

PLANTILLA DE ENTREGA DE TRABAJO

CIB201-198-223081-ONL-SEGURIDAD DE CABLEADO Y DATACENTER

Semana 3

Jonathan Joel Salinas Santibañez

Índice

[Introducción 4](#_Toc46485953)

[Desarrollo 5](#_Toc46485954)

[Conclusión 6](#_Toc46485955)

[Bibliografía 7](#_Toc46485956)

# Introducción

El presente informe se enfoca en un incidente de seguridad que tuvo lugar en el centro de datos de AIEP, ubicado en el primer piso de su sede Grajales. Este incidente destacó la falta de medidas de seguridad física efectivas en el centro de datos, lo que resultó en una violación de seguridad significativa y consecuencias graves para la institución educativa. En este informe, analizaremos la causa principal de la violación de seguridad, recomendaremos medidas para prevenir futuras vulnerabilidades, identificaremos la vulnerabilidad que permitió la propagación del incendio y propondremos soluciones para la mitigación automática de incendios en el futuro. Además, se destacarán las ventajas de implementar un control de acceso en un rack de comunicaciones para garantizar la integridad y disponibilidad de los sistemas críticos en un entorno de centro de datos.

# Desarrollo

Causa principal de violación de seguridad en el rack de comunicaciones:

La causa principal de la violación de seguridad en el rack de comunicaciones fue el acceso no autorizado de Don Carlos a la sala del centro de datos. Al conectar un hervidor y un alargador eléctrico al rack de los switches, creó un riesgo de sobrecarga eléctrica que resultó en el sobrecalentamiento y posterior incendio del equipo.

Herramienta o equipamiento recomendado para prevenir la vulnerabilidad en el rack de comunicaciones:

Para prevenir futuras vulnerabilidades en el rack de comunicaciones, se recomienda implementar un sistema de control de acceso físico, como una cerradura electrónica con tarjeta de acceso o un lector de huellas dactilares en la puerta de la sala del centro de datos. Esto garantizará que solo personas autorizadas puedan ingresar y manipular los equipos.

Vulnerabilidad que permitió la propagación del incendio por una hora:

La vulnerabilidad que permitió que el incendio se propagara durante una hora fue la falta de un sistema de detección y extinción automática de incendios en el rack de comunicaciones. La falta de un sistema adecuado para detectar y combatir el fuego de manera inmediata permitió que el incendio se extendiera antes de que el personal de seguridad lo descubriera.

Herramienta o equipamiento recomendado para apagar automáticamente futuros incendios en un rack:

Para garantizar una respuesta más rápida y efectiva a futuros incendios en un rack de comunicaciones, se debe implementar un sistema de supresión de incendios automático, como un sistema de extinción de incendios por gas inerte o un sistema de rociadores automáticos. Estos sistemas pueden detectar y extinguir incendios de manera rápida y eficiente, minimizando el daño a los equipos y evitando tiempos prolongados de inactividad.

Ventajas de un control de acceso en un rack de comunicaciones:

Cuatro ventajas de implementar un control de acceso en un rack de comunicaciones son:

1. Seguridad mejorada: Impide el acceso no autorizado a la sala del centro de datos y al equipo crítico, protegiéndolo de robos y manipulaciones no autorizadas.
2. Registro de actividad: Permite llevar un registro de quién accede a la sala y cuándo, lo que facilita la auditoría de la seguridad y la responsabilidad.
3. Prevención de accidentes: Evita situaciones como la descrita en el incidente, donde personas no autorizadas pueden causar daños accidentales a los equipos.
4. Mayor disponibilidad: Garantiza que solo personal autorizado pueda acceder al rack de comunicaciones, reduciendo el riesgo de interrupciones no planificadas en los servicios de red.

# Conclusión

El incidente ocurrido en el centro de datos de AIEP, que resultó en una semana de inactividad en toda la sede, puso de manifiesto la importancia crítica de abordar las deficiencias en la seguridad física y la gestión de riesgos en entornos de centros de datos.