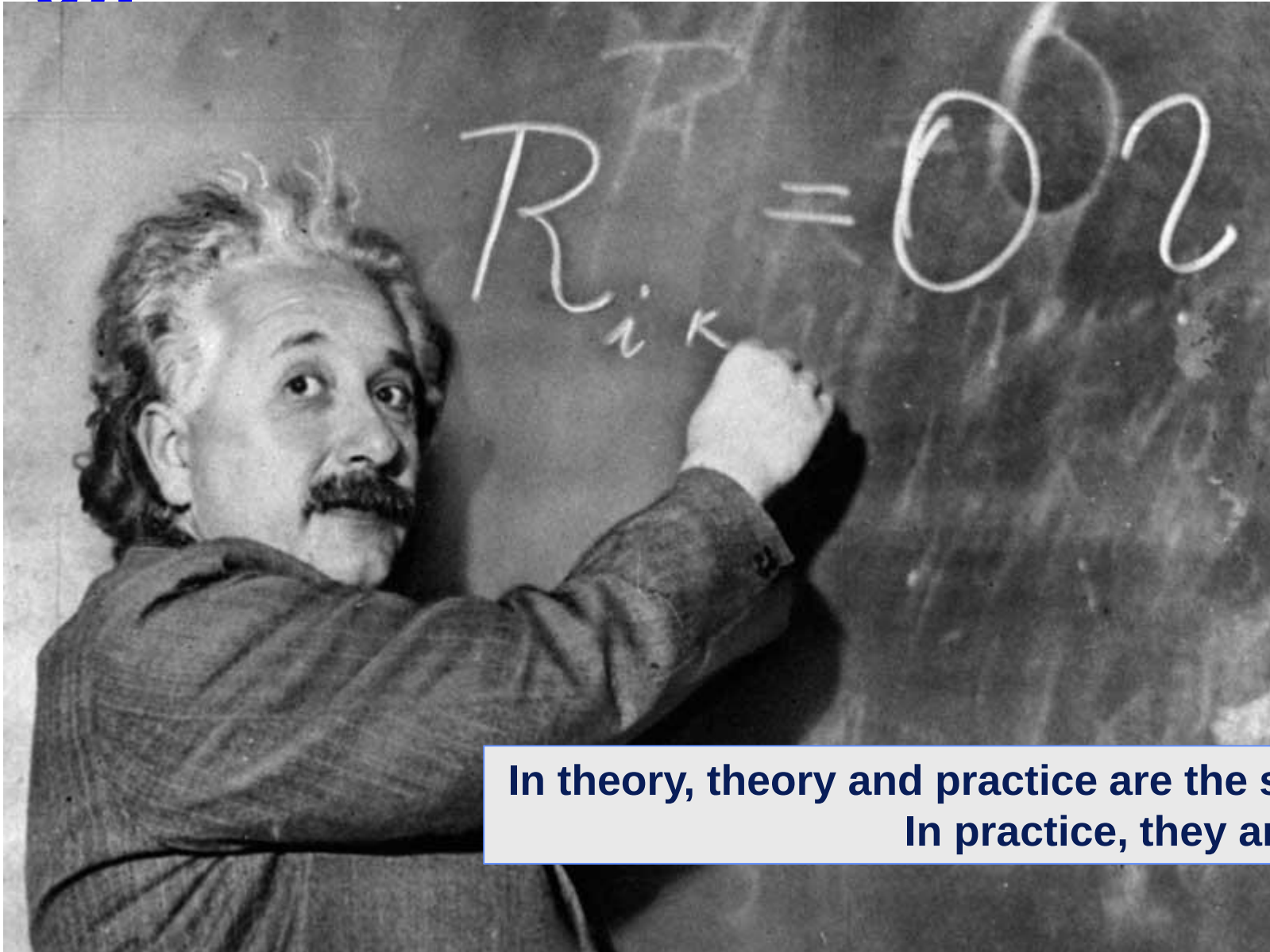
- Confidencialidad de la información
 - protección de las copias de seguridad
 - protección de los procesos de copia, transporte y restauración
 - protección de las claves de cifra y autenticación
 - disponibilidad de las claves
- Integridad de la información
 - ídem
- Actualidad de la información (RPO)

- BS 25999-1:2006
Business Continuity Management. Code of Practice
 - práctica
- BS 25999-2:2007
Specification for Business Continuity Management
 - certificable
 - reemplazada por ISO 22301

1. Cuando ocurre el desastre no hay tiempo para pensar
 - antes hay que entender el negocio y marcar objetivos
 - antes hay que analizar posibles escenarios
 - antes hay que asignar roles y escribirlo todo
2. Hay que ejecutar [ciegamente] un plan para tontos
 - comité de crisis: activación y comunicación
 - DRP
 - pueden no estar disponibles las personas
3. No hay que esperar al desastre para probar el plan
 - proveedores

dit

para acabar



**In theory, theory and practice are the same.
In practice, they are not.**