



Confiabilidad y Disponibilidad en sistemas de misión crítica

Oscar Olivera.

Manager

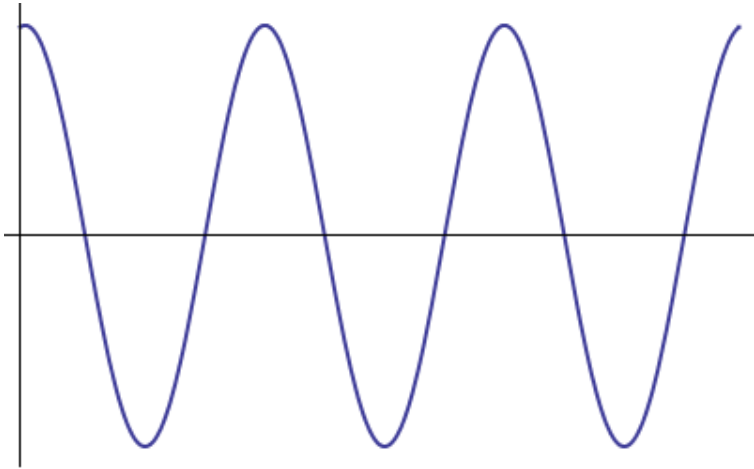
Data Infrastructure and Power Quality Solutions

oscar.olivera@legrand.com – 318 455 9471

designed to be better.



FUNDAMENTAL...



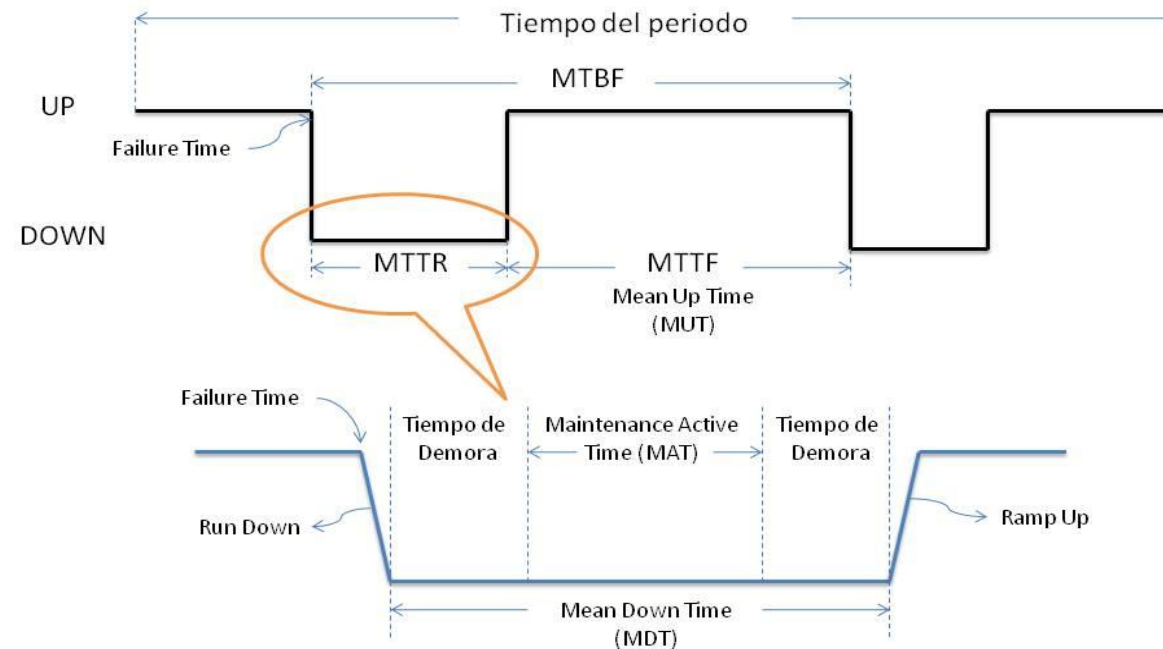
SERVICIO DISPONIBLE



SERVICIO CONFIABLE

DISPONIBILIDAD Y CONFIABILIDAD

EL COSTE DEL
TIEMPO DE
INACTIVIDAD...



MTBF – MTTR - MUT

DISPONIBILIDAD Y CONFIABILIDAD

$$Availability = \left(\frac{Total\ Uptime}{Total\ Scheduled\ Time} \right)$$

$$Availability = \frac{MTBF}{MTBF + MTTR}$$

$$MTBF = \left(\frac{Running\ Time}{Number\ of\ Failures} \right)$$

$$MTBF = \frac{Total\ Working\ Time - Total\ Breakdown\ Time}{Total\ Breakdown\ Incidences}$$

$$MTTR = \frac{Total\ Breakdown\ Time}{Total\ Breakdown\ Incidences}$$

MÁQUINA 1	ENERO	FEBRERO	MARZO	ABRIL
Corte	31-ene-20	29-feb-20	31-mar-20	30-abr-20
Tiempo Disponible	18.480	34.440	52.080	68.880
Tiempo Muerto	2.299	4.711	7.200	8.568
N° de Fallas	31	60	91	121
MTBF Real (min)	522	495	493	498
MTBF Meta	500	522	522	522
MTTR Real (min)	74	79	79	71
MTTR Meta	75	74	74	74
MTTF Real (min)	448	417	414	428
MTTF Meta	425	448	448	448

Comprobación	18.480	34.440	52.080	68.880
Resultado	VERDADERO	VERDADERO	VERDADERO	VERDADERO

Disponibilidad Real	88%	86%	86%	88%
Disponibilidad Meta	90%	90%	90%	90%

MTBF – MTTR - MUT

REDUNDANCIA

RESILIENCIA

CAPACIDAD DE UN SISTEMA PARA RESISTIR
UNA PERTURBACIÓN GRAVE

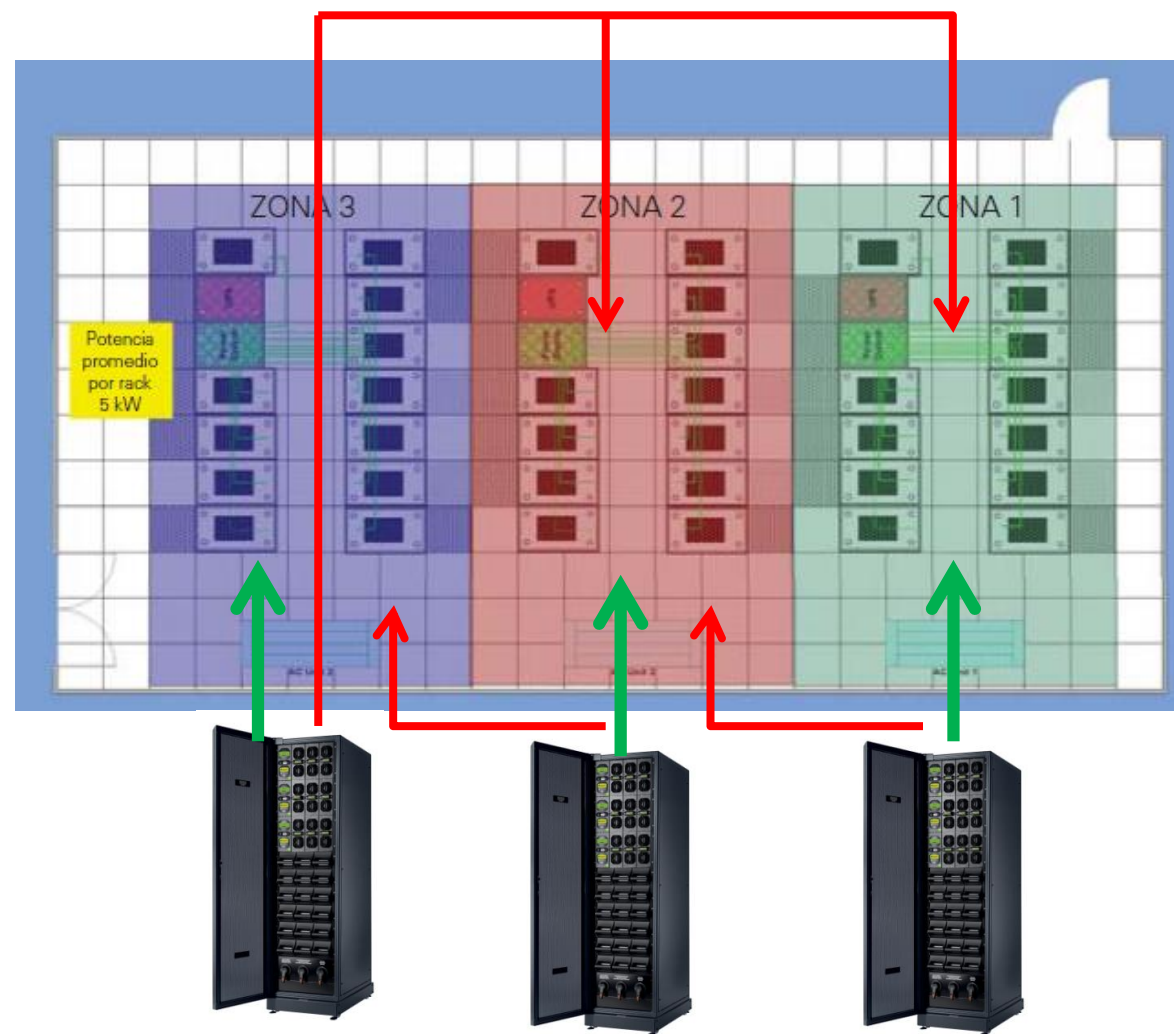
**DISPONIBILIDAD
CONFIABILIDAD Y**



ARQUITECTURAS REDUNDANTES

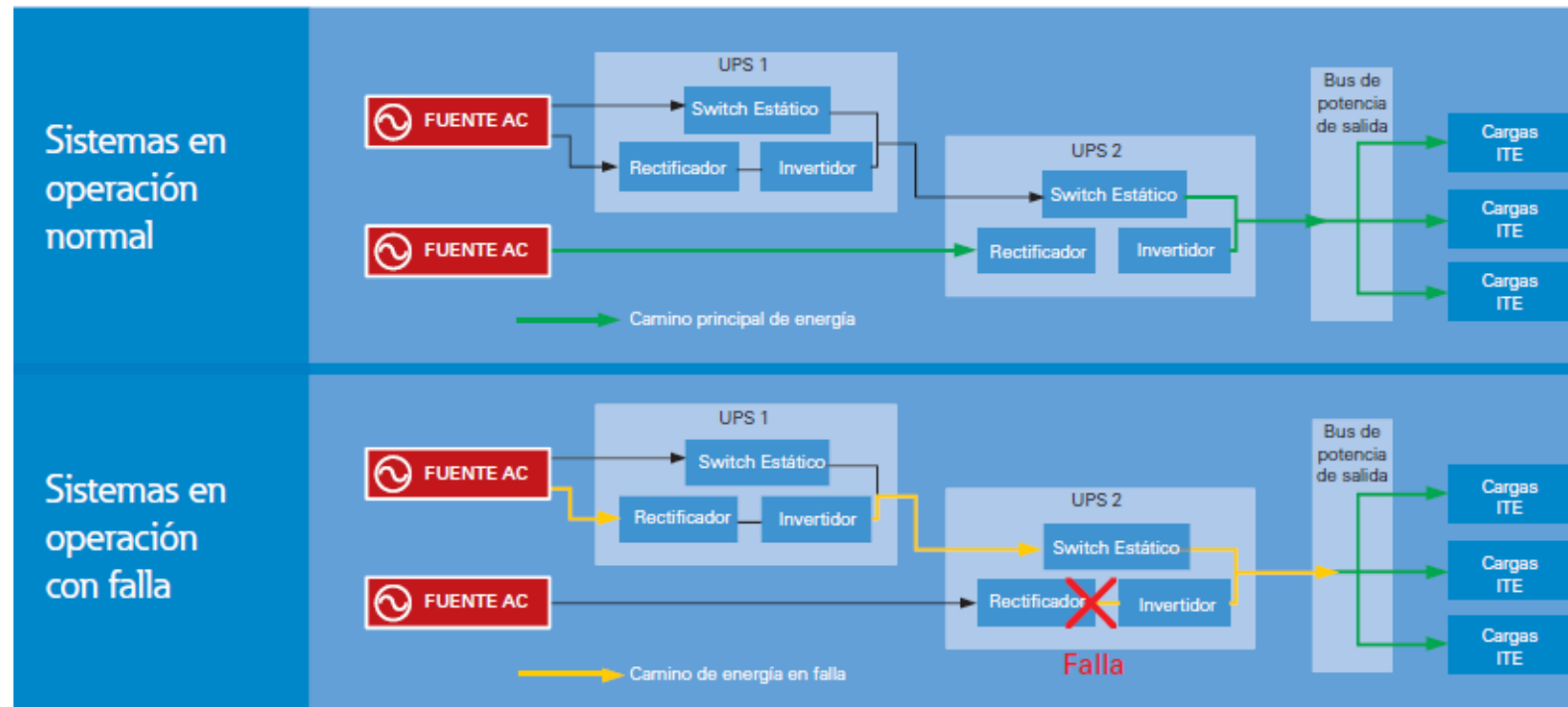
1. ZONAL
2. SERIE REDUNDANTE
3. PARALELO REDUNDANTE

1. ZONAL



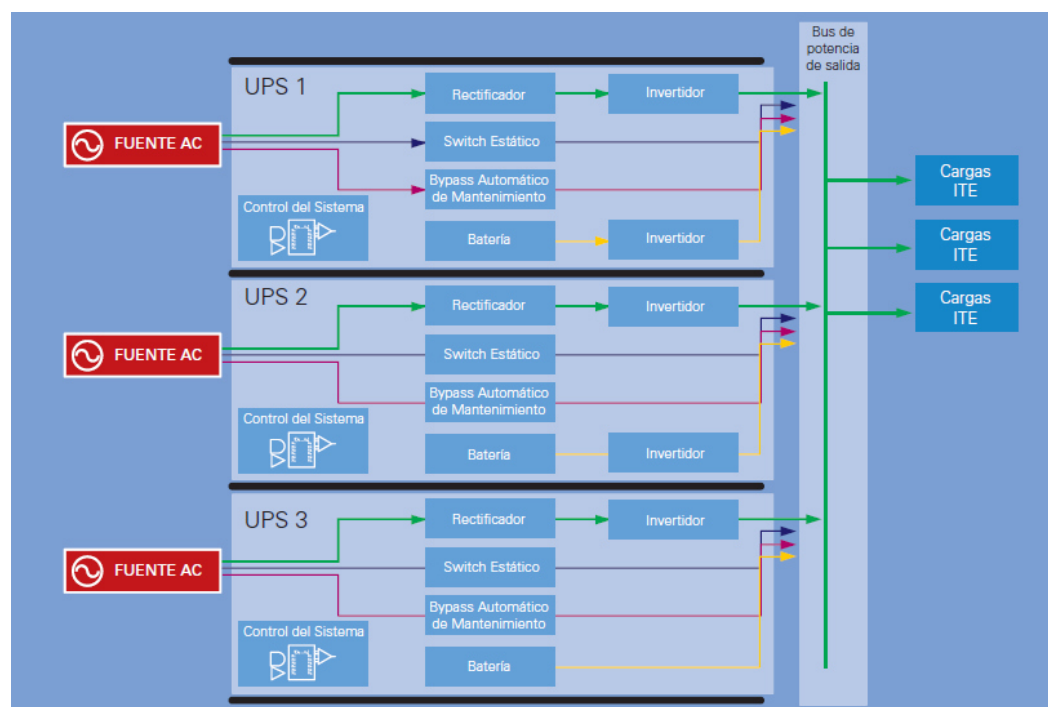
ARQUITECTURAS REDUNDANTES

2. SERIE REDUNDANTE



ARQUITECTURAS REDUNDANTES

3. PARALELO REDUNDANTE



**CUANDO HACEMOS UN DISEÑO,
SE DEBEN REDUCIR AL MÁXIMO
LOS PUNTOS DE FALLA**

DEFINICIONES IMPORTANTES

Definición de los niveles de redundancia

N - Satisface los requisitos básicos son redundancia

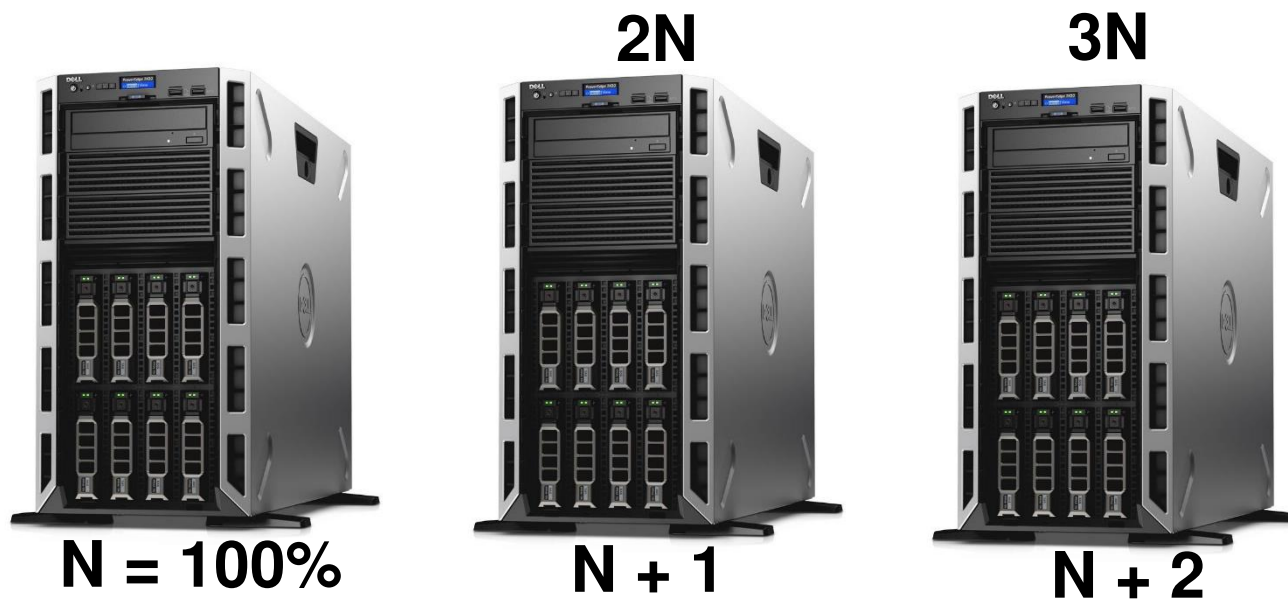
N+1 - Una unidad/camino/modulo por encima del requisito básico; la suspensión de una sola unidad no perturbara la operación

2N - Dos unidades/caminos/módulos completos por encima de cada uno exigido en el sistema básico; el fallo de todo el sistema no perturbara las operaciones

2(N+1) - Dos unidades/caminos/módulos (N+1) completos; el fallo de un sistema sigue preservando la resiliencia de todos los componentes

SER REDUNDANTE ES...

SISTEMAS COMPACTOS



SER REDUNDANTE ES...

SISTEMAS MODULARES



N+1
N+2
N+3
2N

N=100%



2(N+1)
2(N+2)

SER REDUNDANTE ES...

SISTEMAS MODULARES

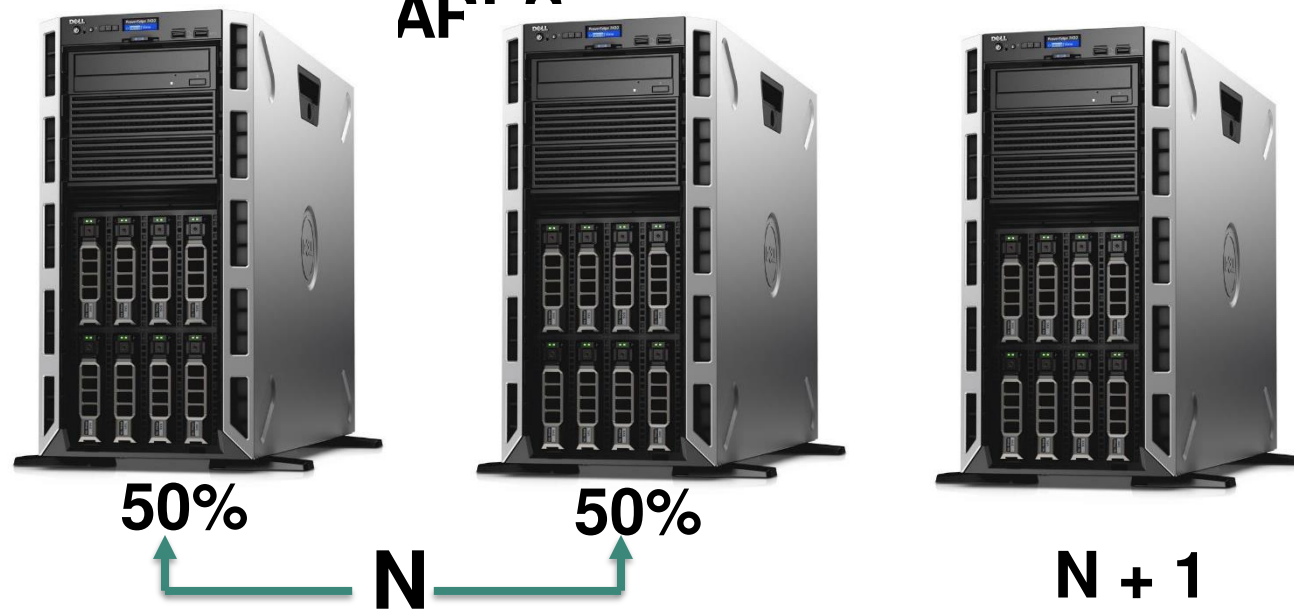


$$2N + X$$

SER REDUNDANTE ES...

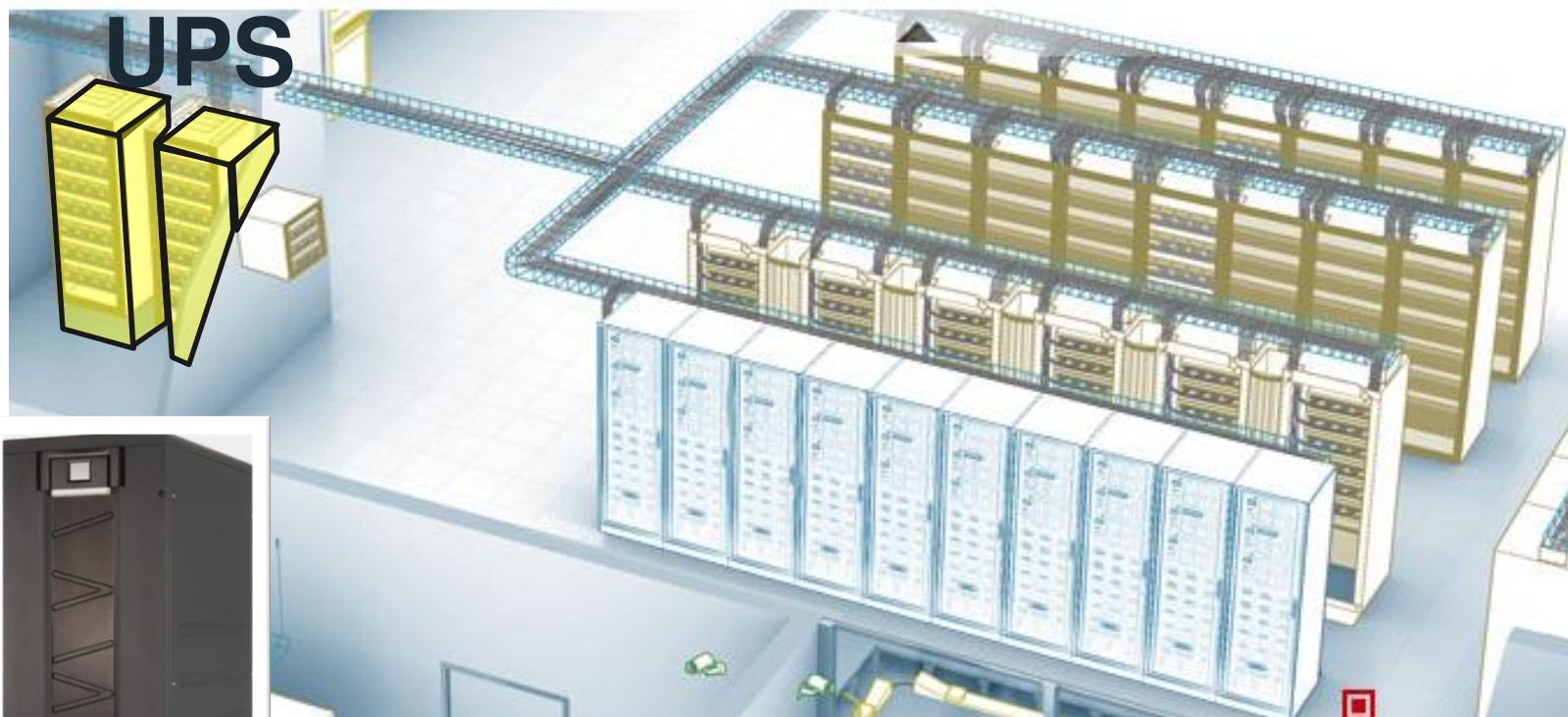
SISTEMAS COMPACTOS COMO

AF50



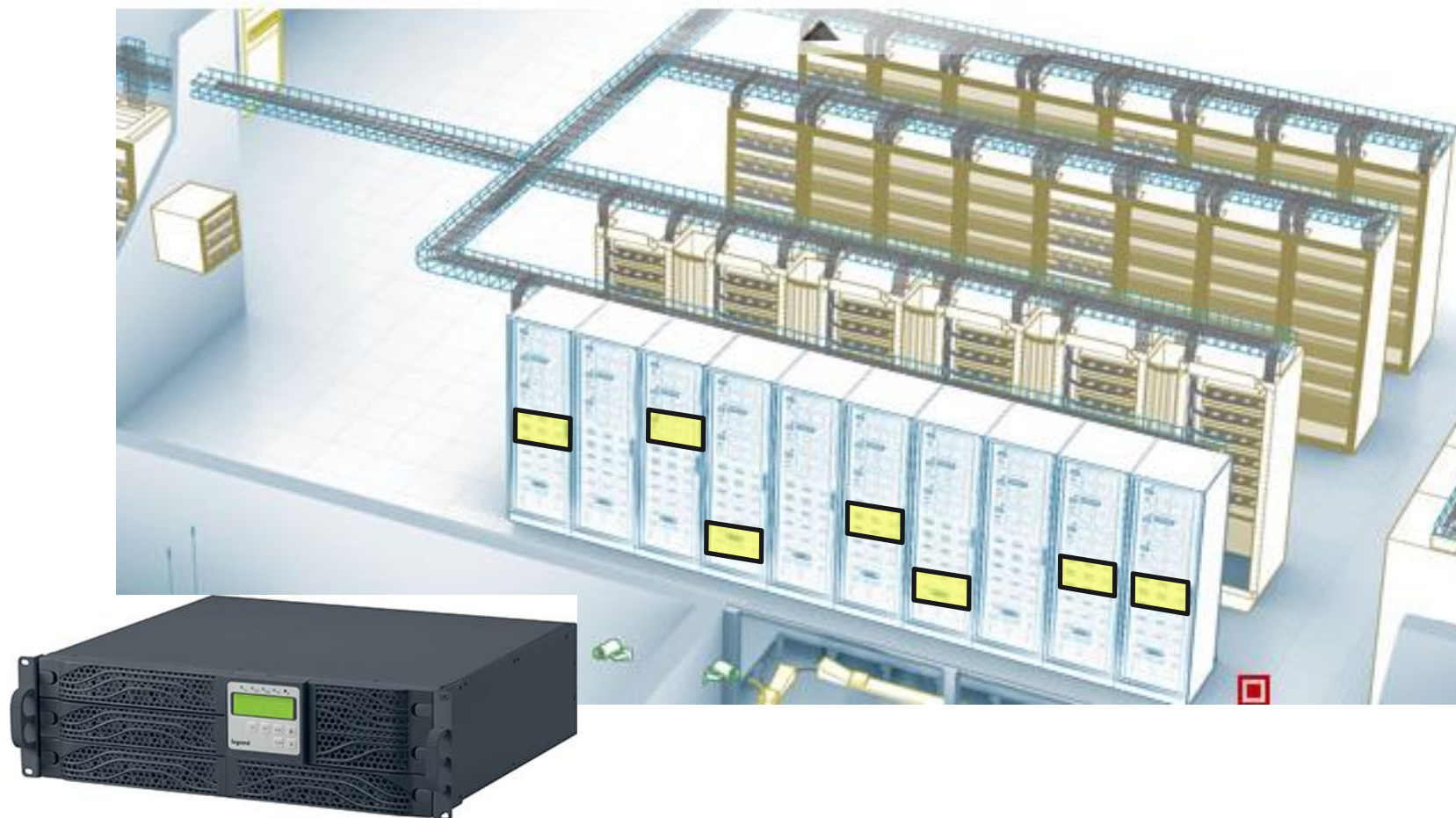


ARQUITECTURA CENTRALIZADA



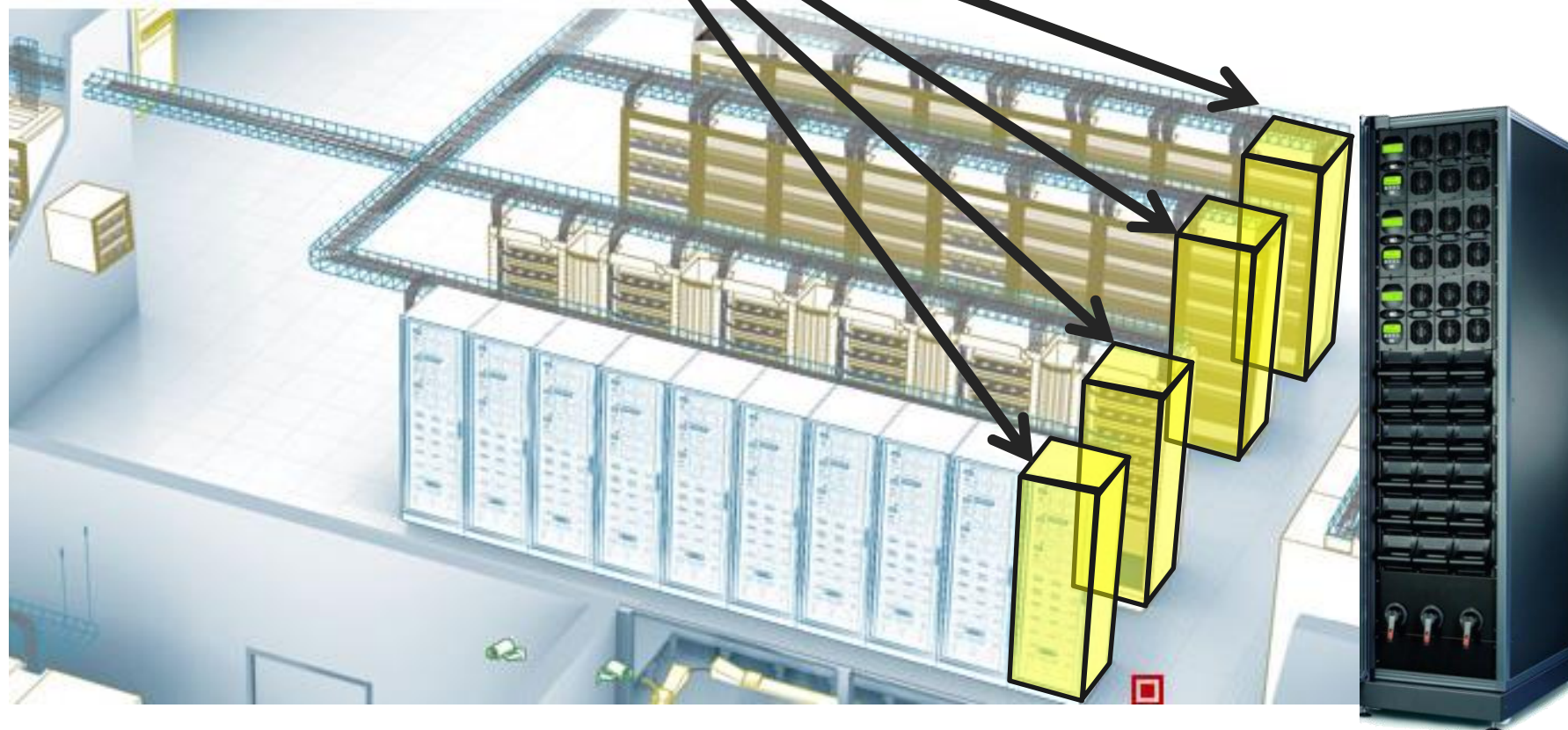


ARQUITECTURA DISTRIBUIDA





ARQUITECTURA MODULAR UPS



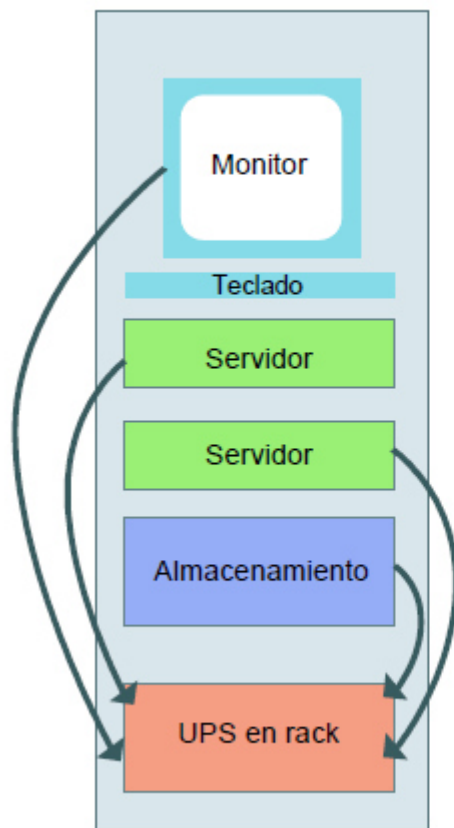


PODEMOS VERLO AL DETALLE

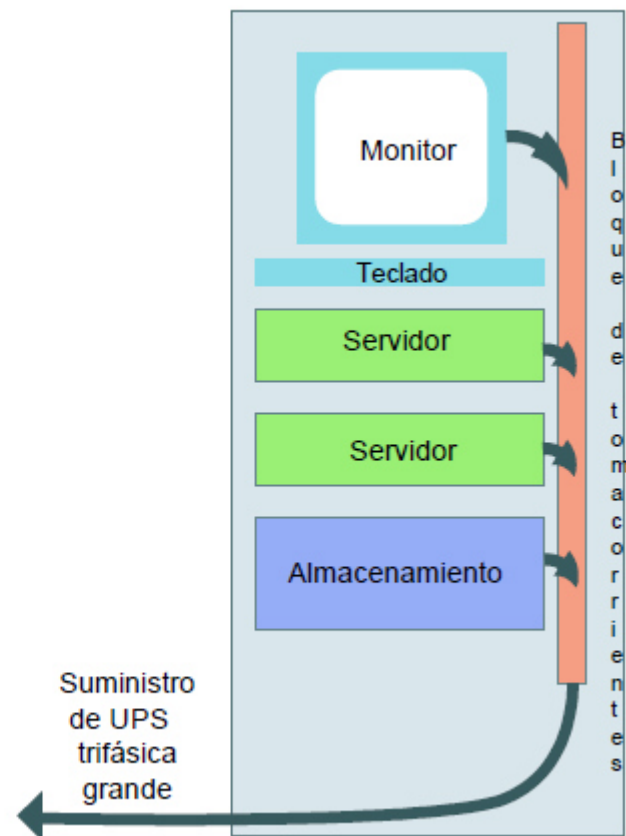




1. BASICO - ESTANDAR

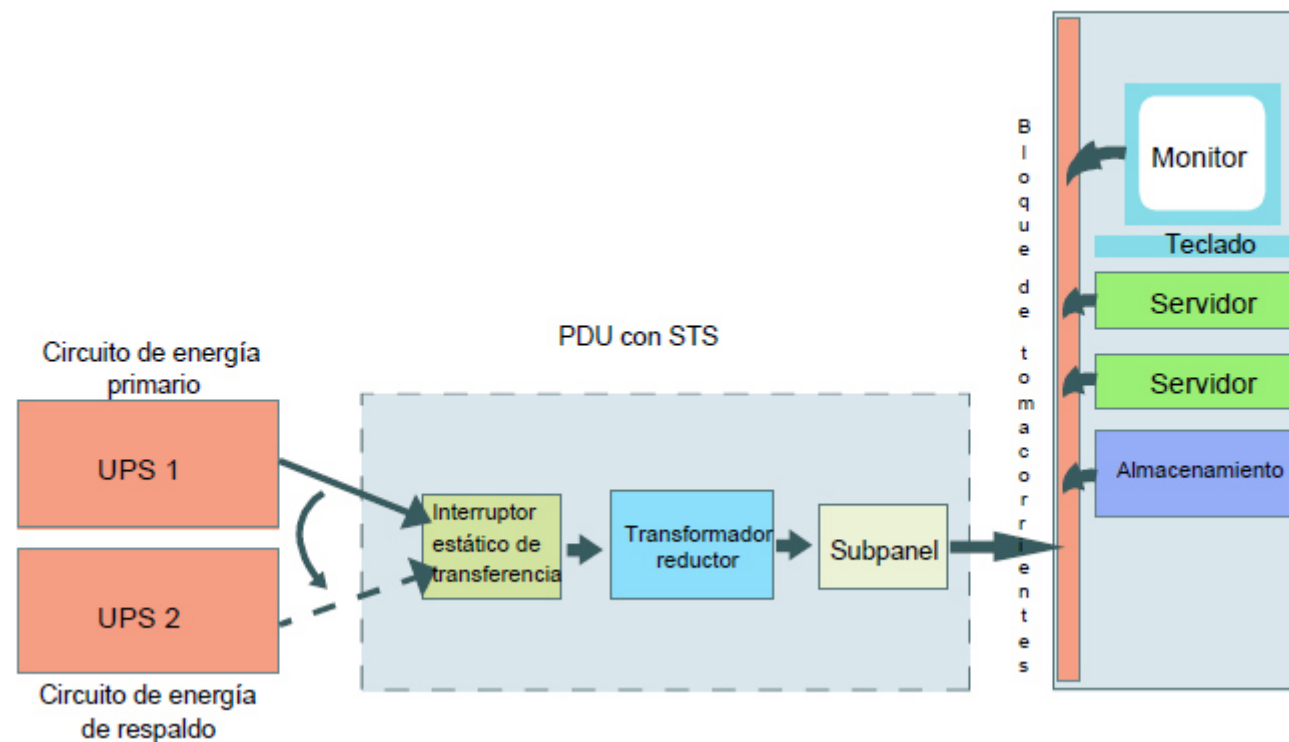


ALIMENTACIÓN EN RACK



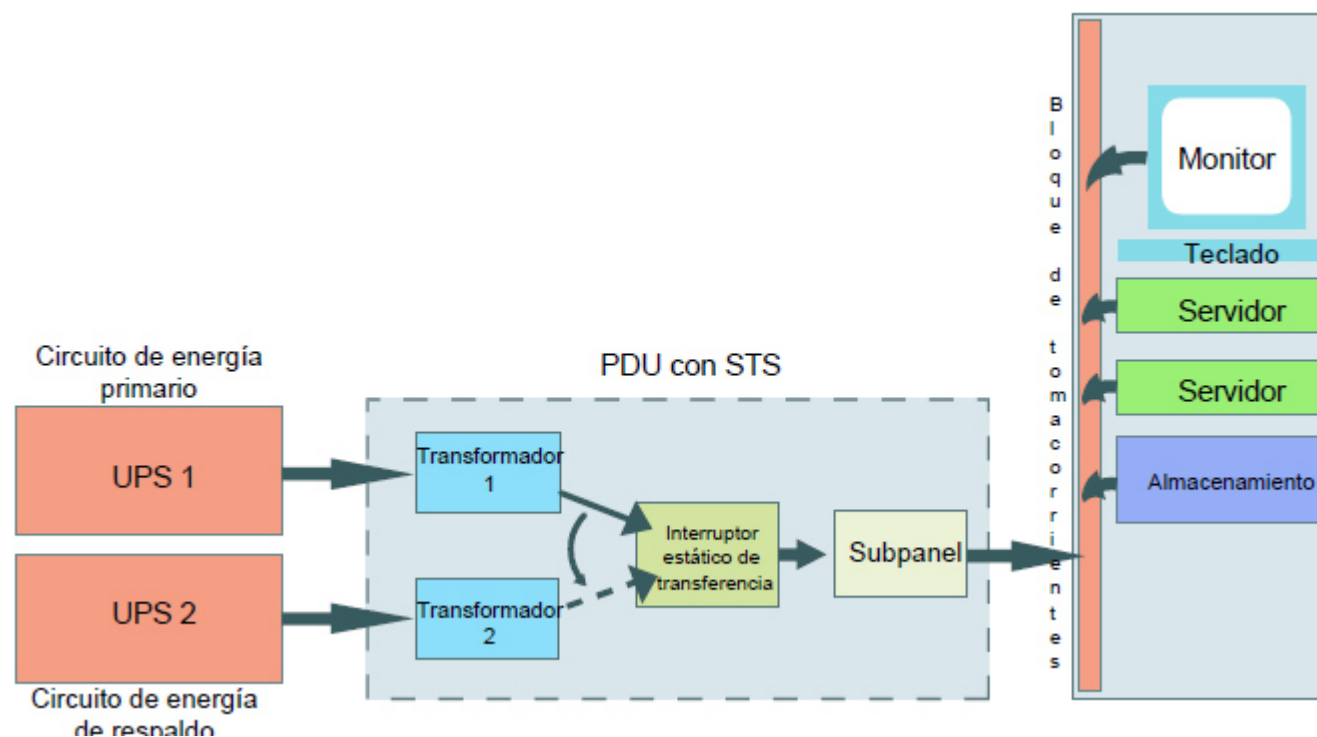


2. REDUNDANCIA EN LA CARGA CON STS



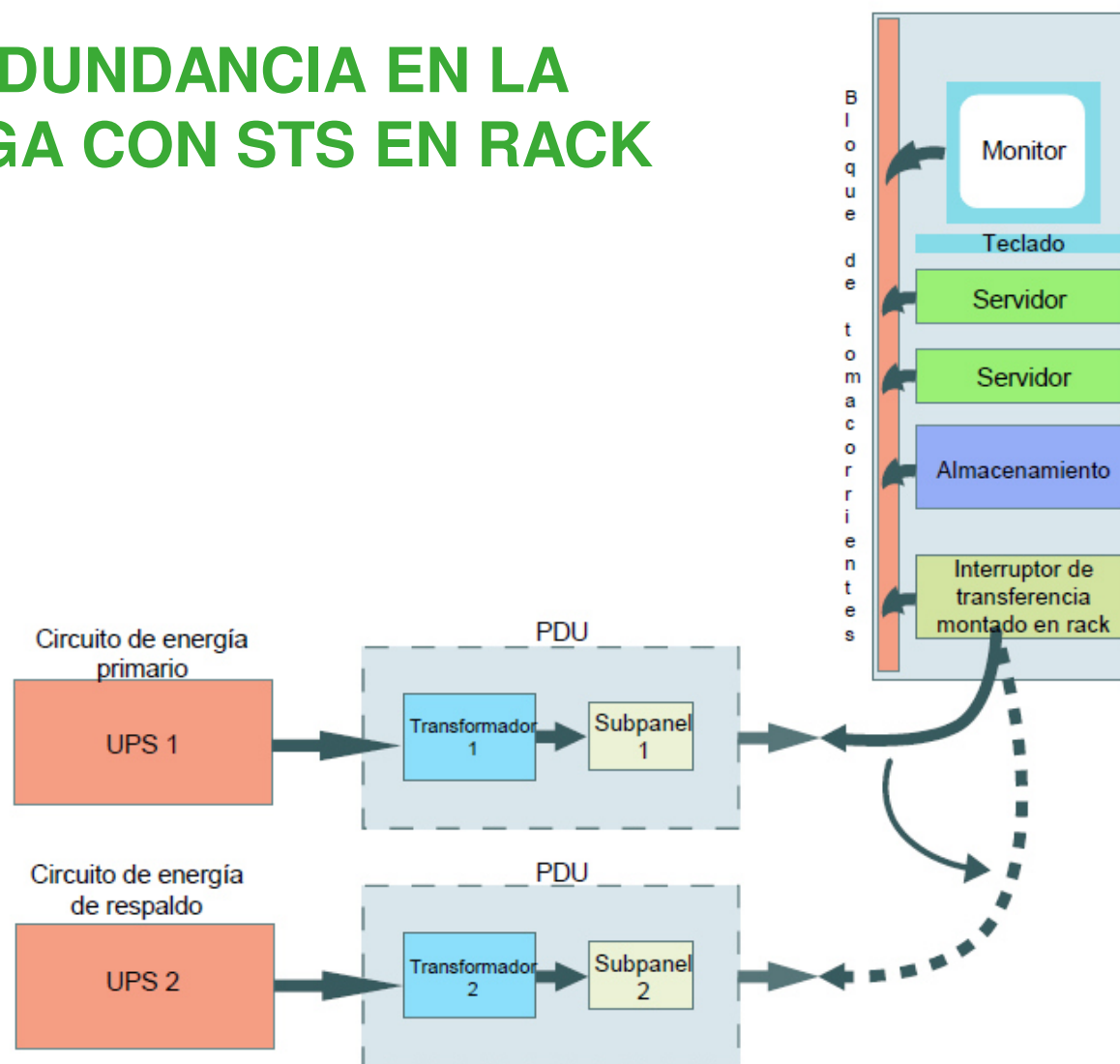


3. REDUNDANCIA EN LA CARGA CON STS Y CON TRAFOS REDUNDANTES



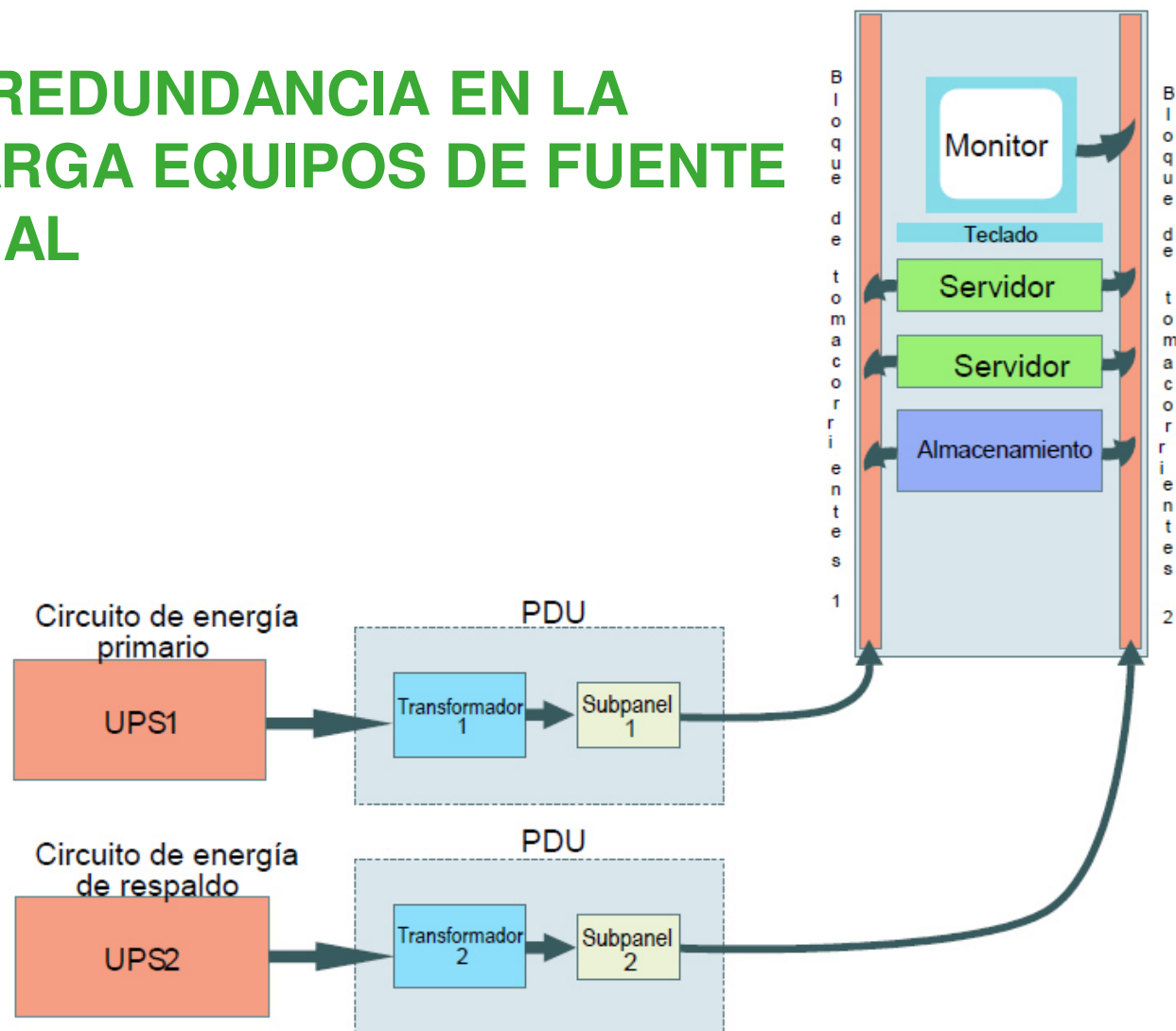


4. REDUNDANCIA EN LA CARGA CON STS EN RACK



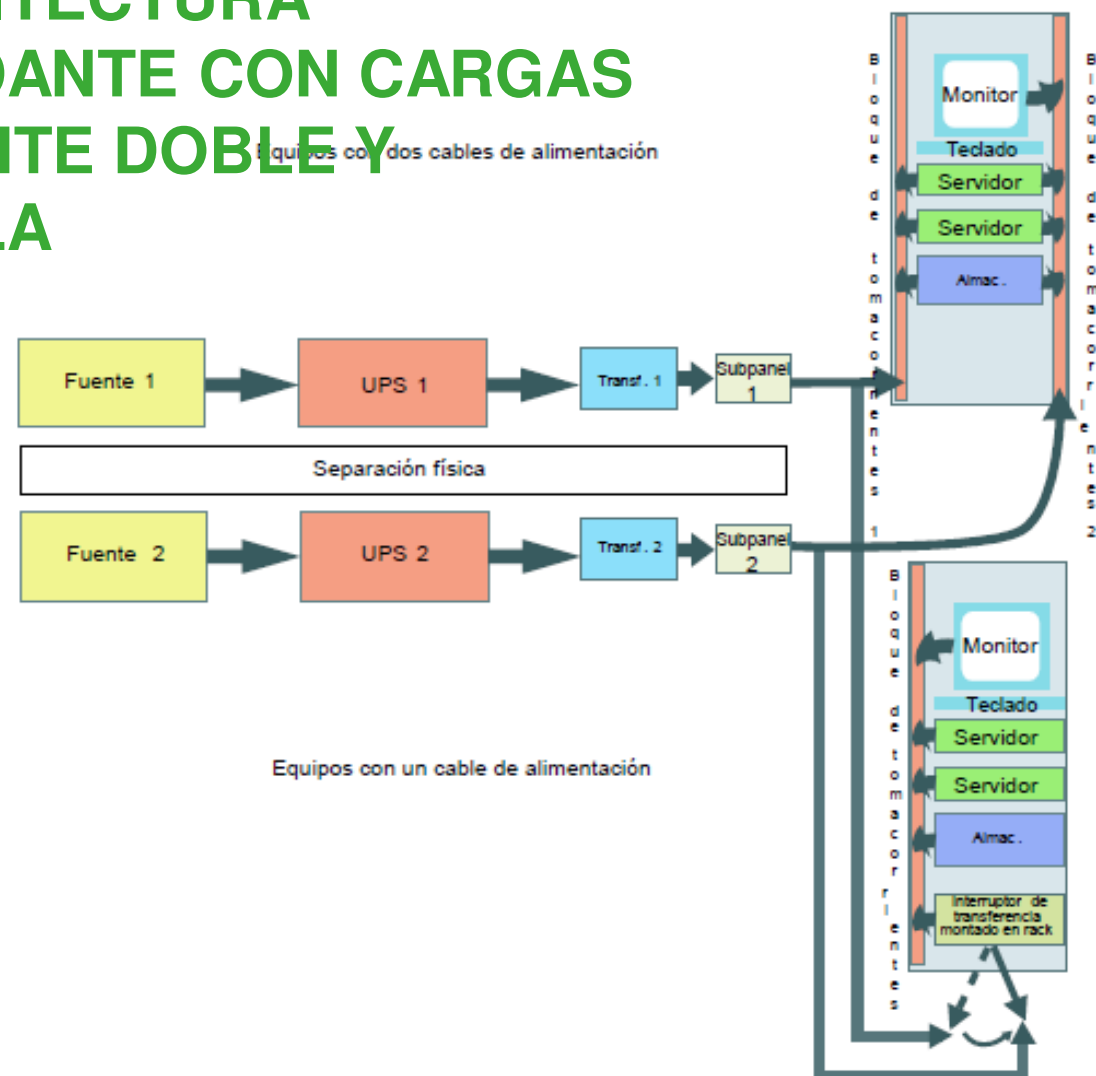


5. REDUNDANCIA EN LA CARGA EQUIPOS DE FUENTE DUAL





6. ARQUITECTURA REDUNDANTE CON CARGAS DE FUENTE DOBLE Y SENCILLA







CIBERSEGURIDAD ACORDE CON LA NORMA - ICREA-Std-131-2021 - Cap. 490

Intro:

Desde 2017, los ataques cibernéticos a infraestructuras se han incrementado un 1,000%; tan solo en 2020, los ciberdelitos acumularon un 600% de acuerdo con la firma PurpleSec. Esto pone en riesgo la continuidad operativa de los Centros de Datos, desde el acceso a servicios hasta el riesgo de pérdida de infraestructura por ataques a la configuración de software.

Definición:

International Computer Room Experts Association pone a disposición de la industria el Sello Negro de Ciberseguridad. La primer certificación de seguridad cibernética para infraestructura de Centros de Datos.

El **Sello Negro** introduce los estándares aplicables a la operación de Centros de Datos para su protección en el mundo digital, siguiendo el modelo Center Internet Security (cisecurity.org), para así brindar más seguridad a la información que reside en el Data Center.

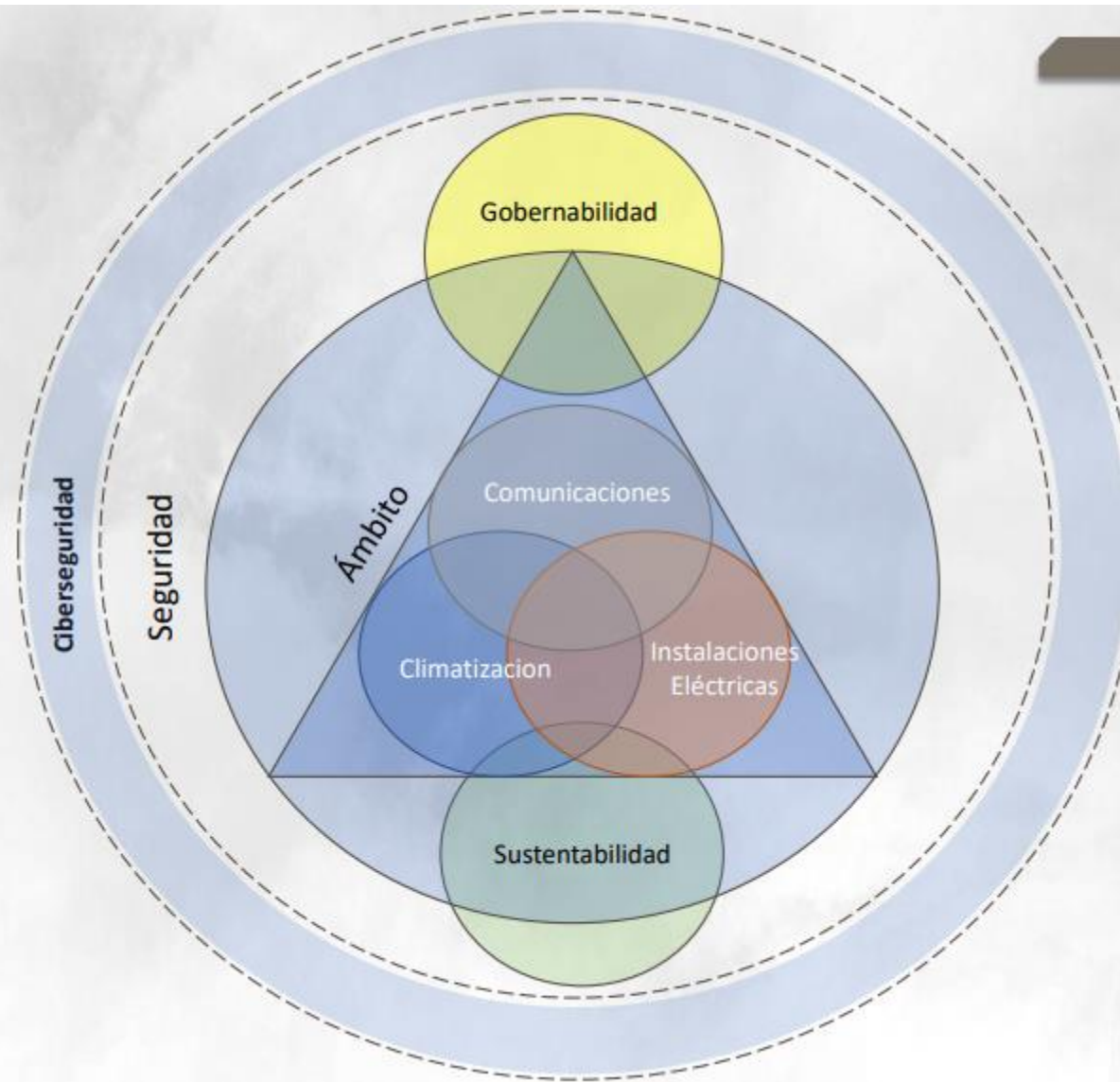
Objetivo:

Complementar la certificación de infraestructura ICREA al asegurar controles de seguridad informática para un cumplimiento de seguridad integral, disminuyendo los riesgos de pérdida, robo, suplantación o no disponibilidad de información.



Los controles de ciberseguridad se mantienen en una constante revisión por una comunidad internacional de la que forman parte nuestros expertos asociados que:

- ✓ **Comparten información** sobre ataques y atacantes, identificación de causas raíz y esto se traduce en tipos de acciones defensivas.
- ✓ Documentan historias de adopción y **comparten herramientas** para resolver problemas.
- ✓ **Dan seguimiento a la evolución de las amenazas**, las capacidades de los adversarios y los vectores actuales de intrusiones.
- ✓ **Mapean los Controles CIS a los marcos regulatorios y de cumplimiento** y dan prioridad colectiva para centrarse en ellos.
- ✓ **Identifican problemas de ciberseguridad** comunes en las organizaciones







1.- Identificar
39



2.- Proteger
80



3.- Detectar
36



4.- Responder
16

4 Disciplinas
20 Controles Maestros y
171 Subcontroles en Ciberseguridad



BASICOS



CIS Center for Internet Security
Ref. <https://www.cisecurity.org/controls>

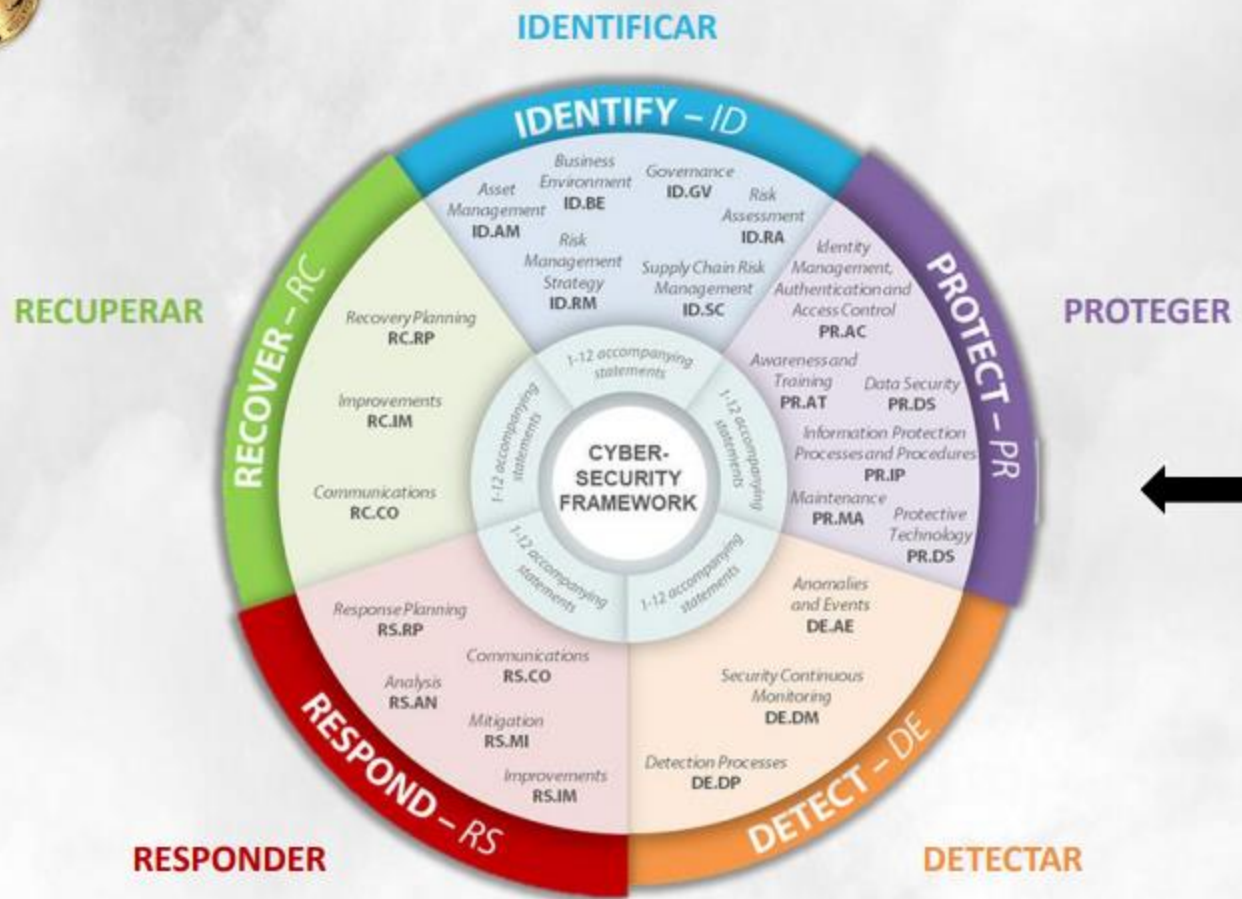


FUNDAMENTALES



ORGANIZATIVOS





*Recover - RC, será
incorporado en la
Norma ICREA 2023
(CIS V8)



Para obtener la certificación en “Sello Negro ICREA”, el Centro de Datos debe:



SHIELD: I

Cumplir con 30
subcontroles de
Ciberseguridad.



SHIELD: II

Cumplir con 61
subcontroles de
Ciberseguridad.



SHIELD: III

Cumplir con 100
subcontroles de
Ciberseguridad.



SHIELD: IV

Cumplir con 140
subcontroles de
Ciberseguridad.



SHIELD: V

Cumplir con 171
subcontroles de
Ciberseguridad.



OSCAR F. OLIVERA

318 4559471

oscar.olivera@legrand.com