

SEGURIDAD FÍSICA

Ing. Alvaro Antezana
ARAM © 2021

OBJETIVOS

Describir las amenazas por su procedencia, y como afectan a los empleado, activos y recursos informáticos.

Describir e identificar medidas de control preventivas, para el resguardo de los empleados, activos y recursos informáticos

TEMARIO

Modelo de seguridad física

- Análisis de riesgos
- Identificación de objetivos de protección física
- Sistemas de protección física

AMENAZAS SEGURIDAD FISICA

- Naturales
- Humanas
- Entorno/Ambiente

DEFENSA DEL PERÍMETRO

- Rejas y puertas
- Pilones y luces
- Cerraduras

SISTEMAS ELECTRÓNICOS DE SEGURIDAD

- CCTV
- Sistema Contra Intrusos
- Molinetes y mantramp

PROTECCIÓN Y VIGILANCIA PRESENCIAL

- Policías
- Seguridad privada
- Recepción y custodio

TEMARIO

SEGURIDAD DEL DATACENTER

- Ubicación
- Climatización
- Energía de respaldo
- Protección contra incendios
- Protección contra filtrado de agua
- Acceso físico
- Paredes, techo y suelo
- Arquitectura
- ANSI/TIA 942
- Tipos de DATACENTER de contingencia

PLAN DE CONTINGENCIA

- Plan de respaldo
- Plan de emergencia
- Plan de recuperación
- Ejemplo de plan de contingencia

SEGURIDAD FÍSICA DE MEDIOS

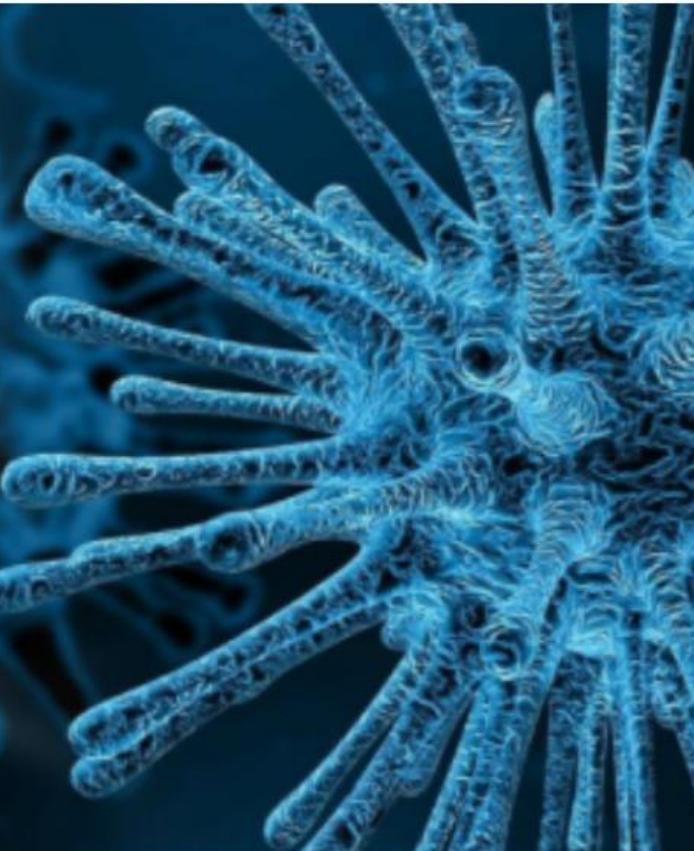
- DLPS
- Cifrado de dispositivos
- Seguridad de los backup
- Limpieza y destrucción de medios
- Destrucción de medios físicos



1. F. CUALIDAD DE **VULNERABLE**

1. ADJ. QUE PUEDE SER HERIDO O
RECIBIR LESIÓN, FÍSICA O MORALMENTE

VULNERABILIDAD



AMENAZAS

De amenaza

1. tr. Dar a entender con actos o palabras que se quiere hacer algún mal a alguien.
2. tr. Dicho de algo malo o dañino: Presentarse como inminente para alguien o algo. Una epidemia amenaza a la población.
3. tr. Dicho de una cosa: Dar indicios de ir a sufrir algo malo o dañino. La casa amenaza ruina.

MODELO DE SEGURIDAD FÍSICA

01

ANALISIS DE RIESGO

- Amenazas
- Vulnerabilidades
- Factores Físicos

02

IDENTIFICACION DE OBJETIVOS DE PROTECCIÓN FÍSICA

- Datacenter
- Ambientes de manejo de valores
- Almacenes
- Acceso Ambientes Restringidos y Pasillos Público

03

SISTEMAS DE PROTECCIÓN FÍSICA

- CCTV
- Sistema Contra Intrusos
- Control de Acceso a Físico
- Planes de contingencias

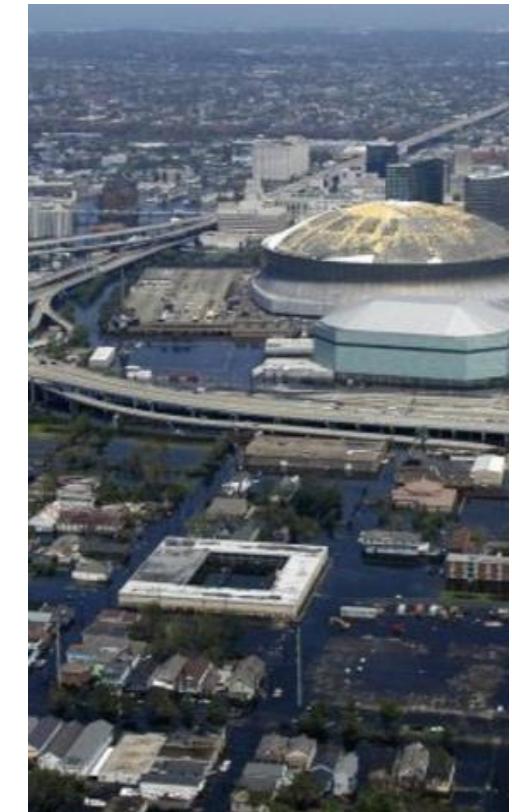
TIPOS DE AMENAZAS QUE AFECTAN A LA SEGURIDAD FÍSICA

Las amenazas que representan eventos disruptivos y que afectan a la seguridad física de las instalaciones a proteger, extendiéndose hacia las personas, así como a los bienes, objetos, materiales y equipos albergados son:

- AMENAZAS NATURALES
- AMENAZAS HUMANAS
- AMENAZAS DEL ENTORNO/AMBIENTE

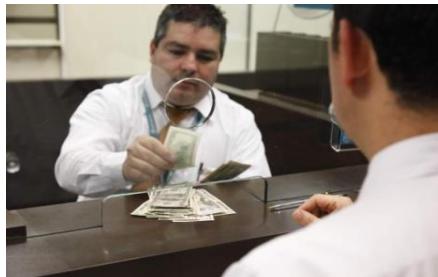
AMENAZAS NATURALES

Casan daños y pérdidas como consecuencia de los efectos originados por la acción de los fenómenos naturales tales como: INUNDACIONES, TERREMOTOS, SISMOS, HURACANES, MAREMOTOS, etc. Las amenazas naturales representan la fuente mas común de devastación.



AMENAZAS HUMANAS (SOCIALES)

Causan daños y pérdidas como consecuencia de los efectos originados por la acción directa o indirecta del hombre, tales como: ROBO, ERRORES Y OMISIONES DE LOS EMPLEADOS, ESPIONAJE, ATAQUES DE HACKERS, DE INGENIERÍA SOCIAL, así como DISTURBIOS CIVILES, ACTOS TERRORISTAS, ACCIONES SUBVERSIVAS, etc. Las amenazas humanas representan la fuente más común de desastres.





Se centran en los ambientes o entornos que albergan los recursos informáticos (almacenamiento, procesamiento y transmisión) vitales o en el Datacenter; estas amenazas están caracterizadas por disrupciones de energía (apagón, baja de voltaje, sobretensiones, picos, etc.), en fallas de los componentes de los sistemas de facilidades o en el accesos físicos no autorizados a sitios restringidos, entre otros.

AMENAZAS DEL ENTORNO/AMBIENTE

DEFENSAS DEL PERÍMETRO

Uno de los objetivos de la seguridad física es proteger los perímetros de los sitios que albergan recursos informáticos (almacenamiento, procesamiento y transmisión) confidenciales o valiosos de una organización:

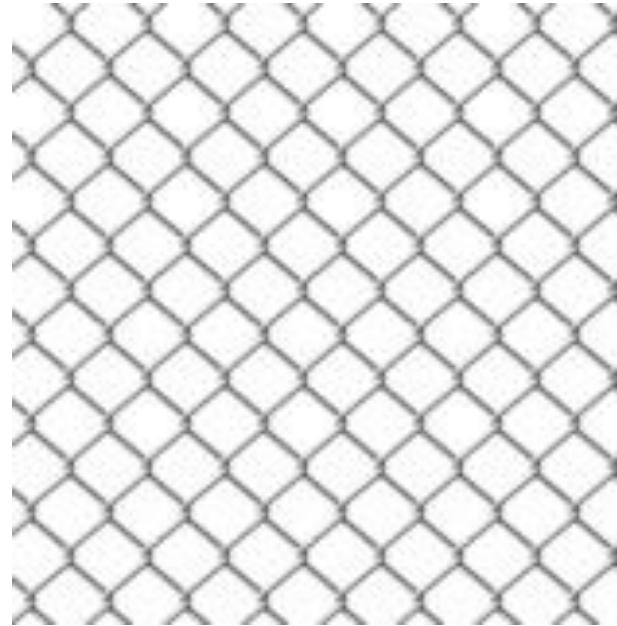
- REJAS Y PUERTAS
- PILONES Y LUCES
- CERRADURAS

REJAS Y PUERTAS

Las rejjas, pueden variar desde elementos de disuasión simples de 1m., como rejjas, a dispositivos de prevención de 2,4 metros, tipo vallas que en la parte superior cuenten con una franja de alambre de púas. Deben ser diseñadas para dirigir la entrada y salida de los puntos controlados, tales como puertas y portones exteriores.

Puertas, pueden variar desde:

- i. ornamentales (clase I)
- ii. acceso general/comercial (clase II)
- iii. garajes de clientes/empleados, acceso industrial/limitado (clase III)
- iv. muelles de carga para camiones de hasta 18 ruedas, hasta Accesos Restrictivos (clase IV) diseñados para soportar choques de autos como en instalaciones criticas de aeropuerto, prisiones, plantas nucleares, etc.





PILONES Y LUCES

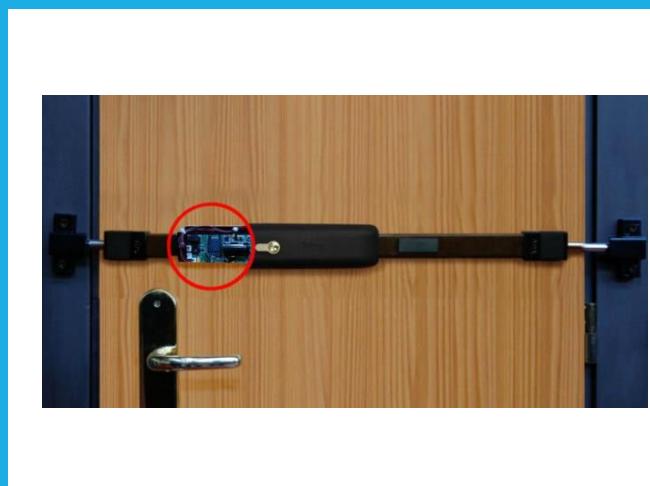
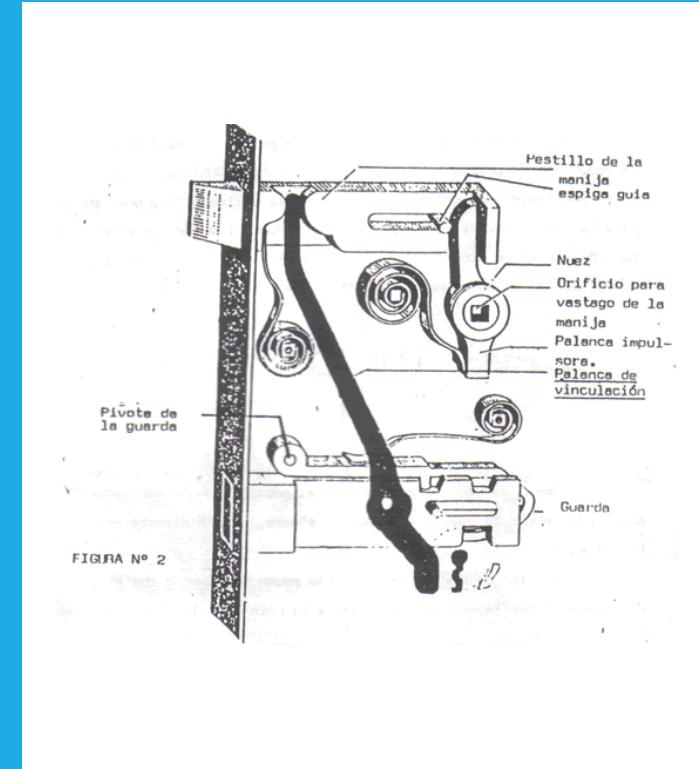
Pilones, un pilón contra tráfico es un poste diseñado para detener un auto o carro, el termino deriva de los postes cortos y resistentes (llamados postes de amarre) utilizados para amarrar los barcos atracados en los muelles.

Luces, pueden actuar como un control disuasorio e investigativo. Deben ser lo suficientemente brillantes como para iluminar el campo deseado de visión (área protegida). Tipos de iluminación incluyen los Fresnel, que es el mismo tipo utilizado originalmente en faros para apuntar la luz en una dirección específica. Un lumen es la cantidad de luz que crea una vela, históricamente se media en pies candela: Lux, basado en el sistema métrico, un lux es un lumen (1 candela) por metro cuadrado.

CERRADURAS

Las cerraduras de puertas y ventanas son un control de seguridad física preventiva para impedir el acceso físico no autorizado. Las cerraduras pueden ser mecánicos (por ejemplo, cerraduras de combinación) o electrónica, a menudo usados con tarjetas inteligentes o tarjetas de banda magnética.

Las llaves de las cerraduras, pueden ser des llaves tradicionales, dispositivos tipo teclado de pines, o de tarjetas de contacto, o biométricos.



SISTEMAS ELECTRÓNICOS DE SEGURIDAD

Los sistemas electrónicos de seguridad se refiere a cualquier equipo electrónico que pueda realizar operaciones de seguridad como vigilancia, control de acceso, control de intrusión en una instalación o área, por ejemplo:

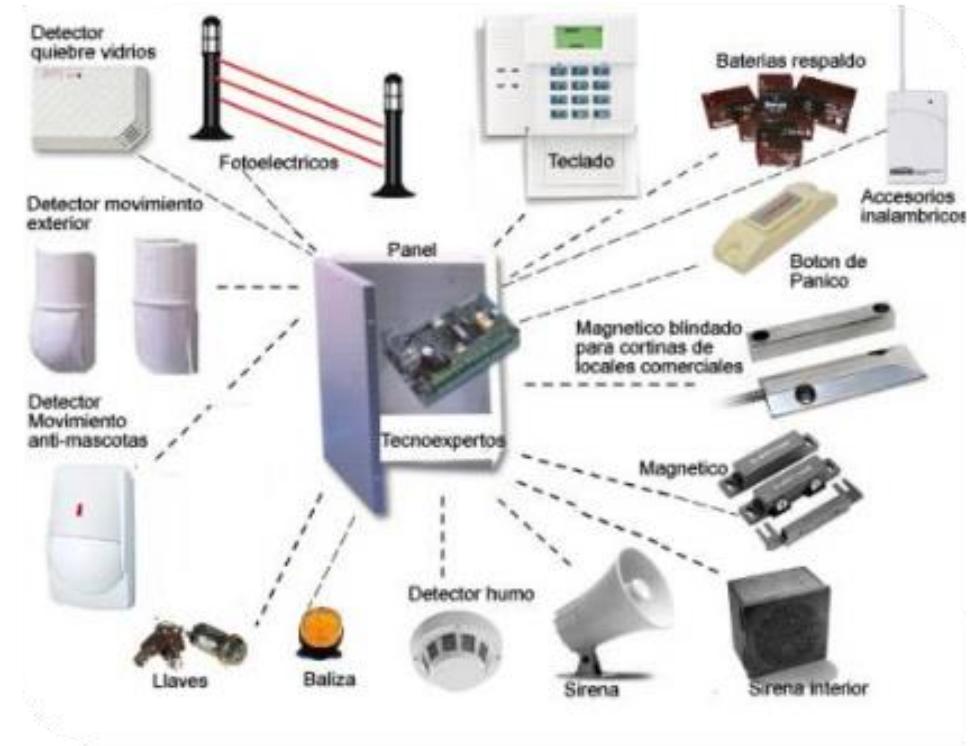
- CCTV
- SISTEMAS CONTRA INTRUSOS
- MANTRAMP Y MOLINETES

CCTV, Circuito cerrado de televisión (CCTV) es un dispositivo investigador utilizado para ayudar, a los guardias o personal de seguridad física, en la detección de presencia de intrusos en áreas restringidas. CCTV utiliza el espectro de luz normal y requieren una luminosidad suficiente en el campo de visibilidad de las cámaras. Con características infrarrojos pueden "ver en la oscuridad", mostrando el calor. Los videos se almacenan en un dispositivo DVR (Digital Video Recorder) o en un NVR (Network Video Recorder)



CCTV

Son sistemas diseñados para proteger ambientes críticos, por el monitoreo de movimiento de los espacios, mediante sensores fotoeléctricos, infrarrojos y otros, así como la identificación de aperturas no autorizadas de puertas y ventanas, a través de contactos magnéticos, y lanzamiento de alertas ante el inicio de posibles incendios detectados por los sensores de humo.



SISTEMA CONTRA INTRUSOS



- Las trampas para hombres son controles preventivos físicos consiste un pasillo entre dos puertas, cada una de las cuales por lo general requiere un forma separada de autentificación para ser abiertas, con el objetivo de que un intruso se encuentre atrapado entre las dos puertas.
- Los molinetes o torniquetes están diseñados para forzar la regla de una persona por autentificación, ambos medidas evitan intrusiones del tipo piggybacking.

MANTRAP Y MOLINETES

PROTECCIÓN Y VIGILANCIA PRESENCIAL

La protección y vigilancia presencial, es un mecanismo de protección para los empleados y recursos informáticos contra, robos asaltos, sabotajes y accesos de personas no autorizados:

- POLICÍAS
- SEGURIDAD PRIVADA
- RECEPCIONISTAS Y CUSTODIOS

CONTROLES DE ACCESO FÍSICO

**Policías, seguridad privada
y custodios**



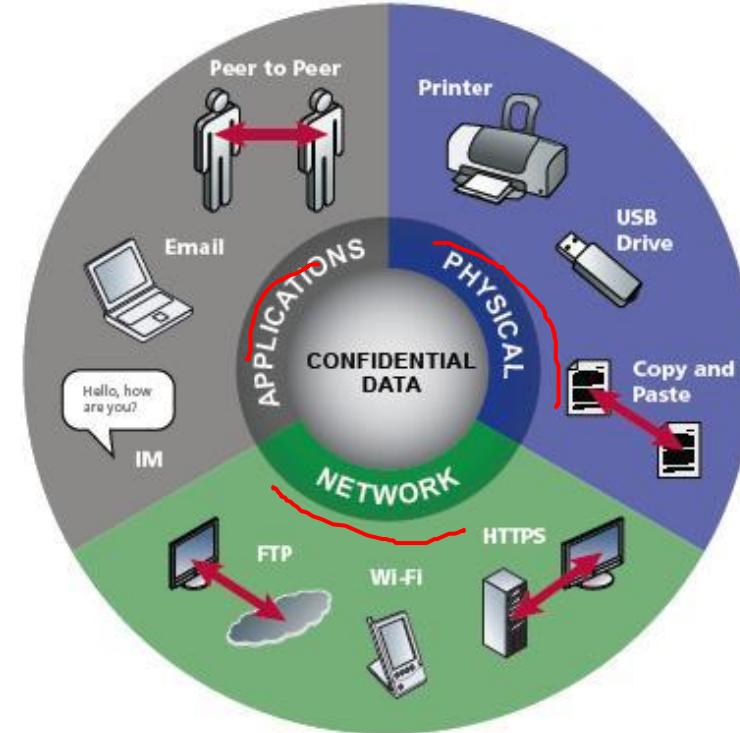
Recepcionistas de lobby

SEGURIDAD FÍSICA DE MEDIOS

La seguridad física de medios de almacenamiento es una de las últimas líneas de defensa en una estrategia de protección en profundidad, en este aspecto tenemos:

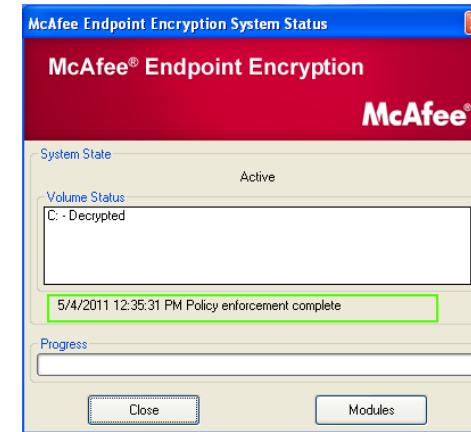
- DLPS
- CIFRADO DE DISPOSITIVOS
- SEGURIDAD DE LOS BACKUP
- LIMPIEZA Y DESTRUCCIÓN DE MEDIOS
- DESTRUCCIÓN DE MEDIOS FÍSICOS

Control de puertos (Interfaces removibles), las computadoras modernas pueden contener varios "puertos" por ejemplo USB, pueden permitir copia de datos desde un sistema. Este tipo de puertos pueden ser discapacitados físicamente; como ejemplo la desactivación de un puerto en la placa base de un sistema, desconectando los cables internos que conectan al puerto, y obstruir físicamente el propio puerto. Los puertos también pueden ser bloqueados por electrónica a través de la directivas del hardware que realizan los sistemas del tipo DLPS.



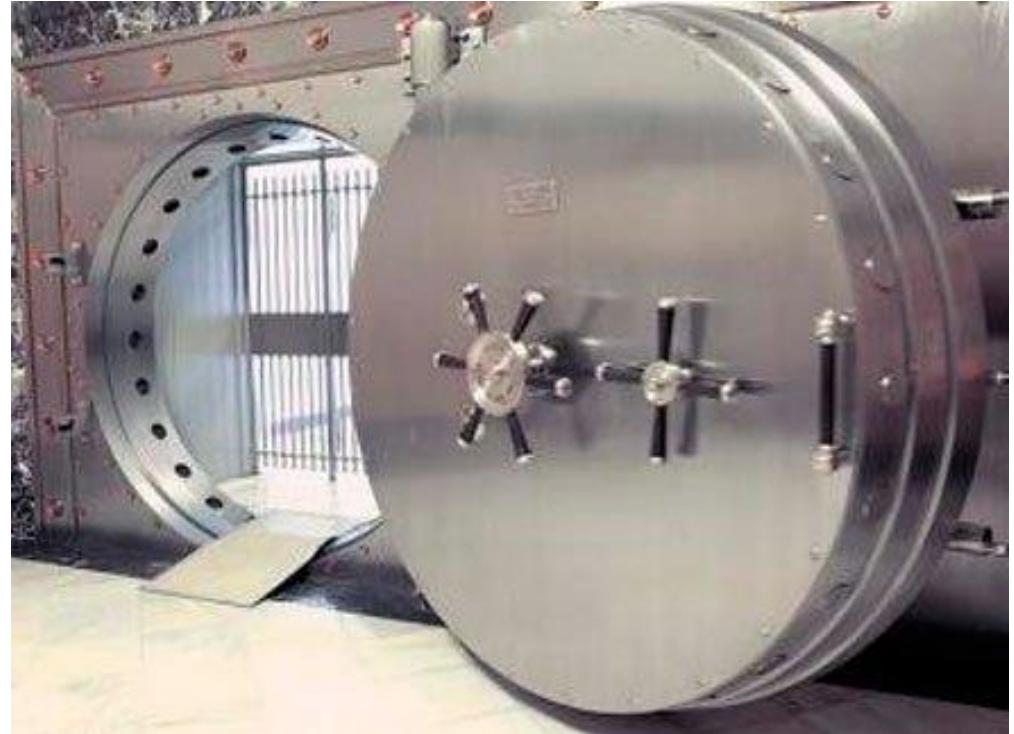
DATA LOSS PREVENTION SYSTEM (DLPS)

Cifrado de Dispositivos y Cintas, el cifrado de dispositivos de almacenamiento y cintas protegen los datos en reposo, y es uno de los pocos controles que protegen los datos después de que las medidas de seguridad física fallaron, es altamente recomendable cifrar completamente los discos o dispositivos de almacenamiento transportables.



CIFRADO DE DISPOSITIVOS

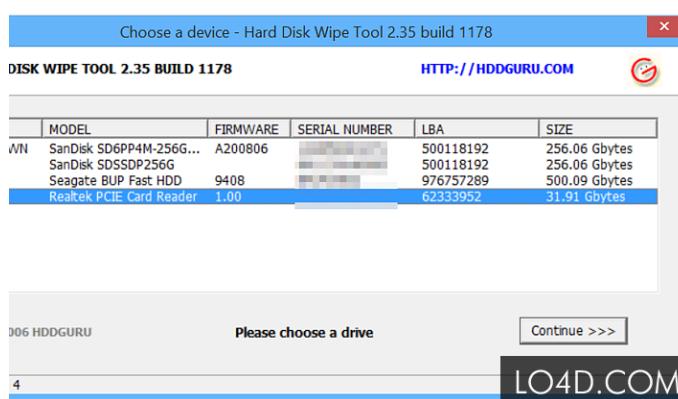
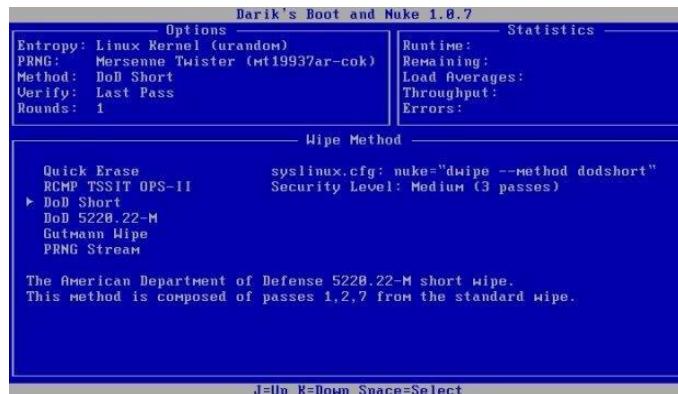
**Almacenamiento y Transporte de Medios,
Todos las copias de seguridad (backups)
sensibles deben ser almacenados fuera del
sitio, ya sea transmitida a través de rede o
movidas físicamente hacia otro sitio
alterno de resguardo seguro. Se deben
seguir procedimientos estrictos para la
utilización de sitios alternos.**



SEGURIDAD DE LOS BACKUP



Limpieza y Destrucción de Medios, Los distintos tipos de Medios de Almacenamiento deben ser limpiados de forma segura (wipe) o destruidos para evitar la recuperación no autorizada de datos, cuando se los quiera reutilizar o se los deseche como basura respectivamente.



LIMPIEZA Y DESTRUCCIÓN DE MEDIOS

Coartadores de papel, la documentación física puede contener información muy sensible o valiosa de la organización, por lo que es importante su destrucción, idealmente por cortadoras del tipo triturador, que realizan cortes cruzados dejando el papel como confeti.



6. DESTRUCCIÓN DE MEDIOS FÍSICOS

SEGURIDAD DEL DATACENTER

El DATACENTER es el corazón de la organización, si deja de funcionar o para su operación, las consecuencias pueden ser catastróficas, por tal motivo la seguridad física es muy importante evitar posibles amenazas, los principales aspectos a considerar son:

- UBICACIÓN
- CLIMATIZACIÓN
- ENERGÍA DE RESPALDO
- PROTECCIÓN CONTRA INCENDIOS
- PROTECCIÓN CONTRA FILTRADO DE AGUA
- ACCESO FÍSICO
- PAREDES, TECHO Y SUELO
- ARQUITECTURA
- ANSI/TIA 942
- TIPOS DE DATACENTER DE CONTINGENCIA



Zonas que no cuenten con historial de terremotos, inundaciones o hayan sido afectados por incendios forestales.



UBICACIÓN DEL DATACENTER

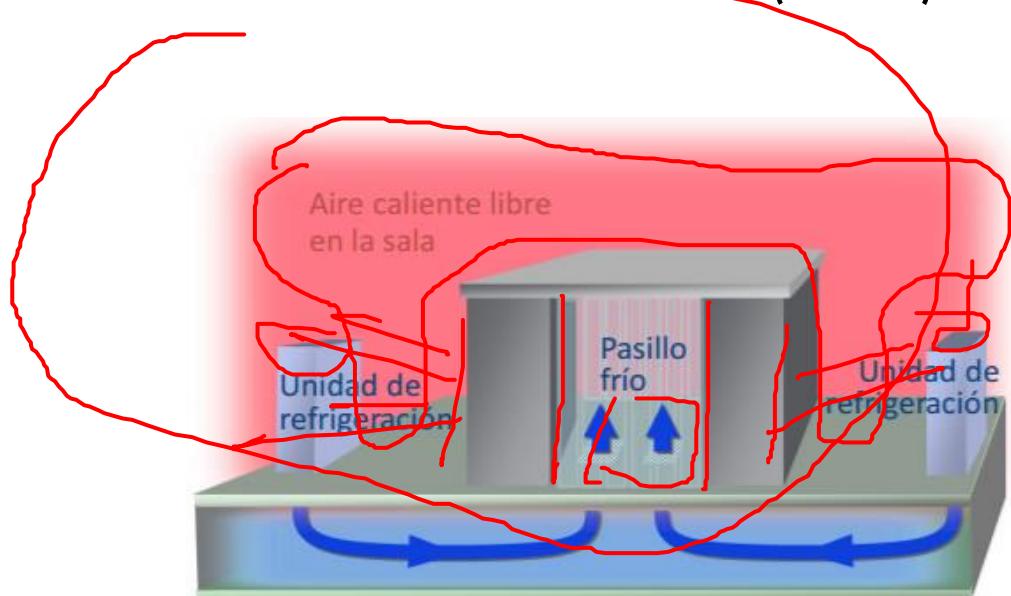


No encontrarse cerca de fuentes de interferencias electromagnéticas, tales como transformadores, motores generadores, equipamiento de rayos X, radares, etc.

UBICACIÓN DEL DATACENTER

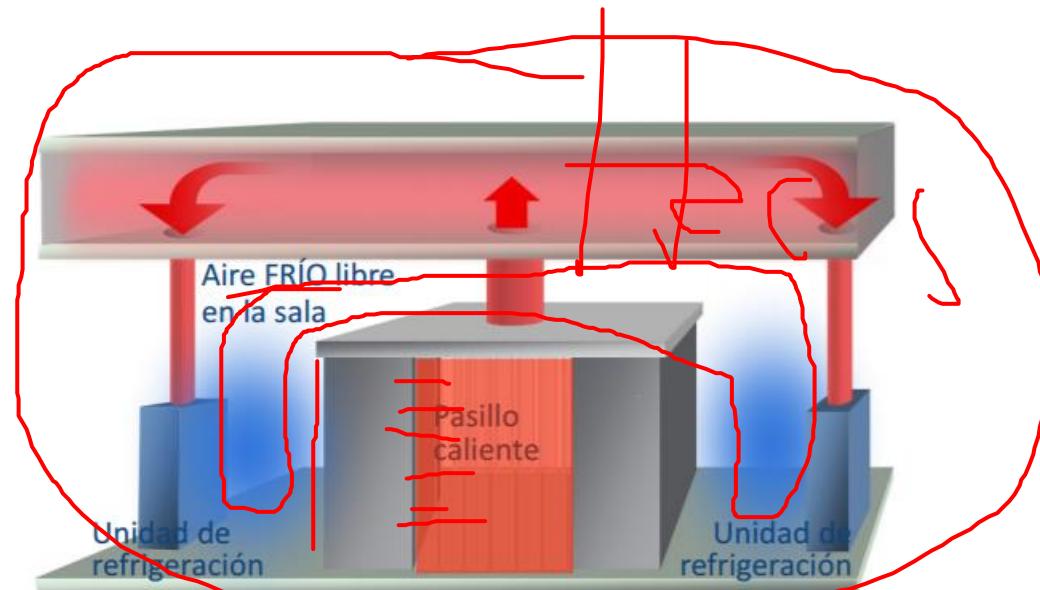
CLIMATIZACIÓN DEL DATACENTER

Contención de aire caliente (HACS) puede ahorrar hasta 43% la Efectividad del Uso de la Energía (PUE) que los sistemas de contención de aire frio (CACS).



Sistema de contención de pasillo frío (CACS)
Cold Aisle Containment System

Hasta 43% (Power Usage Effectiveness PUE)



Sistema de contención de pasillo caliente (HACS)
Hot Aisle Containment System

CLIMATIZACIÓN DEL DATACENTER

Debe tener un sistema dedicado de Calefacción, Ventilación y Aire Acondicionado (HVAC - Heating, Ventilating and Air Conditioning), o en su caso estar conectado al sistema principal HVAC del edificio (no recomendado), el HVAC debe operar las 24 horas/día los 365 días/año proporcionando los niveles adecuados de climatización requeridos interior, por lo que debería estar conectado al sistema de generación de energía de respaldo.

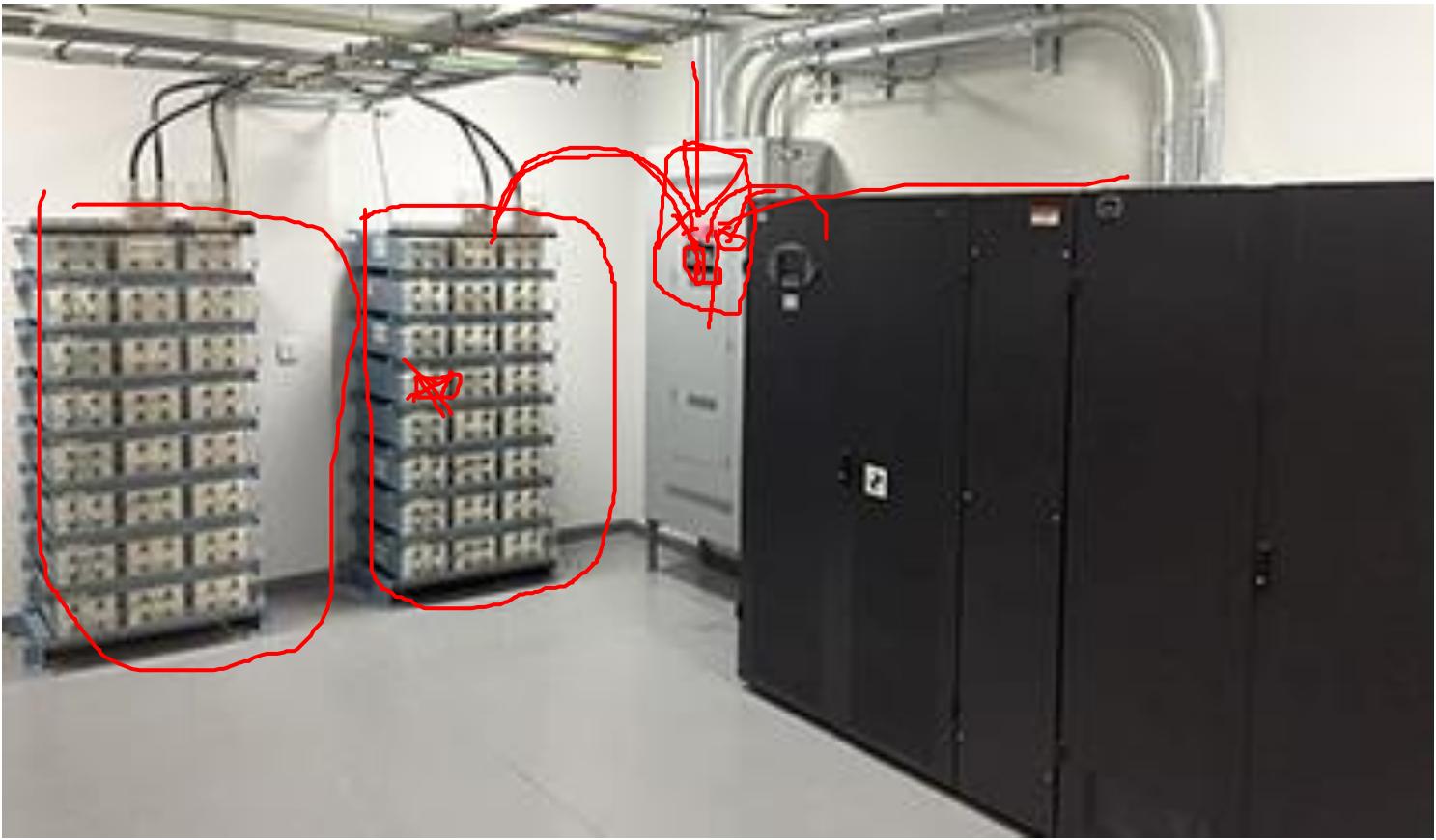


CLIMATIZACIÓN DEL DATACENTER

La temperatura y la humedad deben ser controladas mediante sensores de temperatura y humedad relativa, para proporcionar los rangos de operación continua recomendados:

- Temperatura: 20°C a 25°C
- Humedad relativa: 40% a 55%
- Máximo punto de condensación: 21°C
- Máxima tasa de cambio: 5°C por hora

Las vibraciones mecánicas pueden afectar a los equipos de procesamiento o a la infraestructura del cableado, facilitando fallas de estos servicios a través del tiempo, esto debe ser considerado en el diseño e implementación del cuarto de cómputo, debido a que existe absorción de vibración de las construcciones sobre todo en edificios altos o debido a equipos mecánicos/electrónicos cercanos que generan vibración como grupos generadores, sistemas HVAC, etc.



ENERGÍA DE RESPALDO DEL DATACENTER

Debe existir paneles eléctricos o unidades de distribución de energía (PDUs - Power Distribution Units) independientes conectados a circuitos eléctricos separados que alimenten el cuarto de cómputo. Las salidas de conveniencia (para la conexión de equipos de limpieza y/o mantenimiento) no deben ser alimentadas mediante los paneles eléctricos o PDUs que son usados por el equipamiento de computación o telecomunicaciones del Datacenter.



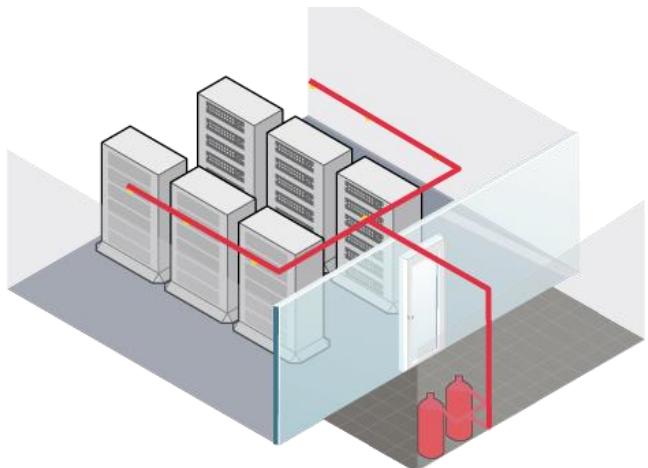
Los paneles eléctricos deben estar soportados por el sistema de generación de energía de respaldo.
El sistema eléctrico debe estar soportado por el sistema de aterramiento o puesta a tierra adecuado.



ENERGÍA DE RESPALDO DEL DATACENTER



Se debe prever un sistema de detección y protección contra incendios, así como extintores portátiles adecuados para las características electro/mecánicas del equipamiento contenido en el Centro de Datos.



PROTECCIÓN CONTRA INCENDIOS

PROTECCIÓN CONTRA FILTRACIONES DE AGUA

Donde existe un riesgo de ingreso de agua, debe ser proporcionado un medio para su evacuación de los espacios utilizados por el Datacenter (como ejemplo un drenaje por el suelo). Adicionalmente, al menos un drenaje u otro medio de evacuación de agua por cada 100 m² de área deben ser proporcionados. Todas las tuberías de agua y drenaje que corren a través del Centro de Datos deben ser ubicadas lejos y no de forma directa sobre el equipamiento de procesamiento en esta área.



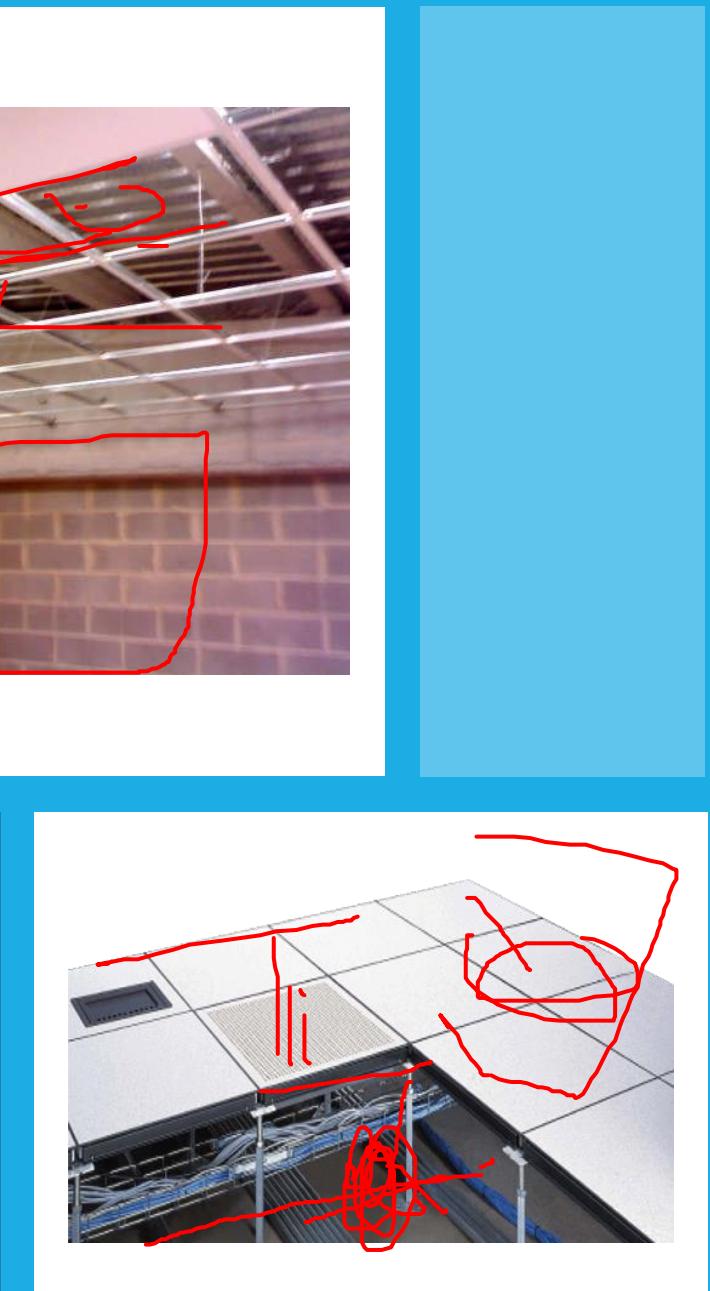
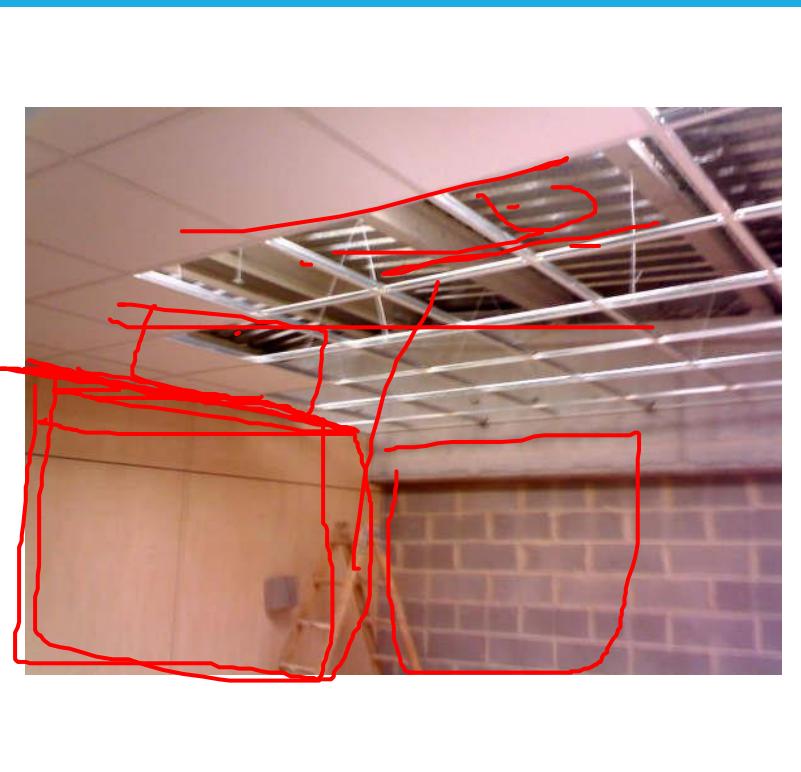
La puertas de acceso deben proporcionar sólo el ingreso a personal autorizado, por lo que se debe incluir mecanismos de doble factor de autentificación, en el sistema control de acceso físico.



ACCESO FÍSICO AL DATACENTER

PAREDES, SUELOS Y TECHOS DEL DATACENTER

Las paredes alrededor de cualquier perímetro interno de seguridad, como un Datacenter deben ser construidos desde "losa a losa", lo que significa que deben comenzar en la losa del suelo y recorrer hasta la losa del techo. Para que un intruso no sea capaz de pasar por debajo de una pared que comience desde el piso técnico (piso elevado), o trepar por una pared que concluye en el techo falso.



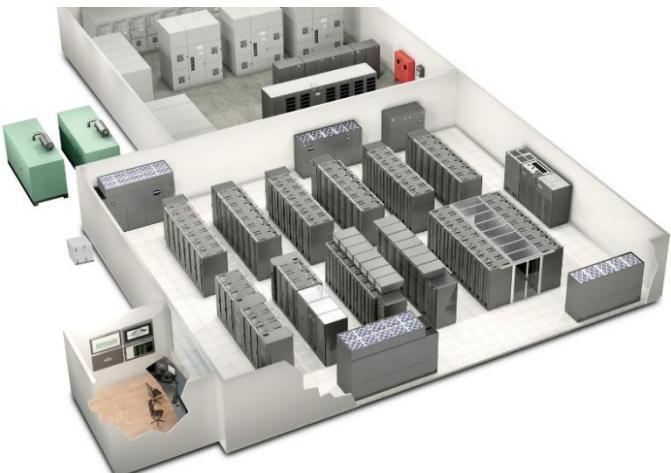
ARQUITECTURA DEL DATACENTER

Que no tengan ventanas en sus muros perimetrales, para evitar accesos no autorizados o influenciar en la carga calórica en su interior.





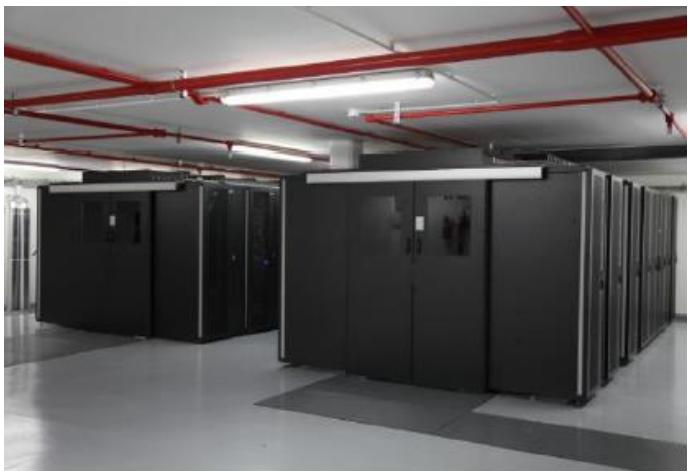
Debe tener el tamaño adecuado para soportar el equipamiento actual más un posible crecimiento futuro, los equipos tales como distribuidores de energía o sistemas de acondicionamiento y UPS de hasta 100 kVA son permitidos en su interior, exceptuando baterías de célula de plomo, UPS de más de 100 kVA deberían estar ubicadas en un cuarto separado.



ARQUITECTURA DEL DATACENTER



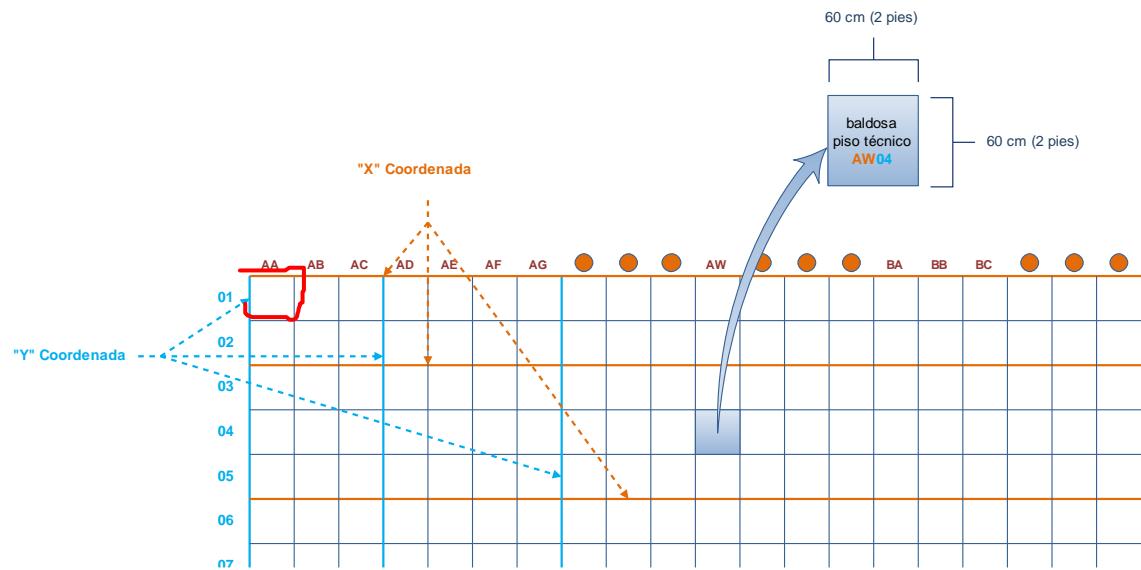
La altura mínima del cuarto de cómputo debe ser de 2.6 m desde el piso terminando a cualquier obstáculo, como aspersores, dispositivos de iluminación o cámaras, los requerimientos de refrigeración o gabinetes (racks) más altos 2.13 m pueden requerir mayor altura en los techos.



ARQUITECTURA DEL DATACENTER

ARQUITECTURA DEL DATACENTER

Los pisos, paredes y techos deben tener un sellador, pintura o de un material que minimice el polvo y aislé la humedad, el piso técnico debe tener propiedades antiestáticas (IEC 61000-4-2) y deben soportar la carga distribuida y concentrada del equipamiento (mínima 7.2 kPa = 150 lbf/ft² o 854.42 kgf/m² recomendada 12kPa =250 lbf/ft² o 1220.60 kgf/m²).



Finalmente la arquitectura debe prever riesgos sísmicos, de inundaciones, convulsiones sociales, incendios y otros que puedan afectar la continuidad de sus operaciones, si se usa señalización, debe ser desarrollada dentro del plan de seguridad del edificio.



ARQUITECTURA DEL DATACENTER

TIER I

- DC BÁSICO: Es frecuente la interrupción de la disponibilidad del DC por factores externos, debido a que no cuenta con generadores eléctricos o sistemas de climatización redundantes. Una vez al año o cuando sea necesario, el DC no estará disponible, por la realización de tareas de mantenimiento. Disponibilidad promedio de **99,67%**.

TIER II

- DC REDUNDANTE: Tiene caídas menos frecuentes porque cuenta con una fuente alternativa de energía y una infraestructura de climatización n+1. Pueden realizarse algunas tareas de mantenimiento sin tener que dejar el DC fuera de línea. Su disponibilidad es del **99,74%**.

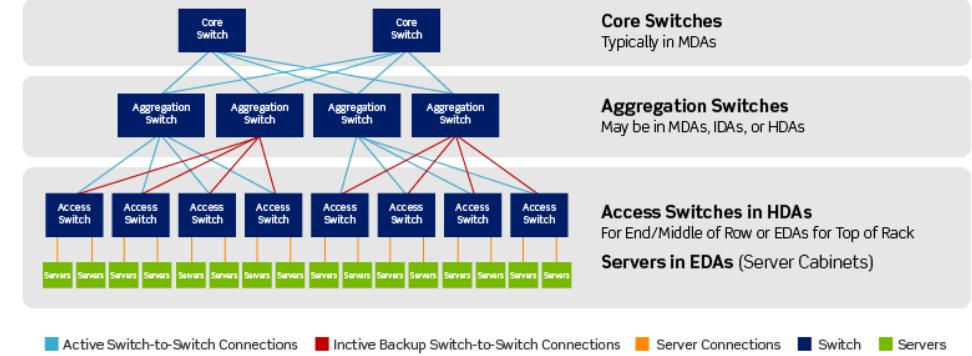
TIER III

- DC CONCURRENTEMENTE MANTENIBLE: Cuenta con una tolerancia a fallos mayor porque posee fuentes de energía alternativas y climatización redundante 2n (activo/pasivo). El mantenimiento puede realizarse sin ningún tipo de interrupción del servicio. Tier III incluye también la posibilidad de avanzar hacia tier IV sin interrumpir el servicio. Tiene una disponibilidad del **99,98%**.

TIER IV

- DC TOLERANTE A FALLOS: Tiene múltiples elementos redundantes 2(n+1) en electricidad y climatización lo que le permite soportar situaciones críticas sin dejar el DC offline. El mantenimiento se realiza sin afectar el funcionamiento del DC aún en situaciones de emergencia. Su disponibilidad es del **99,99%**.

ANSI/TIA-942-A-1: THREE-TIER ARCHITECTURE



ANSI/TIA 942 NIVELES DE DATACENTER

Redundant

- Sitio con las mismas capacidades y configuraciones del primario.
- Recibe las copias de respaldo en tiempo real.
- Más caro, los usuarios no sufren ninguna disminución en disponibilidad de datos.

Hot

- Equipado con facilidades de energía, climatización y comunicación.
- Equipamiento tecnológico completamente configurado, donde las operaciones pueden reubicarse después de un desastre.
- Se reanudan las operaciones en tiempos hasta 1 hora.

Warm

- Equipado con facilidades de energía, climatización, comunicación y equipamiento.
- Las operaciones inician después de restaurar las copias de seguridad de los datos del sitio original, esta restauración puede ser superior al día.



TIPOS DATACENTER ANTE CONTINGENCIAS



- Se cuenta con la estructura del sitio, facilidades de energía y comunicaciones.
- Requiere la compra del equipamiento tecnológico necesario.
- Debe configurarse el equipamiento y recurrir a los últimos respaldos disponibles, su operación puede tardar arriba de una semana.

- Infraestructura de un proveedor de servicios en la nube.
- Instalación de los SO, base de datos, sistemas y servicios.
- Requiere el suministro de las copias de respaldo de las configuraciones de los servidores, servicios y datos.



TIPOS DATACENTER ANTE CONTINGENCIAS

PLAN DE CONTINGENCIA

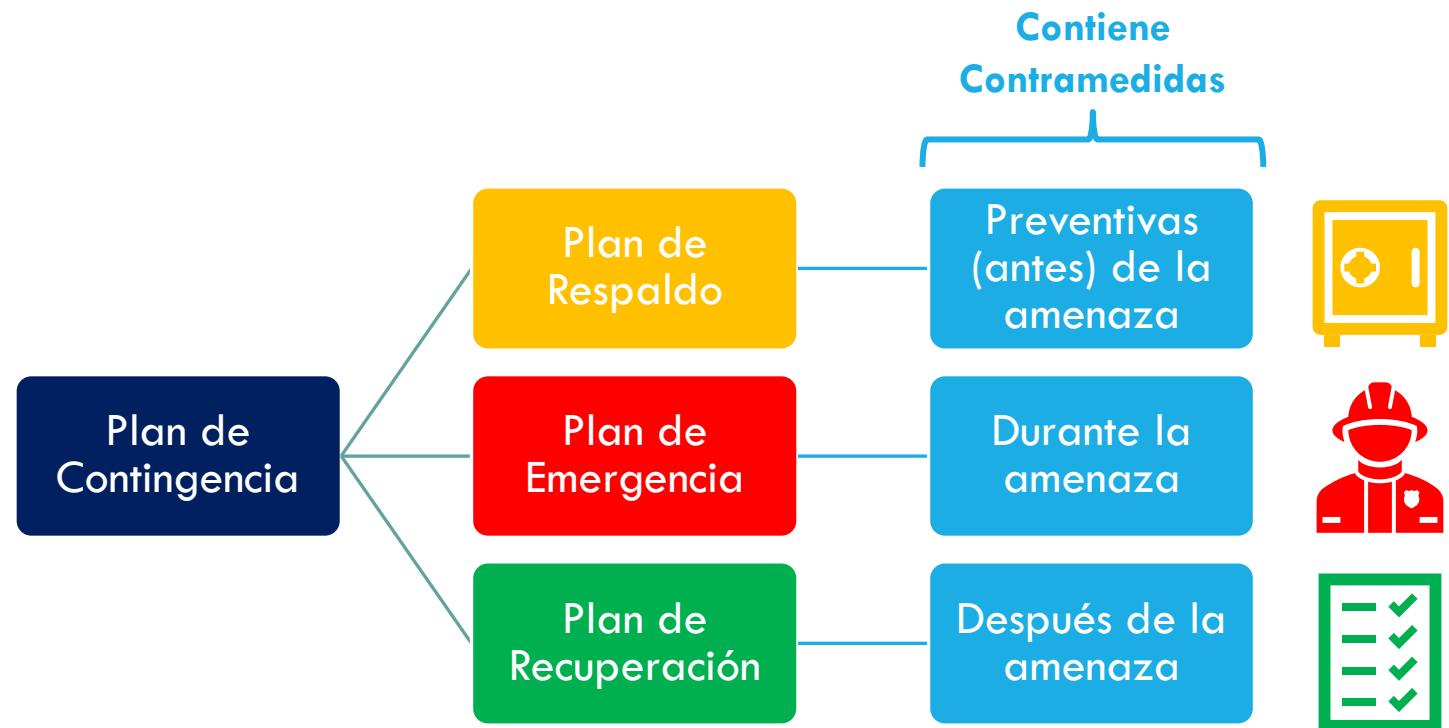
Los planes de contingencia, contienen las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio derivadas de las operaciones informáticas en una empresa, están conformados por:

- PLAN DE RESPALDO
- PLAN DE EMERGENCIA
- PLAN DE RECUPERACIÓN

PLAN DE CONTINGENCIA

Un plan de contingencias es un caso particular del **plan de continuidad del negocio** aplicado a las áreas de informática, sistemas o tecnologías.

Otras áreas pueden tener planes de continuidad que persiguen el mismo objetivo desde otro punto de vista. No obstante, dada la importancia de la utilización de las tecnologías de la información en las organizaciones modernas, el plan de contingencia es el más relevante.



PLAN DE CONTINGENCIA

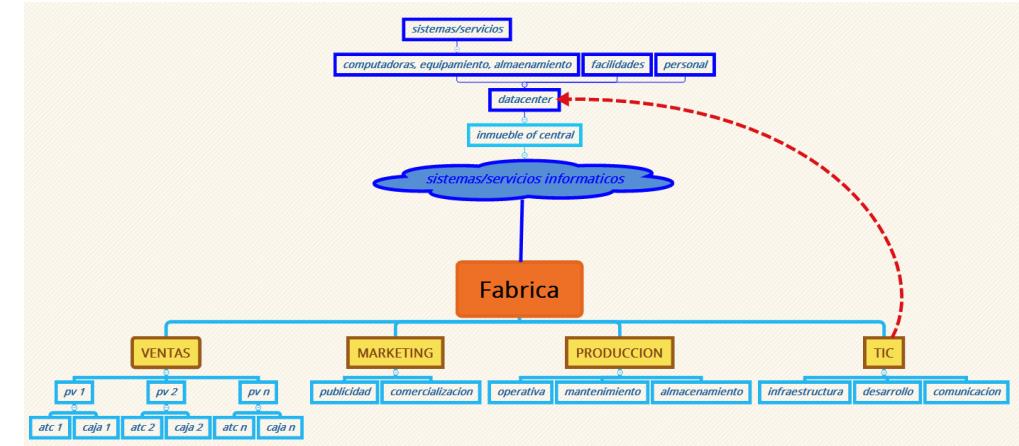
El plan de contingencia, debe definir claramente los recursos necesarios y las responsabilidades en su utilización.



Supongamos una pequeña compañía que se dedica a la fabricación

Una amenaza de incendio en la oficina central, podría llegar a afectar al proceso de negocio dedicado a la venta.

Activos e interdependencias: Oficinas centrales → Datacenter → Computadoras y almacenamiento → Información de pedidos y facturación → Proceso de negocio de ventas → Imagen corporativa



EJEMPLO DE PLAN DE CONTINGENCIA

EJEMPLO DE PLAN DE CONTINGENCIA

Amenaza: Incendio. (los activos afectados son los anteriores y los futuros).

Impacto:

- Perdida de un 10% de clientes.
- Imposibilidad de facturar durante un mes.
- Imposibilidad de admitir pedidos durante un mes.
- Reconstrucción manual de pedidos y facturas a partir de otras fuentes.
- Sanciones por accidente laboral.
- Inversiones en equipamiento y mobiliario.
- Rehabilitación del local.

Riesgo: Posible afectación del proceso de negocio dedicado a la venta.

El plan de contingencias podría contener las siguientes contramedidas:

Medidas físicas y técnicas:

- Extintores contra incendios.
- Detectores de humo.
- Salidas de emergencia.
- Equipos informáticos de respaldo.

Medidas organizativas:

- Seguro de incendios.
- Precontrato de alquiler de equipos informáticos y ubicación alternativa.
- Procedimiento de copia de respaldo.
- Procedimiento de actuación en caso de incendio.
- Contratación de un servicio de auditoría de riesgos laborales.

Medidas humanas:

- Formación para actuar en caso de incendio.
- Designación de un responsable de sala.
- Asignación de roles y responsabilidades para la copia de respaldo.



Plan de respaldo:

- Revisión de extintores.
- Simulacros de incendio.
- Realización de copias de respaldo.
- Custodia de las copias de respaldo (por ejemplo, en la caja fuerte de un banco).
- Revisión de las copias de respaldo.



Plan de emergencia:

- Activación del precontrato de alquiler de equipos informáticos.
- Restauración de las copias de respaldo.
- Reanudación de la actividad.



Plan de recuperación:

- Evaluación de daños.
- Traslado de datos desde la ubicación de emergencia a la habitual.
- Reanudación de la actividad.
- Desactivación del precontrato de alquiler.
- Reclamaciones a la compañía de seguros.

EJEMPLO DE PLAN DE CONTINGENCIA

CONSULTAS O DUDAS?

Este material es facilitado con fines didácticos solo a los estudiantes que cursan alguna asignatura con el autor, su distribución o comercialización sin autorización esta prohibido.

Ing. Alvaro Antezana © 2021



tj.alvaro.antezana.m@upds.net.bo



+591 69304565