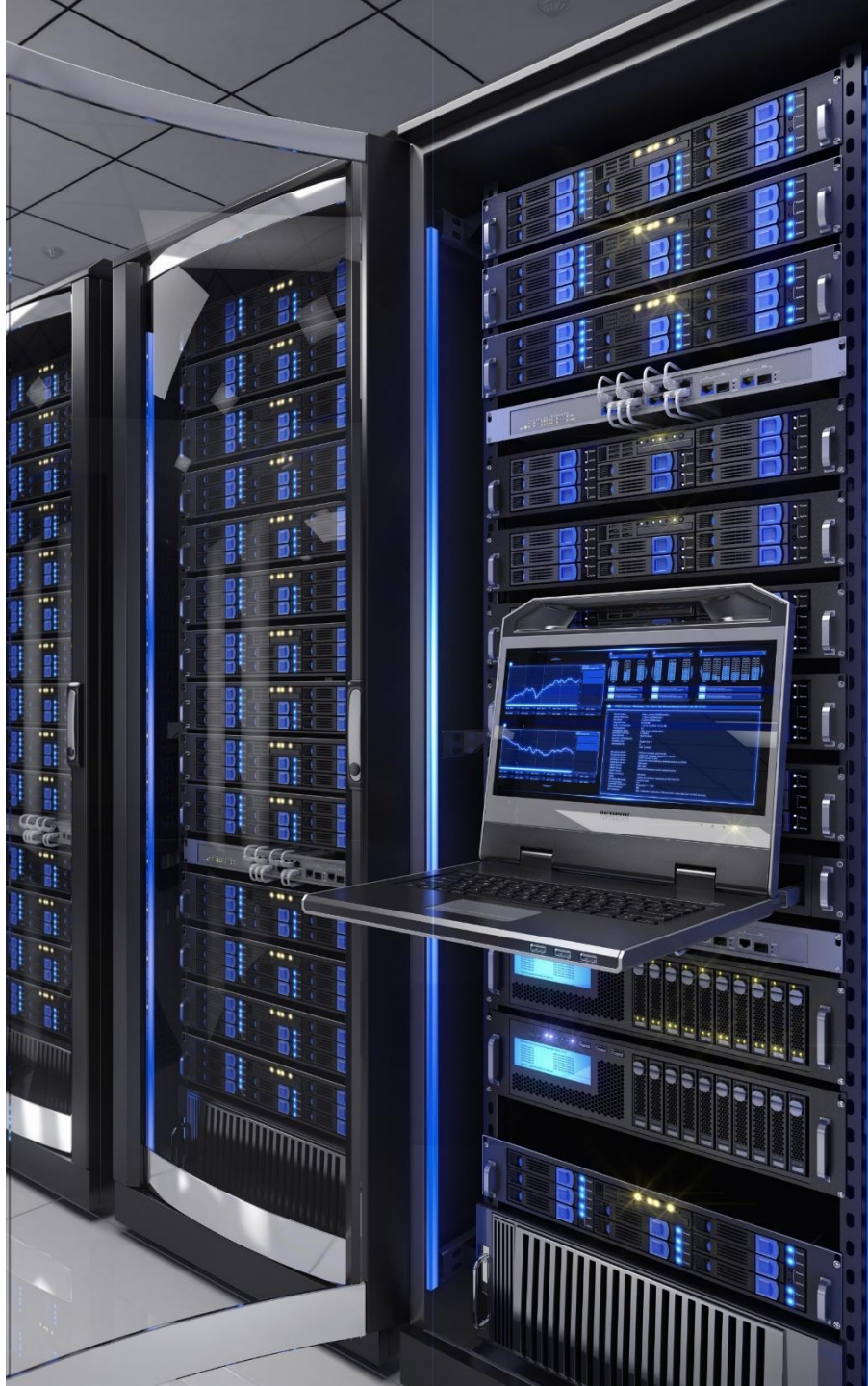
La infraestructura como pilar fundamental de la Ciberseguridad

Oscar Olivera.

Manager
Data Infrastructure and Power Quality Solutions
oscar.olivera@legrand.com – 318 455 9471

designed to be better.



CIBERSEGURIDAD

Ayudar a los negocios de todo tamaño y todo tipo a comprender, administrar, reducir y proteger tanto sus redes como sus datos.

Lo realmente importante es determinar las mejores prácticas para ayudar a decidir dónde tiene que concentrar su tiempo y su dinero en cuestiones de protección y ciberseguridad

*NIST

CIBERSEGURIDAD

- **Identificar**
- **Protección**
- **Detección**

- **Respuesta**
- **Recuperación**

IDENTIFICACIÓN

Haga una lista de todos los equipos, programas software y datos que use, incluyendo computadoras portátiles, teléfonos inteligentes, tablets y dispositivos utilizados en puntos de venta.

Elabore y comparta una política de ciberseguridad de la compañía que cubra los siguientes puntos:

- Funciones y responsabilidades de los empleados, proveedores y todo aquel que tenga acceso a datos delicados.

- Pasos a seguir para protegerse contra un ataque y limitar el daño si se produce un ataque.

PROTECCIÓN

- Controle quiénes acceden a su red y usan sus computadoras y otros dispositivos.
- Use programas de seguridad para proteger los datos.
- Codifique los datos delicados, tanto cuando estén almacenados o en tránsito.
- Haga copias de seguridad de los datos con regularidad.
- Actualice los programas de seguridad con regularidad, en lo posible, automatice estas actualizaciones.
- Implemente políticas formales para la eliminación segura de archivos electrónicos y dispositivos en desuso.
- Capacite sobre ciberseguridad a todas las personas que usen sus computadoras, dispositivos y redes. Usted puede ayudar a los empleados a comprender su riesgo personal además de la función crucial que cumplen en el lugar de trabajo.

DETECCIÓN

- Monitoree sus computadoras para controlar si detecta acceso de personal no autorizado a sus computadoras, dispositivos (soportes de almacenamiento de datos de tipo USB) y software.
- Revise su red para controlar si detecta usuarios o conexiones no autorizados.
- Investigue cualquier actividad inusual en su red o por parte de su personal.

RESPUESTA

Implemente un plan para:

- Notificar a los clientes, empleados y otros cuyos datos pudieran estar en riesgo.
- Mantener en funcionamiento las operaciones del negocio.
- Reportar el ataque a los encargados del cumplimiento de la ley y otras autoridades.
- Investigar y contener un ataque.
- Actualizar su política y plan de ciberseguridad con las lecciones aprendidas.
- Prepararse para eventos inadvertidos (como emergencias climáticas) que puedan poner en riesgo los datos.
- Ponga a prueba su plan con regularidad

RECUPERACIÓN

Después de un ataque:

- Repare y restaure los equipos y las partes de su red que resultaron afectados.
- Mantenga informados a sus empleados y clientes de sus actividades de respuesta y recuperación.

Pero y la infraestructura???

INFRAESTRUCTURA

NORMATIVIDAD

RECOMENDACIONES…
BUENAS PRACTICAS…
REFERENCIA…
REQUERIMIENTOS MÍNIMOS…

TECNOLOGIA

MARCAS…
NUMEROS DE PARTE…
1er MUNDO Vs 3r MUNDO…
REALIDADES…

RESPONSABILIDAD DEL FABRICANTE

legrand®

- EL GRUPO
- PRESENCIA MUNDIAL
- NUESTROS COMPROMISOS
- INVERSORES Y ACCIONISTAS
- PRENSA
- TRABAJANDO @ LEGRAND
- NUESTRAS SOLUCIONES
- Nuestra oferta internacional

Para informar de un problema de seguridad o solicitudes de privacidad, vaya a la siguiente página:

CIBERSEGURIDAD EN LEGRAND

Legrand está desplegando un plan maestro de ciberseguridad que tiene como objetivo fortalecer y complementar todas las medidas de protección, detección y respuesta ya implementadas como parte de su política de seguridad.

APRENDE MÁS +

CIBERSEGURIDAD PARA PRODUCTOS CONECTADOS

Los productos conectados exponen potencialmente a los clientes a riesgos específicos relacionados con la ciberdelincuencia y la seguridad de los datos. Para abordar estos riesgos, Legrand implementa un programa específico dedicado a la seguridad y el procesamiento de datos personales para dispositivos conectados, nube y aplicacione

APRENDE MÁS +

PRIVACIDAD DE DATOS

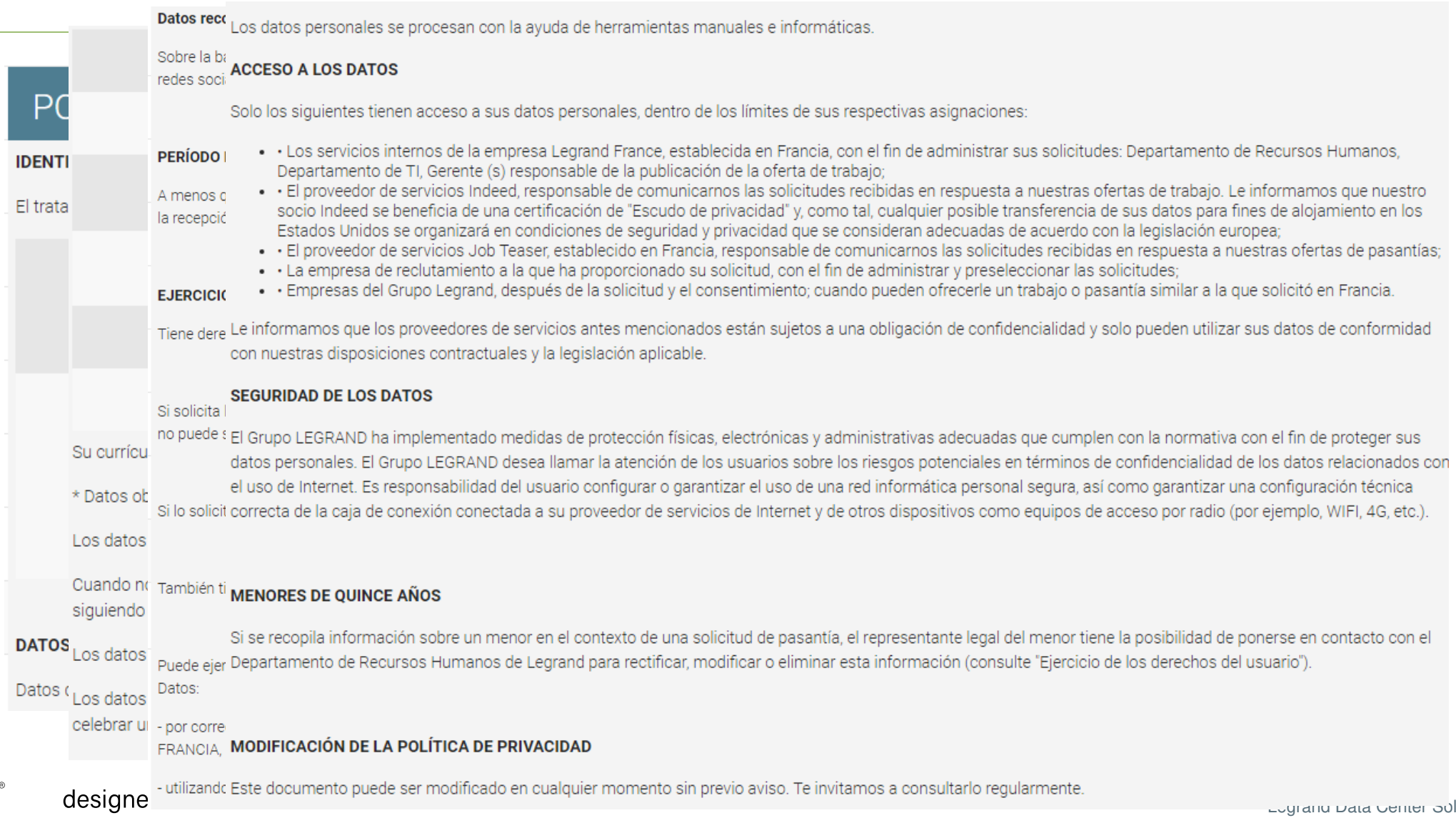
Legrand garantiza a nuestros usuarios una experiencia cada vez más fiable y segura, al tiempo que garantiza la total confidencialidad de los datos personales.

APRENDE MÁS +

PRIVACIDAD DE LOS DATOS DE RECLUTAMIENTO

APRENDE MÁS +

RESPONSABILIDAD DEL FABRICANTE



Los datos personales se procesan con la ayuda de herramientas manuales e informáticas.

ACCESO A LOS DATOS

Solo los siguientes tienen acceso a sus datos personales, dentro de los límites de sus respectivas asignaciones:

- • Los servicios internos de la empresa Legrand France, establecida en Francia, con el fin de administrar sus solicitudes: Departamento de Recursos Humanos, Departamento de TI, Gerente (s) responsable de la publicación de la oferta de trabajo;
- • El proveedor de servicios Indeed, responsable de comunicarnos las solicitudes recibidas en respuesta a nuestras ofertas de trabajo. Le informamos que nuestro socio Indeed se beneficia de una certificación de "Escudo de privacidad" y, como tal, cualquier posible transferencia de sus datos para fines de alojamiento en los Estados Unidos se organizará en condiciones de seguridad y privacidad que se consideran adecuadas de acuerdo con la legislación europea;
- • El proveedor de servicios Job Teaser, establecido en Francia, responsable de comunicarnos las solicitudes recibidas en respuesta a nuestras ofertas de pasantías;
- • La empresa de reclutamiento a la que ha proporcionado su solicitud, con el fin de administrar y preseleccionar las solicitudes;
- • Empresas del Grupo Legrand, después de la solicitud y el consentimiento; cuando pueden ofrecerle un trabajo o pasantía similar a la que solicitó en Francia.

Le informamos que los proveedores de servicios antes mencionados están sujetos a una obligación de confidencialidad y solo pueden utilizar sus datos de conformidad con nuestras disposiciones contractuales y la legislación aplicable.

SEGURIDAD DE LOS DATOS

El Grupo LEGRAND ha implementado medidas de protección físicas, electrónicas y administrativas adecuadas que cumplen con la normativa con el fin de proteger sus datos personales. El Grupo LEGRAND desea llamar la atención de los usuarios sobre los riesgos potenciales en términos de confidencialidad de los datos relacionados con el uso de Internet. Es responsabilidad del usuario configurar o garantizar el uso de una red informática personal segura, así como garantizar una configuración técnica correcta de la caja de conexión conectada a su proveedor de servicios de Internet y de otros dispositivos como equipos de acceso por radio (por ejemplo, WIFI, 4G, etc.).

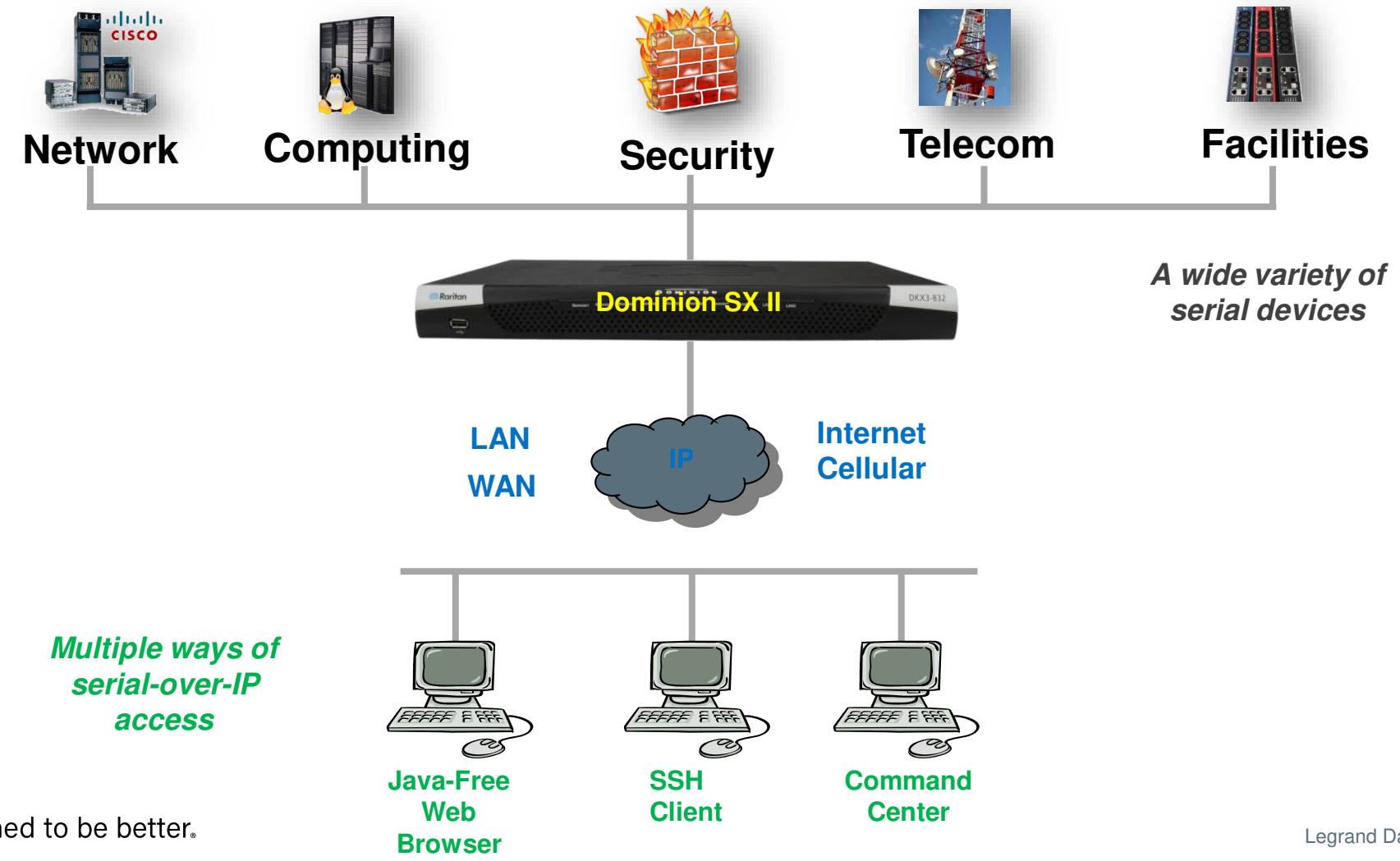
MENORES DE QUINCE AÑOS

Si se recopila información sobre un menor en el contexto de una solicitud de pasantía, el representante legal del menor tiene la posibilidad de ponerse en contacto con el Departamento de Recursos Humanos de Legrand para rectificar, modificar o eliminar esta información (consulte "Ejercicio de los derechos del usuario").

MODIFICACIÓN DE LA POLÍTICA DE PRIVACIDAD

Este documento puede ser modificado en cualquier momento sin previo aviso. Te invitamos a consultarlo regularmente.

INTEGRACIÓN VS ACCESO



Raritan Secure Switch

National Information Assurance Partnership

Common Criteria Certificate

is awarded to

Raritan, Inc.

for

Raritan Secure KVM Switch Series (model RSS-102, RSS-102C, RSS-104, RSS-104C)

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 3.1) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Date Issued: 2018-02-13

Validation Report Number: CCEVS-VR-VID10865-2018

CCTL: Leidos Common Criteria Testing Laboratory

Assurance Level: PP Compliant

Protection Profile Identifier:
Protection Profile for Peripheral Sharing Switch Version 3.0

Original Signed By
Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Original Signed By
Deputy National Manager National Security Systems
National Security Agency

INFRAESTRUCTURA

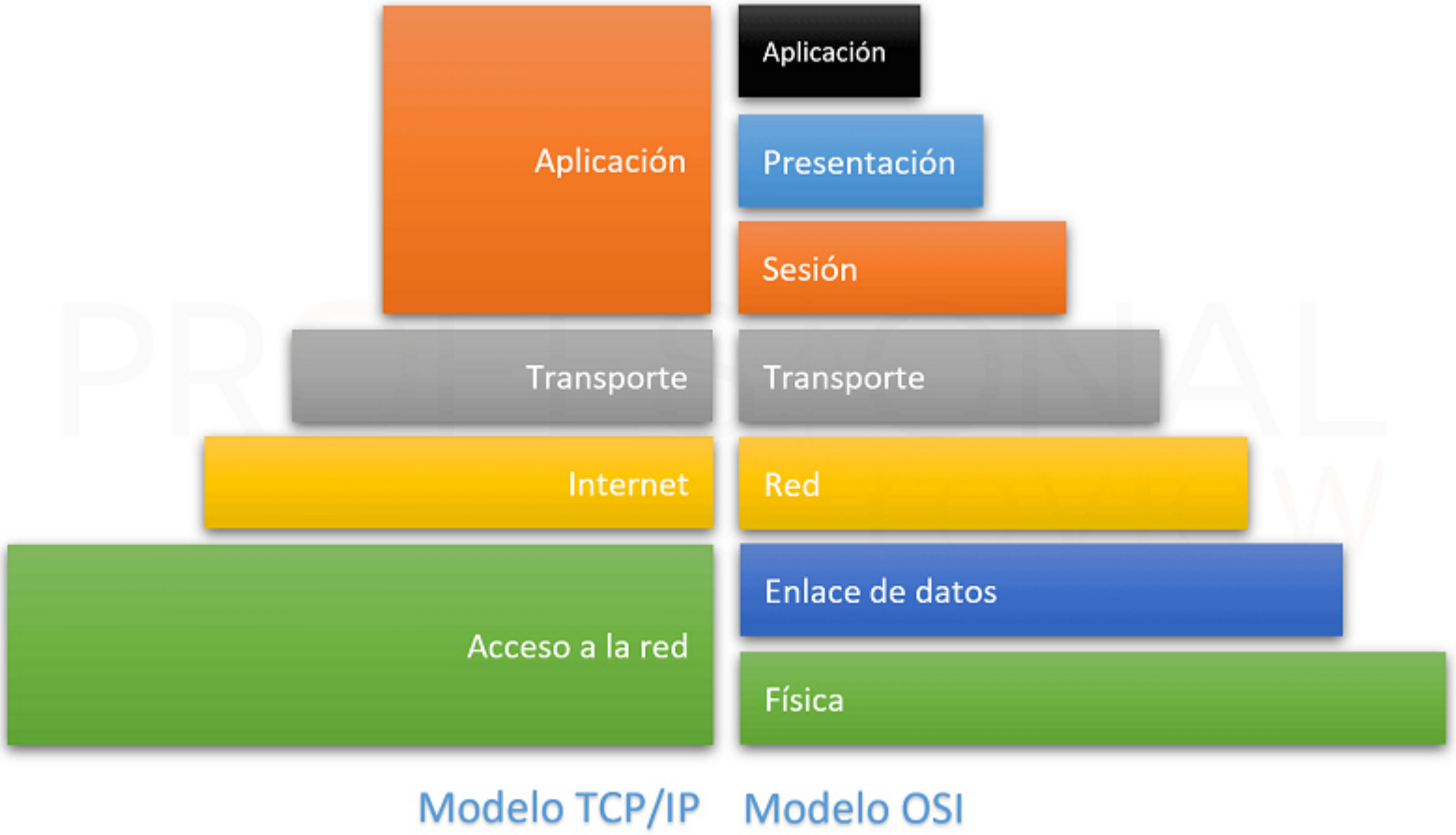
PARA PROYECTOS DE TECNOLOGÍA ES NECESARIO

COMPATIBILIDAD

INFRAESTRUCTURA ELECTRICA

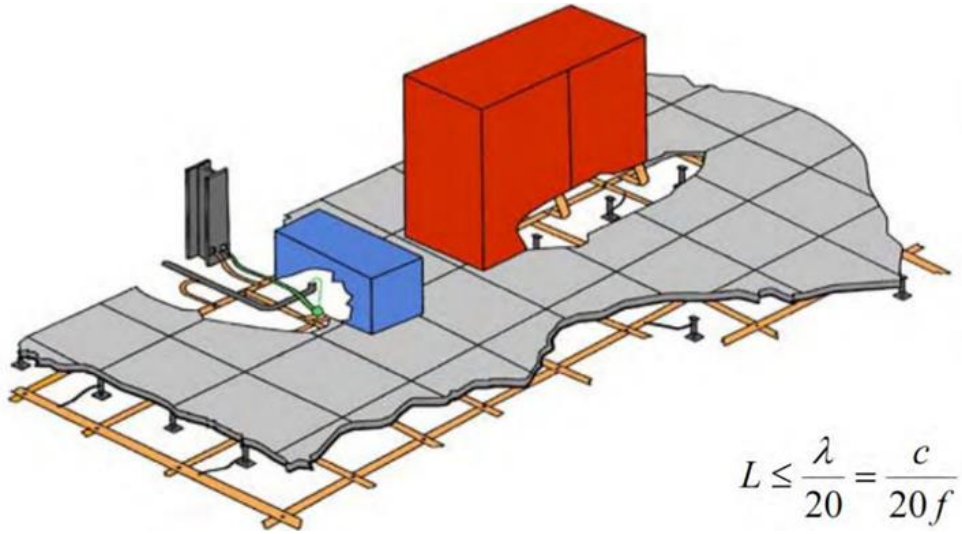
INFRAESTRUCTURA TELECOMUNCIACIONES

INFRAESTRUCTURA

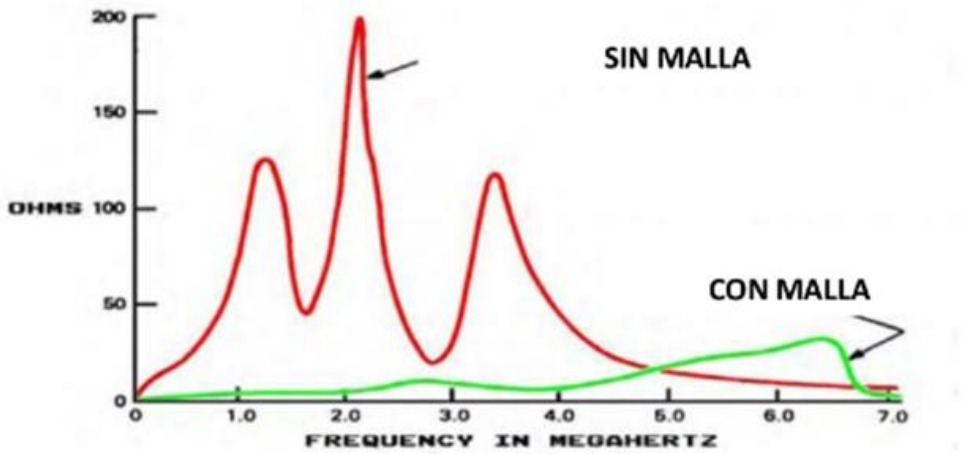


INFRAESTRUCTURA ELECTRICA

(Signal Reference Grid)

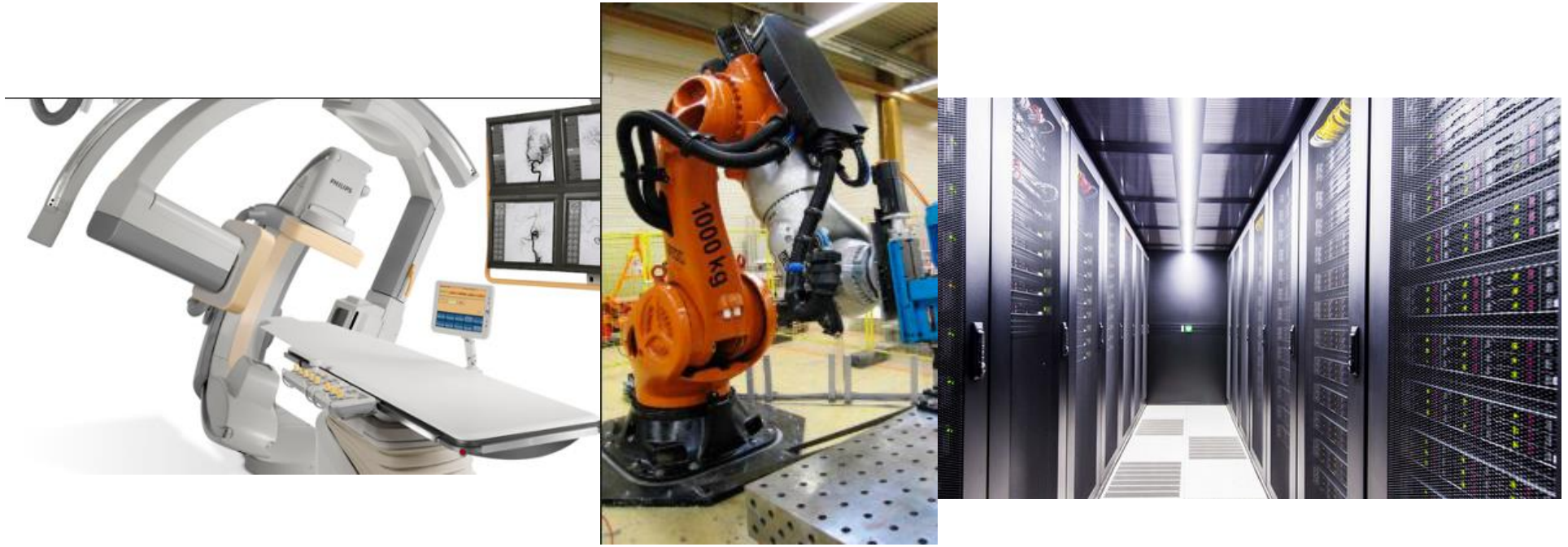


Señales de interferencia en equipos de alta frecuencia



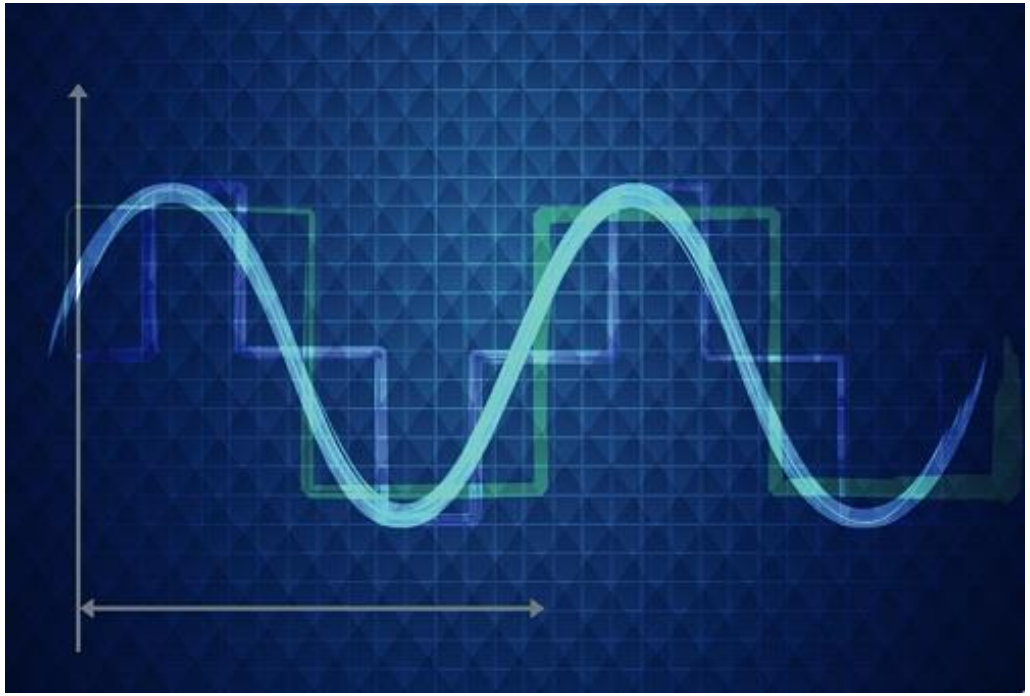
INFRAESTRUCTURA ELECTRICA

CADA CARGA CRITICA-SENSIBLE TIENE "REQUERIMIENTOS ELECTRICOS ESPECIFICOS"



INFRAESTRUCTURA ELECTRICA

…DESDE LOS EQUIPOS



INFRAESTRUCTURA ELECTRICA

CLASIFICACIÓN EN 62040-3

XXX	YY	ZZZ
Dependencia de la salida respecto de la entrada	Forma de onda en salida	Prestaciones dinámicas en salida

CLASIFICACIÓN EN 62040-3

VFI	SS	111
VI	XX	112
VFD	YY	113

Los SAI con mejores prestaciones tienen clasificación: VFI SS 111

La primera parte de la clasificación (XXX) define el tipo de SAI:

- **VFI** (Voltage and Frequency Independent): se trata del SAI en el cual la salida es independiente de las variaciones de la tensión de alimentación (red) y las variaciones de frecuencia son controladas dentro de los límites prescritos por la norma IEC EN 61000-2-2.
- **VFD** (Voltage and Frequency Dependent): se trata del SAI en el cual la salida depende de la variación de la tensión de alimentación (red) y de las variaciones de frecuencia.
- **VI** (Voltage Independent): se trata del SAI en el cual las variaciones de la tensión de alimentación son estabilizadas por dispositivos de regulación electrónicos/pasivos dentro de los límites del funcionamiento normal.

La segunda parte del código de clasificación (YY) define la forma de la onda de salida durante el funcionamiento normal y con batería:

- **SS**: sinusoidal (THDu < 8%)
- **XX**: sinusoidal con carga lineal; no-sinusoidal con carga distorsionante (THDu > 8%)
- **YY**: no sinusoidal

La tercera parte del código de clasificación (ZZZ) define la prestación dinámica de la tensión de salida a las variaciones de carga en tres condiciones diferentes:

- **111** variaciones de las modalidades operativas (normal y con batería),
- **112** inserción de la carga lineal escalonada en modo normal o con batería,
- **113** inserción de la carga no-lineal escalonada en modo normal o con batería.

INFRAESTRUCTURA ELECTRICA

Annex F
(normative)

Tables

Table F.1 – Rated impulse voltage for equipment energized directly from the low-voltage mains

Nominal voltage of the supply system [1] based on IEC 60038 [3]		Voltage line to neutral derived from nominal voltages a.c. or d.c. up to and including	Rated impulse voltage [2]			
			Overvoltage category [4]			
Three phase	Single phase		I	II	III	IV
V	V	V	V	V	V	V
		50	330	500	800	1 500
		100	500	800	1 500	2 500
	120-240	150 [5]	800	1 500	2 500	4 000
230/400 277/480		300	1 500	2 500	4 000	6 000
400/690		600	2 500	4 000	6 000	8 000
1 000		1 000	4 000	6 000	8 000	12 000

1) See Annex B for application to existing different low-voltage mains and their nominal voltages.

2) Equipment with these rated impulse voltages can be used in installations in accordance with IEC 60364-4-44.

3) The / mark indicates a four-wire three-phase distribution system. The lower value is the voltage line-to-neutral, while the higher value is the voltage line-to-line. Where only one value is indicated, it refers to three-wire, three-phase systems and specifies the value line-to-line.

4) See 4.3.3.2.2 for an explanation of the overvoltage categories.

5) Nominal voltages for single-phase systems in Japan are 100 V or 100-200 V. However, the value of the rated impulse voltage for the voltages is determined from columns applicable to the voltage line to neutral of 150 V (See Annex B).

designed to be better.

INFRAESTRUCTURA ELECTRICA

420.11 Transformadores:

Los transformadores que alimenten ambientes TIC deberán soportar contenidos armónicos importantes y corrientes de excitación de hasta 400 veces las corrientes nominales de los equipos; por lo que estos transformadores deberán ser del tipo de alto factor K.

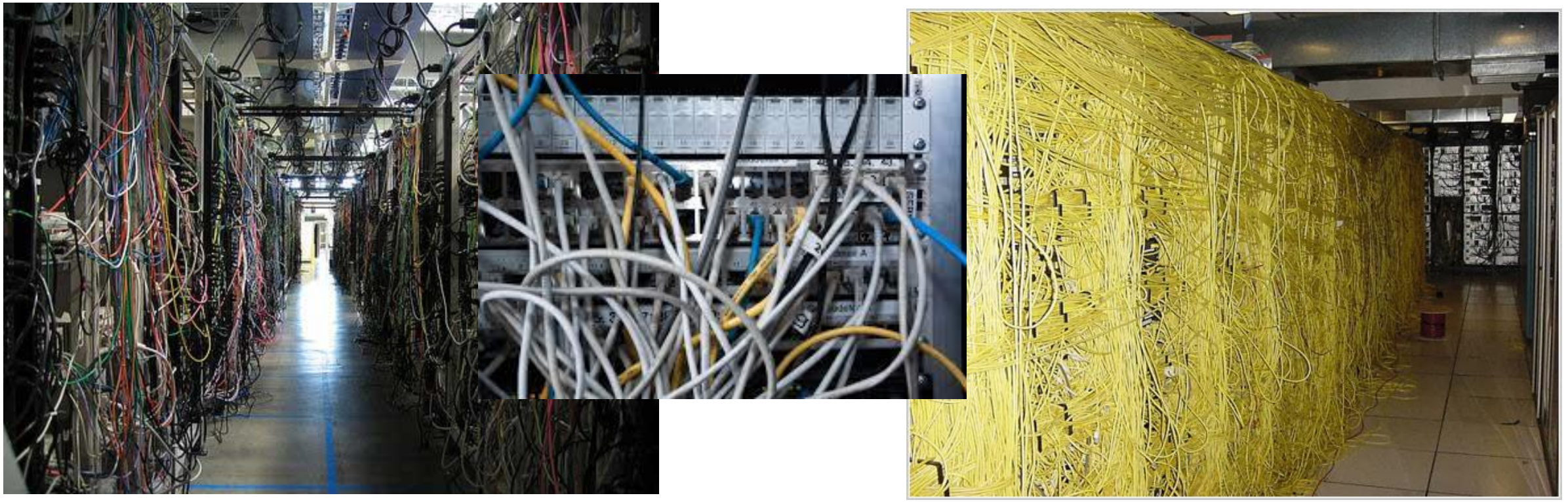
El factor K para subestaciones que alimenten equipos de TIC no podrá ser menor a K3.

El factor K no podrá ser menor a 20 en zonas posteriores a los UPS.

Deberá contar con todas las protecciones tal y como lo establece el NEC-450, 240 y 250.

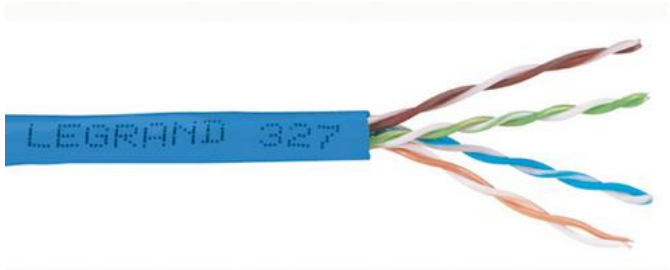
Los transformadores de factor K podrán ser sustituidos por arreglos que garanticen que estos no se sobrecalienten por el manejo excesivo de armónicas provenientes de las cargas variables típicas de los CPD.

INFRAESTRUCTURA DE TELECOMUNICACIONES



INFRAESTRUCTURA DE TELECOMUNICACIONES

- Cableado de par trenzado balanceado de 100 ohm

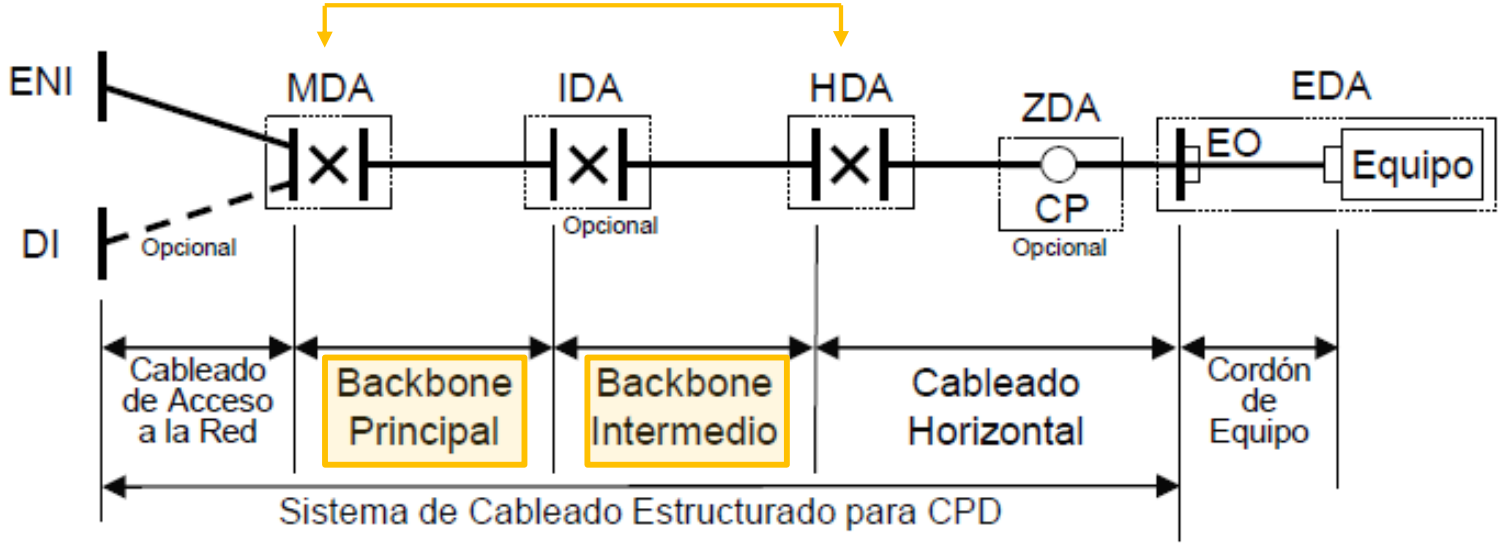


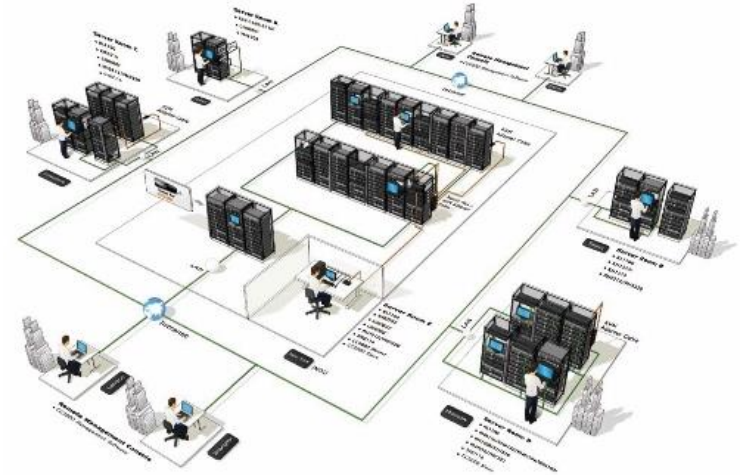
- Fibra óptica multimodo o monomodo

INFRAESTRUCTURA DE TELECOMUNICACIONES

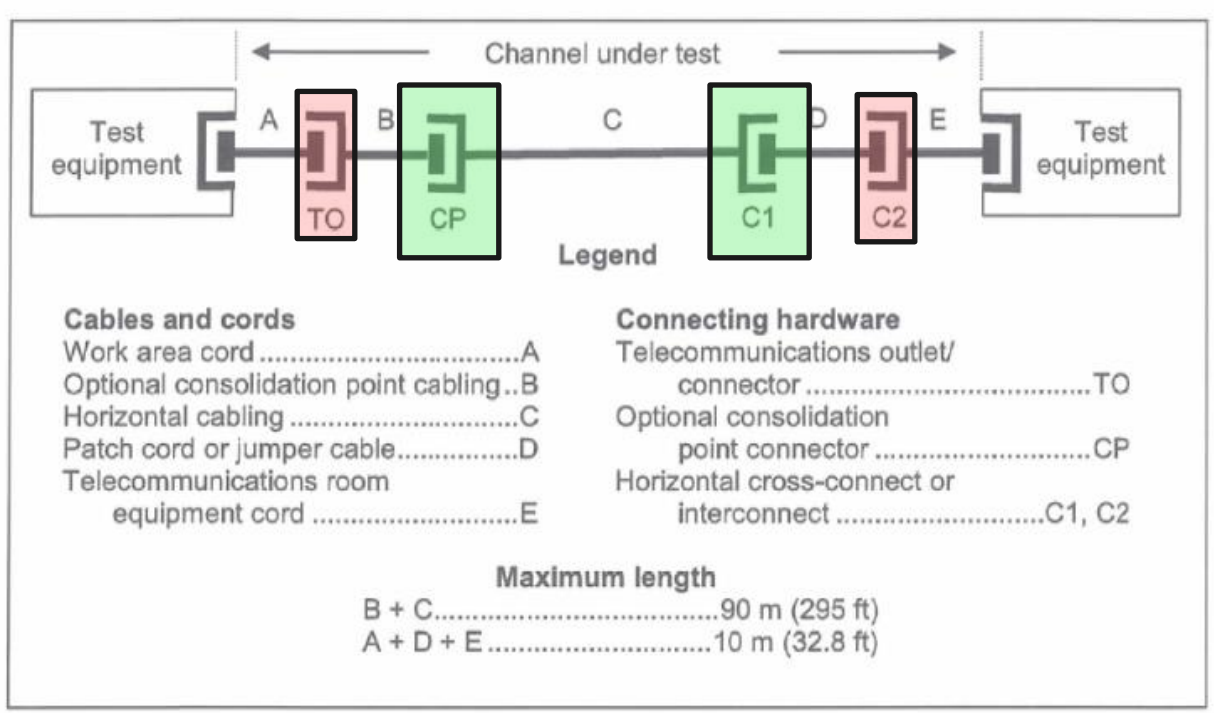
EF

SUBSISTEMAS





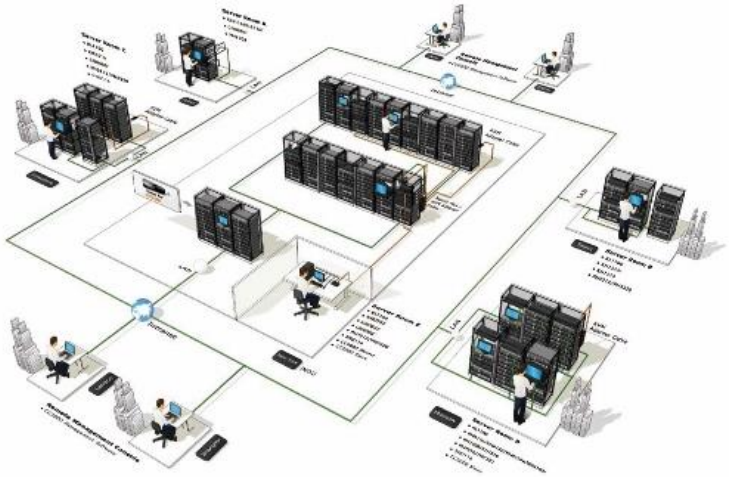
INFRAESTRUCTURA DE TELECOMUNICACIONES



Se permite un máximo de 4 conexiones para aplicaciones de las aplicaciones

Máximo 2 conexiones para aplicaciones a 40G

SHORT LINK



INFRAESTRUCTURA DE TELECOMUNICACIONES

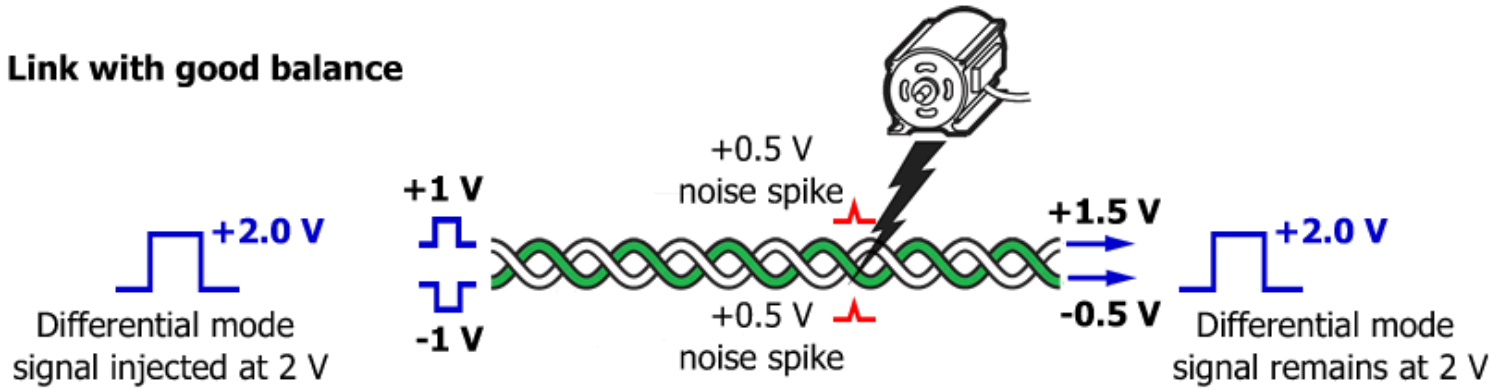
TCL : pérdida de conversión transversal (Transverse Conversion Loss)
TCTL: pérdida de transferencia de conversión transversal
ELTCTL: pérdida de transferencia de conversión transversal de mismo nivel (Equal Level Transverse Conversion Transfer Loss)

Tanto TCL como ELTCTL son mediciones importantes en los estándares de cableado. Definen un rendimiento mínimo para el equilibrio, el parámetro clave para ayudar a determinar la inmunidad al ruido.

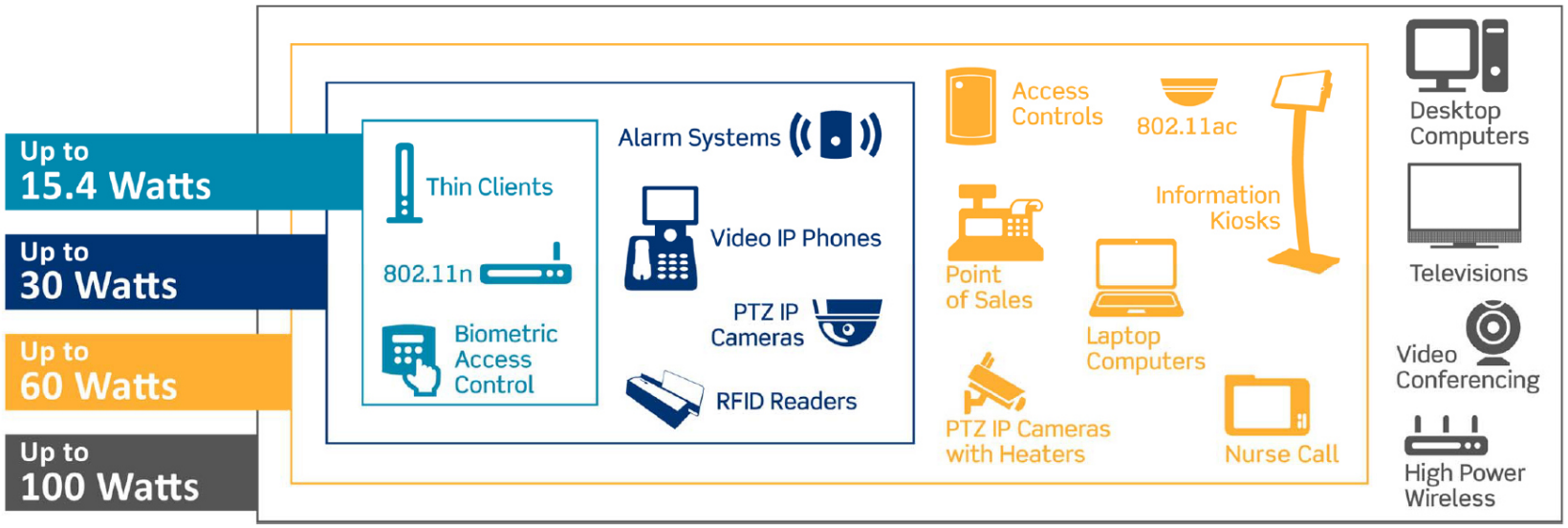
CM: Modo Común : RF y otras interferencias, energía, cc, etc,
DM: Modo Diferencial: desfasado 180 grados.

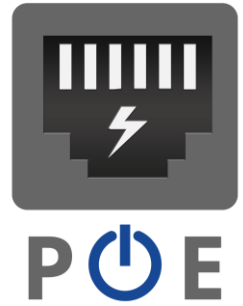
TCL (dB): cat 6a/F/FA es de 20,3..... Especificados a 30Mhz
ELTCL(dB): cat 6a (0,5) + (0,3)

CDNEXT (common-mode to differential mode near-end crosstalk)



INFRAESTRUCTURA DE TELECOMUNICACIONES





IEC 60512-99-002
IEEE 802.3bt

La conclusión…?

1. Conocer mi infraestructura física (comunicaciones, eléctrica, mecánica y facilities), tanto desde el diseño como en la implementación.
2. Conocer los equipos instalados (operativos y no operativos), más la proyección.
3. Conocer las políticas, (fortalezas y debilidades) de los fabricantes que elegí tanto a nivel operativo de cada equipo como en Ciber seguridad y tomar las acciones pertinentes.

AHORA SI…
PODEMOS HABLAR DE CONFIABILIDAD Y DISPONIBILIDAD

legrand®

OSCAR F. OLIVERA
318 4559471
oscar.olivera@legrand.com