

# Tecnología de la información. Instalaciones e infraestructuras de centros de datos. Parte 1: Conceptos generales

Information technology. Data centre facilities and infrastructures. Part 1: General concepts

(EQV. ISO/IEC TS 22237-1:2018 Information technology - Data centre facilities and infrastructures - Part 1: General concepts)

**2019-12-27**  
**1ª Edición**

R.D. N° 030-2019-INACAL/DN. Publicada el 2020-01-07

Precio basado en 36 páginas

I.C.S.: 35.020

ESTA NORMA ES RECOMENDABLE

Descriptores: Tecnología de información, instalación, infraestructura, centro de datos, conceptos generales

© ISO/IEC 2018

Todos los derechos son reservados. A menos que se especifique lo contrario, ninguna parte de esta publicación podrá ser reproducida o utilizada por cualquier medio, electrónico o mecánico, incluyendo fotocopia o publicándolo en el Internet o intranet, sin permiso por escrito del INACAL, único representante de la ISO/IEC en territorio peruano.

© INACAL 2019

Todos los derechos son reservados. A menos que se especifique lo contrario, ninguna parte de esta publicación podrá ser reproducida o utilizada por cualquier medio, electrónico o mecánico, incluyendo fotocopia o publicándolo en el internet o intranet, sin permiso por escrito del INACAL.

INACAL

Calle Las Camelias 817, San Isidro  
Lima - Perú  
Tel.: +51 1 640-8820  
[publicaciones@inacal.gob.pe](mailto:publicaciones@inacal.gob.pe)  
[www.inacal.gob.pe](http://www.inacal.gob.pe)

# ÍNDICE

	página
ÍNDICE	ii
PRÓLOGO	iii
PRÓLOGO (ISO)	vi
INTRODUCCIÓN	viii
1 Objeto y campo de aplicación	1
2 Referencias normativas	2
3 Términos, definiciones y términos abreviados	3
3.1 Términos y definiciones	3
3.2 Términos abreviados	9
4 Conformidad	10
5 Análisis de riesgo del negocio	10
5.1 General	10
5.2 Análisis de costo de tiempo de inactividad	11
5.3 Análisis de riesgo	12
6 Visión general del diseño de centro de datos	14
6.1 General	14
6.2 Espacios e instalaciones	15
7 Sistema de clasificación para centro de datos	18
7.1 General	18
7.2 Disponibilidad	19
7.3 Seguridad física	21
7.3.1 General	21
7.3.2 Protección contra el acceso no autorizado	22
7.3.3 Protección contra eventos ambientales	23
7.4 Habilitación de eficiencia energética	25
7.4.1 General	25
7.4.2 Sistema de distribución de energía	26
7.4.3 Seguimiento y control ambiental	26
ANEXO A (informativo) Principios generales de diseño	27
BIBLIOGRAFÍA	36

## PRÓLOGO

### A. RESEÑA HISTÓRICA

A.1 El Instituto Nacional de Calidad - INACAL, a través de la Dirección de Normalización es la autoridad competente que aprueba las Normas Técnicas Peruanas a nivel nacional. Es miembro de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), en representación del país.

A.2 El presente Proyecto de Especificación Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Centro de datos y ambientes de TI, mediante el Sistema 1 o de Adopción, durante los meses de febrero a junio de 2019, utilizando como antecedente a la norma ISO/IEC TS 22237-1:2018 Information technology. Data center facilities and infrastructures. Part 1: General concepts.

A.3 El Comité Técnico de Normalización de Centro de datos y ambientes de TI presentó a la Dirección de Normalización -DN-, con fecha 2019-11-05, el PETP-ISO/IEC TS 22237-1:2019, para su revisión y aprobación, siendo sometido a la etapa de discusión pública el 2019-11-22. No habiéndose recibido observaciones, fue oficializada como Norma Técnica Peruana **ETP-ISO/IEC TS 22237-1:2019 Tecnología de la información. Instalaciones e infraestructuras de centros de datos - Parte 1: Conceptos generales**. 1ª Edición, el 07 de enero de 2020.

A.4 El presente Proyecto de Especificación Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada de acuerdo a las Guías Peruanas GP 001:2016 y GP 002:2016.

### B. INSTITUCIONES QUE PARTICIPARON EN LA ELABORACIÓN DE LA ESPECIFICACIÓN TÉCNICA PERUANA

Secretaría

Universidad Nacional Federico Villareal -  
Facultad de Ingeniería Electrónica e  
Informática

Secretario

Francisco Madrid Cisneros

**ENTIDAD****REPRESENTANTE**

ASOCIACIÓN DE USUARIOS DE  
INTERNET DEL PERÚ

Andree Ronaldo Ramirez Mejia

BICSI PERÚ

Yuri William Bravo Asencios  
Rosalia Zarate Vargas

COLEGIO DE ARQUITECTOS DEL PERU  
LIMA

Eva Constanza Remar Castro

COLEGIOS DE INGENIEROS DEL PERU  
CUSCO

Julio Revatta Tagle

ENGINE TECH E. I. R. L.

Carlos Diaz Neyra

ELPA

Claudio Silva De La Jara

FLUKE NETWORKS

Alvaro Jesús Cayo Urrutia  
Maria Guadalupe Zuñiga Rodriguez

FURUKAWA

Fernando Alberto Fuenmayor Rubio  
Itzel Bustinza Angulo

GMD

Ramon Castro Carpio  
Jose Palacios Perleche

INTEGRITY

Juan Carlos Espinoza Revilla

LEGRAND-TICINO

Jorge Luis Alcántara Gavidia

PANDUIT

Pablo Huapaya Bardi

PCM - SEGDI

Cesar Vilchez Inga

SAPIA

Marco Antonio Ayala Travezaño

SATRA PERU

Guido Mitchell Yauri Castro

SIEMON

Jorge Manuel Barrionuevo Delgado  
Daniel Arce Escalante

UAP

Juan Carlos Marca Delgado  
Julio Cernaque Vera

UNFV

Jose Enrique Pastor Castillo

UNMSM

Winston Ugaz Cachay

VERTIV PERU

Cesar Linares Solorzano  
Fernando Llaque Godard

**"PROHIBIDA SU REPRODUCCIÓN Y/O COMERCIALIZACIÓN"**

## **PRÓLOGO (ISO)**

ISO (la Organización Internacional de Normalización) e IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la estandarización mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos por la organización respectiva para tratar campos específicos de actividad técnica. Los comités técnicos de ISO y IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en colaboración con ISO e IEC, también participan en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, ISO/IEC JTC 1.

Los procedimientos utilizados para desarrollar este documento y los destinados a su mantenimiento adicional se describen en las Directivas ISO/IEC, Parte 1. En particular, deben tenerse en cuenta los diferentes criterios de aprobación necesarios para los diferentes tipos de documentos. Este documento se redactó de acuerdo con las reglas editoriales de las Directivas ISO/IEC, Parte 2 (consulte [www.iso.org/directives](http://www.iso.org/directives)).

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan ser objeto de derechos de patente. ISO e IEC no serán responsables de la identificación de cualquiera o todos los derechos de patente. Los detalles de cualquier derecho de patente identificado durante el desarrollo del documento estarán en la Introducción y/o en la lista ISO de declaraciones de patentes recibidas (véase [www.iso.org/patents](http://www.iso.org/patents)).

Cualquier nombre comercial utilizado en este documento es información que se proporciona para la comodidad de los usuarios y no constituye un aval.

Para obtener una explicación sobre el significado de los términos y expresiones específicos de ISO relacionados con la evaluación de la conformidad, así como información sobre la adhesión de ISO a los principios de la Organización Mundial del Comercio (OMC) en los Obstáculos Técnicos al Comercio (OTC), consulte la siguiente URL: [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html).

Este documento fue preparado por el Comité Técnico ISO/IEC JTC1, Tecnología de la Información, Subcomité SC 39, Sostenibilidad para y por la Tecnología de la Información.

Puede encontrar una lista de todas las partes de la serie ISO/IEC TS 22237 en el sitio web de ISO.

**"PROHIBIDA SU REPRODUCCIÓN Y/O COMERCIALIZACIÓN"**



## INTRODUCCIÓN

El acceso irrestricto a la información basada en internet demandada por la sociedad de la información ha llevado a un crecimiento exponencial tanto del tráfico de Internet como del volumen de datos almacenados/recuperados. Los centros de datos alojan y respaldan la tecnología de la información y los equipos de red de telecomunicaciones para el procesamiento de datos, almacenamiento de datos y transporte de datos. Son necesarios tanto por los operadores de red (que prestan esos servicios a las instalaciones del cliente) como por las empresas que se encuentran dentro de esas instalaciones del cliente.

Los centros de datos necesitan proporcionar instalaciones e infraestructuras modulares, escalables y flexibles para adaptarse fácilmente a los requisitos rápidamente cambiantes del mercado. Además, el consumo de energía de los centros de datos se ha vuelto crítico tanto desde el punto de vista medioambiental (reducción de la huella de carbono) como con respecto a consideraciones económicas (costo de la energía) para el operador del centro de datos.

La implementación de centros de datos varía en términos de:

- a) propósito (empresa, co-ubicación, co-alojamiento (co-hosting), u operador de red);
- b) nivel de seguridad;
- c) tamaño físico;
- d) ubicación (construcciones móviles, temporales y permanentes).

Las necesidades de los centros de datos también varían en términos de la disponibilidad del servicio, la provisión de seguridad y los objetivos para la eficiencia energética. Estas necesidades y objetivos influyen en el diseño de los centros de datos en términos de construcción de edificio, distribución de energía, control medioambiental y seguridad física. Se requiere de gestión efectiva e información operativa para monitorear el logro de las necesidades y objetivos definidos.

La serie ISO/IEC TS 22237 especifica requisitos y recomendaciones para respaldar las distintas partes involucradas en el diseño, planificación, adquisición, integración, instalación, operación y mantenimiento de instalaciones e infraestructuras dentro de los centros de datos. Estas partes incluyen:

- 1) propietarios, gerentes de instalaciones, gerentes de TIC, gerentes de proyectos, contratistas principales;
- 2) arquitectos, consultores, diseñadores de edificios y constructores, diseñadores de sistema y de instalaciones;
- 3) proveedores de equipos;
- 4) instaladores, mantenedores.

En el momento de la publicación del presente documento, la serie ISO/IEC TS 22237 comprenderá los siguientes documentos:

ISO/IEC TS 22237-1, Tecnología de la información – Instalaciones e infraestructuras de centros de datos – Parte 1: Conceptos generales;

ISO/IEC TS 22237-2, Tecnología de la información – Instalaciones e infraestructuras de centros de datos – Parte 2: Construcción de edificio;

ISO/IEC TS 22237-3, Tecnología de la información – Instalaciones e infraestructuras de centros de datos – Parte 3: Distribución de energía;

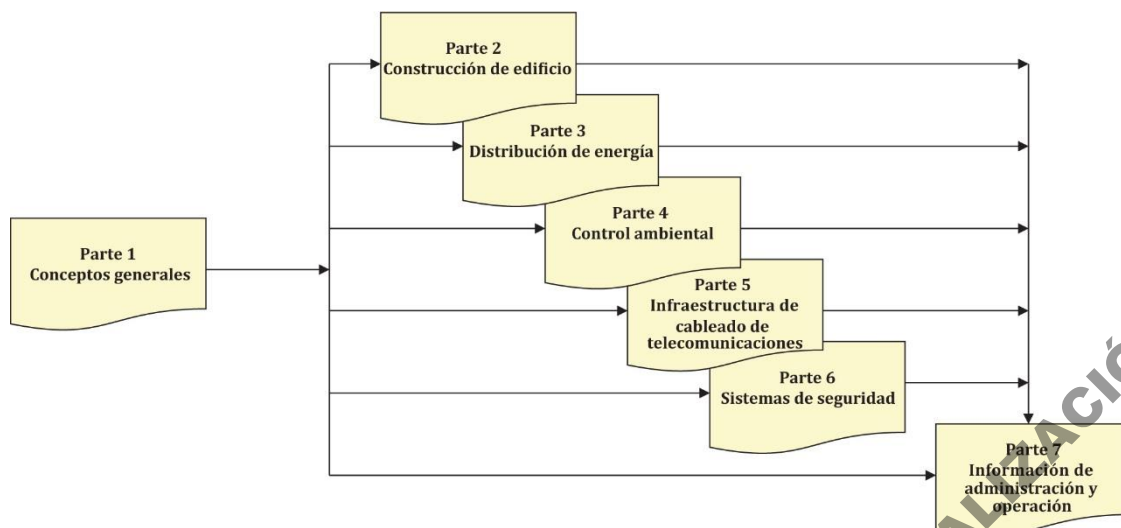
ISO/IEC TS 22237-4, Tecnología de la información – Instalaciones e infraestructuras de centros de datos – Parte 4: Control ambiental;

ISO/IEC TS 22237-5, Tecnología de la información – Instalaciones e infraestructuras de centros de datos – Parte 5: Infraestructura de cableado de telecomunicaciones;

ISO/IEC TS 22237-6, Tecnología de la información – Instalaciones e infraestructuras de centros de datos – Parte 6: Sistemas de seguridad;

ISO/IEC TS 22237-7, Tecnología de la información – Instalaciones e infraestructuras de centros de datos – Parte 7: Información de administración y operación;

La interrelación de las especificaciones dentro de la serie ISO/IEC TS 22237 se muestra en la Figura 1.



**Figura 1 - Relación esquemática entre la serie de documentos ISO/IEC TS 22237**

Este documento define los conceptos generales para el diseño y operación de los centros de datos. Esto incluye un análisis de riesgo comercial y de costos operativos, así como un sistema de clasificación para centros de datos con respecto a "disponibilidad", "seguridad física" y "habilitación de eficiencia energética".

ISO/IEC TS 22237-2 a ISO/IEC TS 22237-7 especifica requisitos y recomendaciones para instalaciones e infraestructuras particulares para soportar la clasificación relevante de "disponibilidad", "seguridad física" y "habilitación de eficiencia energética" seleccionada de ISO/IEC TS 22237-1.

ISO/IEC TS 22237-7 aborda la información operacional y de gestión (de acuerdo con los requisitos de ISO/IEC TS 22237-1).

Este documento está destinado a ser utilizado en colaboración entre o por arquitectos, diseñadores y constructores de edificios, diseñadores de sistema y de instalación.

La serie ISO/IEC TS 22237 no aborda la selección de tecnología de la información y equipos de telecomunicaciones en red, software y asuntos asociados a la configuración.

---0000000---

## Tecnología de la información. Instalaciones e infraestructuras de centros de datos - Parte 1: Conceptos generales

### 1 Objeto y campo de aplicación

Este documento:

- a) detalla los problemas que son abordados en un análisis de riesgo comercial y de costos operativos que permite la aplicación de una clasificación adecuada del centro de datos;
- b) define los aspectos comunes de los centros de datos, incluida la terminología, los parámetros y los modelos de referencia (elementos funcionales y su adaptación) que abordan el tamaño y la complejidad de su finalidad prevista;
- c) describe los aspectos generales de las instalaciones y las infraestructuras necesarias para apoyar la operación efectiva de las telecomunicaciones dentro de los centros de datos;
- d) especifica un sistema de clasificación, basado en los criterios clave de "disponibilidad", "seguridad" y "eficiencia energética" durante la vida planificada del centro de datos, para la provisión de instalaciones e infraestructura efectivas;
- e) describe los principios generales de diseño para los centros de datos en los que se basan los requisitos de la serie ISO/IEC TS 22237, incluidos símbolos, etiquetas, codificación en dibujos, aseguramiento de la calidad y educación.

Los siguientes temas están fuera del alcance de la serie ISO/IEC TS 22237:

- 1) la selección de tecnología de la información y equipos de telecomunicaciones en red, software y problemas de configuración asociados;

- 2) los requisitos de seguridad y compatibilidad electromagnética (EMC) (cubiertos por otras normas y reglamentos). Sin embargo, la información dada en la serie ISO/IEC TS 22237 puede ser de ayuda para cumplir con estas normas y reglamentos).

## 2 Referencias normativas

Los siguientes documentos se mencionan en el texto de tal manera que algunos o todos sus contenidos constituyen requisitos de este documento. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha, se aplica la última edición del documento referenciado (incluidas las enmiendas).

ISO/IEC TS 22237-2 <sup>1)</sup>	Tecnología de la información - Instalaciones e infraestructuras de centros de datos - Parte 2: Construcción de edificios
ISO/IEC TS 22237-3 <sup>2)</sup>	Tecnología de la información - Instalaciones e infraestructuras de centros de datos - Parte 3: Distribución de energía
ISO/IEC TS 22237-4 <sup>3)</sup>	Tecnología de la información - Instalaciones e infraestructuras de centros de datos - Parte 4: Control ambiental
ISO/IEC TS 22237-5 <sup>4)</sup>	Tecnología de la información - Instalaciones e infraestructuras de centros de datos - Parte 5: Infraestructura de cableado de telecomunicaciones
ISO/IEC TS 22237-6 <sup>5)</sup>	Tecnología de la información - Instalaciones

<sup>1)</sup> La ETP-ISO/IEC TS 22237-2:2019 adopta la ISO/IEC TS 22237-2:2018

<sup>2)</sup> La ETP-ISO/IEC TS 22237-3:2019 adopta la ISO/IEC TS 22237-3:2018

<sup>3)</sup> La ETP-ISO/IEC TS 22237-4:2019 adopta la ISO/IEC TS 22237-4:2018

<sup>4)</sup> La ETP-ISO/IEC TS 22237-5:2019 adopta la ISO/IEC TS 22237-5:2018

<sup>5)</sup> La ETP-ISO/IEC TS 22237-6:2019 adopta la ISO/IEC TS 22237-6:2018

e infraestructuras de centros de datos - Parte  
6: Sistemas de seguridad

### 3 Términos, definiciones y términos abreviados

#### 3.1 Términos y definiciones

Para los propósitos de esta Especificación Técnica Peruana, se aplican los siguientes términos y definiciones.

ISO e IEC mantienen bases de datos terminológicas para su uso en la estandarización en las siguientes direcciones:

- IEC Electropedia: disponible en <http://www.electropedia.org/>
- ISO en línea: disponible en <https://www.iso.org/obp>

##### 3.1.1

##### **disponibilidad**

capacidad de un elemento para estar en un estado para realizar una función requerida bajo condiciones dadas en un instante de tiempo dado o en un intervalo de tiempo dado, suponiendo que se proporcionan los recursos externos requeridos

[FUENTE: IEC 60050-191:1990, 191-02-05]

##### 3.1.2

##### **instalaciones de entrada a la edificación**

instalación que proporciona todos los servicios mecánicos y eléctricos necesarios para la entrada de cables de telecomunicaciones en un edificio y que puede permitir la transición del cable externo al interno

##### 3.1.3

##### **construcción de seguridad**

instalaciones y sistemas necesarios para proporcionar los niveles de seguridad necesarios en

la entrada y dentro de la construcción que contiene el centro de datos

#### **3.1.4 gabinete**

construcción cerrada para albergar equipos de tecnología de la información y otros

[FUENTE: IEC 14763-2:2012,31.7, modificado-eliminado las palabras “previsto” y “componentes y”]

#### **3.1.5 centro de datos co-alojamiento (co-hosting)**

centro de datos en el que se proporciona a múltiples clientes acceso a la (s) red (es), servidores y equipos de almacenamiento en los que operan sus propios servicios / aplicaciones

NOTA 1 a la entrada: Tanto el equipo de tecnología de la información como la infraestructura de soporte del edificio se proporcionan como un servicio por parte del operador del centro de datos.

#### **3.1.6 centro de datos de co-ubicación**

centro de datos en el que varios clientes ubican su propia red (es), servidores y equipos de almacenamiento

NOTA 1 a la entrada: El operador del centro de datos proporciona la infraestructura de soporte del edificio (como distribución de energía y control ambiental) como un servicio.

#### **3.1.7 espacio de la sala de cómputo**

área dentro del centro de datos donde se colocan los equipos de procesamiento de datos, de almacenamiento de datos y de telecomunicaciones que proporciona la función principal del centro de datos

#### **3.1.8 espacio de la sala de control**

área dentro del centro de datos utilizados para controlar la operatividad del centro de datos y para actuar como un punto central para todas las funciones de control y seguimiento

### 3.1.9

#### **centro de datos**

estructura o grupo de estructuras, dedicadas al alojamiento centralizado, interconexión y operación de tecnología de la información y equipos de telecomunicaciones en red que proporcionan servicios de almacenamiento, procesamiento y transporte de datos junto con todas las instalaciones e infraestructuras para distribución de energía y control ambiental junto con los niveles necesarios de se requiere de resiliencia y seguridad para proporcionar la disponibilidad del servicio deseada

NOTA 1 a la entrada: Una estructura puede consistir en múltiples edificios y/o espacios con funciones específicas para respaldar la función primaria.

NOTA 2 a la entrada: Los límites de la estructura o espacio considerado como centro de datos, que incluye el equipo de tecnología de la información y la comunicación y los controles ambientales de apoyo, se pueden definir dentro de una estructura o edificio más grande.

[FUENTE: IEC 30134-1:2016, 3.1.4]

### 3.1.10

#### **seguridad de centro de datos**

instalaciones y sistemas necesarios que proporcionan los niveles de seguridad necesarios en la entrada y en el centro de datos

### 3.1.11

#### **punto de demarcación**

punto donde el control operativo o la propiedad cambia

### 3.1.12

#### **espacio de distribución eléctrica**

área utilizada para albergar las instalaciones para la distribución de la energía eléctrica entre el espacio del transformador y los espacios eléctricos dentro del centro de datos o en otro lugar dentro del establecimiento o edificios individuales dentro del establecimiento

### 3.1.13

#### **espacio eléctrico**

área dentro del centro de datos utilizado para albergar las instalaciones para brindar y controlar la energía eléctrica a los espacios del centro de datos [incluyendo cuadros de



distribución, baterías, sistemas de alimentación ininterrumpida (UPS), etc.]

### **3.1.14**

#### **centro de datos empresariales**

centro de datos que es operado por una empresa que tiene el único propósito de la entrega y administración de servicios a sus empleados y clientes

### **3.1.15**

#### **seguridad externa del establecimiento**

instalaciones y sistemas que proporcionan los niveles de seguridad requeridos para el área entre el edificio y el límite del establecimiento

### **3.1.16**

#### **habilitación de eficiencia energética**

capacidad de medir el consumo de energía y permitir el cálculo y el informe de la eficiencia energética de las diversas instalaciones e infraestructuras

### **3.1.17**

#### **instalaciones**

espacios y vías que albergan una infraestructura específica

### **3.1.18**

#### **capacidad funcional**

capacidad del centro de datos (o sistema o subsistema) para brindar su función prevista

### **3.1.19**

#### **espacio del generador**

área utilizada para albergar la instalación de equipos de generación de energía eléctrica junto con el almacenamiento asociado de combustibles o equipos de conversión de energía

### **3.1.20**

#### **espacio para custodia**

área dentro del centro de datos utilizada para la custodia del equipo antes de ponerse en servicio o de haber sido retirado de servicio

### 3.1.21

#### **infraestructura**

sistemas técnicos que proporcionan capacidad funcional del centro de datos

EJEMPLO: Distribución de energía, control ambiental y seguridad física.

### 3.1.22

#### **distribuidor principal**

distribuidor utilizado para realizar conexiones entre el subsistema de cableado de distribución principal, el subsistema de cableado de acceso a la red y los subsistemas de cableado y el equipo activo

[FUENTE: ISO/IEC 11801-5: 2017, 3.1.6, modificado; eliminado "como se especifica en ISO/IEC 11801-1".]

### 3.1.23

#### **espacio mecánico**

área que se utiliza para albergar equipos mecánicos e infraestructura que proporciona control ambiental para los espacios del centro de datos (incluidos enfriadores y sistemas de tratamiento de agua, manejo del aire y extinción de incendios)

### 3.1.24

#### **centro de datos del operador de red**

centro de datos que tiene el propósito principal de la entrega y gestión de servicios de banda ancha para los clientes operadores

### 3.1.25

#### **seguridad física**

medidas (combinando controles físicos y tecnológicos), procedimientos y responsabilidades para mantener el nivel de disponibilidad deseado para las instalaciones e infraestructuras de los centros de datos en relación con el control de acceso y los eventos ambientales

### 3.1.26

#### **periodo de inactividad planificado**

periodo de tiempo durante el cual un sistema o subsistema no proporciona capacidad funcional mientras se somete a mantenimiento o se desconecta para probar la respuesta de un sistema o subsistema relacionado

### **3.1.27**

#### **instalación de entrada del establecimiento**

espacio que proporciona todos los servicios mecánicos y eléctricos necesarios para la entrada de cables dentro del establecimiento

### **3.1.28**

#### **espacio de almacenamiento**

área protegida donde se pueden almacenar bienes generales y / o bienes del centro de datos

### **3.1.29**

#### **telecomunicaciones**

rama de tecnología relacionada con la transmisión, emisión y recepción de señales, señales, escritos, imágenes y sonidos, es decir, información de cualquier naturaleza por cable, radio, óptica u otros sistemas electromagnéticos

[FUENTE: ISO/IEC 11801-1: 2017, 3.1.78, modificado - Se eliminó la nota 1 de la entrada]

### **3.1.30**

#### **cableado de telecomunicaciones**

infraestructura de cableado de telecomunicaciones desde el (los) espacio (s) de telecomunicaciones a la instalación de entrada de las instalaciones

### **3.1.31**

#### **equipo de telecomunicación**

equipo dentro del centro de datos que brinda servicios de telecomunicaciones dentro del centro de datos

### **3.1.32**

#### **espacio de telecomunicaciones**

área que puede albergar puntos de demarcación y equipos de telecomunicaciones asociados con la instalación de entrada del edificio y que puede permitir a los proveedores de servicios acceso restringido al centro de datos

### 3.1.33

#### **espacio de prueba**

área dentro del centro de datos utilizado para la prueba y configuración del equipo antes de ponerse en servicio

### 3.1.34

#### **espacio del transformador**

área utilizada para el alojamiento del equipo necesario para convertir los circuitos eléctricos primarios a niveles apropiados para la conexión al equipo dentro de las instalaciones o edificios individuales dentro de las instalaciones

### 3.1.35

#### **sistema de alimentación ininterrumpida**

combinación de convertidores, interruptores y dispositivos de almacenamiento de energía (como baterías), que constituyen un sistema de energía para mantener la continuidad de la energía de carga en caso de falla de la alimentación de entrada.

NOTA 1 a la entrada: La continuidad de la potencia de carga ocurre cuando el voltaje y la frecuencia se encuentran dentro de las bandas de tolerancia de estado estacionario y transitorio, y con distorsión e interrupciones dentro de los límites especificados para la carga. La falla de la alimentación de entrada ocurre cuando el voltaje y la frecuencia están fuera de las bandas nominales de estado estable y tolerancia transitoria o con distorsión o interrupciones fuera de los límites especificados para el UPS.

[FUENTE: IEC 62040-1: 2008, 3.1.1]

### 3.1.36

#### **tiempo de inactividad no planificado**

el tiempo necesario, después de una falla de la capacidad funcional, para reparar la infraestructura relevante junto con el tiempo de "reinicio" necesario para recuperar la capacidad funcional después de esa reparación

## 3.2

### **Términos abreviados**

A los fines de este documento, se aplican los siguientes términos abreviados:

CRAC    Aire Acondicionado / Acondicionado de la Sala de    Cómputo

ffs	para un estudio posterior
MTBF	Tiempo Medio entre Fallos
MTTR	Tiempo medio para la Recuperación
NOC	Centro de Operaciones de Red
UPS	Fuente de Poder Ininterrumpible

## 4 Conformidad

Para que un diseño de centro de datos sea conforme a este documento:

- a) se debe completar un análisis de riesgo comercial de acuerdo con la Cláusula 5;
- b) se debe seleccionar una Clase de disponibilidad apropiada en 7.2 utilizando un análisis de riesgo comercial en la Cláusula 5;
- c) se debe seleccionar una Clase de protección apropiada en 7.3 usando un análisis de riesgo comercial en la Cláusula 5;
- d) se debe seleccionar un nivel apropiado de habilitación de la eficiencia energética en 7.4;
- e) se debe aplicarlos principios generales de diseño del Anexo A.

## 5 Análisis de riesgo del negocio

### 5.1 General

La disponibilidad general de un centro de datos es una medida de la continuidad de su procesamiento de datos, almacenamiento, y funciones de transporte. Se determina el nivel aceptable de disponibilidad general de un centro de datos por una serie de factores, incluyendo:

- a) un análisis de costos de tiempo de inactividad (ver 5.2) - el costo asociado con una falla en la provisión del servicio, que depende de una serie de factores, incluida la función y la importancia del centro de datos;
- b) presiones comerciales aplicadas externamente (por ejemplo, costos de seguro).

La disponibilidad de cada una de las instalaciones e infraestructuras del centro de datos necesarias para respaldar la disponibilidad general deseada se describe mediante una clasificación de disponibilidad (véase 7.2). El diseño de cada una de las infraestructuras del centro de datos debe tener en cuenta su impacto en la disponibilidad general y los costes asociados con el tiempo de inactividad previsto asociado a fallas o mantenimiento planificado. El diseño y la seguridad física de las instalaciones y las infraestructuras del centro de datos pueden someterse a un análisis de riesgos (véase 5.3) que mapea los eventos de riesgo identificados con los requisitos de la clasificación de disponibilidad (véase 7.2). Este análisis identifica los aspectos de las instalaciones y las infraestructuras que requieren inversión en términos de mejoras de diseño para reducir su impacto y / o probabilidad de dichos eventos de riesgo.

## 5.2 Análisis de costo de tiempo de inactividad

Este documento no define los métodos de análisis para el costo del tiempo de inactividad. Los estándares tales como IEC 31010 proporcionan una guía útil.

Los elementos a considerar dentro de dicho análisis dependerán del propósito del centro de datos.

Algunas organizaciones pueden asignar un valor monetario (o rango) a la pérdida de servicio que puede incluir lo siguiente:

- a) sanciones financieras inmediatas;
- b) pérdidas consecuentes;
- c) una evaluación del daño a largo plazo a la reputación empresarial, por ejemplo, un proveedor de servicios de Internet o una institución financiera.

Aunque a menudo se considera el costo al analizar el tiempo de inactividad, también se deben considerar otros impactos.

Los centros de datos que contienen información de seguridad de vida, legal, médica y penal pueden tener consecuencias reconocidas individualmente a partir del tiempo de inactividad no programado.

### 5.3 Análisis de riesgo

Este documento no define los métodos de análisis de riesgos. Los estándares tales como IEC 31010 proporcionan una guía útil.

El análisis de riesgo se puede usar como una herramienta de gestión que permite la comparación con el riesgo total aceptable y muestra las tendencias resultantes de la actividad de mitigación. A los efectos de esta norma, el riesgo asociado con un evento relacionado con las instalaciones e infraestructuras del centro de datos que interrumpe la prestación del servicio del centro de datos se define como un riesgo de evento que es una función del impacto y probabilidad donde:

- a) impacto es la magnitud o severidad de los incidentes o impactos adversos, la duración expresada nominal o nominalmente esperada de la pérdida del servicio (disponibilidad) del evento;
- b) la probabilidad es la posibilidad del evento.

El impacto del riesgo puede evaluarse usando diferentes unidades de medida, por ejemplo costo, seguridad, etc.

El riesgo total para la capacidad funcional del centro de datos es una función de los riesgos de eventos asociados con cada instalación e infraestructura siempre que esos riesgos se cuantifiquen sobre la misma base. Si se relaciona con el resultado del análisis del costo del tiempo de inactividad (ver 5.2), se puede estimar el valor financiero del riesgo total.

Los riesgos considerados deberían incluir amenazas externas que pueden afectar las instalaciones y las infraestructuras, incluida, en particular, la ubicación, que puede ser geográfica (tráfico aéreo, inundaciones, etc.), política (guerras, focos de conflicto, terror, etc.) o afectar las relaciones de vecindad (si, por ejemplo, existen riesgos de incendio debido a estaciones de llenado, almacenamiento de productos químicos, etc.) y, por lo tanto, influyen en la probabilidad de un posible tiempo de inactividad.

Además, los riesgos potenciales derivados de los ataques del propio personal de la empresa y del exterior deberían formar parte de la evaluación general de riesgos.

El impacto se puede categorizar como:

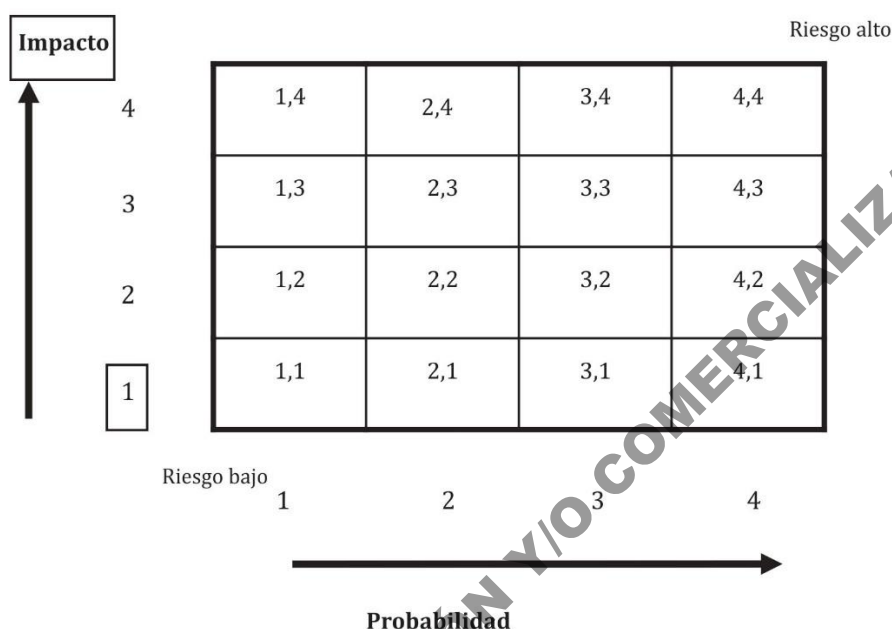
- 1) bajo: pérdida de servicios no críticos;
- 2) medio: falla de los componentes críticos del sistema pero sin pérdida de redundancia;
- 3) alto: pérdida de redundancia crítica del sistema pero sin pérdida de servicio para los clientes;
- 4) crítico: Pérdida del servicio crítico para uno o más clientes o pérdida de la vida (que puede ampliarse para tratar lesiones personales).

La probabilidad de que ocurra un evento se puede definir de manera similar, es decir:

- muy bajo;
- bajo;
- medio;
- alto.

Cada riesgo se puede cuantificar en un mapa de riesgos como se muestra en la Figura 2. Los eventos de alto riesgo habitan en la esquina superior derecha de la figura y los eventos de bajo riesgo habitan en la esquina inferior izquierda.





**Figura 2 – Ejemplo de mapa de riesgo**

Habiendo identificado el riesgo de los posibles eventos asociados con las instalaciones e infraestructuras del centro de datos, se determinará el costo de inactividad con ese evento para permitir que se tomen decisiones de diseño que reduzcan el riesgo (mediante la reducción del impacto o la probabilidad del evento).

## 6 Visión general del diseño de centro de datos

### 6.1 General

Un centro de datos comprende uno o más edificios o uno o más espacios dentro de esos edificios, cuya función principal es acomodar el equipo que procesa, entrega y / o almacena información. Del mismo modo, los centros de datos tienen una variedad de propósitos, incluidos los servicios de co-alojamiento (co-hosting), co-ubicación, empresa y operador de red.

Los centros de datos pueden diferir significativamente con respecto a su tamaño físico. En el extremo inferior del rango de tamaño, pueden albergar una pequeña cantidad de equipos de almacenamiento y servidores para proporcionar servicios de tecnología de la información a la infraestructura de cableado de un edificio. En el extremo superior del rango de tamaño, pueden albergar una gran cantidad de dicho equipo que requiere sofisticadas instalaciones de distribución de energía y control ambiental ubicadas en uno o más edificios dedicados a garantizar el funcionamiento del centro de datos.

Esta cláusula proporciona una visión general del diseño general para los centros de datos, independientemente de su tamaño.

NOTA: El diseño del cableado genérico está cubierto por ISO/IEC TS 22237-5, mientras que la instalación de dicho cableado se especifica en ISO/IEC 14763-2.

## 6.2 Espacios e instalaciones

La Figura 3 muestra una representación esquemática de los espacios requeridos por un gran centro de datos dentro de un edificio y dentro de las instalaciones que contienen uno o más edificios.

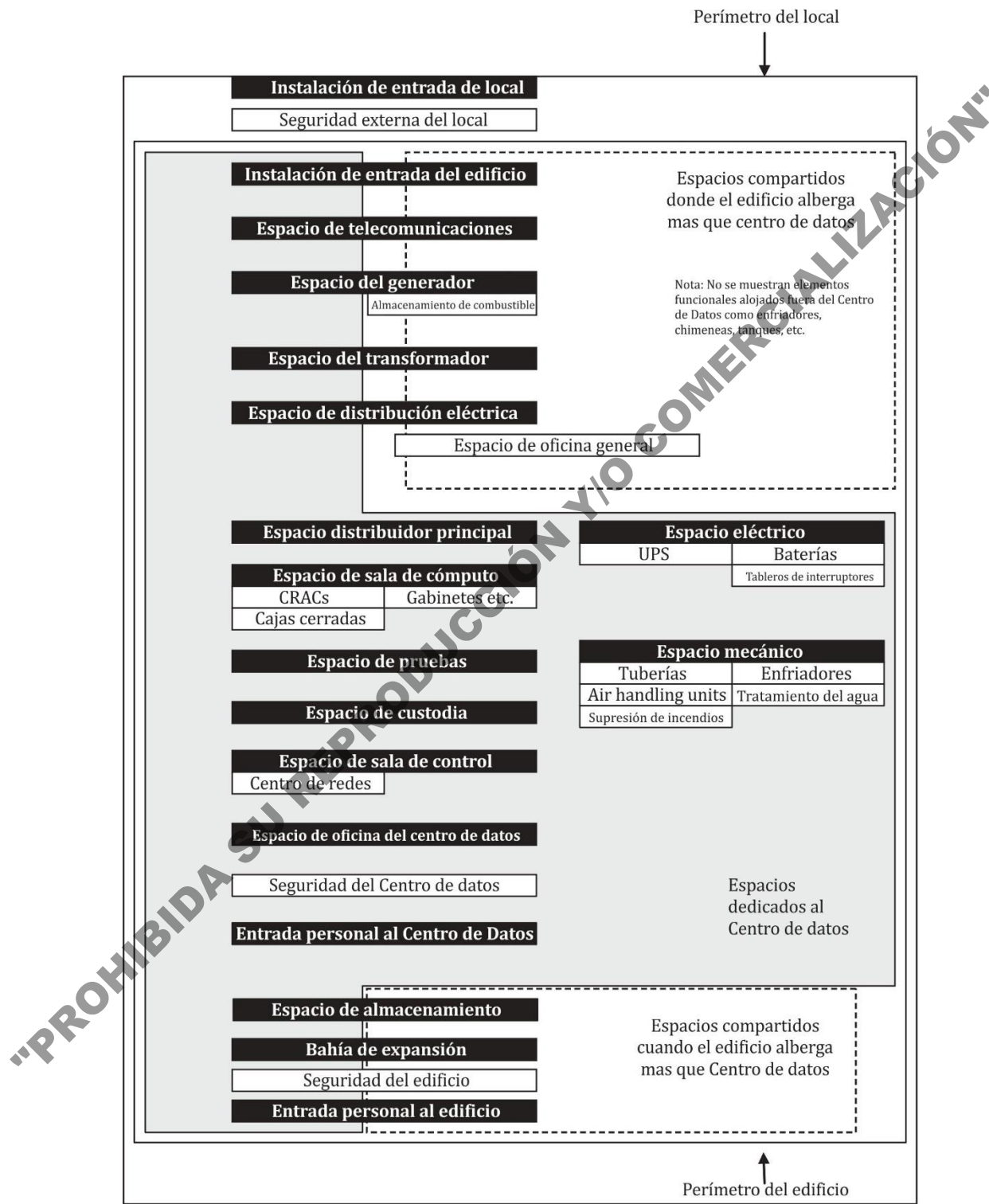
El centro de datos puede compartir ciertos espacios con el resto del edificio, incluidos:

- a) instalaciones de entrada a la edificación;
- b) entrada (s) de personal;
- c) zona de carga y descarga;
- d) espacio (s) de generadores, incluido el almacenamiento de combustible;
- e) espacio (s) de transformador;
- f) espacio (s) de distribución eléctrica;
- g) espacios de telecomunicaciones.

La necesidad de los espacios e instalaciones anteriores dentro del edificio depende del propósito tanto del edificio como del centro de datos. Cualquier intercambio de estos espacios e instalaciones dependerá del tamaño, pero también de las clases de disponibilidad y protección definidas del centro de datos y las funciones del resto del edificio. Por ejemplo, en los edificios que albergan grandes centros de datos, las instalaciones y los espacios que soportan el centro de datos pueden dedicarse al centro de datos con espacios separados para el resto del edificio.

El área dentro del edificio designado como un centro de datos puede contener los siguientes espacios:

- 1) entrada (s) de personal;
- 2) espacio (s) principal (es) del distribuidor;
- 3) espacio (s) de sala de cómputo y espacio (s) de prueba asociados;
- 4) espacio (s) eléctrico (s);
- 5) espacio (s) mecánico (s);
- 6) espacio (s) de la sala de control;
- 7) espacio (s) de oficina;
- 8) espacio (s) de almacenamiento y almacenamiento.



**Figura 3 - Diagrama esquemático típico de las instalaciones que contienen un centro de datos**

Dentro del área del edificio designado como centro de datos, la necesidad y el contenido de los espacios depende del propósito del centro de datos, su consumo anticipado de energía y la necesidad de control ambiental.

La necesidad de segregación de espacios depende de consideraciones de seguridad, requisitos de seguridad y sobre la necesidad de control ambiental.

Como ejemplos, un centro de datos de una pequeña empresa puede comprender una habitación individual que tiene la función de un espacio de sala de informática y un espacio eléctrico sin segregación física, mientras que un centro de datos grande puede requerir uno o más espacios segregados de cada tipo identificado en la Figura 3.

## **7 Sistema de clasificación para centro de datos**

### **7.1 General**

Para efectos de la serie ISO/IEC TS 22237, los centros de datos se clasifican con respecto a:

- a) Clases de disponibilidad (ver 7.2);
- b) Clases de protección (ver 7.3);
- c) Niveles de habilitación eficientes de energía (ver 7.4).

Las combinaciones de las tres clasificaciones se utilizan para determinar los requisitos y recomendaciones relevantes para las siguientes instalaciones e infraestructuras de acuerdo con el análisis de riesgo en la Cláusula 5:

- 1) construcción de edificios (ver ISO/IEC TS 22237-2);
- 2) distribución de potencia (ver ISO/IEC TS 22237-3);
- 3) control ambiental (ver ISO/IEC TS 22237-4);

- 4) infraestructura de cableado de telecomunicaciones (ver ISO/IEC TS 22237-5);
- 5) sistemas de seguridad (ver ISO/IEC TS 22237-6).

## 7.2 Disponibilidad

La disponibilidad requerida de las instalaciones y las infraestructuras que respaldan la funcionalidad del centro de datos es de suma importancia. El propietario / usuario del centro de datos debe determinar la disponibilidad deseada del conjunto general de instalaciones e infraestructuras utilizando el análisis de riesgos del negocio y el análisis de costos de tiempo de inactividad (Cláusula 5). Se reconoce que los requisitos de disponibilidad pueden variar con la hora del día, la semana o el mes.

Las diferentes Clases de Disponibilidad cualitativa para el conjunto global de instalaciones e infraestructuras del centro de datos se definen como se muestra en la Tabla 1. La disponibilidad de todo el centro de datos depende de las Clases de disponibilidad de sus infraestructuras individuales, como la fuente y distribución de energía, control ambiental y seguridad. Los requisitos para una instalación o infraestructura específica de una clase de disponibilidad dada son especificados en ISO/IEC TS 22237-3, ISO/IEC TS 22237-4 e ISO/IEC TS 22237-6, respectivamente.

Con el propósito que el conjunto de instalaciones e infraestructuras del centro de datos se considere como una Clase de Disponibilidad determinada, el diseño de cada instalación e infraestructura individual enumeradas en la Tabla 1 debe cumplir o superar esa clase de disponibilidad.

NOTA: Cuando el diseño de la instalación y la infraestructura de control ambiental sea de clase mejorada 4 como se describe en la norma ISO/IEC TS 22237-4, el conjunto de instalaciones e infraestructuras del centro de datos se considerará de la clase mejorada 4 siempre que todas las demás instalaciones e infraestructuras de la Tabla 1 son de Clase 4.

La provisión de Clases de mayor Disponibilidad generalmente requiere una mayor inversión, por ejemplo en diseño, construcción, componentes, sistemas y recursos humanos. Por ejemplo, una mayor inversión en componentes puede resultar en un mayor Tiempo Medio entre Fallas (MTBF) o un Tiempo Medio Reducido para la Recuperación (MTTR). El MTBF de una infraestructura particular proporciona información en relación con la probabilidad del evento como se analiza en el 5.3. El MTTR de una infraestructura particular proporciona

una indicación del impacto del evento como se discutió en el 5.3.

**Tabla 1 - Clases de disponibilidad e implementaciones de ejemplo**

	<b>Disponibilidad Clase 1</b>	<b>Disponibilidad Clase 2</b>	<b>Disponibilidad Clase 3</b>	<b>Disponibilidad Clase 4</b>
Disponibilidad de conjunto general de instalaciones e infraestructuras	Bajo	Medio	Alto	Muy alto
Ejemplo de distribución de potencia (ver ISO/IEC TS 22237-3)	Ruta única (sin redundancia de componentes)	Ruta única (elasticidad proporcionada por la redundancia de los componentes)	Multi-ruta (resiliencia proporcionada por la redundancia de los sistemas)	Multi-ruta (tolerante a fallas incluso durante el mantenimiento)
Ejemplo de control ambiental (ver ISO/IEC TS 22237-4)	Sin requisitos específicos	Ruta única (sin redundancia de componentes)	Ruta única (elasticidad proporcionada por la redundancia de los componentes)	Multi-ruta (resiliencia proporcionada por la redundancia de los sistemas), permite el mantenimiento durante la operación
Ejemplo de cableado de telecomunicaciones (ver ISO/IEC TS 22237-5)	Ruta única usando conexiones directas	Ruta única con infraestructura fija	Multi-ruta usando infraestructura fija	Multi-ruta utilizando infraestructura fija con diversas vías

NOTA 1: Los requisitos y recomendaciones para la construcción de centros de datos que proporcionan las clases de protección deseadas para garantizar la disponibilidad de las instalaciones y las infraestructuras se tratan en ISO/IEC TS 22237-2.

NOTA 2: La clase 4 mejorada que proporciona una solución de múltiples rutas (tolerante a fallas incluso durante el mantenimiento) se especifica en ISO/IEC TS 22237-4.

NOTA 3: Los requisitos y las recomendaciones para la seguridad física de los espacios de los centros de datos para garantizar la disponibilidad de las instalaciones y las infraestructuras se tratan en ISO/IEC TS 22237-6.

De ser posible, la determinación de la disponibilidad para subsistemas y componentes debe

incluir posibles expansiones futuras en el centro de datos para fines de resiliencia.

Se debe prestar más atención a la seguridad física de las instalaciones y las infraestructuras descritas en 7.3, que describen otros factores importantes para la disponibilidad general de todo el centro de datos.

Además del diseño y la instalación de soluciones técnicas más sofisticadas, la implementación de clases de mayor disponibilidad implica la aplicación de estructuras organizacionales efectivas para administrar el funcionamiento de esas soluciones técnicas que incluyen, entre otras:

- a) la disponibilidad de personal de servicio capacitado;
- b) almacenamiento de repuestos;
- c) el establecimiento de contratos de mantenimiento;
- d) acceso rápido a instrucciones precisas que definen las acciones y comunicaciones requeridas en caso de una falla del sistema.

## **7.3 Seguridad física**

### **7.3.1 General**

La seguridad física provista para las instalaciones e infraestructuras de un centro de datos tiene una influencia tanto en la probabilidad como en el impacto de los eventos de riesgo (ver 5.3) ya que el objetivo de la seguridad física es proteger contra:

- a) acceso no autorizado (ver 7.3.2);
- b) eventos ambientales internos (ver 7.3.3);
- c) eventos ambientales externos (ver 7.3.3).



### 7.3.2 Protección contra el acceso no autorizado

Las áreas del centro de datos y sus alrededores se definirán en términos de clases de protección contra el acceso no autorizado como se muestra en la Tabla 2. Dependiendo de la definición del objetivo de protección, el propietario / usuario del centro de datos seleccionará la clase de protección adecuada.

**Tabla 2 - Clases de protección**

<b>Tipo de protección</b>	<b>Clase de protección 1</b>	<b>Clase de protección 2</b>	<b>Clase de protección 3</b>	<b>Clase de protección 4</b>
Protección contra el acceso no autorizado	Área pública o semipública	Área accesible para todo el personal autorizado (empleados y visitantes)	Área restringida para empleados y visitantes especificados (otro personal con acceso a la Clase de Protección 2 debe estar acompañado por personal autorizado para acceder a las áreas de Protección de Clase 3)	Área restringida para empleados específicos que tienen una necesidad identificada de tener acceso (otro personal con acceso a áreas de Clase 2 o Clase 3 debe estar acompañado por personal autorizado para acceder a áreas de Clase 4)

Dentro del centro de datos, las restricciones de acceso dependen del propósito del centro de datos (por ejemplo, empresa versus ubicación conjunta). Los criterios de diseño se basan en un análisis de las necesidades que definen los requisitos y recomendaciones apropiados.

ISO/IEC TS 22237-2 especifica los requisitos y proporciona recomendaciones para la ubicación y construcción de los centros de datos en apoyo de la zonificación de la clase de protección deseada.

ISO/IEC TS 22237-3 especifica los requisitos y proporciona recomendaciones para los sistemas de distribución de energía en apoyo de la clase de protección deseada.

ISO/IEC TS 22237-4 especifica los requisitos y proporciona recomendaciones para los sistemas de control ambiental en apoyo de la clase de protección deseada.

ISO/IEC TS 22237-6 especifica los requisitos y proporciona recomendaciones para los sistemas de seguridad y protección en apoyo de la clase de protección deseada.

### 7.3.3 Protección contra eventos ambientales

Las áreas del centro de datos y sus alrededores se definirán en términos de clases de protección contra eventos ambientales como se muestra en la Tabla 3. Dependiendo de la definición del objetivo de protección, el propietario / usuario del centro de datos seleccionará la clase de protección adecuada para cada tipo de protección se muestra en la Tabla 3.

**Tabla 3 – Protección contra medios ambientales**

<b>Tipo de protección</b>	<b>Clase de protección 1</b>	<b>Clase de protección 2</b>	<b>Clase de protección 3</b>	<b>Clase de protección 4</b>
Protección contra fuego interno	No se aplica protección especial	El área requiere protección contra incendios mediante un sistema de detección y supresión, que mantiene la función de esa área durante un incendio en esa zona o en una zona de Clase 1.	El área requiere estar protegida contra incendios mediante un sistema de detección y supresión, que mantiene la función de esa área durante un incendio en esa área o una en un área de Clase 1 o Clase 2.	El área debe estar protegida contra incendios mediante un sistema de detección y supresión, que permite asegurar la función crítica del centro de datos durante un incendio en esa área o en otro lugar en el centro de datos.

Protección contra otros eventos internos	No se aplica protección especial	Mitigación aplicada	Mitigación aplicada	Mitigación aplicada
Protección contra eventos ambientales externos	No se aplica protección especial	Mitigación aplicada	Mitigación aplicada	Mitigación aplicada

La protección contra eventos ambientales internos y externos incluye todas las medidas necesarias para garantizar la clase de disponibilidad deseada para las instalaciones y las infraestructuras del centro de datos, incluida la construcción de edificios, los sistemas de protección y las medidas organizativas.

Los eventos ambientales internos incluyen sobrecalentamiento, incendios, descargas electrostáticas, agua, etc. que afectan la función de las infraestructuras del centro de datos.

Los eventos ambientales externos incluyen incendios, inundaciones, terremotos, explosiones y otras formas de desastres naturales (rayos y otros efectos electromagnéticos).

Bajo condiciones óptimas, los riesgos planteados por eventos ambientales externos se mitigan mediante la selección de la ubicación del centro de datos (ver ISO/IEC TS 22237-2). Sin embargo, en la mayoría de las situaciones, se deben aplicar soluciones de diseño alternativas a las instalaciones e infraestructuras del centro de datos para proporcionarles un grado aceptable de seguridad frente a dichos eventos.

ISO/IEC TS 22237-2 especifica los requisitos y proporciona recomendaciones para la ubicación y construcción de centros de datos para respaldar la clase de protección deseada contra eventos ambientales.

ISO/IEC TS 22237-3 especifica los requisitos y proporciona recomendaciones para los sistemas de distribución de energía en apoyo de la clase de protección deseada contra eventos ambientales.

ISO/IEC TS 22237-4 especifica los requisitos y proporciona recomendaciones para los sistemas de control ambiental en apoyo de la clase de protección deseada contra eventos

ambientales.

ISO/IEC TS 22237-6 especifica los requisitos y proporciona recomendaciones para los sistemas de seguridad y protección en apoyo de la clase de protección deseada.

## **7.4 Habilitación de eficiencia energética**

### **7.4.1 General**

La capacidad de medir el consumo de energía y permitir el cálculo y el informe de la eficiencia energética de las diversas instalaciones e infraestructuras que respaldan el funcionamiento de un centro de datos es fundamental para el logro de los objetivos de eficiencia energética.

Se definen tres niveles de granularidad:

- a) Nivel 1: un régimen de medición que proporciona información global simple para el centro de datos en su conjunto;
- b) Nivel 2: un régimen de medición proporciona información detallada para instalaciones e infraestructuras específicas dentro del centro de datos;
- c) Nivel 3: un régimen de medición proporciona datos granulares para los elementos dentro de los espacios del centro de datos.

Pasar de un nivel de complejidad a un nivel superior requiere un mayor nivel de infraestructura de medición / seguimiento.

El propietario / usuario del centro de datos definirá el nivel de habilitación de la eficiencia energética adecuado antes del diseño del centro de datos.

El nivel de habilitación de eficiencia energética deseado puede determinarse por:

- 1) un análisis de costos operativos;

- 2) requisitos normativos o legislativos externos;
- 3) reglas definidas por el usuario.

#### **7.4.2 Sistema de distribución de energía**

ISO/IEC TS 22237-3 describe los elementos de los sistemas de distribución de energía para centros de datos y define los requisitos y recomendaciones para las infraestructuras de medición / seguimiento de los sistemas de distribución de energía en apoyo del nivel de complejidad deseado.

#### **7.4.3 Seguimiento y control ambiental**

ISO/IEC TS 22237-4 describe los elementos de los sistemas de control ambiental para centros de datos y define los requisitos y recomendaciones para las infraestructuras de medición / seguimiento de los sistemas de control ambiental en apoyo del nivel de complejidad deseado.

## ANEXO A (INFORMATIVO)

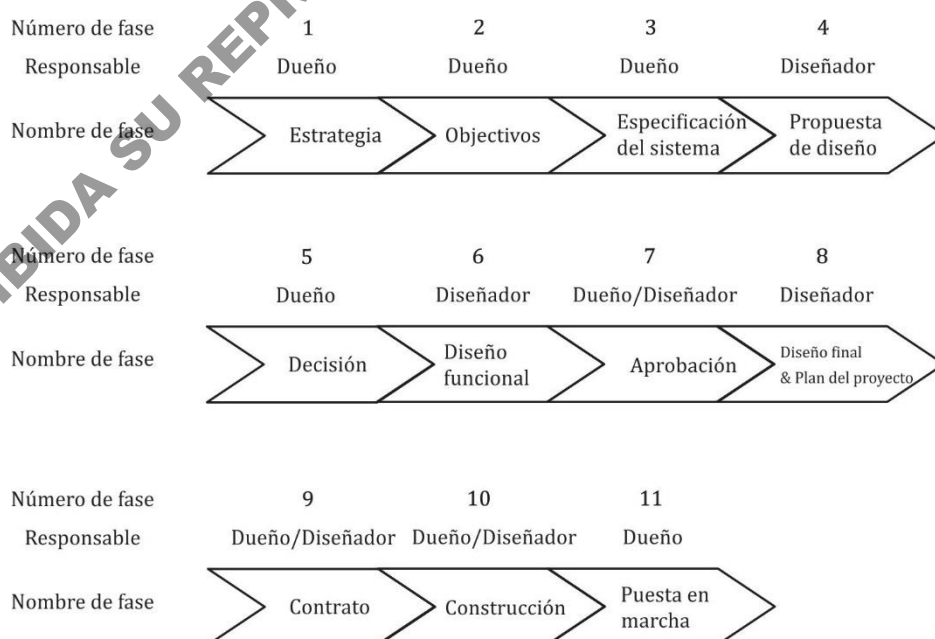
### Principios generales de diseño

#### A.1 Proceso de diseño

##### A.1.1 Introducción

El diseño eficaz del centro de datos requiere la división del proyecto en fases. Cada fase tiene su propia entrada y salida. Todas estas fases siguen una línea de tiempo secuencial, lo que resulta en el plan final del proyecto, lo que lleva a la emisión de un contrato para la instalación del centro de datos que permite que comience la fase operativa. Las fases se pueden ejecutar varias veces si es necesario para lograr los objetivos acordados o definidos.

La Figura A.1 enumera todas las fases en su orden secuencial, incluidas las descripciones de las fases y las responsabilidades.



**Figura A.1 – Fases de diseño**

© ISO/IEC 2018 - © INACAL 2019 - Todos los derechos son reservados

### **A.1.2 Fase 1 – Estrategia**

Esta fase es para la recopilación de información con el fin de definir los objetivos del proyecto. La siguiente información es requerida:

- a) estrategia de continuidad del negocio;
- b) estrategia de TI;
- c) estrategia de centro de datos corporativo;
- d) requisitos / expectativas generales del cliente;
- e) análisis de carga / demanda / costos actuales;
- f) ruta de la tecnología de infraestructura esperada;
- g) "pronóstico" de instalaciones futuras y demanda de infraestructura (espacio, potencia y ubicaciones);
- h) selección de ubicación

### **A.1.3 Fase 2 – Objetivos**

Esta fase es utilizada por el propietario para convertir la estrategia en objetivos. Los resultados son los siguientes:

- a) correlación con la estrategia del centro de datos corporativo;
- b) puntos de referencia de diseño (tamaño / niveles de rendimiento);
- c) análisis de riesgo;
- d) definición de flujo de trabajo;
- e) plano de planta general y catálogo de materiales.

#### **A.1.4 Fase 3 – Especificaciones del sistema**

Esta fase define las especificaciones objetivo para todas las infraestructuras con el siguiente resultado:

- a) especificación de objetivos para la distribución de energía;
- b) especificación de objetivos para el control ambiental;
- c) especificación de objetivo para la seguridad física;
- d) especificación de objetivos para detección de incendios y extinción de incendios;
- e) especificación de objetivos para planificación de telecomunicaciones;
- f) especificación de objetivos para la operación y gestión del centro de datos;
- g) especificación de objetivos para la fase de construcción.

#### **A.1.5 Fase 4 – Propuesta de diseño**

El diseñador utiliza las especificaciones y los objetivos para crear una propuesta de diseño para todas las infraestructuras que ofrecen varias opciones para el propietario. La propuesta de diseño contiene:

- a) propuesta de diseño para la distribución de energía;
- b) propuesta de diseño para control ambiental;
- c) propuesta de diseño para la seguridad física;
- d) propuesta de diseño para detección de incendios y lucha contra incendios;
- e) especificación de objetivos para planificación de telecomunicaciones;
- f) propuesta de diseño para la operación y administración del centro de datos;
- g) propuesta de diseño para la fase de construcción;



- h) modelos de costo para las opciones propuestas.

#### **A.1.6 Fase 5 – Decisión**

El propietario selecciona el diseño entre las opciones de diseño disponibles y los modelos de costos (compatibles con el diseñador).

#### **A.1.7 Fase 6 – Diseño funcional**

El diseñador convierte la selección del propietario en diseño funcional. El diseño funcional contiene:

- a) diseño funcional para distribución de energía;
- b) diseño funcional para control ambiental;
- c) diseño funcional para la seguridad física;
- d) diseño funcional para detección de incendios y lucha contra incendios;
- e) especificación de objetivos para planificación de telecomunicaciones;
- f) diseño funcional para la operación y administración del centro de datos;
- g) diseño funcional para la fase de construcción;
- h) modelo de costo "ajuste fino" para la opción seleccionada.

#### **A.1.8 Fase 7 – Aprobación**

El propietario aprueba el diseño funcional y los modelos de costos (respaldados por el diseñador).

#### **A.1.9 Fase 8 – Diseño final y plan del proyecto**

El diseñador define el volumen y / o las piezas para todas las infraestructuras diseñadas según A.1.7. Además, se define el flujo de trabajo del proyecto y todos los hitos y cronogramas del proyecto, lo que da como resultado un plan de implementación general.

#### **A.1.10 Fase 9 – Contrato**

El propietario (con el apoyo del diseñador) selecciona al contratista (s).

#### **A.1.11 Fase 10 – Construcción**

El propietario y el diseñador supervisan la construcción durante todo el tiempo de construcción. La verificación de aceptación para todas las infraestructuras y para todo el centro de datos se ejecuta hasta que el centro de datos se pone en servicio.

#### **A.1.12 Fase 11 – Operación**

Entregar al propietario para la operación.

### **A.2 Principios de diseño para disponibilidad**

#### **A.2.1 General**

Los principios del A.2.2 a A.2.10 (presentados en orden alfabético) son clave para lograr la clase de disponibilidad deseada definida en 7.2.

#### **A.2.2 Automatización**

Automatización significa un mecanismo automático basado en reglas para permitir que los sistemas se recuperen por sí mismos.

### **A.2.3 Autonomía**

Los subsistemas autónomos llevan a cabo tareas de forma independiente y transparente y son esenciales para la realización de sistemas tolerantes a fallas.

### **A.2.4 Tolerancia a fallas**

Los sistemas con tolerancia a fallas aseguran la provisión del servicio en el caso de perturbaciones y permiten la continuación de los procesos en caso de fallas de los subsistemas.

### **A.2.5 Mantenibilidad**

La capacidad de mantenimiento por diseño brinda acceso a los sistemas para fines de mantenimiento y permite un mantenimiento / reparación / intercambio rentable de las infraestructuras.

### **A.2.6 Priorización**

La priorización significa un tratamiento preferencial de los procesos críticos de la empresa o sus recursos de apoyo y representa un principio importante para la planificación y el diseño orientados a los requisitos.

### **A.2.7 Redundancia**

La redundancia describe la duplicación de la instalación y / o infraestructura iguales o comparables.

Hay dos tipos diferentes de redundancia, una relacionada con el nivel del sistema y otra relacionada con el nivel del dispositivo. El objetivo es alcanzar la clase de disponibilidad definida.

#### **A.2.8 Robustez**

Robustez describe la inmunidad contra impactos externos para prevenir fallas. La solidez generalmente aumenta al usar materiales de mayor calidad y / o diseño robusto de las arquitecturas de hardware y software.

#### **A.2.9 Escalabilidad**

La escalabilidad de los requisitos futuros como parte del diseño inicial garantiza la capacidad de reaccionar ante los cambios en el tamaño, la aplicación y el propósito de las instalaciones e infraestructuras del centro de datos, así como su implementación eficiente.

#### **A.2.10 Simplicidad**

La simplicidad de las instalaciones y las infraestructuras garantiza una tasa de error reducida. Además, proporciona un mantenimiento simplificado, más económico y más rápido a un costo reducido.

### **A.3 Diseño del concepto de EMC**

La compatibilidad electromagnética (EMC) es la capacidad de un sistema o dispositivo para operar normalmente en su entorno sin alterar la función de otros sistemas y / o dispositivos dentro del mismo entorno. En un centro de datos existen posibles fuentes de perturbación electromagnéticas internas y externas que podrían interrumpir el funcionamiento de los sistemas y / o dispositivos dentro del centro de datos, o incluso dañarlos. La implementación práctica de un concepto efectivo de EMC, basado en una ubicación y un análisis específico del objeto, minimizará el riesgo de mal funcionamiento del equipo y / o del sistema debido a tales perturbaciones en apoyo de la Clase de disponibilidad deseada de 7.2.

Hay una serie de normas internacionales que especifican las medidas que deben tomarse para minimizar la interferencia electromagnética. Éstas incluyen:

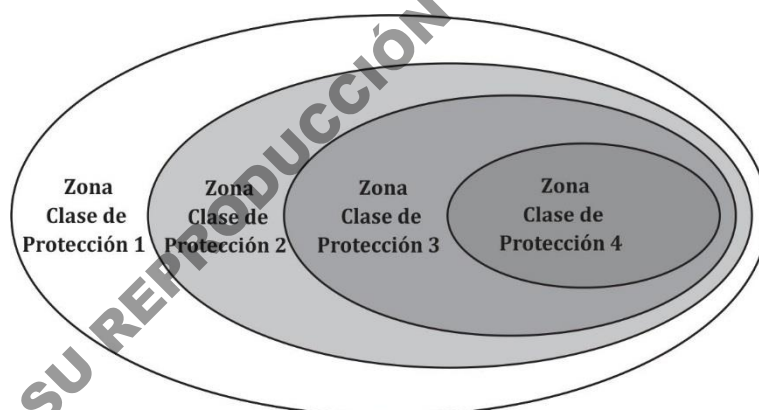
- a) protección contra rayos como se define en la serie IEC 62305;

- b) conexión equipotencial mallada tridimensional y puesta a tierra como se define en ISO/IEC 30129;
- c) planificación e instalación de cableado de tecnología de la información, tal como se define en ISO/IEC 14763 - 2.

Además, un análisis de EMC específico de ubicación y objeto puede requerir acciones adicionales para garantizar la función y disponibilidad del centro de datos.

#### A.4 Principios de diseño para la seguridad física

La implementación de la seguridad física en los centros de datos y sus funciones complementarias de infraestructura técnica se basa en un modelo de zonificación que se muestra en la Figura A.2 como se especifica en ISO/IEC TS 22237 - 6.



**Figura A.2 – Diagrama esquemático de las zonas de seguridad del centro de datos**

#### A.5 Principios de diseño para la eficiencia energética

La eficiencia energética dentro de un centro de datos está impulsada por:

- a) una necesidad de reducir el costo de las operaciones (es decir, menor consumo de energía);
- b) apoyo de iniciativas locales y regionales.

El papel del diseñador del centro de datos es seleccionar las soluciones adecuadas para cumplir los objetivos de eficiencia energética definidos para las instalaciones y las infraestructuras. Los niveles de habilitación de eficiencia energética se definen en 7.4 para permitir la evaluación de la eficiencia energética.

Las prácticas recomendadas sobre el diseño del centro de datos de eficiencia energética y más información sobre la eficiencia energética en los centros de datos se pueden encontrar en ISO/IEC TR 30133.

"PROHIBIDA SU REPRODUCCIÓN Y/O COMERCIALIZACIÓN"

## BIBLIOGRAFÍA

- [1] ISO/IEC TS 22237-7, *Information technology — Data center facilities and infrastructures — Part 7: Management and operational information*
- [2] ISO/IEC 11801-1:2017, *Information technology — Generic cabling for customer premises — Part 1: General requirements*
- [3] ISO/IEC 11801-5:2017, *Information technology — Generic cabling for customer premises — Part 5: Data centres*
- [4] ISO/IEC 14763-2, *Information technology — Implementation and operation of customer premises cabling — Part 2: Planning and installation*
- [5] ISO/IEC 30129, *Information technology — Telecommunications bonding networks for buildings and other structures*
- [6] ISO/IEC TR 301331<sup>6</sup>, *Information technology — Data centres — Guidelines for resource efficient data centres*
- [7] IEC 31010, *Risk management — Risk assessment techniques*
- [8] IEC 62305 (all parts), *Protection against lightning*

---

<sup>6</sup> En desarrollo. Etapa en el momento de la publicación: ISO/IEC PDTR 30133.