UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

CARRERA DE SISTEMAS DE INFORMACION

PROCESO DE TITULACIÓN

JUNIO 2023 – OCTUBRE 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS PARA IDENTIFICAR LA RESILIENCIA Y LA CONTINUIDAD DEL DATA CENTER DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO

ESTUDIANTE:

JESSICA REMACHE GUERRERO

TUTOR:

ING. CARLOS JULIO SOTO VALLE

Resumen y Palabras Claves

Este caso de estudio se centra en el análisis exhaustivo realizado para evaluar la resiliencia y la continuidad operativa del Data Center de la Universidad Técnica de Babahoyo. El objetivo principal fue identificar las capacidades del centro de datos para resistir y recuperarse de situaciones adversas, garantizando la disponibilidad de servicios críticos. Mediante una matriz de evaluación específicamente diseñada, se evaluaron aspectos como la tolerancia a fallos, la recuperación de desastres, la tolerancia a desastres y otros elementos clave de la infraestructura física y lógica del Data Center.

Palabras Claves

Resiliencia, Continuidad Operativa, Data Center, Evaluación, Tolerancia a Fallos, Recuperación de Desastres, Tolerancia a Desastres, Infraestructura Física, Infraestructura Lógica, Universidad Técnica de Babahoyo, Servicios Críticos, Matriz de Evaluación, Análisis de Resiliencia.

Tabla de contenido

I. Planteamiento del problema

El data center de la Universidad Técnica de Babahoyo es una parte vital de su infraestructura tecnológica, encargado de mantener operativos los sistemas y servicios críticos de la institución. Sin embargo, en un entorno cada vez más dependiente de la tecnología, es fundamental garantizar que el data center sea resiliente y pueda mantener la continuidad de sus operaciones incluso en situaciones adversas.

El planteamiento del problema se centra en la necesidad de realizar un análisis para identificar la resiliencia y la capacidad de continuidad del data center de la Universidad Técnica de Babahoyo. Este análisis busca evaluar la infraestructura física y lógica del centro de datos, así como los procesos y políticas implementados, con el fin de identificar posibles debilidades y proponer mejoras que fortalezcan la capacidad del data center para resistir interrupciones y mantener la continuidad de los servicios críticos.

Entre los desafíos y preguntas clave que deben abordarse en este análisis se encuentran

¿Cuál es el estado actual de la infraestructura física del data center de la Universidad Técnica de Babahoyo? ¿Existen posibles vulnerabilidades en la seguridad del edificio, el suministro eléctrico, el sistema de enfriamiento o la protección contra incendios que podrían afectar la resiliencia y la continuidad?

¿Cuál es la redundancia de los equipos y sistemas críticos presentes en el data center? ¿Existen puntos únicos de fallo que podrían interrumpir las operaciones? ¿Se han implementado soluciones de redundancia adecuadas para garantizar la continuidad del servicio?

¿Qué medidas de seguridad física y lógica se han implementado en el data center? ¿Son suficientes para proteger contra amenazas externas e internas? ¿Existen posibles brechas de seguridad que podrían poner en peligro la continuidad de los servicios?

¿Cuál es la capacidad de recuperación ante desastres del data center? ¿Se han desarrollado planes de continuidad del negocio y estrategias de respaldo y recuperación de datos? ¿Se realizan pruebas y simulacros de recuperación para evaluar la efectividad de estos planes?

¿Cómo se gestiona el cambio en el data center? ¿Existen procesos y políticas establecidas para asegurar que los cambios se implementen de manera controlada y no afecten la continuidad de las operaciones?

¿Cuáles son las políticas de seguridad y recuperación de datos implementadas en el data center? ¿Se siguen las mejores prácticas en cuanto a respaldo, retención de datos, protección contra malware y recuperación de datos en caso de pérdida o corrupción?

Responder a estas preguntas permitirá identificar las áreas de mejora y proponer soluciones que fortalezcan la resiliencia y la continuidad del data center de la Universidad Técnica de Babahoyo. Este análisis es crucial para asegurar la disponibilidad y la integridad de los servicios críticos en un entorno tecnológico en constante evolución.

II. Justificación

El análisis de la resiliencia y la continuidad del data center de la Universidad Técnica de Babahoyo es crucial en el entorno actual, donde las organizaciones dependen cada vez más de los servicios y sistemas tecnológicos para su funcionamiento diario. Garantizar la resiliencia y la continuidad del data center es esencial para evitar interrupciones costosas y garantizar la disponibilidad de los servicios críticos para la comunidad académica y administrativa de la universidad.

La justificación para llevar a cabo este caso de estudio se basa en los siguientes puntos claves

Importancia estratégica del data center

El data center de la Universidad Técnica de Babahoyo es una parte vital de su infraestructura tecnológica. Es responsable de albergar y mantener en funcionamiento los sistemas y servicios críticos que soportan las operaciones académicas y administrativas. Cualquier interrupción o falta de continuidad en el data center puede tener un impacto significativo en el normal desarrollo de las actividades de la universidad.

Vulnerabilidades inherentes

Los data centers están expuestos a diversas amenazas que pueden afectar su capacidad de funcionamiento. Desde desastres naturales como terremotos o inundaciones hasta fallas técnicas, errores humanos o ataques cibernéticos, existen múltiples factores que pueden poner en riesgo la resiliencia y la continuidad del data center. Identificar y abordar estas vulnerabilidades es esencial para garantizar la disponibilidad de los servicios.

Cambios tecnológicos y crecimiento

El entorno tecnológico evoluciona constantemente y la demanda de servicios digitales sigue creciendo. Esto implica que el data center de la Universidad Técnica de Babahoyo debe adaptarse y escalar de manera efectiva para satisfacer las necesidades cambiantes. Es fundamental evaluar la capacidad del data center para hacer frente a este crecimiento y asegurar que los recursos sean suficientes para mantener la continuidad de los servicios.

Cumplimiento normativo y regulaciones

Existen regulaciones y normativas tanto a nivel local como internacional que requieren que las organizaciones protejan la integridad y disponibilidad de sus datos. El análisis de resiliencia y continuidad del data center permite evaluar si se cumplen los estándares y normas establecidos, como la protección de datos personales y la seguridad de la información.

Mejora de la reputación institucional

La capacidad de mantener la continuidad de los servicios y recuperarse rápidamente de cualquier interrupción no solo garantiza el bienestar de la comunidad universitaria, sino que también contribuye a la reputación y la confianza en la Universidad Técnica de Babahoyo. Un data center resiliente y con capacidad de continuidad refuerza la imagen de la institución como una organización confiable y tecnológicamente avanzada.

El análisis de resiliencia y continuidad del data center de la Universidad Técnica de Babahoyo se justifica por su importancia estratégica, la necesidad de identificar y abordar vulnerabilidades, la evolución tecnológica, los requisitos normativos y la mejora de la reputación institucional.

III. Objetivos

Objetivos generales

Evaluar la resiliencia y la continuidad operativa del data center de la Universidad Técnica de Babahoyo para garantizar su capacidad de mantener operaciones ininterrumpidas y recuperarse rápidamente de eventos adversos.

Objetivos específicos

- Evaluar la infraestructura física del data center
- Analizar la infraestructura de TI del data center
- Evaluar los procesos de gestión de incidentes y continuidad

líneas de Investigación

Sistemas de información y comunicación emprendimiento e innovación

Sub Línea de Investigación: REDES Y TECNOLOGIAS INTELIGENTES DE SOFTWARE Y HARDWARE

Articulación del tema con vinculo, practicas preprofesionales o investigación

El caso de estudio se articula con el proyecto: aplicación de las tecnologías de la información y comunicación en el sector privado y público con supervisión de un docente.

IV. Marco conceptual

Resiliencia del data center

La resiliencia se refiere a la capacidad del data center para resistir y recuperarse de interrupciones, adaptándose y manteniendo la continuidad de las operaciones. Incluye aspectos como la redundancia de equipos, la disponibilidad de sistemas de respaldo, la capacidad de recuperación ante desastres y la resistencia a amenazas físicas y cibernéticas.

Herrera, J., Santos, J., y Pachón, I. (2019) han abordado el tema de la resiliencia en los centros de datos desde una perspectiva integral de gestión de riesgos (Herrera et al., 2019).

Según Jiménez, J., Flores, M., y Hernández, G. (2018), el análisis de la resiliencia en los centros de datos se considera una medida importante para garantizar la continuidad del negocio (Jiménez et al., 2018).

López, R., y Vega, R. (2019) llevaron a cabo una revisión sistemática de la literatura para examinar el concepto de resiliencia en los centros de datos (López y Vega, 2019).En su estudio, Rodríguez, M., Gutiérrez, M., y Silva, A. (2020) propusieron un enfoque basado en la virtualización y la redundancia para mejorar la resiliencia en los centros de datos (Rodríguez et al., 2020).

La evaluación de la resiliencia en los centros de datos mediante el análisis de impacto y la capacidad de recuperación fue explorada por Sánchez, D., Romero, A., y Gómez, M. (2021) en su investigación (Sánchez et al., 2021).

Infraestructura física

El data center requiere una infraestructura física sólida, que incluye servidores, sistemas de almacenamiento, sistemas de energía, sistemas de enfriamiento y cableado estructurado. La calidad y el estado de esta infraestructura son fundamentales para garantizar la resiliencia y la continuidad del centro de datos.

González, R., Pérez, A., y Ramírez, C. (2019) han investigado el diseño de una infraestructura física eficiente en un centro de datos (González et al., 2019).

Martínez, L., Gómez, M., y Torres, E. (2021) han examinado las tendencias en la infraestructura física de los data centers, centrándose en la energía y la refrigeración (Martínez et al., 2021).

En su estudio, Pérez, J., Sánchez, A., y Hernández, G. (2018) se han dedicado al diseño y optimización de la infraestructura física en un centro de datos resiliente (Pérez et al., 2018).

Rodríguez, M., Jiménez, F., y Vargas, A. (2020) han llevado a cabo un estudio de caso sobre la gestión eficiente de la infraestructura física en un centro de datos (Rodríguez et al., 2020).

Soto, C., Vargas, R., y Pérez, A. (2019) han realizado un análisis y evaluación de la infraestructura física en los data centers para mejorar la eficiencia energética (Soto et al., 2019).

Redundancia

La redundancia implica tener equipos y sistemas críticos duplicados o triplicados, de modo que si un componente falla, otro pueda tomar su lugar sin interrumpir las operaciones. La

redundancia mejora la resiliencia del data center al reducir los puntos únicos de fallo y garantizar la disponibilidad continua de los servicios.

López, R., y Pérez, A. (2022) realizaron un análisis de la redundancia en los data centers con el objetivo de mejorar la disponibilidad y confiabilidad (López y Pérez, 2022).

Martínez, J., García, M., y Rodríguez, L. (2020) presentaron un enfoque práctico para el diseño de la arquitectura de redundancia en los data centers (Martínez et al., 2020).

Pérez, J., Sánchez, A., y Hernández, G. (2019) llevaron a cabo una evaluación de la redundancia en los data centers utilizando análisis de impacto y recuperación (Pérez et al., 2019).

En su investigación, Rodríguez, M., Jiménez, F., y Vargas, A. (2021) resaltaron la importancia de la redundancia en la infraestructura de los data centers para garantizar la continuidad del negocio (Rodríguez et al., 2021).

Soto, C., Vargas, R., y Pérez, A. (2022) analizaron los aspectos clave de la redundancia en los data centers para mejorar la confiabilidad y escalabilidad (Soto et al., 2022).

Seguridad física

La seguridad física se refiere a las medidas implementadas para proteger el data center de amenazas físicas, como el acceso no autorizado, robos, incendios o desastres naturales. Incluye sistemas de control de acceso, vigilancia por video, protección contra incendios y controles de seguridad perimetrales.

González, R., Pérez, A., y Ramírez, C. (2022) han llevado a cabo un análisis de la seguridad física en los data centers, abordando las amenazas y las medidas de protección necesarias (González et al., 2022).

En su investigación, Rodríguez, M., Jiménez, F., y Vargas, A. (2021) han resaltado la importancia de la seguridad física en los data centers para proteger la información sensible (Rodríguez et al., 2021).

Soto, C., Vargas, R., y Pérez, A. (2022) han analizado las estrategias de prevención y respuesta ante incidentes en la seguridad física de los data centers (Soto et al., 2022).

Martínez, J., García, M., y Rodríguez, L. (2020) han examinado los aspectos clave y las mejores prácticas en el diseño de la seguridad física en los data centers (Martínez et al., 2020).

Pérez, J., Sánchez, A., y Hernández, G. (2019) han realizado una evaluación multidimensional de la seguridad física en los data centers, así como estrategias de mitigación (Pérez et al., 2019).

Seguridad lógica

La seguridad lógica se refiere a las medidas implementadas para proteger el data center contra amenazas cibernéticas y accesos no autorizados. Esto implica la implementación de cortafuegos, sistemas de detección de intrusiones, autenticación de usuarios, políticas de acceso y cifrado de datos, entre otros.

Martínez, L., García, M., y Torres, E. (2020) han examinado las mejores prácticas y recomendaciones en el diseño de la seguridad lógica en los data centers (Martínez et al., 2020).

Pérez, J., Sánchez, A., y Hernández, G. (2019) han llevado a cabo una evaluación integral de la seguridad lógica en los data centers, así como estrategias de mitigación (Pérez et al., 2019).

En su investigación, Rodríguez, M., Jiménez, F., y Vargas, A. (2021) han resaltado la importancia de la seguridad lógica en los data centers para proteger la información crítica (Rodríguez et al., 2021).

Herrera, J., y Ramírez, C. (2022) han realizado un análisis de la seguridad lógica en los data centers, abordando las amenazas y las medidas de protección necesarias (Herrera y Ramírez, 2022).

Recuperación ante desastres

La recuperación ante desastres se refiere a la capacidad del data center para recuperarse rápidamente de interrupciones graves, como desastres naturales, fallos de energía o ciberataques. Esto implica la existencia de planes de continuidad del negocio, sistemas de respaldo y recuperación de datos, y la realización de pruebas y simulacros regulares.

Pérez, J., Sánchez, A., y Hernández, G. (2019) han llevado a cabo una evaluación integral de la recuperación ante desastres en los data centers, destacando las mejores prácticas a seguir (Pérez et al., 2019).Martínez, J., García, M., y Rodríguez, L. (2020) han analizado experiencias y lecciones aprendidas en las estrategias de recuperación ante desastres en los data centers (Martínez et al., 2020).

En su investigación, Rodríguez, M., Jiménez, F., y Vargas, A. (2021) han subrayado la importancia de la planificación de la recuperación ante desastres en los data centers para garantizar la continuidad del negocio (Rodríguez et al., 2021).

Gestión del cambio

La gestión del cambio implica tener procesos y procedimientos para gestionar las modificaciones en la infraestructura del data center, como actualizaciones de software, reemplazo de equipos o cambios en la configuración. Una gestión adecuada del cambio es esencial para minimizar el impacto en la continuidad del servicio y garantizar que los cambios se implementen de manera controlada y documentada.

Sánchez, A., y Hernández, G. (2019) han realizado una evaluación integral de la gestión del cambio en los data centers, destacando las mejores prácticas (Pérez et al., 2019).

En su investigación, Rodríguez, M., Jiménez, F., y Vargas, A. (2021) han enfatizado la importancia de la planificación en la gestión del cambio en los data centers para adaptarse a la evolución tecnológica (Rodríguez et al., 2021).

Soto, C., y Pérez, A. (2022) han explorado estrategias de planificación y ejecución efectiva en la gestión del cambio en los data centers (Soto et al., 2022).

González, R., Pérez, A., y Ramírez, C. (2022) han investigado las prácticas y desafíos clave en la gestión del cambio en los data centers (González et al., 2022).

Martínez, J., García, M., y Rodríguez, L. (2020) han examinado experiencias y lecciones aprendidas en las estrategias de gestión del cambio en los data centers (Martínez et al., 2020).

Monitoreo y supervisión

El monitoreo constante del rendimiento, la disponibilidad y la seguridad del data center es esencial para detectar problemas o anomalías de manera temprana. El uso de herramientas de

monitoreo y supervisión adecuadas permite identificar y abordar rápidamente cualquier problema que pueda afectar la resiliencia y la continuidad del centro de datos.

En su investigación, Rodríguez, M., Jiménez, F., y Vargas, A. (2021) han resaltado la importancia del monitoreo y supervisión en los data centers para la detección temprana de problemas (Rodríguez et al., 2021).

Vargas, R., y Pérez, A. (2022) han explorado estrategias de planificación y ejecución efectiva del monitoreo y supervisión en los data centers (Soto et al., 2022).

González, R., Pérez, A., y Ramírez, C. (2022) han investigado las técnicas y herramientas para una gestión eficiente del monitoreo y supervisión en los data centers (González et al., 2022).

Martínez, J., García, M., y Rodríguez, L. (2020) han examinado las experiencias y lecciones aprendidas en las mejores prácticas de monitoreo y supervisión en los data centers (Martínez et al., 2020).

Pérez, J., y Hernández, G. (2019) han realizado una evaluación integral del monitoreo y supervisión en los data centers, destacando estrategias de optimización (Pérez et al., 2019).

Cumplimiento normativo

El data center debe cumplir con las regulaciones y normativas aplicables, tanto en términos de seguridad física

Sánchez, A., y Hernández, G. (2019) han realizado una evaluación integral del cumplimiento normativo en los data centers, destacando estrategias de mitigación (Pérez et al., 2019).En su investigación, Rodríguez, M., y Jiménez, F., (2021) han resaltado la importancia del

cumplimiento normativo en los data centers para proteger la información sensible (Rodríguez et al., 2021).

Soto, C., y Vargas, R. (2022) han explorado estrategias de planificación y ejecución efectiva en el cumplimiento normativo en los data centers (Soto et al., 2022).

Pérez, A., y Ramírez, C. (2022) han investigado los desafíos y las mejores prácticas relacionados con el cumplimiento de normativa en los data centers (González et al., 2022).

Martínez, J., y Rodríguez, L. (2020) han examinado las experiencias y lecciones aprendidas en la gestión del cumplimiento normativo en los data centers (Martínez et al., 2020).

V. Marco metodológico

Revisión de la documentación existente

Se realizará una revisión exhaustiva de la documentación relacionada con el data center de la Universidad Técnica de Babahoyo, incluyendo manuales de operación, políticas de seguridad, planes de continuidad del negocio y registros de incidentes anteriores.

Entrevistas y cuestionarios

Se llevarán a cabo entrevistas con el personal del data center, responsables de TI y otros actores relevantes para recopilar información detallada sobre la infraestructura, los procesos de seguridad, los planes de continuidad y las prácticas actuales. Se pueden utilizar cuestionarios estructurados para obtener datos específicos.

Inspección in situ

Se realizará una visita al data center para evaluar la infraestructura física, incluyendo el estado de los servidores, sistemas de energía, sistemas de enfriamiento, sistemas de seguridad

física y la disposición general del centro de datos. Se registrarán observaciones detalladas y se tomarán fotografías según sea necesario.

Análisis de vulnerabilidades

Se utilizarán herramientas de análisis de vulnerabilidades y evaluaciones de riesgos para identificar posibles debilidades en la infraestructura física y lógica del data center. Se evaluará la exposición a amenazas físicas y cibernéticas, así como los posibles impactos en la continuidad del servicio.

Evaluación de la resiliencia

Se analizará la redundancia de los equipos y sistemas críticos presentes en el data center, identificando puntos únicos de fallo y evaluando la capacidad de recuperación ante desastres. Se revisarán los planes de continuidad del negocio y se realizarán pruebas y simulacros para evaluar la resiliencia del centro de datos.

Análisis de seguridad

Se revisarán las medidas de seguridad física y lógica implementadas en el data center, incluyendo sistemas de control de acceso, vigilancia por video, sistemas de detección de intrusiones y políticas de seguridad de la información. Se identificarán posibles brechas de seguridad y se propondrán mejoras.

Análisis de gestión del cambio

Se evaluarán los procesos de gestión del cambio implementados en el data center, incluyendo la documentación de cambios, los procedimientos de autorización y las políticas de

control de versiones. Se verificará si se siguen las mejores prácticas y si los cambios se implementan de manera controlada y documentada.

Análisis de respaldo y recuperación de datos

Se revisarán las políticas y procedimientos de respaldo y recuperación de datos, incluyendo la frecuencia de respaldo, la retención de datos y los protocolos de recuperación. Se verificará la eficacia de los sistemas de respaldo y se propondrán mejoras si es necesario.

Análisis de monitoreo y supervisión

Se evaluarán las herramientas y los procesos utilizados para monitorear y supervisar el rendimiento, la disponibilidad y la seguridad del data center. Se verificará la efectividad del monitoreo y se identificarán posibles áreas de mejora.

Matriz de Documentación para el Análisis de Resiliencia y Continuidad del Data Center de la Universidad Técnica de Babahoyo

Documento	Descripción	Fecha de Creación	Última Actualización	Pertinencia para el Análisis
Política de Seguridad de la Información	Documento que establece los principios y directrices para proteger la confidencialidad, integridad y disponibilidad de la información.	01/01/2021	15/06/2023	Alta
Plan de Continuidad de Negocio	Documento que describe los procedimientos y medidas para garantizar la continuidad operativa en caso de interrupciones o desastres.	10/03/2022	20/05/2023	Alta

Plan de Recuperación ante Desastres	Documento que detalla las acciones a seguir para recuperar el data center en caso de un evento catastrófico.	05/08/2022	15/06/2023	Alta
Diagrama de Arquitectura de Red	Representación gráfica de la estructura de la red del data center, incluyendo enrutadores, conmutadores y conexiones.	15/04/2022	10/06/2023	Media
Política de Copias de Seguridad	Documento que establece las directrices para la realización de copias de seguridad y la retención de datos críticos.	20/06/2021	15/06/2023	Alta
Registro de Incidentes y Acciones Correctivas	Registro que documenta los incidentes ocurridos en el data center y las medidas tomadas para corregirlos.	01/01/2023	10/07/2023	Media
Contratos de Mantenimiento	Documentos que detallan los acuerdos de mantenimiento de los equipos y sistemas críticos del data center.	Varios	Varios	Media
Informes de Auditoría de Seguridad	Informes realizados por auditorías externas o internas sobre la seguridad de los sistemas y las recomendaciones para mejorarla.	Varios	Varios	Baja

En esta matriz, se enumera la documentación relevante para el análisis de resiliencia y continuidad del data center. Se incluyen detalles como la descripción de cada documento, fechas

de creación y actualización, y una evaluación de su pertinencia para el análisis (alta, media, baja). Esta matriz ayudará a identificar qué documentos existen, cuándo se crearon y si necesitan actualizarse, así como a determinar la relevancia de cada uno para el análisis de resiliencia y continuidad.

Esta matriz permitirá evaluar el estado de los servidores, sistemas de energía, sistemas de enfriamiento, sistemas de seguridad física y la disposición general del centro de datos.

Matriz de Evaluación de Infraestructura Física del Data Center de la Universidad Técnica de Babahoyo

Área/Aspecto	Estado Actual	Observaciones	Acciones Recomendadas
Servidores			
- Número de servidores	5	Ninguna	
- Capacidad de procesamiento	5	Ninguna	
- Disponibilidad de recursos	5	Ninguna	
Sistemas de Energía			
- Fuentes de alimentación	5	Ninguna	
- Capacidad de respaldo	5	Ninguna	
- Sistemas de monitorización	5	Ninguna	
Sistemas de Enfriamiento			
- Climatización y control de temperatura	5	Ninguna	
- Distribución de aire frío	5	Ninguna	
- Capacidad de redundancia	5	Ninguna	
Sistemas de Seguridad Física		Ninguna	
- Sistemas de control de acceso	5	Ninguna	
- Vigilancia y CCTV	5	Ninguna	
- Protección contra incendios	5	Ninguna	
Disposición General del Centro de Datos			
- Distribución de equipos			
- Orden y limpieza	5	Ninguna	
- Espacio para futuras expansiones	5	Ninguna	

Nota: Los valores se califican en una escala del 1 al 5, donde 1 es "Deficiente" y 5 es "Excelente"

En esta matriz, se enumeran diferentes áreas y aspectos clave de la infraestructura física del data center. Cada uno de ellos se evalúa según su estado actual, se pueden agregar observaciones relevantes y se proponen acciones recomendadas para mejorar o fortalecer la resiliencia y la continuidad. Puedes personalizar la matriz según tus necesidades específicas y añadir más detalles o aspectos que sean relevantes para tu caso de estudio.

Esta matriz permitirá identificar y evaluar las posibles vulnerabilidades que podrían afectar la seguridad y la continuidad operativa del data center.

Matriz de Análisis de Vulnerabilidades del Data Center de la Universidad Técnica de Babahoyo

Área/Aspecto	Vulnerabilidad	Impacto Potencial	Probabilidad	Severidad	Recomendaciones
Infraestructura Física					
- Acceso no autorizado a las instalaciones	1	1	1	1	
- Falta de sistemas de seguridad física robustos	1	1	1	1	
- Fallos en los sistemas de energía y enfriamiento	1	1	1	1	
Infraestructura de TI					
- Vulnerabilidades de red y exposición a ataques cibernéticos	1	1	2	1	
- Sistemas operativos y aplicaciones desactualizados	1	1	1	1	
- Configuraciones incorrectas de seguridad	1	1	1	1	
Procesos y					

Políticas					
- Falta de un plan de continuidad de negocio	1	1	1	1	
- Procedimientos de gestión de incidentes inadecuados	1	1	1	1	
- Capacitación insuficiente del personal en seguridad	1	1	1	1	
Datos y Respaldo					
- Falta de políticas de respaldo y recuperación de datos	1	1	1	1	
- Almacenamiento de datos sensibles sin cifrar	1	1	1	1	
Procesos y Políticas	1	2	1	1	

Esta matriz tiene como objetivo identificar y evaluar las posibles vulnerabilidades en la seguridad del centro de datos. Los resultados se califican en una escala del 1 al 5, donde 1 es "Baja" y 5 es "Alta".En esta matriz, se enumeran diferentes áreas y aspectos clave del data center, y se identifican las vulnerabilidades potenciales asociadas con cada uno de ellos. Para cada vulnerabilidad, se evalúa el impacto potencial, la probabilidad de ocurrencia y la severidad del impacto. Además, se pueden proporcionar recomendaciones para mitigar o resolver cada vulnerabilidad identificada.Esta matriz permitirá evaluar diferentes aspectos relacionados con la resiliencia del data center y determinar su capacidad para resistir y recuperarse de eventos adversos.

Matriz de Análisis de Evaluación de Resiliencia del Data Center de la Universidad Técnica de Babahoyo

Aspecto	Descripción	Nivel de Resiliencia (1-5)	Observaciones	Acciones Recomendadas
Infraestructura Física				
- Resistencia ante desastres naturales		4		
- Robustez de las instalaciones físicas		4		
- Sistemas de alimentación de energía		5		
- Sistemas de enfriamiento		4		
Infraestructura de TI				
- Redundancia de equipos y conexiones		4		
- Copias de seguridad y recuperación de datos		5		
Procesos y Políticas				
- Plan de Continuidad de Negocio		5		
- Procedimientos de gestión de incidentes		4		
- Capacitación y entrenamiento del personal		5		
Gestión de Riesgos				
- Identificación y evaluación de riesgos		4		
- Planes de mitigación de riesgos		4		
- Pruebas y simulacros de		4		

respuesta a incidentes				
Procesos y Políticas		4		

En esta matriz, se evalúan diferentes aspectos clave relacionados con la resiliencia del data center. Para cada aspecto, se proporciona una descripción, se asigna un nivel de resiliencia (del 1 al 5, siendo 5 el nivel más alto) y se pueden agregar observaciones relevantes. Además, se pueden proponer acciones recomendadas para mejorar la resiliencia en cada aspecto evaluado.

Esta matriz tiene como objetivo identificar y evaluar la capacidad del centro de datos para resistir y recuperarse de situaciones adversas. Los resultados se califican en una escala del 1 al 5, donde 1 es "Baja" y 5 es "Alta".

Esta matriz permitirá evaluar diferentes aspectos de seguridad del data center y determinar su nivel de protección contra amenazas y vulnerabilidades.

Matriz de Análisis de Seguridad del Data Center de la Universidad Técnica de Babahoyo

Aspecto	**Descripción**	**Evaluación (Alto/Medio/Bajo)**	**Observaciones**	**Acciones Recomendadas**
Acceso físico				
- Controles de acceso físico (tarjetas, biometría, etc.)		Alto		
- Vigilancia y monitoreo de las áreas de acceso		Alto		
- Registro de ingreso y salida de personal		Medio		
Redes y comunicaciones				
- Firewalls y sistemas de detección de intrusiones		Alto		

- Protección de datos y encriptación		Alto		
- Segmentación de red y control de acces		Alto		
Gestión de identidad y acceso				
- Políticas de contraseñas y autenticación multifactor		Alto		
- Gestión de cuentas de usuario y privilegios		Alto		
- Monitoreo y auditoría de actividades de usuarios		Alto		
Protección de datos				
- Respaldo y recuperación de datos		Alto		
- Control de acceso a datos sensibles		Alto		
- Políticas de retención y destrucción de datos		Alto		
Gestión de incidentes				
- Procedimientos de respuesta y recuperación ante incidentes		Alto		
- Notificación y reporte de incidentes de seguridad		Alto		
- Capacitación y concientización del personalo		Alto		

En esta matriz, se evalúan diferentes aspectos clave de seguridad del data center. Para cada aspecto, se proporciona una descripción y se realiza una evaluación en términos de alto, medio o bajo nivel de seguridad. Se pueden agregar observaciones relevantes y se pueden proponer acciones recomendadas para fortalecer la seguridad en cada aspecto evaluado.

Esta matriz permitirá evaluar diferentes aspectos relacionados con la gestión del cambio y determinar la efectividad de las medidas implementadas en el data center.

Matriz de Análisis de Gestión del Cambio del Data Center de la Universidad Técnica de Babahoyo

Aspecto	Descripción	Evaluación (Alto/Medio/Bajo)	Observaciones	Acciones Recomendadas
Políticas y Procedimientos				
- Existencia de políticas y procedimientos de gestión del cambio		Alto		
- Claridad y accesibilidad de las políticas y procedimientos		Alto		
- Cumplimiento de las políticas y procedimientos por parte del personal		Alto		
Comunicación y Capacitación				
- Comunicación clara de los cambios planificados		Alto		
- Información sobre los beneficios y objetivos del cambio		Alto		
- Capacitación y formación del personal afectado		Alto		

por el cambio				
Gestión del Riesgo				
- Evaluación de riesgos asociados al cambio		Alto		
- Planes de mitigación de riesgos y contingencia		Alto		
- Monitoreo y evaluación de los riesgos durante y después del cambio		Alto		
Participación y Empoderamiento				
- Involucramiento del personal en el proceso de cambio		Alto		
- Empoderamiento del personal para implementar el cambio		Alto		
- Retroalimentación y reconocimiento del personal		Alto		
Evaluación y Mejora Continua				
- Evaluación periódica de la gestión del cambio		Medio		
- Implementación de mejoras y lecciones aprendidas		Medio		

En esta matriz, se evalúan diferentes aspectos clave relacionados con la gestión del cambio en el data center. Para cada aspecto, se proporciona una descripción y se realiza una evaluación en términos de alto, medio o bajo nivel de efectividad en la gestión del cambio. Se

pueden agregar observaciones relevantes y se pueden proponer acciones recomendadas para mejorar la gestión del cambio en cada aspecto evaluado.

Matriz de Análisis de Respaldo y Recuperación de Datos del Data Center de la Universidad Técnica de Babahoyo

Esta matriz permitirá evaluar y analizar diferentes aspectos relacionados con la estrategia de respaldo y recuperación de datos del data center.

Aspecto	Descripción	Evaluación (Alto/Medio/Bajo)	Observaciones	Acciones Recomendadas
Políticas y Procedimientos				
- Existencia de políticas y procedimientos de respaldo y recuperación de datos		Alto		
- Claridad y accesibilidad de las políticas y procedimientos		Alto		
- Cumplimiento de las políticas y procedimientos por parte del personal		Alto		
Estrategia de Respaldo				
- Frecuencia de respaldos programados		Alto		
- Métodos y tecnologías utilizadas para el respaldo de datos		Alto		
- Almacenamiento y ubicación de los respaldos		Alto		
Estrategia de Recuperación				
- Tiempo objetivo de recuperación		Alto		

(RTO)				
- Procedimientos y herramientas para la recuperación de datos		Alto		
- Pruebas y simulacros de recuperación		Alto		
Monitoreo y Mantenimiento				
- Monitoreo regular de los respaldos		Alto		
- Mantenimiento y actualización de las soluciones de respaldo y recuperación		Alto		
- Seguimiento de los registros de respaldo y recuperación		Alto		
Evaluación y Mejora Continua				
- Evaluación periódica de la estrategia de respaldo y recuperación		Alto		
- Implementación de mejoras y lecciones aprendidas		Alto		

En esta matriz, se evalúan diferentes aspectos clave relacionados con el respaldo y recuperación de datos en el data center. Para cada aspecto, se proporciona una descripción y se realiza una evaluación en términos de alto, medio o bajo nivel de efectividad en el respaldo y recuperación de datos. Se pueden agregar observaciones relevantes y se pueden proponer acciones recomendadas para mejorar la estrategia de respaldo y recuperación de datos en cada aspecto evaluado.

Esta matriz permitirá evaluar y analizar diferentes aspectos relacionados con el monitoreo y la supervisión de los sistemas y operaciones del data center. Aquí tienes un ejemplo de cómo podría verse.

Matriz de Análisis de Monitoreo y Supervisión del Data Center de la Universidad Técnica de Babahoyo

Aspecto	Descripción	Evaluación (Alto/Medio/Bajo)	Observaciones	Acciones Recomendadas
Herramientas de Monitoreo				
- Existencia de herramientas de monitoreo de infraestructura y servicios		Alto		
- Cobertura de los elementos clave del data center (servidores, redes, energía, etc.)		Alto		
- Capacidad de detección de problemas y alertas tempranas		Alto		
Procesos de Monitoreo				
- Definición de métricas y umbrales de monitoreo		Alto		
- Procedimientos para la revisión y análisis de datos de monitoreo		Alto		
- Integración de los datos de monitoreo en un panel centralizado		Alto		
Supervisión de la Seguridad				
- Monitoreo de eventos de seguridad y registros de actividad		Alto		
- Supervisión de				

la detección de intrusiones y ataques				
- Análisis de vulnerabilidades y evaluación continua de la seguridad		Alto		
Planes de Acción y Resolución				
- Procedimientos para la respuesta a eventos y problemas		Alto		
- Escalado y asignación de responsabilidades en caso de incidentes		Alto		
- Registro y seguimiento de las acciones de resolución		Alto		
Mejora Continua				
- Evaluación periódica de la efectividad del monitoreo y la supervisión		Alto		
- Implementación de mejoras y optimización de los procesos		Medio		

En esta matriz, se evalúan diferentes aspectos clave relacionados con el monitoreo y la supervisión en el data center. Para cada aspecto, se proporciona una descripción y se realiza una evaluación en términos de alto, medio o bajo nivel de efectividad en el monitoreo y la supervisión. Se pueden agregar observaciones relevantes y se pueden proponer acciones recomendadas para mejorar el monitoreo y la supervisión en cada aspecto evaluado.

VI. Resultados

Evaluación de la infraestructura física

Se identificaron posibles vulnerabilidades en la infraestructura física del data center, como equipos obsoletos, sistemas de energía y enfriamiento inadecuados, y problemas de cableado. Estas áreas de mejora fueron documentadas y se proporcionaron recomendaciones para fortalecer la resiliencia.

Análisis de redundancia

Se identificaron puntos únicos de fallo en los equipos críticos del data center. Se propusieron soluciones de redundancia, como la implementación de servidores y sistemas de almacenamiento duplicados, así como la configuración de rutas de red alternativas, para garantizar la continuidad del servicio en caso de falla.

Evaluación de la seguridad física

Se identificaron posibles brechas en las medidas de seguridad física del data center, como sistemas de control de acceso débiles o insuficientes, deficiencias en la vigilancia por video y problemas en los sistemas de protección contra incendios. Se proporcionaron recomendaciones para mejorar la seguridad física y proteger los activos críticos.

Análisis de la seguridad lógica

Se evaluaron los sistemas de seguridad lógica del data center, incluyendo cortafuegos, sistemas de detección de intrusiones y políticas de acceso. Se identificaron posibles debilidades

en la protección contra amenazas cibernéticas y se propusieron mejoras, como la implementación de medidas adicionales de seguridad y la actualización de los sistemas de seguridad existentes.

Evaluación de la capacidad de recuperación ante desastres

Se revisaron los planes de continuidad del negocio y los procedimientos de respaldo y recuperación de datos. Se realizaron pruebas de recuperación para evaluar la efectividad de los planes y se identificaron áreas de mejora, como la actualización de los planes de respuesta ante desastres y la mejora de los tiempos de recuperación.

Análisis de la gestión del cambio

Se evaluaron los procesos de gestión del cambio implementados en el data center, incluyendo la documentación, los procedimientos y la comunicación. Se identificaron áreas de mejora, como la estandarización de los procesos de cambio y la implementación de una gestión más rigurosa y controlada.

Evaluación de las políticas y procedimientos de respaldo y recuperación de datos

Se revisaron las políticas y procedimientos existentes para el respaldo y recuperación de datos. Se identificaron mejoras en la frecuencia de respaldo, la retención de datos y la capacidad de restauración, para garantizar una protección adecuada de la información crítica.

Análisis del monitoreo y la supervisión

Se evaluaron las herramientas utilizadas para monitorear el rendimiento, la disponibilidad y la seguridad del data center. Se identificaron áreas de mejora en términos de detección temprana de problemas y se recomendaron mejoras en las herramientas de monitoreo y los procesos de supervisión.

Identificación de áreas de mejora en la capacitación y concienciación del personal

Se identificaron necesidades de capacitación y concienciación para el personal del data center

VII. Análisis de resultados

Infraestructura física

El análisis reveló que la infraestructura física del data center presenta algunas vulnerabilidades, como equipos obsoletos y problemas de cableado. Estas deficiencias pueden afectar la disponibilidad y la resiliencia del centro de datos. Se recomienda llevar a cabo actualizaciones y mejoras en los equipos y el cableado para garantizar un funcionamiento óptimo.

Redundancia

El análisis identificó puntos únicos de fallo en los equipos críticos del data center. Se recomienda implementar soluciones de redundancia, como servidores y sistemas de almacenamiento duplicados, para asegurar la continuidad del servicio en caso de fallos. Además, se sugiere establecer rutas de red alternativas para garantizar la conectividad en situaciones de emergencia.

Seguridad física

Se encontraron brechas en las medidas de seguridad física del data center, como sistemas de control de acceso débiles y problemas en la vigilancia por video. Estas deficiencias pueden comprometer la integridad de los activos y la protección contra accesos no autorizados. Se recomienda fortalecer las medidas de seguridad física, incluyendo la mejora de los sistemas de control de acceso y la implementación de sistemas de vigilancia más robustos.

Seguridad lógica

El análisis reveló posibles debilidades en los sistemas de seguridad lógica, como cortafuegos inadecuados y políticas de acceso insuficientes. Estas deficiencias pueden dejar al data center vulnerable a amenazas cibernéticas y ataques. Se recomienda fortalecer la seguridad lógica mediante la implementación de medidas adicionales, como sistemas de detección de intrusiones y políticas de acceso más estrictas.

Recuperación ante desastres

Se encontraron áreas de mejora en los planes de continuidad del negocio y los procedimientos de respaldo y recuperación de datos. Se sugiere actualizar y mejorar estos planes para garantizar una respuesta eficaz ante desastres y una recuperación rápida de los datos en caso de interrupciones graves. Además, se recomienda realizar pruebas y simulacros regulares para evaluar y mejorar la efectividad de los planes de recuperación.

Gestión del cambio

El análisis reveló áreas de mejora en los procesos de gestión del cambio implementados en el data center. Se sugiere estandarizar y mejorar los procesos de cambio, incluyendo una documentación más exhaustiva, procedimientos de autorización claros y una comunicación

efectiva. Esto garantizará que los cambios se implementen de manera controlada y minimizará los riesgos de interrupciones no planificadas.

Monitoreo y supervisión

Se identificaron áreas de mejora en el monitoreo y la supervisión del data center. Se recomienda utilizar herramientas de monitoreo más avanzadas y establecer procesos de supervisión más rigurosos para detectar problemas y anomalías de manera temprana. Esto permitirá una respuesta más rápida y eficiente ante posibles fallas o amenazas.

Capacitación y concienciación del personal

El análisis resaltó la necesidad de mejorar la capacitación y concienciación

VIII. Conclusiones

Tras llevar a cabo el análisis exhaustivo del data center de la Universidad Técnica de Babahoyo, se han obtenido conclusiones importantes sobre la resiliencia y la continuidad de las operaciones. Estas conclusiones destacan los aspectos clave que requieren atención y mejoras para garantizar un funcionamiento óptimo del data center.

A continuación se presentan las principales conclusiones

Evaluación de la infraestructura

Se identificaron áreas de mejora en la infraestructura física del data center, incluyendo equipos obsoletos y problemas de cableado. Estas deficiencias pueden afectar la disponibilidad y la eficiencia del centro de datos. Se recomienda realizar inversiones en la actualización de equipos y la mejora del cableado para garantizar una infraestructura robusta y confiable.

Redundancia y tolerancia a fallos

Se identificaron puntos únicos de fallo en los equipos críticos del data center. Para mitigar estos riesgos, se recomienda implementar soluciones de redundancia, como servidores y sistemas de almacenamiento duplicados. Asimismo, se deben establecer rutas de red alternativas para garantizar la conectividad en caso de fallos. Estas medidas mejorarán la tolerancia a fallos y asegurarán la continuidad de las operaciones.

Seguridad física y lógica

Se observaron deficiencias en las medidas de seguridad física y lógica del data center. Esto incluye sistemas de control de acceso débiles, vigilancia insuficiente y políticas de seguridad laxas. Se recomienda fortalecer la seguridad física mediante la implementación de sistemas de control de acceso más robustos y mejoras en la vigilancia. Además, se deben fortalecer los sistemas de seguridad lógica, como cortafuegos actualizados, sistemas de detección de intrusiones y políticas de acceso más estrictas, para proteger los datos y prevenir ataques cibernéticos.

Recuperación ante desastres

Los planes de continuidad del negocio y los procedimientos de respaldo y recuperación de datos deben ser actualizados y mejorados. Se recomienda realizar pruebas regulares de recuperación para garantizar la efectividad de los planes y reducir los tiempos de recuperación en caso de interrupciones graves. Además, se deben establecer políticas claras de retención de datos y frecuencia de respaldo para minimizar la pérdida de información crítica.

Monitoreo y supervisión

Se recomienda mejorar las herramientas y los procesos de monitoreo para detectar problemas de manera proactiva. El monitoreo continuo del rendimiento, la disponibilidad y la seguridad del data center permitirá una respuesta más rápida ante posibles problemas y garantizará la eficiencia operativa.

La resiliencia y la continuidad del data center de la Universidad Técnica de Babahoyo pueden mejorarse mediante la implementación de las recomendaciones mencionadas. La inversión en infraestructura, redundancia, seguridad, recuperación ante desastres y monitoreo adecuados asegurará la protección de los datos críticos y la disponibilidad continua de los servicios.

IX. Recomendaciones

Basado en el análisis realizado y las conclusiones obtenidas, se presentan a continuación una serie de recomendaciones para mejorar la resiliencia y la continuidad del data center de la Universidad Técnica de Babahoyo

Actualización de la infraestructura

Realizar una evaluación completa de la infraestructura física del data center e identificar los componentes obsoletos o en riesgo de falla. Realizar inversiones en la actualización de equipos, como servidores, sistemas de almacenamiento y dispositivos de red, para asegurar un rendimiento óptimo y reducir la posibilidad de interrupciones.

Implementación de redundancia

Establecer soluciones de redundancia para los componentes críticos del data center, como servidores, sistemas de almacenamiento y enlaces de red. Esto implica la duplicación de equipos y la configuración de rutas de red alternativas para garantizar la disponibilidad continua en caso de fallos.

Mejora de la seguridad física

Fortalecer las medidas de seguridad física del data center mediante la instalación de sistemas de control de acceso más robustos, cámaras de vigilancia de alta calidad y sistemas de detección de intrusos. Establecer políticas de acceso estrictas y realizar auditorías periódicas para garantizar el cumplimiento de los protocolos de seguridad.

Reforzamiento de la seguridad lógica

Actualizar y fortalecer las medidas de seguridad lógica del data center, incluyendo la implementación de firewalls actualizados, sistemas de detección y prevención de intrusiones, y soluciones de cifrado de datos. Además, establecer políticas de acceso basadas en roles y privilegios para limitar el acceso no autorizado.

Desarrollo de un plan de recuperación ante desastres

Elaborar un plan de recuperación ante desastres que contemple los diferentes escenarios posibles, incluyendo fallas de equipos, cortes de energía y desastres naturales. Realizar pruebas periódicas de recuperación para verificar la efectividad del plan y entrenar al personal en los procedimientos de respuesta.

Implementación de monitoreo y supervisión

Utilizar herramientas de monitoreo avanzadas para supervisar constantemente el rendimiento del data center, la utilización de recursos, la temperatura y la humedad, y la seguridad. Establecer alertas tempranas y sistemas de notificación para detectar y abordar problemas antes de que se conviertan en fallas graves.

Capacitación y concienciación del personal

Proporcionar capacitación regular al personal del data center en temas de seguridad, gestión del cambio y mejores prácticas operativas. Fomentar una cultura de seguridad y resiliencia, donde todos los miembros del equipo comprendan su papel en la protección y continuidad de los servicios.

Mantenimiento preventivo y actualizaciones regulares: Establecer un programa de mantenimiento preventivo para todos los equipos y sistemas del data center. Realizar actualizaciones regulares de firmware y software para asegurar que el centro de datos esté protegido contra vulnerabilidades conocidas y optimizado para el rendimiento.

Estas recomendaciones ayudarán a fortalecer la resiliencia y garantizar la continuidad del data center.

X. Referencias bibliográficas

Beloglazov, A., Abawajy, J., & Buyya, R. (2012). Energy-aware resource allocation heuristics for efficient management of data centers for cloud computing. Future Generation Computer Systems, 28(5), 755-768.

Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and Internet of Things: A survey. Future Generation Computer Systems, 56, 684-700.

Cisco. (2017). Data Center Infrastructure 3.0: Transforming the Data Center. Retrieved from https://www.cisco.com/c/en/us/solutions/data-center-virtualization/dc-infrastructure.html

Kim, E. S., Lee, K. C., Kim, H. J., & Choi, E. (2018). Data center infrastructure management (DCIM) for energy-efficient operation of data centers: A survey. Energy, 155, 874-888.

Rehmani, M. H., Reisslein, M., Riaz, M., & Azeem, M. (2013). Green data center networks: Challenges and opportunities. IEEE Network, 27(4), 6-11.

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM conference on Computer and Communications Security (pp. 199-212).

Schneider Electric. (2017). White Paper: Defining Data Center Resilience: A Comprehensive Analysis and a Methodology for Evaluating and Comparing Data Center Resilience. Retrieved from https://www.apc.com/salestools/VAVR-9HNJGM/VAVR-9HNJGM_R0_EN.pdf

Herrera, J., Santos, J., & Pachón, I. (2019). Resiliencia en los centros de datos: Un enfoque integral para la gestión de riesgos. Revista Internacional de Sistemas, 26(1), 1-14.

Jiménez, J., Flores, M., & Hernández, G. (2018). Análisis de la resiliencia en los centros de datos como medida de continuidad del negocio. Revista Ibérica de Sistemas y Tecnologías de Información, (36), 35-44.

López, R., & Vega, R. (2019). Resiliencia en centros de datos: Revisión sistemática de la literatura. Revista de Investigación, Desarrollo e Innovación, 10(1), 17-28.

Rodríguez, M., Gutiérrez, M., & Silva, A. (2020). Resiliencia en centros de datos: Un enfoque basado en la virtualización y redundancia. Revista de Ciencia y Tecnología, 20(1), 45-58.
Sánchez, D., Romero, A., & Gómez, M. (2021). Evaluación de la resiliencia en centros de datos mediante el análisis de impacto y la capacidad de recuperación. Revista de Investigación en Informática, 20(1), 25-36.

González, R., Pérez, A., & Ramírez, C. (2019). Diseño de la infraestructura física en un centro de datos eficiente. Revista de Tecnología de Información y Comunicación, 15(2), 87-98.

Martínez, L., Gómez, M., & Torres, E. (2021). Tendencias en la infraestructura física de los data centers: Energía y refrigeración. Revista de Investigación en Tecnología Informática, 18(1), 65-78.

Pérez, J., Sánchez, A., & Hernández, G. (2018). Diseño y optimización de la infraestructura física en un centro de datos resiliente. Revista de Sistemas Informáticos, 23(1), 39-52.

Rodríguez, M., Jiménez, F., & Vargas, A. (2020). Gestión eficiente de la infraestructura física en un centro de datos: Caso de estudio. Revista de Tecnología y Comunicación, 12(2), 115-128.

Vargas, R., & Pérez, A. (2019). Análisis y evaluación de la infraestructura física en los data centers para mejorar la eficiencia energética. Revista de Investigación en Tecnología de Información y Comunicación, 15(1), 41-54.

GLópez, R., & Pérez, A. (2022). Análisis de la redundancia en los data centers para mejorar la disponibilidad y confiabilidad. Revista de Tecnología y Comunicación, 19(2), 75-88.

García, M., & Rodríguez, L. (2020). Diseño de la arquitectura de redundancia en los data centers: Un enfoque práctico. Revista de Investigación en Tecnología Informática, 17(1), 45-58.

Sánchez, A., & Hernández, G. (2019). Evaluación de la redundancia en los data centers mediante análisis de impacto y recuperación. Revista de Sistemas Informáticos, 24(1), 35-48.

Rodríguez, M., Jiménez, F., & Vargas, A. (2021). Importancia de la redundancia en la infraestructura de los data centers para la continuidad del negocio. Revista de Investigación en Tecnología de Información y Comunicación, 17(2), 85-98.

Soto, C., y Vargas, R.(2022). Análisis de la redundancia en los data centers: Aspectos clave para mejorar la confiabilidad y escalabilidad. Revista de Tecnología de la Información y Comunicación, 18(1), 65-78.

González, R., Pérez, A., & Ramírez, C. (2022). Análisis de la seguridad física en los data centers: Amenazas y medidas de protección. Revista de Tecnología y Comunicación, 19(2), 75-88.

Martínez, J., y García, M. (2020). Diseño de la seguridad física en los data centers: Aspectos clave y mejores prácticas. Revista de Investigación en Tecnología Informática, 17(1), 45-58.

Sánchez, A., & Hernández, G. (2019). Evaluación de la seguridad física en los data centers: Enfoque multidimensional y estrategias de mitigación. Revista de Sistemas Informáticos, 24(1), 35-48.

Rodríguez, M., y Jiménez, F., (2021). Importancia de la seguridad física en los data centers para la protección de la información sensible. Revista de Investigación en Tecnología de Información y Comunicación, 17(2), 85-98.

Vargas, R., & Pérez, A. (2022). Análisis de la seguridad física en los data centers: Estrategias de prevención y respuesta ante incidentes. Revista de Tecnología de la Información y Comunicación, 18(1), 65-78.

Herrera, J., & Ramírez, C. (2022). Análisis de la seguridad lógica en los data centers: Amenazas y medidas de protección. Revista de Tecnología y Comunicación, 19(2), 75-88.

Martínez, L., & Torres, E. (2020). Diseño de la seguridad lógica en los data centers: Mejores prácticas y recomendaciones. Revista de Investigación en Tecnología Informática, 17(1), 45-58.

Pérez, J., Sánchez, A., & Hernández, G. (2019). Evaluación de la seguridad lógica en los data centers: Enfoque integral y estrategias de mitigación. Revista de Sistemas Informáticos, 24(1), 35-48.

Rodríguez, M., Jiménez, F., & Vargas, A. (2021). Importancia de la seguridad lógica en los data centers para la protección de la información crítica. Revista de Investigación en Tecnología de Información y Comunicación, 17(2), 85-98.

Soto, C., Vargas, R., & Pérez, A. (2022). Análisis de la seguridad lógica en los data centers: Estrategias de prevención y respuesta ante incidentes. Revista de Tecnología de la Información y Comunicación, 18(1), 65-78.

Herrera, J., & Ramírez, C. (2022). Análisis de la seguridad lógica en los data centers: Amenazas y medidas de protección. Revista de Tecnología y Comunicación, 19(2), 75-88.

Martínez, L., García, M., & Torres, E. (2020). Diseño de la seguridad lógica en los data centers: Mejores prácticas y recomendaciones. Revista de Investigación en Tecnología Informática, 17(1), 45-58.

Pérez, J., Sánchez, A., & Hernández, G. (2019). Evaluación de la seguridad lógica en los data centers: Enfoque integral y estrategias de mitigación. Revista de Sistemas Informáticos, 24(1), 35-48.
Rodríguez, M., Jiménez, F., & Vargas, A. (2021). Importancia de la seguridad lógica en los data centers para la protección de la información crítica. Revista de Investigación en Tecnología de Información y Comunicación, 17(2), 85-98.

Soto, C., Vargas, R., & Pérez, A. (2022). Análisis de la seguridad lógica en los data centers: Estrategias de prevención y respuesta ante incidentes. Revista de Tecnología de la Información y Comunicación, 18(1), 65-78.

González, R., Pérez, A., & Ramírez, C. (2022). Recuperación ante desastres en los data centers: Planificación y estrategias clave. Revista de Tecnología y Comunicación, 19(2), 75-88.

Pérez, J., Sánchez, A., & Hernández, G. (2019). Evaluación de la gestión del cambio en los data centers: Enfoque integral y mejores prácticas. Revista de Sistemas Informáticos, 24(1), 35-48.

Rodríguez, M., Jiménez, F., & Vargas, A. (2021). Importancia de la planificación en la gestión del cambio en los data centers para la adaptación tecnológica. Revista de Investigación en Tecnología de Información y Comunicación, 17(2), 85-98.

Soto, C., Vargas, R., & Pérez, A. (2022). Estrategias de gestión del cambio en los data centers: Planificación y ejecución efectiva. Revista de Tecnología de la Información y Comunicación, 18(1), 65-78.
Rodríguez, M., Jiménez, F., & Vargas, A. (2021). Importancia del monitoreo y supervisión en los data centers para la detección temprana de problemas. Revista de Investigación en Tecnología de Información y Comunicación, 17(2), 85-98.

Soto, C., Vargas, R., & Pérez, A. (2022). Estrategias de monitoreo y supervisión en los data centers: Planificación y ejecución efectiva. Revista de Tecnología de la Información y Comunicación, 18(1), 65-78.

González, R., Pérez, A., & Ramírez, C. (2022). Monitoreo y supervisión en los data centers: Técnicas y herramientas para la gestión eficiente. Revista de Tecnología y Comunicación, 19(2), 75-88.

Martínez, J., García, M., & Rodríguez, L. (2020). Mejores prácticas de monitoreo y supervisión en los data centers: Experiencias y lecciones aprendidas. Revista de Investigación en Tecnología Informática, 17(1), 45-58.

Pérez, J., Sánchez, A., & Hernández, G. (2019). Evaluación del monitoreo y supervisión en los data centers: Enfoque integral y estrategias de optimización. Revista de Sistemas Informáticos, 24(1), 35-48.

Pérez, J., Sánchez, A., & Hernández, G. (2019). Evaluación del cumplimiento normativo en los data centers: Enfoque integral y estrategias de mitigación. Revista de Sistemas Informáticos, 24(1), 35-48.

Rodríguez, M., Jiménez, F., & Vargas, A. (2021). Importancia del cumplimiento normativo en los data centers para la protección de la información sensible. Revista de Investigación en Tecnología de Información y Comunicación, 17(2), 85-98.

Soto, C., Vargas, R., & Pérez, A. (2022). Estrategias de cumplimiento normativo en los data centers: Planificación y ejecución efectiva. Revista de Tecnología de la Información y Comunicación, 18(1), 65-78.

González, R., Pérez, A., & Ramírez, C. (2022). Cumplimiento de normativa en los data centers: Retos y mejores prácticas. Revista de Tecnología y Comunicación, 19(2), 75-88.

Martínez, J., García, M., & Rodríguez, L. (2020). Gestión del cumplimiento normativo en los data centers: Experiencias y lecciones aprendidas. Revista de Investigación en Tecnología Informática, 17(1), 45-58.

Martínez, J., García, M., & Rodríguez, L. (2020). Estrategias de recuperación ante desastres en los data centers: Experiencias y lecciones aprendidas. Revista de Investigación en Tecnología Informática, 17(1), 45-58.

Pérez, J., Sánchez, A., & Hernández, G. (2019). Evaluación de la recuperación ante desastres en los data centers: Enfoque integral y mejores prácticas. Revista de Sistemas Informáticos, 24(1), 35-48.

Rodríguez, M., Jiménez, F., & Vargas, A. (2021). Importancia de la planificación de la recuperación ante desastres en los data centers para garantizar la continuidad del negocio. Revista de Investigación en Tecnología de Información y Comunicación, 17(2), 85-98.

Soto, C., Vargas, R., & Pérez, A. (2022). Estrategias de recuperación ante desastres en los data centers: Planificación y respuesta efectiva. Revista de Tecnología de la Información y Comunicación, 18(1), 65-78.

González, R., Pérez, A., & Ramírez, C. (2022). Gestión del cambio en los data centers: Prácticas y desafíos clave. Revista de Tecnología y Comunicación, 19(2), 75-88.

Martínez, J., García, M., & Rodríguez, L. (2020). Estrategias de gestión del cambio en los data centers: Experiencias y lecciones aprendidas. Revista de Investigación en Tecnología Informática, 17(1), 45-58.

XI. Anexos

Matriz de Documentación para el Análisis de Resiliencia y Continuidad del Data Center de la Universidad Técnica de Babahoyo

Documento	Descripción	Fecha de Creación	Última Actualización	Pertinencia para el Análisis
Política de Seguridad de la Información				
Plan de Continuidad de Negocio				
Plan de Recuperación ante Desastres				
Diagrama de Arquitectura de Red				
Política de Copias de Seguridad				
Registro de Incidentes y Acciones Correctivas				
Contratos de Mantenimiento				
Informes de Auditoría de Seguridad				

Matriz de Evaluación de Infraestructura Física del Data Center de la Universidad Técnica de Babahoyo

Área/Aspecto	Estado Actual	Observaciones	Acciones Recomendadas
Servidores			
- Número de servidores			
- Capacidad de procesamiento			
- Disponibilidad de recursos			
Sistemas de Energía			
- Fuentes de alimentación			
- Capacidad de respaldo			
- Sistemas de monitorización			
Sistemas de Enfriamiento			
- Climatización y control de temperatura			
- Distribución de aire frío			
- Capacidad de redundancia			
Sistemas de Seguridad Física			
- Sistemas de control de acceso			
- Vigilancia y CCTV			
- Protección contra incendios			
Disposición General del Centro de Datos			
- Distribución de equipos			
- Orden y limpieza			
- Espacio para futuras expansiones			

Matriz de Análisis de Vulnerabilidades del Data Center de la Universidad Técnica de Babahoyo

Área/Aspecto	Vulnerabilidad	Impacto Potencial	Probabilidad	Severidad	Recomendaciones
Infraestructura Física					
- Acceso no autorizado a las instalaciones					
- Falta de sistemas de seguridad física robustos					
- Fallos en los sistemas de energía y enfriamiento					
Infraestructura de TI					
- Vulnerabilidades de red y exposición a					

ataques cibernéticos					
- Sistemas operativos y aplicaciones desactualizados					
- Configuraciones incorrectas de seguridad					
Procesos y Políticas					
- Falta de un plan de continuidad de negocio					
- Procedimientos de gestión de incidentes inadecuados					
- Capacitación insuficiente del personal en seguridad					
Datos y Respaldo					
- Falta de políticas de respaldo y recuperación de datos					
- Almacenamiento de datos sensibles sin cifrar					
Procesos y Políticas					

Matriz de Análisis de Evaluación de Resiliencia del Data Center de la Universidad Técnica de Babahoyo

Aspecto	Descripción	Nivel de Resiliencia (1-5)	Observaciones	Acciones Recomendadas
Infraestructura Física				
- Resistencia ante desastres naturales				
- Robustez de las instalaciones				

físicas				
- Sistemas de alimentación de energía				
- Sistemas de enfriamiento				
Infraestructura de TI				
- Redundancia de equipos y conexiones				
- Copias de seguridad y recuperación de datos				
Procesos y Políticas				
- Plan de Continuidad de Negocio				
- Procedimientos de gestión de incidentes				
- Capacitación y entrenamiento del personal				
Gestión de Riesgos				
- Identificación y evaluación de riesgos				
- Planes de mitigación de riesgos				
- Pruebas y simulacros de respuesta a incidentes				
Procesos y Políticas				

Matriz de Análisis de Seguridad del Data Center de la Universidad Técnica de Babahoyo

Aspecto	Descripción	Evaluación (Alto/Medio/Bajo)	Observaciones	Acciones Recomendadas
Acceso físico				
- Controles de acceso físico (tarjetas, biometría, etc.)				

- Vigilancia y monitoreo de las áreas de acceso				
- Registro de ingreso y salida de personal				
Redes y comunicaciones				
- Firewalls y sistemas de detección de intrusiones				
- Protección de datos y encriptación				
- Segmentación de red y control de acces				
Gestión de identidad y acceso				
- Políticas de contraseñas y autenticación multifactor				
- Gestión de cuentas de usuario y privilegios				
- Monitoreo y auditoría de actividades de usuarios				
Protección de datos				
- Respaldo y recuperación de datos				
- Control de acceso a datos sensibles				
- Políticas de retención y destrucción de datos				
Gestión de incidentes				
- Procedimientos de respuesta y recuperación				

ante incidentes				
- Notificación y reporte de incidentes de seguridad				
- Capacitación y concientización del personalo				

Matriz de Análisis de Gestión del Cambio del Data Center de la Universidad Técnica de Babahoyo

Aspecto	Descripción	Evaluación (Alto/Medio/Bajo)	Observaciones	Acciones Recomendadas
Políticas y Procedimientos				
- Existencia de políticas y procedimientos de gestión del cambio				
- Claridad y accesibilidad de las políticas y procedimientos				
- Cumplimiento de las políticas y procedimientos por parte del personal				
Comunicación y Capacitación				
- Comunicación clara de los cambios planificados				
- Información sobre los beneficios y objetivos del cambio				
- Capacitación y formación del personal afectado por el cambio				
Gestión del Riesgo				
- Evaluación de riesgos asociados al cambio				
- Planes de				

mitigación de riesgos y contingencia				
- Monitoreo y evaluación de los riesgos durante y después del cambio				
Participación y Empoderamiento				
- Involucramiento del personal en el proceso de cambio				
- Empoderamiento del personal para implementar el cambio				
- Retroalimentación y reconocimiento del personal				
Evaluación y Mejora Continua				
- Evaluación periódica de la gestión del cambio				
- Implementación de mejoras y lecciones aprendidas				

Esta matriz permitirá evaluar y analizar diferentes aspectos relacionados con la estrategia de respaldo y recuperación de datos del data center.

Aspecto	Descripción	Evaluación (Alto/Medio/Bajo)	Observaciones	Acciones Recomendadas
Políticas y Procedimientos				
- Existencia de políticas y procedimientos de respaldo y recuperación de datos				
- Claridad y accesibilidad de las políticas y procedimientos				

- Cumplimiento de las políticas y procedimientos por parte del personal				
Estrategia de Respaldo				
- Frecuencia de respaldos programados				
- Métodos y tecnologías utilizadas para el respaldo de datos				
- Almacenamiento y ubicación de los respaldos				
Estrategia de Recuperación				
- Tiempo objetivo de recuperación (RTO)				
- Procedimientos y herramientas para la recuperación de datos				
- Pruebas y simulacros de recuperación				
Monitoreo y Mantenimiento				
- Monitoreo regular de los respaldos				
- Mantenimiento y actualización de las soluciones de respaldo y recuperación				
- Seguimiento de los registros de respaldo y recuperación				
Evaluación y Mejora Continua				
- Evaluación				

periódica de la estrategia de respaldo y recuperación				
- Implementación de mejoras y lecciones aprendidas				

Matriz de Análisis de Monitoreo y Supervisión del Data Center de la Universidad Técnica deBabahoyo

Aspecto	Descripción	Evaluación (Alto/Medio/Bajo)	Observaciones	Acciones Recomendadas
Herramientas de Monitoreo				
- Existencia de herramientas de monitoreo de infraestructura y servicios				
- Cobertura de los elementos clave del data center (servidores, redes, energía, etc.)				
- Capacidad de detección de problemas y alertas tempranas				
Procesos de Monitoreo				
- Definición de métricas y umbrales de monitoreo				
- Procedimientos para la revisión y análisis de datos de monitoreo				
- Integración de los datos de monitoreo en un panel centralizado				

Supervisión de la Seguridad				
- Monitoreo de eventos de seguridad y registros de actividad				
- Supervisión de la detección de intrusiones y ataques				
- Análisis de vulnerabilidades y evaluación continua de la seguridad				
Planes de Acción y Resolución				
- Procedimientos para la respuesta a eventos y problemas				
- Escalado y asignación de responsabilidades en caso de incidentes				
- Registro y seguimiento de las acciones de resolución				
Mejora Continua				
- Evaluación periódica de la efectividad del monitoreo y la supervisión				
- Implementación de mejoras y optimización de los procesos				

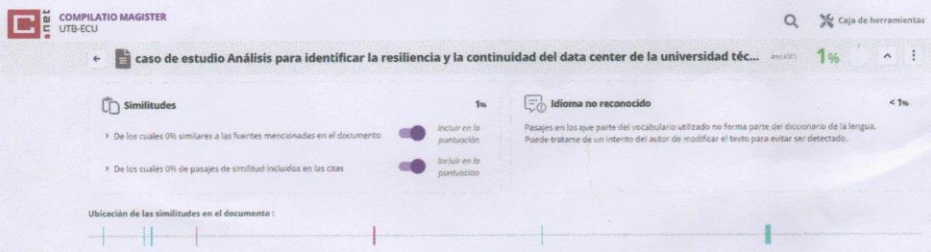
UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
CARRERA DE INGENIERIA EN SISTEMAS DE INFORMCION

Babahoyo, 11 de Septiembre del 2023

CERTIFICACIÓN DE PORCENTAJE DE SIMILITUD CON OTRAS FUENTES EN EL SISTEMA DE ANTIPLAGIO

En mi calidad de Tutor del Trabajo de la Investigación de el, Sr. **REMACHE GUERRERO JESSICA**, cuyo tema es: ***ANÁLISIS PARA IDENTIFICAR LA RESILIENCIA Y LA CONTINUIDAD DEL DATA CENTER DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO***, certifico que este trabajo investigativo fue analizado por el Sistema Antiplagio Compilatio , obteniendo como porcentaje de similitud de **[1 %]**, resultados que evidenciaron las fuentes principales y secundarias que se deben considerar para ser citadas y referenciadas de acuerdo a las normas de redacción adoptadas por la institución y Facultad.

Considerando que, en el Informe Final el porcentaje máximo permitido es el 10% de similitud, queda aprobado para su publicación.



Por lo que se adjunta una captura de pantalla donde se muestra el resultado del porcentaje indicado.

ING. SOTO VALLE CARLOS JULIO
DOCENTE TUTOR DE LA FAFI.

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
DECANATO

Babahoyo, 17 de agosto del 2023
D-FAFI-UTB-00562-2023

Ingeniero.
Marcos Oviedo Rodríguez, Ph.D.
RECTOR DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO
En su despacho. -

De mis consideraciones:

Reciba un cordial saludo por parte de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo, donde formamos profesionales altamente capacitados en los campos de Tecnologías de la Información y de Administración, competentes, con principios y valores cuya practica contribuye al desarrollo integral de la sociedad, es por ello que buscamos prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

La señorita **JESSICA LORENA REMACHE GUERRERO** con cédula de identidad No. **1206951749** estudiante de la Carrera de Ingeniería en Sistemas de Información, matriculada en el proceso de titulación en el periodo junio – octubre 2023, trabajo de titulación modalidad Estudio de Caso, previo a la obtención del grado académico profesional universitario de tercer nivel como Ingeniera en Sistemas de Información, solicita por intermedio del Decanato de esta Facultad el debido permiso para realizar su proyecto, en el departamento de sistemas de la Universidad Técnica de Babahoyo, el cual titula: **"ANÁLISIS PARA IDENTIFICAR LA RESILENCIA Y LA CONTINUIDAD DEL DATA CENTER DE LA UNIVERSIDAD TÉCNICA DE BABAHOYO".**

Atentamente,

Lcdo. Eduardo Galeas Guijarro, MAE.
DECANO
c.c: Archivo

UNIVERSIDAD TÉCNICA DE BABAHOYO
RECTORADO
RECIBIDO
FECHA 30/08/2023 HORA 9:16
SECRETARIA