

# SEGURIDAD DE CABLEADO Y DATACENTER



## Unidad 1

## Seguridad de Redes del Datacenter



## **ESCUELA DE CONSTRUCCIÓN E INGENIERÍA**

**Director:** Marcelo Lucero Yáñez

### **ELABORACIÓN**

**Experto disciplinar:** Eder Morán Heredia

**Diseñadora instruccional:** Luisa García Ospina

**Editora instruccional:** Emilia De la Cruz Barrés

### **VALIDACIÓN**

**Experto disciplinar:** Gabriel Urra Varas

**Jefa de Diseño Instruccional:** Alejandra San Juan Reyes

### **EQUIPO DE DESARROLLO**

Welearn

**AÑO**

2022



# Tabla de contenidos

Aprendizaje esperado .....	4
Introducción.....	5
1. Barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial .....	6
1.1. La importancia de los auditores.....	6
1.2. Estrategia de segmentación .....	8
1.3. Seguridad física de un centro de datos.....	9
1.3.1. Capa 1: Defensa perimetral.....	9
1.3.2. Capa 2: Zona Limpia .....	11
1.3.3. Capa 3: Fachada de las instalaciones y área de recepción .....	12
1.3.4. Capa 4: Pasillo, área de acompañamiento y espacio gris.....	13
1.3.5. Capa 5: Sala del centro de datos y espacio blanco .....	14
1.3.6. Capa 6: Gabinete del centro de datos.....	16



2. Ingeniería social .....	19
3. Comparativo de sistemas biométricos .....	22
4. Cámaras y sensores .....	28
5. Distribución segura en planta física: capacidad eléctrica, aire acondicionado, refrigeración, extintores y control de acceso.....	36
6. Electricidad: aterramiento, generadores, Ups, emisiones de equipos y fallas por arco eléctrico .....	41
7. Temperatura y Humedad .....	45
Cierre .....	47
Referencias bibliográficas .....	48

# Aprendizaje esperado

Determinan esquema de data center, considerando niveles de seguridad física y lógica.

Identifican arquitectura lógica y física de un rack de comunicaciones, considerando aspectos de seguridad y vulnerabilidad.



Fuente: itdigitalsecurity.es. (s/f). Recuperado en agosto del 2022, disponible en:

<https://bit.ly/3BhPkWV>

# Introducción

## **¿Cómo se determina la seguridad física y lógica de un datacenter?**

En la mayoría de las organizaciones y empresas la seguridad de la información ha comenzado a considerarse como uno de los pilares muy importantes, el proceso de cómo gestionar la tecnología de información, se ha convertido en un elemento preponderante en toda estrategia de negocio relacionado con el manejo de los datos.

El uso de metodologías estratégicas que garanticen una gestión segura de los procesos de negocios es una respuesta a las exigencias que realizan los clientes en el mercado presente.

Esta necesidad ha impulsado el planteamiento de nuevos paradigmas en el entorno TI, basado en políticas y procedimientos. Para ello se aplican los estándares, códigos de buenas prácticas, desarrollo de políticas, inducción al personal y evaluación del riesgo. Involucrándose en cada una de las etapas del proceso que realiza el usuario o durante la gestión comercial que la empresa requiera.

Con la apertura de la tecnología Cloud Computing, se ha abierto innumerables oportunidades de creación de nuevas relaciones comerciales. El cual genera que el proceso de protección de datos sea un tema preponderante, ya que abarca desde el negocio más pequeño, hasta la más compleja de las organizaciones, donde TI es participe. Además, es importante establecer que, en una economía globalizada como ocurre actualmente; donde los países y organizaciones están relacionadas. También surge la necesidad de unificación de los criterios en las políticas de protección segura. Por lo que, es de vital importancia certificar dichos procesos.

# **1. Barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial**

Gestionar la seguridad física es cumplir con los reglamentos y estándares; aquellos que define el cumplimiento en varias industrias, los cuales tienen un conocimiento cada vez mayor; los controles de acceso a las instalaciones ayudan a protegerse contra las amenazas que interfieran con los sistemas integrales de energía y telecomunicaciones, generando una operación continua del centro de datos.

## **1.1. La importancia de los auditores**

Los auditores deben establecer si un centro de datos cumple con los estándares establecidos y adecuados, esto siempre se realizará como mejora y no debe de considerarse como un proceso obstruccionista, por lo contrario de mejoramiento. Los auditores ven cosas diferentes y sus interpretaciones pueden ser un reto a ser tratado; tener claridad en los planes y el proceso de auditoría, minimiza el riesgo de dejar una organización propensa al problema de la interpretación los logros, este proceso es muy importante para que la empresa auditada suba de nivel, porque los resultados se enfocan en mejoras de: Nivel de madurez de la empresa, establecer políticas seguras, establecer vulnerabilidades, un norte hacia el direccionamiento estratégico del negocio

(es decir hasta donde se quiere crecer). Una vez establecidas las conclusiones de una auditoría, es posible dar los siguientes pasos del planeamiento estratégico.

El diseño y estructura de un centro de datos permite la efectividad de los sistemas que lo componen; para ello se soportara sobre estándares que nos servirán de guías generales, amplias y de referencia, creando un modelo comprensivo y estratégico.

Asimismo, se obtendrá las certificaciones deseadas sin embargo hay que establecer antes del diseño, todos los estándares que se refieren al centro de datos, los más relevantes son:

- **ANSI BICSI 002-1014:** Las mejores prácticas para el diseño del centro de datos.
- **TIA 942:** Establece requisitos para la infraestructura y las telecomunicaciones dentro de los centros de datos.
- **UPTIME INSTTUTE:** Se enfoca en mejorar el rendimiento, eficiencia y confiabilidad de la infraestructura critica para el negocio.
- **ASIS:** Busca estándares de seguridad avanzados a nivel global.
- **SANS:** Las mejores prácticas y estándares de seguridad de la información.
- **ONVIF:** Se enfocan en la compatibilidad de productos de seguridad física basadas en red.

Un enfoque por capa mejora, conlleva a obtener las certificaciones necesarias y aprovecha los estándares más relevantes, construyendo un enfoque holístico. Es importante destacar que, para todos los estándares generales de diseño del centro de



datos, el componente del sistema de seguridad física cumple con lo requerido por los expertos. Esto incluye los estándares tecnológicos para la infraestructura de red, la infraestructura y la seguridad físicas.

## 1.2. Estrategia de segmentación

Las seis capas de la seguridad física definida soportan la estrategia de microsegmentación, con el objetivo de defender físicamente el centro de Datos, teniendo en consideración que esta no debe de limitar el rendimiento del centro de datos.

Una estrategia de macro-estación busca limitar del daño de una amenaza al soportar las 5D's de la seguridad perimetral, que mencionamos a continuación:

- Disuadir.
- Detectar.
- Demorar.
- Defender.
- Denegar.

Un modelo de seguridad física por capas proporciona una serie estratégica de obstáculos para protegerse de posibles incursiones físicas en el centro de datos, haciéndolo cada vez más difícil de acceder a la información crítica.

## 1.3. Seguridad física de un centro de datos

### 1.3.1. Capa 1: Defensa perimetral

La primera capa defensa perimetral, controla el acceso autorizado a la propiedad del centro de datos, si se establece adecuadamente la capa de defensa perimetral, reduciendo los costos totales de un sistema de seguridad de las instalaciones del centro de datos y mejora la efectividad del plan de seguridad.

Otro término es la filosofía de control territorial, en la cual la vigilancia natural y el control de acceso son utilizados, por ejemplo: las bermas, rocas grandes, vista despejada sin arboles ni arbustos en el camino y otros métodos de control de acceso natural. Esto no solo ayuda al monitoreo, sino que sirve como un procedimiento disuasivo. Ayuda a la defensa perimetral y generalmente se logra a bajos costos.

- **Integración:** La mayoría de los centros de datos no tienen señales que indiquen los tipos de negocio.
- **Muros:** Primera línea para la protección de las instalaciones, una muralla la más sencilla posible separa las instalaciones del ambiente.
- **Sensores para seguridad:** Los sensores para los sistemas de intrusión del perímetro usan un tipo de cable especial (cobre y fibra óptica), también utiliza la electrónica para sentir vibraciones y perturbaciones e identificar si hay algún intruso, estas soluciones pueden desarrollarse como zonas de muros, paredes y aplicaciones bajo tierra.

- **Luz del perímetro:** La iluminación es preponderante en el sistema de protección perimetral del datacenter, proporciona un cubrimiento visual mejorado del personal de seguridad y las cámaras de videovigilancia, sino que mejora la iluminación perimetral.
- **Cámaras térmicas:** El área perimetral exterior e interior pueden ser monitoreadas por cámaras térmicas, en muchos casos, únicamente el punto de entrada principal estará bien iluminado, las cámaras establecen la confirmación de alguien que está fuera de las instalaciones
- **Estación de seguridad vehicular:** Es una cabina de seguridad para personas adentro, es un punto de entrada vehicular, el cual contiene una cámara y/o un sistema de audio que permite comunicarse en forma interna con aquellas personas en el vehículo mientras se acercan a un punto de verificación.
- **Reconocimiento de placas vehiculares (LPR):** Las cámaras sensibles a infrarrojos (LPR) son capaces de visualizar las placas de los vehículos incluso a los vehículos con desplazamiento rápido o veloz y desde niveles de luz del sol brillante hasta la oscuridad completa.
- **Protección contra intrusos:** Las barreras que se levantan desde el subsuelo y el muro de tabiquería con un reforzamiento tal que debe ser diseñado a pruebas de choques puede usarse para vehículos que deseen acceder al lugar.

### 1.3.2. Capa 2: Zona Limpia

Dentro de la protección perimetral la amenaza puede tener acceso a las áreas críticas eléctricas y mecánicas, tales como: la planta de energía eléctrica, el cableado principal de suministro, así como los generadores y tanques de gasolina, también la accesibilidad por los muelles de carga y puntos de entradas secundarios.

- **Videovigilancia:** El monitoreo digital mediante cámaras previstas; para ello, es importante el seguimiento en exteriores e interiores, debe servir como disuasivo y como herramienta de monitoreo, también como una forma de respaldo del incidente ya actuado, un sistema de monitoreo debe ayudar a seguir de cerca de un atacante y debe establecerse como una política de seguridad.
- **Estrategia de video:** Debe soportar los protocolos de seguridad y establecer diversas estrategias incluyendo lo siguiente:
  - ✓ Un enfoque de recurso de energía ¿Qué está cerca de la infraestructura energética, tanques, áreas de carga y generadores?
  - ✓ Se debe utilizar cámaras de 180° y de alta resolución. Por ejemplo: las cámaras tipo PTZ nos ayuda, porque nos brinda una cobertura constante.
  - ✓ Detección e identificación de las personas dentro de la zona limpia.
  - ✓ Obtener un cubrimiento completo de la zona limpia, inclusive debe considerar visualizarse dentro del edificio, considerando un barrido de cámaras desde el exterior.
- **Sensores de alteración de cableado:** En los data center es importante incluir sensores de detección de intrusos físicos que deben proteger las

telecomunicaciones críticas y la infraestructura de cableado de transmisión de suministro eléctrico.

- **Puertas perimetrales laterales:** Es otro componente de la zona libre, por ejemplo: las puertas auxiliares como barrera física con único punto de cerradura (picaporte o pistilo), en el accionar es fácil de vencer, en todo caso si el presupuesto lo permite, es necesario mejorar el cierre con sistemas multipunto.
- **Uso controlado del sistema de llaves:** En el sistema de manejo de llaves existe variedad de componentes que respaldaran el control total del acceso a las llaves, en primera instancia están bajo el control del fabricante y en ninguna circunstancia deberán copiarse, el manejo y distribución son restringido a un control de monitoreo especial y con delegación de responsabilidades.

### *1.3.3. Capa 3: Fachada de las instalaciones y área de recepción*

El control de las visitas e inclusive del personal que labora en las instalaciones se está convirtiendo en una parte más amplia en el cumplimiento de las regulaciones, el PCI DSS (Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (*Payment Card Industry Data Security Standard* – PCI DSS por sus siglas en inglés) es un estándar de seguridad orientado a la definición de controles para la protección de los datos del titular de la tarjeta y/o datos confidenciales, por ejemplo, entre los más relevantes son:

- **Verificación de invitados a través de sistemas compatibles:** Debe integrarse y sincronizarse con las acciones que realizan los administradores de recursos para verificar el estado del empleado o contratista.

- **Entrada múltiple:** Es cuando se realiza las operaciones de seguridad, el visitante recibe el carnet con lectura de tarjetas.
- **Videovigilancia:** Al igual que los elementos, el video es crítico cuando el visitante ingresa al edificio a realizar un ataque, se recomiendan cámaras de alta resolución para proporcionar una identificación clara de quien es la persona.
- **Responsabilidad de todos:** Cuando se establecen políticas de responsabilidad, estas previamente deben ser autorizado por la alta gerencia y luego por todos y cada uno de los colaboradores.

#### *1.3.4. Capa 4: Pasillo, área de acompañamiento y espacio gris*

La mayoría de los data center se enfocan mucho en el espacio en blanco del data center, pero existe el pasillo gris, pasillo y las áreas de acompañamiento en general son un espacio en el cual las medidas de seguridad apropiadas son descuidadas.

- **Esclusas de seguridad para ingreso y salida:** Diferenciando desde una persona en singular hasta el control de un grupo de personas es importante la atención al detalle ya que se aprovecha de esta situación de ingreso en grupos para que los potenciales intrusos ingresen sin los permisos especiales.
- **Infraestructura de control de acceso:** En cada puerta de las instalaciones del espacio gris a la infraestructura deben considerarse puertas y cerraduras de alta seguridad.
- **Puertas y cerraduras de seguridad:** Establecidas para los accesos a todos los niveles del área gris y el área libre a nivel de todos los accesos las cerraduras que

se ubican solo en el picaporte sino además del lado de las bisagras lo que como consecuencia tiene un nivel mayor de protección.

- **Video:** Herramienta de apoyo muy importantes para el aseguramiento del espacio gris y puede cobertura en la forma más adecuada para los pasillos del área gris para ello se contará con:
  - ✓ Cámaras de alta resolución.
  - ✓ Cámaras de 360° o 180° que pueden cubrir un área significativa.
  - ✓ Cámaras con micrófonos y altavoces para mejorar la capacidad del personal.
  - ✓ La detección de movimiento que alerta del movimiento dentro de las áreas sensibles.
  - ✓ Identificación de quien fue a planta como video de respaldo.
- **Planes de emergencia adecuados:** Se debe contar con un área adicional para enfocarse son las salidas en caso de incendio de todos los puntos de las instalaciones adicionalmente se establecerán pasos luego de producirse un siniestro **¿Cómo actuar antes, durante y después de un siniestro?**

### *1.3.5. Capa 5: Sala del centro de datos y espacio blanco*

Al explorarse la importancia de cada capa de protección, se hace evidente que cada capa individual de protección es de vital trascendencia el control de acceso a la sala del datacenter, el intento de alguien de robarse un servidor o de subir un virus no podrá volverse realidad si no se le concede acceso al piso.

- **Esclusas de seguridad:** Una característica de muchos data center es la esclusa de seguridad, requiere de un acceso autorizado a una sala pequeña, en las cuales ambos lados de las puertas deben cerrar y luego otro proceso de autorización permite que otro individuo ingrese.
- **Cerramiento:** Proporciona protección mejorada para separar y asegurar los gabinetes de clientes específicos o el equipamiento de red debe tener medidas ideales de seguridad para soportar el control de acceso detección de intruso y videovigilancia.
- **Video:** En los diferentes usos para el video en las diferentes capas, pero para el data center principalmente y el espacio en blanco, hay cámaras que quedan definidas que pueden usarse, una de 360° puede usarse en los pasillos frío o caliente. Basándose en cómo se integra en el control del acceso del gabinete es oslo ejemplos también dependiendo del tipo de uso y área que se debe destinar un tipo de cámara las más conocidas son:
  - ✓ Cámara PTZ.
  - ✓ Cámaras de luz baja.
  - ✓ Cámaras térmicas.
- **El factor triple de la biométrica:** En el caso de algunos data center incluso con protocolos de alta seguridad, aun confían en los carnets que requieren la autenticación dual incluso al proteger la esquina interior del datacenter las mejores prácticas indican el uso de la identificación biométrica al estar cerca de los datos más importantes.




- **La biométrica:** La biométrica, ya sea por huellas dactilares, escaneo del iris o de otra forma, prueba de forma positiva la identidad de un individuo, las tarjetas de autenticación dual proveen la apariencia de seguridad.
- **Conveniencia:** Los sistemas biométricos evitan situaciones en las cuales una tarjeta se pierde o se extravía, lo cual resolver requiere tiempo, energía, esfuerzo, y costos, una huella dactilar o iris no necesita reemplazo obteniendo una solución más eficiente.
- **Costos:** Los costos administrativos de un sistema biométrico a lo largo del tiempo es más económico que el uso de las tarjetas.

### *1.3.6. Capa 6: Gabinete del centro de datos*

La infraestructura de TI se debe albergar en el gabinete del datacenter, por regla general estos gabinetes son inseguros. El control de acceso se implementa para cumplir más regulaciones. La capacidad de identificar positivamente a quien ingresa es esos gabinetes.

- **Un problema de llaves:** Generalmente en muchos gabinetes son ubicados con una única llave maestra, cada llave maestra, aunque como lo indica su nombre puede abrir todos los gabinetes del centro de datos o en todo caso del mismo modelo.

Esta situación crea una situación de seguridad de muchos data center las implicaciones de acceso son significativas incluyen los siguientes:

- ✓ Robo de Servidores.
  - ✓ Robo de almacenamiento.
  - ✓ Transmisión de virus.
  - ✓ Interrupción de energía o conectividad.
- **Restricciones de llaves:** Si las condiciones exigen utilizar un acceso de llave se deben tomar los pasos para reducir los riesgos en la manipulación y responsabilidad.
  - **Soporte de mejores prácticas:** El uso de mejores prácticas es usado para disminuir el riesgo de alguna forma la aplicación de las políticas como ejemplo incluyen el rastreo estricto de todos aquellos a los que se les otorgo acceso al espacio en blanco, no permitir que los visitantes estén solos en el centro de datos.
-  Se necesita además un plan para el control de acceso al gabinete para los centros de datos que son privados.

- **Productos de control de acceso para el gabinete:** En los últimos tiempos el número de productos de control de acceso que intentan resolver el problema de la seguridad del gabinete se ha incrementado en el mercado, generalmente se usa la biometría de autenticación dual (o más factores) en una forma de asegurar a aquellos que tengan la autorización del uso del gabinete.
- **Reporte de auditoría:** Para obtener un nivel adecuado de seguridad y cumplimiento a través de un reporte verificable de auditoría, esto se limita a horas específicas o a personas autorizadas para el ingreso por ejemplo un contratista solo tendrá autorización de ingreso y uso de un horario determinado.
- **Compatibilidad y video:** El control de acceso, el proceso de integración de la videovigilancia y el control de acceso crea un reporte verificable de auditoría aquellos que se encuentran dentro del gabinete.
- **Lector de gabinete integrado o de final de fila:** ya sea integrado en el picaporte o a través de un sistema de accesibilidad en el gabinete al final de la fila.

## 2. Ingeniería social

Actualmente como es visto por las empresas u organizaciones los datos e información de cualquier índole se ha vuelto un bien invaluable para la sustentación económica de la empresa, ya sea como parte de un activo o como soporte se gasta innumerables recursos en su protección; Sin embargo, hay un activo que no se ha podido controlar por completo; el hombre; y dada su complejidad, se convierte en un elemento voluble y difícil de proteger ante relaciones sociales entonces sustentándonos en esta información podremos conceptualizar que la ingeniería social es:

Es el acto de manipular a las personas a través de técnicas de psicología y habilidades sociales para hacer que la persona influenciada sin saberlo nos dé la información necesaria o en todo caso obtener a través de ella el acceso a la información o a un sistema o en todo caso la ejecución de una actividad más elaborada como un ataque cibernético, secuestro, engaño etc.

Los conceptos asociados a la ingeniería social datan de la década de los 90's y fueron difundidos por *Kevin Mitnick* también conocido con el sobrenombre "Condor" considerado como uno de los mejores hackers de la historia según *Mitnick*, la ingeniería social es posible por la explotación de 4 aspectos básicos inherentes al ser humano.

1. Todos queremos ayudar.
2. El primer movimiento es siempre de confianza hacia el otro.
3. No nos gusta decir no.
4. A todos nos gusta que nos alaben.

Estas características permiten de alguna manera aprovechar las falencias de la condición humana para idear una estrategia que permita influir sobre la toma de decisiones.

Dentro de las condiciones de penetración que tienen los ciber-delincuentes, se hace uso de algunas características básicas de todo ser humano tales premisas son:

- **Curiosidad:** Hace que la curiosidad del ser humano al ver páginas con acceso prohibidos con contenido explícito o de algún tipo de interés sui-generis.
- **Atracción:** Relacionados a las redes sociales o algún tipo de página de interés empático la idea es suplantar la identidad ayudándose de imágenes sugerentes o de grandes atributos a fin de enredar mediante técnicas de engaño.
- **Miedo:** Se usa el Mail y esto es que suplantando un nombre genera miedo e incertidumbre logrando objetivos mediante la coerción y obteniendo datos confidenciales ayudas o auxilios para ingresar a sitios prohibidos.
- **Empatía:** Apela a las buenas acciones de la víctima por medio de correos alusivos a personas con enfermedades terminales u obras caritativas, solicitando auxilios de dinero o consignación directa en su forma más simple.

Cuando se habla de ingeniería social desde una perspectiva del ciberdelincuente se suele hablar de cuatro vectores (es decir tipos de ataques) los más importantes son:

- **Phishing:** Significa pesca o suplantación de identidad utilizando el engaño como lo hace el pescador con el fin de embaucar a la víctima y obtener lo prohibido.

- **SMiShing:** Si, es algo real, y significa "*SMS phishing*" o *phishing* a través de mensajes de texto, llega un mensaje al móvil con un enlace en el que, con un simple clic, los atacantes pueden robar credenciales o cargar malware.
- **Vishing:** Es "*voice phishing*" es decir, por voz o por teléfono. Este ataque se ha incrementado es fácil barato y más lucrativo.
- **Impersonation:** Imitación o interpretación de un rol. En el pasado año, se han recolectado variada información de suplantación como el de policías, agentes federales y otras profesiones.

### 3. Comparativo de sistemas biométricos

De acuerdo con la revista (USERS) el cual escribe que:

"La biometría es estudio de métodos automáticos para el reconocimiento de personas basados en rasgos de conducta o físico. Etimológicamente, proviene del griego BIOS (vida) y metro (medida). En nuestro campo, es la aplicación de métodos matemáticos y tecnológicos para identificar o verificar identidad"

Pacheco, federico G, Jara, Héctor. *Seguridad Física y Biometría en USER*. 2009 vol.

173No 352, p 59.

Asimismo, el objetivo es controlar la accesibilidad de las personas no autorizadas, con el fin de proteger los datos y realizar un buen desempeño de la gestión de seguridad.

Este tipo de tecnología se encarga de verificar la identidad del usuario comprobando factores que estén relacionados con la biología de la persona.

- **Sistema biométrico:** Es la implementación de algoritmos de reconocimiento biométrico que básicamente se apoyan en la comparación de una representación digital de un rasgo físico o de comportamiento con uno previamente registrado. Se usa una metodología basada en características fisiológicas es más confiable que uno que adopta características de comportamiento. De acuerdo con el libro (*handbook of biometrics*) el cual afirma que, se puede ver que un sistema biométrico genérico tiene cuatro módulos

principales: Un módulo sensor, Un módulo de evaluación de calidad y extracción de características; un módulo a juego; y un módulo de base de datos.

- **Módulo de sensor:** Se requiere un lector o escáner biométrico adecuado para adquirir los datos biométricos sin procesar de una persona, para obtener imágenes de huellas digitales, por ejemplo, define la interfaz hombre-máquina.
- **Evaluación de calidad y módulo de extracción de características:** Primero se evalúa la calidad de los datos biométricos adquiridos por el sensor para determinar la identidad del proceso posterior. Por lo general se aplican los algoritmos de mejora de señal para mejorar la calidad.
- **Módulo de coincidencia y toma de decisiones:** Referidas a las características extraídas que comparar con las planillas almacenadas para generar puntuaciones de coincidencia.
- **La base de datos actúa como el depósito de información biométrica:** Durante el proceso de inscripción, el conjunto de características extraídas de la muestra biométrica sin procesar (es decir la plantilla) se almacena en la base de datos junto con cierta información biográfica caracterizando al usuario.

## Verificación e Identificación

Los sistemas biométricos operan en dos módulos.

- **Verificación:** Basados en el método de la comparación, por ejemplo, la persona afirma que es María Sánchez y ofrece la huella digital; el sistema acepta o rechaza el reclamo basado en la comparación del patrón ofrecido (consulta o entrada) y



el patrón registrado (referencia) asociado con la identidad reclamada (María Sánchez).

- **Identificación:** ¿Se encuentra esta persona en la base de datos? Dado un numero generalmente grande (por ejemplo, millones) de identidades inscritas, existen actualmente dos escenarios de identidad.

- ✓ **Identificación positiva:** La persona que el sistema biométrico lo conoce.

- ✓ **Identificación negativa:** La persona afirma que el sistema biométrico no lo conoce.

En ambos escenarios, el sistema confirma o niega la afirmación de la persona al adquirir su muestra biométrica.

- **Características biométricas:** A continuación, se detallan como características biométricas:

- ✓ **Universalidad:** Cada persona o individuo tiene un solo rasgo biométrico que se está utilizando.

- ✓ **Singularidad:** No debe existir dos personas iguales en términos del rasgo biométrico usado.

- ✓ **Permanencia:** El rasgo biométrico de un individuo debe ser permanente e invariable durante un periodo de tiempo con relación al algoritmo establecido.

- ✓ **Rendimiento:** El rasgo biométrico debe ser invariable con el tiempo.

- ✓ **Medibilidad:** Debería adquirir y digitalizar el rasgo biométrico utilizando los dispositivos adecuados.
  - ✓ **Burla:** Facilidad con que cuenta el atacante puede imitar el rasgo de un individuo.
  - ✓ **Recopilar:** El rasgo biométrico debe ser medible.
  - ✓ **Rendimiento:** EL proceso del rasgo biométrico debe ser preciso y rápido.
  - ✓ **Seguro:** Debe ser seguro y no se puede copiar.
  - ✓ **Aceptabilidad:** Las personas deben estar dispuesta a aceptar el sistema biométrico.
- **Autenticación basada en biometría:** Los sistemas biométricos se dividen en diversos tipos como son los fisiológicos y de comportamientos.

### **Tipos de Biometría**

Dentro de los tipos o características en las cuales es posible este proceso están:

- **Fisiológica:**
  - ✓ Reconocimiento de Voz.
  - ✓ Reconocimiento de la retina e iris.
  - ✓ Reconocimiento por voz.
  - ✓ Reconocimiento de la huella dactilar.
  - ✓ Reconocimiento de la palma de la mano.

- **Comportamiento:**

- ✓ Reconocimiento de la vascular.
- ✓ Reconocimiento del Oído.
- ✓ Dinámica de Tecleo.
- ✓ Dinámica de Firma.
- ✓ Estilo de Marcha.
- ✓ Movimientos de Labios.

**Tipos de biometría conductual:** La biometría del comportamiento humano es aquella que mide los patrones de posición en oposición de las características físicas entre los cuales están:

- Dinámica de tecleo.
- Reconocimiento de firma.
- Estilo de marcha.
- Movimiento de los labios.

## Comparativa de sistemas biométricos

A continuación, en la tabla siguiente se realiza una comparativa de los diversos sistemas biométricos:

	Ojo (iris)	Ojo (retina)	Huella dactilar	Vascular Dedo	Vascular Mano	Geometría Mano	Escritura y Firma	voz	Cara 2D	Cara 2D
Fiabilidad	Muy alta	Muy alta	Muy alta	Muy alta	Muy alta	Alta	Media	Alta	Media	Alta
Facilidad de uso	Media	Baja	Alta	Muy alta	Muy alta	Alta	Alta	Alta	Alta	Alta
Prevención de Ataque	Muy alta	Muy alta	Alta	Muy alta	Muy alta	Alta	Media	Media	Media	Alta
Aceptación	Media	Baja	Alta	Alta	Alta	Alta	Muy Alta	Alta	Muy alta	Muy alta
Estabilidad	Alta	Alta	Alta	Alta	Alta	Media	Baja	media	media	Alta

## 4. Cámaras y sensores

Los sistemas de seguridad se plantean desde hace un tiempo debido a la necesidad de las personas para proteger su integridad física o simplemente proteger la información que está relacionado a una información sensible.

Tomando en cuenta los diferentes objetivos que cumplen los equipos de seguridad no cabría duda de que estos elementos nos faciliten el resguardo y protección dejando atrás el arriesgar nuestras vidas.

Parte de un sistema de Telemetría consiste en la medición de distancias por medio de información digital, consiste en un transductor como un dispositivo de entrada, el transductor convierte una magnitud física como la temperatura presión o vibraciones en una señal eléctrica correspondiente que es transmitida a una distancia efectos de medición y registro.

### **Circuito Cerrado de Televisión (CCTV)**

El circuito Cerrado de Televisión proviene del inglés *Closed Circuit Television* es una tecnología de videovigilancia diseñada para vigilar una diversidad de ambientes y actividades se denomina circuito cerrado de televisión ya que como su nombre lo indica todos los elementos están enlazados.

Un CCTV puede ser conceptualizado como un medio de enviar imágenes desde un lugar a otro, siendo estas imágenes en tiempo real, ya que este sistema proporciona una supervisión óptica constante de todo tipo de incidencias en el espacio protegido. Como consecuencia de esto el uso masivo del circuito cerrado de televisión (CCTV) es

una aplicación en sistemas de seguridad para vigilancia control de intrusismo y registro visual de algún tipo de intrusión o ataque en el centro de datos.

### **La tecnología de las cámaras**

Según los últimos estudios de mercado la instalación de cámaras de vigilancia en cualquier ámbito y sobre todo en los *data center* se ha incrementado exponencialmente frente a una cifras impresionantes de ventas de cámaras analógicas, Las cámaras de red han emergido como la categoría de mayor crecimiento y según las predicciones el auge de las cámaras digitales va sobrepasar hasta reemplazarlas en el mercado actual, se sigue aun optando por combinar este tipo de tecnologías analógico-digital por cuanto es preponderante el costo con los cuales se ejecuta hay que considerar que el uso de cámaras son ideales para muchos mercados estándar así como el creciente mercado de la seguridad residencial.

- Empresa.
- Centros comerciales.
- Instituciones bancarias y financieras.
- Ayuntamientos.
- Campus universitarios.
- Escuelas primarias.
- Gobierno.
- Transporte.

- Militar.
- Refuerzo legal.

## Elementos del sistema de Videovigilancia

Aunque todos los elementos son necesarios es importante mencionar que la red por la cual se transporta el video, el servidor y los componentes de almacenamiento son equipos generales sin embargo hay que mencionar los diferentes tipos de cámaras las cuales se detallan a continuación:

- **Cámara de red:** Un cámara de red funciona como un servidor independiente en una red y se coloca siempre y cuando exista una red en las instalaciones, más conocidas como cámaras IP puede tener funcionalidades avanzadas al tener un servidor web, servidor ftp, cliente ftp, cliente de correo electrónico.
- **Cámara red fija:** Cuando se necesita un enfoque en forma directa esta se coloca en una dirección abarcando solo lo que el lente capta.
- **Cámara de red fija tipo domo:** Es una cámara preinstalada en una carcasa se dirige en cualquier dirección, la dificultad radica en la dificultad para observar en qué dirección apunta la cámara.
- **Cámara de red PTZ:** Tiene la facilidad de rotar alrededor de eje vertical-horizontal, así como tiene la propiedad de alejarse y acercarse hasta que la lente o el diseño de la cámara lo permita, se usan generalmente en interiores.
- **Amara de red PTZ no mecánica:** Tiene un sensor de megapíxeles y una lente de visión amplia que le permite tener una Angulo de 100-180grados además de

tener la facilidad de tener zoom de la cámara sin necesidad de movimiento mecánico.

- **Cámara de red domo PTZ (Pan-Tilt-Zoom):** Tiene una cobertura mayor debido a su diseño permite un giro de 360grados y una inclinación que puede ser de 180grados, son ideales para el uso de instalaciones discretas.

## Sensores

Los sensores son componentes electrónicos que recogen información del mundo "real" y le entregan al sistema de control de forma que el sistema de control "entienda" y pueda realizar el procesamiento de la información real la "entienda" y la procese a fin de tomar una decisión, por ejemplo, un sensor de temperatura de estado de puerta(abierto/cerrada), de humedad, de velocidad del aire, de nivel de CO2, etc.

La principal función es transportar un parámetro o estado físico del entorno que nos rodea en una información que se traduzca a señales eléctricas que proporcionaremos al sistema de control.

Generalmente los sensores están ligados a los actuadores, que son dispositivos que siguiendo las órdenes del sistema de control (usa sensores/actuadores) y es capaz de realizar acciones que repercuten en el mundo real, por ejemplo, en data center para la apertura automática de puertas o sistemas de vigilancia o sensores de movimiento en el mismo data center hay infinita de aplicaciones en lo que se usan los sensores/actuadores y los principios de aplicación también merecen un enfoque diferente.

Un ejemplo de sistema de control donde interviene los sensores, actuadores podría ser en un estacionamiento:



*"Un sensor de luz le indica al sistema de control que hay poca luz en lo estacionamientos que vigilamos y el sistema de control por lo tanto ordenara a los actuadores que hay que activar los faroles definidos para ello, activa un actuador que hará el trabajo de prender los faroles que se iluminen de tal manera que el sensor se apagara al recibir la luz adecuada"*

Para realizar las mediciones del mundo real tanto mecánicas eléctricas, térmicas, químicas etc., existen los sensores y/o transductores.

Los sensores reciben los cambios de la magnitud descrita líneas arriba, dependiendo de que tipo de magnitud deberá medir un sensor de flujo, no medirá temperatura o viceversa, una vez recibida la información del mundo real el sensor mismo transformará la información en señales eléctricas de tal manera que se pueda leer y tomar las decisiones correctas.

Existen gran cantidad de sensores para medidas de todo tipo, por tanto, se pueden clasificar de forma diferente.

#### **Según el tipo de salida que proporcionan:**

- **Analógicos:** Entregan salida de nivel variables en función del parámetro que miden.
- **Binarios:** Entregan un nivel "todo" - "nada" (1/0).
- **Digitales:** Entregan la información relativa a la medida con un protocolo de comunicación específico que el fabricante facilita.

### Según su estructura interna, tipo de sensor:

- **Pasivos:** No precisan de alimentación: resistencias que cambian de valor según luz o temperatura.
- **Activos:** Tienen circuitos electrónicos que alimentar y necesitan una fuente de energía.

### Según el tipo de parámetros que son capaces de detectar:

- **Mecánicos:** Relacionado a acciones físicas de fuerza masa y gravedad.
- **Ambientales:** Medidas de temperatura, humedad pluviometría, velocidad del viento.
- **Químicos:** Control de niveles de partes por millón (unidad de medida) de tal manera que comparan los niveles de oxígeno, contaminación en el aire, azúcar en la sangre.

Qué parámetros miden y cómo nos entregan su valor: Los valores asociados a al sensor: Temperatura, humedad, luz, acidez, velocidad, abierto cerrado y nos entregan un valor eléctrico del tipo:

- Salida analógica 0 a 10Vcc.
- Salida de 0 a 5Vcc.
- Salida de Bucle de corriente de 0 a 20 mA etc.

Otras características importantes:

- Rangos de medida.
- Resolución de medida.
- Precisión.
- Tiempo de medida.
- Repetitividad.
- Linealidad.

**Montaje y conexión:** Normalmente se montan según las necesidades de medida para ello se leerán las recomendaciones del fabricante para su ubicación.

- El esquema de conexión está en el *datasheet* del sensor.
- Antes de conectar asegúrese con los parámetros y formas de alimentación para evitar averías.
- Después del conexionado se verificará, si es posible, el funcionamiento del sensor.
- Intentar anticiparse a problemas posteriores que se puedan dar en la instalación.
- La mayoría de los sensores van conectados al sistema de control.

En el caso de sensores de para la puesta en marcha de sistemas, seleccionar opciones, ajustar parámetros, etc. Se trata de los pulsadores, interruptores conmutadores, potenciómetros, teclados numéricos y alfanuméricos, etc. También son parte relevante en un sistema de control entre los más importantes en un datacenter se puede visualizar en la imagen:



Figura 1: Sensores de un Datacenter

Fuente: Docplayer. (s/f). Recuperado en agosto del 2022, disponible en:

[https://docplayer.es/docs-images/41/2868433/images/page\\_19.jpg](https://docplayer.es/docs-images/41/2868433/images/page_19.jpg)

## 5. Distribución segura en planta física: capacidad eléctrica, aire acondicionado, refrigeración, extintores y control de acceso

Dentro de un tipo de estándar para el diseño del *data center* existe un estándar: El ANSI/TIA-942 creado por los miembros de la industria, consultores y usuarios con las mejores prácticas para la construcción y gestión del *data center* este estándar incluye un anexo sobre los grados de disponibilidad TIER que indican el nivel de fiabilidad de un data center.

- TIER I-*Data center* básico.
- TIER II – *Data center* con componentes redundantes.
- TIER III – *Data center* con mantenimiento concurrente.
- TIER IV – *Data center* tolerante a fallos.

Un *data center* TIER IV está pensado para que el servidor de una sala de TI tenga una fuente de alimentación eléctrica independiente y activa a la vez calculada con la base instala de servidores y que se replica enteramente con un margen adicional (del 10%) para nunca tener el sistema eléctrico en pleno.

Un *data center* debe ser modular; lo que permite la escalabilidad cada módulo con uno o varias salas IT que funcionan de manera autosuficiente.

## **Sistema Eléctrico**

Un sistema eléctrico es la base fundamental para la correcta operación de un equipo electrónico, como los que serán usados en el *data center* necesario contar con un sistema eléctrico totalmente de confianza y que brinde un servicio siempre disponible.

El sistema eléctrico debe estar disponible, ya que los equipos electrónicos realizan miles de transacciones por segundo. Como referencia si se tienen un proceso de replicación de un data center de un banco en ningún momento el sistema debe ser interrumpido.

## **Sistema de Climatización**

La salida de calor de cada uno de los servidores el traslado de la información dentro del cableado y el calor en si afecta negativamente en el rendimiento del equipo y acorta su vida útil.

En el planteamiento del diseño se exige comprender la cantidad calorífica de los equipos junto con el que produce otras fuentes de calor que generalmente está en un rack como los SAI (Sistema de alimentación ininterrumpida) la alimentación eléctrica, las unidades de aire acondicionado, iluminación y las personas.

En una instalación típica las cargas de más peso son: el 70% son equipos de TI; el 9% la iluminación; el 6% a la distribución de la alimentación y el 2% a las personas.

Además del calor el sistema de aire acondicionado para un data center está diseñado para controlar la humedad.

## Refrigeración

Como cualquier tipo de tecnología los sistemas de refrigeración han ido avanzando en cuanto a las actualizaciones y han mejorado a lo largo de los años, se vera la última tecnología en sistemas de refrigeración, y que métodos utilizan los data center de cara a poder mantener la temperatura de sus instalaciones dentro de los límites.

Existen dos maneras de refrigeración de los *data center* que pasamos a explicar:

- **Basados en aire:** Como bien dice el nombre este tipo de refrigeración se basa en cañerías de aire para enfriar los dispositivos, la idea es separar el aire caliente del aire frío, básicamente se bombea aire frío hacia los equipos y luego se succiona el aire caliente, este modelo de refrigeración es poco eficiente ya que se deben bombear lo que suma una cantidad de energía.
- **Basados en liquido:** Por otro lado, estos sistemas basados en líquido se basan en contenedores de agua fría la que se bombea a través de tuberías que pasan entre los racks y equipos, se mantiene una barrera entre los dispositivos el agua que circula ya que el agua conduce la electricidad y podría dañar los componentes si existe contacto.

## Extintores

Existen en la actualidad diferentes tipos de extintores que funcionan a través de agua, gas o mezcla química para enfrentar las llamas. La decisión de implementar un tipo de extintor dependerá del tipo de fuego.

- Clasificación de fuego de un data center:
  - ✓ **Fuego clase A:** Son los fuegos producidos por materiales orgánicos sólidos como son la madera, el cartón, los papeles, telas etc.
  - ✓ **Fuego de clase B:** Son los fuegos iniciados por líquidos inflamables y materiales que arden con facilidad, como la gasolina el, el petróleo, entre otros.
  - ✓ **Fuego clase C:** Son originados por equipamiento eléctrico energizado, como por ejemplo computadores, servidores y herramientas eléctricas.
- Tipos de extintores que usar:
  - ✓ **LA NFPA 75:** Estándar para la protección contra incendios de tecnología de la información.

Se deberán usar los extintores de incendios portátiles listados de tipo dióxido de carbono o agente halogenado para la protección de los equipos electrónicos; NFPA 10 norma para extintores portátiles.

Se deben proporcionar extintores listados con una calificación mínima de 2A para uso en incendios en materiales combustibles ordinarios como papel y plásticos, Los extintores secos no se permitirán.

- Entre los muchos extintes tenemos los siguientes:
  - ✓ **Extintor a base de agua pulverizada:** No conduce la electricidad es recomendada para los fuegos del tipo A y C y la boquilla está diseñada para que salga el agua en forma de niebla.



- ✓ **Extintor a base de dióxido de carbono:** No conduce la electricidad es un gas que no es combustible es óptimo para los fuegos de clase B y C.
- ✓ **Extintor de halotron:** Es un gas limpio que no deja residuos y no es conductor de electricidad se libera en forma líquida y se gasifica extinguiendo por enfriamiento y sofocación recomendada para los fuegos clase A, B y C.

## Control de accesos

Definido como el control de acceso se trata sobre los sistemas que protegen a los objetos de valor y también sobre la decisión de acceder al área; puede ser usado para el control a espacios físicos o la información dentro del sistema.

- Tipos de Controles
  - ✓ **Controles administrativos:** Ayudan a hacer frente a las amenazas internas, como el robo de información privilegiada o violación de la base de datos
  - ✓ **Controles Físicos:** Se usan para disuadir y prevenir eventos desastrosos dentro de un ambiente físico
  - ✓ **Controles Técnicos o Lógicos:** Restringen al acceso a los sistemas de información y protegen la información que ellos contienen; tales como el cifrado, tarjetas inteligentes, listado de control de acceso etc.

## **6. Electricidad: aterramiento, generadores, Ups, emisiones de equipos y fallas por arco eléctrico**

Las normas de la industria de los gabinetes eléctricos existen en la promoción de la seguridad la eficiencia en el diseño define los niveles mínimos de los equipos relacionados al sistema eléctrico.

### **Requerimientos previos al diseño eléctrico**

Al elegir la ubicación del edificio la compañía de suministro eléctrico deberá proveer la capacidad eléctrica necesaria para su funcionamiento y su futuro crecimiento el diseño se debe contemplar la capacidad, crecimiento, mantención y la redundancia de la instalación ya que la carga eléctrica del data center seguramente se incrementará con el paso del tiempo.

### **Selección del generador**

Relacionado a la interacción entre el sistema eléctrico principal y el UPS puede causar problemas si el equipo no es seleccionado adecuadamente deben ser capaces de soportar los efectos de la corriente de armónicos debido a la operación del sistema UPS, las cargas de la computadoras y equipo electrónico en caso de contar con generadores en paralelo, deben establecerse controles con sincronización tanto manual como en forma automática.

### **Respaldo con sistema UPS (*Uninterruptible Power Supply*)**

El sistema del UPS deberá proporcionar el respaldo suficiente (en capacidad y tiempo) para que el sistema pase en estado de *stand By* a tomar la alimentación eléctrica de la carga sin sufrir una interrupción.

El sistema UPS consiste en monitorear sistemas individuales o módulos e UPS en paralelo, de igual manera se aplica a los bancos de baterías provistas para el sistema de UPS el criterio vario desde 0.38 y 2.7 kW por metro cuadrado y deberá contemplarse al menos un 20% adicional en la capacidad del UPS por crecimiento.

### **Uso de unidades PDU (Distribución de fuerza a equipo de telecomunicaciones)**

Se debe considerar el uso de PDUs (*Power Distribution Unit*) para la distribución de energía al equipo electrónico de telecomunicaciones critico en el *data center* el cual resulta más efectivo que el uso de tableros y transformadores, lo tableros de distribución que alimentan a los DPU pueden ser montados en una sala de fuerza remota.

### **Aterramiento (Puesta a tierra)**

El calibre del conductor de puesta a tierra deber ser al menos de 4 AWG de cobre desnudo enterrado a 1 metro de profundidad, el aterrizaje de las columnas de acero del edificio deberá estar conectado a la malla general del sistema a tierras ninguna sección del sistema a tierra deberá exceder 5 (Ohms)

En cuanto al anterior del *data center*, en la sala de comunicaciones consiste en un amalla de 9 x 10 metros y el calibre no deberá ser menor al calibre 6 AWG o equivalente. El conductor de cobre podrá ser desnudo o preferentemente aislado para evitar contactos intermitentes o involuntarios.

## Consideraciones del arco eléctrico para tu centro de datos

Cuando se trata el diseño del *data center* es clave en la realización del planteamiento el diseño de los espacios es clave para anticipar peligros potenciales relacionados a fallas como lo es el arco eléctrico.

La prevención cobra aún más importancia ya que no es posible interrumpir el circuito para evitar el problema.

Un arco eléctrico, se producto de una falla del equipo, del conductor, o de una conexión accidental, puede ser mortal. La liberación de energía puede causar incidentes a nivel físico e incluso la muerte, así como la destrucción total o parcial del *data center*.

Para evitar el arco eléctrico es necesario tener las siguientes consideraciones:

- **Correcta instalación de equipos**

Es importante asegurar que los equipos se instalen de manera correcta, Un pequeño error en este trabajo podría desencadenar graves problemas como un arco eléctrico además del mantenimiento.

- **Equipos debidamente equipados**

Una vez instalados los equipos dentro del *data center* estos deberían estar debidamente etiquetados. Estos deben contar con los diagramas necesarios o advertencia de seguridad provistos a simple vista para los trabajadores.

- **Implementación de soluciones para prevenir el arco eléctrico**

Además de la adecuada vestimenta (guantes, protectores, cascos, calzado de seguridad) es fundamental el uso de soluciones resistentes al arco eléctrico como los gabinetes especializados, este equipo especial protegerá contra el arco eléctrico.

## 7. Temperatura y Humedad

El aumento de la demanda del uso de los *data center* y las solicitudes de procesamiento de datos ha conllevado a las grandes empresa invertir en nuevas instalaciones para prestar servicios basados en la web y un número mayor de usuarios en esas instalaciones, ello demandara tener las mejores condiciones óptimas , tanto de temperatura como de humedad es vital para el funcionamiento de los equipamientos establecidos en el *data center* son instalaciones con gran demanda de energía que actualmente consumen más de 1.3% de la producción total de electricidad del mundo este uso de la energía eléctrica se traduce también en calor que tiene que ser transportado y disipado lejos de los bastidores de los equipos para mantener la temperatura y la función correcta por que corremos el riesgo de perder equipos porque su tiempo de vida útil se acorta o las temperaturas afectarán equipos altamente sensibles.

La refrigeración y el aire acondicionado serán parte de este procedimiento en el control de la temperatura. El proceso de enfriamiento del refrigerante usado consume mucha energía, pero puede ser reducido si durante el diseño la ubicación se considera el clima.

### **Temperatura adecuada**

La directriz ASHARE 2011 recomienda que las condiciones de temperatura que debe manejar el data center esta promedia entre los 18 a 27° C y la humedad de 25 a 80% HR(temperatura del punto de rocío 5 a 15°C) en una instalación típica la sala de servidores debe estar climatizada dividiendo lo equipos en filas (pasillos calientes ) y alimentando con aire acondicionado fresco entre las filas (pasillo fríos) generalmente a través del piso ello obligará a que el aire caliente suba sobre las filas y este aire se

extraiga desde el techo. La temperatura se controla usando una unidad de aire acondicionado de la sala de servidores (CRAC) que realiza funciones de calefacción y refrigeración.

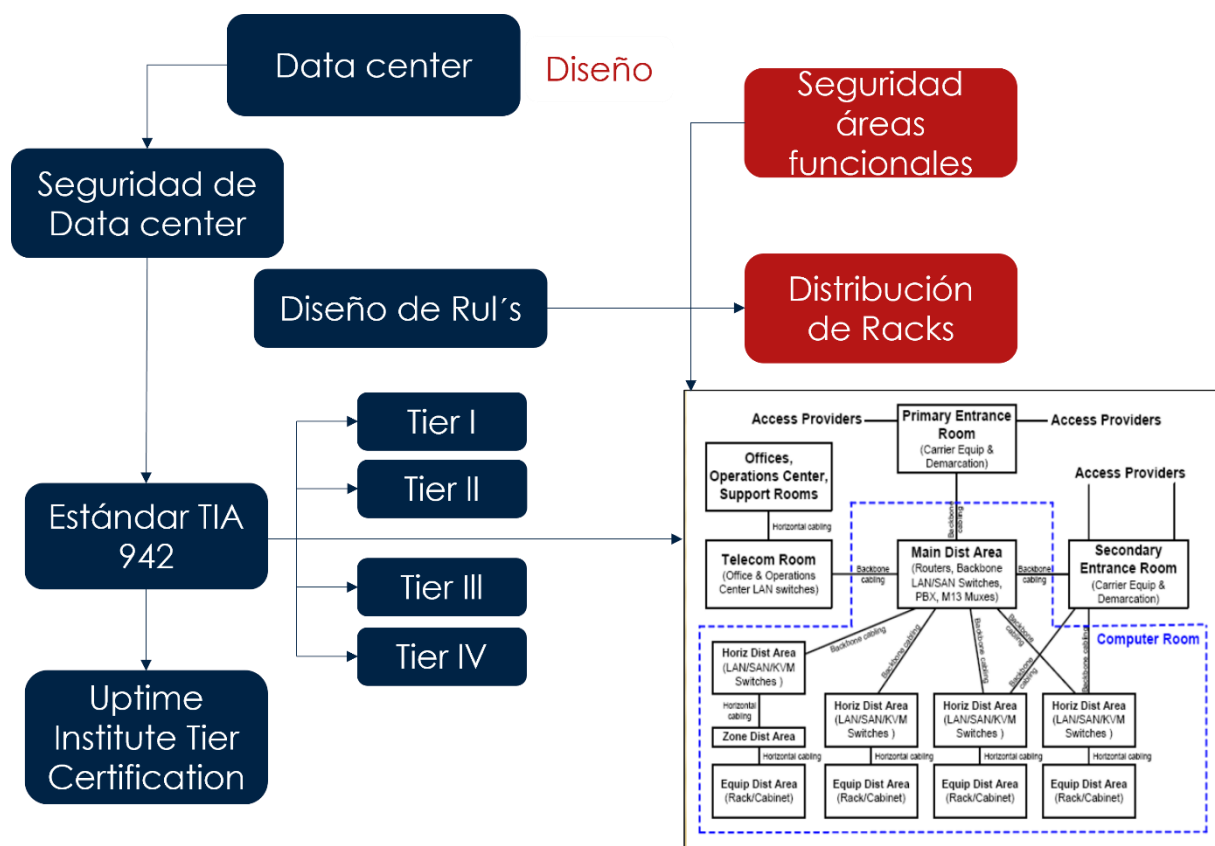
### **Mantenimiento de los niveles de humedad**

Además de la temperatura la humedad también es crítica por lo tanto este porcentaje de agua en el aire afectará los componentes de la sala de servidores, especialmente con climas fríos es donde se usa economizadores de aire, el contenido de agua absoluta del aire es naturalmente bajo. La humedad relativa del aire disminuye cuando se calienta, lo que significa que se puede caer por debajo del nivel deseado. El aire seco aumenta el riesgo de electricidad estática y requiere humificación extra ya sea mediante la aplicación de rocíos de agua o humidificadores por aspersión o evaporativos.

Cuando la temperatura excede los límites aceptables, el aire entrante tiene que ser enfriado, con el fin de minimizar la necesidad de refrigeración mecánica que consume energías puede lograr eso mediante la pulverización de niebla de agua-que evapora en el aire entrante. En sistemas en los que se utiliza líquido como soporte térmico, el refrigerante puede enfriarse en torres de enfriamiento que son intercambiadoras de calor que emplean el principio de refrigeración similar. El control eficaz de las torres de enfriamiento requiere la lectura de los datos de humedad y temperatura que a su vez permiten una máxima eficiencia de enfriamiento con un uso de energía minimizado y también proporciona un medio para el monitoreo de potencias de la torre de enfriamiento.

# Cierre

Por medio del siguiente organizador gráfico, se destacan las ideas clave de esta semana:



## ¿Cómo se determina la Seguridad Física y Lógica de un data center?

Dependiendo del tipo de metodología y dependiendo del tamaño del establecimiento se aplicará el estándar TIA -942 para lograr unificar ideas respecto al diseño de las áreas de tecnología este estándar tipifica o divide la infraestructura soporte de un centro de datos en cuatro subsistemas: Telecomunicaciones; Arquitectura sistema Eléctrico, y Sistema mecánico.



# Referencias bibliográficas

- TIA Standard. (2005). *Telecommunications Infrastructure Standard for DataCenter*. Recuperado en agosto de 2022, disponible en: <https://bit.ly/3bxb9XX>
- Abts, Dennis. *High performance datacenter networks: architectures, algorithms, and opportunities*. ISBN: 9781608454020. Disponible en: <https://bit.ly/3oWyGEF>