SEGURIDAD DE CABLEADO Y DATA CENTER

Unidad 1

Seguridad de Redes del Data center

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

Realizan preparación de esquema de rack de comunicaciones, considerando su seguridad y vulnerabilidad.

Fuente: Freepik. (s/f)

Introducción

¿En qué se diferencia una seguridad activo-pasivo con seguridad físico - lógica?

En un sistema informático así como en los dispositivos que lo sostienen, existen amenazas cuyas circunstancias irán cambiando en cada uno de los centros de datos establecidos, no existe una norma que unifique los diferentes incidencias que atañen a los data center desde un desastre natural como inundaciones, incendios accidentales, tormentas, temperaturas extremas, terremotos que al final conllevan consecuencias devastadoras; asimismo se presentan amenazas ocasionadas por el hombre como pueden ser disturbios, sabotajes internos o externos en forma deliberada, etc.

Para ello las organizaciones deben implementar una política de seguridad y si es basada en una seguridad física que es la aplicación de barreras y contenciones físicas y procedimientos de control, como medidas de prevención y contramedidas de amenazas a los recursos de información confidencial. El buen estudio de la tecnología y su infraestructura que se instala en un edificio y el análisis del entorno físico, son dos partes fundamentales para que soporten las aplicaciones o sistemas de *hardware* o *software* todo con el objetivo de minimizar los riesgos y poder darle continuidad de operaciones en la empresa.

Las medidas de detección que se recomiendan son mantener los ordenadores actualizados y seguras físicamente. Tener personal capaz de manejar contenciones de seguridad. Los administradores de red deben configurar en forma adecuada la red; mantenerse informados constantemente sobre cada una de las vulnerabilidades, control de acceso, las restricciones se acceso a las redes sistemas, aplicaciones, funciones, edificio y datos.

Cuando se indica el estudio de un entorno físico establecemos sin saberlo un análisis de riesgo esto si lo debemos aplicar bajo un tipo de norma o estándar se debe realizar un levantamiento de datos que lleve a tomar decisiones que den como resultado la ubicación del *hardware*, dispositivos de red, centros de cómputo, etc. En este tipo de estudio se revisa la ubicación del edificio, acceso físico de personas, la interconexión de cableado de datos y la conexión eléctrica, controles de temperatura interna o externa, condiciones climáticas los tipos de disposición de equipos o del *hardware*, y los métodos de administración de acceso a los sistemas de *hardware*.

1. Barreras físicas, controles y mecanismos de seguridad dentro y alrededor del rack

En la actualidad establecido la instauración del *software* y la conectividad, la seguridad de la información solo se establece como debate el control de los virus y otro tipo de ataques el uso de *firewalls* y otras alternativas de contención contra las fugas de la información sensible. De lado queda la seguridad física de las instalaciones y de los equipos reconocer esta área ayuda a reconsiderar al área física del data center como una vulnerabilidad y es tarea de todos considerar la integridad física de la infraestructura para así garantizar la disponibilidad segura de la información

Para ello se establecerán una serie de recomendaciones generales para proteger el área de seguridad más inmediata que rodea a los equipos en un centro de datos.

1.1. Clasifique el tamaño y la capacidad de almacenaje del Rack

Significa que se debe considerar durante la construcción cumpla las normas de calidad de fabricación, los estándares, así como el soporte de almacenaje de carga, con el fin de que se ajuste a las necesidades específicas según el tamaño del centro de datos. Se debe considerar los espacios para las maniobras de transporte y colocación. Ya que, mientras mayor sea el tamaño del rack, más compleja será la de instalar nuevos equipos a futuro.

1.2. Siempre piensa en la comodidad y adaptabilidad

Hay que considerar que los gabinetes cuenten con un diseño que cumpla con las expectativas que faciliten la conexión y el montaje de dispositivos de cualquier unidad (servidores, *switches*, router y UPS de cualquier dimensión, inclusive se debe considerar espacio para las baterías adicionales) deben instalarse de forma que permitan un reordenamiento a futuro. Así la escalabilidad será rápida. Deben, incorporar rieles de montaje ajustables para facilitar la instalación. Adicionalmente los paneles laterales deberán ser desmontables.

1.3. Restrinja el acceso e identifique claramente al personal autorizado

En una política firme de seguridad para un centro de datos es importante establecer y restringir el acceso a la mayor cantidad de personas, así se reducen posibles vulnerabilidades. Algunos racks deberán contar con cerraduras especiales de seguridad. También, si es posible, considerar el uso de gabinetes con dispositivos adicionales como *software* de detección de apertura de puertas que envían una alarma al administrador.

1.4. Adopte procedimientos de optimización de flujo de aire en el rack, con el fin de obtener eficiencia de enfriamiento

Esta recomendación será cuando los espacios restringidos no permitan un flujo de aire adecuado. Para ello se establecerán ductos de aire forzado. Se debe tener en consideración que enfriar el frente del gabinete, es un error por cuanto solo se estaría recirculando el aire. Como solución se puede establecer la recirculación separando los racks lo más posible y adicionando ductos de aire para la salida del aire caliente. Con

esto lograríamos el enfriamiento óptimo de los equipos, un tiempo de vida útil mayor, costos menores en mantención, etc.

1.5. Se debe considerar la neutralidad del vendedor o proveedor de los equipos

Con objetivos comerciales de fidelización de los clientes algunos fabricantes producen gabinetes compatibles solamente con otros equipos de la misma marca, sin embargo, deben considerarse gabinetes que ofrezcan un arquitectura abierta y neutral que permita integrar fácilmente con otros racks y accesorios de otros proveedores.

1.6. Se debe permitir en la medida de lo posible, gabinetes optimizados para todas las funciones principales para las que fueron construidos

El enfriamiento, la optimización de distribución de cables, la correcta distribución de energía, monitoreo de servidores y equipos de redes son vitales para mantener operando un centro de datos

Un rack además debe ser la primera línea de defensa de una instalación de TI contra riesgos de la seguridad física, ya que se puede ver afectado el rendimiento de los equipos en su interior si no cuenta con las condiciones adecuadas. Al escoger el modelo perfecto para tu centro de datos se deben tener en cuenta las consideraciones expuestas anteriormente.

1.6.1 Riesgos de seguridad en los centros de datos

Lo que conocemos actualmente con relación a la seguridad lógica es por mucho conocido. Sin embargo, hay otro factor como es el de la seguridad física del data center. No disponer de una seguridad física completa lo vuelve vulnerable, por lo tanto,

la empresa desde un punto de vista podrá hacer grandes inversiones de *firewall*, antivirus, programas *antimalware*, pero sin una visión holística siempre tendrá dificultades en un ataque o un imprevisto.

No importa la dimensión del data center o de la empresa ya que todo está en riesgo de ser vulnerable.

Con relación a las vulnerabilidades físicas hay que tener los siguientes riesgos en que está expuesto el data center.

- Subida o caída de tensión.
- Temperaturas incorrectas o fallos de los equipos de climatización o un mal diseño.
- Incendios.
- Inundaciones y humedad.
- Humo, polvo y partículas en el aire que dañan los discos duros.
- Humo y polvo que dañan los ventiladores de los dispositivos.
- Accesos de personal sin autorización.
- Manipulaciones incorrectas de los equipos.
- Vandalismo, robo, etc.
- Movimientos sísmicos e inundaciones.

1.6.2 Normas y medidas de Seguridad

Para poder diseñar y ejecutar un data center seguro se deben de seguir los estándares previstos. Para ello considérese la norma EN50600 en las que se establecen el diseño para la disponibilidad, seguridad y eficiencia energética para toda la vida útil de los centros de datos.

Se tiene previsto como lo indica el estándar, un Análisis de Riesgo que se debe ir actualizando periódicamente, ya que al acceder a nuevos dispositivos traerán como consecuencia nuevas vulnerabilidades.

Para evitar los riesgos, se debe considerar una infraestructura completamente adecuada a la necesidad de cada cliente. Por ello es importante sostener un sistema eléctrico y de climatización optimizado con sistemas redundantes que garanticen la continuidad del servicio, pero además de la infraestructura eléctrica y de climatización o control de temperaturas hay que considerar otras amenazas.

Una de las claves del data center es su seguridad perimetral que debe garantizar una seguridad estructural contra cualquier amenaza del exterior como intrusiones inapropiadas, vandalismo, inundaciones, polvo, incendio, etc.

Los racks son el eje principal en la protección del data center. El cierre adecuado debe realizarse cumpliendo una serie de requisitos sean efectivos contra amenazas, evitando la penetración de sustancias contaminantes que puedan provocar interrupciones en la operación del data center (partículas, líquidos o gases). Para ello las puertas de acceso de todo nivel deben garantizar que al menos cumplen con la norma IP55, con relación a la resistencia del fuego y la protección contra incendios.

1.6.3 Mecanismos de seguridad dentro y alrededor del Rack

Dentro de los controles de accesibilidad que se deben implementar los más conocidos son:

Control de acceso para Racks

Ayuda a ahorrar costos, al eliminar la necesidad de control del punto de red y punto de alimentación individual para cada rack. Implementando una arquitectura de comunicación sofisticada, se distribuyen las señales y energía eléctrica de un único controlador a un número determinado de racks, así ofrece múltiples opciones de autenticación en cada gabinete o en una fila completa.

Ventajas

- Mantiene la seguridad de los activos del data center.
- Gestionado a través de SQL.
- Permite el seguimiento y la auditoria.
- Bloqueo del sistema en un solo clic.
- Limita el tiempo de acceso.
- Cierre de puertas con huella dactilar.
- Seguridad contra manipulaciones.
- Detección de puerta forzada.
- Bloqueo de Rack digital.
- Mediante dispositivo especial diseñado para el control tanto mecánico como automático de la cerradura.

Las ventajas más considerables son:

- Cerradura inteligente sin batería y sin cables para racks.
- Sensor integrado de puertas y pestillo para confirmación de bloqueo.
- Compatible para auditoría y seguimiento de actividad.
- Opción de operar en modo *Live Access*.
- No requiere conectividad por cable ni controlador adicional.
- Cerradura mecánica existente fácil de instalar.

Smart Locks:

Son cierres inteligentes para puertas correderas, batientes y cajones del centro de datos.

Existen una variedad de soluciones y tipos, las más importantes las detallaremos a continuación:

- **Cerradura mecánica:** cerradura con cierre automático que se integra a la perfección en armarios o cajones nuevos existentes.
  - ✓ Perfecta integración.
  - ✓ Cierre automático.
  - ✓ Pestillo antigolpes.
- **Cerradura *Cam Lock*:** con cierre mecánico que se integra a cualquier material.
  - ✓ Se puede montar en madera o vidrio, metal o acrílico.
  - ✓ Brazo de leva antirretroceso evita robos.

- ✓ Accesibilidad rápida.

- **Cerradura *Drawer Lock*:** diseño para cajones extraíbles.
  - ✓ Uso en paneles simples o dobles.
  - ✓ Diseñados para cajones extraíbles.
  - ✓ Instalación sencilla.

2. Medios de acceso remoto al rack y desde el mismo, durante la gestión

La gestión de un data center por vía remota se está volviendo una forma práctica de control que está soportado en nuevas tecnologías que actualmente se han creado para este fin. Hace ya un tiempo este tipo de conceptos debe ser muy importante por cuanto algunos centros de datos se encuentran en ubicaciones apartadas y es más rápido y económico solucionar problemas de forma remota.

En la práctica es posible ejecutar un data center sin actividad de personal, a esto se le conoce como “luces apagadas”. En la realidad se presentan dificultades para llegar a este tipo de prácticas que están basadas en infraestructura remota. Hay que considerar por un lado las herramientas para proporcionar controles remotos son difíciles de integrar. Por otro lado, los clientes o los propietarios son reacios en confiar en los sistemas remotos, prefiriendo establecer servicio físico y otros equipos directamente.

La coyuntura actual de la pandemia ha obligado a un cambio radical desde la perspectiva de administración y trabajo remoto, lo que ha permitido dar un paso muy importante en el desarrollo de soluciones tecnológicas que lo faciliten. Para ello se deben seguir algunos lineamientos que se describen a continuación.

2.1. Monitoree y Mida la energía

“No se puede administrar lo que no se mide”

Este principio es importante ya que el crecimiento de los paquetes de datos se ha traducido en el desafío de poder administrar el uso eficiente de la energía en un data center.

Para ello se han desarrollado PDU inteligentes para los racks a nivel de entrada y salida del disyuntor.

La medición de la corriente de entrada es importante ya que, determinando el uso de energía del rack se puede relacionar con la disponibilidad de esta. La medición en el tomacorriente puede ayudar a comprender el gasto de energía en horas que el consumo de datos es mayor, así de tal forma, se puede administrar la energía en ciertos momentos donde el consumo es mayor. Optimizando el uso de la energía se traducirá en el abaratamiento de costos, ahorrando energía y dinero.

Los PDU inteligentes ofrecen monitoreo de energía remoto granular de corriente (amperios), voltaje, potencia en kW, factor de potencia y consumo de energía en (kWh) con una precisión de +/-1% brindando información más crítica para ayudar que el centro de datos se mantenga estable y eficiente.

2.2. Identificación de servidores infrautilizados o inactivos

Afortunadamente los PDU inteligentes con medición a nivel de salida determinan qué servidores están siendo infrautilizados o son ineficientes, de tal manera que con una evaluación es posible comprender mejor cómo un equipo activo específico consume energía a través de un análisis del uso de la energía (mediciones en el tiempo consumo y sobresaltos de energía en horas determinadas) con el fin de aminorar costos durante toda la operación. La localización y corrección de un servidor inactivo es más fácil cuando se combina la solución DCIM (Data Center *Infraestructura Managment*) con un PDU inteligentes para racks inteligentes.

2.3. Implementación de sensores ambientales en sus Racks

Se deben instalar en el rack y en el punto del servidor sensores de medición de temperatura, humedad, flujo de aire, vibración, humo, inundación, y presión de aire. Algunos PDU pueden tener sensores preinstalados, mientras que otros proporcionan sensores externos que pueden ser conectados al sistema. Otra idea es implementar una administración de sensores inteligentes completamente independiente, que proporcione los datos de forma centralizada.

Los sensores son dispositivos rentables y fáciles de instalar. Con ellos reducen los sobrecostos de energía, se mejora la confiabilidad y se aumenta la capacidad de rendimiento del data center. Esto permite establecer parámetros para un crecimiento futuro de la instalación. De esta forma los usos de sensores ambientales pueden optimizar el sistema del data center. El acoplamiento de sensores ambientales inteligentes responde a una demanda de eficiencia es por esto qué:

- Garantiza el tiempo de actividad monitoreando al rack en busca de posibles puntos calientes.
- Ahorra en enfriamiento elevando con confianza las temperaturas del centro de datos.
- Mantiene la seguridad del gabinete con sensores de cierre de contacto.
- Mejora la disponibilidad del centro de datos al recibir alertas ambientales.
- Facilita la toma de decisiones sobre el diseño y contención de enfriamiento.
- Establece umbrales y alertas para el monitoreo de instalaciones en el sitio de forma remota.

El conjunto de aplicación de tecnologías de control con el uso de sensores permite realizar un inventario preciso y automatizado y en tiempo real de todos los activos de TIU y sus ubicaciones integradas con el software DCIM.

2.4. Optimización de la gestión de flujo de aire en los gabinetes de los servidores

La gestión de refrigeración en un rack de servidor es un factor de importancia en el PUE (*Power Usage Effectiveness*) ya que refleja la eficiencia energética de un centro de datos. Con un PUE más bajo da como consecuencia un consumo de energía total más bajo del data center. Por lo tanto, es importante que minimizar la fugas para priorizar la recirculación así el aire frío se guía exclusivamente a través del equipo de TI. Por eso el espacio entre el marco del armario y los perfiles de acero debe estar perfectamente sellado.

Se pueden usar paneles de gestión de flujo de aire instalados en la zona inferior, superior, izquierda y derecha.

Estas placas conectan totalmente el armario con los perfiles que se instalan el equipo informático. La gestión del flujo de aire aplicada correctamente generará una mayor eficiencia y prolongará la vida útil del servidor.

2.5. Compruebe el ROI de reemplazo de un servidor

Actualmente la vida útil de un servidor es de cuatro años. El capital de inversión combinado con los gastos operativos será hasta cuatro veces mayor al costo del propio servidor. Es necesario estimar estos costos con las inversiones requeridas en los equipos nuevos para que sean más eficientes energéticamente.

Para los dispositivos que funcionan a máxima carga, los cálculos deben reajustarse en la medida de lo posible. Deben realizarse periódicamente para evaluar la posibilidad

de actualizar el servidor a una generación más nueva y en consecuencia en reducir el consumo.

Por lo tanto, el personal administrativo de TI siempre debe comparar regularmente el consumo de energía del servidor de su centro de datos actual con el consumo de energía para reducir el consumo que tenga sentido tantas veces desde una perspectiva ambiental como financiera.

2.6. Tipos de rPDU

Actualmente los rPDU presentan una infinidad de variedades en cuanto a control y monitoreo, incluso se especifican dentro de sus propuestas tecnología de avanzada y personalizaciones que el cliente propone en cada uno de los centros de datos que lo soporta, sin embargo, clasificaremos solo dos tipos de rack para un mayor alcance los rPDU básico o los rPDU inteligentes.

Dentro de la gama de rPDU inteligentes brindan una serie de características y beneficios de alto rendimiento que ayudan a resolver las necesidades de aplicaciones de baja a alta densidad y en entornos tradicionales y no tradicionales.

Clasifiquemos las rPDU: las rPDU inteligentes cuando agregan capacidades de plataforma de diseño preparadas para el futuro y monitoreo remoto, administración de energía y se pueden describir de la siguiente manera:

- **Rack PDU con medición:** Permite la administración del centro de datos como la visualización de métricas de energía al instante en una pantalla local, esto es ideal al desplazar o mover dispositivos y prevenir sobrecargas son apropiadas para los data center alejados y que la infraestructura energética este alejada de la red local.

- ***Rack PDU monitoreado:*** Observa un monitoreo del uso de la energía tanto en el rack en el acceso remoto mientras administra una distribución de eléctrica confiable en los equipos TI críticos, tiene opciones de configuración de monitoreo a nivel de entrada/salida y proporcionan acceso rápido a la información crítica para la evaluación de tendencias de uso de energía se recomienda para datacenter de alta densidad y que logren controlar y monitorear la efectividad del uso de energía.

- **Rack PDU conmutado:** Proporciona una visión completa del uso de energía de los equipos o dispositivos de TI críticos tanto en el rack como en el control de acceso remoto, con la capacidad e encendido y apagado del sistema en forma remota en cada tomacorriente por lo tanto ayuda al equilibrio energético toda vez que al tener un equipo sobrecargado simplemente cortará la energía o mediante otro soporte trasladará la conectividad a otros equipos de mayor capacidad o previamente diseñado para este tipo de situaciones, tiene opciones de configuración de monitoreo remoto nivel de unidad y nivel de salida, son necesarios en los centros de datos que necesiten limitar el uso de energía en los tomacorrientes para evitar sobrecargas adicionales.

2.7. Gestión Ambiental

El sistema de gestión ambiental proporciona monitoreo remoto de sensores y dispositivos en los data center y salas de equipos, creando un sistema crítico de alerta temprana que monitorea las condiciones del data center y notifica cuando algún incumplimiento establecido anteriormente no se cumpla. También recopila y almacena los datos de los sensores para análisis futuros, lo que ayuda a solucionar problemas y optimiza las condiciones de sitio.

Existe una amplia variedad de sensores de monitoreo tanto en los racks como en los data center alrededor de sus gabinetes de servidores y gabinetes de red, por ejemplo:

- **Sensor de punto de fuga de líquidos:** se usa para la detección de líquidos en puntos específicos dentro de un condensador, existen opciones de detección de fugas por zona y se usa para detectar una fuga en un área específica que forma una barrera perimetral, por ejemplo, alrededor de bombas, enfriadores, calderas, válvulas de control de agua, tuberías de agua destilada.

- **Sensor de temperatura:** controla de monitoreo de la temperatura en centros de datos, gabinetes de servidores de red.

- **Sensor de humo:** se usa para la detección de la presencia de humo en los centros de datos y los espacios informáticos. Este sensor completa el sistema de seguridad existente que ya está en funcionamiento.

- **Sensor de humedad:** se usa para le monitoreo de la humedad de los Racks o del data center, así como gabinetes de red.

- **Sensor magnético de puerta:** se usa para detectar cuando se abre y se cierra la puerta o cuando se quita el panel de acceso del gabinete de un panel de cubierta.

- **Sensor de movimiento:** se usa para la detección de cualesquiera movimientos en un área determinada, inclusive tiene la posibilidad de al detectar el movimiento enciende las luminarias.

2.8. Conmutadores KVM

Los conmutadores KVM establecen en su diseño lograr el control de una sola consola de servidores locales o remotos, lo que garantiza una reproducción de imagen real entre los activos de la sala de control de transmisión y la posibilidad de traslado el equipo informático de un espacio de trabajo centralizado con conmutadores KVM y extensores que pueden gestionar TI desde cualquier ubicación.

Para la protección de intrusiones cibernéticas, los conmutadores KVM brindan acceso seguro a los dispositivos de uso compartido de periféricos, donde puede interactuar de manera confiable con múltiples computadoras o monitores con cero retrasos de conmutación, mientras se quitan las amenazas de dispositivos compartidos que no son de confianza y que están en riesgo de fuga de datos, transferencia o acompañamiento.

Los conmutadores KVM se dividen en dos tipos de modelos:

- **Conmutador analógico:** se accionan mediante un cable conectado directamente desde un ordenador al conmutador KVM y desde allí a la consola de acceso, los cables pueden ser coaxiales o Cat5

- **Conmutador digital:** también conocido como KVM-IP permite el control de servidores a través de una conexión IP y en cualquier lugar (fuera de la red intranet de la empresa) Las computadoras aun necesitan tener una conexión directa al conmutador KVM, pero el usuario que controla estas computadoras no necesita estar conectados directamente al conmutador KVM.

Hay dos formas de acceder a los conmutadores KVM.

- **Conmutador monousuario:** usualmente usado en instalaciones pequeñas como SOHO u oficinas remotas. Permite que una persona acceda a tantas computadoras como sea necesaria desde una consola KVM.

- **Conmutador multi-usuario:** usado en grandes instalaciones y centros de datos que necesitan una gran cantidad de administradores de diferentes servidores.

2.9. *Software* DCIM

El *software* más usado actualmente para data center es DCIM (Data Center *Infraestructura Management*) la gestión de la infraestructura del centro de datos (DCIM) es una opción de solución de supervisión y gestión para entonos críticos desarrollada específicamente para minimizar los riesgos del contexto de dicha infraestructura, a través de una vista 3D completa del data center, con gráficos y pantallas personalizadas, DCIM de la información detallada de la infraestructura y realiza un seguimiento en tiempo real de los parámetros físico y lógicos, entre los cuales se encuentran monitoreo y evaluación de recursos (equipos) gestión del espacio, consumo de energía, humedad, fuego, temperatura, control de acceso (puertas Racks y CCTV) y el monitoreo de eficiencia energética.

La mejora de la energía de los centros de datos es una las aplicaciones más usadas del DCIM ya que mide el consumo de energía necesario para un funcionamiento seguro a altas densidades de consumo, se puede ahorrar según datos hasta un 20% del costo total de propiedad (TCO) del centro de datos al reducir el consumo de energía.

Hay opciones que ofrecen otros beneficios como es la trazabilidad vía radiofrecuencia identificación por radiofrecuencia RFID) de los equipos la integración de la función a DCIM hace posible que todos los equipos presentes en el data center sean identificados y monitoreados mediante etiquetas RFID aprobadas.

Además, DCIM permite vincular el elemento de mantenimiento, es decir cuando existe una indicación de un evento de riesgo el sistema puede comunicarse en forma automática con la empresa responsable del mantenimiento.

3. Protección de *hardware* y medios de almacenamiento de datos

Entre los tipos de seguridad en un data center hacen referencia al recurso a proteger:

- **A la seguridad física:** se refiere a la protección de todos nuestros elementos desde el punto de vista posible desastres naturales como incendios, terremotos o inundaciones, así como también de otras amenazas externas como puede ser robo, problemas eléctricos, etc.

- **A la seguridad lógica:** se encarga de proteger todo lo relacionado con el *software* de información contenida en los equipos, complementa perfectamente a la seguridad física mediante el uso de antivirus, encriptación de la información, ataques de hackers externos y otro mecanismo para la protección y privacidad de la información de cada usuario de la red.

Además de este tipo de seguridad existe la clasificación de la seguridad se focaliza en el momento en que estamos poniendo en marcha las medidas de seguridad.

3.1. Seguridad activa y Seguridad Pasiva

- **La seguridad activa:** es aquella que se centra en prevenir o evitar daños a los sistemas informáticos en conjunto, ya se de *hardware* o de *software do* de red. Los sistemas más comunes relacionados con la seguridad activa como por ejemplo los antivirus, los controles de acceso a las salas de servidores, la encriptación de la información, los sistemas de redundancia de *hardware*, etc.

- **La seguridad pasiva:** Es lo contrario a la seguridad activa, es un complemento que penetra en marcha cuando las medidas de seguridad activa no han sido suficientes para frenar a la amenaza. Un ejemplo claro es el tema de las copias

de seguridad. Realizar copias de seguridad es poner en marcha una seguridad activa ya que nos anticipamos al riesgo de perder información.

Hablamos de Seguridad de *hardware* cuando adoptamos medidas para proteger todos nuestros elementos físicos de posibles daños de cualquier tipo. Es muy similar al concepto de seguridad física, pero la complementa al incluir mecanismos adicionales de protección como por ejemplo el uso de SAI, o sistemas de alimentación ininterrumpidas que protegen a nuestros equipos físicos de sobretensiones o faltas de alimentación de energía.

Considerando dentro de la protección del *Hardware* están los siguientes conceptos:

3.2. SAI (Sistema de Alimentación Ininterrumpida)

En ingles **UPS (*Uninterruptible Power Supply*):** son sistemas de alimentación ininterrumpida, constituyen un elemento básico en la protección de *hardware* y, por extensión, de los datos almacenados en él.

Nos permitirán guardar con seguridad los datos si falla el suministro eléctrico dentro de los tipos de SAI se encuentran:

- **Sistema SAU *offline o standby:*** son los equipos SAI más económicos, se usan para ordenadores personales. No estabilizan la corriente y solo generan la tensión de salida cuando se produce una interrupción de suministro eléctrico, es decir, en estado *standby* el equipo SAI suministra a tensión directamente de la compañía de suministro eléctrico, Apenas corrigen las imperfecciones del suministro eléctrico.

- **SAI Interactivo:** son equipos de gama media-alta que estabilizan la corriente incorporando un estabilizador de voltaje o de salida (AVR). Solo generan la tensión de salida cuando se produce un corete de energía eléctrico, es decir en *standby* el equipo SAI suministra la tensión directamente de la compañía del

suministro eléctrico, pero es tensión estabilizada dentro de unos márgenes de tolerancia.

3.2.1 Regletas Protectoras

Protegen el *hardware* de la acción de los Rayos de las bajadas y subidas de tensión y del ruido eléctrico.

3.2.2 Fuente de energía de Reserva (UPS)

Brinda protección frente a posibles problemas eléctricos, ya que incluye una batería de reserva que se encarga del suministro de energía cuando el voltaje de entrada cae por debajo del nivel normal, la batería permanece inactiva durante el funcionamiento normal. Al disminuir el voltaje, la batería suministra energía de CC a un inversor que la convierte en CA para la computadora, no es tan confiable como una UPS debido al tiempo que demora en pasar al modo de batería.

3.2.3 Grupos Electrógenos

Maquinaria que genera electricidad mediante un motor de combustión interna se utilizan en lugares donde es vital seguir trabajando, por ejemplo. en hospitales pueden tener arranque manual o automático que permitirá que cuando se detecte un fallo en el suministro, se encienda y comience a dar corriente algunos elementos que, de forma genérica, componen un grupo electrógeno:

- Motor.
- Alternador.
- Tubo de escape.
- Depósito.

- Reguladores e indicadores.
- Chasis y protecciones.

3.3. Monitorización del *Hardware*

Podemos comprobar el funcionamiento de los elementos del sistema midiendo sus magnitudes eléctricas. Usaremos un polímero, que nos permitirá conocer la corriente de un determinado dispositivo.

Básicamente consiste en monitorizar el *hardware* a través de programas. La información que nos dan estos programas nos ayuda a la detección de errores y a comprobar el rendimiento del ordenador.

3.3.1. Cableado

Para la seguridad de las personas y los equipos deben estar bien y con materiales en perfecto estado y de buena calidad.

3.3.2. Fijación de componentes físicos

Se deben fijar los componentes físicos de un ordenador, para protegerlo de las vibraciones del propio equipo, también pueden producir vibraciones factores externos como los terremotos.

Al ahora de fijar los equipos, debemos tener en cuenta dejar un espacio suficiente para la ventilación.

Otros componentes físicos:

Entre los componentes para la protección del *hardware* podemos tener:

- Cerradoras para proteger los ordenadores del robo.
- Carcasas.
- Maletín de transporte.
- Refrigeración líquida.
- Protector de pantalla.
- Teclado resistente al agua.

3.4. Seguridad pasiva mecanismos de tolerancia a fallos

La redundancia puede ser de dos tipos:

- **Redundancia estática:** los componentes duplicados siempre están activos y funcionando.
- **Redundancia Mecánica:** cuando se detecta el fallo, el componente redundante empieza a funcionar.
- Algunos elementos redundantes.
- **Discos Duros:** se usan RAID, grupo redundante de discos independientes.
- Fuentes de alimentación.
- Tarjetas de Red.

3.4.1. Renovación de equipos:

Es necesario establecer un programa de renovación de equipos hay factores que hay que tener en cuenta tales como:

- La amortización.
- Coste.
- Coste de instalación.
- Actualización del *Software*.

Se pueden adquirir equipos mediante *leasing* o mediante *renting.*

También es necesario establecer algunos componentes como la adquisición de racks Ignífugos ya que establece medidas de seguridad que aporta a:

- Disminuir el riesgo de cortocircuito.
- Favorecer la colocación en zonas seguras y protegidas por sistemas contraincendios.
- Proporcionar una refrigeración adecuada.
- Son aislantes acústicos.
- Se pueden colocar en armarios ignífugos.

3.5. Medios de almacenamiento de datos

La arquitectura de almacenamiento de los data center es una pieza clave durante el desarrollo de las operaciones de las empresas, no solo administran la cantidad de información, así como establecen los requerimientos a futuro que los usuarios finales solicitan, sin embargo, también son responsables de proveer alta disponibilidad de los recursos principalmente de máquinas virtuales.

Existen diferentes soluciones de almacenamientos y dependerá del uso que se le quiera dar ya sea para respaldo a largo plazo. Acceso infrecuente acceso inmediato o alta disponibilidad para ello se establecer un estudio en este caso para los que estén alineados a los objetivos de las empresas un almacenamiento desproporcionado solo generara costos altos sin considerar el consumo energético en todo caso del crecimiento debe ser progresivo de tal manera que no impacte en los costos de las operaciones se analizan por lo tanto las arquitecturas más importantes de almacenamiento.

3.5.1. DAS - Direct Attached Storage

Es un arquitectura simple y económica ya no siendo muy utilizada en la actualidad básicamente un dispositivo conectado directamente al servidor físico mediante una interfaz SATA o SAS presenta altos porcentajes de desuso ya que el data center actualmente almacena mediante la red.

3.5.2. *NAS - Network-Attached Storage*

Es un servidor de archivos el cual es accedido mediante una red local a través de protocolos de transferencia de archivos FTP, NFS, AFS, SMB etc. Es centralizado y escalable y permite archivos compartidos por múltiples *Hosts* sin embargo al usa la red se pierde rendimiento Generalmente se implementan como servidores ya que los

dispositivos NAS cuentan con CPU, memoria, tarjetas de Red, sin embargo, su propósito es no correr grandes procesos sino almacenar datos.

3.5.3. *Sistema RAID - Redundant Array of Independent Disks*

Además de proveer almacenamiento virtual al combinar uno o más discos de forma lógica, ordenados de acuerdo con ciertas configuraciones, se crearon para la tolerancia a fallos aumento de capacidad y alta disponibilidad en servidores que deben manejar una lata cantidad de datos Una de las ventajas es que mantiene *Hot-swqap* lo que permite cambiar discos de forma física de un servidor, sin impactar los datos y las operaciones las configuraciones típicas en el uso del RAI son:

- **Raid 0, *Disk Strippimng*:** no ofrece redundancia y/o duplicación ya que solamente distribuye los discos entre servidores para almacenar *Throughput* (i.e mayor IOPS) de esta forma se puede estar escribiendo/leyendo 1 solo gran archivo entre varios servidores de forma paralela el inconveniente es que si existe un fallo este debe era ser generalizado afectando todos los discos.

- **RAID 1, *Mirroring*:** este modelo de raid crea copias de seguridad (copias espejo) de un disco en algún otro servidor con tal proveer tolerancia a fallos en caso de que exista algún problema de alguno de los dos discos se accederá al disco de respaldo. La desventaja de RAID 1 es que aumenta al doble a la cantidad de discos que den mantenerse impactando directamente al uso del espacio físico.

- **RAID 10, *Disk Stripping+Mirroring*:** es una combinación entre raid 0 y Raid 1 en la cual se provee el aumento del Throughput de traid 0 además de la tolerancia a fallas de raid1, sin embargo, se deben tener como mínimo 4 discos distribuidos para poder establecer estas mejoras (2 para *stripping* y 2 para *mirroring*) si bien este sistema ofrece alto rendimiento y alta disponibilidad la capacidad de escala es extremadamente baja.

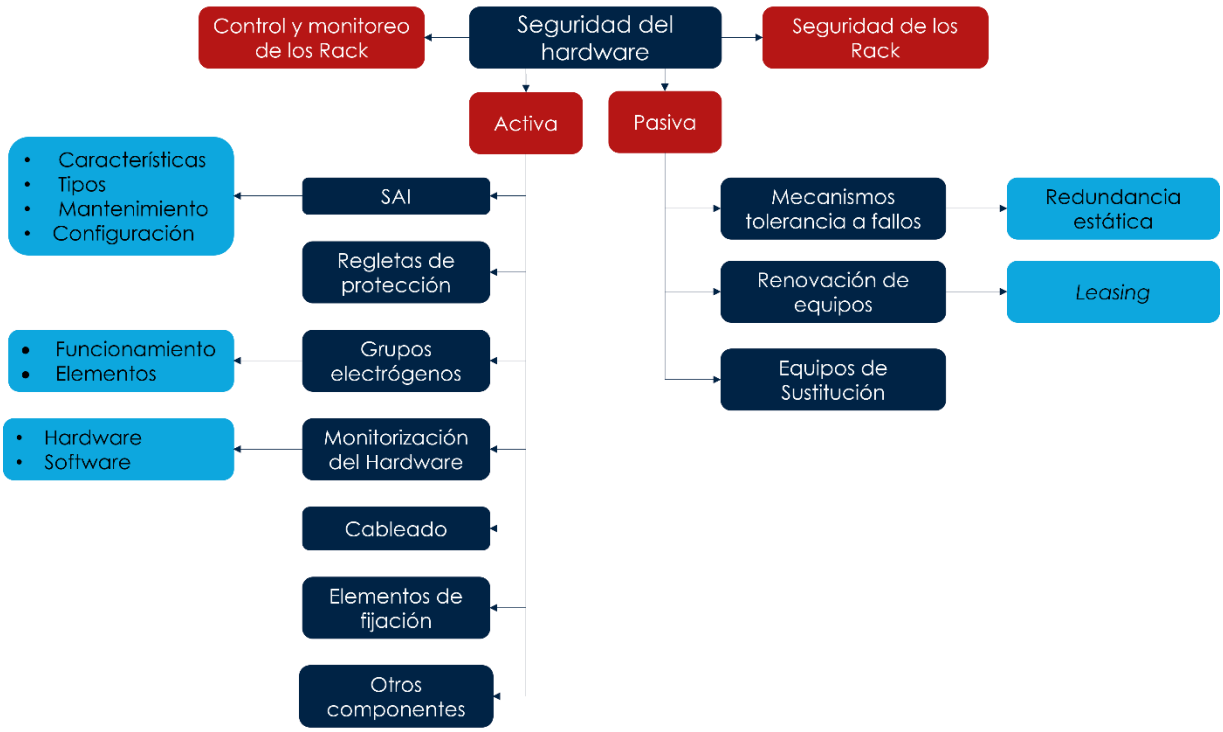
3.5.4. *SAN - Storage Área Network*

Es una arquitectura de almacenamiento ampliamente usada en data center que ofrece escalabilidad, alto rendimiento y alta disponibilidad basada en almacenamiento a través de redes.

La visión de SAN es como ve los servidores en NAS los servidores acceden mediante acceso remoto través de protocolos de la capa de aplicación (con FTP o NFS) sin embargo en la arquitectura SAN los servidores ven al almacenamiento como si fuera un disco anexado a través de LUNs-SAN - *Storage* Área *Networkal Unit Number* (llamado disco lógico) el servidor entonces puede visualizar esta porción de almacenamiento como un disco montable del sistema operativo una ventaja de este acercamiento es dichas porciones de almacenamiento aunque estén compartidas del mismo SAN estén aisladas unas de otras en el sentidos que una VM no pueda acceder a otra LUNs lo que ofrece seguridad.

Cierre

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



¿En qué se diferencia una seguridad Activo-Pasivo con seguridad Físico - Lógica?

La seguridad activa se define como el conjunto de controles que intentan evitar los daños durante un incidente de seguridad es decir cuando existe una ocurrencia y la pasiva está ligada a los daños en forma complementaria de la seguridad pasiva.

En el caso de la seguridad Física y Lógica se refieren al procedimiento para la prevención de incidentes y está relacionado a la protección de los datos físicos como los *hardware* y lógicos referidos a los *software* y aplicaciones.

Referencias bibliográficas

- Abts, Dennis. *High performance datacenter networks: architectures, algorithms, and opportunities ISBN: 9781608454020*. Recuperado en agosto del 2022, disponible en: https://bit.ly/3oqlVSL

- U.S.A.: TIA. (2005). *Telecommunications Infrastructure Standard for Data Centers.* Consultado en agosto 2022, disponible en: https://bit.ly/3bxb9XX