

**Estrategia de monitoreo integral proactivo, apoyada en el protocolo SNMP para
servidores, redes de comunicaciones y elementos de seguridad del data center en la
empresa Transportes Gayco S.A.S**

Cesar Enrique Silva Garcia

Asesor

Mariano Esteban Romero Torres

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería ECBTI

Maestría en Gestión de T.I

2026

Agradecimientos

Expreso mi más sincero agradecimiento a la **empresa Transportes Gayco S.A.S.**, por brindarme la oportunidad de desarrollar este trabajo de investigación y por facilitar el acceso a la información y al entorno tecnológico necesario para llevar a cabo este estudio. Su apoyo y disposición fueron fundamentales para la realización de este proyecto.

Agradezco también a mi asesor, **Mariano Esteban Romero Torres**, por su orientación, acompañamiento y valiosos aportes durante el desarrollo de este trabajo. Su experiencia, conocimiento y guía académica fueron esenciales para estructurar y consolidar esta investigación.

De igual manera, expreso mi gratitud a la **Universidad Nacional Abierta y a Distancia (UNAD)** por la formación académica brindada y por proporcionar las herramientas y el conocimiento necesarios para el desarrollo de este proceso de aprendizaje y crecimiento profesional.

Finalmente, agradezco a todas aquellas personas que, directa o indirectamente, contribuyeron con su apoyo y motivación para la culminación de este trabajo de grado. Correspondiente la maestría en Gestión de T.I.

Dedicatoria

Dedico este trabajo de grado, en primer lugar, a mi familia, quienes han sido el motor que impulsa cada uno de mis esfuerzos y metas. Cada logro alcanzado es reflejo del amor, la motivación y el compromiso que siento por ellos.

De manera muy especial, dedico este trabajo a mi esposa Mónica Arboleda, quien ha sido mi compañera incondicional en este camino. Su apoyo, comprensión y paciencia durante este proceso han sido fundamentales para culminar esta etapa académica.

A mis hijos, Isabella Silva y Ángel Silva, quienes representan mi mayor inspiración. Todo el esfuerzo y empeño que coloco en cada meta que persigo lo hago pensando en brindarles un mejor ejemplo y un futuro lleno de oportunidades.

Este logro también es para ustedes, porque son la razón que me impulsa a seguir creciendo, aprendiendo y superándome cada día.

Resumen

Se pretende realizar el diseño de un sistema de monitoreo integral en la empresa Transportes Gayco S.A.S, utilizando una metodología mixta que permita hacer seguimiento a los elementos que componen el cuarto de equipos, tales como: servidores (monitoreando memoria, discos duros, procesadores, tarjetas de red y logs del sistema); elementos de telecomunicaciones, como routers, switches, UTM y dispositivos inalámbricos; elementos complementarios, como aires acondicionados, UPS, planta eléctrica; y elementos de seguridad perimetral, como cámaras, sistemas biométricos, apertura de puertas, sensores de humedad, humo y temperatura.

Se identificarán los componentes a monitorear mediante análisis y evaluación de riesgos utilizando la metodología Magerit. mediante una matriz de evaluación, se compararán sistemas operativos, aplicaciones, sensores y protocolos para diseñar la solución e integrar componentes y proponer tableros de visualización que faciliten el análisis e interpretación de los resultados.

La propuesta busca centralizar la información de múltiples fuentes en una única plataforma de monitoreo que permite la generación de alertas en tiempo real y la detección temprana de fallas, contribuyendo a mejorar la toma de decisiones, optimizar los tiempos de respuesta ante incidentes y fortalecer la disponibilidad de los servicios, estableciendo una base que permita a la organización evolucionar hacia un modelo de gestión proactiva, alineado con buenas prácticas de gobierno de TI y la continuidad del negocio y la seguridad de la información.

Palabras clave: Monitoreo proactivo, gestión de riesgos, Magerit, gobierno de TI.

Abstract

The aim is to design a comprehensive monitoring system in the company Transportes Gayco S.A.S., using a mixed methodology that allows tracking of the elements that make up the equipment room, such as: servers (monitoring memory, hard drives, processors, network interface cards and system logs); telecommunications elements such as routers, switches, UTM and wireless devices; complementary elements such as air conditioning systems, UPS, power plant; and perimeter security elements such as cameras, biometric systems, door access, humidity, smoke and temperature sensors.

The components to be monitored will be identified through analysis and risk evaluation using the Magerit methodology. Through an evaluation matrix, operating systems, applications, sensors and protocols will be compared to design the solution and integrate components and propose visualization dashboards that facilitate the analysis and interpretation of results.

The proposal seeks to centralize information from multiple sources into a single monitoring platform that enables the generation of real-time alerts and early detection of failures, contributing to improved decision-making, optimizing response times to incidents and strengthening service availability, establishing a foundation that allows the organization to evolve toward a proactive management model, aligned with IT governance best practices and business continuity and information security.

Keywords: Proactive monitoring, risk management, Magerit, IT governance.

Tabla de Contenido

Introducción	19
El Problema de Investigación	20
Descripción del Problema.....	20
Formulación del Problema.....	25
Objetivos.....	25
Objetivo General	25
Objetivos Específicos	26
Justificación	26
Beneficios de Integrar Equipos Complementarios y Auxiliares en la Organización.	30
Beneficios del Monitoreo de Equipos de T.I en Transportes Gayco S.A.S.....	31
Alcance y Delimitación de la Investigación	31
Marco de Referencia	33
Antecedentes.....	33
Marco Teórico	59
Marco Conceptual.....	68
Marco Contextual	72
Marco Legal.....	74
Metodología	76
Enfoque de Investigación	76
Diseño de Investigación.....	76
Categorías o Variables	79
Hipótesis	82

Población:	82
Muestra	83
Técnicas e Instrumentos de Recolección de Información:	83
Técnicas de Recolección de Información	83
Instrumentos de Recolección de Información	84
Técnicas de Análisis de Resultados	84
Validez y Confiabilidad de los Instrumentos	86
Procesamiento de la Información	87
Resultados	89
Definición de los Componentes de Infraestructura TI Susceptibles de Monitoreo en	
Transportes Gayco	89
Inventario de Activos Transportes Gayco S.A.S	89
Valoración de los Activos.....	95
Determinar las Amenazas y Riesgos Asociados a los Activos Tecnológicos.	104
Valoración de Riesgos	106
Selección de los Activos Críticos Data Center Transportes Gayco S.A.S	107
Proponer un Conjunto de Métricas y Componentes Específicos a Monitorear para Cada	
Activo Crítico Identificado	110
Comparación de Sistemas Operativos, Aplicaciones, Sensores, Protocolos y Componentes	
Electrónicos a Través de una Matriz de Evaluación que Permita Seleccionar los Componentes	
más Eficientes de Monitoreo para Generación de Alertas en Tiempo Real.	113
Sistemas Operativos Recomendados para el Monitoreo de Data Center.....	113
Aplicaciones para el Monitoreo Integral o Parcial de Data Center	115

Sensores y Componentes Electrónicos para el Monitoreo Integral del Datacenter	118
Protocolos de Monitoreo	127
Matriz de Evaluación de Sistemas Operativos	151
Matriz de Evaluación de Aplicaciones y Herramientas	158
Matriz de Evaluación de Sensores y Componentes Electrónicos	167
Matriz de Evaluación de Protocolos.	180
Análisis Costo-Beneficio y Viabilidad de Implementación de las Herramientas de Monitoreo	202
Diseño de los Elementos para Instalación de Agentes en Dispositivos, Configuración SNMP, Definición de Alertas y Visualización de Métricas, para la Implementación de la Estrategia	211
Arquitectura Lógica y Física de la Plataforma de Monitoreo	211
Matriz de Evaluación de OIDs/MIBs	224
Matriz Polling vs Trap	226
Plantilla SNMPv3 Estándar	228
Propuesta de Visualización de Métricas de Monitoreo de Infraestructura TI	233
Diseño Dashboard Ejecutivo.	234
Diseño Dashboard Rendimiento de Servidores	236
Diseño Dashboard Rendimiento de Red	237
Diseño Dashboard Seguridad del Data Center	239
Diseño Dashboard Energía y Ambiente.	240
Diseño Dashboard SLA y Gestión de Disponibilidad.	242
Diseño Dashboard Monitoreo de Aplicaciones	243
Impacto Esperado de la Estrategia de Monitoreo Integral	244

Conclusiones	247
Recomendaciones	248
Referencias Bibliográficas	249
Apéndices.....	264

Lista de Figuras

Figura 1 <i>Diagrama del Arbol de Problemas Sobre la Falta de Sistemas Integrales de Monitoreo para Data Center en Pymes en Colombia</i>	20
Figura 2 <i>Distribución de los Principales Tipos de Ciberataques a Nivel Mundial.....</i>	27
Figura 3 <i>Principales Riesgos Empresariales en Colombia y Relevancia de los Ciberataques Como Amenaza Global</i>	29
Figura 4 <i>Porcentaje de Activos por Nivel de Riesgo</i>	110
Figura 5 <i>Diseño Físico de la Solución de Monitoreo Integral para el Cuarto de Equipos de Gayco S.A.S.....</i>	212
Figura 6 <i>Tipo de Cable Empleado en la Infraestructura del Sistema de Monitoreo.....</i>	213
Figura 7 <i>Diseño Lógico de la Arquitectura de Monitoreo Representado Mediante ArchiMate</i>	217
Figura 8 <i>Dashboard Ejecutivo para el Monitoreo Integral del Data Center de Transportes Gayco S.A.S.....</i>	234
Figura 9 <i>Dashboard de Monitoreo del Rendimiento de Servidores del Data Center de Transportes Gayco S.A.S.</i>	236
Figura 10 <i>Dashboard de Monitoreo del Rendimiento de Red del Data Center de Transportes Gayco S.A.S.....</i>	237
Figura 11 <i>Dashboard de Monitoreo de Seguridad del Data Center de Transportes Gayco S.A.S.</i>	239
Figura 12 <i>Dashboard de Monitoreo de Energía y Ambiente del Data Center de Transportes Gayco S.A.S.....</i>	240
Figura 13 <i>SLA y Gestión de Disponibilidad del Sistema de Monitoreo del Data Center de Transportes Gayco S.A.S.</i>	242

Figura 14 *Dashboard de Monitoreo de Aplicaciones del Data Center de Transportes Gayco*

S.A.S. 243

Lista de Tablas

Tabla 1 <i>Nomenclatura de Activos</i>	89
Tabla 2 <i>Inventario de Activos de Información de la Categoría Datos de Transportes Gayco....</i>	90
Tabla 3 <i>Inventario de Activos de Información de la Categoría Claves Criptográficas de Transportes Gayco.....</i>	91
Tabla 4 <i>Inventario de Activos de Información de la Categoría Hardware de Transportes Gayco</i>	91
Tabla 5 <i>Inventario de Activos de Información de la Categoría Redes y Comunicaciones de Transportes Gayco.....</i>	92
Tabla 6 <i>Inventario de Activos de Información de la Categoría Soportes de Información de Transportes Gayco.....</i>	92
Tabla 7 <i>Inventario de Activos de Información de la Categoría Software de Aplicaciones de Transportes Gayco.....</i>	93
Tabla 8 <i>Inventario de Activos de Información de la Categoría Personal de Transportes Gayco</i>	94
Tabla 9 <i>Inventario de Activos de Información de la Categoría Servicios de Transportes Gayco</i>	94
Tabla 10 <i>Inventario de Activos de Información de la Categoría Elementos Auxiliares de Transportes Gayco.....</i>	95
Tabla 11 <i>Inventario de Activos de Información de la Categoría Instalaciones de Transportes Gayco</i>	95
Tabla 12 <i>Criterios de Valoración</i>	96
Tabla 13 <i>Descripción de las Dimensiones de Valoración</i>	97
Tabla 14 <i>Valoración de Impacto de los Activos de Información de la Categoría Datos</i>	98

Tabla 15 <i>Valoración de Impacto de los Activos de Información de la Categoría Claves Criptográficas</i>	99
Tabla 16 <i>Valoración de Impacto de los Activos de Información de la Categoría Hardware</i>	99
Tabla 17 <i>Valoración de Impacto de los Activos de Información de la Categoría Redes y Comunicaciones</i>	100
Tabla 18 <i>Valoración de Impacto de los Activos de Información de la Categoría Soportes de Información</i>	101
Tabla 19 <i>Valoración de Impacto de los Activos de Información de la Categoría Software de Aplicaciones</i>	101
Tabla 20 <i>Valoración de Impacto de los Activos de Información de la Categoría Servicios</i>	102
Tabla 21 <i>Valoración de Impacto de los Activos de Información de la Categoría Personal</i>	102
Tabla 22 <i>Valoración de Impacto de los Activos de Información de la Categoría Elementos Auxiliares</i>	103
Tabla 23 <i>Valoración de Impacto de los Activos de Información de la Categoría Instalaciones</i>	103
Tabla 24 <i>Valoración de la Amenaza en Cuanto a Frecuencia</i>	104
Tabla 25 <i>Matriz de Degradación Según el Nivel de Impacto</i>	105
Tabla 26 <i>Matriz de Riesgo</i>	106
Tabla 27 <i>Nivel de Riesgo</i>	107
Tabla 28 <i>Riesgo Total por Activo</i>	108
Tabla 29 <i>Cantidad de Activos por Nivel de Riesgo</i>	109
Tabla 30 <i>Activos con Riesgo Extremo</i>	111
Tabla 31 <i>Criterios para la Evaluación de Sistemas Operativos</i>	151

Tabla 32 <i>Evaluación de Sistemas Operativos Según el Criterio de Funcionalidad para Monitoreo</i>	152
Tabla 33 <i>Evaluación de Sistemas Operativos Según el Criterio de Criterios Técnicos</i>	153
Tabla 34 <i>Evaluación de Sistemas Operativos Según el Criterio de Seguridad</i>	154
Tabla 35 <i>Evaluación de Sistemas Operativos Según el Criterio de Operación y Mantenimiento</i>	155
Tabla 36 <i>Evaluación de Sistemas Operativos Según el Criterio de Costos</i>	156
Tabla 37 <i>Evaluación de Sistemas Operativos Según el Criterio de Alineación Estratégica y Riesgos</i>	157
Tabla 38 <i>Criterios para la Evaluación de Aplicaciones y Herramientas de Monitoreo</i>	159
Tabla 39 <i>Evaluación de Aplicaciones y Herramientas de Monitoreo Según el Criterio de Funcionalidad para Monitoreo</i>	159
Tabla 40 <i>Evaluación de Aplicaciones y Herramientas de Monitoreo Según el Criterio de Criterios Técnicos</i>	161
Tabla 41 <i>Evaluación de Aplicaciones y Herramientas de Monitoreo Según el Criterio de Seguridad</i>	162
Tabla 42 <i>Evaluación de Aplicaciones y Herramientas de Monitoreo Según el Criterio de Operación y Mantenimiento</i>	163
Tabla 43 <i>Evaluación de Aplicaciones y Herramientas de Monitoreo Según el Criterio de Costos</i>	164
Tabla 44 <i>Evaluación de Aplicaciones y Herramientas de Monitoreo Según el Criterio de Alineación Estratégica</i>	165
Tabla 45 <i>Criterios para la Evaluación de Sensores y Componentes Electrónicos</i>	167

Tabla 46 <i>Evaluación de Sensores de Temperatura Según Criterios Técnicos y Operativos.....</i>	168
Tabla 47 <i>Evaluación de Sensores de Humedad Según Criterios Técnicos y Operativos</i>	169
Tabla 48 <i>Evaluación de Sensores de Detección de Agua según Criterios Técnicos y Operativos</i>	170
Tabla 49 <i>Evaluación de Sensores de Detección de Agua Según Criterios Técnicos y Operativos</i>	171
Tabla 50 <i>Evaluación de Sensores de Detección de Humo e Incendio Según Criterios Técnicos y Operativos.....</i>	172
Tabla 51 <i>Evaluación de Sensores de Detección de Humo e Incendio Según Criterios Técnicos y Operativos.....</i>	173
Tabla 52 <i>Evaluación de Sensores de Apertura y Estado Según Criterios Técnicos y Operativos</i>	174
Tabla 53 <i>Evaluación de Sensores de Apertura y Estado Según Criterios Técnicos y Operativos</i>	174
Tabla 54 <i>Evaluación de Unidades de Distribución de Energía Según Criterios Técnicos y Operativos.....</i>	175
Tabla 55 <i>Evaluación de Unidades de Distribución de Energía Según Criterios Técnicos y Operativos.....</i>	176
Tabla 56 <i>Evaluación de Tableros Inteligentes Según Criterios Técnicos y Operativos.....</i>	177
Tabla 57 <i>Evaluación de Breakers Inteligentes Según Criterios Técnicos y Operativos</i>	178
Tabla 58 <i>Evaluación de Breakers Inteligentes Según Criterios Técnicos y Operativos</i>	179
Tabla 59 <i>Criterios para la Evaluación de Protocolos de Monitoreo</i>	181
Tabla 60 <i>Evaluación de Protocolos SNMP Según Criterios Técnicos y Operativos.....</i>	182

Tabla 61 <i>Evaluación de Protocolos Syslog Según Criterios Técnicos y Operativos</i>	183
Tabla 62 <i>Evaluación de Protocolos Modbus Según Criterios Técnicos y Operativos</i>	184
Tabla 63 <i>Evaluación de Protocolos BACnet Según Criterios Técnicos y Operativos</i>	185
Tabla 64 <i>Evaluación de Protocolos de Comunicación Serie Según Criterios Técnicos y Operativos</i>	186
Tabla 65 <i>Evaluación de Protocolos Fieldbus Según Criterios Técnicos y Operativos</i>	188
Tabla 66 <i>Evaluación de Protocolos MQTT Según Criterios Técnicos y Operativos</i>	189
Tabla 67 <i>Evaluación de Protocolos AMQP Según Criterios Técnicos y Operativos</i>	190
Tabla 68 <i>Evaluación de Protocolos HTTP(S) Según Criterios Técnicos y Operativos</i>	191
Tabla 69 <i>Evaluación de Protocolos REST Según Criterios Técnicos y Operativos</i>	192
Tabla 70 <i>Evaluación de Variantes del Protocolo WebSocket Según Criterios Técnicos y Operativos</i>	193
Tabla 71 <i>Evaluación de Variantes del Protocolo SMTP Según Criterios Técnicos y Operativos.</i>	194
Tabla 72 <i>Evaluación de Variantes SMS Según Criterios Técnicos y Operativos (Parte 1)</i>	195
Tabla 73 <i>Evaluación de Variantes SMS Según Criterios Técnicos y Operativos (Parte 2)</i>	196
Tabla 74 <i>Evaluación de Mecanismos de Notificación Tipo Push Según Criterios Técnicos y Operativos</i>	197
Tabla 75 <i>Evaluación de Variantes del Protocolo NTP Según Criterios Técnicos y Operativos</i>	198
Tabla 76 <i>Evaluación de Protocolos SSH Según Criterios Técnicos y Operativos</i>	199
Tabla 77 <i>Evaluación de Protocolos Analógicos Según Criterios Técnicos y Operativos</i>	200
Tabla 78 <i>Equipos de Monitoreo Seleccionados y Costos Estimados de Implementación para la Estrategia de Monitoreo Integral</i>	202

Tabla 79 <i>Relación Entre los Principales Riesgos Identificados y los Equipos de Monitoreo Propuestos</i>	205
Tabla 80 <i>Estimación de Pérdidas Potenciales por Incidentes Críticos</i>	208
Tabla 81 <i>Variables Utilizadas para el Cálculo del ROSI de la Solución de Monitoreo Propuesta</i>	209
Tabla 82 <i>Integración Física y Comunicación de los Activos del Sistema de Monitoreo</i>	214
Tabla 83 <i>Arquitectura Lógica de la Capa de Negocio (Business) Según ArchiMate</i>	218
Tabla 84 <i>Capa de Aplicación del Diseño Lógico del Sistema de Monitoreo</i>	220
Tabla 85 <i>Capa de Tecnología del Diseño Lógico – Servicios Tecnológicos y su Realización..</i>	221
Tabla 86 <i>Capa de Tecnología del Diseño Lógico – Conectividad Física y Asociaciones Tecnológicas</i>	222
Tabla 87 <i>Matriz de OIDs y MIBs para el Sistema de Monitoreo</i>	225
Tabla 88 <i>Matriz Polling vs. Trap para la Recolección de Métricas SNMP</i>	227
Tabla 89 <i>Plantilla SNMP Estándar para el Switch Core</i>	229
Tabla 90 <i>Plantilla SNMP Estándar para Routers ISP</i>	230
Tabla 91 <i>Plantilla SNMP Estándar para el UTM/Firewall</i>	231
Tabla 92 <i>Plantilla SNMP Estándar para la UPS del Sistema de Monitoreo</i>	232
Tabla 93 <i>Análisis Comparativo General del Estado del Monitoreo Antes y Después de la Implementación de la Estrategia Integral</i>	246

Lista de Apéndices

Apéndice A <i>Valoración Detallada de Amenazas de los Activos de Información de Transportes Gayco</i>	264
Apéndice B <i>Valoración de Riesgos Activos de Información Transportes Gayco.....</i>	306
Apéndice C <i>Activos Críticos Transportes Gayco</i>	345
Apéndice D <i>Identificación de Elementos y Componentes a Monitorear en el Data Center</i>	393

Introducción

En el contexto empresarial actual, donde la disponibilidad y rendimiento de los data centers son pilares fundamentales para la continuidad operativa, resulta estratégico implementar sistemas de monitoreo efectivos. Este estudio aborda específicamente la identificación y supervisión de componentes críticos en el data center de Transportes Gayco S.A.S. mediante el protocolo SNMP, considerando la dependencia crítica de la organización hacia sus sistemas tecnológicos.

El análisis se estructura en cuatro fases clave: primero, la aplicación de la metodología Magerit para evaluar vulnerabilidades y amenazas en dimensiones operacionales esenciales para determinar cuáles son los activos críticos de la organización, segundo, la identificación de diferentes componentes y herramientas para monitoreo de activos, tercero, el diseño e integración de los elementos para instalación de agentes en los dispositivos y por último se proponen tableros de visualización de las diferentes métricas dadas por los activos monitoreados que permitan interpretar fácilmente los resultados obtenidos.

Esta metodología integral busca establecer un marco de supervisión tecnológica que priorice los elementos más sensibles de la infraestructura, contribuyendo significativamente a la optimización de los procesos de gestión preventiva y al fortalecimiento de la eficiencia operacional en entornos tecnológicos críticos.

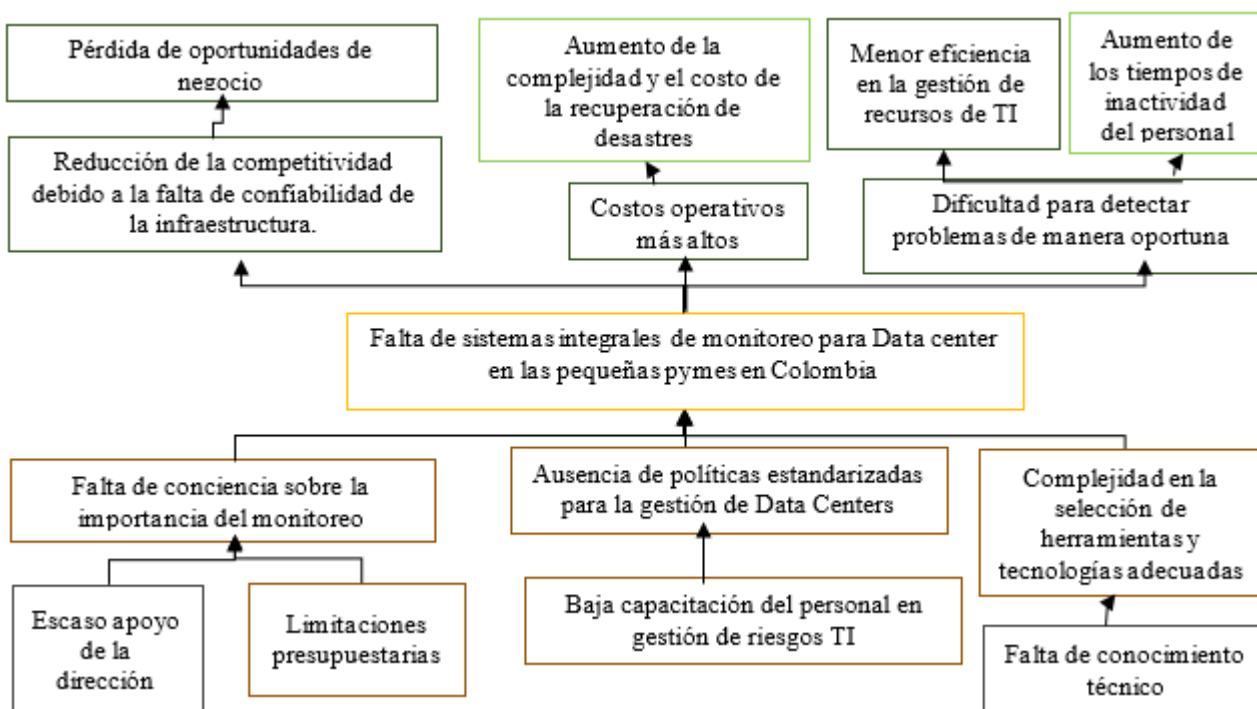
El Problema de Investigación

Descripción del Problema

La Figura 1 presenta una visión general del contexto en el que se enmarca el problema, permitiendo identificar de manera clara los elementos principales y su interacción, mediante esta representación se evidencian las condiciones actuales y los factores que influyen en la situación analizada, sirviendo como punto de partida para comprender la problemática.

Figura 1

Diagrama del Arbol de Problemas Sobre la Falta de Sistemas Integrales de Monitoreo para Data Center en Pymes en Colombia



Nota. Elaboración propia con base en el análisis de causas y efectos asociados a la falta de sistemas integrales de monitoreo para Data Centers en las pequeñas y medianas empresas de Colombia.

Uno de los grandes problemas que enfrenta la monitorización de equipos se centra en cuatro componentes que afectan a todos los sistemas de monitoreo a nivel mundial los cuales se tienen que tener en cuenta a la hora de realizar nuevas soluciones, el primero de estos componentes es la escalabilidad, la simple monitorización de sistemas inalámbricos requiere la agregación y análisis de grandes volúmenes de datos que con el tiempo hace que su crecimiento se pueda dar de manera exponencial.

Otro componente que se aborda como una problemática a resolver en el entorno mundial es la heterogeneidad, debido a que en el monitoreo de entornos inalámbricos se utilizan múltiples dispositivos, protocolos, plataformas, sistemas operativos y otros entornos los cuales son un desafío al momento de establecer un alcance general y cubrir todas las variables a monitorear

Además, también se debe enfatizar la importancia de que estos monitoreos se realicen en tiempo real, una gran cantidad de organizaciones a nivel mundial no toman decisiones de manera rápida y oportuna por la poca capacidad o inexistencia de sus sistemas de monitoreo dando cabida a reparaciones costosas o fallos de seguridad poniendo en riesgo los datos y activos de información de la organización.(Itaya et al., 2023)

Los data centers actuales a nivel mundial trabajan en entornos altamente complejos, compuestos por una multitud de componentes interconectados (servidores, redes, almacenamiento, aplicaciones, sistemas complementarios y de seguridad, etc.). Esta complejidad dificulta significativamente la tarea de monitorear y comprender el estado general del sistema, la interconexión entre los diferentes elementos que componen un data center hace que una falla en un elemento pueda afectar el funcionamiento de otros, lo que a su vez puede desencadenar una cascada de problemas y alertas confusas que no permitan identificar eficientemente la raíz del problema, asimismo los data centers son entornos dinámicos, donde la carga de trabajo, la

configuración y la topología de la red pueden cambiar en cualquier momento, esto produce que sea difícil mantener un diagnóstico adecuado y preciso de la salud del sistema.(Kulikov, 2020)

La falta de una plataforma de monitoreo unificada y escalable y personalizada que pueda manejar múltiples cantidades de equipos y protocolos presentes en un data center, y que además permita visualizar y analizar los datos de manera efectiva para detectar problemas y optimizar el rendimiento, es un talón de Aquiles para las organizaciones que buscan controlar eficientemente la salud de sus activos de información para responder proactivamente a fallos.(Nagano et al., 2021)

Según (Alsadhan & Park, 2021) otro de los inconvenientes principales que se presentan a nivel internacional es la detección proactiva de amenazas en entornos de data center con múltiples activos y volúmenes de información elevados, debido a que no solo es importante detectar incidentes de seguridad ya ocurridos, sino también anticiparse a posibles ataques y fallas.

Por último, la necesidad de coordinar y sincronizar un gran número de dispositivos con capacidades computacionales limitadas, que operan en entornos dinámicos y heterogéneos, al ser autónomos, la toma de decisiones locales basadas en su propia información puede llevar a incoherencias en la toma de decisiones globales y a una falta de visión unificada del sistema, debido a que mantener una sincronización precisa entre los dispositivos, es crucial para garantizar la coherencia de los datos y la toma de decisiones coordinada. Sin embargo, las latencias de comunicación y los errores de sincronización pueden introducir incoherencias que afecten los datos obtenidos y no obtener los resultados esperados obteniendo falsos positivos u omisión de información.(Forti et al., 2021)

Colombia presenta condiciones climáticas variables que pueden afectar el funcionamiento de los equipos del data center. Las fallas en aires acondicionados o dispositivos de control de temperatura pueden ocasionar daños críticos en los equipos fundamentales de la organización debido a la carga de trabajo a la que se someten los diferentes dispositivos que se encuentran en el cuarto de equipos generando temperaturas altas, sobre todo en ciudades a nivel del mar donde su temperatura promedio es superior a los 22° de manera constante.(Andrés et al., 2021)

Según (Cevallos Velásquez, 2022) Colombia, se encuentra localizado en el Cinturón de Fuego del Pacífico. Dicha ubicación lo convierte en un país con un nivel de amenaza sísmica alta, esto puede afectar a los pequeños data center que se encuentran en zonas donde los sismos son recurrentes y pueden afectar la disponibilidad de la información de las organizaciones,

Las empresas en Colombia poco o nada tienen en cuenta la regulación del país referente a la seguridad de la información, aunque esta es exigente en cuanto al manejo de información confidencial, información de terceros, conservación, borrado y niveles de servicio, resaltando los derechos de autor y los delitos concernientes en la violación de la integridad, confidencialidad y disponibilidad de la información mediante diferentes leyes, decretos, normas y políticas las cuales las organizaciones tienen que tener presente para no incurrir en pérdidas financieras o multas por omisión o desacato. (Andrés Jiménez-Almeira & López, 2023)

(Paola A. Sánchez-Sánchez, 2021) afirma que las PYMES en Colombia, a pesar de enfrentar las mismas amenazas cibernéticas que las grandes corporaciones, operan bajo una desventaja significativa. La falta de recursos especializados, presupuestos limitados y equipos de seguridad reducidos las exponen de manera desproporcionada a ciberataques. Esta brecha en capacidades las vuelve blancos más atractivos para los ciberdelincuentes.

Transportes Gayco tiene un pequeño data center, en esta organización por lo general invierten en equipos adecuados al tamaño de sus procesos y flujo de información, estos equipos son una gran parte del costo del que se invierte en T.I. Los servidores, equipos de telecomunicaciones, complementarios y de seguridad tienen unas características especiales de funcionamiento y de continuidad que hace que su costo sea elevado como también el mantenimiento y la reparación de los mismos. Cuando uno de estos elementos complementarios o de seguridad falla, pueden ocurrir pérdidas en los equipos principales de T.I, tales como sobre calentamiento, daño eléctrico, robo e incendio, esto puede causar afectaciones en la continuidad del negocio de la organización y presentar pérdidas económicas de impacto alto en los objetivos estratégicos de la empresa.

Además de no tener en cuenta elementos vitales para el correcto funcionamiento de los equipos de T.I el monitoreo no se hace de manera integral, se realiza mediante diferentes aplicaciones que tienen los dispositivos por separado y en el mejor escenario se integra monitoreo de Hardware Software y redes mediante aplicaciones de pago por lo general costosas que no integran todos los elementos que componen un centro de datos en las Pymes y las alarmas en ocasiones pueden ignorarse debido a su poca o baja interacción con los administradores del sistema.

En la actualidad, Transportes Gayco S.A.S. enfrenta dificultades en la gestión de su infraestructura tecnológica debido a la ausencia de un sistema integral de monitoreo en su data center, el monitoreo se realiza en ocasiones de forma fragmentada mediante diferentes herramientas y aplicaciones independientes o en los equipos complementarios que no cuentan con ninguna herramienta de monitoreo esta labor no se hace, lo que impide contar con una visión unificada del estado de los equipos y dificulta la detección temprana de fallas esto trae como

consecuencia que los incidentes técnicos se atienden de manera reactiva mas no proactiva, generando tiempos prolongados de reparación (MTTR), una disminución del tiempo medio entre fallas (MTBF) y una baja disponibilidad de los activos críticos.

El estado ideal de la organización implica disponer de una plataforma centralizada de monitoreo capaz de integrar todos los elementos del data center para ofrecer alertas automáticas, análisis predictivos y gestión proactiva es por esto que la brecha entre la situación actual y la deseada radica en la falta de integración, automatización y visibilidad de la infraestructura tecnológica.

Formulación del Problema

¿De qué manera la implementación de una estrategia integral de monitoreo del data center en la empresa Transportes Gayco S.A.S. puede cerrar la brecha existente entre el monitoreo fragmentado actual y un modelo unificado que optimice la gestión de la infraestructura tecnológica, reduzca el tiempo medio entre fallas (MTBF) y el tiempo medio de reparación (MTTR), incrementando la disponibilidad de los activos críticos?

Objetivos

Objetivo General

Desarrollar una estrategia de monitoreo integral de dispositivos TI de un data center, basada en la definición de una arquitectura de monitoreo apoyada en protocolos estandarizados de gestión y supervisión, orientada al mejoramiento de la gestión de fallas y la disponibilidad de los recursos de TI

Objetivos Específicos

Definir los componentes hardware, software, servidores, redes de comunicaciones y elementos de seguridad, mediante un análisis de riesgos, para la determinación de las características susceptibles de monitoreo en la empresa transportes Gayco.

Comparar sistemas operativos, aplicaciones, sensores, protocolos y componentes electrónicos a través de una matriz de evaluación que permita seleccionar los elementos más eficientes para un monitoreo integral.

Diseñar la integración de los elementos de monitoreo de infraestructura TI, a partir de los resultados de las matrices de evaluación previamente definidas, mediante la arquitectura de la solución de monitoreo que abarca los diseños físico y lógico para el establecimiento de una estrategia de monitoreo integral y estructurada.

Proponer un tablero de visualización de métricas de monitoreo, mediante el uso de la herramienta Power BI, a partir de los resultados obtenidos en los objetivos anteriores, con el fin de facilitar el análisis, la interpretación y el seguimiento del estado de la infraestructura TI como apoyo a la toma de decisiones.

Justificación

El monitoreo integral de los equipos de un data center es una medida de seguridad esencial para las pymes. Permite a las empresas reaccionar de manera eficiente ante cualquier tipo de eventualidad presentada para salvaguardar la confidencialidad, integridad y disponibilidad de la información.

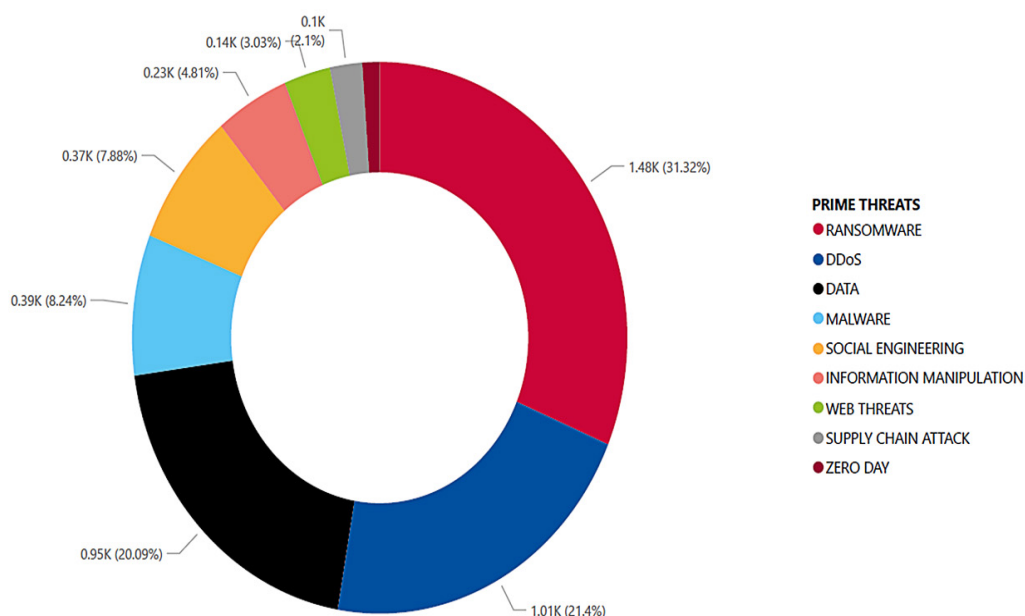
El desaprovechamiento de los recursos, inapropiada detección de errores a nivel hardware, software y red que se presentan tanto por ataques externos como ineficiencias

operativas internas permiten que las herramientas de monitoreo se posesionen cada vez más en el ámbito de la ciberseguridad (Rodas Mendoza, 2022)

En el contexto actual del aumento de ciberataques que según (Maya Horowitz, 2024) en el introduction to the 2024 cyber security report muestra la clasificación de los casos atendidos por el Centro de Respuesta a Incidentes de Ciberseguridad en el año 2023, agrupados según la causa o motivo que originó cada incidente.

Figura 2

Distribución de los Principales Tipos de Ciberataques a Nivel Mundial



Nota. Distribución porcentual de los principales tipos de amenazas de ciberseguridad, donde el *ransomware* representa el mayor porcentaje de incidentes, seguido por los ataques de denegación de servicio (DDoS) y otros tipos de amenazas. **Adaptado de Ciberataques a empresas: amenazas y consecuencias**, por Orange (2023). <https://blog.orange.es/empresas/ciberataques-a-empresas-amenazas-consecuencias/>

La figura 2 muestra como resultado que el Ramsonware es la principal amenaza que aqueja a las empresas a nivel mundial, por esto según(Sood, 2023)Es importante que las empresas identifiquen los riesgos y amenazas para tomar las medidas necesarias de protección, siendo la seguridad en la nube una responsabilidad compartida entre todas las partes interesadas por lo tanto mantener estas a amenaza controladas se convierte en un desafío que hace necesario tener sistema de monitoreo que permita vigilar y conocer en tiempo real la salud de los elementos de T,I de acuerdo a esto (Alsadhan & Park, 2021) asegura que las soluciones de monitoreo recientes no logran integrar eficientemente cantidades significativas de datos dispares de una cantidad determinada de herramientas de seguridad, analizar los datos, priorizar las actividades de remediación e informar de manera tal de orientar la respuesta oportuna y apropiada.

Otro de los desafíos que se enfrentan las organizaciones al momento de seleccionar. Implementar o diseñar una herramienta de monitoreo según (Costa et al., 2022) es la elección de métricas a recopilar para diagnosticar de manera eficiente un activo, esto debido a la creciente demanda de servicios, nuevas tecnologías y datos para recopilar(Abramov & Porkhachev, 2022)

En el ámbito nacional Colombia no se queda atrás en cuanto al elevado riesgo que presenta sus sistemas de información y T.I, según (La República, 2024) los ataques cibernéticos se están consolidando como los principales riesgos para las empresas en el año 2024 consolidando al Ramsonware como una de las amenazas que más afecta a las organizaciones del país detrás de incendios y explosiones, catástrofes naturales e interrupciones del negocio.

Figura 3

Principales Riesgos Empresariales en Colombia y Relevancia de los Ciberataques Como Amenaza Global

TOP 10 DE RIESGOS EN COLOMBIA

	Riesgo	%	2023	Tendencia
1	Incendios y explosiones	46% 	8 (11%)	↑
2	Catástrofes Naturales	43% 	Nuevo	↑
3	Interrupción del Negocio	41% 	2 (39%)	↓
4	Incidentes cibernéticos	30% 	1 (72%)	↓
5	Riesgos políticos y violencia	27% 	Nuevo	↑
6	Cambio climático	22% 	3 (28%)	↓
7	Desarrollos Macroeconómicos	19% 	4 (22%)	↓
8	Robo, fraude, corrupción	14% 	8 (11%)	—
9	Crisis energética	11% 	4 (22%)	↓
10	Desarrollos del mercado	11% 	Nuevo	↑

Fuente: Barómetro de Riesgos de Allianz / Gráfico: LR-GR

Nota. Distribución de los principales riesgos para las empresas en Colombia, donde los incidentes cibernéticos aparecen entre los riesgos más relevantes para las organizaciones.

Adaptado de *Los ataques cibernéticos serán el principal riesgo global para las empresas en 2024*, por La República (2024). <https://www.larepublica.co>

(Lopez Naranjo, 2021) afirma que no solo las amenazas descritas presentan un riesgo alto para las empresas del país, es importante que estas organizaciones cuenten con herramientas que puedan aumentar el nivel de disponibilidad de sus equipos de T.I. independientemente si la falla es de un componente interno o externo sea bien con intención o sin intención de que esta ocurra.

Además(Castaño Saldarriaga, n.d.)sustenta esta afirmación, indicando la importancia del monitoreo constante para la calidad de un servicio en infraestructuras críticas, destacando el incremento del ancho de banda en las organizaciones colombianas y la necesidad de proteger los datos y la infraestructura.

Entre otros elementos clave para la implementación de sistemas de monitoreo en el país se encuentra la mejora de la eficiencia operativa de la organización y algunas circulares o requerimientos de información y ciberseguridad como describe (Mariño-García, 2020) sobre los requisitos de la circular 007 del 2018 que les exige a las instituciones financiera el monitoreo de los logs de sus activos de información.

En el ámbito local, la empresa transportes Gayco S.A.S en sus 21 años de existencia ha presentado desafíos en cuenta a afectaciones en su disponibilidad, confidencialidad e integridad de su información, quedando en ocasiones hasta una semana operando parcialmente o varios días algunos de sus servidores sin operación, esto se presenta por daños en Hardware, Software ocasionado algunas veces por fallos en los equipos auxiliares como lo son UPS o aires acondicionados.

Beneficios de Integrar Equipos Complementarios y Auxiliares en la Organización.

Además de los equipos de TI tradicionales, los data centers modernos también incluyen una serie de equipos complementarios, como UPS, aires acondicionados, sensores de humo, cámaras y sistemas biométricos. La integración de estos equipos en la aplicación de monitoreo permite garantizar el correcto y constante funcionamiento de los activos críticos de la organización.

Beneficios del Monitoreo de Equipos de T.I en Transportes Gayco S.A.S

Alertas en Tiempo real. La aplicación de monitoreo recopila la información suministrada por los diferentes sensores Hardware y software y envía alertas de manera inmediata a los equipos de gestión de incidentes de la organización sobre cualquier anomalía en los equipos que componen el data center. Esto permite a la empresa reaccionar rápidamente ante cualquier evento inesperado como sugiere (Gómez-Rodríguez, 2024) las alertas son una solución exitosa en cuanto a resolver problemas de tráfico excesivo dando una respuesta proactiva a problemas antes de que estos se presenten, además ayudan a minimizar el impacto de una eventualidad.

Reportes para Análisis y Evaluación. La aplicación de monitoreo guarda cada incidencia para posteriores análisis o impresión de reportes. (Abram, 2024) indica que esto ayuda a las empresas a mejorar su comprensión de los riesgos de seguridad y a optimizar sus procesos de gestión de incidentes para la correspondiente toma de decisiones en la organización identificando áreas de cambio, actualización y mejora.

Complemento de Seguridad. La aplicación de monitoreo puede ser un complemento de seguridad para los IDS/IPS, sistemas SIEM, Antivirus y S.G.S.I con que cuente la Transportes Gayco. Como resultado esto ayuda a las empresas a crear una estrategia de seguridad más completa y efectiva.

Alcance y Delimitación de la Investigación

El alcance de la presente investigación se centra en el diseño de una estrategia integral de monitoreo para el data center de la empresa Transportes Gayco S.A.S., abordando de manera estructurada las diferentes capas de la infraestructura tecnológica de la organización.

El estudio inicia con la identificación, inventario y valoración de los activos de información, aplicando la metodología Magerit, con el fin de determinar su nivel de criticidad en cuanto a los riesgos con mayor probabilidad de ser materializados, de acuerdo a esto se establecen los activos críticos que requieren monitoreo continuo (24/7) dentro del entorno del data center.

Posteriormente, la investigación comprende la evaluación y selección de los componentes tecnológicos necesarios para el monitoreo, incluyendo sistemas operativos, herramientas de software, sensores, protocolos de comunicación y elementos electrónicos, mediante el uso de matrices comparativas que permiten identificar las alternativas más eficientes y adecuadas para la organización.

El alcance también incluye el diseño de la arquitectura de la solución de monitoreo, contemplando tanto el enfoque lógico como físico, en donde se define la integración de los diferentes dispositivos, agentes, mecanismos de recolección de datos (como SNMP, Syslog, entre otros) y la configuración de alertas para la gestión de eventos en tiempo real.

Por último, la investigación se extiende hasta la propuesta de visualización de la información, mediante el diseño de dashboards en Power BI simulados, orientados a representar métricas clave de desempeño como lo son, disponibilidad, seguridad, red, energía y ambiente, con el propósito de facilitar el análisis, la toma de decisiones y la gestión proactiva de la infraestructura TI.

En cuanto a la delimitación, el estudio se restringe al diseño de la solución de monitoreo, sin contemplar su implementación física en ambiente productivo, el análisis se enfoca exclusivamente en el data center de la empresa Transportes Gayco S.A.S., sin incluir otras sedes o infraestructuras externas y se limita a los activos identificados dentro del cuarto de equipos.

Marco de Referencia

Antecedentes

A Measurement-Based Power Consumption Model of a Server by Considering Inlet Air Temperatures.

Modelo de consumo de energía de un servidor basado en mediciones que considera la temperatura del aire de entrada, es un artículo de investigación el cual se enfoca en el consumo energético de un servidor en torno a factores térmicos y la eficiencia energética.

Debido a que pocos modelos y estudios tienen en cuenta el aire de entrada, este estudio realizó un mensaje experimental para analizar estos factores. Se evaluó el aire de entrada y la utilización de la CPU en el consumo de energía de los servidores.

En el experimento la temperatura de ingreso a los servidores se ajustó entre los 20 °C a 35 °C y se empezó a incrementar paulatinamente en 5 °C el análisis se hizo con SPECpower_ssj2008 es un punto de referencia estándar de la industria que mide el rendimiento y el consumo de energía de los servidores. Fue desarrollado por la Standard Performance Evaluation Corporation (SPEC) en 2008, esto se utilizó para cambiar las cargas de trabajo de la CPU del servidor de estado inactivo a 100% con intervalos de 10%.

Cuando la temperatura de entrada cambia de 20 °C a 35 °C la potencia aumento 17, 60 W Funcionando en modo de alto rendimiento, en diferentes tipos de modo de funcionamiento del servidor como DAPC y OS el consumo de energía muestra una relación lineal con la temperatura de la CPU esta función se adapta bien cuando la temperatura es inferior a 80 °C Para los modos de funcionamiento de alto rendimiento y estación de trabajo, el consumo de energía del servidor es proporcional a la diferencia de temperatura.

El modo de correlación utilizado en este artículo de investigación puede utilizarse para aplicarse en otros en servidores configurados, esto puede ayudar a las organizaciones a reducir consumos energéticos de manera eficiente. (Jin et al., 2022)

El artículo: A measurement-based power consumption model of a server by considering inlet air temperatures, nos ayuda a responder: ¿Qué elementos, características, equipos y factores internos y externos debo tener en cuenta para realizar monitoreo a equipos de T.I.? debido a que nos indica cómo factores externos como el aire de entrada afectan factores internos como la temperatura de la CPU y a equipos como servidores de diferentes características en su consumo energético.

Smart Monitoring of Wireless Environments with Real-Time Aggregation and Analysis

Monitoreo inteligente de entornos inalámbricos con agregación y análisis en tiempo real. Este artículo científico explica de manera detallada como se ha diseñado un sistema inalámbrico inteligente para la monitorización de entornos en interiores complejos, esto lo hace en fábricas inteligente en tiempo real con Hardware comercial y software de código abierto.

El sistema recopila información de receptores inalámbricos que se encuentran distribuidos, crea celdas espaciales y almacena los datos en contenedores temporales para luego calcular las tramas de datos de métricas inalámbricas espacio- temporales. Para esto se implementaron dos tipos de sensores en el prototipo, el primer sensor de captura de paquetes y el segundo sensor de análisis espectrales, y recopilación, indexación, agregación y análisis automáticos de datos en línea. Este prototipo informa de las métricas de calidad inalámbrica con una resolución espacial a un metro de distancia con tiempos de actualización periódicos inferiores a los 10 segundos.(Itaya et al., 2023)

Este artículo nos ayuda a resolver la siguiente pregunta ¿Qué elementos, características, equipos y factores internos y externos debo tener en cuenta para realizar monitoreo a equipos de T.I.? debido a que nos proporciona información de elementos a tener en cuenta como lo son Hardware y software de dispositivos inalámbricos, características tales como el rendimiento, la disponibilidad y seguridad de dispositivos inalámbricos, factores internos tales como la carga de trabajo, configuración y software de dispositivos inalámbricos.

Empirical Cloud Security: Practical Intelligence to Evaluate Risks and Attacks

Este libro proporciona un enfoque práctico para evaluar los riesgos y ataques de seguridad en la nube. El libro está dirigido a profesionales de la seguridad y la evaluación de riesgos, ingenieros de DevOps, probadores de penetración, ingenieros de seguridad en la nube y desarrolladores de software en la nube que estén interesados en aprender enfoques prácticos para la seguridad en la nube.

Este libro aborda los siguientes temas:

Privacidad de datos: Entre los aspectos importantes encontramos, cumplimiento normativo, gestión del conocimiento y la protección de datos personales.

Evaluación del riesgo y controles de seguridad: como se deben de realizar evaluaciones de riesgo en la nube y como se implementan controles para mitigar los riesgos identificados, también se aborda el análisis de amenazas y vulnerabilidades.

Controles relacionados con la monitorización continua: Se abordan temas como registro, supervisión y análisis de eventos de seguridad.

Recuperación de desastres y continuidad del negocio: Cubre temas como planificación de recuperación de desastres y gestión de continuidad del negocio.

El libro también incluye una serie de casos de estudio reales que muestran cómo se han aplicado los principios y prácticas de seguridad en la nube en el mundo real. (Sood, 2023)

El libro responde a la pregunta ¿Qué beneficios obtienen las empresas de la implementación de un sistema de monitoreo de equipos de T.I.? indicando beneficios específicos como:

Mejora de la disponibilidad: Un sistema de monitoreo de equipos de TI puede ayudar a las organizaciones a detectar y resolver problemas de hardware o software de manera proactiva.

Mejora del rendimiento: Un sistema de monitoreo de equipos de TI ayuda a las empresas a identificar cuellos de botella de rendimiento y tomar medidas efectivas para mejorarlo.

Mejora de la seguridad: Un sistema de monitoreo de equipos de TI ayuda a las empresas a detectar amenazas de seguridad y tomar medidas para mitigarlas.

Mejora de la eficiencia: Un sistema de monitoreo de equipos de TI ayuda a las empresas a ahorrar tiempo y dinero al automatizar tareas que permiten la administración de TI.

Creation of Forecast Algorithm for Networking Hardware Malfunction in the context of small number of breakdowns

Creación de un algoritmo de pronóstico de fallas de hardware de red en el contexto de un pequeño número de averías, este artículo de investigación propone un algoritmo de pronóstico de fallas de hardware de red en el contexto de un pequeño número de averías. El algoritmo se basa en un modelo de aprendizaje automático que se entrena con datos históricos de fallas de hardware de red.

El algoritmo se evaluó utilizando un conjunto de datos de fallas de hardware de red de un centro de datos. Los resultados mostraron que el algoritmo es capaz de predecir fallas de hardware de red con una precisión de más del 80%.

El algoritmo se puede utilizar para ayudar a los administradores de redes a prevenir fallas de hardware de red y a mejorar la disponibilidad de sus redes.

Por ejemplo, si el algoritmo predice que un servidor tiene un alto riesgo de fallar, la empresa puede reemplazar el servidor antes de que falle. Esto puede ayudar a evitar una interrupción del servicio y a ahorrar dinero a la empresa en costos de reparación.

El algoritmo se basa en un modelo de aprendizaje automático que se entrena con datos históricos de fallas de hardware de red. El modelo de aprendizaje automático aprende a identificar patrones en los datos que pueden indicar que un equipo está en riesgo de fallar.

Una vez que el modelo de aprendizaje automático está entrenado, se puede utilizar para predecir la probabilidad de falla de cualquier equipo de la red. Las empresas pueden utilizar estas predicciones para tomar medidas preventivas para evitar fallas de hardware de red. (Myrzatay, 2020)

Este artículo responde a la pregunta ¿Qué elementos, características, equipos y factores internos y externos debo tener en cuenta para realizar monitoreo a equipos de T.I.? mencionando elementos de Hardware, software y datos, características tales como rendimiento, seguridad y disponibilidad, equipos de infraestructura de monitoreo, también en el documento se tienen en cuenta factores internos y externos tales como configuraciones, cargas de trabajo y el ambiente.

Endless'' Workload Analysis of Large-Scale Supercomputers

El artículo científico, Análisis de carga de trabajo "infinito" de supercomputadoras a gran escala, aborda el tema de la complejidad del monitoreo de computadoras a gran escala debido a su importancia en la organización, el tamaño y la carga de trabajo de sus componentes causando así que estos se averíen de vez en cuando por lo tanto estas supercomputadoras requieren una monitorización constante, estos controles se establecen en la práctica diaria de cualquier centro

de datos, hay que prestar atención de la forma que se utilizan estas supercomputadoras y sus recursos informáticos de manera eficiente y completa, siendo un problema que aún está lejos de resolverse, llevando a los administradores de sistemas obtener pocos conocimientos sobre la calidad del flujo de trabajos de su supercomputadora así como las diferentes formas de mejorarla.

En este artículo se presenta un sistema de informes en bucle que nos permiten tener cualquier nivel de detalle de cualquier tipo de aspecto que describa la calidad de carga de trabajo de la súper computadora, desde el sistema general hasta los lanzamientos de trabajos individuales ofreciendo flexibilidad debido a que suministra un nivel infinito de escenarios de carga de trabajo lo que permite determinar diferentes escenarios de degradación y fallo de hardware de supercomputadoras.

Este sistema de informes se basa en el paquete de software TASC el cual tiene como objetivo identificar y analizar temas de rendimiento de las super computadoras. (Shvets & Voevodin, 2021)

Este artículo resuelve a la pregunta ¿Qué elementos, características, equipos y factores internos y externos debo tener en cuenta para realizar monitoreo a equipos de T.I.? Menciona la importancia de monitorear elementos como hardware, software y datos, características como rendimiento, disponibilidad y seguridad, factores internos como el software instalado y las cargas de trabajo en las supercomputadoras y factores externos como el ambiente y la red.

Optical Link Monitoring in Fibre-to-the-x Passive Optical Network (FTTx PON): A Comprehensive Survey

El artículo de revisión Monitoreo de enlaces ópticos en redes ópticas pasivas de fibra hasta el hogar (FTTx PON): Una revisión completa. Sugiere que por la penetración de redes de

fibra ópticas de tipo pasivo en las redes de hogar es necesario mantener la integridad de las mismas. Se establecen mejores prácticas en cuanto a la instalación y mantenimiento de redes de fibra óptica, también es importante monitorear la degradación de la fibra óptica en el tiempo para ofrecer un servicio más eficiente garantizando el nivel de servicio pactado con el cliente. Una falla menor en PON puede resultar en una pérdida masiva de datos debido a la pasividad de los elementos involucrados en la distribución óptica. Desafortunadamente el monitoreo de redes PON no es efectivo debido a la rápida y constante evolución de esta tecnología. Por lo tanto, un sistema de monitoreo puede mejorar la calidad del servicio de manera sustancial.

Debido a esto este estudio presenta una revisión del progreso de rendimiento en sistemas de monitoreo actuales de redes PON, se realiza una investigación acerca de los avances en mejoras de sistemas de rendimiento de enlaces ópticos se tienen en cuenta factores como, la precisión, la medición, velocidad de medición, relación señal a ruido, resolución espacial y rango dinámico, también se compararon los diferentes enfoques existentes buscando un marco de monitoreo ideal para finalmente abordar desafíos y perspectivas en cuanto a esfuerzos en la formulación de un sistema de monitoreo de enlaces ópticos eficaz en PON.(Usman et al., 2020)

El monitoreo de equipos de redes PON es una tarea importante para garantizar el rendimiento y la disponibilidad de los sistemas. Al tener en cuenta los elementos, características, equipos y factores internos y externos mencionados en el artículo, se puede realizar un monitoreo eficaz que ayude a prevenir problemas y mejorar el rendimiento y responder la pregunta ¿Qué elementos, características, equipos y factores internos y externos debo tener en cuenta para realizar monitoreo a equipos de T.I.?

A Real-Time Hardware-in-the-Loop (HIL) Cybersecurity Testbed for+ Power Electronics Devices and Systems in Cyber-Physical Environments

El artículo un banco de pruebas de ciberseguridad en tiempo real de hardware en el bucle (HIL) para dispositivos y sistemas electrónicos de potencia en entornos ciber físicos, La ciberseguridad de la electrónica de potencia (PE) es cada día más esencial, ya que sistemas como energías renovables, almacenamiento de energía y estaciones de carga de vehículos eléctricos utilizan dispositivos PE para conectarse a las redes eléctricas con complejos sistemas de comunicación y computación para el control avanzado y la mejora de la conciencia situacional en entornos de redes inteligentes. Sin embargo, la investigación y el desarrollo de la ciberseguridad de la (PE) se ven obstaculizados por la falta de un banco de pruebas de seguridad en tiempo real que incorpore eventos cibernéticos reales.

Debido a esto se propone un banco de pruebas de ciberseguridad en tiempo real de hardware en el bucle (HIL) para sistemas PE en entornos ciber físicos. El banco de pruebas de seguridad propuesto consta de:

1. un simulador de sistemas PE en tiempo real;
2. un sistema cibernético en tiempo real que utiliza sistemas de red reales y un servidor.
3. herramientas de pruebas de penetración que generan ciberataques reales como eventos cibernéticos.

Se crean varios ciberataques reales y se proporcionan sus impactos en un sistema PE para validar la viabilidad del banco de pruebas de seguridad propuesto.

Los autores utilizan este banco de pruebas para evaluar los efectos de ataques cibernéticos a sistemas PE en red, este banco de pruebas de seguridad puede utilizarse para evaluar la seguridad en nuevos sistemas PE, identificar y corregir vulnerabilidades en estos

sistemas existentes y desarrollar y evaluar medidas de mitigación para los sistemas PE. (J. Choi et al., 2021)

Este artículo responde a la pregunta ¿Por qué es importante el monitoreo de equipos de T.I. en las empresas? Debido a que proporciona un caso de uso específico para el monitoreo de la ciberseguridad de dispositivos y sistemas electrónicos de potencia (PE) en entornos ciber físicos.

Opimon: A Transparent, Low-Overhead Monitoring System for OpenFlow Networks.

Opimon: Un sistema de monitoreo transparente y de bajo impacto para redes OpenFlow: Las redes open Flow son una implementación ampliamente utilizada en la arquitectura de redes por software debido a que los sistemas convencionales de monitoreo son incapaces de abarcar las redes OpenFlow, los investigadores han desarrollado diferentes sistemas que se adaptan a este tipo de redes, sin embargo, estos sistemas dependen de un controlador específico o un API los cuales pueden limitar su aplicabilidad.

Este estudio propone un sistema de monitoreo transparente para redes OpenFlow denominado Opimon este sistema monitorea la topología de la red, las estadísticas de los switches y las tablas de flujo en una red Open Flow el resultado se visualiza a través de una interfaz web en tiempo real. Este sistema monitorea la red

interponiendo un servidor proxy entre el controlador y los switches e intercepta todos los mensajes OpenFlow intercambiados, este diseño permite compatibilidad entre cualquier tipo de Switch o Controlador OpenFlow.

Se probó la funcionalidad de Opimon en una red virtual construida con un banco de pruebas OpenFlow internacional a gran escala (PRAGMA-ENT). Además, medimos la sobrecarga de rendimiento incurrida por Opimon y demostramos que la sobrecarga en términos

de latencia y rendimiento fue inferior al 3% y al 5%, respectivamente. (Watanakeesuntorn et al., 2022)

Este artículo responde a la pregunta: ¿Por qué es importante el monitoreo de equipos de T.I. en las empresas? proporciona información que puede ayudar a las empresas a seleccionar las herramientas y técnicas de monitoreo adecuadas para sus necesidades específicas al proporcionar información sobre los siguientes elementos, características, equipos y factores internos y externos que se deben tener en cuenta para realizar monitoreo a equipos de TI.

Architecture and Key Components of the Improved Digital Center for Monitoring and Management of the National Research Computer Network of Russia.

El artículo, Arquitectura y componentes clave del centro digital mejorado para el monitoreo y la gestión de la red nacional de computadoras de investigación de Rusia pretende enfocarse en el desarrollo y la creación de un nuevo sistema de software para garantizar el funcionamiento eficaz del Centro de Operaciones de Red de la Red Nacional de Computadoras de Investigación de Rusia, El NOC es un centro de control que supervisa y gestiona el funcionamiento de la red. El nuevo sistema de software está diseñado para mejorar la fiabilidad, el rendimiento y la seguridad de la red.

El artículo describe las tareas típicas del NOC, así como el software y las herramientas que se utilizan para resolver las tareas seleccionadas, luego el sistema presenta el estado actual del monitoreo y la gestión de NIKS.

La parte principal del artículo se enfoca en la arquitectura y composición del nuevo sistema, este sistema se basa en una arquitectura distribuida y modular, esto permite que pueda escalar de manera sencilla para satisfacer las necesidades de la red también incluye diferentes tipos de módulos para para monitorear y gestionar las redes.

Otro tema importante que aborda el artículo es describir como el software interactúa con sistemas externos como con el software de facturación para informar sobre el uso de la red de los clientes. (Abramov & Porkhachev, 2022)

El artículo resuelve la pregunta de cómo mejorar la fiabilidad, el rendimiento y la seguridad de una red describiendo el desarrollo de un nuevo sistema de software para el Centro de Operaciones de Red de la Red Nacional de Computadoras de Investigación de Rusia, el cual permite mejorar la fiabilidad y rendimiento de la red ayudando a detectar y a responder problemas de red como un ataque de manera eficaz, mejorando la seguridad de la red.

Monitoring Fog Computing: A Review, Taxonomy and Open Challenges

Monitoreo de la computación de niebla: es un artículo de revisión, donde se revisa la taxonomía y desafíos abiertos, aborda la computación de niebla afirmando que es un paradigma de computación distribuida que extiende la computación en la nube al borde de la red, más cerca de los dispositivos y los usuarios. El sistema de la niebla es el proceso de gestión de los recursos y servicios de la computación para satisfacer las necesidades de los usuarios y aplicaciones. La monitorización es una funcionalidad de organización esencial, ya que permite a los organizadores a recopilar información sobre el estado de los recursos y servicios de la niebla, e identificar y resolver problemas de forma rápida y eficaz.

Existen varias soluciones y herramientas de monitorización en la nube, pero ninguna de ellas está diseñada específicamente para la computación de niebla. Las soluciones de monitorización de la niebla son escasas y es posible que no estén preparadas para componer un servicio organizado.

Además, se presenta una nueva taxonomía de soluciones de monitorización de la niebla, basada en una revisión sistemática de la literatura. La taxonomía identifica tres categorías principales de soluciones de monitorización de la niebla:

monitorización de infraestructura: se monitoriza el estado de los recursos físicos tales como, servidores, redes y dispositivos de almacenamiento.

monitorización de servicios: Monitorizar el estado de los servicios de la niebla, como bases de datos, aplicaciones web y servicios de streaming.

monitorización de extremo a extremo: monitorizar el rendimiento y la disponibilidad de los servicios de la niebla desde la perspectiva del usuario final.

El artículo también tiene en cuenta algunos de los desafíos más importantes:

Heterogeneidad de los recursos y servicios de la niebla, el Dinamismo de la niebla: La computación de niebla es un entorno dinámico, donde los recursos y servicios pueden aparecer y desaparecer rápidamente. Esto dificulta el mantenimiento de una visión actualizada del estado de la niebla y la seguridad y privacidad: La monitorización de la niebla debe realizarse de forma segura y privada, para evitar el acceso no autorizado a datos sensibles.(Costa et al., 2022)

El artículo responde a la siguiente pregunta de investigación: ¿Qué elementos, características, equipos y factores internos y externos debo tener en cuenta para realizar monitoreo a equipos de T.I.? debido a que identifica características tales como disponibilidad, rendimiento y seguridad, equipos entre ellos están herramientas de software, agentes plataformas y servidores de monitoreo e identifica 4 factores internos que se deben tener en cuanto en monitoreo de T.I. entre ellos tenemos la estrategia y la infraestructura de T.I, recursos humanos y costos

An Analytical Computing Infrastructure for Monitoring Dynamic Networks Based on Knowledge Graphs.

El artículo una infraestructura de computación analítica para el monitoreo de redes dinámicas basada en gráficos de conocimiento afirma que el monitoreo de redes dinámicas suele estar diseñado para resolver un número predefinido de tareas. Los nuevos requisitos suponen un costoso esfuerzo de desarrollo y, a veces, incluso requieren cambios en la arquitectura del sistema. Los gráficos de conocimiento son herramientas potentes y flexibles para la integración de información y están respaldados por un conjunto de vocabularios y lenguajes estandarizados (el conjunto de herramientas de la "Web semántica"). En este artículo se discute la aplicación de los gráficos de conocimiento para desarrollar y analizar una infraestructura de computación analítica para un sistema de monitoreo de redes dinámicas. Como ejemplo de red dinámica, se considera una red de telecomunicaciones multiservicio. El sistema presentado combina modelos estáticos de una red de telecomunicaciones y datos de monitoreo dinámicos, y permite obtener informes analíticos complejos mediante consultas SPARQL sobre el gráfico de conocimiento. Estos informes son de crucial importancia para los interesados en la red para mejorar los servicios y el rendimiento de esta.

Los gráficos de conocimiento son una forma de representar datos que permite a las computadoras comprender el significado de los datos y las relaciones entre ellos. Los gráficos de conocimiento se pueden utilizar para representar una amplia gama de información, incluidas las redes dinámicas. (Kulikov, 2020)

El artículo responde a la pregunta ¿Cómo se puede desarrollar un sistema integral para el monitoreo en pymes? Dándonos insumos como la forma en que debemos establecer los objetivos del monitoreo la recolección el almacenamiento la visualización y el análisis de datos.

Architecture of Cloud Telecommunication Network Monitoring Platform Based on Knowledge Graphs.

Arquitectura de una plataforma de monitoreo de redes de telecomunicaciones en la nube basada en gráficos de conocimiento es un artículo científico que describe una nueva plataforma en nube para el monitoreo de redes basada en gráficos de conocimiento los cuales son una forma de representar datos que permiten que las computadoras comprender el significado de estos y relacionarlos entre sí.

Esta plataforma permite a los operadores de telecomunicaciones recibir análisis modernos, mediante el uso de ontología de plataforma flexible, con el objetivo de conectar las RT de los operadores de telecomunicaciones a la plataforma de monitoreo con bajos costos.

Se presenta un ejemplo de estudio de caso en donde en el que se combina segmentos de red de operadores que utilizan diversos sistemas de monitoreo con diferentes ontologías de dominio y se demuestra cómo construir un único informe de múltiples datos de monitoreo en segmentos diferentes. (Kirill Krinkin et al., 2021)

El artículo responde la pregunta ¿Qué beneficios obtienen las empresas de la implementación de un sistema de monitoreo de equipos de T.I.? de la siguiente manera: Mejora la visibilidad el rendimiento y la seguridad en las organizaciones reduciendo costos operativos.

Towards the Automatic and Schedule-Aware Alerting of Internetwork Time Series.

Hacia la Alerta Automática y Consciente del Horario de las Series de Tiempo de Interredes. Un factor importante que puede tener todo sistema de monitoreo de redes es un módulo de alerta para series de tiempo, este módulo tiene como objetivo activar una alerta cuando se detecta algún comportamiento anómalo en los patrones de serie de tiempo, esta

búsqueda de anomalías puede ser supervisada por los administradores del sistema y los umbrales de consideración de anomalías se establecen de manera manual, también esta investigación se centra en cómo realizar esta tarea de manera automática y no supervisada aliviando la carga de los administradores de redes, basándose en la experiencia de monitoreo de docenas de redes se ha desarrollado un reproductor de anomalías reales esto nos ayuda a recrear estos problemas y por lo tanto a parametrizar estos sistemas de alerta sin supervisión. Además, como novedad, En artículo se proponemos considerar la plantilla de los administradores de redes como un parámetro significativo para configurar los umbrales del módulo de alerta, evitando así las alarmas que no recibirán atención. También en este artículo se propone medir y clasificar las alarmas por relevancia, y relacionarlas con el tiempo a resolver para elaborar, cronogramas automáticos para los miembros del personal, según su disponibilidad horaria.

todas estas propuestas se han puesto en práctica en diversos despliegues de sistemas de monitorización en redes en funcionamiento, lo que nos evidencia su utilidad y baja demanda de recursos. (Perdices et al., 2021)

El artículo responde a la pregunta: ¿Qué beneficios obtienen las empresas de la implementación de un sistema de monitoreo de equipos de T.I.? debido a que se centra específicamente en los beneficios de un sistema de monitoreo que utiliza alertas automáticas y de acuerdo al horario de la organización. Estas alertas pueden ayudar a las empresas a identificar problemas de manera más eficiente y oportuna

Lightweight self-organising distributed monitoring of Fog infrastructures

El artículo Monitoreo distribuido ligero autoorganizado de infraestructuras de niebla afirma que las aplicaciones de niebla de última generación tendrán como principal aliado habilitador el monitoreo de infraestructuras manteniendo heterogeneidad de sus plataformas

también la disponibilidad de recursos en el borde entre usuarios y los datos y la alta dinámica de la nube y el IoT.

En este artículo se describe al prototipo de monitoreo FogMon el cual fue diseñado bajo el lenguaje de programación C++ especial ,mente dirigido a infraestructuras de niebla, este prototipo monitoriza los equipos de hardware en diferentes nodos de la infraestructura, la calidad de la red de extremo a extremo en estos nodos y los dispositivos IoT existentes contando con tipología de red de par a par autoorganizada con mecanismos de autoorganización y actualizaciones de monitoreo diferenciales, garantizando la escalabilidad, sobrecarga y tolerancia a fallos, los experimentos realizados en un banco de pruebas real demuestran que la intrusión de FogMon es baja y que la topología utilizada es resistente a las infraestructuras dinámicas.(Forti et al., 2021)

Este artículo de investigación responde a la pregunta ¿Qué elementos, características, equipos y factores internos y externos debo tener en cuenta para realizar monitoreo a equipos de T.I.? puesto que describe elementos tales como recursos de hardware, aplicaciones, datos y seguridad con sus correspondientes características de escalabilidad, tolerancia a fallos y la baja sobre carga en comunicación, en los equipos identifica sensores, agentes y servidores de monitoreo y en factores externos los requisitos regulatorio y amenazas de seguridad.

A Method for Source Detection in Multiple Faults For Telecommunication Systems.

Un método para la detección de fuentes de múltiples fallas en sistemas de telecomunicaciones es un artículo de investigación donde aborda a los sistemas de telecomunicaciones actuales, y la capa de hardware y una gran cantidad de aplicaciones de software que funcionan sobre ella. Teniendo en cuenta los sistemas de soporte a la operación (OSS) que proporcionan el control de esta compleja estructura ofrecen servicios como el

inventario de servidores y redes, el descubrimiento de la topología de la red, la gestión de los registros de la red y la utilización de la capacidad de la red. Aunque los sistemas OSS pueden supervisar los fallos del sistema y los cuellos de botella para el personal de mantenimiento, los sistemas de supervisión de la red existentes son insuficientes para los proveedores de servicios, sus deficiencias son la incapacidad de identificar y notificar el origen de los fallos cuando se producen varios fallos. En este artículo se presenta una capa de detección de fallos OSS que puede analizar los fallos simples y múltiples que se producen en los sistemas de telecomunicaciones, este sistema Puede determinar las fuentes de los fallos con gran rapidez y precisión, y realizar las notificaciones necesarias al personal de soporte pertinente en un corto espacio de tiempo. Probamos el sistema de detección de fallos desarrollado con datos reales y los resultados demuestran que el sistema desarrollado es muy eficaz para determinar los fallos del sistema. (Berk et al., n.d.)

Este artículo resuelve la pregunta: ¿Por qué es importante el monitoreo de equipos de TI en las empresas? demostrando que el monitoreo de equipos de tecnologías de información es esencial para la detección de fallas, mostrando un método de detección de fallas en sistemas de telecomunicaciones utilizando datos de monitoreo para identificar la fuente de los fallos, este principio se puede utilizar para cualquier tipo de sistema de información incluyendo sistemas empresariales.

A Two-Layer Architecture for Failure Prediction Based on High-Dimension Monitoring Sequences

Una arquitectura de dos capas para la predicción de fallas basada en secuencias de monitoreo de alta dimensión es un artículo de investigación que cuenta con los siguientes elementos:

Revisión de la literatura: en este apartado afirma que los métodos de texto que se documentan en trabajos anteriores presentan algunas irregularidades debido a la complejidad de los modelos complejos que se construyen y se limita a realizar una revisión bibliográfica acerca de la predicción y diagnósticos de fallos basados en texto o datos de monitoreo temporal.

Marco de predicción: El artículo presenta un marco de predicción que se compone de dos capas, una capa de predicción de anomalías y otra capa de clasificación que predice si el nodo falla en un tiempo predeterminado.

El marco de predicción se evalúa en conjuntos de datos reales de sistemas distribuidos a gran escala y demuestra ser eficaz para predecir fallos.

Caso de estudio: el autor del artículo recopiló los datos de una de las empresas más grandes de seguridad de china y utilizó su sistema de auto monitorización el cual contiene los siguientes componentes:

Logstash,: Analiza todo tipo de registros.

Kafka: transmite grandes volúmenes de datos a JStorm con baja latencia.

JStorm: Que ofrece agregación y cálculo de datos sobre la marcha.

Elasticsearch: Almacena, busca y analiza grandes cantidades de datos.

El sistema genera alerta cuando se infringe alguna de las reglas establecidas por los administradores, los datos utilizados contienen 30 nodos del componente Elasticsearch, este almacena los datos de negociación que se encuentra centralizado en la empresa.

Estos atributos se están registrando cada minuto desde el 8 de noviembre del 2018 al 22 de noviembre del mismo año además hay más 20.000 observaciones por cada secuencia y menos del 0.5% quedan etiquetadas por el sistema de auto monitorización.

Por último, se procesan los datos agrupándolos y promediando las secuencias cada media hora, esto se realiza en este intervalo de tiempo debido a que entre menos tiempo el monitoreo es más propenso a ruido. (Wang et al., 2021)

Este artículo de investigación responde a la pregunta ¿Qué beneficios obtienen las empresas de la implementación de un sistema de monitoreo de equipos de T.I.? de la siguiente manera: Aborda aspectos de como el monitoreo de alta dimensión mejora la disponibilidad, el rendimiento, y reduce costos en las organizaciones al predecir fallos de manera eficiente y proactiva

Design and Implementation of Device Monitoring SaaS for DIY-IoT Systems.

El artículo de investigación denominado Diseño e implementación de SaaS de monitoreo de dispositivos para sistemas de IoT DIY propone una nueva plataforma de monitoreo como servicio para apoyar a los sistemas IoT desarrollados por usuarios finales, la propuesta consta de tres módulos para monitorear la disponibilidad de diferentes tipos de equipos IoT y permite a los usuarios finales operar su sistema de manera fácil.

Módulos:

Realización de informes de supervivencia en diversos dispositivos IoT.

Interfaz web.

Backend sin servidor.

La investigación demuestra que SDK y el daemon motch son herramientas eficaces para monitorear dispositivos IoT y los costos de funcionamiento son adecuados.(Nagano et al., 2021)

El artículo responde a la pregunta: ¿Qué elementos, características, equipos y factores internos y externos debo tener en cuenta para realizar monitoreo a equipos de TI.? Debido a que tiene en cuenta datos de monitoreo, modelos de análisis y alertas, Características como

disponibilidad, escalabilidad y flexibilidad de los sistemas de monitoreo y factores externos como el ambiente, la integridad de los datos y la seguridad.

Leveraging Information Security Continuous Monitoring to Enhance Cybersecurity

El Artículo de investigación Aprovechar el monitoreo continuo de la seguridad de la información para mejorar la ciberseguridad argumenta la importancia del monitoreo continuo de la seguridad de la información debido a que los ataques a sistemas informáticos federales de EEUU cada vez son más implacables y sofisticados con probabilidades cada vez mayores a causar daños significativos y aunque se invierte más recursos estos ataques siguen creciendo. Es importante la detección oportuna de vulnerabilidades para reducir o eliminar la violación y las consecuencias que esta pueda tener en el sistema. La monitorización continua de la seguridad de la información (ISCM) aprovecha la tecnología para pasar de una ciberseguridad centrada en el cumplimiento a una gestión de riesgos basada en datos, además la monitorización continua permite saber que está sucediendo en tiempo real para responder a las tasas explosivas de vulnerabilidades, amenazas persistentes y enemigos decididos.

A pesar de todo lo prometedor que se analiza en esta tecnología las agencias gubernamentales aun presentan muchos desafíos entono a esta solución, por todo esto en este artículo se aborda la necesidad del monitoreo continuo en la seguridad de la información y su estado actual, se analiza sus desafíos de seguridad y se proponen estrategias futuras para aprovechar de la mejor manera esta tecnología. (Alsadhan & Park, 2021)

Este articulo responde a la pregunta ¿Qué beneficios obtienen las empresas de la implementación de un sistema de monitoreo de equipos de TI.? E ISCM ayuda a las organizaciones a mejorar su seguridad, detectando amenaza y vulnerabilidades en tiempo real

para reaccionar oportunamente a estas violaciones de seguridad mejorando en cuento a la protección de datos y continuidad del negocio.

Monitoring as a Service Over a 5G Network Slice.

Monitoreo como servicio sobre una red 5G, el network slice. Argumenta el funcionamiento de múltiples redes virtuales sobre una infraestructura común, se considera un mecanismo importante para dar servicio a la multitud de inquilinos a los que se dirigen los próximos sistemas de quinta generación (5G), de forma flexible y rentable. Se prevé que uno de los modelos más populares para los clientes sea el modelo de Network Slice as a Service (NSaaS). Este modelo permite a un cliente de servicios de red solicitar y configurar un Network Slice y ofrecerlo como un servicio. Sin embargo, para garantizar que se cumplen los acuerdos de nivel de servicio acordados para el Network Slice entregado, es necesario habilitar mecanismos de monitorización y telemetría a varios niveles de recursos: la infraestructura programable, el núcleo y la red de acceso (RAN) 5G y los recursos del NS. Este artículo presenta un enfoque para ofrecer dichos mecanismos de monitorización y telemetría como un servicio para el emergente modelo de entrega 5G NSaaS.(D. Giannopoulos, 2021)

El artículo Monitoring as a service over a 5G network responde a la pregunta ¿Qué beneficios obtienen las empresas de la implementación de un sistema de monitoreo de equipos de T.I.? mostrando como el monitoreo como servicio permite a las empresas tener una visibilidad completa de las redes 5G permitiendo así a responder a los inconvenientes de seguridad presentados de manera más rápida siendo un servicio flexible que se adapta a las necesidades de cada compañía.

Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Survey.

Aprendizaje profundo para la monitorización y el análisis del tráfico de red (NTMA): Este artículo de revisión bibliográfica documenta la importancia que tiene una revisión completa de las aplicaciones de aprendizaje profundo en la aplicaciones de Monitorización y Análisis del Tráfico de Red debido a el auge de sistemas de comunicación modernas como el IoT y las redes celares que generan una cantidad masiva y heterogénea de datos de tráfico, para estos escenarios la gestión de monitorización de tráfico y análisis enfrenta algunos desafíos y problemas entre estos tenemos la precisión y el procesamiento eficaz de grandes volúmenes de datos en tiempo real y el patrón de trafico de red en las redes celulares, este presenta un comportamiento complejo debido a la movilidad de los dispositivos y la heterogeneidad de la red, el aprendizaje profundo se ha utilizado para analizar grandes volúmenes de datos ocultos y complejos, esto éxitos ha motivado a los investigadores a aplicar modelos de aprendizaje en aplicaciones (NTMA). Como la clasificación y la predicción de tráfico. (Abbasi et al., 2021)

El articulo resuelve la pregunta de ¿Cómo se puede desarrollar un sistema integral para el monitoreo en pymes? Debido a que destaca aspectos importantes de la monitorización de equipos de T.I ayuda a salvaguardar los activos de información de las organizaciones. También el articulo proporciona una visión general de las diferentes técnicas de monitoreo que se encuentran en el mercado actual.

Intelligent Network Applications Monitoring and Diagnosis Employing Software Sensing and Machine Learning Solutions.

El artículo de Monitoreo y diagnóstico inteligentes de aplicaciones de red mediante técnicas de detección de software y aprendizaje automático, presenta una investigación de campo sobre la detección y recuperación de software y hardware de red en caso de fallo, mal

funcionamiento o acceso no autorizados, se realiza un estudio de caso comparando el motor un motor de IA Davis con el funcionamiento del mantenimiento humano, también menciona el tema de la eficacia de los agentes de IA en la detección de fallos de funcionamiento abarcando las nuevas tecnologías como IoT, ciudades y vehículos inteligentes.

En la segunda parte del artículo se propone una nueva solución para la detección de fallos en aplicaciones y redes de comunicaciones, mediante una solución que se basa en una combinación de análisis de series temporales, dependencia de largo alcance y control predictivo. Los resultados de las simulaciones muestran que el algoritmo propuesto es eficaz para detectar fallos de aplicaciones o intrusiones no autorizadas en el tráfico de redes de comunicaciones. (Minea et al., 2021)

Este artículo responde a la pregunta ¿Qué elementos, características, equipos y factores internos y externos debo tener en cuenta para realizar monitoreo a equipos de T.I.? debido a que identifica elementos como aplicaciones, hardware, Software y redes que se tienen en cuenta para el monitoreo en data center, también identifica las características correspondientes y los factores interno y externos como la infraestructura de T.I y amenazas.

Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures.

Gestión de eventos e información de seguridad (SIEM): Análisis, tendencias y uso en infraestructuras críticas, es un artículo de investigación en donde se examinan los sistemas de gestión de eventos de seguridad (SIEM), estos sistemas en la actualidad se utilizan para prevenir, detectar y responder a ciberataque, estas soluciones han evolucionado en sistemas integrales identificando áreas de alto riesgo centrándose proactivamente en la mitigación disminuyendo costos y tiempo de respuesta a incidentes.

En la actualidad estos SIEM se está integrando a soluciones Big Data, en este documento se examinan diferentes tipos de SIEM con respecto a su funcionalidad crítica y se brinda un análisis de los factores externos que afectan estos sistemas a corto o largo plazo, se realiza una lista para mejorar la próxima generación de estos sistemas y la revisión de sistemas existentes, así como un análisis de sus beneficios y su uso en infraestructuras críticas (González-Granadillo et al., 2021)

El artículo resuelve la pregunta: ¿Qué beneficios obtienen las empresas de la implementación de un sistema de monitoreo de equipos de T.I? debido a que menciona beneficios como los sistemas de monitoreo puede mejorar la visibilidad, proporcionando una visión general del entorno de T.I, previenen problemas, aumentan la eficiencia de la organización y reduce costos en cuanto a evitar daños en la infraestructura de T.I.

Automated Tool Based on Deep Learning to Assess Voltage Dips Validity: Integration in the QUEEN MV Network Monitoring System

El artículo de investigación Herramienta automatizada basada en aprendizaje profundo para evaluar la validez de las caídas de tensión: Integración en el sistema de monitorización de redes de MT QuEEN presenta el desarrollo de una herramienta automatizada llamada QuEEN PyService, está destinada a la extracción de señales de tensión de eventos de la base de datos del sistema de monitorización de la red de distribución QuEEN, para el análisis avanzado de la calidad de la energía eléctrica. La aplicación ha permitido la integración del clasificador DELFI (Aprendizaje profundo para la identificación de caídas de tensión falsas), desarrollado recientemente por RSE, lo que ha hecho posible por primera vez la validación intensiva de este último en un gran número de caídas de tensión. Gracias a esta herramienta, se ha realizado una comparación entre el rendimiento de DELFI y el de un criterio anterior basado en la medición

del segundo armónico de tensión, utilizando datos registrados por 61 unidades de medida en el período 2015-2020. El análisis se ha centrado en los índices tradicionales de recuento de caídas de tensión de la calidad de la energía eléctrica, N2a y N3b. Los resultados muestran que el uso del clasificador DELFI aumenta el N2a y el N3b en un 20,6 % y un 38,8 %, respectivamente, con respecto al criterio QuEEN. (Zanoni et al., 2021)

Este artículo responde la pregunta: ¿Qué elementos, características, equipos y factores internos y externos debo tener en cuenta para realizar monitoreo a equipos de T.I? el artículo menciona elementos como equipos de T.I y métodos de monitoreo, características como la escalabilidad y facilidad de uso y factores internos y externos como políticas y procedimientos y amenazas de seguridad.

AmLight Real Time In-Band Telemetry Within the NoviFlow Switches.

Telemetría en banda en tiempo real de AmLight dentro de los conmutadores NoviFlow es un artículo técnico en donde se afirma que la resolución de problemas y la monitorización de redes son esenciales en la rutina de gestión de redes. Un nuevo enfoque, la telemetría de red en banda en tiempo real (INT), permite monitorizar el plano de datos a velocidad de línea. Su mecanismo funciona adjuntando telemetría de red en tiempo real a cada paquete, lo que permite una monitorización granular. El despliegue de INT es posible mediante dos variantes: programar los conmutadores utilizando el lenguaje de programación P4 o instalar nuevo hardware que soporte esta función. Esta metodología aporta ventajas a las redes de redes definidas por software (SDN) en términos de granularidad de la monitorización.

El enfoque AmLight-INT aborda las actividades de resolución de problemas en las redes SDN. El objetivo detrás de la implementación y aplicaciones de INT en torno a este enfoque es reforzar la capacidad y la capacidad de mitigación de problemas de red en todo el nuevo chipset

Intel (también conocido como Barefoot Tofino). El enfoque AmLight-INT ha requerido la implementación de nuevo software para manejar el proceso de recolección de todos los informes de telemetría INT.

La solución AmLight-INT incluye algunas aplicaciones desarrolladas recientemente, como el INT Collector, QueueTop, ProofOfTransit y TCP Health Checker. La investigación se realizó gracias a la colaboración entre la industria y el mundo académico. La información proporcionada por el proyecto AmLight-INT aporta información útil para comprender algunos detalles relacionados con el uso y el estado de la red. (Bezerra Jeronimo A. and Ibarra, 2022)

El artículo resuelve la pregunta ¿Qué elementos, características, equipos y factores internos y externos debo tener en cuenta para realizar monitoreo a equipos de T.I.? mencionando elementos como equipos de T.I y métodos de monitoreo características como flexibilidad y facilidad de uso y equipos como los SIEM y factores externos como la creación de nuevas tecnologías o amenazas.

Towards Cloud-Based Unobtrusive Monitoring in Remote Multi-Vendor Environments.

El artículo Hacia el monitoreo no intrusivo basado en la nube en entornos remotos de múltiples proveedores propone una plataforma de monitoreo no intrusivo basada en agentes, con la capacidad de monitorear servicios externos e internos utilizando contenedores Sidecar a nivel de microservicio monitorea el estado y las métricas que el sistema arroja, La investigación se desarrolló como parte del proyecto DynAMo y diversos socios de la industria participaron, la evaluación del prototipo demuestra que solo se utilizó el 0.02% de CPU en promedio, en un ambiente de microservicios controlado detectando rápidamente nuevas anomalías. (Moeyersons et al., 2022)

El artículo resuelve la pregunta: ¿Cómo se puede desarrollar un sistema integral para el monitoreo en pymes? El enfoque de una plataforma no intrusiva basada en agentes es una muy buena base para desarrollar sistemas de monitores que utilicen pocos recursos y detecte rápida y eficazmente las anomalías.

Marco Teórico

Un sistema de monitoreo integral para Data Center permite a las organizaciones salvaguardar la disponibilidad de los equipos y componentes del cuarto de equipos, detectar y solucionar problemas de forma temprana y optimizar el rendimiento de los equipos y componentes del data center, el cual es una infraestructura física que debe tener parámetros adecuados que permita garantizar la seguridad y respaldo de los equipos críticos de una organización. (Pacios, 2019)

También se debe resaltar la importancia de fortalecer la coherencia conceptual entre los ejes de monitoreo integral, resiliencia tecnológica y gobierno de TI, con el fin de garantizar una comprensión más profunda y una articulación efectiva, debido a que el monitoreo integral no debe concebirse únicamente como un proceso técnico de observación o registro, sino como un mecanismo estratégico que posibilita la continuidad operativa y la estabilidad de los servicios tecnológicos ante posibles incidentes o fallas.

La resiliencia tecnológica se sitúa como un elemento clave en la teoría del presente documento que permite a la organización anticipar, resistir y recuperarse de interrupciones en los sistemas de información, asegurando la disponibilidad y confiabilidad de los servicios críticos. (Roffia & Dabić, 2024)

Esta relación se encuentra directamente vinculada con el gobierno de tecnologías de información, definido como el conjunto de estructuras, políticas y procesos mediante los cuales

se garantiza que el uso de la tecnología esté alineado para ayudar a conseguir los objetivos estratégicos de la organización.

Desde esta perspectiva, el monitoreo integral y la resiliencia tecnológica deben orientarse en principios de gobernanza que permitan la toma de decisiones, la asignación de responsabilidades y la gestión de riesgos tecnológicos de manera efectiva.(Lowry et al., 2025)

Para fortalecer el componente teórico del presente documento, se recomienda el uso de marcos de referencia reconocidos internacionalmente como COBIT 2019 e ITIL 4, los cuales ofrecen lineamientos y buenas prácticas que permiten estructurar adecuadamente la gestión y supervisión de los servicios de TI en la empresa Transportes Gayco S.A.S.

Según (Grivin Mokodaser et al., 2024) COBIT 2019 es un marco de trabajo para gobernanza y gestión de T.I asegura que las inversiones tecnológicas generen valor y mitiguen los riesgos asociados a su operación. Por su parte, como lo indica (Al-Ashmoery et al., 2021) ITIL 4 se centra en la creación de valor a través de la gestión eficiente del ciclo de vida de los servicios, incorporando principios de mejora continua, colaboración y adaptación al cambio en las organizaciones de cualquier índole.

De esta manera, la integración conceptual entre monitoreo integral, resiliencia tecnológica y gobierno de TI, sustentada en los marcos COBIT 2019 e ITIL 4, contribuye a consolidar una base teórica sólida que respalde el diseño y la implementación de estrategias efectivas de gestión tecnológica dentro de la organización.

Asimismo, se hace necesario analizar el impacto que la estrategia de monitoreo integral puede tener en la eficiencia energética, la sostenibilidad y la seguridad de la información dentro del Data Center de la empresa Transportes Gayco S.A.S debido a que un monitoreo efectivo no solo permite identificar y prevenir fallos técnicos, también optimizar el consumo energético al

gestionar de forma inteligente la carga de trabajo de los equipos evitando así sobrecargas de trabajo y uso indebido, contribuyendo a la sostenibilidad ambiental y a la reducción de costos operativos.(Katal et al., 2023a)

Desde la perspectiva de (Kitsios et al., 2023), la implementación de un sistema de monitoreo integral se articula con los principios establecidos en la norma ISO/IEC 27001:2022, al fortalecer la detección temprana de incidentes, el control de accesos, la integridad de los datos críticos aumentando el tiempo de disponibilidad de los activos. Además de su alineación con la Ley 1581 de 2012 puede mejorar y garantizar el cumplimiento normativo en materia de protección de datos personales, asegurando que las operaciones tecnológicas se desarrollen bajo estándares de la legislación colombiana e internacional

En conjunto, este enfoque integral contribuye a una gestión tecnológica más sostenible, eficiente y segura, alineando la infraestructura del Data Center de la empresa Transportes Gayco S.A.S con las buenas prácticas internacionales de gobernanza y gestión de tecnologías de la información.

La clasificación de los data center de acuerdo a su tamaño es un factor determinante de acuerdo a las necesidades específicas de las organizaciones desde pequeños Data Center diseñados para pequeñas empresas que tienen recursos limitados en cuanto almacenamiento y procesamiento de datos, pasando por data center medianos, los cuales tienen necesidades de almacenamiento entre 100 terabytes y un petabit utilizados por empresas gubernamentales y organizaciones con necesidades de almacenamiento y procesamiento enfocadas a misión crítica y requerimientos empresariales, hasta grandes data centers y mega data centers que tienen capacidades en 1 petabit y más de 10 petabits con grandes capacidades tecnológicas y de seguridad.(Hayes, 2018; Khan, 2020; Leclair, 2019; McGrath, 2021)

Los data center tienen múltiples componentes entre lo más importantes tenemos los servidores, estos equipos Informáticos proveen, administran y controlan diferentes tipos de servicios a una red de computadoras de una organización, caracterizándose por tener un hardware y software más robusto en comparación con los demás equipos ofimáticos en cuanto a: Refrigeración, redundancia, capacidad y durabilidad de componentes. (Marchionni, 2011)

Los objetivos del monitoreo de servidores pueden variar según las necesidades, pero por lo general se pueden tener en cuenta, garantizar la disponibilidad del servidor, mejorar el rendimiento del servidor y prevenir problemas, este implica recopilar datos de una variedad de fuentes, incluyendo el hardware del servidor como la CPU, entre estos tenemos la RAM y el disco duro, el software como sistema operativo y las aplicaciones y por último los elementos de red como switch, routers, firewall, tarjetas de red y dispositivos inalámbricos (C. García-Hernández, 2023)

Existen una variedad de herramientas de monitoreo de servidores disponibles, que van desde soluciones gratuitas y de código abierto hasta soluciones comerciales de alta gama. Las herramientas de monitoreo de servidores pueden recopilar datos de una variedad de fuentes, analizar los datos y generar alertas cuando se detectan problemas en diferentes tipos de servidores como los servidores de Impresión, estos se encargan de conectar múltiples impresoras para poderlas compartir en la red, servidores web: que se encargan de almacenar y administrar sitios que se pueden acceder desde internet o una intranet por medio del protocolo HTTP o HTTPS, se tienen también los servidores de base de datos, manejan grandes volúmenes de información a través de diferentes motores de base de datos, y el servidor de correo electrónico, suministrando servicios de administración, seguridad y almacenamiento de correos electrónicos en una organización, con los servidores de directorio, almacenando las cuentas de usuario de la

red, permitiendo configurar políticas grupales y los servidores de redes, que permiten la comunicación entre los diferentes equipos que componen una red, dando servicios como DHCP, NAT, Proxy, VPN, por último tenemos los servidores de archivos para compartir carpetas y los servidores de seguridad y monitoreo para monitorear, vigilar y controlar amenazas, vulnerabilidades y los diferentes componentes que pueden afectar la seguridad en la red. (Marchionni, 2011)

Un sistema de monitoreo integral para data center está compuesto por sensores, que recopilan datos de los equipos y componentes del data center, estos sensores se pueden clasificar en función de la variable que miden. Los principales tipos de sensores que se utilizan en los sistemas de monitoreo de data center tenemos sensores de estado: Miden el estado de los equipos y componentes del data center. Por ejemplo, pueden medir la temperatura, la humedad, la presión, el voltaje, la corriente, también tenemos sensores de rendimiento: Miden el rendimiento de los componentes del data center, pueden medir la velocidad de la CPU, la memoria, el disco duro, la red, etc. y sensores de consumo de energía: Miden el consumo de energía de los equipos y componentes del cuarto de equipos de la organización.

Otros componentes importantes son los agentes de monitoreo, permiten recopilar datos de los sensores y los envían al sistema de monitoreo, utilizando una base de datos para recopilar datos suministrados de los sensores y los agentes de monitoreo y teniendo un software de monitoreo, para analizar los datos almacenados en la base de datos y presentarlos en forma de informes o alertas. (García-López, 2023)

Todos estos componentes realizan funciones de monitoreo integral en data center utilizando sensores y agentes de monitoreo para recopilar datos de los equipos y componentes.

Estos datos pueden incluir información sobre el estado de los equipos, el rendimiento de

los componentes, el consumo de energía, etc. Además, el software de monitoreo analiza los datos recopilados por los sensores y los agentes de monitoreo. Este análisis permite identificar problemas potenciales, tendencias y oportunidades de mejora, el software de monitoreo presenta los datos analizados en forma de informes o alertas. Estos informes y alertas ayudan a los administradores del data center a tomar decisiones informadas. (García-López, 2023)

Los data center también cuentan con sistemas complementarios de seguridad y respaldo los cuales son una serie de medidas que se implementan para garantizar la seguridad y la disponibilidad de los datos y los sistemas informáticos. Estos sistemas se complementan entre sí para proporcionar una protección más completa a los sistemas de monitoreo. Los sistemas de seguridad se encargan de proteger los datos y los sistemas informáticos de los ataques externos. Algunos de los sistemas de seguridad más comunes son los firewalls estos dispositivos se utilizan para bloquear el acceso no autorizado a una red restringiendo el tráfico entrante y saliente de esta, Es importante monitorear los registros de eventos del firewall para detectar problemas o amenazas. También es importante monitorear el estado de las actualizaciones del firewall para asegurarse de que siempre están instaladas. Debemos tener en cuenta el antivirus que se utilizan para detectar y eliminar virus y otros programas malignos, es importante monitorear los registros de eventos del antivirus para detectar problemas o amenazas. También es importante monitorear el estado de las actualizaciones del antivirus para asegurarse de que siempre están instaladas, no menos importante están los IDS/IPS se utilizan para detectar, bloquear y alertar sobre actividades sospechosas en una red Es importante monitorear los registros de eventos del IDS/IPS para detectar problemas o amenazas. También es importante configurar los IDS/IPS para que generen alertas cuando detecten actividades sospechosas. Por último, pero no menos importante se debe tener en cuenta el sistema de gestión unificada de

amenazas (UTM) integrando en un solo dispositivo de seguridad, antivirus, firewall, antispam IDS/IPS, Proxy Web, filtrado de contenido, escáner de vulnerabilidades, VPN, es importante monitorear los registros de eventos del UTM para detectar problemas o amenazas. También es importante monitorear el estado de las actualizaciones del UTM para asegurarse de que siempre están instaladas. (Uptime Institute., 2023)

Otros sistemas para tener en cuenta en el monitoreo de data center son los sistemas de respaldo que se encargan de crear copias de seguridad de los datos y los sistemas informáticos. En caso de pérdida de datos o un fallo del sistema, las copias de seguridad se pueden utilizar para restaurar los datos y los sistemas a su estado anterior estos equipos utilizan servicios de monitoreo similares a los servidores.

Además de los sistemas de seguridad y de respaldo, existen otros sistemas complementarios que pueden ayudar a mejorar la seguridad y la disponibilidad de un Data Center. Algunos de estos sistemas como Los SIEM que recopilan y analizan datos de seguridad de una variedad de fuentes para ayudar a identificar y responder a amenazas, es importante monitorear los registros de eventos para detectar problemas o amenazas. También es importante monitorear las alertas generadas por el SIEM para asegurarse de que se están respondiendo correctamente y los DR se utilizan para restaurar los datos y los sistemas en caso de desastres. Es importante revisar el plan de DR periódicamente para asegurarse de que está actualizado y que cumple con las necesidades de la organización. También es imperativo probar los procedimientos de DR periódicamente para asegurarse de que se pueden implementar correctamente. (Gartner, 2022)

Entre uno de los elementos más importantes como sistemas complementarios en un data center están las UPS también conocido por sus siglas en español (SFI) Sistema de fuerza

interrumpible, este dispositivo permite almacenar energía eléctrica para que en el momento que sucede un fallo en el suministro, pueda respaldar proporcionando la electricidad suficiente para el correcto funcionamiento de los equipos que tenga conectados, además permite mejoras en la calidad de la corriente eléctrica que reciben los dispositivos eliminando picos de voltaje, armónicos y demás elementos que puedan afectar una red eléctrica.(W.N.H. Ibrahim A.A. El-Sheikh M.A. El-Sherif M.A. El-Khodary M.A. Ibrahim M.S. Al-Sharawy, 2016)

En el monitoreo de una UPS permite recopilar datos sobre el estado y el rendimiento de la UPS. Estos datos se pueden utilizar para identificar problemas potenciales, mejorar el rendimiento de la UPS y garantizar que esté siempre disponible para proporcionar energía de respaldo.

Hay dos formas principales de monitorear una UPS tenemos como manera más sencilla el monitoreo local el cual se realiza utilizando la pantalla LCD o la interfaz de usuario de la UPS, también tenemos el monitoreo remoto: Esta forma de monitoreo permite recopilar datos de la UPS desde una ubicación remota. Se puede realizar utilizando un software de monitoreo de UPS o un dispositivo de monitoreo de red, las métricas más importantes que se deben monitorear en una UPS incluyen:

Voltaje de entrada: Este es el voltaje de la red eléctrica que alimenta la UPS.

Voltaje de salida: Este es el voltaje que la UPS proporciona a los dispositivos conectados.

Corriente de salida: Esta es la corriente que la UPS está proporcionando a los dispositivos conectados.

Estado de la batería: Esta métrica indica el estado de la batería de la UPS, que puede ser baja, media o alta.

Tiempo de funcionamiento restante: Esta métrica indica cuánto tiempo puede

proporcionar energía de respaldo la UPS con la carga actual.

Temperatura: La temperatura de la UPS puede afectar su rendimiento y vida útil.

Humedad: La humedad excesiva puede dañar los componentes electrónicos de la UPS.

Alarmas: Las alarmas de la UPS pueden indicar problemas potenciales, como una batería baja o un problema con la entrada de la red eléctrica.

Teniendo en cuenta estos componentes tendremos una visión global de lo que se debe monitorear en una UPS sin pasar por alto los diferentes tipos de UPS que hay en el mercado como las UPS de corriente continua, UPS de corriente alterna, UPS de estado de espera y UPS Line – interactive(in-line)(W.N.H. Ibrahim A.A. El-Sheikh M.A. El-Sherif M.A. El-Khodary M.A. Ibrahim M.S. Al-Sharawy, 2016)

Otros sistemas no menos importantes que componen los data center son los aires acondicionados, que permiten mantener una temperatura acorde a los equipos que se encuentran en el centro de datos, el monitoreo de un aire acondicionado es esencial para recopilar datos sobre el estado y el rendimiento del aire acondicionado. Estos datos se pueden utilizar para identificar problemas potenciales, mejorar el rendimiento del aire acondicionado y garantizar su eficiencia energética con el objetivo de:(C. , P.-M. J. , y G.-L. A. García-Hernández, 2021)

Garantizar el funcionamiento adecuado del aire acondicionado: El monitoreo de aire acondicionado ayuda a identificar problemas potenciales antes de que causen una interrupción del servicio.

Mejorar el rendimiento del aire acondicionado: El monitoreo de aire acondicionado puede ayudar a identificar áreas de mejora en el rendimiento del aire acondicionado, como la eficiencia energética o el confort térmico.

Prevenir problemas: El monitoreo de aire acondicionado puede ayudar a prevenir

problemas, como fallas de componentes o fugas de refrigerante

Elementos del Monitoreo de Aire Acondicionado:

El monitoreo de aire acondicionado implica recopilar datos de una variedad de fuentes, incluidas:

Sensores: Los sensores son dispositivos que recopilan datos del aire acondicionado. Estos sensores pueden ser físicos, como termómetros o medidores de flujo de aire, o lógicos, como contadores de errores o registros de funcionamiento.

Herramientas de monitoreo: Las herramientas de monitoreo permiten recopilar, analizar y visualizar los datos recopilados por los sensores.

Por último, se tienen en cuenta sistemas de detección de humo que permiten enviar alertas o informa de manera automática cuando hay presencia de humo en las instalaciones del data center también, sistemas de control de acceso y sistemas CCTV los cuales nos permiten tener un registro de las actividades que se realizan en el centro de datos de la organización.

Marco Conceptual

Monitoreo de Infraestructura TI

El monitoreo de infraestructura TI es el proceso mediante el cual se recopila, analiza y supervisa información sobre el estado, rendimiento y disponibilidad de los componentes tecnológicos de una organización. Según (Misal, n.d.) este proceso permite identificar fallas, anomalías o degradaciones en el servicio, facilitando una gestión proactiva de los recursos tecnológicos.

En el contexto del presente estudio, el monitoreo se concibe como un sistema integral, que no solo incluye servidores y redes, sino también elementos complementarios como UPS, sistemas de climatización y dispositivos de seguridad.

Data Center

De acuerdo con (Guo, 2022) Un data center es una infraestructura física y lógica destinada al almacenamiento, procesamiento y gestión de la información de una organización, compuesto por servidores, redes de comunicación, sistemas de almacenamiento, aplicaciones y elementos de soporte como energía, refrigeración y seguridad.

En esta investigación, el data center se aborda como un ecosistema interdependiente, donde la falla de un componente puede afectar el funcionamiento global del sistema, lo que justifica la necesidad de un monitoreo integral.

Activos de Información

En el documento (Ross et al., 2021) describen que los activos de información son todos aquellos recursos que soportan los procesos de la organización y que tienen valor para la misma, incluyendo hardware, software, datos, redes, servicios, personal y elementos auxiliares.

Estos activos son identificados y clasificados en el estudio mediante la metodología Magerit, permitiendo determinar su criticidad y priorizar su monitoreo.

Gestión de Riesgos (Magerit)

La gestión de riesgos es el proceso de identificación, análisis y evaluación de amenazas y vulnerabilidades que pueden afectar los activos de información donde la metodología Magerit, según (coordinación de contenidos et al., 2012) es un marco oficial español estructurado que permite valorar los riesgos considerando dimensiones como: Disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad.

En esta investigación, Magerit es fundamental para determinar qué activos deben ser monitoreados prioritariamente y establecer una base técnica para el diseño de la solución.

Monitoreo 24/7 (Continuo)

El monitoreo 24/7 hace referencia a la supervisión continua de los sistemas tecnológicos durante todo el tiempo (24 horas al día, 7 días a la semana), de acuerdo con (Dempsey et al., 2020) permite garantizar la detección oportuna de incidentes, en este enfoque permite pasar de un modelo reactivo a uno proactivo, reduciendo tiempos de respuesta (MTTR) y aumentando la disponibilidad de los servicios.

Protocolos de Monitoreo.

(Al-Fuqaha et al., 2015) describe que los protocolos de monitoreo son mecanismos de comunicación que permiten la recolección y transmisión de información desde los dispositivos hacia las plataformas de supervisión, permitiendo la interoperabilidad entre dispositivos heterogéneos, característica fundamental en entornos de data center.

Sensores y Monitoreo Ambiental

Según (Dharshani & Annamalai, 2023) los sensores son dispositivos que permiten medir variables físicas del entorno del data center, tales como: Temperatura, humedad, presencia de humo, fugas de agua y estado de puertas entre otros, el monitoreo ambiental es clave para garantizar condiciones óptimas de operación y prevenir fallas en los equipos críticos.

Arquitectura de Monitoreo

Según (Chakian & García, 2012) la arquitectura de monitoreo puede entenderse como una estructura compuesta por diversos componentes que permiten la recolección, procesamiento y análisis de la información, incluyendo agentes o sensores, mecanismos de transmisión de datos,

módulos de análisis y sistemas de almacenamiento, los cuales trabajan de manera conjunta para supervisar el estado de los sistemas.

En el documento, la arquitectura se diseña para permitir la integración de múltiples tecnologías y protocolos, asegurando escalabilidad y eficiencia.

Alertas y Gestión de Eventos

De acuerdo con (Ligus, 2013) las alertas son notificaciones generadas automáticamente cuando una métrica supera un umbral definido o se detecta un comportamiento anómalo, las cuales se pueden clasificar en: alertas de rendimiento, alertas de disponibilidad, alertas de seguridad y alertas ambientales, las cuales su correcta configuración permite una respuesta oportuna ante incidentes, reduciendo el impacto en la operación.

Indicadores de Gestión (KPIs)

(Liu et al., 2024) afirman que los indicadores clave de desempeño (KPIs) son métricas utilizadas para evaluar el estado y eficiencia de la infraestructura TI, entre los principales indicadores se encuentran: MTTR (Mean Time To Repair): Tiempo medio de reparación, MTBF (Mean Time Between Failures): Tiempo medio entre fallas, disponibilidad del sistema y uso de CPU, memoria y red, permitiendo medir el impacto de la estrategia de monitoreo en la organización.

Visualización de Datos (Dashboards)

Según (Knafllic, 2015) la visualización de datos consiste en la representación gráfica de la información recolectada, facilitando su interpretación, permitiendo transformar datos en información útil para la toma de decisiones de la organización.

Para esta investigación, se propone el uso de **Power BI** para el diseño de dashboards que integren: el estado de servidores, rendimiento de red, seguridad, energía y ambiente, disponibilidad y SLA.

Monitoreo Integral

(Ramírez Fernández, 2023) describe que el monitoreo integral es un enfoque que busca supervisar de manera unificada todos los componentes del data center, incluyendo la infraestructura física, sistemas tecnológicos, seguridad y ambiente, teniendo este concepto como el eje central de la investigación, ya que permite superar el monitoreo fragmentado y lograr una visión holística del estado de la infraestructura TI.

Marco Contextual

La presente investigación se desarrolla en el contexto de la empresa Transportes Gayco S.A.S., ubicada en la ciudad de Villavicencio, departamento del Meta, Colombia, una región estratégica para la actividad logística y de transporte en el país. Villavicencio cuenta con una población aproximada inferior a los 600.000 habitantes, consolidándose como un punto clave de conexión entre el centro del país y la región de los Llanos Orientales.

La ubicación de la Transportes Gayco en Villavicencio representa un entorno particular caracterizado por condiciones climáticas cálidas y variables, así como por su cercanía a zonas de producción de hidrocarburos, influyendo directamente en la operación de la infraestructura tecnológica, especialmente en lo relacionado con la gestión térmica y energética de los equipos del data center.

Adicionalmente, la ciudad se posiciona como un nodo logístico relevante, lo que incrementa la importancia de contar con sistemas tecnológicos confiables que soporten las operaciones de transporte y garanticen la continuidad del negocio.

La empresa Transportes Gayco S.A.S. es una empresa del sector transporte con más de 20 años una planta de personal inferior a 500 empleados, lo que la clasifica como una pequeña y mediana empresa (PYME) dentro del contexto colombiano.

Transportes Gayco, se especializa en el transporte de hidrocarburos, combustibles y alimentos, actividades que requieren altos niveles de control operativo, trazabilidad y disponibilidad de la información, debido a su impacto en la cadena de suministro y en sectores estratégicos de la economía.

Para el desarrollo de sus operaciones, la empresa cuenta con una flota superior a 300 tractocamiones, lo que implica una gestión logística compleja, soportada por sistemas de información como el ERP Syscom carga y sistemas de seguimiento satelital denominado Logitracs, que permiten la planificación, seguimiento y control de las actividades de transporte.

Actualmente, Transportes Gayco se encuentra en un proceso de fortalecimiento de su infraestructura física, evidenciado en la construcción de su sede propia sobre la avenida Puerto López en Villavicencio (Meta), una de las principales vías de acceso de la ciudad. Este crecimiento organizacional implica también la necesidad de consolidar una infraestructura tecnológica más robusta, alineada con la expansión de sus operaciones.

En este contexto, el data center de la organización cumple un papel fundamental como soporte de los sistemas de información que permiten la gestión de la operación, la comunicación interna y externa, y el almacenamiento de datos críticos.

Dada la naturaleza de su operación, Transportes Gayco depende en gran medida de sus sistemas tecnológicos para garantizar, la trazabilidad de los servicios de transporte, la gestión de la información operativa y administrativa la comunicación entre áreas y procesos y la continuidad de los servicios

Sin embargo, como ocurre en muchas PYMES, la infraestructura tecnológica presenta desafíos asociados a la integración, supervisión y control de los diferentes componentes, lo que genera la necesidad de implementar soluciones que permitan una gestión más eficiente.

En este entorno descrito, la investigación se orienta al diseño de una estrategia de monitoreo integral del data center, que responda a las necesidades específicas de una empresa del sector transporte con alto nivel de operación logística y dependencia tecnológica.

El contexto particular de Transportes Gayco S.A.S., caracterizado por su ubicación geográfica, su crecimiento organizacional, la naturaleza de sus servicios y la complejidad de su operación, hace evidente la importancia de contar con herramientas que permitan supervisar de manera continua y centralizada la infraestructura TI, contribuyendo a la mejora de la disponibilidad, la seguridad y la eficiencia operativa.

Marco Legal

Ley 1581 de 2012

Esta ley regula el tratamiento de datos de personales usados en el datacenter de la empresa transportes Gayco. (Función Pública, 2012)

ISO/IEC 27001

Según (Rodríguez et al., 2023) esta norma internacional busca proteger la confidencialidad, disponibilidad e integridad de la información recomendada para certificar el datacenter de la empresa transportes Gayco

Ley 1273 de 2009 (Delitos Informáticos)

(Suarez Valencia, 2025) afirma que esta ley penaliza delitos informáticos como: robo. Suplantación de identidad, acceso no autorizado o daños, algunos de estos delitos pueden ser informados y documentados por el sistema de monitoreo.

Norma NTC 60364 (Instalaciones Eléctricas)

(Jaramillo, n.d.) Indica que esta norma nos permite establecer los requisitos para la instalación de UPS y como debemos medir sus parámetros eléctricos.

Ley 697 de 2001

Según (Mejía et al., 2022) esta ley promueve la eficiencia energética en equipos de monitoreo y enfriamiento.

Metodología

Enfoque de Investigación

La presente investigación se desarrolla bajo un enfoque mixto, debido a que integra técnicas y procedimientos de carácter cuantitativo y cualitativo para el análisis de la infraestructura tecnológica del data center de la empresa Transportes Gayco S.A.S.

El componente cuantitativo se evidencia en la identificación, valoración y clasificación de los activos de información mediante la metodología Magerit, así como en la aplicación de matrices de evaluación para comparar sistemas operativos, herramientas de monitoreo, sensores, protocolos y demás componentes tecnológicos. Este enfoque permite asignar valores, establecer niveles de riesgo y realizar comparaciones objetivas que apoyan la toma de decisiones.

Por su parte, el componente cualitativo se orienta al análisis del contexto organizacional, la revisión documental, la consulta de estándares y buenas prácticas en monitoreo de infraestructura TI, y la interpretación de los resultados obtenidos en las matrices de evaluación. De esta manera, se busca comprender las necesidades específicas de la organización y sustentar técnicamente el diseño de la solución propuesta.

La combinación de ambos enfoques permite abordar el problema de investigación de manera integral, articulando la valoración objetiva de los activos y tecnologías con la comprensión del entorno operativo y las necesidades estratégicas de la empresa. Esto facilita la formulación de una propuesta de monitoreo coherente con las condiciones reales del data center y con los objetivos del estudio.

Diseño de Investigación.

Etapas 1: Valorar los Elementos que Componen un Cuarto de Equipos en una Pyme

Mediante una recopilación bibliográfica y la realización de un inventario detallado de los

diferentes elementos HW, software, redes y equipos complementarios que componen el cuarto de equipos de Transportes Gayco.

Se tendrá en cuenta las características de los componentes Hardware y software examinado en cada equipo elementos como procesador, RAM, almacenamiento, tarjetas de red, velocidad, ancho de banda, categoría de cableado estructurado sistemas operativos, aplicaciones bases de datos, virtualización con sus respectivas versiones, funcionalidades y requisitos exigidos por el H.W. niveles de temperatura óptimos recomendados y voltajes de funcionamiento de servidores, equipos de telecomunicaciones y suplementarios de la organización

Por último, mediante la metodología Magerit se realizará un análisis y evaluación de riesgos de los activos de información recolectados para determinar los diferentes dispositivos que deben ser monitoreados.

Etapas 2: Diagnosticar los Componentes que se van a Utilizar para Monitorear los Diferentes Elementos que se Encuentran en el Cuarto de Equipos

Por medio de la recopilación bibliográfica se determinan los diferentes elementos que interactúan para una monitorización integral de servidores, equipos de telecomunicaciones, elementos de seguridad y complementarios en un cuarto de equipos

Mediante una matriz de evaluación cuantitativa y cualitativa se considerarán los puntos a favor y en contra de los diferentes sistemas operativos, herramientas, sensores aplicaciones y demás elementos que permiten realizar un monitoreo integral a un cuarto de equipos en la empresa transportes Gayco,

Etapas 3: Diseño de Elementos para Integración de Componentes de Monitorización del Cuarto de Equipos

En esta fase se diseña la forma en que se integran las herramientas y los dispositivos de

monitoreo de la infraestructura TI, a partir de los resultados de las matrices de evaluación previamente definidas. El diseño contempla la integración de los distintos mecanismos de recolección y gestión de eventos, así como la definición de las alertas asociadas, considerando la arquitectura de la solución de monitoreo desde los niveles lógico y físico. Adicionalmente, se incluye la selección de los componentes tecnológicos necesarios, tales como sistemas operativos, aplicativos, servicios, bases de datos y demás elementos que permiten administrar, supervisar y analizar de forma continua el comportamiento de los dispositivos ubicados en el cuarto de equipos de la empresa Transportes Gayco S.A.S...

Etap 4: Proponer un Tablero de Visualización de Métricas de Monitoreo

En esta fase se identifican y organizan las métricas de monitoreo definidas previamente, con base en los resultados obtenidos en los objetivos anteriores, con el fin de establecer los elementos de información que serán representados en el tablero de visualización. A partir de esta definición, se diseña la estructura del dashboard considerando los indicadores clave, los tipos de visualización y la forma en que la información será presentada para facilitar su interpretación.

Posteriormente, mediante el uso de la herramienta Power BI, se propone el diseño del tablero de visualización, integrando las métricas seleccionadas y estableciendo una representación clara y comprensible del estado de la infraestructura TI. Este diseño se orienta a apoyar el análisis del comportamiento de los dispositivos monitoreados.

Finalmente, el tablero propuesto se analiza desde un enfoque funcional y descriptivo, con el propósito de evaluar su utilidad como apoyo para el seguimiento, la supervisión y la toma de decisiones relacionadas con la gestión de la infraestructura del cuarto de equipos de la empresa Transportes Gayco S.A.S.

Categorías o Variables

Infraestructura Física

Esta categoría comprende las variables ambientales y operativas que influyen en el funcionamiento del cuarto de equipos. En este sentido, se consideran variables térmicas como la temperatura mínima, máxima y promedio; condiciones de humedad, tanto relativa como absoluta y el consumo energético, analizado a nivel total, por equipo y por área. Se incluyen variables relacionadas con el flujo de aire, específicamente su velocidad y volumen, las vibraciones, evaluadas mediante su amplitud y frecuencia. Además, se contemplan factores de riesgo como la detección y extinción de incendios, el monitoreo de posibles inundaciones mediante el nivel de agua y sistemas de detección, y el control del estado, carga y tiempo de uso de las baterías.

Redes

La categoría de redes comprende las variables relacionadas con el desempeño y la calidad del servicio de comunicación entre dispositivos, se analiza la latencia, entendida como el tiempo de respuesta entre dispositivos, la pérdida de paquetes, como el porcentaje de paquetes que no llegan a su destino y el ancho de banda utilizado, evaluado por interfaz y por servicio, se considera el jitter, definido como la variación en el tiempo de retardo, así como la disponibilidad de la red, expresada en términos de tiempo de funcionamiento frente al tiempo de inactividad y se estudia el tráfico de red, teniendo en cuenta su volumen y el tipo de protocolo empleado, como HTTP, FTP, entre otros.

Servidores

La categoría de servidores comprende las variables asociadas al rendimiento, capacidad operativa y estado funcional de los equipos que soportan los servicios tecnológicos de la organización, se analiza la utilización de la CPU, medida como el porcentaje de uso del

procesador, la memoria, considerando su nivel de utilización y el uso de memoria swap y el almacenamiento en disco, evaluado a partir del espacio disponible y la tasa de entrada y salida de datos (E/S), se monitorea la temperatura de los componentes internos, debido a su impacto en la estabilidad y vida útil del hardware. Además se contempla el estado operativo del servidor, identificando si se encuentra en funcionamiento, apagado o en modo de espera.

Almacenamiento

La categoría de almacenamiento comprende las variables relacionadas con la capacidad, rendimiento y disponibilidad de los sistemas destinados a la gestión de datos, se analiza la capacidad utilizada, expresada como el porcentaje de espacio ocupado respecto al total disponible y se evalúa la tasa de transferencia de datos, considerando las velocidades de lectura y escritura, indicadores clave del desempeño del sistema, se miden las operaciones de entrada y salida por segundo (IOPS), que permiten determinar la capacidad de procesamiento de solicitudes simultáneas y finalmente, se examina la disponibilidad del sistema de almacenamiento, medida en términos de tiempo de funcionamiento frente al tiempo de inactividad.

Aplicaciones

La categoría de aplicaciones comprende las variables asociadas al desempeño, disponibilidad y estabilidad de los sistemas informáticos utilizados por la organización, se evalúa la disponibilidad del servicio mediante el análisis del tiempo de respuesta y la tasa de errores, indicadores fundamentales para medir la calidad de atención a las solicitudes de los usuarios. Además, se analiza el rendimiento de las aplicaciones a través de métricas como las transacciones por segundo y el tiempo de procesamiento, las cuales permiten determinar la eficiencia operativa del sistema también, se examina la utilización de recursos, considerando el

consumo de CPU, memoria y disco, con el fin de identificar posibles limitaciones o cuellos de botella. Finalmente, se revisan los registros de eventos (logs), prestando especial atención a errores y advertencias que puedan afectar la continuidad del servicio.

Seguridad

La categoría de seguridad comprende las variables relacionadas con la protección, integridad y control de los sistemas tecnológicos de la organización, se analizan los intentos de intrusión, considerando tanto el número de eventos registrados como su origen, con el fin de identificar posibles amenazas externas o internas, adicionalmente se evalúan las vulnerabilidades detectadas y corregidas, lo que permite medir el nivel de exposición del sistema y la efectividad de las acciones de mitigación implementadas y se examinan los incidentes de seguridad, clasificándolos según su tipo e impacto, para determinar su gravedad y repercusión en la operación. Por último, se revisa la configuración de seguridad, específicamente el cumplimiento de las políticas establecidas, como indicador del grado de alineación con las buenas prácticas y normativas vigentes.

Gestión

La categoría de gestión comprende las variables relacionadas con la administración operativa y el control de los procesos asociados a la infraestructura tecnológica, se analizan los tickets de soporte, considerando tanto el número de solicitudes registradas como el tiempo de resolución, con el fin de evaluar la eficiencia en la atención de incidentes, se examinan los cambios en la configuración, teniendo en cuenta la fecha, el usuario responsable y la descripción de la modificación realizada, lo cual permite garantizar trazabilidad y control. Finalmente, se evalúan los costos asociados a la operación, incluyendo gastos de energía, mantenimiento y personal, como indicadores del impacto económico de la gestión tecnológica.

Hipótesis

El diseño de una estrategia de monitoreo integral para el data center de la empresa Transportes Gayco S.A.S., basada en una arquitectura de monitoreo integral y en el uso de protocolos y mecanismos estandarizados, permitirá mejorar la gestión de fallas, reducir los tiempos de respuesta ante incidentes y aumentar la disponibilidad de los recursos tecnológicos.

Población:

La población objeto de estudio está conformada por la totalidad de los activos de información que integran la infraestructura del data center de la empresa Transportes Gayco S.A.S.

Estos activos incluyen componentes tecnológicos de diversa naturaleza, tales como hardware (servidores, equipos de cómputo), software (aplicaciones, sistemas operativos y bases de datos), dispositivos de red (switches, routers y puntos de acceso), elementos de seguridad (firewall, sistemas de monitoreo y protección), así como componentes auxiliares de infraestructura, entre ellos sistemas de alimentación eléctrica (UPS), aire acondicionado, sistemas de detección de incendios y otros elementos que garantizan la operación del entorno tecnológico.

En este contexto, la unidad de análisis corresponde a cada uno de los activos de información identificados dentro del data center, los cuales son evaluados mediante la metodología de gestión de riesgos Magerit, con el propósito de determinar su nivel de criticidad y establecer los requerimientos de monitoreo.

Muestra

En la presente investigación no se realiza un muestreo probabilístico ni no probabilístico, dado que la población objeto de estudio es reducida y completamente accesible.

En este sentido, se adopta un censo, en el cual se consideran la totalidad de los activos de información que conforman el data center de la empresa Transportes Gayco S.A.S., incluyendo componentes de hardware, software, redes, seguridad y elementos auxiliares.

La decisión de trabajar con la totalidad de la población permite obtener una visión integral del estado de la infraestructura tecnológica, garantizando que todos los activos relevantes sean evaluados dentro del análisis de riesgos y del diseño del sistema de monitoreo.

De esta manera, se asegura una mayor precisión en los resultados, evitando sesgos derivados de la selección de una muestra parcial y permitiendo una adecuada identificación de los activos críticos que requieren monitoreo.

Técnicas e Instrumentos de Recolección de Información:

Para el desarrollo de la presente investigación se emplea un enfoque mixto, integrando técnicas e instrumentos de recolección de información de carácter cuantitativo y cualitativo, con el fin de obtener una visión integral del estado del data center y sus necesidades de monitoreo.

Técnicas de Recolección de Información

Las técnicas utilizadas permiten obtener información relevante desde diferentes perspectivas:

Entrevistas. Se realizan entrevistas a personal técnico y usuarios relacionados con la gestión del data center, con el fin de identificar necesidades, problemáticas y requerimientos asociados al monitoreo de la infraestructura.

Observación. Se aplica la observación directa del entorno del data center, permitiendo analizar el funcionamiento de los equipos, las condiciones ambientales y las prácticas operativas existentes.

Revisión Documental. Se analizan documentos, registros y configuraciones existentes en la organización, con el propósito de comprender el estado actual de la infraestructura tecnológica.

Instrumentos de Recolección de Información

Cuestionarios. Se emplean cuestionarios estructurados y semiestructurados para recolectar información sobre el uso, desempeño y percepción del sistema de monitoreo actual.

Guías de Entrevista. Se diseñan guías que orientan la aplicación de entrevistas, asegurando la recolección de información relevante y alineada con los objetivos del estudio.

Formatos de Observación. Se utilizan formatos que permiten registrar de manera sistemática las condiciones y características del entorno del data center.

Registros del Sistema (logs). Se analizan los registros generados por los sistemas, como servidores, switch, UTM, UPS y demás para identificar eventos, fallas y comportamientos relevantes en la infraestructura.

Técnicas de Análisis de Resultados

El análisis de resultados en la presente investigación se realiza mediante un enfoque mixto, integrando técnicas cuantitativas y cualitativas que permiten interpretar la información recolectada sobre los activos del data center y las condiciones de monitoreo de la organización.

Análisis Descriptivo

El análisis descriptivo se emplea para organizar, resumir y presentar la información recolectada a través de tablas, matrices y representaciones gráficas. permitiendo identificar el

comportamiento de los datos, facilitando la interpretación de variables como niveles de riesgo, criticidad de los activos y resultados obtenidos en las matrices de evaluación. Se utilizan herramientas como tablas comparativas y gráficos para visualizar la distribución de los activos según su nivel de riesgo, permitiendo una comprensión clara del estado actual de la infraestructura.

Análisis Comparativo

El análisis comparativo se utiliza para evaluar diferentes tecnologías, herramientas y componentes asociados al sistema de monitoreo, con el fin de identificar la alternativa más adecuada para la organización. Este análisis se realiza mediante matrices de evaluación en las cuales se asignan criterios y ponderaciones a cada alternativa, permitiendo establecer diferencias y seleccionar las opciones más viables en función de su desempeño, funcionalidad y adecuación al contexto del data center.

Análisis de Riesgos

El análisis de riesgos se desarrolla con base en la metodología Magerit, permitiendo identificar, evaluar y clasificar los riesgos asociados a los activos de información del data center.

A partir de la valoración de probabilidad e impacto, se determinan niveles de riesgo (aceptable, tolerante, intolerante y extremo), lo que facilita la priorización de acciones y la identificación de activos críticos que requieren monitoreo permanente.

Análisis Cualitativo

El análisis cualitativo se aplica a la información obtenida mediante entrevistas y observación, permitiendo interpretar percepciones, experiencias y necesidades relacionadas con el monitoreo del data center.

Este análisis se realiza mediante la identificación de patrones, categorías y aspectos relevantes, contribuyendo a complementar los resultados cuantitativos y proporcionando una visión integral del problema de estudio.

Validez y Confiabilidad de los Instrumentos

La validez y confiabilidad de los instrumentos de recolección de información del presente trabajo de investigación constituyen aspectos fundamentales para garantizar la calidad y rigor metodológico del presente estudio.

Validez

La validez se refiere al grado en que los instrumentos utilizados miden de manera adecuada las variables de estudio relacionadas con el sistema de monitoreo del data center. En este proyecto, la validez se garantiza mediante la revisión teórica y documental de estándares, buenas prácticas y literatura especializada en monitoreo de infraestructura TI, lo cual permite asegurar que los criterios evaluados en entrevistas, observaciones y matrices de análisis estén alineados con los objetivos de la investigación.

Asimismo, se realiza una validación de contenido a partir de la coherencia entre los instrumentos diseñados y los objetivos específicos del estudio, especialmente en la identificación de componentes críticos, evaluación de tecnologías y análisis de resultados obtenidos en las matrices de valoración.

Confiabilidad

La confiabilidad hace referencia a la consistencia y estabilidad de los resultados obtenidos a través de los instrumentos aplicados. En este estudio, se garantiza mediante la aplicación sistemática de los instrumentos bajo criterios uniformes, tales como escalas de

valoración definidas (por ejemplo, de 1 a 5 en matrices de evaluación), lo cual permite mantener homogeneidad en la medición y comparación de resultados.

Adicionalmente, la confiabilidad se respalda en la triangulación de la información, combinando datos cuantitativos (matrices de evaluación, análisis estadístico) y cualitativos (entrevistas y observación), lo que permite contrastar resultados y fortalecer la consistencia de los hallazgos.

Control de Calidad de los Datos

Como parte del aseguramiento de la validez y confiabilidad, se realiza un proceso de limpieza, verificación y preparación de datos, garantizando que la información sea completa, consistente y libre de errores antes de su análisis

Procesamiento de la Información

El procesamiento de la información constituye una fase fundamental dentro del desarrollo de la presente investigación, ya que permite organizar, depurar y preparar los datos recolectados mediante las diferentes técnicas e instrumentos aplicados, con el fin de facilitar su análisis e interpretación.

Limpieza y preparación de datos

En esta etapa se realiza la verificación y depuración de la información obtenida a partir de entrevistas, observación, análisis de registros y matrices de evaluación. El objetivo principal es garantizar que los datos sean completos, consistentes y estén libres de errores que puedan afectar la validez de los resultados.

Para ello, se llevan a cabo actividades como la revisión de registros duplicados, la corrección de inconsistencias en la información recolectada y la validación de los datos frente a

los criterios definidos en la investigación. Luego se organiza la información en tablas y matrices, facilitando su clasificación y posterior análisis.

Se realiza la estructuración de los datos en formatos adecuados que permitan su interpretación, especialmente en las matrices de evaluación y valoración de riesgos, donde se consolidan los valores obtenidos para cada activo de información.

Organización y Consolidación de la Información

Una vez depurada la información, se procede a su organización mediante la clasificación de los datos según su naturaleza (cuantitativa y cualitativa). Los datos cuantitativos, como los valores de riesgo y las calificaciones asignadas en las matrices, son estructurados en tablas que permiten su comparación y análisis.

Por su parte, la información cualitativa obtenida a través de entrevistas y observación es sistematizada mediante la identificación de patrones, categorías y aspectos relevantes relacionados con el monitoreo del data center.

La consolidación de la información permite integrar los diferentes tipos de datos recolectados, facilitando una visión integral del estado de los activos y de las condiciones del entorno tecnológico analizado.

Preparación para el Análisis

Finalmente, los datos organizados y consolidados son preparados para su análisis mediante técnicas descriptivas y comparativas, permitiendo identificar tendencias, niveles de riesgo y aspectos críticos dentro de la infraestructura del data center.

En esta fase, se estructuran los resultados en matrices, tablas y representaciones gráficas, las cuales sirven como base para el análisis de resultados y la toma de decisiones en el diseño del sistema de monitoreo propuesto.

Resultados

Definición de los Componentes de Infraestructura TI Susceptibles de Monitoreo en Transportes Gayco

Inventario de Activos Transportes Gayco S.A.S

Los activos de la empresa transportes Gayco S.A.S se toman teniendo en cuenta la tipificación dada por la metodología Magerit en donde se clasifican dentro de una jerarquía, determinada para cada uno, el nombre, la nomenclatura, la descripción del activo y el responsable de la información como lo exige la norma ISO 27001:2013.

En la Tabla 1 se presenta la nomenclatura utilizada para la identificación y clasificación de los activos de información considerados en el presente estudio, con el propósito de manejar una referencia estándar a lo largo del documento.

Tabla 1

Nomenclatura de Activos

Nomenclatura	Nombre
D	Datos
S	Servicios
SW	Software de aplicaciones
HW	Hardware
COM	Redes y comunicaciones
MEDIA	Soportes de información
K	Claves criptográficas
L	Instalaciones
AUX	Elementos auxiliares
P	Personal

Nota. En la presente tabla se evidencia la nomenclatura que utiliza Magerit para identificar los activos de información.

En la Tabla 2 se presenta el inventario de activos de información correspondiente a la categoría Datos, clasificados según su descripción, responsable y cantidad, con el fin de facilitar su identificación y gestión dentro de la organización.

Tabla 2

Inventario de Activos de Información de la Categoría Datos de Transportes Gayco

Código	Nombre	Nomenclatura del activo	Descripción	Responsable	Cantidad
1	Datos	D	Gestión documental	Gestión documental	2.52 GB
2	Datos	D	Almacén	Compras	76.7 MB
3	Datos	D	Compras	Compras	9.89 GB
4	Datos	D	Contabilidad	Contabilidad	92.8 GB
5	Datos	D	Facturación	Facturación	325 GB
6	Datos	D	Gerencia	Gerencia	20.3 GB
7	Datos	D	Gerencia 2021	Gerencia	7.96 MB
8	Datos	D	Gerencia Gayco	Gerencia	2.33 GB
9	Datos	D	Gestión comercial	Gerencia comercial	437 MB
10	Datos	D	HSEQ	HSEQ	2.49 GB
11	Datos	D	Mantenimiento	Mantenimiento	152 MB
12	Datos	D	Operaciones	Operaciones	32.9 GB
13	Datos	D	Proveedores 2022	Compras	2.08 GB
14	Datos	D	Seguridad física	Seguridad física	174 GB
15	Datos	D	Sistema de gestión	HSEQ	142 GB
16	Datos	D	Talento humano	Talento humano	79.4 GB
17	Datos	D	Tesorería	Tesorería	1.29 GB
18	Datos	D	Vehículos	Seguridad física	74.5 GB

Nota. Activos de información categoría Datos de la empresa transportes Gayco.

En la Tabla 3 se presenta el inventario de activos de información correspondiente a la categoría Claves criptográficas, identificados como parte de los mecanismos de protección de la información de la organización.

Tabla 3

Inventario de Activos de Información de la Categoría Claves Criptográficas de Transportes

Gayco

Código	Nombre	Nomenclatura del activo	Descripción	Responsable	Cantidad
19	Claves criptográficas	K	BitLocker discos externos	IT	3

Nota. Claves criptográficas de la empresa transportes Gayco.

En la Tabla 4 se presenta el inventario de activos de información correspondiente a la categoría Hardware, utilizados para el soporte de la infraestructura tecnológica de la organización.

Tabla 4

Inventario de Activos de Información de la Categoría Hardware de Transportes Gayco

Código	Nombre	Nomenclatura del activo	Descripción	Responsable	Cantidad
20	Hardware	HW	Servidor ecoplanta	IT	1
21	Hardware	HW	Servidor hipervisor	IT	1
22	Hardware	HW	Servidor Soluxionar	IT	1
23	Hardware	HW	Servidor dominio	IT	1
24	Hardware	HW	Servidores de archivos	IT	1
25	Hardware	HW	Monitores	IT	2
26	Hardware	HW	Switch administrable	IT	3
27	Hardware	HW	Switch almacén	IT	1
28	Hardware	HW	UTM	MediaCommerce	1
29	Hardware	HW	Router proveedores	IT	2
30	Hardware	HW	Access point	IT	5

Nota. Hardware de la empresa Transportes Gayco.

La Tabla 5 presenta el inventario de activos de información correspondiente a la categoría Redes y comunicaciones, identificados como parte de la infraestructura de conectividad de la organización.

Tabla 5

Inventario de Activos de Información de la Categoría Redes y Comunicaciones de Transportes Gayco

Código	Nombre	Nomenclatura del activo	Descripción	Responsable	Cantidad
31	Redes y comunicaciones	COM	LAN	IT	1
32	Redes y comunicaciones	COM	Internet empresarial backup	IFX	1
33	Redes y comunicaciones	COM	Internet empresarial	MediaCommerce	1
34	Redes y comunicaciones	COM	Red inalámbrica	IT	5

Nota. Redes y comunicaciones empresa Transportes Gayco

En la Tabla 6 se presenta el inventario de activos de información correspondiente a la categoría Soportes de información, utilizados para el almacenamiento y respaldo de la información de la organización.

Tabla 6

Inventario de Activos de Información de la Categoría Soportes de Información de Transportes Gayco

Código	Nombre	Nomenclatura del activo	Descripción	Responsable	Cantidad
35	Soportes de información	MEDIA	Servidor NAS Ecoplanta	IT	1
36	Soportes de información	MEDIA	Disco duro externo	IT	1

Código	Nombre	Nomenclatura del activo	Descripción	Responsable	Cantidad
37	Soportes de información	MEDIA	Servidor NAS Soluxionar	IT	1

Nota. Soportes de información empresa Transportes Gayco

En la Tabla 7 se presenta el inventario de activos de información correspondiente a la categoría Software de aplicaciones, utilizados para el soporte de los procesos operativos y administrativos de la organización.

Tabla 7

Inventario de Activos de Información de la Categoría Software de Aplicaciones de Transportes Gayco

Código	Nombre	Nomenclatura del activo	Descripción	Responsable	Cantidad
38	Software de aplicaciones	SW	Syscom	Syscom	1
39	Software de aplicaciones	SW	Docuarchive	Contasoft	1
40	Software de aplicaciones	SW	Antivirus Kaspersky Office Small	IT	4
41	Software de aplicaciones	SW	Plataforma GLPI	IT	1
42	Software de aplicaciones	SW	Plataforma OCS Inventory	IT	1
43	Software de aplicaciones	SW	VPN Sophos	MediaCommerce	1

Nota. Software empresa Transportes Gayco.

En la Tabla 8 se presenta el inventario de activos de información correspondiente a la categoría Personal, que interviene en la gestión, administración y soporte de los sistemas de información de la organización.

Tabla 8*Inventario de Activos de Información de la Categoría Personal de Transportes Gayco*

Código	Nombre	Nomenclatura del activo	Descripción	Responsable	Cantidad
44	Personal	P	Director T.I.	Gerencia	1
45	Personal	P	Gerencia	Junta directiva	1
46	Personal	P	Auxiliar T.I.	Director T.I.	1
47	Personal	P	Consultor T.I.	Gerencia	1

Nota. Personal de la empresa Transportes Gayco.

En la Tabla 9 se presenta el inventario de activos de información correspondiente a la categoría Servicios, los cuales soportan la operación, conectividad y disponibilidad de los sistemas de información de la organización.

Tabla 9*Inventario de Activos de Información de la Categoría Servicios de Transportes Gayco*

Código	Nombre	Nomenclatura del activo	Descripción	Responsable	Cantidad
48	Servicios	S	Correo Microsoft Office 365	Controles empresariales	72
49	Servicios	S	Dominio	GoDaddy	5
50	Servicios	S	Hosting	Bluehost	4
51	Servicios	S	Virtualización	IT	1
52	Servicios	S	RDS	IT	1
53	Servicios	S	Almacenamiento en la nube	Dropbox	2

Nota. Servicios empresa Transportes Gayco.

En la Tabla 10 se presenta el inventario de activos de información correspondiente a la categoría Elementos auxiliares, que brindan soporte a la infraestructura tecnológica.

Tabla 10*Inventario de Activos de Información de la Categoría Elementos Auxiliares de Transportes**Gayco*

Código	Nombre	Nomenclatura del activo	Descripción	Responsable	Cantidad
54	Elementos auxiliares	AUX	Aire acondicionado cuarto de equipos	IT	1
55	Elementos auxiliares	AUX	UPS	IT	2
56	Elementos auxiliares	AUX	Planta eléctrica	IT	1

Nota. Elementos auxiliares empresa Transportes Gayco.

En la Tabla 11 se presenta el inventario de activos de información correspondiente a la categoría Instalaciones, relacionadas con los espacios físicos que soportan la operación de los sistemas de información de la organización.

Tabla 11*Inventario de Activos de Información de la Categoría Instalaciones de Transportes Gayco*

Código	Nombre	Nomenclatura del activo	Descripción	Responsable	Cantidad
57	Instalaciones	L	Data center	IT	1

Nota. Instalaciones empresa Transportes Gayco.***Valoración de los Activos***

Se establecen los siguientes criterios de valoración cuantitativa eligiendo una escala detallada de seis valores, siendo cero un valor despreciable a efectos de riesgo y seis un valor que afectaría gravemente a la organización. Estos valores cuentan con su correspondiente significado cualitativo, teóricamente se puede utilizar cualquier valor siempre y cuando se utilice una escala

común que permita comparar riesgos en todas las dimensiones (Ministerio de Hacienda y Función Pública, 2018)

En la Tabla 12 se presentan los criterios de valoración utilizados para asignar el nivel de impacto de los activos de información, relacionando el valor cuantitativo (0 a 6) con su correspondiente interpretación cualitativa, con el fin de estandarizar la evaluación del riesgo en la organización.

Tabla 12

Criterios de Valoración

Detalle del criterio	Valor cuantitativo	Valor cualitativo
Daño o impacto muy alto en los objetivos de la organización	6	Muy alto
Daño o impacto alto en los objetivos de la organización	$> 4 \text{ y } < 6$	Alto
Daño o impacto medio en los objetivos de la organización	$> 2 \text{ y } < 4$	Medio
Daño o impacto bajo en los objetivos de la organización	$> 0 \text{ y } < 2$	Bajo
Daño o impacto irrelevante en los objetivos de la organización	0	Irrelevante

Nota. Los criterios de valoración cuantitativa se establecen en un rango de 0, que representa un daño irrelevante, hasta 6, que corresponde a un daño o impacto muy alto en la organización.

Dimensiones de Valoración. Cuando se materializa una amenaza las dimensiones se utilizan para valorar las consecuencias en cuanto a disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, se hacen unas preguntas clave y de acuerdo con la respuesta se determina si el valor es alto o bajo determinando la afectación en los objetivos de la organización.

En la Tabla 13 se presentan las dimensiones de valoración empleadas para evaluar el impacto de los activos de información en función de su disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

Tabla 13*Descripción de las Dimensiones de Valoración*

Dimensión	Pregunta	Descripción
Disponibilidad (D)	¿Qué relevancia tiene el activo si no está disponible?	Tendrá un valor muy alto si el activo, al no estar disponible, afecta considerablemente la continuidad de la operación. Será bajo si no afecta las operaciones.
Integridad (I)	¿Qué relevancia tiene el activo si este es modificado o alterado?	Tendrá un valor muy alto si el activo, al ser modificado o alterado, afecta gravemente a la empresa. Será bajo si los cambios no afectan las operaciones.
Confidencialidad (C)	¿Qué relevancia tiene el activo si es manipulado o conocido por una persona no autorizada?	Tendrá un valor muy alto si exponer o divulgar el activo ocasiona consecuencias negativas. Será bajo si no genera consecuencias.
Autenticidad (A)	¿Qué relevancia tiene el activo si no se controla el acceso?	Tendrá un valor muy alto si no se controla el acceso al activo, ocasionando afectaciones a la empresa.
Trazabilidad (T)	¿Qué relevancia tiene el activo si no existe constancia de su uso?	Será muy alto si el seguimiento de su uso no se puede controlar. Será bajo si el seguimiento es controlable.

Nota. La tabla describe los criterios que deben considerarse para la valoración de las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de los activos de información en la organización Transportes Gayco.

Análisis de la Valoración de Activos. El resultado del análisis muestra 27 activos que presentan una afectación muy alta teniendo en cuenta el promedio de todas las dimensiones de valoración que presentan resultados mayores a 6. 5 de estos activos se encuentran clasificados como datos, 9 de estos activos se clasifican como hardware, 5 se clasifican como redes de comunicaciones, 2 de media, 1 de software, 2 de servicios, 3 de equipamiento auxiliar y el activo

de instalaciones el data center, estos son activos críticos para la organización en donde se deben centrar esfuerzos para su protección y correcto funcionamiento.

Adicionalmente se deben tener en cuenta activos de valor alto cuyo resultado cuantitativo presentan valores mayores a 4 y menores que 6, de estos se determinaron que 24 activos en total pertenecen a este rango, clasificándose como activos muy importantes en la organización en donde cualquier afectación a las dimensiones de valoración puede afectar de manera significativa los objetivos estratégicos de transportes Gayco S.A.S

En la Tabla 14 se presenta la valoración del impacto de los activos de información correspondientes a la categoría Datos, a partir del análisis de las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, con el fin de determinar su nivel de afectación sobre los objetivos de la organización.

Tabla 14

Valoración de Impacto de los Activos de Información de la Categoría Datos

Activo	D I C A T	Valor cuantitativo	Valor cualitativo
Gestión documental	3 6 2 4 6	4.2	Alto
Almacén	4 6 3 3 6	4.4	Alto
Compras	4 6 3 3 6	4.4	Alto
Contabilidad	6 6 5 5 5	5.4	Alto
Facturación	6 6 5 5 5	5.4	Alto
Gerencia	6 6 6 6 6	6.0	Muy alto
Gerencia 2021	6 6 6 6 6	6.0	Muy alto
Gerencia Gayco	6 6 6 6 6	6.0	Muy alto
Gestión comercial	4 6 5 5 5	5.0	Alto
HSEQ	4 6 4 4 3	4.2	Alto
Mantenimiento	3 6 3 4 4	4.0	Alto
Operaciones	6 6 6 6 5	5.8	Alto
Proveedores 2022	3 3 3 3 3	3.0	Medio
Seguridad física	5 6 5 5 5	5.2	Alto
Sistema de gestión	3 6 5 5 5	4.8	Alto
Talento humano	6 6 6 6 6	6.0	Muy alto

Activo	D I C A T	Valor cuantitativo	Valor cualitativo
Tesorería	6 6 6 6 6	6.0	Muy alto
Vehículos	3 6 3 3 3	3.6	Medio

Nota. La valoración cuantitativa corresponde al promedio de las dimensiones de disponibilidad (D), integridad (I), confidencialidad (C), autenticidad (A) y trazabilidad (T), según los criterios definidos previamente.

En la Tabla 15 se presenta la valoración de impacto de los activos de información correspondientes a la categoría Claves criptográficas, considerando las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

Tabla 15

Valoración de Impacto de los Activos de Información de la Categoría Claves Criptográficas

Activo	D I C A T	Valor cuantitativo	Valor cualitativo
BitLocker discos externos	6 6 6 6 6	6.0	Muy alto

Nota. La valoración cuantitativa corresponde al promedio de las dimensiones de disponibilidad (D), integridad (I), confidencialidad (C), autenticidad (A) y trazabilidad (T).

En la Tabla 16 se presenta la valoración de impacto de los activos de información correspondientes a la categoría Hardware, a partir de las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

Tabla 16

Valoración de Impacto de los Activos de Información de la Categoría Hardware

Activo	D I C A T	Valor cuantitativo	Valor cualitativo
Servidor Ecoplanta	6 6 6 6 6	6.0	Muy alto
Servidor Soluxionar	6 6 6 6 6	6.0	Muy alto
Servidor hipervisor	6 6 6 6 6	6.0	Muy alto
Servidor dominio	6 6 6 6 6	6.0	Muy alto

Activo	D I C A T	Valor cuantitativo	Valor cualitativo
Servidores de archivos	6 6 6 6 6	6.0	Muy alto
Switch administrable	6 6 6 6 6	6.0	Muy alto
Switch almacén	5 3 5 5 5	4.6	Alto
UTM	6 6 6 6 6	6.0	Muy alto
Router proveedores	6 6 6 6 6	6.0	Muy alto
Access point	5 5 5 5 6	5.2	Alto
Monitores	6 3 1 6 3	3.8	Medio

Nota. La valoración cuantitativa corresponde al promedio de las dimensiones de disponibilidad

(D), integridad (I), confidencialidad (C), autenticidad (A) y trazabilidad (T).

En la Tabla 17 se presenta la valoración del impacto de los activos de información correspondientes a la categoría Redes y comunicaciones, considerando las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

Tabla 17

Valoración de Impacto de los Activos de Información de la Categoría Redes y Comunicaciones

Activo	D I C A T	Valor cuantitativo	Valor cualitativo
LAN	6 6 6 6 6	6.0	Muy alto
Internet empresarial backup	4 4 5 5 5	4.6	Alto
Internet empresarial	6 6 6 6 6	6.0	Muy alto
Red inalámbrica	5 5 5 6 5	5.2	Alto

Nota. La valoración cuantitativa corresponde al promedio de las dimensiones de disponibilidad

(D), integridad (I), confidencialidad (C), autenticidad (A) y trazabilidad (T).

En la Tabla 18 se presenta la valoración del impacto de los activos de información correspondientes a la categoría Soportes de información, utilizados para el almacenamiento y respaldo de la información de la organización.

Tabla 18

Valoración de Impacto de los Activos de Información de la Categoría Soportes de Información

Activo	D I C A T	Valor cuantitativo	Valor cualitativo
Servidor NAS Ecoplanta	6 6 6 6 6	6.0	Muy alto
Disco duro externo	3 6 6 6 6	5.4	Alto
Servidor NAS Soluxionar	6 6 6 6 6	6.0	Muy alto

Nota. La valoración cuantitativa corresponde al promedio de las dimensiones de disponibilidad

(D), integridad (I), confidencialidad (C), autenticidad (A) y trazabilidad (T).

En la Tabla 19 se presenta la valoración del impacto de los activos de información correspondientes a la categoría Software de aplicaciones, considerando su influencia en los procesos operativos y administrativos de la organización.

Tabla 19

Valoración de Impacto de los Activos de Información de la Categoría Software de Aplicaciones

Activo	D I C A T	Valor cuantitativo	Valor cualitativo
Syscom	6 6 6 6 6	6.0	Muy alto
Docuarchive	6 6 3 6 6	5.4	Alto

Nota. La valoración cuantitativa corresponde al promedio de las dimensiones de disponibilidad

(D), integridad (I), confidencialidad (C), autenticidad (A) y trazabilidad (T).

En la Tabla 20 se presenta la valoración del impacto de los activos de información correspondientes a la categoría Servicios, considerando las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, con el fin de determinar su nivel de afectación sobre los objetivos de la organización.

Tabla 20

Valoración de Impacto de los Activos de Información de la Categoría Servicios

Activo	D I C A T	Valor cuantitativo	Valor cualitativo
Correo Microsoft Office 365	6 6 6 6 6	6.0	Muy alto
Dominio	6 6 6 6 6	6.0	Muy alto
Hosting	4 6 2 5 2	3.8	Medio
Almacenamiento en la nube	4 6 6 6 6	5.6	Alto
Virtualización	6 6 6 6 6	6.0	Muy alto
RDS	6 6 6 6 6	6.0	Muy alto

Nota. La valoración cuantitativa corresponde al promedio de las dimensiones de disponibilidad (D), integridad (I), confidencialidad (C), autenticidad (A) y trazabilidad (T), de acuerdo con los criterios definidos previamente.

En la Tabla 21 se presenta la valoración del impacto de los activos de información correspondientes a la categoría Personal, considerando las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, con el fin de determinar su nivel de afectación sobre los objetivos de la organización.

Tabla 21

Valoración de Impacto de los Activos de Información de la Categoría Personal

Activo	D I C A T	Valor cuantitativo	Valor cualitativo
Director de T.I.	5 5 6 5 5	5.2	Alto
Auxiliar T.I.	3 3 5 5 5	4.2	Alto
Gerencia	5 5 5 5 4	4.8	Alto
Consultor T.I.	2 4 5 4 2	3.4	Medio

Nota. La valoración cuantitativa corresponde al promedio de las dimensiones de disponibilidad (D), integridad (I), confidencialidad (C), autenticidad (A) y trazabilidad (T), de acuerdo con los criterios definidos previamente.

En la Tabla 22 se presenta la valoración del impacto de los activos de información correspondientes a la categoría Elementos auxiliares, considerando las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, con el fin de determinar su nivel de afectación sobre los objetivos de la organización.

Tabla 22

Valoración de Impacto de los Activos de Información de la Categoría Elementos Auxiliares

Activo	D I C A T	Valor cuantitativo	Valor cualitativo
Aire acondicionado cuarto de equipos	6 6 6 6 6	6.0	Muy alto
UPS	6 6 6 6 6	6.0	Muy alto
Planta eléctrica	6 6 6 6 6	6.0	Muy alto

Nota. La valoración cuantitativa corresponde al promedio de las dimensiones de disponibilidad (D), integridad (I), confidencialidad (C), autenticidad (A) y trazabilidad (T), de acuerdo con los criterios definidos previamente.

En la Tabla 23 se presenta la valoración del impacto de los activos de información correspondientes a la categoría Instalaciones, considerando su relevancia para la continuidad operativa y la seguridad de la infraestructura tecnológica de la organización.

Tabla 23

Valoración de Impacto de los Activos de Información de la Categoría Instalaciones

Activo	D I C A T	Valor cuantitativo	Valor cualitativo
Data center	6 6 6 6 6	6.0	Muy alto

Nota. La valoración cuantitativa corresponde al promedio de las dimensiones de disponibilidad (D), integridad (I), confidencialidad (C), autenticidad (A) y trazabilidad (T), de acuerdo con los criterios definidos previamente.

Determinar las Amenazas y Riesgos Asociados a los Activos Tecnológicos.

Para la valoración de amenazas se tienen en cuenta todos los activos, Magerit cuenta con un catálogo de amenazas que tiene mas de 58 componentes en donde cada una cuenta con un código, el tipo de activo, las dimensiones que se ven afectadas por la amenaza ordenadas de la más a menos relevante y por último la descripción.

También se tiene en cuenta la frecuencia que es la probabilidad de que la amenaza se materialice en un determinado tiempo y de acuerdo con Magerit se valora de la siguiente forma:

En la Tabla 24 se presenta la valoración de la amenaza en cuanto a su frecuencia de ocurrencia, relacionando la valoración cualitativa con su correspondiente valor cuantitativo, con el fin de estimar la probabilidad de materialización de las amenazas.

Tabla 24

Valoración de la Amenaza en Cuanto a Frecuencia

Valoración cualitativa	Frecuencia	Valor cuantitativo
Muy alta (MA)	A diario	5
Alta (A)	Mensualmente	4
Media (M)	Una vez al año	3
Baja (B)	Cada varios años	2
Muy baja (MB)	Cada 10 años	1

Nota. La tabla presenta la relación entre la valoración cualitativa y cuantitativa de la frecuencia con la que una amenaza puede repetirse.

Adicionalmente se tiene en cuenta la degradación que es el desgaste del activo sufre cada vez que una amenaza se materializa, para un análisis práctico manejamos una degradación leve o mínima valorada cuantitativamente con el 1%, una degradación intermedia valorada en 50% y una degradación muy alta del 100% en donde el activo sufriría un daño en la totalidad de sus componentes.

Posteriormente tenemos en cuenta el impacto en donde se determina que tanto daño hace la amenaza a la organización para cumplir sus objetivos en donde el valor 1 se determina como muy bajo, el 2 bajo, el 3 medio, el 5 alto y el 8 muy alto.

Por último, se toman los valores dados cuantitativamente de la degradación y el impacto para determinar el daño impacto cuantitativo, para esto se debe tener en cuenta la siguiente tabla.

En la Tabla 25 se presenta la matriz de degradación utilizada para determinar el nivel de impacto de los riesgos, relacionando el impacto cualitativo con el porcentaje de degradación del activo, con el fin de priorizar las acciones de tratamiento.

Tabla 25

Matriz de Degradación Según el Nivel de Impacto

Impacto	1 %	50 %	100 %
Muy alto	3	5	8
Alto	2	3	5
Medio	1	2	3
Bajo	1	1	2
Muy bajo	1	1	1

Nota. La matriz permite priorizar las acciones de gestión del riesgo en función del nivel de impacto y el grado de degradación del activo.

Ejemplo: Un impacto "Muy alto" (8) con degradación 100% tendría la máxima puntuación (8), lo que indicaría un problema crítico que requiere atención inmediata.

Un impacto "Bajo" (2) con degradación 1% tendría una puntuación baja (1), lo que sugiere un riesgo mínimo.

A partir de los criterios de frecuencia, degradación e impacto, se llevó a cabo la valoración de las amenazas que afectan a los activos de información. El análisis completo y detallado de dicha valoración se presenta en el Anexo A.

Valoración de Riesgos

Según (Whitman & Mattord, 2021) El riesgo informático es la probabilidad de que una amenaza explote una vulnerabilidad, causando daños a sistemas o datos.

Cuanto más veces se repita esta probabilidad mayor es el riesgo de que esta se termine materializando y afectando a la organización, de acuerdo a este concepto para realizar la siguiente valoración de riesgos se toman en cuenta todos los ítems tomados en la valoración de amenazas relacionadas en el anexo A excepto la columna de degradación, tomando como ítems más relevantes la probabilidad (frecuencia) y el daño impacto valor cuantitativo, estos dos ítems se multiplican y da los valores como se ejemplifica en la siguiente tabla:

En la Tabla 26 se presenta la matriz de riesgo utilizada para determinar el nivel de riesgo resultante a partir de la combinación entre la probabilidad de ocurrencia y el impacto asociado a las amenazas identificadas.

Tabla 26

Matriz de Riesgo

Probabilidad \ Impacto	1	2	3	5	8
5	5	10	15	25	40
4	4	8	12	20	32
3	3	6	9	15	24
2	2	4	6	10	16
1	1	2	3	5	8

Nota. El valor mínimo de la probabilidad o frecuencia es 1 y el valor máximo es 5; en cuanto al impacto, el valor mínimo es 1 y el valor máximo es 8. El nivel de riesgo se obtiene a partir del producto entre la probabilidad y el impacto.

Con el resultado obtenido podemos determinar el nivel de riesgo cualitativo identificando los activos con mayor probabilidad de ser afectados por una amenaza que nos representan un nivel de riesgo significativo.

En la Tabla 27 se presenta la clasificación del nivel de riesgo utilizada para interpretar los valores obtenidos a partir de la matriz de riesgo, permitiendo establecer la prioridad de tratamiento de los riesgos identificados.

Tabla 27

Nivel de Riesgo

Rango del valor	Nivel de riesgo
11–40	Extremo
8–10	Intolerante
3–7	Tolerante
1–2	Aceptable

Nota. La tabla establece la categorización del nivel de riesgo en función del valor obtenido del producto entre la probabilidad y el impacto, de acuerdo con la metodología aplicada.

De acuerdo con los criterios definidos para la evaluación del riesgo, se realizó la valoración detallada de los riesgos asociados a los activos de información, considerando la probabilidad de ocurrencia y el impacto correspondiente. El desarrollo completo de esta valoración se presenta en el Anexo B.

Selección de los Activos Críticos Data Center Transportes Gayco S.A.S

Para la selección de los activos críticos de la empresa, tomamos el valor cuantitativo del riesgo dado en el anexo B y sumamos cada uno de estos valores que pertenecen al activo correspondiente, determinando así un valor de riesgo total por activo.

Creamos una tabla denominada riesgo total por activo y la personalizamos de acuerdo a los valores mínimos y máximos que se dieron como resultado de la suma del nivel de riesgo cualitativo por activo.

En la Tabla 28 se presenta la clasificación del riesgo total por activo, obtenida a partir de la suma de los valores de riesgo asociados a cada activo, con el fin de determinar su nivel de criticidad y la prioridad de tratamiento.

Tabla 28

Riesgo Total por Activo

Rango de riesgo cuantitativo	Nivel de riesgo	Interpretación
300–449	Extremo	Riesgo crítico. Requiere acciones inmediatas y mitigación prioritaria.
150–299	Intolerante	Riesgo alto. Necesita planificación urgente para reducir el impacto.
50–149	Tolerante	Riesgo moderado. Monitorear y aplicar controles según disponibilidad.
42–49	Aceptable	Riesgo bajo. No requiere acciones inmediatas, pero se debe mantener supervisión.

Nota. La tabla presenta la interpretación de la valoración cuantitativa y cualitativa del riesgo total, obtenida a partir de la suma de los valores de riesgo asociados a cada activo.

Como podemos observar en la tabla 28 el valor mínimo arranca desde 42 a 49 el cual es un nivel de riesgo aceptable que no requiere acciones inmediatas por parte de la organización.

El valor de 50 a 149 es un nivel que se determina tolerante, el cual se recomienda tener en cuenta para tomar acciones, pero no de manera inmediata.

El nivel intolerante empieza desde 150 hasta 299 y se le recomienda a la organización empezar a planificar acciones para que no afecte a la organización.

Por último, tenemos el nivel extremo su valor comienza en 300 y termina en 499 que fue el valor del activo más alto en este análisis, la organización debe tomar acciones inmediatas de mitigación y luego de obtener los valores cuantitativos y cualitativos asociados a cada riesgo identificado, se procedió a aplicar dichos resultados en la tabla de riesgo total por activo, con el fin de determinar el nivel de criticidad de cada activo de información. Este proceso se realizó tomando como base la tabla de valoración de riesgos en el anexo B, en la cual se integran los valores de probabilidad e impacto para establecer la clasificación final del riesgo. El desarrollo detallado de esta valoración se presenta en el Anexo C. del presente documento.

Luego de tener esta información se determina cuantos activos pertenecen a cada uno de los niveles riesgos definidos teniendo como resultado que la organización presenta la mayoría de sus activos en el data center con un nivel de riesgo extremo.

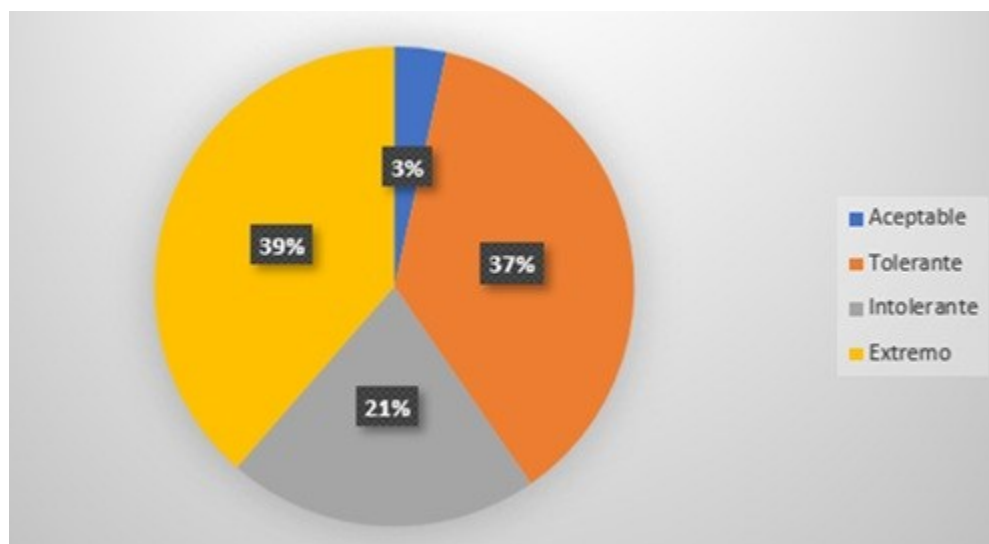
En la **Tabla 29** se presenta la cantidad de activos de información clasificados según su nivel de riesgo, con el fin de evidenciar la distribución y concentración de activos en cada categoría de riesgo identificada.

Tabla 29

Cantidad de Activos por Nivel de Riesgo

Nivel de riesgo	Cantidad de activos
Aceptable	2
Tolerante	21
Intolerante	12
Extremo	22

Nota. La tabla muestra la cantidad de activos de información clasificados por nivel de riesgo, permitiendo identificar aquellos que requieren mayor prioridad de tratamiento.

Figura 4*Porcentaje de Activos por Nivel de Riesgo*

Nota. La figura muestra la distribución porcentual de los activos de información según su nivel de riesgo, con base en los resultados obtenidos en la Tabla 29.

Como podemos observar en la Figura 4 de 57 activos tan solo el 3% presenta un nivel de riesgo aceptable, el 37% un nivel de riesgo tolerante, el 21% intolerante y el 39% presenta un riesgo extremo.

Proponer un Conjunto de Métricas y Componentes Específicos a Monitorear para Cada Activo Crítico Identificado

Para el cumplimiento de este objetivo tomaremos todos los activos de información que presente un nivel de riesgo extremo tomados del Anexo C, para ser monitoreados de manera integral, debido a que la empresa transportes Gayco necesita tomar acciones inmediatas para comenzar con la mitigación de los riesgos identificados se identificaron 22 activos de información con este tipo de riesgo representados en la siguiente tabla.

En la Tabla 30 se presentan los activos de información identificados con nivel de riesgo extremo, con el fin de priorizar su tratamiento dentro del proceso de gestión de riesgos de la organización.

Tabla 30

Activos con Riesgo Extremo

N.º	Tipo de activo	Cod. activo	Activo	Riesgo total cuantitativo	Nivel de riesgo
1	Hardware	HW	Servidor Ecoplanta	373	Extremo
2	Hardware	HW	Servidor hipervisor	373	Extremo
3	Hardware	HW	Servidor dominio	373	Extremo
4	Hardware	HW	Servidores de archivos	373	Extremo
5	Hardware	HW	Servidor Soluxionar	373	Extremo
6	Hardware	HW	Switch administrable	373	Extremo
7	Hardware	HW	UTM	373	Extremo
8	Redes y comunicaciones	COM	Router proveedores	373	Extremo
9	Redes y comunicaciones	COM	LAN	306	Extremo
10	Redes y comunicaciones	COM	Internet empresarial backup	388	Extremo
11	Redes y comunicaciones	COM	Internet empresarial	444	Extremo
12	Redes y comunicaciones	COM	Red inalámbrica	312	Extremo
13	Soportes de información	MEDIA	Servidor NAS Soluxionar	440	Extremo
14	Software	SW	Syscom	449	Extremo
15	Software	SW	Docuarchive	449	Extremo
16	Servicios	S	Dominio	415	Extremo
17	Servicios	S	Almacenamiento en la nube	305	Extremo
18	Servicios	S	Virtualización	423	Extremo
19	Servicios	S	RDS	423	Extremo
20	Elementos auxiliares	AUX	Aire acondicionado cuarto de equipos	382	Extremo
21	Elementos auxiliares	AUX	UPS	424	Extremo

N.º Tipo de activo	Cod. activo	Activo	Riesgo total cuantitativo	Nivel de riesgo
22 Elementos auxiliares	AUX	Planta eléctrica	415	Extremo

Nota. Se identificaron 22 activos de información clasificados con nivel de riesgo extremo, los cuales requieren tratamiento prioritario.

Ahora se identifican los elementos, componentes y características que se tendrán en cuenta para monitorear cada activo anteriormente seleccionado por su nivel de riesgo.

Como en la organización se cuenta con 5 servidores sus elementos y componentes a monitorear son los mismos.

Según (Julian, 2017) el diseño de un sistema de monitoreo efectivo en un centro de datos debe incluir tanto la infraestructura física como consumo de energía, temperatura, ventilación y disponibilidad de hardware como los componentes lógicos relacionados con aplicaciones, servicios de red y seguridad. De esta forma, el monitoreo integral permite detectar anomalías de forma temprana, mejorar la eficiencia operativa y garantizar la continuidad del servicio.

De acuerdo con los resultados obtenidos del análisis de riesgos, se elaboró el Anexo D, en el cual se presentan las características, elementos y componentes a monitorear por cada activo de información de la empresa Transportes Gayco S.A.S.. Este anexo tiene como finalidad apoyar el proceso de seguimiento y control, permitiendo identificar los aspectos críticos que deben ser supervisados para reducir la probabilidad de materialización de riesgos y asegurar la continuidad de los servicios.

Comparación de Sistemas Operativos, Aplicaciones, Sensores, Protocolos y Componentes Electrónicos a Través de una Matriz de Evaluación que Permita Seleccionar los Componentes más Eficientes de Monitoreo para Generación de Alertas en Tiempo Real.

Sistemas Operativos Recomendados para el Monitoreo de Data Center

Los sistemas operativos juegan un papel crucial en el monitoreo y la administración de centros de datos, ya que se recomienda el uso de sistemas operativos robustos y estables, tales como Linux y Windows Server, además de sistemas embebidos en equipos de red y energía, dado que ofrecen soporte nativo para protocolos de monitoreo como SNMP y WMI, asegurando compatibilidad y escalabilidad.(Zheng et al., 2019)

De acuerdo con esto haremos una descripción exhaustiva de los sistemas operativos más populares para el monitoreo de equipos en un data center.

Ubuntu Server. Este sistema operativo se ha consolidado como una de las alternativas más confiables para la gestión y monitoreo integral de dispositivos TI, incluyendo servidores, equipos de red, sistemas de climatización y elementos de seguridad, con un diseño modular y de código abierto permite la integración de plataformas como *Nagios*, *Zabbix* o *ntopng*, optimizando la recolección de métricas en tiempo real y la generación de alertas tempranas, Ubuntu destaca por su bajo consumo de recursos, estabilidad, costo y capacidad de personalización, lo que facilita su implementación en entornos heterogéneos y escalables.

De acuerdo con (Sahara et al., 2024) Ubuntu Server ha demostrado ser eficiente en la creación de sistemas de monitoreo y seguridad de redes, evidenciando su versatilidad y eficacia en escenarios prácticos, todas estas características, sumadas a su amplio soporte comunitario y actualizaciones constantes, convierten a Ubuntu Server en una plataforma idónea para incrementar la disponibilidad de los servicios y reducir el tiempo medio entre fallas (MTBF) y de

reparación (MTTR), factores críticos en la operación de un datacenter moderno como el que tiene la empresa transportes Gayco.

Red Hat Enterprise Linux. Según (Red Hat Documentation., 2025) este sistema operativo se perfila como una plataforma altamente adecuada para el monitoreo en centros de datos, debido a su robustez, capacidades integradas y soporte activo. La documentación técnica oficial destaca que Red Hat incorpora herramientas de monitoreo de rendimiento como TuneD, perf y Performance Co-Pilot (PCP), las cuales permiten recolectar métricas clave del sistema, visualizar actividad, detectar cuellos de botella y optimizar el uso de recursos como CPU, memoria y energía.

De acuerdo con el portal (Rooted In Linux., 2024) el ecosistema de Red Hat Enterprise incluye RHEL System Roles, módulos automatizados que pueden ser gestionados mediante Ansible, estos roles permiten configurar infraestructuras de observabilidad de forma sistemática, facilitando la provisión de agentes de monitoreo, recolección de métricas, generación de alertas y visualización mediante dashboards

Windows Server. Windows Server 2022 se presenta como un sistema operativo idóneo para el monitoreo de data centers, ya que ofrece una plataforma robusta y segura que se integra de manera nativa con herramientas como System Center Operations Manager (SCOM). Esta solución de Microsoft proporciona monitoreo centralizado de la infraestructura, recolectando métricas críticas de rendimiento, disponibilidad y seguridad en servidores, aplicaciones y servicios.

SCOM incorpora *management packs* especializados que permiten supervisar tecnologías específicas (como SQL Server, Active Directory o servicios en la nube), facilitando la detección temprana de incidentes y la correlación inteligente de eventos. Al integrarse con entornos

híbridos mediante Azure, SCOM potencia las capacidades de Windows Server 2022 al ofrecer visibilidad completa del centro de datos y automatización en la respuesta a fallas, lo que refuerza la continuidad operativa y la gestión proactiva de infraestructuras modernas que demandan alta disponibilidad y seguridad reforzada (DevX Editorial Staff., 2024)

Vmware ESXi. VMware ESXi presenta características interesantes para el monitoreo integral de datacenters debido a su arquitectura de hipervisor bare-metal, que permite ejecutar múltiples máquinas virtuales sobre un único hardware físico y gestionar de manera centralizada los recursos de todo el centro de datos.

Según (Savola, 2021) ESXi facilita la supervisión de métricas críticas de rendimiento, como CPU, memoria, almacenamiento y red entre otros, no solo a nivel de servidor individual, sino también a través de clústeres y entornos virtualizados completos ademas de la integración con herramientas como vCenter Server que permite consolidar información de múltiples hosts, crear alertas proactivas, optimizar recursos y garantizar la disponibilidad y continuidad operativa de aplicaciones y servicios, todas estas capacidades hacen de ESXi una solución robusta para la administración y monitoreo integral de infraestructuras modernas, ofreciendo visibilidad completa y control centralizado de todos los componentes críticos del datacenter para el monitoreo y gestión integral de infraestructuras críticas.

Aplicaciones para el Monitoreo Integral o Parcial de Data Center

Zabbix. Zabbix es una solución de monitoreo empresarial de código abierto que permite la supervisión de servidores, redes, aplicaciones y servicios, permite integración con protocolos SNMP, IPMI, JMX entre otros, facilitando el monitoreo de dispositivos como UPS, aires acondicionados y plantas eléctricas, con arquitectura escalable y su capacidad para almacenar

datos en bases de datos relacionales lo hacen adecuado para entornos de datacenters.(Zabbix LLC., 2023)

Nagios Core. Nagios Core es una plataforma de monitoreo de código abierto que proporciona monitoreo de servidores, redes y aplicaciones, utilizando SNMP para la supervisión de dispositivos de red y puede integrarse con sensores de temperatura y otros dispositivos mediante plugins personalizados, además es compatible con sistemas operativos Linux, Windows y Unix, y permite la personalización a través de su arquitectura modular.(Nagios Enterprises, 2022)

Prometheus con SNMP Exporter. Prometheus es un sistema de monitoreo de código abierto que utiliza un modelo de datos dimensional y un lenguaje de consulta flexible mediante del SNMP Exporter, Prometheus puede recolectar métricas de dispositivos que soportan SNMP, como switches, routers y sensores de infraestructura, todos los datos recolectados pueden visualizarse en Grafana, ofreciendo una solución completa para el monitoreo de datacenters.(Prometheus, 2023)

PRTG Network Monitor. PRTG Network Monitor es una herramienta de monitoreo que utiliza sensores para supervisar la infraestructura de TI. Soporta SNMP, WMI, HTTP, entre otros protocolos, y permite la integración con dispositivos como UPS, sistemas de climatización y sensores de temperatura, maneja una interfaz intuitiva y su capacidad de descubrimiento automático facilitan la implementación en entornos de datacenters. (Paessler AG, n.d.)

Icinga. Icinga es una herramienta de monitoreo de código abierto que ofrece supervisión de redes y servidores, Soporta SNMP y puede integrarse con dispositivos de infraestructura mediante plugins específicos, maneja una arquitectura modular y su capacidad para integrarse

con otras herramientas como Logstash puede ser adecuado para entornos de monitoreo complejos.(Icinga, 2023)

LibreNMS. LibreNMS es una plataforma de monitoreo de código abierto que se especializa en la supervisión de dispositivos de red, utiliza SNMP para recolectar métricas y ofrece integración con una amplia variedad de dispositivos, con su capacidad de descubrimiento automático y su compatibilidad con sistemas operativos Linux y Windows lo hacen adecuado para entornos de datacenters que requieren monitoreo de red junto con sistemas críticos de infraestructura eléctrica como UPS y plantas eléctricas. (DevOpsCube, 2023)

Grafana. Grafana es una plataforma de visualización y análisis de métricas open-source, que permite crear dashboards personalizados para monitoreo en tiempo real y análisis histórico. sin recopilar métricas directamente, sino que se integra con fuentes de datos como Prometheus, InfluxDB, Zabbix, LibreNMS y otros, permitiendo combinar información de servidores, redes, sensores de temperatura, UPS y sistemas de climatización, presentando compatible con entornos Windows, Linux y VMware, y permite generar alertas y reportes visuales, consolidando datos de múltiples sistemas en una vista única e integral del datacenter (Grafana Labs, 2023)

ABB Ability Data Center Automation. ABB Ability Data Center Automation es una solución industrial modular y escalable diseñada para entornos de centro de datos, tanto “on-premise” como híbridos, que integra funciones de DCIM con sistemas eléctricos (EPMS), mecánicos (como HVAC/BMS) y de infraestructura de TI bajo una única plataforma.

Es una plataforma de pago que proporciona visualización en tiempo real de los activos físicos, alertas y diagnósticos, automatización de sistemas eléctricos y de climatización, realiza apoyo para la gestión de capacidad, previsión energética y eficiencia operativa, la plataforma permite una vista a nivel de sala, zona o componente, facilita la interoperabilidad con múltiples

equipos y protocolos, reduce la dependencia de entradas manuales para métricas y KPIs, y mejora la confiabilidad, continuidad y sostenibilidad operativa (ABB, n.d.)

Sensores y Componentes Electrónicos para el Monitoreo Integral del Datacenter

Según (Katal et al., 2023b) el monitoreo inteligente de la infraestructura física de un data center mediante los diferentes sensores disponibles en el mercado puede mejorar significativamente la eficiencia energética, la detección temprana de fallos y reduce el número de alertas inesperadas, lo cual permite una operación más confiable y disponible. Por esto que identificamos los siguientes sensores que pueden ayudar a hacer mas eficiente y confiable el monitoreo del Datacenter en Transportes Gayco:

Sensor de Temperatura. (López et al., 2024) afirma que un sensor de temperatura es un dispositivo que mide la temperatura (del aire, de una superficie o de un fluido) y la transforma en una señal eléctrica o digital que puede ser leída por instrumentos, controladores o sistemas de monitoreo.

Tipos de sensores comunes. Los sensores de temperatura utilizados en sistemas de monitoreo pueden clasificarse en diferentes tipos según su principio de funcionamiento. Entre ellos se encuentran los RTD (por ejemplo, PT100), que consisten en resistencias cuyo valor varía casi linealmente con la temperatura, ofreciendo alta precisión y estabilidad. Otro tipo es el termistor, una resistencia semiconductora con gran sensibilidad en rangos reducidos de temperatura; aunque es muy preciso, su comportamiento no es lineal. También se encuentran los termopares, formados por una pareja de metales que generan una pequeña tensión eléctrica proporcional a la diferencia de temperatura, lo que les permite operar en rangos amplios y con respuesta rápida.

Existen sensores semiconductores o circuitos integrados (IC), que son chips digitales capaces de entregar la temperatura directamente en formato digital mediante protocolos como I²C, 1-Wire o RS-485, lo que facilita su integración en sistemas de monitoreo. Finalmente, los sensores infrarrojos (IR) sin contacto permiten medir la temperatura superficial a distancia, siendo útiles en aplicaciones donde no es posible o conveniente el contacto directo con el objeto de medición.

Sensor de Humedad. (Arman Kuzubasoglu, 2022) afirma que es un transductor que mide la temperatura (del aire, una superficie o un fluido) y la convierte en una señal eléctrica o digital que puede leer un instrumento, PLC, registrador o sistema de monitoreo e internamente convierte la variable térmica en resistencia, voltaje, corriente o datos digitales según la tecnología entre estos existen:

Sensores Capacitivos, miden la humedad a partir de la variación de la capacitancia de un dieléctrico higroscópico. Este tipo de sensor ofrece una respuesta estable a lo largo del tiempo y normalmente opera en un rango de medición que va desde 0 % hasta 100 % de humedad relativa (HR). Además, presentan precisiones típicas entre ± 2 % y ± 3 % HR y se caracterizan por su bajo consumo de energía, lo que los hace adecuados para aplicaciones de monitoreo continuo en entornos controlados.

Sensores Resistivos. Detectan la humedad mediante el cambio en la resistencia eléctrica de un material sensible cuando varía la cantidad de humedad presente en el ambiente. Su diseño es relativamente simple, lo que los convierte en una alternativa más económica. Sin embargo, su precisión típica suele ser alrededor de ± 5 % HR y pueden verse afectados por factores ambientales como polvo, químicos o fenómenos de condensación, lo que puede influir en la exactitud de las mediciones.

Sensor de Fugas de Agua. En el artículo (Farah & Shahrour, 2024) se define como un dispositivo diseñado para detectar la presencia de agua o humedad anómala en una ubicación concreta y convertir esa detección en una señal eléctrica o digital. Al activarse, el sensor genera una alarma local y/o la envía a un sistema de monitoreo, permitiendo respuesta automática o humana entre estos existen:

Sensores Puntuales. Estos sensores detectan agua en un punto concreto (p. ej. debajo de un rack o junto a un equipo), tienen salida típica en contacto seco / relé o salida digital y son útiles para puntos críticos y detecciones rápidas localizadas.

Cables Detectores. Es un Cable largo que detecta presencia de agua a lo largo de su longitud (linear). Es ideal para pasillos, alrededor de perimetrales, bajo losas o a lo largo de bandejas de tuberías y permiten identificar la zona aproximada de la fuga (con controladores adecuados).

Sondas de Cadena / Manguera. Son similares al cable, pero resistente y pensado para áreas industriales o sub-suelos; detecta contacto líquido a lo largo.

Interruptores de Flotador / Flotadores. Estos sensores detectan acumulación de agua que eleva el flotador (útil en sumideros, bombas de condensado y fosas) y se usan para activación por nivel.

Sensores Capacitivos / Táctiles / Ópticos. Estos sensores miden cambio de capacitancia o conductividad al contacto con líquido; a menudo más sensibles y menos propensos a corrosión. Los ópticos detectan humedad en superficie y tienen menor mantenimiento.

Sensores de Humedad Relativa / Sensores de Condensación. Estos sensores no detectan directamente una fuga, pero alertan sobre condiciones que favorecen condensación y riesgo de goteo.

Sensores Inalámbricos / IoT. Pueden ser sensores puntuales o de cable con radio (Zigbee, LoRaWAN, Wi-Fi, Sigfox) para ubicaciones sin cableado y son convenientes para instalaciones rápidas o áreas remotas; requieren gestión de baterías y seguridad.

Sensor de Humo. Según (Jayaweera & Yu, 2008) Un sensor de humo (detector de humo) es un dispositivo que detecta partículas de combustión o cambios asociados a un incendio (partículas visibles, partículas sub-visibles, luz dispersada, humo transportado por el aire) y genera una señal (relé, contacto libre de potencial, salida analógica o digital, mensaje en bus/IP) para activar alarmas, notificar sistemas de control (BMS/DCIM) o disparar acciones automáticas (supresión, corte de energía, evacuación). Internamente convierte la presencia de partículas o señales físicas en una lectura eléctrica o digital que puede procesar un panel de alarma o plataforma de monitoreo, en el mercado se encuentran los siguientes tipos:

Detectores Puntuales Fotoeléctricos (Ópticos). Detectan la dispersión de luz por partículas de humo dentro de una cámara teniendo como ventaja principal que son muy sensibles a incendios de combustión lenta o “smoldering” (humo denso). Se utiliza en la detección general en salas y pasillos y es bueno para evitar falsas alarmas por chispas.

Detectores Puntuales por Ionización. Miden cambios en la ionización de una cámara causados por partículas finas de combustión. Su ventaja principal es la respuesta rápida a incendios con llamas (partículas muy finas) y como desventaja presenta mayor susceptibilidad a falsas alarmas por aerosoles; manejo regulado por normativas.

Detectores Multicanal / Multicriterio. Combinan fotoeléctrico, termista/termopar (temperatura), CO u otros parámetros y aplican algoritmos para confirmar fuego. La ventaja principal es la alta fiabilidad y menor tasa de falsas alarmas, recomendados en entornos complejos como data centers.

Detectores por Haz (Beam Detectors). Es un haz óptico atraviesa la sala; la atenuación del haz por humo activa la alarma siendo su ventaja principal cubrir grandes espacios con pocos dispositivos (naves, salas altas). Su desventaja radica en que requieren alineación y pueden verse afectados por polvo/obstrucciones.

Detectores Aspirantes (Aspirating Systems, p. ej. VESDA). Es una red de tubos aspira aire continuamente hacia una cámara de muestreo central donde se analizan partículas con alta sensibilidad siendo su ventaja principal la detección extremadamente temprana (ideal para data centers), monitorización continua y sensibilidad ajustable. Su uso recomendado es en pasillos, bajo losas, falsos pisos y salas con alta criticidad.

Detectores Lineales / Cables Detectores. Es un cable o conjunto lineal que detecta la presencia de humo/partículas a lo largo de su longitud, utilizándose en protección perimetral o zonas largas bajo bandejas/canales.

Detectores por Aspiración con Análisis por Espectrometría / Partículas. Estos sensores presentan análisis avanzado del tamaño y tipo de partículas para distinguir fuentes (humo, polvo). Teniendo como ventaja que reduce falsos positivos y permite clasificación temprana del evento.

Apertura de Puertas. En el artículo (Malek et al., 2025) se determina que un sensor de apertura de puertas es un dispositivo que detecta si una puerta está abierta o cerrada y convierte ese estado en una señal eléctrica o digital que un sistema de monitoreo puede leer. Por lo general

consta de dos elementos: un elemento fijado al marco (electrónica) y otro a la hoja de la puerta (imán o actuador). Cuando la hoja se separa del marco, cambia el estado del sensor (cerrado o abierto) y se genera una alarma o registro. Cuenta con los siguientes tipos:

Contacto Magnético — Superficial o Empotrado. Es el sensor más común y económico. Un imán en la hoja y un contacto en el marco; cuando se separan, el contacto cambia, puede ser surface-mounted (visible) o recessed/flush (empotrado, más discreto) y su salida es en contacto seco (NC/NO).

Sensor Hall. Similar a reed pero sin contactos mecánicos; más robusto y con mayor vida útil tiene salida digital y mayor tolerancia a vibraciones.

Interruptor de Palanca. Switch mecánico que actúa cuando la puerta cierra; resistente, pero con partes móviles.

Sensores Ópticos / Fotoeléctricos de Proximidad. Detectan la presencia/posición por haz o reflexión. Útiles en puertas corredizas o vidriadas.

Sensores de Proximidad Capacitivos. Detectan cambio capacitivo al acercarse la hoja; usados en puertas con acabado especial.

Sensores Inalámbricos / IoT. Integran contactos magnéticos/ Hall y transmiten por Zigbee, LoRa, Wi-Fi, etc. Convenientes donde no se quiere cablear.

Sensores con Tamper y Diagnóstico. Incluyen detección de manipulación (desmontaje) y auto-test; recomendados en entornos críticos.

Sensores de Apertura con Autenticación Antegrada (Acceso). Combinan detector de puerta + lector RFID/teclado para control y registro de acceso

PDU Inteligente. Según (Faisal et al., 2017) Un PDU inteligente (Intelligent Power Distribution Unit, iPDU) es una unidad de distribución eléctrica para racks que, además de repartir potencia, incorpora sensores y electrónica de medida. Estos sensores miden corriente, tensión, potencia y energía, y pueden integrar sensores ambientales como de temperatura y humedad, sensores de fugas o de apertura de puerta. La iPDU convierte esas lecturas en señales eléctricas/digitales y las comunica a diferentes sistemas de monitoreo, generando alarmas y permitiendo a su vez control remoto. En el mercado existen los siguientes tipos de PDU según su funcionalidad eléctrica:

PDU Pasiva / Básica. Distribuye energía sin medición ni comunicación. (No “inteligente”.)

PDU con Medición (Metered). Mide parámetros eléctricos a nivel global del PDU (corriente total, kW, kWh) y es útil para monitoreo energético básico.

PDU con Medición por Salida (Outlet-Level Metering). Mide consumo por toma/por equipo — permite contabilizar y detectar anomalías por servidor.

PDU con Conmutación (Switched PDU). Permite cortar/activar individualmente salidas (reinicio remoto de equipos), y es frecuentemente combinado con medición por salida.

PDU con Monitorización de Circuito/Branch. Mide corrientes por rama o circuito, útil en PDUs de alta densidad y para balanceo de fases.

PDU modular / Escalable. Diseñada para crecer o cambiar módulos de medida/salida.

PDU Con Sensores Integrados. Viene con sensores ambientales integrados: temperatura (probes), humedad, presión diferencial además de sensores de detección de agua (entrada para cable detector o sensor) y sensor de apertura/tamper.y conn sensores de fuga a tierra / monitor de

corriente de fuga (GFI/earth leakage). Además tiene medidores de calidad de energía: armónicos, factor de potencia, picos/inrush.

Tableros Electrónicos Inteligentes. Un tablero eléctrico inteligente (Omokere et al., 2023) lo describe como un cuadro de distribución que, además de la función general de distribuir y proteger la energía eléctrica, incorpora medición, sensores, electrónica de control y comunicaciones. Convierte señales eléctricas como corriente, tensión, energía o eventos en datos digitales que pueden ser leídos, almacenados y gestionados por sistemas y plataformas de energía). Por lo general integra medidores, transformadores de corriente (CT), unidades de comunicaciones, relés digitales y a en algunas ocasiones PLCs o módulos de control embebidos, existiendo los siguientes tipos:

Por Función. El tablero medido (Metered) registra variables eléctricas a nivel general. El tablero monitoreado (Monitored) permite, además, la transmisión remota de datos mediante protocolos como Modbus o SNMP. El tablero controlable o conmutado (Switched/Controlled) incorpora la posibilidad de operar interruptores (breakers) de forma remota. Por su parte, el tablero multicircuito con medición por rama (Branch/Outlet-level) ofrece visibilidad granular por circuito o equipo específico. Finalmente, el tablero con lógica o PLC integrada permite ejecutar automatizaciones locales complejas sin depender directamente de un sistema SCADA.

Por Nivel de Tensión. Existen tableros de media tensión (MT) — tableros y celdas con relés digitales y comunicación IEC 61850 y de baja tensión (BT) — tableros rack/room para distribución final; muy usados en data centers.

Por Arquitectura Física. Según su arquitectura física, los tableros pueden clasificarse en monolíticos o centralizados, donde un tablero principal (MSB/MDB) alimenta subtableros dependientes. También pueden ser modulares o escalables, compuestos por módulos

intercambiables que permiten ampliar o ajustar la capacidad sin reemplazar completamente el sistema. Finalmente, existen configuraciones redundantes o de doble bus (dual-bus), diseñadas para garantizar alta disponibilidad mediante esquemas de alimentación A/B.

Por Funcionalidades Especiales. En función de sus características avanzadas, los tableros pueden incorporar sistemas de transferencia automática (ATS) para la gestión de fuentes primarias y secundarias de alimentación y pueden integrar capacidades de análisis de calidad de energía, incluyendo la medición de armónicos y flicker. Algunos modelos incluyen protección diferencial o monitoreo de fuga a tierra, orientados a la seguridad eléctrica. Finalmente, existen tableros integrados con sistemas de supresión o detección de incendios, diseñados para entornos críticos donde la continuidad operativa y la protección son prioritarias.

Brakers Inteligentes. (Yin et al., 2022) describe a un breaker inteligente como un dispositivo de protección eléctrico que, además de realizar la función tradicional de abrir, cerrar y proteger contra sobre corriente, cortocircuito y fallo a tierra, incorpora medición, electrónica de protección, diagnóstico y comunicaciones. Integra un módulo electrónico (unidad de disparo digital o relé electrónico) que monitoriza corriente, tensión y otros parámetros; registra eventos; permite la operación de sus funciones de manera remota y se conecta a sistemas de gestión como, SCADA, BMS y DCIM, mediante protocolos industriales.

MCB / Miniature Circuit Breaker con Módulo Inteligente. Se utilizan para circuitos de baja corriente (protección por rama) y suelen ofrecer telemetría básica y relés de disparo con salida digital.

MCCB Inteligente (Molded Case Circuit Breaker). Se utilizan para corrientes medianas/altas en distribución de rack/room, presentan medición por rama, funciones de disparo ajustables, comunicación Modbus/SNMP mediante módulo.

ACB Inteligente (Air Circuit Breaker). Se utilizan para alimentadores y tableros principales (MSB), por lo general tienen disparador digital avanzado (relé electrónico), registro de fallas, comunicaciones IEC 61850/Modbus y altas capacidades de interrupción.

Breakers con Funciones de Protección Avanzada / Relés Digitales. Vienen integrados con relés de protección (ANSI/IEEE) para coordinación, protección de transformadores, e incluyen registro de eventos, oscilografías y análisis de fallo.

RCBO / RCDs Inteligentes. Presentan protección por sobre corriente + diferencial (fuga a tierra) con capacidad de telemetría es útil para detección de corrientes de fuga en racks/zonas críticas.

Breakers con Medición por Outlet / Per-Outlet Breakers. Breakers integrados en PDU's inteligentes o marcos de distribución que miden por salida y permiten control granular.

Breakers Inalámbricos / IoT-Enabled. Son dispositivos con conectividad inalámbrica para entornos donde el cableado es difícil; suelen usarse para monitorización menos crítica o provisoria.

Protocolos de Monitoreo

SNMP. (Alhilali et al., 2023) afirma que SNMP (Simple Network Management Protocol) es un protocolo estándar de Internet para monitoreo y gestión de dispositivos de red (switches, routers, servidores, PDU's, UPS, sensores, etc.). define un modelo cliente-servidor: los agents en los dispositivos exponen información operacional (objetos) y el manager que es la plataforma de monitoreo consulta o recibe notificaciones, por último la información se organiza con MIBs (Management Information Bases) y se identifica por OIDs (Object Identifiers) según el SMI (Structure of Management Information).

Nos permite recolectar métricas de la CPU, temperatura, uso de la interfaz, estado de tomas en PDU, nos suministra alertas en tiempo real como cuando se incie un fallo en un dispositivo o se aumente la temperatura, además de configuración remota e identificación automática de dispositivos y sus características encontrando los siguientes tipos:

SNMPv1 (Original). Es muy simple; autenticación basada en community strings (texto claro). Su seguridad es limitada no recomendable en redes productivas.

SNMPv2c. Presenta mejoras en eficiencia (GETBULK), pero sigue usando community (sin seguridad real) y es más eficiente para lecturas de tablas.

SNMPv3. Incorpora un modelo de seguridad robusto basado en USM (User-based Security Model) y VACM (View-based Access Control Model), permitiendo un control detallado de usuarios y vistas de acceso. Soporta distintos niveles de seguridad: *noAuthNoPriv*, sin autenticación ni cifrado; *authNoPriv*, con autenticación mediante HMAC (MD5 o SHA) sin cifrado; y *authPriv*, que añade autenticación y privacidad mediante cifrado como DES o AES. En conjunto, SNMPv3 garantiza integridad, autenticación, confidencialidad y protección contra ataques de repetición (replay), siendo la versión recomendada para entornos críticos.

SNMP Traps. Es una notificación asíncrona enviada por un agent SNMP (el dispositivo que se gestiona) hacia un manager (sistema de monitoreo). Mientras que el manager habitualmente “polls” (consulta) valores con operaciones GET, el trap permite que el agente informe inmediatamente al manager sobre eventos relevantes (por ejemplo: caída de interfaz, fallo de UPS, temperatura crítica).

Técnicamente un trap es un PDU SNMP que contiene: identificador de la entidad (enterprise OID), marca temporal/agent address, y una lista de varbinds (pares OID–valor) que

describen el evento que sirve para notificar eventos y alarmas en tiempo real, reduciendo la latencia y permitiendo la integración en flujos de operación encontrando los siguientes tipos:

SNMPv1 TRAP. formato original; incluye generic-trap y specific-trap. Ejemplos de generic: coldStart, warmStart, linkDown, linkUp, authenticationFailure.

SNMPv2 TRAP. usa la PDU TRAP con varbinds y soporta GETBULK en otras operaciones.

Inform (v2/v3). similar a TRAP pero con confirmación (ack) del manager → mayor fiabilidad.

Syslog. Según (Gerhards R, 2009) Syslog es un protocolo estándar para registro centralizado de mensajes de log generados por sistemas operativos, aplicaciones, dispositivos de red y servicios. Un dispositivo (syslog client) envía mensajes a un syslog server/collector entre ellos tenemos: rsyslog, syslog-ng, syslogd, SIEM. Por lo general los mensajes contienen información como prioridad, timestamp, hostname, nombre de programa/proceso y el texto del mensaje, en donde podemos centralizar los log de diferentes dispositivos como routers, switch, servidores y aplicaciones entre otros, para realizar auditoria forense y detectar incidentes y correlacionarlos. Para Syslog encontramos los siguientes tipos / estándares y formatos;

BSD Syslog (RFC 3164). formato “legacy” ampliamente usado (PRI|HEADER MSG).

IETF Syslog (RFC 5424). formato estructurado (mejor manejo de campos, timestamp, structured-data).

Transporte por UDP/TCP. tradicionalmente UDP/514 (sin conexión), TCP/514 (más fiable).

Syslog sobre TLS (RFC 5425). syslog con cifrado/TLS para seguridad.

Modbus. (Enas Dhuhri Kusuma, 2024) describe a Modbus como un protocolo de comunicación industrial utilizado para el intercambio de datos entre dispositivos industriales y controladores lógicos programables (PLC). Permite la transmisión de información de proceso mediante un modelo cliente-servidor, facilitando la interoperabilidad entre sistemas distintos y la integración de datos en entornos de supervisión y automatización industrial, incluyendo sistemas de monitoreo y control de instalaciones y edificios, presentando los siguientes tipos:

Modbus RTU. Modbus RTU es un protocolo de comunicación serial que opera sobre medios físicos como RS-485 o RS-232. Utiliza un formato de trama binaria compacta con verificación de errores mediante CRC16, lo que lo hace eficiente y confiable en entornos industriales. Su topología típica es en bus multidrop (especialmente sobre RS-485), donde un dispositivo maestro se comunica con múltiples dispositivos esclavos direccionados generalmente en el rango de 1 a 247. Debido a su bajo consumo de ancho de banda y simplicidad, es ampliamente utilizado en aplicaciones de planta eléctrica, automatización industrial y sistemas HVAC.

Modbus ASCII. Modbus ASCII es una variante del protocolo Modbus que opera sobre medio serial y utiliza tramas codificadas en formato ASCII, lo que facilita su lectura y depuración. Emplea verificación de errores mediante LRC (Longitudinal Redundancy Check). Aunque resulta más legible que Modbus RTU, es menos eficiente debido al mayor tamaño de sus tramas, por lo que actualmente su uso es menos frecuente en aplicaciones industriales modernas.

Modbus TCP/IP (Modbus TCP). Modbus TCP es una versión del protocolo que opera sobre redes Ethernet utilizando TCP/IP, generalmente a través del puerto 502. En este esquema, la unidad de datos Modbus (PDU) se encapsula dentro de un encabezado MBAP (Modbus Application Protocol), que incluye campos como Transaction ID, Protocol ID, Length y Unit ID.

Su principal ventaja es la mayor velocidad de comunicación y la facilidad de integración con redes IP y sistemas SCADA modernos, lo que lo convierte en una opción ampliamente adoptada en entornos industriales actuales.

Modbus Sobre TCP con Túneles / Modbus RTU over TCP. Es un puente entre RTU y TCP para integrar dispositivos seriales a redes Ethernet vía gateways/serial servers.

Modbus Plus (propietario). Es una red token-passing propietaria de Modicon/Schneider (menos usada hoy).

Modbus UDP (poco frecuente). Modbus UDP es una variante del protocolo que opera sobre UDP en redes IP, a diferencia de Modbus TCP no establece conexión previa entre los dispositivos. Debido a su naturaleza sin conexión, puede ofrecer menor latencia, pero también menor fiabilidad en comparación con TCP, ya que no garantiza la entrega de los paquetes. Su uso es poco frecuente y se limita a entornos específicos donde se prioriza velocidad sobre confiabilidad.

BACnet. (W. H. Choi & Lewe, 2024) indica que (Building Automation and Control networks) es un protocolo de comunicación abierto diseñado para que los distintos sistemas de automatización de edificios puedan interoperar entre sí, incluso si son de diferentes fabricantes, fue desarrollado por ASHRAE y está estandarizado como ISO 16484-5. Es utilizado ampliamente en edificios inteligentes para integrar la iluminación, aires acondicionado y calefacción, Control de acceso, monitoreo energético y sistemas de seguridad, podemos encontrar los siguientes tipos:

BACnet/IP. BACnet/IP es un protocolo de comunicación diseñado para la automatización y gestión de edificios, que opera sobre redes Ethernet y TCP/IP. Actualmente es uno de los estándares más utilizados en sistemas de control de edificios (BMS), debido a su alta velocidad de comunicación y amplia compatibilidad con infraestructuras IT modernas. Resulta

especialmente adecuado para edificaciones inteligentes y para la integración de sistemas remotos de climatización, iluminación, seguridad y gestión energética.

BACnet MS/TP (Master-Slave / Token Passing). BACnet MS/TP es una variante del protocolo BACnet que opera sobre comunicación serial RS-485 bajo un esquema de paso de token (Token Passing) entre dispositivos maestro-esclavo. Se caracteriza por ser una solución económica y robusta, ampliamente utilizada en controladores de campo dentro de sistemas de automatización de edificios. Su velocidad típica de operación oscila entre 9.6 kbps y 115.2 kbps, lo que lo hace adecuado para aplicaciones distribuidas donde se prioriza estabilidad y bajo costo sobre altas tasas de transmisión.

BACnet Ethernet. BACnet Ethernet es una implementación del protocolo BACnet que opera directamente sobre redes Ethernet sin utilizar la capa IP. Aunque fue una de las primeras adaptaciones del estándar a redes de mayor velocidad, actualmente su uso es poco frecuente debido a las limitaciones de interoperabilidad con infraestructuras IP modernas. En la práctica, ha sido reemplazado ampliamente por BACnet/IP, que ofrece mayor flexibilidad, escalabilidad e integración con redes empresariales actuales.

BACnet PTP (Point-To-Point). BACnet PTP es una modalidad del protocolo diseñada para comunicaciones punto a punto, utilizada principalmente sobre enlaces seriales y conexiones mediante módem. Fue empleada en escenarios donde se requería comunicación directa entre dos dispositivos sin infraestructura de red compleja. En la actualidad se encuentra prácticamente en desuso, debido a la adopción de tecnologías basadas en Ethernet e IP que ofrecen mayor velocidad, escalabilidad e integración con redes modernas.

BACnet LonTalk. BACnet LonTalk es una implementación del protocolo BACnet que opera sobre la red LonWorks, permitiendo la integración de dispositivos dentro de esa

arquitectura específica. Fue utilizado en determinados sistemas de automatización, especialmente en entornos donde LonWorks era la infraestructura predominante. Actualmente su uso es limitado y se encuentra principalmente en instalaciones antiguas, habiendo sido reemplazado en la mayoría de los casos por BACnet/IP en redes modernas.

Protocolos Serie. (Chen, 2024) La comunicación serie es un método para enviar datos bit a bit a través de un solo canal de transmisión, siendo uno de los métodos más antiguos y aún más utilizados en automatización industrial, electrónica y sistemas embebidos. En vez de usar muchos cables (como la comunicación paralela), usa solo dos o tres líneas para enviar y recibir información usándose principalmente para comunicación entre dispositivos de control, automatización industrial, configuración de equipos, electrónica y microcontroladores e integración con Modbus RTU, encontrando los siguientes tipos:

RS-232. RS-232 es un estándar de comunicación serial diseñado para enlaces punto a punto entre dos dispositivos. Permite distancias de transmisión de hasta aproximadamente 15 metros y velocidades que pueden alcanzar los 115 kbps, dependiendo de la configuración y el entorno. Opera mediante niveles de señalización de voltaje típicamente de ± 12 V, diferenciándose de interfaces TTL, lo que lo hace adecuado para aplicaciones industriales y equipos legacy.

RS-485. RS-485 es un estándar de comunicación serial diseñado para topologías multidrop, permitiendo la conexión de hasta 32 dispositivos en un mismo bus. Ofrece alcances de transmisión de hasta aproximadamente 1200 metros, dependiendo de la velocidad y las condiciones del cableado. Utiliza señalización diferencial, lo que le proporciona alta inmunidad al ruido eléctrico y lo hace especialmente adecuado para entornos industriales y aplicaciones de automatización.

RS-422. RS-422 es un estándar de comunicación serial similar a RS-485, pero diseñado principalmente para enlaces punto a punto. Ofrece alta estabilidad en transmisiones a largas distancias y, al igual que RS-485, utiliza señalización diferencial, lo que le proporciona buena inmunidad al ruido eléctrico. Es común en aplicaciones industriales donde se requiere mayor alcance que RS-232, pero sin necesidad de una topología multidrop.

UART (Universal Asynchronous Receiver/Transmitter). UART es una interfaz de comunicación serial asíncrona utilizada principalmente a nivel de microcontroladores y sistemas embebidos. Opera mediante dos líneas principales, transmisión (TX) y recepción (RX), permitiendo el intercambio de datos sin necesidad de señal de reloj compartida. Es ampliamente empleada como base para estándares físicos como RS-232, RS-422 y RS-485, así como para comunicación directa entre dispositivos electrónicos.

SPI (Serial Peripheral Interface) Voltajes Típicos: 3.3V o 5V (TTL). SPI es una interfaz de comunicación serial síncrona utilizada principalmente en sistemas embebidos y microcontroladores. Opera típicamente con niveles de voltaje de 3.3 V o 5 V (TTL) y se caracteriza por su alta velocidad de transmisión. Requiere múltiples líneas de señal, incluyendo reloj (CLK), datos de salida del maestro (MOSI), datos de entrada al maestro (MISO) y selección de dispositivo (CS), lo que permite comunicación eficiente entre un dispositivo maestro y uno o varios dispositivos esclavos.

I2C (Inter-Integrated Circuit) Es una interfaz de comunicación serial síncrona ampliamente utilizada en sistemas embebidos y dispositivos electrónicos integrados. Opera mediante solo dos líneas principales: datos (SDA) y reloj (SCL), lo que simplifica el cableado y la integración de múltiples dispositivos en un mismo bus. Permite direccionar hasta 128

dispositivos mediante esquemas de direccionamiento estándar, siendo ideal para la comunicación entre microcontroladores, sensores y periféricos de baja y media velocidad.

Fieldbuses. En el artículo de (Babel, 2022) se entiende que es un sistema de comunicación digital diseñado para conectar sensores, actuadores, PLCs y controladores en la automatización industrial, siendo la evolución moderna de las señales analógicas 4–20 mA, permitiendo que múltiples dispositivos compartan una misma red utilizado para transmitir datos de sensores, recibir órdenes de control, reportar fallas, diagnosticar dispositivos presentando los siguientes tipos:

Fieldbus Basado en RS-485 Los sistemas Fieldbus basados en RS-485 emplean comunicación diferencial, lo que les proporciona alta tolerancia al ruido eléctrico en entornos industriales. Permiten distancias de transmisión de hasta aproximadamente 1200 metros y pueden alcanzar velocidades de hasta 10 Mbps, dependiendo del protocolo específico y la configuración. Utilizan típicamente una topología de bus lineal y soportan la conexión de entre 32 y 256 dispositivos en el mismo segmento, según el diseño del sistema y el tipo de transceptores utilizados.

Fieldbus 1-Wire. Es un sistema de comunicación que utiliza una única línea de datos junto con tierra (GND), lo que simplifica significativamente el cableado. Se caracteriza por operar a baja velocidad y permitir distancias típicas de hasta aproximadamente 100 metros, dependiendo de la topología y las condiciones de instalación. Soporta múltiples dispositivos en el mismo bus mediante direccionamiento único, siendo una solución económica y de fácil implementación, comúnmente utilizada en sensores y aplicaciones de monitoreo básico.

MQTT. (Kaganurmeth et al., 2025) describe a MQTT (Message Queuing Telemetry Transport) como un protocolo de mensajería ligero, diseñado para enviar datos entre dispositivos usando muy poco ancho de banda.

Es uno de los protocolos más usados en IoT (Internet de las Cosas), domótica, Comunicaciones entre microcontroladores y movilidad y transporte, presentando los siguientes tipos:

MQTT Estándar (v3.1.1). MQTT versión 3.1.1 es el estándar más ampliamente utilizado dentro de los protocolos de mensajería ligera para IoT y sistemas de monitoreo. Se basa en un modelo de publicación/suscripción (publish/subscribe) mediante un broker central, lo que facilita la comunicación eficiente entre múltiples dispositivos. Es altamente compatible con diversas plataformas, lenguajes de programación y sistemas embebidos, convirtiéndose en una solución versátil para aplicaciones de telemetría, automatización y monitoreo remoto.

MQTT 5.0. MQTT 5.0 es una versión avanzada del protocolo que incorpora mejoras significativas respecto a la versión 3.1.1, especialmente en gestión de errores y control de comunicación. Introduce códigos de razón (reason codes) que permiten una identificación más precisa de fallos, así como propiedades adicionales en los mensajes para mayor flexibilidad y personalización. Además, mejora el control del flujo y la administración de sesiones, optimizando el rendimiento en entornos complejos. Es ampliamente utilizado en sistemas IoT avanzados que requieren mayor robustez, trazabilidad y escalabilidad en la comunicación.

MQTT-SN (MQTT para Sensores). MQTT-SN (MQTT for Sensor Networks) es una adaptación del protocolo MQTT diseñada para operar en redes que no utilizan TCP/IP, optimizando el consumo de recursos en dispositivos de baja potencia. Está orientado a entornos con limitaciones de ancho de banda y energía, siendo especialmente adecuado para tecnologías

como ZigBee, LoRa y Bluetooth Mesh. Su diseño ligero permite integrar sensores y nodos IoT en arquitecturas distribuidas sin requerir una pila IP completa.

WebSockets + MQTT. La integración de WebSockets con MQTT permite utilizar el protocolo directamente desde navegadores web, facilitando la comunicación en tiempo real sin necesidad de clientes TCP tradicionales. Esta combinación es ampliamente utilizada en el desarrollo de dashboards y plataformas IoT, ya que permite visualizar datos, recibir actualizaciones instantáneas y gestionar dispositivos desde interfaces web modernas.

AMQP (Petrescu et al., 2025) afirma que AMQP (Advanced Message Queuing Protocol) es un protocolo de mensajería a nivel de aplicación diseñado para comunicaciones confiables, seguras y organizadas entre aplicaciones en sistemas distribuidos. Proporciona mecanismos de encolado, enrutamiento y confirmación de mensajes, y se utiliza principalmente en arquitecturas empresariales y aplicaciones backend para la integración de servicios, procesamiento de eventos y comunicación entre sistemas distribuidos, presentando los siguientes tipos:

AMQP 0-9-1 (El Más Utilizado). AMQP 0-9-1 es una de las versiones más utilizadas del protocolo Advanced Message Queuing Protocol, ampliamente implementada en plataformas como RabbitMQ. Está orientado a arquitecturas basadas en colas de mensajes, utilizando conceptos como *exchanges*, *queues* y *bindings* para enrutar información de manera flexible y controlada. Se caracteriza por su alta configurabilidad y facilidad de implementación en sistemas distribuidos. Además, existe AMQP 1.0, versión estandarizada por ISO, que amplía la interoperabilidad y formaliza el protocolo a nivel internacional.

REST. Representational State Transfer no es un protocolo, sino un estilo de arquitectura para diseñar servicios web, sin embargo, comúnmente se le llama “protocolo REST” por su uso estandarizado en APIs. REST se basa en principios que permiten crear servicios ligeros,

escalables, simples y compatibles con HTTP y se usa para crea APIs web, aplicaciones móviles, servicios en la nube, integración de sistemas, micorservicios e IoT, presentando los siguientes tipos:

RESTful (REST puro). RESTful, o REST puro, es un estilo arquitectónico para el diseño de APIs que cumple con los seis principios definidos por REST, incluyendo cliente-servidor, ausencia de estado (stateless), cacheabilidad, interfaz uniforme, sistema en capas y código bajo demanda (opcional). Se basa en el uso de métodos HTTP estándar como GET, POST, PUT y DELETE para la manipulación de recursos identificados mediante URI. Ejemplos representativos de APIs que siguen este enfoque son las API de GitHub y Spotify, ampliamente utilizadas en entornos web y aplicaciones modernas.

REST-like (No Cumple Todos los Principios). REST-like se refiere a implementaciones que utilizan HTTP como base de comunicación, pero que no cumplen estrictamente con todos los principios definidos por la arquitectura REST. Es un enfoque muy común en entornos empresariales, donde se prioriza la funcionalidad práctica sobre la adherencia completa al modelo teórico. En muchos casos, estas APIs no son completamente stateless o emplean el método POST para múltiples tipos de operaciones, sin diferenciar adecuadamente entre acciones como consulta, creación o actualización de recursos.

HATEOAS (REST Avanzado). HATEOAS (Hypermedia As The Engine Of Application State) es una extensión del modelo REST que incorpora enlaces hipermedia dentro de las respuestas del servidor, permitiendo guiar dinámicamente al cliente en las acciones disponibles sobre los recursos. Este enfoque mejora la auto documentación y la navegabilidad de la API, ya que el cliente puede descubrir las operaciones posibles mediante los enlaces proporcionados, sin necesidad de conocimiento previo estático de la estructura del servicio.

REST con JSON:API o HAL. REST puede complementarse con formatos estandarizados como JSON:API o HAL, los cuales definen estructuras específicas para la representación de recursos y relaciones en formato JSON. Estos estándares buscan mejorar la consistencia, interoperabilidad y claridad en el diseño de APIs, facilitando la integración entre sistemas y reduciendo ambigüedades en la implementación de servicios web.

RESTful APIs con Autenticación Avanzada. Las RESTful APIs pueden incorporar mecanismos de autenticación y seguridad adicionales para reforzar el control de acceso y la protección de datos. Aunque no constituyen un tipo formal de arquitectura, representan una variante común en entornos empresariales y sistemas críticos. Entre los esquemas más utilizados se encuentran la integración con OAuth 2.0 para autorización delegada, el uso de JSON Web Tokens (JWT) para autenticación basada en tokens, la implementación de API Keys para control básico de acceso y la autenticación mediante MutuaL TLS (mTLS), que valida tanto al cliente como al servidor. Estas estrategias permiten fortalecer la seguridad en APIs expuestas a redes públicas o infraestructuras distribuidas.

WebSocket. Según (Melnikov A., 2011) WebSocket es un protocolo de comunicación bidireccional y en tiempo real, que permite mantener una conexión abierta entre un cliente como navegador, app, IoT y un servidor, a diferencia de HTTP que es petición – respuesta, WebSocket permite Comunicación full-duplex, conexión permanente sin necesidad de refrescar la página. muy baja latencia y envío continuo de datos, usado en videojuegos, chats, trading, precios y telemetría en tiempo real, IoT y dashboard en vivo para el monitoreo de servidores y seguridad, presentando los siguientes tipos:

WebSocket Estándar. WebSocket estándar es un protocolo de comunicación bidireccional que permite mantener una conexión persistente entre cliente y servidor sobre TCP.

En su forma básica (ws://), opera sin cifrado, lo que implica que los datos transmitidos pueden ser interceptados si no se implementan mecanismos adicionales de seguridad. Se utiliza comúnmente en aplicaciones que requieren comunicación en tiempo real, como sistemas de monitoreo, dashboards interactivos y notificaciones instantáneas.

WebSocket Seguro. WebSocket seguro (WSS) es la versión cifrada del protocolo WebSocket y opera sobre TLS/SSL, de manera similar a HTTPS respecto a HTTP. Utiliza el esquema wss://, lo que garantiza la confidencialidad e integridad de los datos transmitidos entre cliente y servidor. Es la opción recomendada para aplicaciones en producción, especialmente en sistemas de monitoreo, plataformas IoT y servicios web expuestos a redes públicas.

WebSocket + STOMP La combinación de WebSocket con STOMP permite utilizar un protocolo de mensajería estructurado sobre una conexión WebSocket persistente. STOMP (Simple Text Oriented Messaging Protocol) define un formato estándar de intercambio de mensajes basado en comandos y cabeceras, facilitando la integración con brokers de mensajería como ActiveMQ o RabbitMQ. Esta arquitectura es común en aplicaciones web que requieren comunicación en tiempo real con soporte de colas, suscripciones y gestión estructurada de mensajes.

WebSocket + Socket.io. La integración de WebSocket con Socket.IO proporciona una capa adicional de abstracción que facilita la comunicación en tiempo real entre cliente y servidor. Socket.IO incorpora funcionalidades como reconexión automática, gestión de salas (rooms) para segmentación de usuarios y manejo de eventos personalizados, lo que simplifica el desarrollo de aplicaciones interactivas. Además, ofrece compatibilidad con navegadores antiguos mediante mecanismos de transporte alternativos cuando WebSocket no está disponible.

WebSocket Binario vs. Texto. WebSocket admite dos formatos principales de transmisión de datos: texto y binario. El modo texto utiliza codificación UTF-8 y es comúnmente empleado para intercambiar mensajes estructurados como JSON en aplicaciones de chat o eventos en tiempo real. El modo binario, en cambio, permite transmitir datos en formato más compacto y eficiente, siendo adecuado para imágenes, audio o flujos de telemetría de alta velocidad donde se requiere menor sobrecarga y mayor rendimiento.

SMTP. (Howser, 2020) menciona que SMTP (Simple Mail Transfer Protocol) es el protocolo estándar utilizado para enviar correos electrónicos a través de Internet, encargándose del transporte del correo, mas no de su recepción. Se usa principalmente para enviar correos desde aplicaciones o programas, comunicación entre correos, integración con sistemas empresariales y envío masivo de mensajes y marketing, presentando los siguientes tipos:

MSA (Mail Submission Agent). El MSA (Mail Submission Agent) es el componente encargado de recibir correos electrónicos enviados por usuarios autenticados para su posterior procesamiento y entrega. Opera comúnmente a través del puerto 587 y es utilizado por clientes de correo como Outlook o Thunderbird para enviar mensajes hacia el servidor de correo saliente, aplicando mecanismos de autenticación y políticas de seguridad antes de reenviarlos al sistema de transporte de correo (MTA).

MTA (Mail Transfer Agent). El MTA (Mail Transfer Agent) es el componente responsable de transferir correos electrónicos entre servidores mediante el protocolo SMTP, generalmente a través del puerto 25. Su función principal es enrutar y entregar los mensajes hacia el servidor de destino correspondiente. Entre las implementaciones más utilizadas se encuentran Postfix, Exim y Sendmail, ampliamente empleadas en infraestructuras de correo electrónico empresariales.

SMTP Relay. Un SMTP Relay es un servidor intermediario encargado de reenviar correos electrónicos hacia otros servidores de destino. Se utiliza comúnmente para centralizar el envío de mensajes, aplicar políticas de seguridad y gestionar grandes volúmenes de correo, como en campañas masivas o notificaciones automáticas. Permite además controlar autenticación, filtrado y reputación de envío antes de que los mensajes salgan hacia Internet.

SMS. (Ekwonwune & Enyinnaya, 2020) describe que SMS (Short Message Service) es un protocolo estándar utilizado para enviar mensajes de texto cortos (máximo 160 caracteres) a través de redes móviles, no depende de Internet; funciona sobre la red celular 2G, 3G, 4G e incluso 5G, basándose en la infraestructura tradicional de telefonía móvil, se utiliza de forma general para comunicación, verificación de identidad, alertas y notificaciones, presentando los siguientes tipos:

SMS MT (Mobile Terminated). SMS MT (Mobile Terminated) se refiere a los mensajes de texto que son recibidos por el teléfono móvil del usuario, el mensaje es enviado desde una plataforma o servidor hacia el dispositivo final, siendo común en notificaciones automáticas, alertas, códigos de verificación y comunicaciones empresariales dirigidas al cliente.

SMS MO (Mobile Originated). SMS MO (Mobile Originated) se refiere a los mensajes de texto que son enviados desde el teléfono móvil del usuario hacia una plataforma o servidor. Este esquema es utilizado en servicios interactivos, suscripciones, votaciones, confirmaciones o respuestas a notificaciones, permitiendo la comunicación iniciada por el usuario hacia el sistema central.

SMS P2P (Person-to-Person). SMS P2P (Person-to-Person) corresponde a la mensajería tradicional intercambiada directamente entre usuarios a través de sus dispositivos móviles. Este

tipo de comunicación está regulado por operadores y normativas para prevenir el envío masivo no autorizado y reducir prácticas de spam, diferenciándose de los esquemas empresariales o automatizados como A2P (Application-to-Person).

SMS A2P (Application-to-Person). SMS A2P (Application-to-Person) se refiere a los mensajes generados automáticamente por sistemas, aplicaciones o servidores y enviados hacia dispositivos móviles de usuarios finales. Este esquema es ampliamente utilizado para notificaciones, alertas, autenticación de doble factor (OTP), recordatorios y comunicaciones empresariales. A diferencia del modelo P2P, el tráfico A2P suele estar sujeto a regulaciones específicas y acuerdos con operadores para controlar volumen, trazabilidad y prevención de spam.

Flash SMS. El Flash SMS es un tipo de mensaje de texto que se muestra directamente en la pantalla del dispositivo al momento de su recepción, sin almacenarse automáticamente en la bandeja de entrada. Se utiliza comúnmente para notificaciones urgentes, alertas críticas o mensajes temporales que requieren atención inmediata del usuario.

Binary SMS. El Binary SMS es un tipo de mensaje que transmite datos en formato binario en lugar de texto legible para el usuario. Se utiliza para el envío de configuraciones, tonos, logos, parámetros técnicos o información estructurada entre dispositivos y sistemas. A diferencia del SMS tradicional, su contenido no está destinado a visualización directa, sino al procesamiento interno por parte del equipo receptor.

Premium SMS. El Premium SMS es un tipo de mensaje de texto asociado a servicios de pago, donde el costo del mensaje incluye una tarifa adicional que es facturada al usuario. Se utiliza para suscripciones, votaciones, donaciones, descargas de contenido o servicios de valor

agregado. Este modelo está regulado por operadores y autoridades para garantizar transparencia en la facturación y protección del consumidor.

Long SMS (Concatenado). El Long SMS, también conocido como SMS concatenado, permite el envío de mensajes que superan el límite estándar de 160 caracteres. Para ello, el contenido se divide en múltiples segmentos que son transmitidos por separado y posteriormente reensamblados en el dispositivo receptor, mostrándose como un único mensaje continuo para el usuario.

Push (APIs). (Wu, 2022) da a entender que el Protocolo Push, no es un único protocolo formal, sino un modelo de comunicación en el que un servidor envía información al cliente de manera automática, sin que el cliente tenga que solicitarla continuamente, haciendo lo opuesto al modelo pull, donde el cliente debe consultar periódicamente. Se utiliza para aplicaciones móviles, E-commerce y marketing, Juegos en tiempo real, Seguridad y autenticación, Monitoreo, sistemas empresariales y aplicaciones web, presentando los siguientes tipos:

Push Móvil Tradicional (App Push). El push móvil tradicional, también conocido como App Push, permite el envío de notificaciones desde servidores hacia aplicaciones instaladas en dispositivos móviles. En el ecosistema iOS, este servicio se implementa mediante APNs (Apple Push Notification Service), mientras que en Android se utiliza FCM (Firebase Cloud Messaging). Este tipo de notificación es ampliamente empleado para alertas, mensajes en tiempo real, recordatorios y actualizaciones dentro de aplicaciones móviles.

Web Push (Navegadores). Web Push es un mecanismo de notificaciones que permite enviar mensajes desde un servidor hacia navegadores web, incluso cuando el usuario no tiene abierta la página activa. Se basa en la Web Push API y en el uso de Service Workers para gestionar la recepción y visualización de las notificaciones en segundo plano. Su implementación

requiere el uso obligatorio de HTTPS, garantizando seguridad y cifrado en la comunicación entre el servidor y el navegador.

Push Corporativo o Empresarial (Push Interno). El push corporativo o empresarial se refiere a sistemas de notificación utilizados dentro de organizaciones para la gestión de alertas y comunicaciones internas. Se emplea comúnmente para alertas de sistemas, actualizaciones en dashboards internos y notificaciones dirigidas a aplicaciones corporativas. Su implementación suele integrarse con APIs REST, WebSockets o Server-Sent Events (SSE), permitiendo la transmisión en tiempo real de eventos críticos dentro de la infraestructura tecnológica de la empresa.

Push por Mensajería Instantánea (Push API Externa). El push por mensajería instantánea utiliza APIs externas de plataformas de comunicación para enviar notificaciones directamente a aplicaciones de mensajería utilizadas por los usuarios. Entre las implementaciones más comunes se encuentran WhatsApp Business API, Telegram Bot API y Messenger API. Este enfoque permite integrar sistemas empresariales con canales de comunicación ampliamente adoptados, facilitando el envío de alertas, notificaciones transaccionales y mensajes automatizados a través de plataformas de uso cotidiano.

Push en IoT (Machine-to-Machine). El push en entornos IoT (Machine-to-Machine) se utiliza para la transmisión automática de eventos y datos entre dispositivos sin intervención humana. Entre los mecanismos más comunes se encuentra MQTT, basado en el modelo publish/subscribe para la publicación de eventos; WebSockets, que permiten comunicación bidireccional en tiempo real; y CoAP Observations, que posibilita la notificación de cambios de estado en dispositivos de bajo consumo. Este tipo de push es fundamental en arquitecturas distribuidas de sensores, telemetría y sistemas industriales.

Push Para Autenticación (Push 2FA). El push para autenticación, comúnmente utilizado en esquemas de doble factor (2FA), permite enviar solicitudes de verificación directamente al dispositivo del usuario para aprobar o rechazar intentos de inicio de sesión. Su implementación suele basarse en servicios como APNs en iOS, FCM en Android o APIs propietarias integradas en aplicaciones de autenticación. Este mecanismo mejora la seguridad al añadir un factor adicional de validación en tiempo real, reduciendo riesgos asociados al uso exclusivo de contraseñas.

NTP. Según (Burbank & Kasch, 2010) NTP (Network Time Protocol) es un protocolo diseñado para sincronizar la hora y la fecha de los equipos en una red con una precisión muy alta, permitiendo que servidores, computadores, ruteadores, sistemas industriales y dispositivos IoT mantengan la misma hora exacta, incluso si están en diferentes lugares del mundo. Se usa para registros (logs) coherentes, validación de certificados, detección de incidentes, auditorías, y protocolos que dependen de tiempos exactos y presenta los siguientes tipos:

NTP (Tradicional o Completo). NTP (Network Time Protocol) es un protocolo de sincronización de tiempo completo, robusto y de alta precisión, utilizado para alinear los relojes de dispositivos en redes IP. Emplea algoritmos avanzados de compensación y filtrado para minimizar errores de latencia y desviación, siendo común en servidores, routers y sistemas críticos. Su precisión puede alcanzar el rango de milisegundos e incluso microsegundos, dependiendo de la infraestructura y la jerarquía de servidores utilizados.

SNTP (Simple Network Time Protocol). SNTP es una versión simplificada del protocolo NTP, diseñada para dispositivos que requieren sincronización de tiempo básica con menor consumo de recursos. Su implementación es más ligera y no incorpora todos los algoritmos

avanzados de compensación presentes en NTP. Es común en dispositivos pequeños, equipos IoT y sistemas embebidos, ofreciendo una precisión en el orden de milisegundos, aunque inferior a la alcanzada por NTP completo.

NTPv3 / NTPv4 (versiones). NTPv3 es una versión anterior del protocolo Network Time Protocol, ampliamente utilizada en sistemas antiguos y en implementaciones previas a la estandarización moderna. NTPv4 representa la versión actual y mejorada, incorporando mayor precisión, mejor manejo de redes de alta velocidad y compatibilidad con IPv6. Además, optimiza los algoritmos de sincronización y filtrado, permitiendo una gestión más eficiente en infraestructuras modernas y entornos distribuidos.

SSH. Según (Lonvick. C., 2006) SSH (Secure Shell) es un protocolo de comunicación seguro que permite acceder remotamente a servidores o dispositivos y ejecutar comandos de manera segura transfiriendo archivos cifrados y administrando sistemas a través de redes inseguras como Internet. SSH reemplaza a protocolos inseguros como **Telnet**, **rlogin** y **FTP**, ya que cifra toda la comunicación, presentando los siguientes tipos:

SSH-1. SSH-1 es la primera versión del protocolo Secure Shell, diseñada para proporcionar acceso remoto seguro mediante cifrado. Sin embargo, presenta vulnerabilidades conocidas en sus mecanismos criptográficos y de integridad, por lo que actualmente se considera insegura y no debe utilizarse en entornos productivos.

SSH-2. SSH-2 es la versión moderna y actualmente utilizada del protocolo Secure Shell. Incorpora mecanismos de cifrado más robustos, mejores métodos de autenticación y controles de integridad reforzados, garantizando comunicaciones seguras frente a ataques de interceptación o manipulación. Es el estándar implementado en prácticamente todos los sistemas operativos y dispositivos actuales para acceso remoto seguro y transferencia cifrada de datos.

SFTP (SSH File Transfer Protocol). SFTP es un protocolo de transferencia de archivos que opera sobre SSH, proporcionando cifrado completo tanto para la autenticación como para la transmisión de datos. A diferencia de FTP y FTPS, SFTP utiliza un único canal seguro basado en SSH, lo que simplifica la configuración y mejora la seguridad en entornos productivos. Es ampliamente utilizado para la transferencia segura de archivos en servidores y sistemas empresariales.

SCP. SCP es un protocolo utilizado para la copia simple de archivos entre sistemas a través de una conexión segura basada en SSH. Aunque proporciona cifrado durante la transferencia, su funcionalidad es limitada en comparación con SFTP, ya que no ofrece capacidades avanzadas de gestión de archivos. Actualmente ha quedado en gran medida desplazado por SFTP en entornos modernos debido a su mayor flexibilidad y seguridad mejorada.

SSH Tunneling / Port Forwarding. SSH Tunneling, también conocido como Port Forwarding, es una técnica que permite redirigir tráfico de red a través de un canal cifrado SSH. Puede implementarse como Local Forwarding, que permite acceder desde un equipo local a servicios remotos; Remote Forwarding, que habilita el acceso remoto a servicios ubicados en la máquina local; y Dynamic Forwarding (SOCKS5), que convierte la conexión SSH en un proxy seguro para enrutar múltiples conexiones. Esta técnica se utiliza ampliamente para acceso seguro, pruebas de servicios y protección de tráfico en redes no confiables.

HTTPS. (Fun & Samsudin, 2021) describe que (HyperText Transfer Protocol Secure) es la versión segura del protocolo HTTP.

Se usa para que la comunicación entre el usuario (navegador, app) y un servidor web sea cifrada, íntegra y autenticada. HTTPS funciona combinando el protocolo HTTP intercambio de información y TLS/SSL este protocolo que cifra y asegura esa información. HTTPS se utiliza para una navegación web segura, Apps móviles, APIs rest, microservicios e IoT, presenta los siguientes tipos:

HTTPS Estándar. HTTPS estándar es la versión segura del protocolo HTTP, que combina HTTP con TLS (Transport Layer Security) para cifrar la comunicación entre cliente y servidor. Es el mecanismo más utilizado actualmente para proteger la confidencialidad, integridad y autenticación de datos en aplicaciones web, APIs y servicios en línea, garantizando transmisión segura frente a interceptaciones o ataques de tipo Man-in-the-Middle.

HTTPS Mutuo (mTLS). HTTPS mutuo (mTLS) es una variante de HTTPS en la que tanto el cliente como el servidor deben presentar certificados digitales para autenticarse mutuamente durante el establecimiento de la conexión TLS. Este mecanismo añade una capa adicional de seguridad al garantizar autenticación bidireccional, siendo ampliamente utilizado en arquitecturas de microservicios, entornos empresariales de alta seguridad y sistemas críticos como los médicos o financieros.

HTTPS con HTTP/2. HTTPS con HTTP/2 combina el protocolo seguro HTTPS con la versión mejorada HTTP/2, optimizando el rendimiento de las comunicaciones web. Incorpora multiplexación de múltiples solicitudes sobre una sola conexión TCP, compresión de encabezados (headers) y mejor gestión de recursos, lo que reduce latencia y mejora la eficiencia en aplicaciones modernas y APIs de alto tráfico.

HTTPS con HTTP/3 (QUIC). HTTPS con HTTP/3 utiliza el protocolo QUIC en lugar de TCP como capa de transporte, funcionando sobre UDP para mejorar la velocidad y reducir la

latencia. Ofrece tiempos de establecimiento de conexión más rápidos, mejor rendimiento en redes móviles o inestables y menor impacto ante pérdida de paquetes. Esta versión representa la evolución más reciente del protocolo HTTP, optimizada para entornos modernos de alta demanda y movilidad.

Protocolos Analógicos Industriales. En el artículo (Trimetta Wintio et al., 2025) se describe que los protocolos analógicos industriales son métodos tradicionales para transmitir señales de medición o control entre sensores, instrumentos y PLCs, no son “protocolos” digitales como Modbus o CAN, sino formas de representar una variable física (temperatura, presión, nivel, etc.) mediante una señal eléctrica analógica, sus principales usos son automatización industrial, Instrumentación de plantas, sensores de temperatura, presión, caudal, nivel, actuadores y válvulas de control, Sistemas HVAC y BMS, Control de procesos en fábricas, laboratorios y sistemas de pesaje, para este protocolo existen los siguientes tipos:

Protocolo / Señal 4–20 mA (corriente). La señal 4–20 mA es un estándar de transmisión analógica ampliamente utilizado en instrumentación industrial para la medición y control de variables como presión, temperatura o nivel. Se caracteriza por su alta inmunidad al ruido eléctrico y su capacidad para recorrer largas distancias, típicamente entre 100 y 1000 metros, sin degradación significativa de la señal. Además, facilita el diagnóstico de fallas, ya que una lectura de 0 mA suele indicar interrupción o error en el circuito. Al basarse en corriente y no en voltaje, no depende de caídas de tensión en la línea, lo que la convierte en un estándar robusto y confiable a nivel mundial en entornos industriales.

Protocolo / Señal 0–10 V (voltaje). La señal 0–10 V es un estándar analógico basado en voltaje, utilizado para la transmisión de variables de control en sistemas de automatización. Se caracteriza por su facilidad de generación y medición, lo que simplifica su implementación en

dispositivos electrónicos y controladores. Es ampliamente compatible con actuadores HVAC, como dampers y variadores de velocidad, además de ser una solución económica y muy utilizada en automatización comercial y de edificios.

Matriz de Evaluación de Sistemas Operativos

En la Tabla 31 se presentan los criterios definidos para la evaluación de sistemas operativos, teniendo en cuenta los objetivos del proyecto, la arquitectura del sistema de monitoreo, los requerimientos del *data center* de la empresa y las buenas prácticas recomendadas por marcos de referencia como ITIL, ISO 27001, NIST y MAGERIT, con el fin de seleccionar la opción más adecuada para el monitoreo del *data center* de Transportes Gayco S.A.S.

Tabla 31

Criterios para la Evaluación de Sistemas Operativos

Código	Criterio
A	Funcionalidad para monitoreo
B	Criterios técnicos
C	Seguridad
D	Operación y mantenimiento
E	Costos
F	Alineación estratégica y riesgos

Nota. Los criterios definidos permiten evaluar las alternativas de sistemas operativos para el monitoreo del *data center*, considerando aspectos técnicos, operativos, de seguridad, costos y alineación con la estrategia de gestión de riesgos de la organización.

En la Tabla 32 se presenta la evaluación comparativa de los sistemas operativos seleccionados para el monitoreo del *datacenter*, considerando el criterio de funcionalidad para monitoreo y sus respectivos subcriterios, con el fin de identificar la plataforma que ofrece mayores capacidades técnicas y operativas para la gestión de la infraestructura.

Tabla 32

Evaluación de Sistemas Operativos Según el Criterio de Funcionalidad para Monitoreo

Subcriterio	Descripción	Ubuntu Server	Red Hat Enterprise Linux	Windows Server	VMware ESXi
Soporte nativo de SNMP	Incluye o facilita el uso de <i>snmpd</i> y servicios SNMP	5	5	3	4
Compatibilidad con herramientas de monitoreo	Zabbix, Nagios, Prometheus y agentes disponibles	5	5	4	3
Gestión de logs	Facilidad para enviar logs a SIEM o <i>syslog</i> centralizado	5	5	4	3
Soporte de protocolos clave	SSH, HTTPS, <i>syslog</i> y APIs	5	5	3	4

Nota. La valoración se realizó en una escala de 1 a 5, donde 1 representa un nivel bajo de cumplimiento del criterio y 5 representa un nivel alto.

De acuerdo con los resultados obtenidos, se evidencia que Ubuntu Server y Red Hat Enterprise Linux presentan el mejor desempeño en cuanto a funcionalidad para monitoreo, debido a su amplio soporte nativo de SNMP, compatibilidad con herramientas de monitoreo y capacidades avanzadas para la gestión de logs. Por su parte, Windows Server y VMware ESXi cumplen de manera adecuada con los requisitos evaluados, aunque presentan algunas limitaciones que los hacen óptimos como plataforma principal de monitoreo.

En la Tabla 33 se presenta la evaluación comparativa de los sistemas operativos considerando el criterio de criterios técnicos, teniendo en cuenta aspectos como estabilidad, requisitos de hardware, escalabilidad y soporte para virtualización y contenedores, con el fin de determinar su idoneidad para el entorno de monitoreo del *data center*.

Tabla 33*Evaluación de Sistemas Operativos Según el Criterio de Criterios Técnicos*

Subcriterio	Descripción	Ubuntu Server	Red Hat Enterprise Linux	Windows Server	VMware ESXi
Estabilidad del sistema operativo	Madurez, estabilidad y frecuencia de fallos	4	5	4	5
Requisitos de hardware	Consumo de RAM y CPU, eficiencia	5	4	3	4
Escalabilidad	Capacidad para crecer e integrar servicios	5	5	4	4
Soporte para virtualización y contenedores	KVM, Hyper-V, Docker y LXC	5	5	3	3

Nota. La valoración se realizó en una escala de 1 a 5, donde 1 representa un nivel bajo de cumplimiento del criterio y 5 representa un nivel alto.

De acuerdo con los resultados obtenidos, Red Hat Enterprise Linux y Ubuntu Server destacan por su estabilidad, eficiencia en el uso de recursos y amplio soporte para virtualización y contenedores, lo que los posiciona como opciones sólidas para entornos de monitoreo. Windows Server presenta un desempeño adecuado, aunque con mayores requisitos de hardware, mientras que VMware ESXi ofrece una alta estabilidad, pero con menor flexibilidad fuera del ámbito de la virtualización.

En la Tabla 34 se presenta la evaluación comparativa de los sistemas operativos considerando el criterio de seguridad, analizando los mecanismos de hardening, la gestión de parches, el historial de vulnerabilidades y la integración con controles de seguridad, con el fin de identificar la plataforma que ofrece mayores garantías para la protección del data center.

Tabla 34*Evaluación de Sistemas Operativos Según el Criterio de Seguridad*

Subcriterio	Descripción	Ubuntu Server	Red Hat Enterprise Linux	Windows Server	VMware ESXi
Mecanismos de <i>hardening</i>	SELinux, AppArmor, firewall y cifrado	4	5	4	4
Gestión de parches	Facilidad, frecuencia y calidad de actualizaciones	5	5	4	4
Historial de vulnerabilidades	Exposición a ataques y soporte de la comunidad	4	5	3	4
Integración con controles de seguridad	AD/LDAP, SIEM, antivirus y monitoreo	4	5	5	3

Nota. La valoración se realizó en una escala de 1 a 5, donde 1 representa un nivel bajo de cumplimiento del criterio y 5 representa un nivel alto.

De acuerdo con los resultados obtenidos, Red Hat Enterprise Linux y Ubuntu Server ofrecen el nivel de seguridad más sólido, gracias a sus mecanismos avanzados de *hardening*, gestión eficiente de parches y menor exposición a vulnerabilidades. Windows Server presenta un buen nivel de control e integración con soluciones corporativas, aunque con una mayor superficie de ataque. Por su parte, VMware ESXi ofrece un entorno seguro, pero con limitaciones en la integración de controles de seguridad avanzados.

En la Tabla 35 se presenta la evaluación comparativa de los sistemas operativos considerando el criterio de operación y mantenimiento, analizando la facilidad de administración, la disponibilidad de personal capacitado, las capacidades de automatización y la integración con los procesos actuales de tecnología de la información, con el fin de determinar la alternativa más adecuada para la gestión operativa del data center.

Tabla 35*Evaluación de Sistemas Operativos Según el Criterio de Operación y Mantenimiento*

Subcriterio	Descripción	Ubuntu Server	Red Hat Enterprise Linux	Windows Server	VMware ESXi
Facilidad de administración	Curva de aprendizaje y herramientas disponibles	4	4	5	3
Disponibilidad de personal capacitado	Facilidad para encontrar administradores	4	3	5	3
Automatización	Compatibilidad con Ansible, PowerShell y <i>scripts</i>	5	5	4	3
Integración con procesos actuales de TI	RespalDOS, inventario y mesa de ayuda	4	4	5	3

Nota. La valoración se realizó en una escala de 1 a 5, donde 1 representa un nivel bajo de cumplimiento del criterio y 5 representa un nivel alto.

De acuerdo con los resultados obtenidos, Windows Server ofrece una administración más sencilla y una mayor disponibilidad de personal capacitado, lo que facilita las labores operativas diarias. Por su parte, Ubuntu Server y Red Hat Enterprise Linux destacan por sus capacidades de automatización y buena integración operativa. VMware ESXi cumple con los criterios evaluados, aunque presenta menor flexibilidad para tareas generales de mantenimiento.

En la Tabla 36 se presenta la evaluación comparativa de los sistemas operativos considerando el criterio de **costos**, analizando el costo de licenciamiento, el costo total de propiedad (TCO) y la disponibilidad de comunidad y soporte externo, con el fin de identificar la alternativa más conveniente desde el punto de vista costo–beneficio para la organización.

Tabla 36*Evaluación de Sistemas Operativos Según el Criterio de Costos*

Subcriterio	Descripción	Ubuntu Server	Red Hat Enterprise Linux	Windows Server	VMware ESXi
Costo de licenciamiento	Pago único, anual, por CPU o gratuito	5	2	2	3
Costo total de propiedad (TCO)	Soporte, mantenimiento y capacitación	5	3	3	3
Comunidad y soporte externo	Disponibilidad de foros y documentación	5	4	4	3

Nota. La valoración se realizó en una escala de 1 a 5, donde 1 representa un nivel bajo de cumplimiento del criterio y 5 representa un nivel alto.

De acuerdo con los resultados obtenidos, Ubuntu Server presenta el menor costo y una amplia comunidad de soporte, lo que lo convierte en la opción más favorable en términos de costo–beneficio. Red Hat Enterprise Linux y Windows Server implican mayores costos asociados a licenciamiento y mantenimiento, aunque ofrecen soporte empresarial robusto. VMware ESXi presenta costos moderados, pero con menor disponibilidad de soporte externo, lo que reduce su competitividad frente a otras alternativas.

En la Tabla 37 se presenta la evaluación comparativa de los sistemas operativos considerando el criterio de alineación estratégica y riesgos, analizando su contribución a la disponibilidad, compatibilidad con estándares y nivel de riesgo operativo, con el fin de identificar la alternativa que mejor se alinea con la estrategia organizacional y la gestión de riesgos.

Tabla 37

Evaluación de Sistemas Operativos Según el Criterio de Alineación Estratégica y Riesgos

Subcriterio	Descripción	Ubuntu Server	Red Hat Enterprise Linux	Windows Server	VMware ESXi
Contribución a la disponibilidad (MTBF/MTTR)	Impacto en continuidad y recuperación	4	5	4	4
Compatibilidad con estándares	ISO 27001, auditorías y políticas de TI	4	5	5	4
Riesgo operativo	Probabilidad de fallos y falta de soporte	4	5	3	4
Puntuación total	—	100	99	84	78

Nota. La puntuación total corresponde a la suma ponderada de los criterios evaluados en la matriz de evaluación de sistemas operativos.

De acuerdo con los resultados obtenidos, Red Hat Enterprise Linux destaca por su alta alineación con estándares internacionales, menor riesgo operativo y fuerte contribución a la disponibilidad del servicio. Ubuntu Server mantiene un buen equilibrio general, presentando una alineación estratégica adecuada. Windows Server resulta competitivo, aunque con un mayor riesgo operativo, mientras que VMware ESXi ofrece estabilidad, pero con menor compatibilidad estratégica global frente a las demás alternativas evaluadas.

La puntuación total evidencia que Ubuntu Server (100 puntos) y Red Hat Enterprise Linux – RHEL (99 puntos) son las plataformas más adecuadas para soportar una estrategia de monitoreo integral proactivo, superando claramente a Windows Server (84 puntos) y VMware ESXi (78 puntos). Ambos sistemas Linux destacan por su sólido soporte de SNMP, amplia

disponibilidad de herramientas de monitoreo, estabilidad operativa, escalabilidad y altos niveles de seguridad mediante mecanismos de hardening y gestión eficiente de parches.

Aunque RHEL presenta una ligera ventaja en estabilidad certificada, alineación con estándares y menor riesgo operativo, Ubuntu Server se posiciona como la opción más conveniente al ofrecer un desempeño equivalente en funcionalidad, seguridad y automatización, pero con menor costo de licenciamiento y TCO, además de una fuerte comunidad de soporte.

Windows Server destaca por su facilidad administrativa, pero implica mayores costos y una mayor superficie de ataque, mientras que VMware ESXi resulta adecuado solo para virtualización, con menor flexibilidad como plataforma central de monitoreo.

De acuerdo con esto podemos observar que Ubuntu Server se justifica como la mejor elección al equilibrar rendimiento, seguridad, escalabilidad y costo, alineándose de forma óptima con las necesidades técnicas y estratégicas del proyecto.

Matriz de Evaluación de Aplicaciones y Herramientas

Para desarrollar los criterios de la matriz de evaluación de herramientas de monitoreo, se tuvieron en cuenta de forma directa los lineamientos técnicos, metodológicos y estratégicos definidos en el documento del Proyecto de Grado, asegurando coherencia entre el diagnóstico, los objetivos y la solución propuesta.

En la Tabla 38 se presentan los criterios definidos para la evaluación de aplicaciones y herramientas de monitoreo, establecidos con base en los lineamientos técnicos, metodológicos y estratégicos del Proyecto de Grado, con el fin de asegurar coherencia entre el diagnóstico, los objetivos y la solución propuesta.

Tabla 38*Criterios para la Evaluación de Aplicaciones y Herramientas de Monitoreo*

Código	Criterio
A	Funcionalidad para monitoreo
B	Criterios técnicos
C	Seguridad
D	Operación y mantenimiento
E	Costos
F	Alineación estratégica

Nota. Los criterios establecidos permiten evaluar de manera integral las aplicaciones y herramientas de monitoreo, considerando aspectos funcionales, técnicos, de seguridad, operativos, económicos y estratégicos.

En la Tabla 39 se presenta la evaluación comparativa de las aplicaciones y herramientas de monitoreo considerando el criterio de funcionalidad para monitoreo, analizando aspectos como el alcance del monitoreo, la compatibilidad con el sistema operativo, el soporte de protocolos, el autodiscover, la visualización, las alertas y la integración con hardware, con el fin de identificar la herramienta más adecuada para el monitoreo integral del data center.

Tabla 39
Evaluación de Aplicaciones y Herramientas de Monitoreo Según el Criterio de Funcionalidad para Monitoreo

Subcriterio	Descripción	Zabbix	Nagios Core	Prometheus + SNMP	PRTG Network Monitor	Icinga	LibreNMS	ABB Ability DCA
Alcance del monitoreo	Cobertura de servidores, red, energía, clima y seguridad	5	3	3	5	4	3	5

Subcriterio	Descripción	Zabbix	Nagios Core	Prometheus + SNMP	PRTG Network Monitor	Icinga	LibreNMS	ABB Ability DCA
Compatibilidad con Ubuntu Server	Agentes, paquetes <i>.deb</i> y estabilidad en Linux	5	4	5	2	4	5	2
Soporte de protocolos	SNMPv3, <i>syslog</i> , API, SSH, IPMI y Modbus	5	4	4	4	4	5	5
Autodescubrimiento	Detección automática de dispositivos	4	2	2	5	3	4	5
Dashboards y visualización	Paneles personalizables, mapas de red y racks	4	2	3	4	3	3	5
Alertas y notificaciones	Email, SMS, <i>webhooks</i> , Telegram y escalamiento	5	3	3	5	4	3	5
Integración con hardware	UPS, climatización, sensores, CCTV y <i>switches</i>	4	2	2	4	3	3	5

Nota. La valoración se realizó en una escala de 1 a 5, donde 1 representa un nivel bajo de cumplimiento del criterio y 5 representa un nivel alto.

De acuerdo con los resultados obtenidos, Zabbix y ABB Ability DCA ofrecen el alcance más completo para el monitoreo integral, destacándose por su amplia cobertura, capacidades de integración y mecanismos avanzados de alertamiento. PRTG Network Monitor presenta un buen equilibrio entre facilidad de uso y funcionalidad. Por su parte, Nagios Core, Prometheus y LibreNMS resultan adecuados para escenarios específicos, aunque con limitaciones en cobertura y automatización frente a las demás herramientas evaluadas.

En la Tabla 40 se presenta la evaluación comparativa de las aplicaciones y herramientas de monitoreo considerando el criterio de criterios técnicos, analizando aspectos como el rendimiento y consumo de recursos, la escalabilidad, la arquitectura distribuida y la integración con entornos de virtualización, con el fin de identificar la herramienta más adecuada para el monitoreo del data center.

Tabla 40

Evaluación de Aplicaciones y Herramientas de Monitoreo Según el Criterio de Criterios

Técnicos

Subcriterio	Descripción	Zabbix	Nagios Core	Prometheus + SNMP	PRTG Network Monitor	Icinga	LibreNMS	ABB Ability DCA
Rendimiento y consumo	Eficiencia del agente y del <i>backend</i>	4	3	5	3	4	4	4
Escalabilidad	Capacidad de crecimiento horizontal y vertical	5	4	5	3	4	4	5
Arquitectura distribuida	Soporte para <i>proxies</i> , nodos remotos y alta disponibilidad	5	3	5	2	4	3	5
Integración con virtualización	VMware, Proxmox y KVM	4	3	3	4	3	3	5

Nota. La valoración se realizó en una escala de 1 a 5, donde 1 representa un nivel bajo de cumplimiento del criterio y 5 representa un nivel alto.

De acuerdo con los resultados obtenidos, Zabbix y ABB Ability DCA destacan por su alta escalabilidad y arquitectura distribuida, lo que los hace adecuados para entornos de monitoreo complejos. Prometheus ofrece un excelente rendimiento técnico, mientras que PRTG

Network Monitor e Icinga presentan un desempeño equilibrado. Por su parte, Nagios Core y LibreNMS resultan más limitados en términos de integración y crecimiento estructural.

En la Tabla 41 se presenta la evaluación comparativa de las aplicaciones y herramientas de monitoreo considerando el criterio de seguridad, analizando aspectos como la gestión de roles y accesos, los mecanismos de cifrado, el historial de vulnerabilidades y la integración con controles de seguridad, con el fin de identificar la herramienta que ofrece mayores garantías para la protección del entorno de monitoreo.

Tabla 41

Evaluación de Aplicaciones y Herramientas de Monitoreo Según el Criterio de Seguridad

Subcriterio	Descripción	Zabbix	Nagios Core	Prometheus + SNMP	PRTG Network Monitor	Icinga	LibreNMS	ABB Ability DCA
Gestión de roles y accesos	Control de usuarios, perfiles y permisos	5	3	3	3	4	3	5
Cifrado y comunicaciones seguras	TLS, HTTPS, cifrado de credenciales	5	3	3	3	4	3	5
Historial de vulnerabilidades	Exposición a fallos y rapidez de corrección	5	3	3	3	4	3	5
Integración con controles de seguridad	SIEM, autenticación, auditoría y registros	5	3	3	3	4	3	5

Nota. La valoración se realizó en una escala de 1 a 5, donde 1 representa un nivel bajo de cumplimiento del criterio y 5 representa un nivel alto.

De acuerdo con los resultados obtenidos, Zabbix y ABB Ability DCA presentan el nivel de seguridad más sólido, gracias a su adecuada gestión de roles, mecanismos de cifrado

avanzados y menor exposición a vulnerabilidades. Icinga ofrece un buen nivel de seguridad general, mientras que Nagios Core, Prometheus y LibreNMS muestran capacidades aceptables, aunque con menor robustez integral. PRTG Network Monitor se mantiene estable, pero con limitaciones frente a los controles de seguridad más avanzados.

En la Tabla 42 se presenta la evaluación comparativa de las aplicaciones y herramientas de monitoreo considerando el criterio de operación y mantenimiento, analizando aspectos como la facilidad de instalación, facilidad de uso, disponibilidad de comunidad y soporte, así como la disponibilidad de talento en el mercado, con el fin de identificar la herramienta que ofrece mayores ventajas para su operación continua en la organización.

Tabla 42

Evaluación de Aplicaciones y Herramientas de Monitoreo Según el Criterio de Operación y Mantenimiento

Subcriterio	Descripción	Zabbix	Nagios Core	Prometheus + SNMP	PRTG Network Monitor	Icinga	LibreNMS	ABB Ability DCA
Facilidad de instalación	Repositorios, contenedores y documentación	5	3	4	2	4	5	2
Facilidad de uso	Curva de aprendizaje e interfaz amigable	4	2	3	4	3	3	4
Comunidad y soporte	Documentación, foros y soporte comercial	5	4	5	4	4	5	2
Disponibilidad de talento	Experiencia común en el mercado	5	3	4	3	4	4	2

Nota. La valoración se realizó en una escala de 1 a 5, donde 1 representa un nivel bajo de cumplimiento del criterio y 5 representa un nivel alto.

De acuerdo con los resultados obtenidos, Zabbix destaca por su facilidad de instalación, amplia comunidad de soporte y alta disponibilidad de talento en el mercado, lo que facilita su operación y mantenimiento. Icinga y LibreNMS presentan un buen desempeño general en términos operativos. Nagios Core y Prometheus requieren mayor experiencia técnica para su administración, mientras que PRTG Network Monitor y ABB Ability DCA presentan mayores limitaciones en instalación y soporte en entornos Linux.

En la Tabla 43 se presenta la evaluación comparativa de las aplicaciones y herramientas de monitoreo considerando el criterio de costos, analizando aspectos como el modelo de licenciamiento y el costo total de propiedad (TCO), con el fin de identificar las alternativas más viables para la organización en escenarios con restricciones presupuestales.

Tabla 43

Evaluación de Aplicaciones y Herramientas de Monitoreo Según el Criterio de Costos

Subcriterio	Descripción	Zabbix	Nagios Core	Prometheus + SNMP	PRTG Network Monitor	Icinga	LibreNMS	ABB Ability DCA
Licenciamiento	Gratis, suscripción o pago por dispositivo	5	5	5	2	5	5	1
Costo total de propiedad (TCO)	Mantenimiento, soporte y escalamiento	5	4	5	3	4	5	2

Nota. La valoración se realizó en una escala de 1 a 5, donde 1 representa un nivel bajo de cumplimiento del criterio y 5 representa un nivel alto.

De acuerdo con los resultados obtenidos, Zabbix, Nagios Core, Prometheus e Icinga presentan los mejores resultados en términos de costos, al tratarse de soluciones libres con bajo costo total de propiedad. LibreNMS también resulta una alternativa económica y competitiva.

Por el contrario, PRTG Network Monitor y especialmente ABB Ability DCA implican mayores gastos asociados a licenciamiento y soporte, lo que reduce su viabilidad en escenarios con restricciones presupuestales.

En la Tabla 44 se presenta la evaluación comparativa de las aplicaciones y herramientas de monitoreo considerando el criterio de alineación estratégica, analizando su contribución a la disponibilidad del servicio, el cumplimiento de estándares y el nivel de riesgo operativo, con el fin de identificar la herramienta que mejor se articula con los objetivos estratégicos de la organización.

Tabla 44

Evaluación de Aplicaciones y Herramientas de Monitoreo Según el Criterio de Alineación Estratégica

Subcriterio	Descripción	Zabbix	Nagios Core	Prometheus + SNMP	PRTG Network Monitor	Icinga	LibreNMS	ABB Ability DCA
Contribución a MTBF/MTTR	Reducción de fallas y tiempo de recuperación	5	3	4	5	4	3	5
Compatibilidad con estándares	ISO 27001 y auditorías de TI	5	3	4	5	4	3	5
Riesgo operativo	Estabilidad, dependencia y criticidad	5	3	4	4	4	3	5
Puntuación total	—	108	72	89	87	88	85	94

Nota. La puntuación total corresponde a la suma de los valores obtenidos en los criterios de funcionalidad, criterios técnicos, seguridad, operación y mantenimiento, costos y alineación estratégica.

De acuerdo con los resultados obtenidos, Zabbix y ABB Ability DCA presentan la mayor alineación con los objetivos estratégicos de la organización, destacándose por su aporte a la disponibilidad, cumplimiento de estándares y bajo riesgo operativo. Prometheus e Icinga mantienen un equilibrio adecuado entre desempeño técnico y alineación estratégica, mientras que PRTG Network Monitor ofrece un nivel aceptable. Por su parte, Nagios Core y LibreNMS evidencian una menor madurez estratégica frente a las demás alternativas evaluadas.

Las matrices de evaluación correspondientes a los criterios de funcionalidad, criterios técnicos, seguridad, operación y mantenimiento, costos y alineación estratégica, evidencian que Zabbix (108 puntos) y ABB Ability DCA (94 puntos) son las herramientas con mejor desempeño global para un esquema de monitoreo integral. Zabbix se posiciona como la opción más equilibrada y conveniente, al destacar en alcance de monitoreo, compatibilidad con Ubuntu Server, soporte de protocolos, automatización, escalabilidad, seguridad y alineación estratégica, además de ofrecer bajo costo de licenciamiento y TCO, lo que resulta clave para un entorno PyME. ABB Ability DCA presenta capacidades avanzadas en integración con hardware y alta disponibilidad, pero su mayor costo y dependencia de licencias limitan su viabilidad frente a Zabbix.

Herramientas como PRTG e Icinga muestran buen desempeño general, aunque con restricciones en costos o profundidad de integración, mientras que Nagios Core, Prometheus y LibreNMS resultan más limitadas en cobertura, automatización y madurez estratégica para un monitoreo integral centralizado.

Podemos observar claramente que Zabbix se justifica como la herramienta principal por su robustez técnica, flexibilidad, seguridad, escalabilidad y sostenibilidad económica, alineándose plenamente con los objetivos del proyecto para la empresa transportes Gayco S.A.S.

Adicionalmente, Grafana puede integrarse como capa adicional de visualización para potenciar el análisis avanzado de métricas, dashboards personalizados y correlación histórica de datos provenientes de Zabbix o Prometheus, mejorando la toma de decisiones y el enfoque predictivo del monitoreo sin reemplazar la plataforma principal.

Matriz de Evaluación de Sensores y Componentes Electrónicos

En la Tabla 45 se presentan los criterios definidos para la evaluación de sensores y componentes electrónicos, los cuales permiten seleccionar los dispositivos más adecuados para el monitoreo integral del data center de Transportes Gayco S.A.S. priorizando la continuidad del servicio, la detección temprana de fallos y la compatibilidad con la plataforma Zabbix sobre Ubuntu Server.

Tabla 45

Criterios para la Evaluación de Sensores y Componentes Electrónicos

Código	Criterio
A	Precisión
B	Confiabilidad
C	Escalabilidad
D	Compatibilidad (Ubuntu/Zabbix)
E	Costo
F	Mantenimiento
G	Disponibilidad
H	Nivel de actualización

Nota. Los criterios establecidos permiten evaluar de manera cuantitativa y cualitativa los sensores y componentes electrónicos, considerando su desempeño técnico, compatibilidad con la plataforma de monitoreo y viabilidad operativa en el *data center* de la organización.

En la Tabla 46 se presenta la evaluación comparativa de sensores de temperatura utilizados para el monitoreo ambiental del data center, considerando criterios de precisión,

confiabilidad, escalabilidad, compatibilidad con Ubuntu/Zabbix, costo, mantenimiento, disponibilidad y nivel de actualización, con el fin de identificar la alternativa más adecuada para el sistema de monitoreo propuesto.

Tabla 46

Evaluación de Sensores de Temperatura Según Criterios Técnicos y Operativos

Criterio	RTD (Resistance Temperature Detector)	Termistor	Termopar	Sensor semiconductor / IC	Sensor infrarrojo (IR)
Precisión	5	4	3	3	3
Confiabilidad	5	4	4	3	3
Escalabilidad	4	4	3	5	4
Compatibilidad (Ubuntu/Zabbix)	4	4	3	5	4
Costo	3	5	4	5	2
Mantenimiento	4	4	3	5	3
Disponibilidad	5	5	5	5	4
Nivel de actualización	5	4	3	5	4
Puntaje ponderado	35	34	28	36	27

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

De acuerdo con los resultados obtenidos, el sensor semiconductor/IC alcanza el mayor puntaje ponderado (36), destacándose por su alta escalabilidad, excelente compatibilidad con Ubuntu/Zabbix, bajo costo y mínimo mantenimiento, lo que lo convierte en la opción más equilibrada para un sistema de monitoreo moderno.

El RTD (35) y el termistor (34) presentan también un desempeño sólido, especialmente en términos de precisión y confiabilidad, siendo adecuados para entornos críticos donde la

exactitud es prioritaria. En contraste, el termopar y el sensor infrarrojo obtienen menores puntajes, lo que indica una menor idoneidad para el monitoreo ambiental continuo en el data center.

En la Tabla 47 se presenta la evaluación comparativa de sensores de humedad utilizados para el monitoreo ambiental del data center, considerando criterios de precisión, confiabilidad, escalabilidad, compatibilidad con Ubuntu/Zabbix, costo, mantenimiento, disponibilidad y nivel de actualización, con el fin de identificar la alternativa más adecuada para el sistema de monitoreo propuesto.

Tabla 47

Evaluación de Sensores de Humedad Según Criterios Técnicos y Operativos

Criterio	Sensor de humedad capacitivo	Sensor de humedad resistivo
Precisión	5	3
Confiabilidad	5	3
Escalabilidad	5	4
Compatibilidad (Ubuntu/Zabbix)	5	4
Costo	4	5
Mantenimiento	4	3
Disponibilidad	5	5
Nivel de actualización	5	3
Puntaje ponderado	38	30

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

De acuerdo con los resultados obtenidos, el sensor de humedad capacitivo se posiciona como la opción más adecuada al alcanzar el mayor puntaje ponderado (38), destacándose por su alto desempeño en precisión, confiabilidad, escalabilidad, compatibilidad con Ubuntu/Zabbix y

nivel de actualización, lo que lo convierte en la alternativa ideal para el monitoreo ambiental en el data center.

Por su parte, el sensor de humedad resistivo obtiene un puntaje menor (30), evidenciando limitaciones en precisión, confiabilidad y vigencia tecnológica. Aunque representa una opción económica, resulta menos recomendable para entornos críticos donde se requiere estabilidad y exactitud a largo plazo.

En las Tablas 48 y 49 se presenta la evaluación comparativa de sensores de detección de agua utilizados para el monitoreo de fugas en el data center, considerando criterios de precisión, confiabilidad, escalabilidad, compatibilidad con Ubuntu/Zabbix, costo, mantenimiento, disponibilidad y nivel de actualización, con el fin de identificar la alternativa más adecuada para el monitoreo preventivo de infraestructura crítica.

Tabla 48

Evaluación de Sensores de Detección de Agua según Criterios Técnicos y Operativos

Criterio	Sensor puntual de agua (spot)	Cable detector de fugas	Sensor por sonda/manguera	Sensor por flotador
Precisión	3	5	4	3
Confiabilidad	4	5	4	3
Escalabilidad	3	5	4	2
Compatibilidad (Ubuntu/Zabbix)	5	5	5	3
Costo	5	3	4	5
Mantenimiento	4	4	4	3
Disponibilidad	5	5	5	5
Nivel de actualización	4	5	4	2
Puntaje ponderado	33	37	34	26

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

Tabla 49*Evaluación de Sensores de Detección de Agua Según Criterios Técnicos y Operativos*

Criterio	Sensor capacitivo de agua	Sensor táctil de agua	Sensor óptico de agua	Sensor de humedad/condensación	Sensor inalámbrico / IoT para fugas
Precisión	4	3	4	4	3
Confiabilidad	4	3	4	4	3
Escalabilidad	4	3	4	5	5
Compatibilidad (Ubuntu/Zabbix)	4	4	4	5	5
Costo	4	5	3	4	3
Mantenimiento	4	3	3	4	4
Disponibilidad	5	4	4	5	4
Nivel de actualización	4	3	4	5	4
Puntaje ponderado	33	28	30	36	31

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

De acuerdo con los resultados obtenidos, el cable detector de fugas se posiciona como la alternativa más adecuada para el monitoreo de agua en el data center, al alcanzar el mayor puntaje ponderado (37), destacándose por su alta precisión, confiabilidad y cobertura continua en áreas amplias. Le siguen el sensor de humedad/condensación (36) y el sensor por sonda o manguera (34), los cuales complementan el monitoreo al permitir una detección temprana y localizada. En contraste, el sensor por flotador y el sensor táctil de agua presentan los puntajes más bajos, lo que refleja una menor idoneidad para un monitoreo integral y preventivo en infraestructura crítica.

En las Tablas 50 y 51 se presenta la evaluación comparativa de sensores de detección de humo e incendio utilizados para el monitoreo del data center, considerando criterios de precisión, confiabilidad, escalabilidad, compatibilidad con Ubuntu/Zabbix, costo, mantenimiento, disponibilidad y nivel de actualización, con el fin de identificar la alternativa más adecuada para la detección temprana y confiable de eventos de incendio en infraestructura crítica.

Tabla 50

Evaluación de Sensores de Detección de Humo e Incendio Según Criterios Técnicos y Operativos

Criterio	Detector fotoeléctrico	Detector por ionización	Detector multicriterio	Detector por haz (beam)
Precisión	4	3	5	4
Confiabilidad	5	3	5	4
Escalabilidad	4	3	4	5
Compatibilidad (Ubuntu/Zabbix)	4	3	4	4
Costo	4	4	3	3
Mantenimiento	4	3	4	3
Disponibilidad	5	4	4	4
Nivel de actualización	5	2	5	4
Puntaje ponderado	35	25	34	31

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

Tabla 51

Evaluación de Sensores de Detección de Humo e Incendio Según Criterios Técnicos y

Operativos

Criterio	Detector por aspiración (VESDA)	Detector lineal / cable	Aspiración con análisis avanzado
Precisión	5	4	5
Confiabilidad	5	4	5
Escalabilidad	5	5	5
Compatibilidad (Ubuntu/Zabbix)	5	4	5
Costo	2	3	1
Mantenimiento	4	4	4
Disponibilidad	4	4	3
Nivel de actualización	5	4	5
Puntaje ponderado	35	32	33

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

De acuerdo con los resultados obtenidos, los detectores fotoeléctricos y los sistemas de aspiración (VESDA) alcanzan el mayor puntaje ponderado (35), posicionándose como las alternativas más adecuadas para el monitoreo de humo e incendio en el data center, gracias a su alta precisión, confiabilidad y nivel de actualización tecnológica. El detector multicriterio y la aspiración con análisis avanzado presentan también un desempeño sobresaliente, al permitir una detección temprana y reducir la probabilidad de falsas alarmas. En contraste, el detector por ionización obtiene el puntaje más bajo, evidenciando una menor idoneidad y vigencia tecnológica para infraestructuras críticas modernas.

En las Tablas 52 y 53 se presenta la evaluación comparativa de sensores de apertura y estado utilizados para el monitoreo de accesos y condiciones operativas en el data center, considerando criterios técnicos y operativos que permiten identificar las alternativas más adecuadas para entornos críticos de alta disponibilidad.

Tabla 52

Evaluación de Sensores de Apertura y Estado Según Criterios Técnicos y Operativos

Criterio	Contacto magnético	Sensor Hall	Interruptor mecánico	Sensor de proximidad inductivo
Precisión	4	5	3	4
Confiabilidad	5	5	3	5
Escalabilidad	5	4	3	4
Compatibilidad (Ubuntu/Zabbix)	5	4	4	4
Costo	5	4	5	4
Mantenimiento	5	5	3	5
Disponibilidad	5	4	5	4
Nivel de actualización	4	5	2	5
Puntaje ponderado	38	36	28	35

Tabla 53

Evaluación de Sensores de Apertura y Estado Según Criterios Técnicos y Operativos

Criterio	Sensor de proximidad capacitivo	Sensor óptico	Sensor con función <i>tamper</i>
Precisión	4	4	5
Confiabilidad	4	3	5
Escalabilidad	4	4	5
Compatibilidad (Ubuntu/Zabbix)	4	4	5
Costo	4	3	4
Mantenimiento	4	3	5
Disponibilidad	4	4	4
Nivel de actualización	4	4	5

Criterio	Sensor de proximidad capacitivo	Sensor óptico	Sensor con función <i>tamper</i>
Puntaje ponderado	32	29	38

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

De acuerdo con los resultados obtenidos, el contacto magnético y el sensor con función *tamper* alcanzan el mayor puntaje ponderado (38), posicionándose como las opciones más adecuadas para el monitoreo de apertura y estado en el data center, gracias a su alta confiabilidad, facilidad de integración, bajo mantenimiento y buena escalabilidad.

El sensor Hall y el sensor de proximidad inductivo presentan también un desempeño sólido, ofreciendo mayor precisión y robustez operativa. En contraste, el interruptor mecánico y el sensor óptico obtienen los puntajes más bajos, reflejando una menor idoneidad para entornos críticos y de alta disponibilidad.

En las Tablas 54 y 55 se presenta la evaluación comparativa de unidades de distribución de energía (PDU) utilizadas en el data center, considerando criterios técnicos y operativos que permiten identificar las alternativas más adecuadas para un monitoreo energético avanzado, confiable y compatible con la plataforma Ubuntu/Zabbix.

Tabla 54

Evaluación de Unidades de Distribución de Energía Según Criterios Técnicos y Operativos

Criterio	PDU pasiva/básica	PDU con medición (<i>Metered</i>)	PDU con medición por salida
Precisión	1	4	5
Confiabilidad	5	5	5
Escalabilidad	3	4	5

Criterio	PDU pasiva/básica	PDU con medición (<i>Metered</i>)	PDU con medición por salida
Compatibilidad (Ubuntu/Zabbix)	2	4	5
Costo	5	4	3
Mantenimiento	5	4	4
Disponibilidad	5	5	4
Nivel de actualización	2	4	5
Puntaje ponderado	28	34	36

Tabla 55

Evaluación de Unidades de Distribución de Energía Según Criterios Técnicos y Operativos

Criterio	PDU con conmutación (<i>Switched</i>)	PDU con monitoreo por rama	PDU modular/escalable
Precisión	5	5	5
Confiabilidad	5	5	5
Escalabilidad	5	5	5
Compatibilidad (Ubuntu/Zabbix)	5	5	5
Costo	3	3	2
Mantenimiento	4	4	4
Disponibilidad	4	4	4
Nivel de actualización	5	5	5
Puntaje ponderado	36	36	35

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

De acuerdo con los resultados obtenidos, las PDU con medición por salida, las PDU con conmutación (switched) y las PDU con monitoreo por rama alcanzan el mayor puntaje ponderado (36), posicionándose como las alternativas más adecuadas para un data center

moderno, gracias a su alta precisión, confiabilidad, escalabilidad y excelente compatibilidad con Ubuntu/Zabbix.

La PDU modular/escalable presenta también un desempeño sobresaliente, ofreciendo flexibilidad para el crecimiento futuro. En contraste, la PDU pasiva/básica obtiene el puntaje más bajo, evidenciando limitaciones para un monitoreo integral y una gestión energética avanzada en infraestructuras críticas.

En la Tabla 56 se presenta la evaluación comparativa de tableros inteligentes utilizados para la distribución eléctrica en el data center, considerando criterios técnicos y operativos que permiten identificar las alternativas más adecuadas según su nivel de control, confiabilidad y compatibilidad con la plataforma Ubuntu/Zabbix.

Tabla 56

Evaluación de Tableros Inteligentes Según Criterios Técnicos y Operativos

Criterio	Tablero medido	Tablero monitoreado	Tablero controlable / conmutado	Tablero multicircuito	Tablero con lógica / PLC
Precisión	4	4	5	5	5
Confiabilidad	5	5	5	5	5
Escalabilidad	4	4	5	5	5
Compatibilidad (Ubuntu/Zabbix)	4	5	5	5	5
Costo	4	3	3	3	2
Mantenimiento	4	4	4	4	4
Disponibilidad	5	4	4	4	3
Nivel de actualización	4	5	5	5	5
Puntaje ponderado	34	34	36	36	34

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

De acuerdo con los resultados obtenidos, los tableros controlables/conmutados y los tableros multicircuito alcanzan el mayor puntaje ponderado (36), posicionándose como las opciones más adecuadas para el data center debido a su alta precisión, confiabilidad, escalabilidad y excelente compatibilidad con Ubuntu/Zabbix. Estos tableros ofrecen una mayor visibilidad y capacidad de control sobre la distribución eléctrica.

Por su parte, los tableros medidos, monitoreados y los tableros con lógica/PLC presentan puntajes ligeramente menores, reflejando un buen desempeño general, aunque con mayores implicaciones en costo o complejidad, manteniéndose como alternativas viables según el nivel de criticidad y presupuesto.

En las Tablas 57 y 58 se presenta la evaluación comparativa de breakers inteligentes utilizados para el monitoreo eléctrico en el datacenter, considerando criterios de precisión, confiabilidad, escalabilidad, compatibilidad con Ubuntu/Zabbix, costo, mantenimiento, disponibilidad y nivel de actualización, con el fin de identificar la alternativa más adecuada para la supervisión de circuitos críticos en infraestructura de alta disponibilidad.

Tabla 57

Evaluación de Breakers Inteligentes Según Criterios Técnicos y Operativos

Criterio	MCB inteligente	MCCB inteligente	ACB inteligente	Protección avanzada / relés
Precisión	4	5	5	5
Confiabilidad	5	5	5	5
Escalabilidad	4	5	5	5
Compatibilidad (Ubuntu/Zabbix)	4	5	5	5
Costo	4	3	2	2
Mantenimiento	4	4	4	3
Disponibilidad	5	5	4	4
Nivel de actualización	4	5	5	5
Puntaje ponderado	34	37	35	34

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

Tabla 58

Evaluación de Breakers Inteligentes Según Criterios Técnicos y Operativos

Criterio	RCBO / RCD inteligentes	Breakers por outlet	Breakers inalámbricos
Precisión	4	5	3
Confiabilidad	5	5	3
Escalabilidad	4	5	5
Compatibilidad (Ubuntu/Zabbix)	4	5	5
Costo	3	3	3
Mantenimiento	4	4	3
Disponibilidad	5	4	3
Nivel de actualización	4	5	4
Puntaje ponderado	33	36	29

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

El resultado ponderado evidencia que el MCCB inteligente obtiene el mayor puntaje (37), posicionándose como la opción más adecuada para el datacenter por su alta precisión, confiabilidad, escalabilidad y excelente compatibilidad con plataformas de monitoreo. Le siguen los breakers por outlet (36) y el ACB inteligente (35), que destacan por su capacidad de control granular y su aplicación en infraestructuras de alta criticidad. En contraste, los breakers

inalámbricos presentan el puntaje más bajo, lo que refleja limitaciones en confiabilidad y mantenimiento, haciéndolos menos recomendables para circuitos críticos.

De acuerdo con las matrices de evaluación, se evidencia que las soluciones tecnológicas con mayor nivel de inteligencia, integración y vigencia obtienen los puntajes más altos, lo que confirma que para un data center como el que tiene la empresa Transportes Gayco, los componentes modernos y compatibles con plataformas de monitoreo centralizado resultan ser los más adecuados. Sensores capacitivos, sistemas de detección avanzada, PDUs inteligentes, tableros con capacidades de control y breakers inteligentes destacan por su equilibrio entre precisión, confiabilidad, escalabilidad y compatibilidad con Ubuntu/Zabbix.

La matriz muestra que las tecnologías básicas o tradicionales, aunque presentan ventajas en costo y simplicidad, tienden a obtener menores puntajes debido a limitaciones en actualización, visibilidad y capacidad de integración. Los resultados reflejan que una estrategia de monitoreo integral debe priorizar soluciones actualizadas y escalables, incluso con mayores costos iniciales, ya que aportan mayor confiabilidad operativa, reducción de riesgos y sostenibilidad a largo plazo, esto respalda la selección de tecnologías alineadas con la continuidad y criticidad del datacenter de la empresa.

Matriz de Evaluación de Protocolos.

Los criterios de evaluación definidos en la matriz permiten realizar una selección objetiva y coherente de los protocolos que soportarán el sistema de monitoreo integral del datacenter de la empresa Transportes Gayco. La compatibilidad con Ubuntu/Zabbix asegura la correcta integración con la plataforma tecnológica seleccionada, evitando dependencias innecesarias. La confiabilidad garantiza una transmisión estable de la información, fundamental en un entorno de operación continua. La seguridad evalúa la capacidad del protocolo para proteger los datos

mediante autenticación y cifrado, alineándose con buenas prácticas de ciberseguridad. La escalabilidad permite que el sistema crezca sin afectar el rendimiento. La latencia y eficiencia aseguran respuestas oportunas ante eventos críticos. La facilidad de implementación reduce la complejidad operativa y los costos asociados. La disponibilidad y soporte disminuyen el riesgo de obsolescencia y facilitan la resolución de incidentes. Por último, el nivel de actualización prioriza tecnologías vigentes, garantizando sostenibilidad y compatibilidad futura del sistema de monitoreo para la empresa.

En la Tabla 59 se presentan los criterios definidos para la evaluación de protocolos de monitoreo, los cuales permiten analizar de manera comparativa su idoneidad para el datacenter, considerando aspectos técnicos, operativos y de soporte, con el fin de seleccionar aquellos que garanticen compatibilidad, confiabilidad y eficiencia en la gestión de infraestructura crítica.

Tabla 59

Criterios para la Evaluación de Protocolos de Monitoreo

Código	Criterio
A	Compatibilidad con Ubuntu/Zabbix
B	Confiabilidad
C	Seguridad
D	Escalabilidad
E	Latencia / Eficiencia
F	Facilidad de implementación
G	Disponibilidad / Soporte
H	Nivel de actualización

Nota. Los criterios establecidos permiten evaluar de manera cuantitativa y cualitativa los protocolos de monitoreo, considerando su desempeño técnico, compatibilidad con la plataforma de monitoreo, eficiencia operativa y viabilidad de implementación en el *data center* de la organización.

En la Tabla 60 se presenta la evaluación comparativa de las variantes del protocolo SNMP utilizadas para el sistema de monitoreo del datacenter, considerando criterios de compatibilidad con Ubuntu/Zabbix, confiabilidad, seguridad, escalabilidad, eficiencia, facilidad de implementación, disponibilidad y nivel de actualización, con el fin de identificar la opción más adecuada para entornos críticos de infraestructura.

Tabla 60

Evaluación de Protocolos SNMP Según Criterios Técnicos y Operativos

Criterio	SNMPv1	SNMPv2c	SNMPv3	SNMPv1 Trap	SNMPv2 Trap	INFORM
Compatibilidad con Ubuntu/Zabbix	5	5	5	5	5	5
Confiabilidad	3	4	5	3	4	5
Seguridad	1	1	5	1	1	5
Escalabilidad	3	4	5	3	4	4
Latencia / Eficiencia	4	5	4	5	5	4
Facilidad de implementación	5	5	3	5	5	3
Disponibilidad / Soporte	5	5	5	5	5	5
Nivel de actualización	1	2	5	1	2	5
Puntaje ponderado	27	31	37	28	31	36

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

La evaluación evidencia que SNMPv3 es la variante más adecuada para el sistema de monitoreo, al obtener el mayor puntaje ponderado (37), gracias a su alto nivel de seguridad, confiabilidad y compatibilidad con Ubuntu/Zabbix, lo que lo hace ideal para entornos críticos como el data center. Le siguen INFORM (36) y SNMPv2c/Trap (31), que ofrecen buen rendimiento, aunque con limitaciones en seguridad. En contraste, SNMPv1 y SNMPv1 Trap

presentan los puntajes más bajos debido a su obsolescencia y debilidades de seguridad, por lo que no se recomiendan para implementaciones productivas.

En la Tabla 61 se presenta la evaluación comparativa de los protocolos Syslog utilizados para la gestión y monitoreo de eventos en el datacenter, considerando criterios de compatibilidad con Ubuntu/Zabbix, confiabilidad, seguridad, escalabilidad, eficiencia, facilidad de implementación, disponibilidad y nivel de actualización, con el fin de identificar la alternativa más adecuada para entornos críticos de infraestructura.

Tabla 61

Evaluación de Protocolos Syslog Según Criterios Técnicos y Operativos

Criterio	BSD Syslog (RFC 3164)	IETF Syslog (RFC 5424)	UDP	TCP	Syslog sobre TLS
Compatibilidad con Ubuntu/Zabbix	5	5	5	5	5
Confiabilidad	3	5	2	4	5
Seguridad	1	4	1	2	5
Escalabilidad	3	5	3	4	5
Latencia / Eficiencia	5	4	5	4	4
Facilidad de implementación	5	4	5	4	3
Disponibilidad / Soporte	5	5	5	5	5
Nivel de actualización	2	5	2	4	5
Puntaje ponderado	29	37	28	32	37

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

La evaluación evidencia que Syslog sobre TLS y IETF Syslog (RFC 5424) obtienen el mayor puntaje ponderado (37), posicionándose como las opciones más adecuadas para un sistema de monitoreo en el datacenter, gracias a su alto nivel de seguridad, confiabilidad y

compatibilidad con Ubuntu/Zabbix, además de una adecuada escalabilidad. TCP (32) ofrece mayor confiabilidad que UDP (28), aunque con menores garantías de seguridad avanzada. En contraste, UDP y BSD Syslog (RFC 3164) presentan limitaciones importantes en seguridad y nivel de actualización, por lo que no se recomiendan para entornos críticos.

En la Tabla 62 se presenta la evaluación comparativa de las variantes del protocolo Modbus utilizadas para el sistema de monitoreo del datacenter, considerando criterios de compatibilidad con Ubuntu/Zabbix, confiabilidad, seguridad, escalabilidad, eficiencia, facilidad de implementación, disponibilidad y nivel de actualización, con el fin de identificar la alternativa más adecuada para entornos críticos de infraestructura.

Tabla 62

Evaluación de Protocolos Modbus Según Criterios Técnicos y Operativos

Criterio	Modbus RTU	Modbus ASCII	Modbus TCP/IP	Modbus RTU over TCP	Modbus Plus	Modbus UDP
Compatibilidad con Ubuntu/Zabbix	4	3	5	5	2	3
Confiabilidad	5	3	5	4	4	2
Seguridad	1	1	2	2	1	1
Escalabilidad	3	2	5	4	2	3
Latencia / Eficiencia	4	2	5	4	3	4
Facilidad de implementación	4	3	5	4	2	3
Disponibilidad / Soporte	5	4	5	5	2	2
Nivel de actualización	3	2	5	4	1	2
Puntaje ponderado	29	20	37	32	17	20

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

La evaluación evidencia que Modbus TCP/IP es la variante más adecuada para el sistema de monitoreo, al obtener el mayor puntaje ponderado (37), gracias a su alta compatibilidad con Ubuntu/Zabbix, buena escalabilidad y eficiencia, lo que lo hace ideal para entornos de datacenter. En segundo lugar, se ubica Modbus RTU over TCP (32), el cual resulta útil como solución de transición entre entornos industriales y redes IP. Modbus RTU (29) mantiene una confiabilidad aceptable, aunque presenta limitaciones en seguridad y escalabilidad. En contraste, Modbus ASCII, Modbus UDP y Modbus Plus obtienen los puntajes más bajos, por lo que no se recomiendan para implementaciones modernas o críticas.

En la Tabla 63 se presenta la evaluación comparativa de las variantes del protocolo BACnet utilizadas para el monitoreo de infraestructura en el data center, considerando criterios de compatibilidad con Ubuntu/Zabbix, confiabilidad, seguridad, escalabilidad, latencia/eficiencia, facilidad de implementación, disponibilidad y nivel de actualización, con el fin de identificar la alternativa más adecuada para un sistema de monitoreo integral.

Tabla 63

Evaluación de Protocolos BACnet Según Criterios Técnicos y Operativos

Criterio	BACnet/IP	BACnet MS/TP	BACnet Ethernet	BACnet PTP	BACnet LonTalk
Compatibilidad con Ubuntu/Zabbix	5	4	3	2	2
Confiabilidad	5	5	4	3	4
Seguridad	4	2	1	1	1
Escalabilidad	5	3	3	1	2
Latencia / Eficiencia	5	3	4	2	3
Facilidad de implementación	4	3	2	2	2
Disponibilidad / Soporte	5	5	3	2	2
Nivel de actualización	5	4	2	1	1
Puntaje ponderado	38	29	22	14	17

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

La evaluación evidencia que BACnet/IP es claramente la mejor alternativa, al alcanzar el mayor puntaje ponderado (38), destacándose por su alta compatibilidad con Ubuntu/Zabbix, excelente confiabilidad, escalabilidad y bajo nivel de latencia, lo que lo convierte en la opción más adecuada para un sistema de monitoreo integral en un datacenter. BACnet MS/TP (29) se posiciona como una opción válida a nivel de campo, aunque con limitaciones en seguridad y escalabilidad. En contraste, BACnet Ethernet, BACnet PTP y BACnet LonTalk presentan puntajes bajos debido a su obsolescencia, menor soporte y dificultades de integración, por lo que no se recomiendan para nuevos despliegues.

En la Tabla 64 se presenta la evaluación comparativa de los protocolos de comunicación serie utilizados para la integración de sensores y dispositivos de campo en el sistema de monitoreo del datacenter, considerando criterios de compatibilidad con Ubuntu/Zabbix, confiabilidad, seguridad, escalabilidad, latencia/eficiencia, facilidad de implementación, disponibilidad y nivel de actualización, con el fin de identificar el protocolo más adecuado para entornos de infraestructura crítica.

Tabla 64

Evaluación de Protocolos de Comunicación Serie Según Criterios Técnicos y Operativos

Criterio	RS-232	RS-485	RS-422	UART	SPI	I2C
Compatibilidad con Ubuntu/Zabbix	3	4	3	2	2	2
Confiabilidad	3	5	4	4	5	4
Seguridad	1	1	1	1	1	1
Escalabilidad	1	4	2	1	1	2

Criterio	RS-232	RS-485	RS-422	UART	SPI	I2C
Latencia / Eficiencia	3	4	4	4	5	3
Facilidad de implementación	4	4	3	3	2	3
Disponibilidad / Soporte	4	5	3	4	3	4
Nivel de actualización	1	4	2	2	3	3
Puntaje ponderado	20	31	22	21	22	22

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

La evaluación evidencia que RS-485 es el protocolo serie más adecuado, al obtener el mayor puntaje ponderado (31), destacándose por su alta confiabilidad, buena escalabilidad y amplia adopción industrial, lo que lo hace idóneo para la integración de sensores y dispositivos de campo en el sistema de monitoreo. RS-422, SPI e I2C presentan puntajes intermedios, siendo útiles en escenarios específicos o a nivel interno de dispositivos, aunque con limitaciones para un monitoreo centralizado. En contraste, RS-232 y UART obtienen los puntajes más bajos debido a su baja escalabilidad, seguridad limitada y carácter obsoleto, por lo que no se recomiendan para nuevos despliegues en el data center.

En la Tabla 65 se presenta la evaluación comparativa de protocolos Fieldbus utilizados para la integración de sensores y dispositivos de campo en el sistema de monitoreo del data center, considerando criterios de compatibilidad con Ubuntu/Zabbix, confiabilidad, seguridad, escalabilidad, eficiencia, facilidad de implementación, disponibilidad y nivel de actualización, con el fin de identificar la alternativa más adecuada para entornos de infraestructura crítica.

Tabla 65*Evaluación de Protocolos Fieldbus Según Criterios Técnicos y Operativos*

Protocolo	Compatibilidad con Ubuntu/Zabbix	Confiabilidad	Seguridad	Escalabilidad	Latencia / Eficiencia	Facilidad de implementación	Disponibilidad / Soporte	Nivel de actualización	Puntaje ponderado
Fieldbus RS-485	4	5	1	4	4	4	5	4	31
1-Wire	3	3	1	2	2	4	4	3	22

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

Como se observa en la Tabla 65, el protocolo Fieldbus RS-485 obtiene el mayor puntaje ponderado, evidenciando un mejor desempeño en términos de confiabilidad, escalabilidad, disponibilidad y compatibilidad con entornos de monitoreo en data center. Por su parte, 1-Wire presenta un puntaje inferior debido a limitaciones en seguridad, escalabilidad y eficiencia, por lo que su uso se recomienda únicamente en escenarios simples o no críticos.

En la Tabla 66 se presenta la evaluación comparativa de los protocolos de mensajería utilizados para el monitoreo en el data center, considerando criterios de compatibilidad con Ubuntu/Zabbix, confiabilidad, seguridad, escalabilidad, latencia/eficiencia, facilidad de implementación, disponibilidad/soporte y nivel de actualización, con el fin de identificar la alternativa más adecuada para entornos de monitoreo modernos y de alta criticidad.

Tabla 66*Evaluación de Protocolos MQTT Según Criterios Técnicos y Operativos*

Criterio	MQTT 3.1.1	MQTT 5.0	MQTT-SN	WebSockets + MQTT
Compatibilidad con Ubuntu/Zabbix	5	5	3	4
Confiabilidad	5	5	4	4
Seguridad	4	5	3	4
Escalabilidad	5	5	4	5
Latencia / Eficiencia	5	5	5	4
Facilidad de implementación	5	4	3	3
Disponibilidad / Soporte	5	5	3	4
Nivel de actualización	4	5	4	5
Puntaje ponderado	38	39	29	33

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

La tabla 66 muestra que MQTT 5.0 es la alternativa más sólida, al obtener el mayor puntaje ponderado (39), destacándose por su alta compatibilidad con Ubuntu/Zabbix, excelente seguridad, escalabilidad y eficiencia, lo que lo hace ideal para sistemas de monitoreo modernos y de gran escala. MQTT 3.1.1 (38) también presenta un desempeño sobresaliente y sigue siendo una opción robusta y ampliamente adoptada. WebSockets + MQTT (33) resulta adecuado como complemento para visualización en tiempo real. En contraste, MQTT-SN (29) es útil únicamente en escenarios IoT específicos con sensores de bajo consumo, pero no como protocolo principal del data center.

En la Tabla 67 se presenta la evaluación comparativa de los protocolos basados en AMQP utilizados para sistemas de monitoreo, considerando criterios de compatibilidad con Ubuntu/Zabbix, confiabilidad, seguridad, escalabilidad, latencia/eficiencia, facilidad de

implementación, disponibilidad/soporte y nivel de actualización, con el fin de identificar la alternativa más adecuada para su implementación en entornos de data center.

Tabla 67

Evaluación de Protocolos AMQP Según Criterios Técnicos y Operativos

Criterio	AMQP 0-9-1	AMQP 1.0
Compatibilidad con Ubuntu/Zabbix	4	4
Confiabilidad	5	5
Seguridad	4	5
Escalabilidad	5	5
Latencia / Eficiencia	4	4
Facilidad de implementación	4	3
Disponibilidad / Soporte	5	4
Nivel de actualización	4	5
Puntaje ponderado	35	35

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

A partir de los resultados obtenidos, se evidencia que los protocolos AMQP 0-9-1 y AMQP 1.0 presentan un desempeño equivalente en términos generales. No obstante, AMQP 0-9-1 destaca por su mayor facilidad de implementación y adopción operativa, mientras que AMQP 1.0 sobresale en aspectos de seguridad y nivel de actualización, lo que lo hace más adecuado para arquitecturas empresariales complejas y escenarios de integración avanzada.

En la Tabla 68 se presenta la evaluación comparativa de los protocolos HTTP(S) utilizados en el sistema de monitoreo del data center, considerando criterios de compatibilidad con Ubuntu/Zabbix, confiabilidad, seguridad, escalabilidad, eficiencia, facilidad de

implementación, disponibilidad y nivel de actualización, con el fin de identificar la alternativa más adecuada para la exposición de APIs, dashboards y servicios de monitoreo seguros.

Tabla 68

Evaluación de Protocolos HTTP(S) Según Criterios Técnicos y Operativos

Criterio	HTTPS estándar	mTLS	HTTP/2	HTTP/3 (QUIC)
Compatibilidad con Ubuntu/Zabbix	5	5	5	4
Confiabilidad	5	5	5	5
Seguridad	4	5	4	5
Escalabilidad	5	5	5	5
Latencia / Eficiencia	4	3	5	5
Facilidad de implementación	5	3	4	3
Disponibilidad / Soporte	5	4	5	4
Nivel de actualización	4	5	5	5
Puntaje ponderado	37	35	38	36

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

De acuerdo con los resultados obtenidos, HTTP/2 alcanza el mayor puntaje ponderado (38), destacándose por su alta eficiencia, escalabilidad y compatibilidad con Ubuntu/Zabbix, lo que lo convierte en la opción más adecuada para APIs y dashboards del sistema de monitoreo. HTTPS estándar (37) continúa siendo una base sólida y ampliamente adoptada para comunicaciones seguras. HTTP/3 (QUIC) (36) presenta un desempeño sobresaliente y una arquitectura moderna orientada al futuro, aunque con mayor complejidad de implementación. Por su parte, mTLS (35) ofrece el mayor nivel de seguridad, siendo recomendable para integraciones internas críticas, aunque no siempre necesario para todos los servicios del sistema.

En la Tabla 69 se presenta la evaluación comparativa de los protocolos REST utilizados en sistemas de monitoreo, considerando criterios de compatibilidad con Ubuntu/Zabbix, confiabilidad, seguridad, escalabilidad, latencia/eficiencia, facilidad de implementación, disponibilidad/soporte y nivel de actualización, con el fin de identificar la alternativa más adecuada para entornos de datacenter que requieren integraciones seguras, escalables y confiables.

Tabla 69

Evaluación de Protocolos REST Según Criterios Técnicos y Operativos

Criterio	RESTful	REST-like	HATEOAS	REST + OAuth/JWT/API Keys/mTLS
Compatibilidad con Ubuntu/Zabbix	5	5	4	5
Confiabilidad	5	3	5	5
Seguridad	4	3	4	5
Escalabilidad	5	4	5	5
Latencia / Eficiencia	4	4	3	4
Facilidad de implementación	4	5	2	3
Disponibilidad / Soporte	5	5	4	5
Nivel de actualización	5	3	4	5
Puntaje ponderado	37	32	31	37

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

Los resultados evidencian que RESTful y REST con OAuth/JWT/API Keys/mTLS alcanzan el mayor puntaje ponderado (37), posicionándose como las alternativas más adecuadas para sistemas de monitoreo en datacenters. RESTful destaca por su equilibrio entre simplicidad, escalabilidad y compatibilidad con Ubuntu/Zabbix, mientras que REST con mecanismos de

seguridad avanzada sobresale en escenarios que requieren control de acceso robusto y protección de la información. Por su parte, REST-like y HATEOAS presentan desempeños aceptables, aunque con limitaciones en confiabilidad, seguridad o complejidad de implementación, lo que reduce su idoneidad como soluciones principales en entornos críticos.

En la Tabla 70 se presenta la evaluación comparativa de las variantes del protocolo WebSocket utilizadas para sistemas de monitoreo, considerando criterios de compatibilidad con Ubuntu/Zabbix, confiabilidad, seguridad, escalabilidad, latencia/eficiencia, facilidad de implementación, disponibilidad/soporte y nivel de actualización, con el fin de identificar la alternativa más adecuada para comunicaciones en tiempo real dentro del data center.

Tabla 70

Evaluación de Variantes del Protocolo WebSocket Según Criterios Técnicos y Operativos

Criterio	WebSocket estándar	WebSocket seguro (WSS)	WebSocket + STOMP	WebSocket + Socket.io	Texto / Binario
Compatibilidad con Ubuntu/Zabbix	4	5	4	5	4
Confiabilidad	4	5	5	4	4
Seguridad	2	5	4	4	3
Escalabilidad	5	5	5	5	5
Latencia / Eficiencia	5	5	4	4	5
Facilidad de implementación	4	4	3	3	5
Disponibilidad / Soporte	5	5	4	5	5
Nivel de actualización	4	5	4	5	4
Puntaje ponderado	33	39	33	35	35

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

De acuerdo con los resultados obtenidos, el protocolo WebSocket seguro (WSS) alcanza el mayor puntaje ponderado (39), posicionándose como la alternativa más adecuada para sistemas de monitoreo en tiempo real dentro del data center, debido a su alto nivel de seguridad, confiabilidad y compatibilidad con Ubuntu/Zabbix. Las variantes WebSocket + Socket.io y Texto/Binario presentan un desempeño sólido como soluciones complementarias, mientras que WebSocket estándar y WebSocket + STOMP, aunque funcionales, muestran limitaciones principalmente en aspectos de seguridad, por lo que se recomiendan únicamente para escenarios de menor criticidad.

En la Tabla 71 se presenta la evaluación comparativa de variantes del protocolo SMTP utilizadas para el envío de alertas del sistema de monitoreo del data center, considerando criterios de compatibilidad con Ubuntu/Zabbix, confiabilidad, seguridad, escalabilidad, latencia/eficiencia, facilidad de implementación, disponibilidad/soporte y nivel de actualización, con el fin de identificar la alternativa más adecuada para notificaciones críticas en tiempo casi real.

Tabla 71

Evaluación de Variantes del Protocolo SMTP Según Criterios Técnicos y Operativos.

Criterio	MSA	MTA	SMTP Relay
Compatibilidad con Ubuntu/Zabbix	5	5	5
Confiabilidad	5	5	5
Seguridad	4	4	5
Escalabilidad	5	5	5
Latencia / Eficiencia	4	3	4
Facilidad de implementación	4	3	4
Disponibilidad / Soporte	5	5	5
Nivel de actualización	4	4	5
Puntaje ponderado	36	34	38

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

De acuerdo con los resultados obtenidos, SMTP Relay alcanza el mayor puntaje ponderado (38), posicionándose como la opción más adecuada para el envío de alertas críticas en el sistema de monitoreo del data center, gracias a su alta confiabilidad, escalabilidad y nivel de actualización. MSA presenta un desempeño sólido (36), siendo apropiado para entornos internos autenticados, mientras que MTA, aunque confiable, resulta menos eficiente para notificaciones en tiempo casi real, por lo que no se recomienda como alternativa principal.

En las Tablas 72 y 73 se presenta la evaluación comparativa de variantes de SMS utilizadas como mecanismos de notificación y alerta en sistemas de monitoreo, considerando criterios de compatibilidad con Ubuntu/Zabbix, confiabilidad, seguridad, escalabilidad, eficiencia, facilidad de implementación, disponibilidad/soporte y nivel de actualización, con el fin de identificar la alternativa más adecuada para entornos críticos de data center.

Tabla 72

Evaluación de Variantes SMS Según Criterios Técnicos y Operativos (Parte 1)

Criterio	SMS MT	SMS MO	SMS P2P	SMS A2P
Compatibilidad (Ubuntu/Zabbix)	5	4	3	5
Confiabilidad	5	4	3	5
Seguridad	3	3	2	4
Escalabilidad	5	4	3	5
Latencia / Eficiencia	4	3	3	4
Facilidad de implementación	5	4	5	4
Disponibilidad / Soporte	5	5	5	5
Nivel de actualización	4	4	3	5
Puntaje ponderado	36	31	27	37

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

Tabla 73

Evaluación de Variantes SMS Según Criterios Técnicos y Operativos (Parte 2)

Criterio	Flash SMS	Binary SMS	Premium SMS	Long SMS
Compatibilidad (Ubuntu/Zabbix)	4	3	2	5
Confiabilidad	4	4	4	4
Seguridad	2	3	3	3
Escalabilidad	3	3	2	5
Latencia / Eficiencia	4	4	3	3
Facilidad de implementación	4	3	2	5
Disponibilidad / Soporte	3	3	3	5
Nivel de actualización	2	3	2	4
Puntaje ponderado	26	26	21	34

Nota. Los resultados evidencian que SMS A2P y SMS MT presentan los mejores niveles de desempeño para el envío de alertas críticas en sistemas de monitoreo, mientras que variantes como Premium SMS y Binary SMS muestran limitaciones en seguridad, escalabilidad y aplicabilidad en entornos de alta criticidad.

En las tablas se muestra que SMS A2P es la variante más adecuada para el sistema de monitoreo, al alcanzar el mayor puntaje ponderado (37), destacándose por su alta confiabilidad, escalabilidad y compatibilidad con plataformas como Ubuntu/Zabbix, lo que lo hace ideal para el envío de alertas automáticas críticas. SMS MT (36) también presenta un desempeño sólido para notificaciones directas a usuarios finales. Long SMS (34) resulta útil cuando se requiere mayor contenido informativo. En contraste, SMS P2P, Flash SMS, Binary SMS y Premium SMS

obtienen puntajes bajos debido a limitaciones en seguridad, control y aplicabilidad, por lo que no se recomiendan para entornos críticos de data center.

En la Tabla 74 se presenta la evaluación comparativa de los mecanismos de notificación tipo Push utilizados en el sistema de monitoreo del data center, considerando criterios de compatibilidad con Ubuntu/Zabbix, confiabilidad, seguridad, escalabilidad, eficiencia, facilidad de implementación, disponibilidad/soporte y nivel de actualización, con el fin de identificar la alternativa más adecuada para la generación y entrega de alertas críticas.

Tabla 74

Evaluación de Mecanismos de Notificación Tipo Push Según Criterios Técnicos y Operativos

Criterio	APNs FCM		Web Push	Push corporativo	Push por mensajería instantánea	Push IoT	Push 2FA
Compatibilidad (Ubuntu/Zabbix)	4	5	5	5	5	4	4
Confiabilidad	5	5	4	5	4	4	5
Seguridad	5	5	4	5	4	3	5
Escalabilidad	5	5	5	5	5	5	4
Latencia / Eficiencia	4	4	4	4	4	5	4
Facilidad de implementación	3	4	4	3	4	3	3
Disponibilidad / Soporte	5	5	5	4	5	4	5
Nivel de actualización	5	5	5	4	5	3	5
Puntaje ponderado	36	38	36	35	36	31	35

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

Los resultados evidencian que FCM (Firebase Cloud Messaging) alcanza el mayor puntaje ponderado (38), posicionándose como la alternativa más sólida para la entrega de alertas

críticas en el sistema de monitoreo del data center, gracias a su alta confiabilidad, seguridad, escalabilidad y compatibilidad con Ubuntu/Zabbix.

APNs, Web Push y los mecanismos de mensajería instantánea presentan un desempeño alto (36), siendo opciones complementarias viables según el tipo de plataforma y usuario final. Push corporativo y Push 2FA mantienen un buen equilibrio funcional, mientras que Push IoT obtiene el puntaje más bajo (31), lo que indica que su uso es más adecuado para escenarios específicos de sensores y no como canal principal de notificación crítica.

En la Tabla 75 se presenta la evaluación comparativa de variantes del protocolo NTP, utilizadas para la sincronización horaria en sistemas de monitoreo de data center, considerando criterios de compatibilidad con Ubuntu/Zabbix, confiabilidad, seguridad, escalabilidad, latencia/eficiencia, facilidad de implementación, disponibilidad/soporte y nivel de actualización, con el fin de identificar la alternativa más adecuada para infraestructuras críticas.

Tabla 75

Evaluación de Variantes del Protocolo NTP Según Criterios Técnicos y Operativos

Criterio	NTP	SNTP	NTPv3	NTPv4
Compatibilidad con Ubuntu/Zabbix	5	5	4	5
Confiabilidad	5	4	4	5
Seguridad	3	2	2	5
Escalabilidad	5	4	4	5
Latencia / Eficiencia	4	5	4	5
Facilidad de implementación	5	5	4	4
Disponibilidad / Soporte	5	5	4	5
Nivel de actualización	4	4	2	5
Puntaje ponderado	36	34	28	39

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

Los resultados muestran que NTPv4 obtiene el mayor puntaje ponderado (39), destacándose por su alto nivel de seguridad, confiabilidad, precisión y actualización, lo que lo posiciona como la alternativa más adecuada para la sincronización horaria en sistemas de monitoreo de data center.

El NTP clásico (36) continúa siendo una opción sólida y ampliamente soportada, adecuada para entornos productivos tradicionales. SNTP (34) presenta un desempeño aceptable en dispositivos con recursos limitados o aplicaciones no críticas. En contraste, NTPv3 (28) evidencia limitaciones importantes en seguridad y vigencia tecnológica, por lo que no se recomienda para infraestructuras modernas o de alta criticidad.

En la Tabla 76 se presenta la evaluación comparativa de los protocolos de acceso seguro (SSH) empleados en el sistema de monitoreo del data center, considerando criterios de compatibilidad con Ubuntu/Zabbix, confiabilidad, seguridad, escalabilidad, eficiencia, facilidad de implementación, disponibilidad/soporte y nivel de actualización, con el fin de identificar la alternativa más adecuada para entornos críticos de administración y transferencia segura.

Tabla 76

Evaluación de Protocolos SSH Según Criterios Técnicos y Operativos

Criterio	SSH-1	SSH-2	SFTP	SCP	SSH Tunneling
Compatibilidad con Ubuntu/Zabbix	2	5	5	4	5
Confiabilidad	3	5	5	4	5
Seguridad	1	5	5	4	5
Escalabilidad	2	5	4	3	4
Latencia / Eficiencia	3	4	3	4	3
Facilidad de implementación	3	5	4	4	3
Disponibilidad / Soporte	2	5	5	4	5
Nivel de actualización	1	5	5	2	4
Puntaje ponderado	17	39	36	29	34

Nota: La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

Los resultados muestran que SSH-2 es el protocolo más adecuado para la administración segura en el data center, al obtener el mayor puntaje ponderado (39), destacándose por su alto nivel de seguridad, confiabilidad, compatibilidad con Ubuntu/Zabbix y vigencia tecnológica. SFTP presenta un desempeño sólido (36), siendo ideal para transferencias seguras de archivos. SSH Tunneling (34) resulta adecuado como mecanismo complementario para accesos protegidos a servicios internos. En contraste, SCP (29) y especialmente SSH-1 (17) evidencian limitaciones significativas en seguridad y actualización, por lo que no se recomiendan para entornos críticos.

En la Tabla 77 se presenta la evaluación comparativa de protocolos analógicos utilizados para el monitoreo de variables críticas en entornos industriales y de data center, considerando criterios de confiabilidad, seguridad, escalabilidad, latencia, facilidad de implementación, disponibilidad y nivel de actualización, con el fin de identificar la alternativa más adecuada para sistemas de monitoreo continuo y confiable.

Tabla 77

Evaluación de Protocolos Analógicos Según Criterios Técnicos y Operativos

Criterio	4–20 mA	0–10 V
Compatibilidad con Ubuntu/Zabbix	3	3
Confiabilidad	5	3
Seguridad	1	1
Escalabilidad	4	3
Latencia / Eficiencia	5	4
Facilidad de implementación	4	5
Disponibilidad / Soporte	5	5

Criterio	4–20 mA	0–10 V
Nivel de actualización	4	3
Puntaje ponderado	31	27

Nota. La valoración se realizó en una escala de 1 a 5 para cada criterio, donde 5 representa el mayor nivel de cumplimiento. El puntaje ponderado corresponde a la suma de los valores obtenidos por criterio.

Los resultados obtenidos evidencian que la señal 4–20 mA alcanza el mayor puntaje ponderado (31), posicionándose como la opción más adecuada para el monitoreo de variables críticas en entornos industriales y de data center. Su alta confiabilidad, baja latencia e inmunidad al ruido eléctrico la convierten en una alternativa robusta para aplicaciones donde la estabilidad y la detección temprana de fallas son prioritarias.

Por su parte, la señal 0–10 V, aunque presenta ventajas en facilidad de implementación y costos, obtiene un puntaje inferior (27), reflejando mayores limitaciones frente a interferencias eléctricas y estabilidad en distancias largas, por lo que se recomienda únicamente para aplicaciones no críticas o de corto alcance.

De acuerdo con las matrices de evaluación de protocolos, se evidencia una clara preferencia por tecnologías modernas, seguras y nativas IP, alineadas con el entorno de Ubuntu Server y Zabbix y con los requerimientos de un sistema de monitoreo integral para un datacenter. Protocolos como SNMPv3, Syslog sobre TLS, Modbus TCP/IP, BACnet/IP, MQTT 5.0, HTTP/2, NTPv4 y SSH-2 obtienen los puntajes más altos, destacándose por su alta compatibilidad, confiabilidad, escalabilidad, seguridad y nivel de actualización, lo que los convierte en las opciones más adecuadas para operación continua y crítica.

Por el contrario, se observa que versiones antiguas o heredadas (SNMPv1, TLS 1.0/1.1, Modbus Plus, BACnet PTP, RS-232, SSH-1, señales 0–10 V) presentan puntajes bajos,

principalmente por deficiencias en seguridad, escalabilidad y vigencia tecnológica, por lo que no se recomiendan para nuevos despliegues.

Por último, la matriz confirma que la selección de protocolos debe priorizar seguridad, integración IT/OT y sostenibilidad a largo plazo, garantizando un monitoreo confiable, escalable y alineado con buenas prácticas para la continuidad operativa del data center de Transportes Gayco.

Análisis Costo-Beneficio y Viabilidad de Implementación de las Herramientas de Monitoreo

En la Tabla 78 se pueden apreciar los principales equipos y componentes seleccionados para la implementación de la estrategia de monitoreo integral propuesta para el data center de la empresa Transportes Gayco S.A.S., así como una estimación aproximada de los costos asociados a su adquisición, configuración e integración.

La selección de estos elementos se realizó teniendo en cuenta los resultados obtenidos en las matrices de evaluación de herramientas, sensores, protocolos y componentes tecnológicos previamente desarrolladas, además de su compatibilidad con la arquitectura lógica y física planteada para la solución de monitoreo.

Tabla 78

Equipos de Monitoreo Seleccionados y Costos Estimados de Implementación para la Estrategia de Monitoreo Integral

Equipo de monitoreo	Función dentro de la solución	Conexión / protocolo	Costo estimado (COP)
Servidor de monitoreo Zabbix	Centraliza métricas, alertas y eventos de infraestructura TI	LAN / SNMPv3 / Zabbix Agent / Modbus TCP/IP	\$0 si se virtualiza / \$4.000.000–

Equipo de monitoreo	Función dentro de la solución	Conexión / protocolo	Costo estimado (COP)
			\$8.000.000 si es físico
Gateway Modbus RTU/TCP	Integra sensores ambientales, medidor eléctrico y planta eléctrica	RS-485 / Modbus TCP/IP	\$600.000– \$2.500.000
Tarjeta SNMP para UPS	Permite monitorear estado, carga y autonomía de las UPS	SNMP / Ethernet	\$500.000–\$800.000
Medidor eléctrico Modbus	Monitorea variables eléctricas del data center	RS-485 / Modbus	\$600.000– \$1.500.000
Sensor de temperatura	Supervisa la temperatura del cuarto de equipos	Analógico / RS-485	\$280.000–\$565.000
Sensor de humedad	Monitorea la humedad relativa del data center	Analógico / RS-485	\$280.000–\$565.000
Detector de humo	Detecta presencia de humo y genera alertas tempranas	Contacto seco / Gateway Modbus	\$80.000–\$250.000
Sensor magnético de puerta	Detecta aperturas no autorizadas del cuarto de equipos	Contacto seco / Gateway Modbus	\$30.000–\$120.000
Cableado de señal AWG 18–22	Interconecta sensores y dispositivos de monitoreo	Señal analógica / RS-485	\$200.000–\$500.000

Equipo de monitoreo	Función dentro de la solución	Conexión / protocolo	Costo estimado (COP)
Cableado UTP categoría 6	Permite conectividad Ethernet de la solución	Ethernet	\$200.000–\$600.000
Servicio profesional de ingeniería	Configuración, integración, parametrización SNMP, Zabbix y pruebas de funcionamiento	Servicios especializados TI	\$80.000–\$180.000 por hora
Implementación estimada (40–80 horas)	Instalación, configuración, documentación y validación de la solución	Servicios especializados TI	\$3.200.000–\$14.400.000

Nota. Los costos presentados corresponden a estimaciones aproximadas del mercado colombiano para el año 2025 y pueden variar según fabricante, proveedor, complejidad de la implementación y alcance de la solución.

De acuerdo con los costos estimados presentados en la Tabla 78, la implementación de la estrategia integral de monitoreo para el data center de la empresa Transportes Gayco S.A.S. tendría un costo aproximado que oscila entre los \$9.970.000 COP y \$29.300.000 COP, dependiendo del alcance de la solución, el tipo de infraestructura seleccionada y el nivel de integración requerido.

Este valor contempla la adquisición de los principales componentes de monitoreo, incluyendo sensores ambientales, medidores eléctricos, gateway de integración, tarjetas SNMP para UPS, cableado y el servidor de monitoreo, así como los costos asociados a los servicios

profesionales de instalación, configuración, parametrización y pruebas de funcionamiento de la plataforma.

En la Tabla 79 se presenta la relación entre los principales activos y amenazas identificados durante el análisis de riesgos realizado mediante la metodología Magerit y los equipos de monitoreo propuestos dentro de la solución diseñada para Transportes Gayco S.A.S.

La tabla permite evidenciar cómo cada componente de monitoreo contribuye a la mitigación de riesgos asociados a la disponibilidad, continuidad operativa y seguridad del data center, integrando mecanismos de supervisión orientados a la detección temprana de incidentes relacionados con condiciones ambientales, fallas eléctricas, interrupciones de red y accesos no autorizados.

Tabla 79

Relación Entre los Principales Riesgos Identificados y los Equipos de Monitoreo Propuestos

Riesgo identificado	Impacto		Equipo de monitoreo asociado	Beneficio esperado
	potencial en la organización	Activos afectados		
Sobrecalentamiento del data center por fallas en aire acondicionado	Daño de servidores, interrupción de servicios y pérdida de disponibilidad	Servidores, NAS, switches, data center	Sensor de temperatura, Gateway Modbus y servidor Zabbix	Detección temprana de incremento térmico y generación automática de alertas

	Impacto	Activos afectados	Equipo de monitoreo asociado	Beneficio esperado
Riesgo identificado	potencial en la organización			
Fallas eléctricas y variaciones de voltaje	Apagado inesperado de equipos, corrupción de datos y daños en hardware	Servidores, almacenamiento, redes, UPS	Tarjeta SNMP para UPS, medidor eléctrico Modbus y Zabbix	Supervisión del estado eléctrico y reducción de interrupciones operativas
Incendio o presencia de humo en el cuarto de equipos	Pérdida total o parcial de la infraestructura tecnológica	Data center, servidores, redes y almacenamiento	Detector de humo integrado al Gateway Modbus y Zabbix	Alertamiento temprano y reducción del impacto ante incidentes críticos
Acceso físico no autorizado al data center	Manipulación indebida, robo de información o sabotaje	Data center, servidores y equipos de comunicaciones	Sensor magnético de puerta y sistema de alertas Zabbix	Control y monitoreo de accesos físicos al cuarto de equipos
Caídas de red o indisponibilidad de	Interrupción de operaciones logísticas y	LAN, internet	Servidor Zabbix, SNMPv3	Supervisión continua de disponibilidad y

	Impacto	Activos afectados	Equipo de monitoreo asociado	Beneficio esperado
Riesgo identificado	potencial en la organización			
servicios de comunicaciones	pérdida de conectividad	empresarial, switches y routers	y monitoreo de red	reducción del tiempo de respuesta ante fallas

Nota. La relación presentada se elaboró tomando como referencia los riesgos de mayor criticidad identificados mediante la metodología Magerit aplicada a los activos de información de la empresa Transportes Gayco S.A.S.

En la Tabla 80 se presenta una estimación aproximada de las pérdidas potenciales asociadas a incidentes críticos identificados en la infraestructura tecnológica de Transportes Gayco S.A.S.

La tabla relaciona eventos como fallas eléctricas, caídas de conectividad, problemas de climatización y afectaciones en equipos críticos, considerando el impacto operativo generado sobre los servicios y usuarios de la organización. Asimismo, permite evidenciar la importancia de implementar mecanismos de monitoreo preventivo que contribuyan a reducir tiempos de indisponibilidad, minimizar pérdidas económicas y fortalecer la continuidad operativa del data center.

Tabla 80*Estimación de Pérdidas Potenciales por Incidentes Críticos*

Incidente	Impacto estimado	Pérdida potencial aproximada
Caída internet empresarial	Interrupción operativa >100 empleados	\$8M–\$12M
Falla UPS	Apagado servidores y riesgo hardware	\$7M–\$65M
Sobre temperatura	Daño servidores y NAS	\$10M–\$65M
Caída switch core	Pérdida conectividad total	\$5M–\$15M
Incendio	Pérdida parcial infraestructura	>\$100M

Nota. Los valores presentados corresponden a estimaciones aproximadas de pérdidas operativas y tecnológicas derivadas de incidentes críticos en la infraestructura TI de Transportes Gayco S.A.S., considerando tiempos de indisponibilidad, afectación operativa, dependencia de internet y costos asociados a equipos críticos y continuidad del negocio.

De acuerdo con las estimaciones realizadas en la Tabla 81, las pérdidas potenciales asociadas a incidentes críticos pueden oscilar entre los \$85.000.000 COP y más de \$150.000.000 COP, valores significativamente superiores al costo estimado de implementación de la solución de monitoreo.

Esto evidencia que la inversión propuesta resulta viable y justificada, al permitir reducir riesgos operativos, minimizar tiempos de indisponibilidad y fortalecer la continuidad de los servicios críticos de la organización

Análisis ROSI de la Solución Propuesta. Con el propósito de evaluar la viabilidad económica de la estrategia de monitoreo propuesta para el data center de Transportes Gayco S.A.S., se realiza un análisis ROSI (Return on Security Investment), el cual permite estimar el retorno obtenido a partir de la reducción de pérdidas potenciales asociadas a incidentes críticos sobre la infraestructura tecnológica.

Para el cálculo se consideran los costos aproximados de implementación de la solución de monitoreo integral y las pérdidas potenciales identificadas en la Tabla 81, relacionadas con interrupciones operativas, fallas eléctricas, indisponibilidad de servicios críticos y afectaciones sobre equipos tecnológicos de la organización.

La fórmula empleada es la siguiente:

$$\text{ROSI} = (\text{Pérdidas mitigadas} - \text{Costo de implementación}) / \text{costo de implementación} \times 100$$

Para el presente análisis se toman como referencia los siguientes valores aproximados:

Tabla 81

Variables Utilizadas para el Cálculo del ROSI de la Solución de Monitoreo Propuesta

Concepto	Valor estimado
Pérdidas potenciales estimadas	\$150.000.000 COP
Costo promedio implementación solución	\$20.000.000 COP
Porcentaje estimado de mitigación mediante monitoreo	60 %
Pérdidas mitigadas estimadas	\$90.000.000 COP

Nota. Los valores presentados corresponden a estimaciones aproximadas utilizadas para evaluar el retorno de inversión en seguridad (ROSI) de la solución de monitoreo propuesta para Transportes Gayco S.A.S.

Con estos valores se aplica la formula ROSI donde:

$$\text{ROSI} = 90.000.000 - 20.000.000 / 20.000.000 * 100 = 350\%$$

El resultado obtenido evidencia que la implementación de la solución de monitoreo integral resulta económicamente viable para la organización, debido a que la inversión requerida es considerablemente menor frente a las pérdidas potenciales que podrían generarse por incidentes críticos en la infraestructura tecnológica.

El análisis demuestra que la adopción de mecanismos de monitoreo proactivo contribuye significativamente a la reducción del impacto operativo, disminución de tiempos de indisponibilidad y fortalecimiento de la continuidad del negocio, permitiendo obtener un retorno estimado del 350 % sobre la inversión realizada.

Diseño de los Elementos para Instalación de Agentes en Dispositivos, Configuración SNMP, Definición de Alertas y Visualización de Métricas, para la Implementación de la Estrategia
Arquitectura Lógica y Física de la Plataforma de Monitoreo

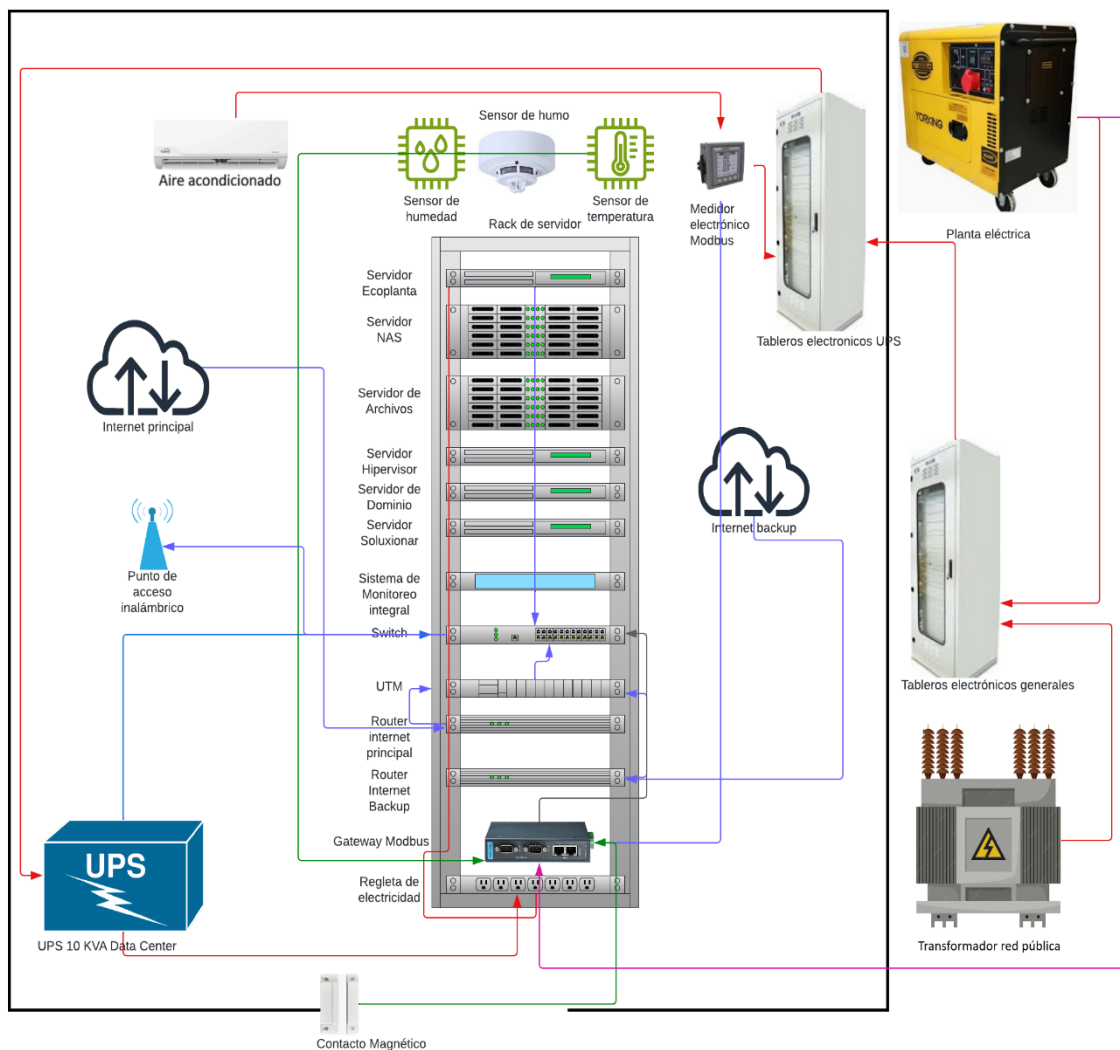
Arquitectura Física. La figura 5 ilustra el diseño físico de una solución de monitoreo integral para el cuarto de equipos de Transportes Gayco S.A.S, en la cual se integran de manera coordinada la infraestructura de red, los servidores, el sistema eléctrico y el monitoreo de variables ambientales del Data Center. El rack central concentra los servidores, los equipos de red, el sistema de monitoreo integral y un gateway Modbus, el cual actúa como eje de comunicación entre los dispositivos de campo y la plataforma de supervisión.

El gateway Modbus permite la integración directa del medidor electrónico de energía y de la planta eléctrica, facilitando la captura de variables eléctricas como consumo, estados y eventos, lo que contribuye al control y análisis del suministro energético. Adicionalmente, el gateway recibe la información proveniente de los sensores de temperatura, humedad, humo y contactos magnéticos, garantizando una supervisión continua y centralizada del entorno.

El aire acondicionado no se conecta de forma directa al sistema de monitoreo; sin embargo, su desempeño es evaluado mediante el análisis de las lecturas de temperatura y humedad obtenidas por los sensores ambientales, así como del consumo eléctrico medido a través del medidor Modbus. En conjunto, la solución incorpora enlaces redundantes de internet, UPS y tableros eléctricos, asegurando alta disponibilidad, continuidad operativa y capacidad de respuesta preventiva ante condiciones anómalas del Data Center.

Figura 5

Diseño Físico de la Solución de Monitoreo Integral para el Cuarto de Equipos de Gayco S.A.S.



Nota: En la imagen se evidencia todos los activos físicos seleccionados a monitorear en el cuarto de equipos con sus respectivos sensores.

Figura 6

Tipo de Cable Empleado en la Infraestructura del Sistema de Monitoreo

TIPO DE CABLE EMPLEADO	
Color	Tipo de cable
	Cable upt cat6
	Cable de señal 2 conductores (AWG 18–22)
	Par trenzado RS-485 (AWG 18–22)
	Cable eléctrico

Nota. La figura presenta la clasificación de los tipos de cable utilizados en el diseño físico de la solución, identificados mediante un código de colores. El color azul corresponde al cable UTP categoría 6 empleado para la transmisión de datos en la red; el color verde representa cables de señal de dos conductores (AWG 18–22) utilizados en sensores; el color morado identifica el cable de comunicación RS-485 (AWG 18–22) para dispositivos industriales; y el color rojo corresponde al cable eléctrico destinado a la alimentación de los equipos.

Tabla de Integración Física y de Comunicación de los Activos del Sistema de Monitoreo. Se realiza la tabla 82 con el propósito de complementar y detallar el diseño físico de la solución de monitoreo integral, describiendo la forma en que se integran los principales dispositivos y equipos que conforman la infraestructura del Data Center de Transportes Gayco. La tabla presenta de manera clara los componentes físicos más relevantes, como los servidores, el sistema de monitoreo, el gateway Modbus, los sensores ambientales y el medidor electrónico de energía, así como su interconexión mediante los protocolos SNMP y Modbus TCP/IP.

Los títulos de cada columna permiten identificar el dispositivo físico monitoreado, el tipo de conexión, el medio de conexión y el destino de la conexión física dentro de la solución. Esta organización facilita la comprensión de la arquitectura física, respalda la correcta instalación e

integración de los equipos y documenta cómo fluye la información desde los dispositivos de campo hasta el sistema de monitoreo central.

Por último, la tabla evidencia que la solución no se limita al monitoreo físico de equipos activos vía SNMP, sino que incorpora Modbus TCP/IP para la supervisión de variables eléctricas y ambientales provenientes del medidor de energía, la planta eléctrica y los sensores. Esta aproximación permite evaluar el desempeño del sistema de aire acondicionado de forma indirecta y cumplir con las recomendaciones ASHRAE, sin intervenir ni modificar el equipo HVAC existente.

Tabla 82

Integración Física y Comunicación de los Activos del Sistema de Monitoreo

Activo o elemento	Tipo de conexión	Tipo de cable	Se conecta físicamente a
Sistema de Monitoreo Integral (Zabbix)	Conexión directa a red LAN	UTP categoría 6	Switch core
Switch core	Conexión de red LAN	UTP categoría 6	UTM/Firewall; Sistema de Monitoreo Integral (Zabbix); servidores (Ecoplanta, NAS, Archivos, Hipervisor, Dominio, Soluxionar); UPS (tarjeta SNMP); puntos de acceso inalámbrico; gateway Modbus
UTM / Firewall	Conexión perimetral LAN–WAN	UTP categoría 6	Routers de Internet; switch core (LAN)
Router de Internet principal	Enlace WAN	UTP categoría 6 / fibra del ISP	Proveedor ISP principal; UTM/Firewall
Router de Internet de respaldo	Enlace WAN	UTP categoría 6 / fibra del ISP	Proveedor ISP de respaldo; UTM/Firewall
UPS 10 kVA del data center	Tarjeta de red SNMP	UTP categoría 6	Gateway Ethernet
Punto de acceso inalámbrico	Conexión LAN	UTP categoría 6	Switch core

Activo o elemento	Tipo de conexión	Tipo de cable	Se conecta físicamente a
Servidor Ecoplanta	Conexión LAN al switch	UTP categoría 6	Switch core
Servidor NAS	Conexión LAN al switch	UTP categoría 6	Switch core
Servidor de archivos	Conexión LAN al switch	UTP categoría 6	Switch core
Servidor hipervisor	Conexión LAN al switch	UTP categoría 6	Switch core
Servidor de dominio	Conexión LAN al switch	UTP categoría 6	Switch core
Servidor Soluxionar	Conexión LAN al switch	UTP categoría 6	Switch core
Aire acondicionado del cuarto de equipos	Medición indirecta vía sensores y medidor eléctrico	Instrumentación / RS-485 / UTP	Tablero eléctrico
Planta eléctrica MODASA MP-210	Controlador digital → gateway → red	Par trenzado RS-485 (AWG 18–22) / UTP categoría 6	Puerto RS-485 del gateway Modbus
Detector de humo	Contacto seco a entrada digital del gateway	Cable de señal de 2 conductores (AWG 18–22)	Entrada digital del gateway Modbus
Sensor de temperatura (analógico)	Entrada analógica al gateway	Cable de instrumentación de 2 conductores (AWG 18–22)	Entrada analógica del gateway Modbus
Sensor de humedad (analógico)	Entrada analógica al gateway	Cable de instrumentación de 2 conductores (AWG 18–22)	Entrada analógica del gateway Modbus
Medidor eléctrico Modbus	Conexión directa a red o vía gateway	UTP categoría 6 / par trenzado RS-485 (AWG 18–22)	Gateway Ethernet
Sensor magnético de puerta	Contacto seco a entrada digital del gateway	Cable de señal de 2 conductores (AWG 18–22)	Entrada digital del gateway Modbus

Nota. La tabla presenta la integración física y los medios de comunicación de los activos que conforman el sistema de monitoreo del *data center*, detallando los tipos de conexión, cableado

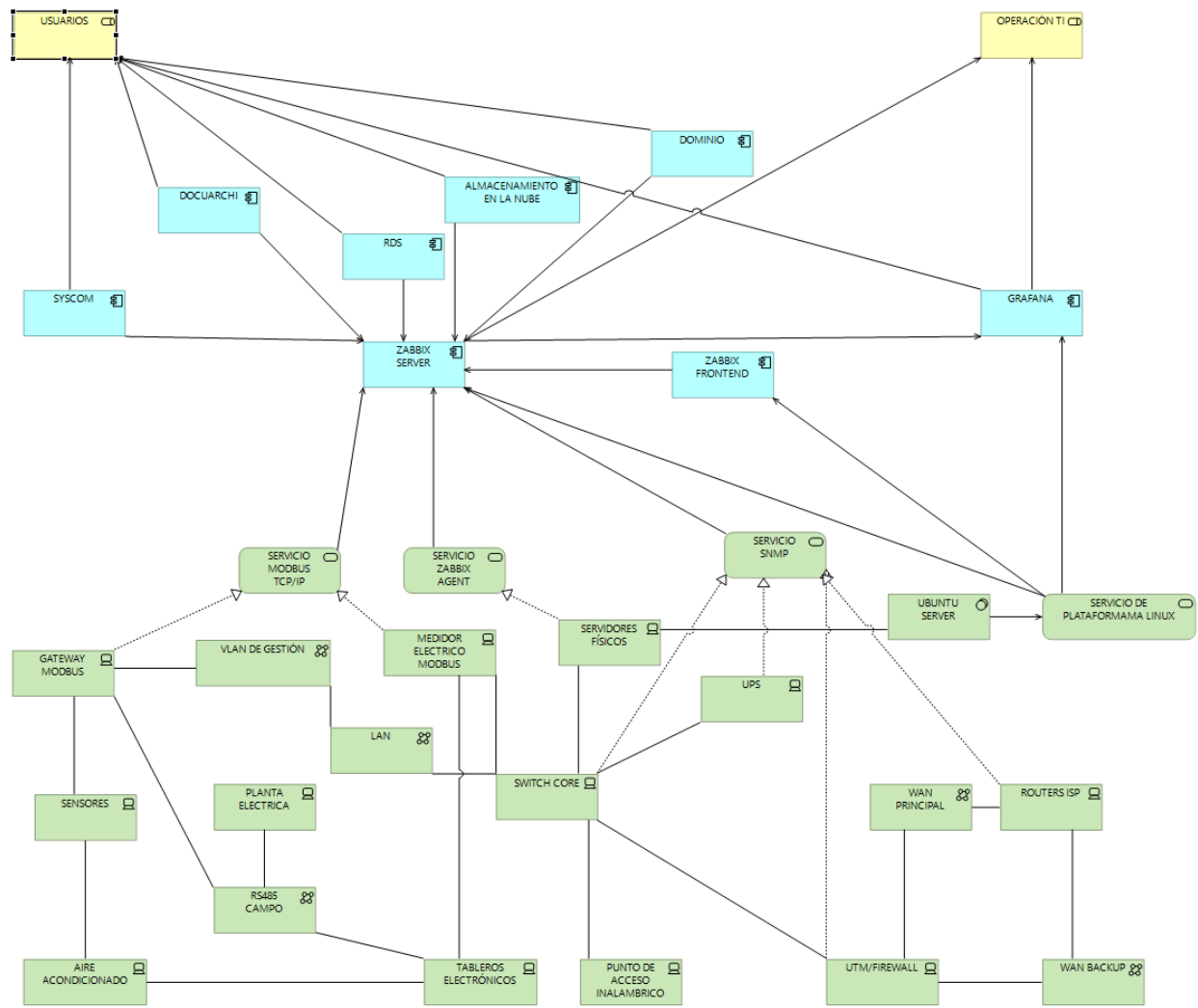
utilizado y los puntos de interconexión, con el fin de evidenciar la arquitectura física y la trazabilidad de la infraestructura supervisada.

Arquitectura Lógica. En la figura 7 se presenta el diseño lógico en ArchiMate que, según, (Opekunova L. A. and Opekunov, 2020) este programa permite representar y comprender de manera estructurada la arquitectura de una plataforma tecnológica de monitoreo y operación TI, mostrando las relaciones entre usuarios, servicios, aplicaciones, infraestructura y componentes físicos.

De igual manera, podemos observar cómo los usuarios y el área de operación TI interactúan con servicios lógicos como el dominio, RDS, almacenamiento en la nube y herramientas de visualización como Grafana, los cuales se apoyan en un servidor Zabbix como núcleo del sistema de monitoreo para la empresa transportes Gayco. Este servidor centraliza la recolección de métricas provenientes de distintos servicios y protocolos, tales como Zabbix Agent, SNMP y Modbus TCP/IP, permitiendo supervisar tanto servidores Linux, servicios web y componentes del sistema operativo, como infraestructura física y eléctrica.

Además, el diseño integra elementos de red y seguridad (switch core, VLAN de gestión, firewall, WAN principal y de respaldo), dispositivos industriales y de energía (UPS, medidores eléctricos, sensores, tableros electrónicos y sistemas de climatización), evidenciando una arquitectura que unifica el monitoreo de TI y OT. El modelo ArchiMate facilita la visualización de dependencias, flujos de información y capas tecnológicas, contribuyendo a una mejor gestión, disponibilidad y toma de decisiones permitiendo así hacer una infraestructura de monitoreo integral para el data center de transportes Gayco S.A.S

Figura 7
Diseño Lógico de la Arquitectura de Monitoreo Representado Mediante ArchiMate



Nota. Representación gráfica del diseño de la solución lógica.

De acuerdo con el diseño lógico elaborado se establece la siguiente tabla donde se relacionan los elementos de origen con los elementos de destino, la capa en la que se encuentran, el modelo ArchiMate, el protocolo o tecnología de interconexión y la descripción. Esta matriz permite visualizar de manera estructurada cómo interactúan los distintos componentes de la arquitectura, facilitando la trazabilidad entre capas de negocio, aplicación y tecnología, apoya la

identificación de dependencias, flujos de información e integraciones existentes, garantizando coherencia con el modelo arquitectónico definido.

El uso de ArchiMate como marco de referencia asegura una representación estandarizada y comprensible de los elementos, mientras que la inclusión de protocolos y tecnologías de interconexión aporta claridad sobre los mecanismos de comunicación. En conjunto, la matriz constituye una herramienta clave para el análisis, validación y documentación del diseño lógico del sistema de monitoreo integral del Data Center de la empresa Transportes Gayco S.A.S.

En la Tabla 83 se presenta la arquitectura lógica desarrollada en la capa de negocio (Business) del modelo ArchiMate, en la cual se identifican las relaciones de tipo Serving entre los sistemas y los actores organizacionales (Usuarios y Operación TI), junto con los protocolos y tecnologías asociados. Esto permite evidenciar cómo los servicios de negocio son provistos y consumidos dentro del sistema de monitoreo, facilitando la comprensión de la interacción funcional entre los componentes y su alineación con las necesidades operativas.

Tabla 83

Arquitectura Lógica de la Capa de Negocio (Business) Según ArchiMate

Elemento origen	Elemento destino	Capa ArchiMate	Tipo de relación	Protocolo / tecnología	Descripción
SYSCOM	Usuarios	Business	Serving	HTTPS	Syscom presta servicios funcionales a los usuarios finales.
DOCUARCHI	Usuarios	Business	Serving	HTTPS	Docuarchi proporciona servicios de gestión documental a los usuarios.
RDS	Usuarios	Business	Serving	RDP/TLS	RDS ofrece acceso remoto seguro a los usuarios.
Almacenamiento en la nube	Usuarios	Business	Serving	HTTPS	Servicio de almacenamiento en la

Elemento origen	Elemento destino	Capa ArchiMate	Tipo de relación	Protocolo / tecnología	Descripción
					nube disponible para los usuarios.
Dominio	Usuarios	Business	Serving	LDAP / Kerberos	El dominio provee servicios de autenticación y control de acceso a los usuarios.
Grafana	Usuarios	Business	Serving	HTTP / HTTPS	Grafana proporciona visualización de métricas, paneles y <i>dashboards</i> de monitoreo a los usuarios.
Zabbix Server	Operación TI	Business	Serving	HTTP/HTTPS, SNMP, Modbus TCP/IP	Zabbix Server suministra alertas y paneles de monitoreo al área de Operación TI.
Grafana	Operación TI	Business	Serving	HTTP / HTTPS	Grafana provee paneles y visualización de métricas para análisis y toma de decisiones por parte de Operación TI.

Nota. La tabla describe la arquitectura lógica desarrollada en la capa de negocio (*Business layer*) del modelo ArchiMate, identificando las relaciones de tipo *Serving* entre los sistemas y los actores organizacionales, así como los protocolos y tecnologías que soportan la provisión de servicios, con el fin de evidenciar la alineación entre los procesos del negocio y las capacidades del sistema de monitoreo.

En la Tabla 84 se presenta la arquitectura lógica correspondiente a la capa de aplicación (Application) del diseño del sistema de monitoreo, modelada bajo el marco ArchiMate. En esta capa se identifican las relaciones de tipo *Serving* entre las aplicaciones, servicios de plataforma y herramientas de monitoreo, permitiendo evidenciar cómo Zabbix y Grafana interactúan con los sistemas corporativos para la supervisión de disponibilidad, servicios y métricas operativas, garantizando el soporte a la operación de TI y la continuidad del negocio.

Tabla 84*Capa de Aplicación del Diseño Lógico del Sistema de Monitoreo*

Elemento origen	Elemento destino	Capa ArchiMate	Tipo de relación	Protocolo / Tecnología	Descripción
SYSCOM	Zabbix Server	Application	Serving	HTTPS / ICMP	Zabbix monitorea la disponibilidad del sistema Syscom.
DOCUARCHI	Zabbix Server	Application	Serving	HTTPS / ICMP	Zabbix monitorea la disponibilidad del sistema Docuarchi.
RDS	Zabbix Server	Application	Serving	TCP / ICMP	Zabbix monitorea el servicio de Escritorio Remoto (RDS).
Almacenamiento en la nube	Zabbix Server	Application	Serving	HTTPS / TCP / ICMP	Zabbix verifica la disponibilidad de los servicios en la nube.
Dominio	Zabbix Server	Application	Serving	LDAP / ICMP	Zabbix monitorea los servicios del dominio y su disponibilidad.
Zabbix Frontend	Zabbix Server	Application	Serving	HTTPS	El frontend consulta y visualiza los datos recolectados por Zabbix Server.
Zabbix Server	Grafana	Application	Serving	API Zabbix / HTTPS	Zabbix Server expone datos de monitoreo consumidos por Grafana.
Servicio de plataforma Linux	Zabbix Server	Application	Serving	Linux OS / systemd	La plataforma Linux soporta la ejecución del servicio Zabbix Server.
Servicio de plataforma Linux	Zabbix Frontend	Application	Serving	Linux OS / Web Stack	Linux provee los servicios base para el frontend web de Zabbix.
Servicio de plataforma Linux	Grafana	Application	Serving	Linux OS / systemd	Linux provee el entorno de ejecución para Grafana.

Nota. La tabla describe las interacciones entre aplicaciones y servicios de plataforma en la capa de aplicación, destacando los protocolos y tecnologías utilizados para el monitoreo, visualización y soporte operativo del sistema de monitoreo implementado.

En las Tablas 85 y 86 se presenta la arquitectura lógica correspondiente a la capa de tecnología (Technology) del diseño del sistema de monitoreo, modelada bajo el marco ArchiMate. En esta capa se describen los servicios tecnológicos, dispositivos físicos, redes y mecanismos de comunicación que soportan la recolección de métricas, la conectividad y la operación de la infraestructura del data center, así como las relaciones de tipo Serving, Realization y Association que articulan la capa tecnológica con los servicios de monitoreo.

Tabla 85

Capa de Tecnología del Diseño Lógico – Servicios Tecnológicos y su Realización

Elemento origen	Elemento destino	Capa ArchiMate	Tipo de relación	Protocolo / Tecnología	Descripción
Servicio Modbus TCP/IP	Zabbix Server	Technology	Serving	Modbus TCP/IP	Entrega métricas eléctricas al sistema de monitoreo Zabbix.
Servicio Zabbix Agent	Zabbix Server	Technology	Serving	Zabbix Agent	Entrega métricas de rendimiento y estado de los servidores.
Servicio SNMP	Zabbix Server	Technology	Serving	SNMPv3	Entrega métricas de red, energía y dispositivos de infraestructura.
Ubuntu Server	Servicio de plataforma Linux	Technology	Serving	Linux Kernel / OS Services	Ubuntu Server provee el sistema operativo base para la plataforma Linux.
Gateway Modbus	Servicio Modbus TCP/IP	Technology	Realization	Modbus TCP/IP	El gateway implementa el servicio Modbus TCP/IP.
Medidor eléctrico Modbus	Servicio Modbus TCP/IP	Technology	Realization	Modbus TCP/IP	El medidor expone variables eléctricas del sistema.

Elemento origen	Elemento destino	Capa ArchiMate	Tipo de relación	Protocolo / Tecnología	Descripción
Servidores físicos	Servicio Zabbix Agent	Technology	Realization	Agente Zabbix	Los servidores ejecutan el agente Zabbix.
Switch core	Servicio SNMP	Technology	Realization	SNMPv3	El switch expone métricas mediante SNMP.
UTM / Firewall	Servicio SNMP	Technology	Realization	SNMPv3	El UTM expone métricas SNMP de seguridad y red.
Routers ISP	Servicio SNMP	Technology	Realization	SNMPv3	Los routers del ISP exponen métricas de conectividad.
UPS	Servicio SNMP	Technology	Realization	SNMPv3	La UPS expone estado y variables eléctricas.

Tabla 86*Capa de Tecnología del Diseño Lógico – Conectividad Física y Asociaciones Tecnológicas*

Elemento origen	Elemento destino	Capa ArchiMate	Tipo de relación	Protocolo / Tecnología	Descripción
Servidores físicos	Ubuntu Server	Technology	Association	Virtualización / Bare metal	Ubuntu Server está desplegado sobre la infraestructura física.
Aire acondicionado	Tableros electrónicos	Technology	Association	Alimentación eléctrica	El aire acondicionado recibe energía y control desde los tableros.
Aire acondicionado	Sensores	Technology	Association	Variables ambientales	El HVAC es monitoreado mediante sensores ambientales.
Sensores	Gateway Modbus	Technology	Association	Señales analógicas y digitales	Sensores cableados al gateway Modbus.
Planta eléctrica	RS-485 campo	Technology	Association	Modbus RTU / RS-485	Transmisión de datos eléctricos por bus de campo.
Tableros electrónicos	RS-485 campo	Technology	Association	Modbus RTU / RS-485	Tableros conectados al bus RS-485.

Elemento origen	Elemento destino	Capa ArchiMate	Tipo de relación	Protocolo / Tecnología	Descripción
Gateway Modbus	RS-485 campo	Technology	Association	RS-485	Gateway conectado al bus de campo.
Gateway Modbus	VLAN de gestión	Technology	Association	Ethernet / 802.1Q	Gateway conectado a la red de gestión.
Medidor eléctrico Modbus	Switch core	Technology	Association	Ethernet / 802.1Q	Medidor conectado a la red LAN.
Medidor eléctrico Modbus	Tableros electrónicos	Technology	Association	Alimentación eléctrica / señales	El medidor está integrado en los tableros eléctricos.
VLAN de gestión	LAN	Technology	Association	802.1Q	Transporte de la VLAN de gestión.
LAN	Switch core	Technology	Association	Ethernet / TCP/IP / ICMP / SNMP	El switch core centraliza la conmutación de la red LAN.
Switch core	UTM / Firewall	Technology	Association	Ethernet / SNMP / ICMP	Troncal entre la LAN y el perímetro.
Routers ISP	WAN principal	Technology	Association	SNMPv3 / ICMP	Enlace principal hacia Internet.
Routers ISP	WAN backup	Technology	Association	SNMPv3 / ICMP	Enlace de respaldo hacia Internet.
UTM / Firewall	WAN principal	Technology	Association	Ethernet / SNMP / ICMP	El UTM gestiona el enlace principal.
UTM / Firewall	WAN backup	Technology	Association	Ethernet / SNMP / ICMP	El UTM gestiona el enlace de respaldo.
Switch core	Servidores físicos	Technology	Association	Ethernet / Agente Zabbix	Servidores conectados al switch core.
Punto de acceso inalámbrico	Switch core	Technology	Association	Ethernet / SNMP	Punto de acceso conectado al switch core.

Nota. Las tablas describen la arquitectura lógica de la capa de tecnología del sistema de monitoreo, identificando los servicios tecnológicos, los elementos físicos que los implementan y las asociaciones de conectividad, energía y comunicación, con el fin de evidenciar la infraestructura que soporta la supervisión integral del data center.

Matriz de Evaluación de OIDs/MIBs

Según (Presuhn, 2002) la matriz de OIDs/MIBs es un instrumento técnico que permite definir y documentar las métricas de monitoreo obtenidas mediante el protocolo SNMP para los distintos activos de la infraestructura. Su propósito principal es identificar qué información se recolecta, desde qué dispositivos y bajo qué estándares, garantizando coherencia entre el diseño lógico y la implementación del sistema de monitoreo.

Un OID (Object Identifier) es un identificador numérico único que representa una métrica específica expuesta por un dispositivo a través de SNMP, como el estado de una interfaz, el uso de CPU, el tráfico de red o el nivel de batería de una UPS. Cada OID apunta a un objeto concreto dentro de la información de gestión del equipo.

Un MIB (Management Information Base) es un conjunto estructurado de definiciones que describe los objetos gestionables de un dispositivo, especificando el significado, tipo de dato y unidad de medida asociada a cada OID. En otras palabras, la MIB actúa como el diccionario que explica qué representa cada OID.

La información contenida en esta matriz se obtiene a partir de MIBs estándar definidas por organismos como el IETF (por ejemplo, IF-MIB, SNMPv2-MIB, UPS-MIB, HOST-RESOURCES-MIB), así como, cuando es pertinente, de MIBs proporcionadas por los fabricantes de los dispositivos. Estas fuentes aseguran que los OIDs utilizados sean reales, documentados y ampliamente soportados.

En la Tabla 87 se presenta la matriz de OIDs/MIBs definida para los activos críticos del sistema de monitoreo, la cual constituye la base para la posterior construcción de la matriz Polling vs. Trap. Esta matriz permite decidir de manera fundamentada el mecanismo de recolección de cada métrica (consulta periódica o notificación por evento) y sirve como insumo

directo para la elaboración de plantillas SNMPv3 y del runbook de instalación y operación del sistema de monitoreo.

Tabla 87

Matriz de OIDs y MIBs para el Sistema de Monitoreo

Activo	Marca	MIB	OID	Métrica	Objetivo de monitoreo
Switch core	Ruijie Networks	IF-MIB	1.3.6.1.2.1.2.2.1.8	Estado de interfaz	Disponibilidad
Switch core	Ruijie Networks	IF-MIB	1.3.6.1.2.1.2.2.1.10	Bytes recibidos	Rendimiento
Switch core	Ruijie Networks	IF-MIB	1.3.6.1.2.1.2.2.1.16	Bytes enviados	Rendimiento
Switch core	Ruijie Networks	SNMPv2-MIB	1.3.6.1.2.1.1.3	Uptime	Estabilidad
Switch core	Ruijie Networks	ENTITY-MIB	1.3.6.1.2.1.47.1.1.1.1.7	Estado físico	Infraestructura
Router ISP	Cisco	IF-MIB	1.3.6.1.2.1.2.2.1.8	Estado WAN	Disponibilidad
Router ISP	Cisco	IF-MIB	1.3.6.1.2.1.2.2.1.10	Tráfico entrante	Capacidad
Router ISP	Cisco	IF-MIB	1.3.6.1.2.1.2.2.1.16	Tráfico saliente	Capacidad
Router ISP	Cisco	SNMPv2-MIB	1.3.6.1.2.1.1.3	Uptime	Continuidad
Router ISP	Cisco	ENTITY-MIB	1.3.6.1.2.1.47	Estado del hardware	Infraestructura
Firewall	Sophos	HOST-RESOURCES-MIB	1.3.6.1.2.1.25.3.3.1.2	Uso de CPU	Rendimiento
Firewall	Sophos	HOST-RESOURCES-MIB	1.3.6.1.2.1.25.2.3.1.6	Uso de RAM	Capacidad
Firewall	Sophos	IF-MIB	1.3.6.1.2.1.2.2.1.8	Estado de interfaz	Disponibilidad
Firewall	Sophos	SNMPv2-MIB	1.3.6.1.2.1.1.3	Uptime	Continuidad
UPS	Powest Titan 10 kVA	UPS-MIB	1.3.6.1.2.1.33.1.2.1	Carga de batería	Energía

Activo	Marca	MIB	OID	Métrica	Objetivo de monitoreo
UPS	Powest Titan 10 kVA	UPS-MIB	1.3.6.1.2.1.33.1.2.4	Estado de batería	Evento crítico
UPS	Powest Titan 10 kVA	UPS-MIB	1.3.6.1.2.1.33.1.3.3.1.4	Voltaje de salida	Calidad eléctrica
UPS	Powest Titan 10 kVA	UPS-MIB	1.3.6.1.2.1.33.1.4.1	Estado de la UPS	Continuidad

Nota. La matriz de OIDs y MIBs identifica las métricas críticas a recolectar mediante SNMP para los activos de red, seguridad y energía del sistema de monitoreo, permitiendo definir de forma estructurada los mecanismos de consulta (*polling*), notificación por eventos (*traps*) y la construcción de plantillas SNMPv3 orientadas a la operación y continuidad del *data center*.

Matriz Polling vs Trap

En la Tabla 88 se presenta La matriz Polling vs. Trap, la cual permite definir el mecanismo de recolección de métricas SNMP de acuerdo con su naturaleza y nivel de criticidad. El método Polling corresponde a consultas periódicas realizadas por el sistema de monitoreo hacia los dispositivos administrados para obtener métricas continuas relacionadas con rendimiento, capacidad y estabilidad, mientras que los Traps corresponden a notificaciones enviadas automáticamente por los dispositivos ante eventos predefinidos o condiciones críticas. Esta distinción permite combinar supervisión continua y notificación inmediata de incidentes, optimizando la eficiencia del monitoreo en la infraestructura tecnológica (B. Choi, 2024)

Tabla 88*Matriz Polling vs. Trap para la Recolección de Métricas SNMP*

Activo	Marca	Métrica	MIB	OID	Método	Justificación
Switch core	Ruijie Networks	Estado de interfaz	IF-MIB	1.3.6.1.2.1.2.2.1.8	Trap	Evento crítico que requiere notificación inmediata.
Switch core	Ruijie Networks	Bytes recibidos	IF-MIB	1.3.6.1.2.1.2.2.1.10	Polling	Métrica continua de rendimiento.
Switch core	Ruijie Networks	Bytes enviados	IF-MIB	1.3.6.1.2.1.2.2.1.16	Polling	Análisis de tráfico de red.
Switch core	Ruijie Networks	Uptime	SNMPv2-MIB	1.3.6.1.2.1.1.3	Polling	Control de estabilidad del dispositivo.
Switch core	Ruijie Networks	Estado físico	ENTITY-MIB	1.3.6.1.2.1.47.1.1.1.1.7	Trap	Detección de fallas de hardware.
Routers ISP	Cisco	Estado WAN	IF-MIB	1.3.6.1.2.1.2.2.1.8	Trap	Caída de enlace crítico hacia Internet.
Routers ISP	Cisco	Tráfico entrante	IF-MIB	1.3.6.1.2.1.2.2.1.10	Polling	Monitoreo del uso de capacidad.
Routers ISP	Cisco	Tráfico saliente	IF-MIB	1.3.6.1.2.1.2.2.1.16	Polling	Análisis de ancho de banda.
Routers ISP	Cisco	Uptime	SNMPv2-MIB	1.3.6.1.2.1.1.3	Polling	Detección de reinicios no programados.
Routers ISP	Cisco	Estado del hardware	ENTITY-MIB	1.3.6.1.2.1.47	Trap	Fallo físico del dispositivo.
UTM / Firewall	Sophos	Uso de CPU	HOST-RESOURCES-MIB	1.3.6.1.2.1.25.3.3.1.2	Polling	Métrica de rendimiento del sistema.
UTM / Firewall	Sophos	Uso de RAM	HOST-RESOURCES-MIB	1.3.6.1.2.1.25.2.3.1.6	Polling	Seguimiento de la capacidad del sistema.
UTM / Firewall	Sophos	Estado de interfaz	IF-MIB	1.3.6.1.2.1.2.2.1.8	Trap	Interrupción de la conectividad de red.

Activo	Marca	Métrica	MIB	OID	Método	Justificación
UTM / Firewall	Sophos	Uptime	SNMPv2-MIB	1.3.6.1.2.1.1.3	Polling	Verificación de continuidad del servicio.
UPS	Powest Titan 10 kVA	Carga de batería	UPS-MIB	1.3.6.1.2.1.33.1.2.1	Polling	Seguimiento de la autonomía energética.
UPS	Powest Titan 10 kVA	Estado de batería	UPS-MIB	1.3.6.1.2.1.33.1.2.4	Trap	Evento crítico relacionado con energía.
UPS	Powest Titan 10 kVA	Voltaje de salida	UPS-MIB	1.3.6.1.2.1.33.1.3.3.1.4	Polling	Control de la calidad eléctrica.
UPS	Powest Titan 10 kVA	Estado de la UPS	UPS-MIB	1.3.6.1.2.1.33.1.4.1	Trap	Fallo del sistema de respaldo eléctrico.

Nota. La matriz Polling vs. Trap permite definir de forma estructurada el método de recolección de métricas SNMP, optimizando el uso de recursos del sistema de monitoreo y asegurando la detección oportuna de eventos críticos que puedan afectar la disponibilidad, continuidad y estabilidad del data center.

Plantilla SNMPv3 Estándar

Con base en el diseño lógico de la plataforma de monitoreo, se realiza la plantilla SNMPv3 estándar para los activos que serán monitoreados mediante este protocolo, esta plantilla define la configuración de monitoreo segura y homogénea para los dispositivos de red, seguridad y energía de la infraestructura. Su objetivo es estandarizar la recolección de métricas mediante SNMPv3, especificando los OIDs, MIBs, el método de obtención (polling o trap) y los parámetros de seguridad asociados. Entre sus elementos más importantes se incluyen la versión SNMP, el nivel de seguridad authPriv, los mecanismos de autenticación y cifrado, y el usuario

SNMPv3, garantizando confidencialidad, integridad y coherencia con el diseño lógico del sistema de monitoreo.

En la Tabla 89 se presenta la plantilla SNMP estándar definida para el switch core, la cual consolida los parámetros técnicos necesarios para la implementación del monitoreo mediante SNMPv3. Esta plantilla sirve como referencia base para la configuración de métricas, métodos de recolección (polling o trap), niveles de seguridad y credenciales, garantizando una supervisión consistente, segura y alineada con la arquitectura de monitoreo del data center.

Tabla 89

Plantilla SNMP Estándar para el Switch Core

Tipo de activo: Red

Activo SWITCH CORE

Marca Ruijie Networks

Métrica	Estado de interfaz	Bytes recibidos	Bytes enviados	Uptime	Estado hardware
MIB	IF-MIB	IF-MIB	IF-MIB	SNMPv2-MIB	ENTITY-MIB
OID	1.3.6.1.2.1.2.2.1.8	1.3.6.1.2.1.2.2.1.10	1.3.6.1.2.1.2.2.1.16	1.3.6.1.2.1.1.3	1.3.6.1.2.1.47.1.1.1.7
Método	Trap	Polling	Polling	Polling	Trap
Versión SNMP	SNMPv3	SNMPv3	SNMPv3	SNMPv3	SNMPv3
Nivel de seguridad	authPriv	authPriv	authPriv	authPriv	authPriv
Autenticación	SHA	SHA	SHA	SHA	SHA
Cifrado	AES	AES	AES	AES	AES
Usuario SNMPv3	zbx_snmpv3	zbx_snmpv3	zbx_snmpv3	zbx_snmpv3	zbx_snmpv3

Nota. La plantilla SNMPv3 define los parámetros de monitoreo seguro para el Switch Core, estableciendo los OID, métodos de recolección (polling o trap) y mecanismos de autenticación y

cifrado utilizados por el sistema de monitoreo, garantizando la confidencialidad, integridad y disponibilidad de la información recolectada.

En la Tabla 90 se presenta la plantilla SNMP estándar definida para los routers del proveedor de servicios de Internet (ISP), la cual establece las métricas, MIBs, OIDs y parámetros de seguridad necesarios para el monitoreo de la disponibilidad, rendimiento y estado del hardware de los enlaces WAN del data center. Esta plantilla permite integrar los routers ISP al sistema de monitoreo integral mediante SNMPv3, garantizando la recolección segura y confiable de información crítica para la gestión de la conectividad externa.

Tabla 90

Plantilla SNMP Estándar para Routers ISP

Tipo de activo	Red				
Activo	ROUTERS ISP				
Marca	Cisco				
Métrica	Estado WAN	Tráfico entrante	Tráfico saliente	Uptime	Estado hardware
MIB	IF-MIB	IF-MIB	IF-MIB	SNMPv2-MIB	ENTITY-MIB
OID	1.3.6.1.2.1.2.2.1.8	1.3.6.1.2.1.2.2.1.10	1.3.6.1.2.1.2.2.1.16	1.3.6.1.2.1.1.3	1.3.6.1.2.1.47
Método (Polling / Trap)	Trap	Polling	Polling	Polling	Trap
Versión SNMP	SNMPv3	SNMPv3	SNMPv3	SNMPv3	SNMPv3
Nivel de seguridad	authPriv	authPriv	authPriv	authPriv	authPriv
Autenticación	SHA	SHA	SHA	SHA	SHA
Cifrado	AES	AES	AES	AES	AES

Métrica	Estado WAN	Tráfico entrante	Tráfico saliente	Uptime	Estado hardware
Usuario SNMPv3	zbx_snmpv3	zbx_snmpv3	zbx_snmpv3	zbx_snmpv3	zbx_snmpv3

Nota. La plantilla SNMPv3 para los routers ISP prioriza el uso de *traps* para eventos críticos como la caída de enlaces WAN o fallas de hardware, mientras que el *polling* se emplea para métricas continuas de rendimiento y estabilidad. El uso del nivel de seguridad *authPriv* con autenticación SHA y cifrado AES garantiza la confidencialidad, integridad y autenticidad de la información de monitoreo transmitida hacia el sistema Zabbix.

En la Tabla 91 se presenta la plantilla SNMP estándar definida para el dispositivo de seguridad perimetral UTM/Firewall, la cual establece las métricas, MIBs, OIDs y parámetros de seguridad utilizados para su monitoreo dentro del sistema de monitoreo integral. Esta plantilla permite asegurar la correcta supervisión del rendimiento, disponibilidad y estado operativo del firewall, garantizando visibilidad continua sobre los recursos críticos de seguridad del data center.

Tabla 91

Plantilla SNMP Estándar para el UTM/Firewall

Tipo de Activo	Seguridad			
Activo	UTM / FIREWALL			
Marca	Sophos			
Métrica	Uso CPU	Uso RAM	Estado interfaz	Uptime
MIB	HOST- RESOURCES-MIB	HOST- RESOURCES-MIB	IF-MIB	SNMPv2- MIB
OID	1.3.6.1.2.1.25.3.3.1.2	1.3.6.1.2.1.25.2.3.1.6	1.3.6.1.2.1.2.2.1.8	1.3.6.1.2.1.1.3
Método (Polling/Trap)	Polling	Polling	Trap	Polling

Métrica	Uso CPU	Uso RAM	Estado interfaz	Uptime
Versión SNMP	SNMPv3	SNMPv3	SNMPv3	SNMPv3
Nivel de seguridad	authPriv	authPriv	authPriv	authPriv
Autenticación	SHA	SHA	SHA	SHA
Cifrado	AES	AES	AES	AES
Usuario SNMPv3	zbx_snmpv3	zbx_snmpv3	zbx_snmpv3	zbx_snmpv3

Nota. La plantilla SNMP se define bajo el estándar SNMPv3 con nivel de seguridad *authPriv*, utilizando autenticación SHA y cifrado AES. Las métricas seleccionadas permiten monitorear el rendimiento (CPU y RAM), la disponibilidad de interfaces y la continuidad operativa del UTM/Firewall, asegurando una supervisión segura y confiable dentro del sistema de monitoreo del data center.

En la Tabla 92 se presenta la plantilla SNMP estándar definida para la UPS del data center, la cual establece las métricas críticas de energía a monitorear, junto con sus respectivos identificadores SNMP, métodos de recolección y parámetros de seguridad. Esta plantilla permite supervisar de forma continua el estado operativo y eléctrico del sistema de respaldo, garantizando la continuidad del servicio y una respuesta oportuna ante eventos críticos de energía.

Tabla 92

Plantilla SNMP Estándar para la UPS del Sistema de Monitoreo

Tipo de Activo	Energía
Activo	UPS
Marca	Powest Titan 10 kVA

Métrica	Carga batería	Estado batería	Voltaje salida	Estado UPS
MIB	UPS-MIB	UPS-MIB	UPS-MIB	UPS-MIB

Métrica	Carga batería	Estado batería	Voltaje salida	Estado UPS
OID	1.3.6.1.2.1.33.1.2.1	1.3.6.1.2.1.33.1.2.4	1.3.6.1.2.1.33.1.3.3.1.4	1.3.6.1.2.1.33.1.4.1
Método (Polling/Trap)	Polling	Trap	Polling	Trap
Versión SNMP	SNMPv3	SNMPv3	SNMPv3	SNMPv3
Nivel de seguridad	authPriv	authPriv	authPriv	authPriv
Autenticación	SHA	SHA	SHA	SHA
Cifrado	AES	AES	AES	AES
Usuario SNMPv3	zbx_snmpv3	zbx_snmpv3	zbx_snmpv3	zbx_snmpv3

Nota. La plantilla SNMP de la UPS prioriza el uso de **SNMPv3 con autenticación y cifrado**

para garantizar la seguridad de la información. Las métricas de carga y voltaje se recolectan mediante *polling* para análisis continuo, mientras que los eventos de estado de batería y de la UPS se gestionan mediante *traps*, permitiendo una notificación inmediata ante fallas críticas del sistema de respaldo energético.

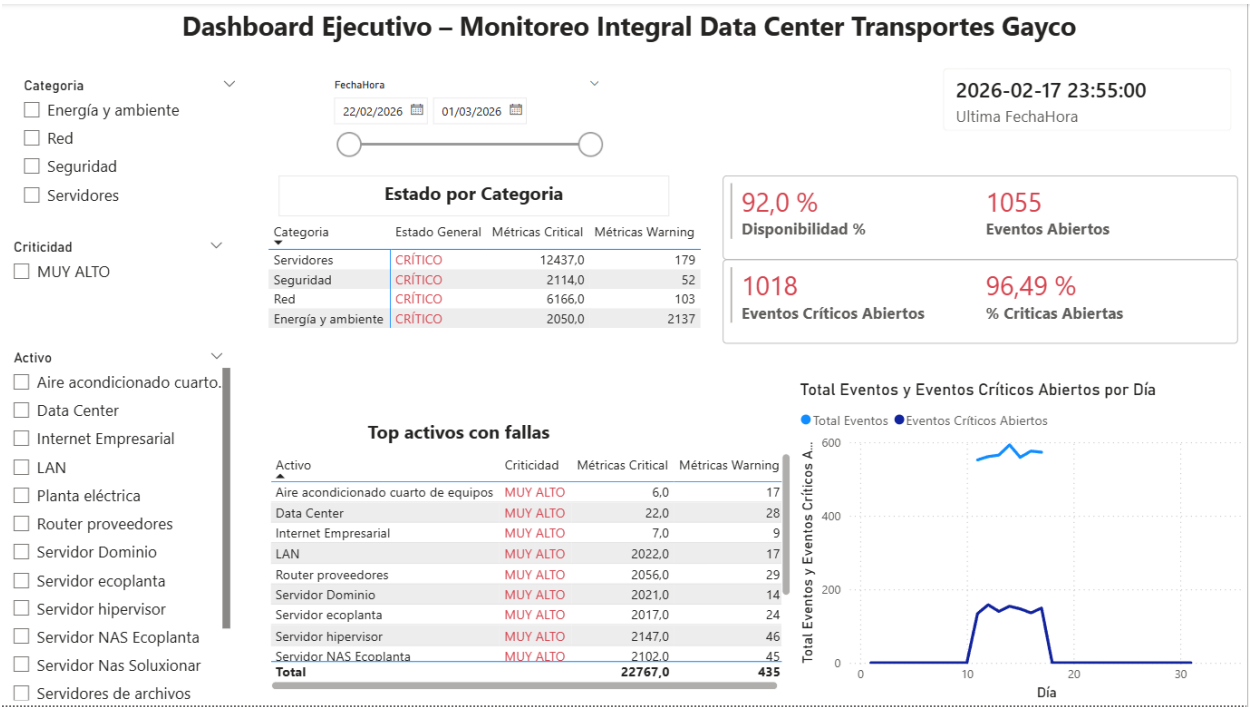
Propuesta de Visualización de Métricas de Monitoreo de Infraestructura TI

En el marco del desarrollo del cuarto objetivo del proyecto de investigación, se presenta el diseño de tableros de visualización orientados al monitoreo de la infraestructura tecnológica del cuarto de equipos de la empresa Transportes Gayco S.A.S. Estos dashboards fueron desarrollados con el propósito de representar de manera gráfica y comprensible las métricas de monitoreo previamente definidas, permitiendo integrar información relevante sobre el estado y comportamiento de los distintos componentes de la infraestructura TI. Mediante el uso de herramientas de visualización, como Power BI, se estructuran diferentes paneles que facilitan la interpretación de los indicadores clave, apoyando las actividades de supervisión, análisis y toma de decisiones relacionadas con la gestión operativa y preventiva del entorno tecnológico.

Diseño Dashboard Ejecutivo.

Figura 8

Dashboard Ejecutivo para el Monitoreo Integral del Data Center de Transportes Gayco S.A.S.



Nota. Dashboard ejecutivo de monitoreo integral del data center de transportes Gayco, fue desarrollado con el propósito de centralizar y visualizar de manera clara el estado operativo de los componentes críticos de la infraestructura tecnológica de la empresa Transportes Gayco S.A.S.

Este tablero integra información proveniente del sistema de monitoreo, permitiendo observar en tiempo real indicadores relacionados con servidores, red, seguridad y condiciones ambientales del cuarto de equipos.

En el panel se presentan métricas clave como el porcentaje de disponibilidad del sistema, la cantidad de eventos abiertos, el número de eventos críticos activos y el porcentaje de criticidad de las alertas detectadas, también incluye una visualización del estado general por categoría, donde se identifican las áreas que presentan condiciones críticas, así como una tabla con los activos que registran mayor cantidad de fallas o alertas, lo que facilita la priorización de acciones de mantenimiento o corrección.

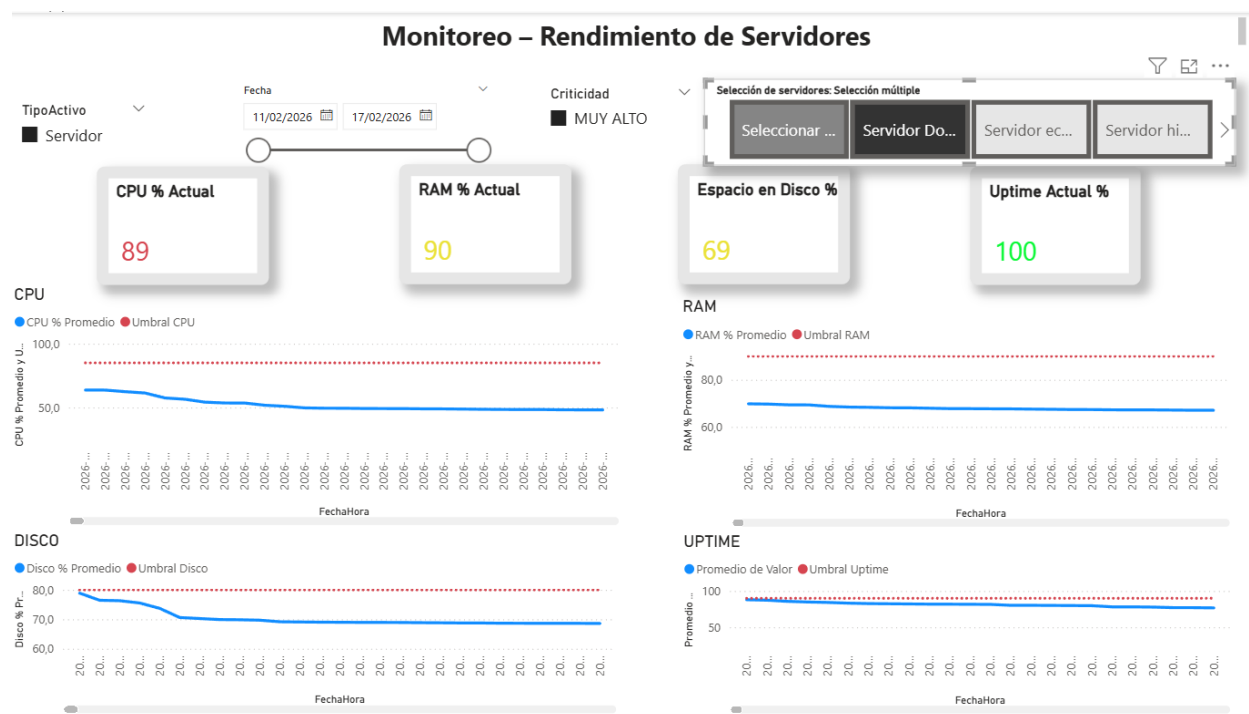
Se incorpora un gráfico temporal que muestra la evolución diaria de los eventos y eventos críticos abiertos, permitiendo identificar tendencias, picos de incidentes y posibles comportamientos anómalos en la infraestructura y por último, el tablero dispone de filtros interactivos por categoría, criticidad, activo y rango de fechas, lo que permite realizar análisis específicos sobre determinados componentes o periodos de tiempo.

Este dashboard funciona como una herramienta de apoyo para la supervisión operativa del data center, facilitando la detección temprana de incidentes, el seguimiento de la disponibilidad de los servicios y la toma de decisiones informadas para garantizar la continuidad y estabilidad de la infraestructura tecnológica en la empresa Transportes Gayco S.A.S.

Diseño Dashboard Rendimiento de Servidores

Figura 9

Dashboard de Monitoreo del Rendimiento de Servidores del Data Center de Transportes Gayco S.A.S.



Nota. Dashboard de Monitoreo – Rendimiento de Servidores, fue desarrollado con el propósito de visualizar el comportamiento y desempeño de los servidores que hacen parte de la infraestructura tecnológica del data center permitiendo supervisar indicadores clave del estado operativo de los equipos,

En la figura 9 se evidencia el análisis del consumo de recursos y la disponibilidad de los servicios, en el panel se presentan métricas principales como el uso actual de CPU, porcentaje de memoria RAM, utilización de espacio en disco y tiempo de disponibilidad (uptime) de los

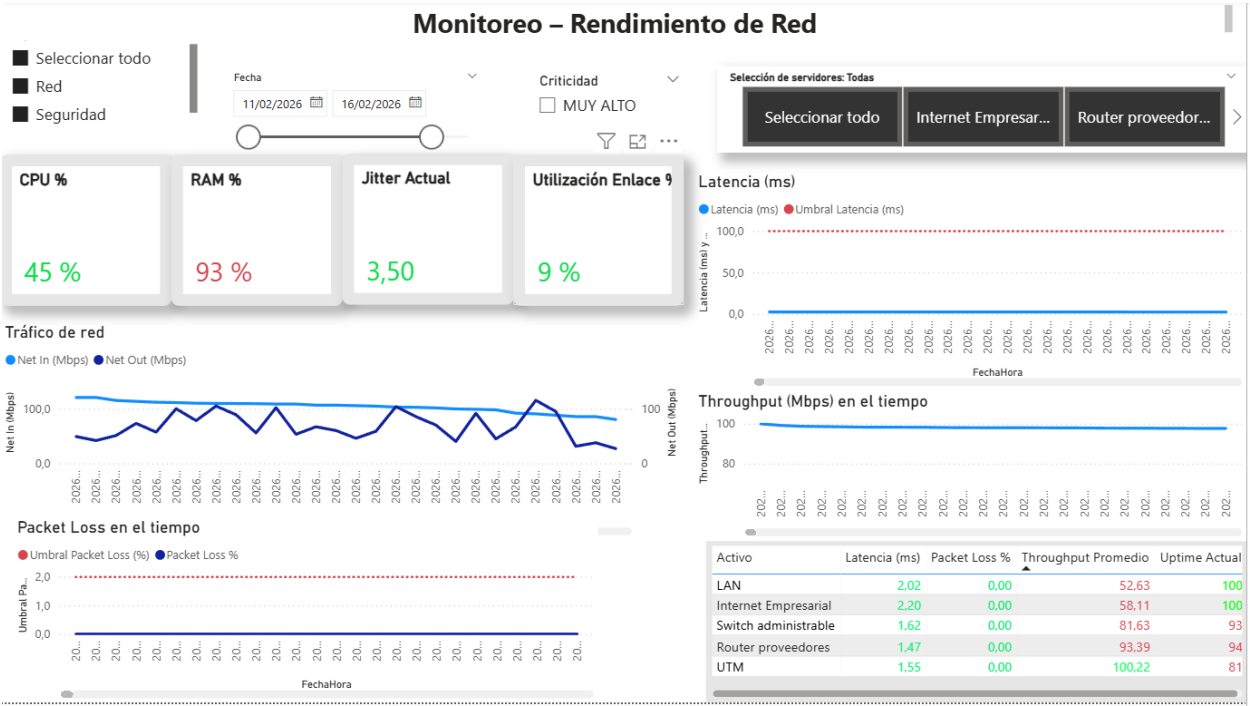
servidores. Además, se incluyen gráficos de tendencia que muestran la evolución de estos indicadores a lo largo del tiempo y permiten compararlos con umbrales definidos para identificar posibles situaciones de riesgo o sobrecarga.

Este dashboard incorpora filtros por fecha, criticidad y selección de servidores, lo que facilita analizar el rendimiento de equipos específicos, sirviendo como una herramienta de apoyo para el seguimiento del desempeño de los servidores, la detección temprana de problemas de capacidad y la toma de decisiones para la gestión y mantenimiento de la infraestructura TI orientada a los servidores de la organización.

Diseño Dashboard Rendimiento de Red

Figura 10

Dashboard de Monitoreo del Rendimiento de Red del Data Center de Transportes Gayco S.A.S



Nota. Este Dashboard fue desarrollado con el objetivo de supervisar el comportamiento y desempeño de los componentes de red que forman parte de la infraestructura tecnológica del data

center, permitiendo visualizar indicadores clave relacionados con la calidad y el rendimiento de la comunicación entre los dispositivos de la red.

El dashboard de Monitoreo – Rendimiento de Red (figura 10) fue desarrollado con el objetivo de supervisar el comportamiento y desempeño de los componentes de red que forman parte de la infraestructura tecnológica del data center, permitiendo visualizar indicadores clave relacionados con la calidad y el rendimiento de la comunicación entre los dispositivos de la red.

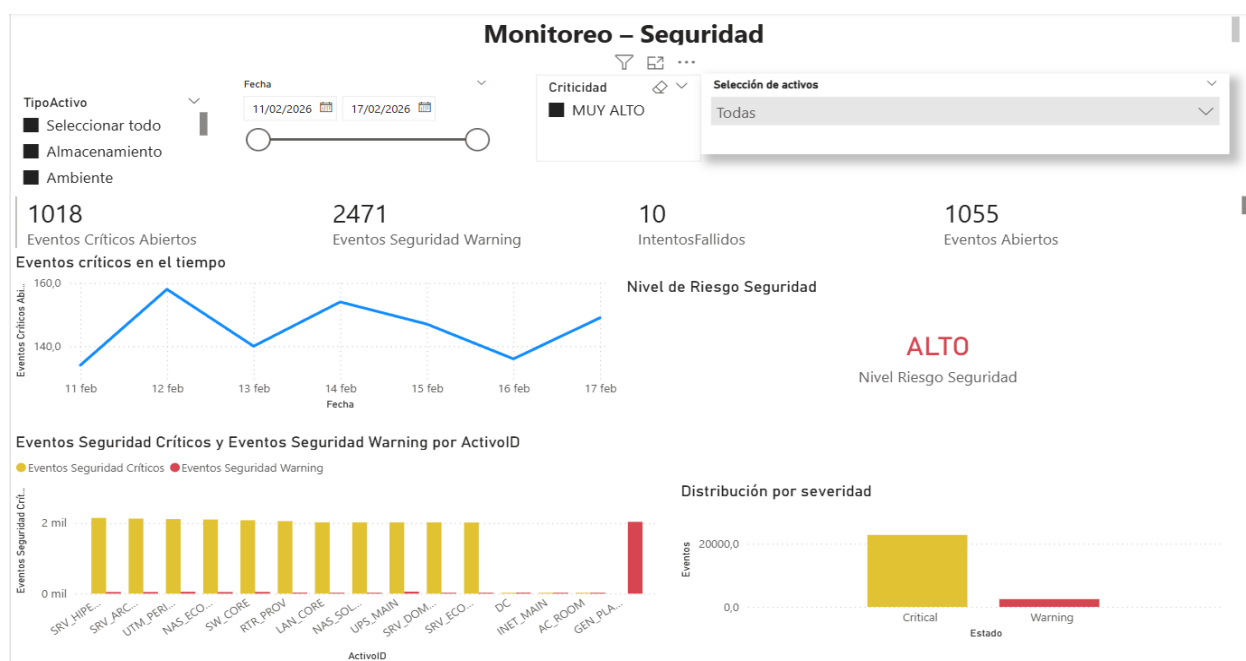
En el panel se presentan métricas principales como el uso de CPU, utilización de memoria, jitter, porcentaje de utilización del enlace y latencia, las cuales permiten evaluar el estado actual de la red y detectar posibles problemas de desempeño, incluyendo gráficos que muestran la evolución del tráfico de red, la latencia, el throughput y la pérdida de paquetes a lo largo del tiempo, facilitando la identificación de anomalías o variaciones en el comportamiento de la red.

El dashboard incorpora filtros por fecha, criticidad y selección de dispositivos de red, permitiendo realizar análisis específicos sobre componentes como routers, switches o enlaces de internet. De esta manera, este tablero sirve como una herramienta para el seguimiento del rendimiento de la red, la detección temprana de fallas y el apoyo en la toma de decisiones para la gestión y optimización de la conectividad de la infraestructura TI.

Diseño Dashboard Seguridad del Data Center

Figura 11

Dashboard de Monitoreo de Seguridad del Data Center de Transportes Gayco S.A.S.



Nota. Este dashboard fue desarrollado con el objetivo de visualizar y analizar los eventos relacionados con la seguridad de la infraestructura tecnológica del data center.

En la figura 11 se evidencia el dashboard de Monitoreo – Seguridad, este tablero permite supervisar las alertas generadas por los sistemas de monitoreo y detectar posibles incidentes que puedan afectar la disponibilidad, integridad o funcionamiento de los activos tecnológicos de la organización.

En el panel se presentan indicadores clave como la cantidad de eventos críticos abiertos, eventos de seguridad tipo warning, intentos fallidos y el total de eventos abiertos, los cuales permiten evaluar el estado general de la seguridad del entorno incluyendo un indicador del nivel

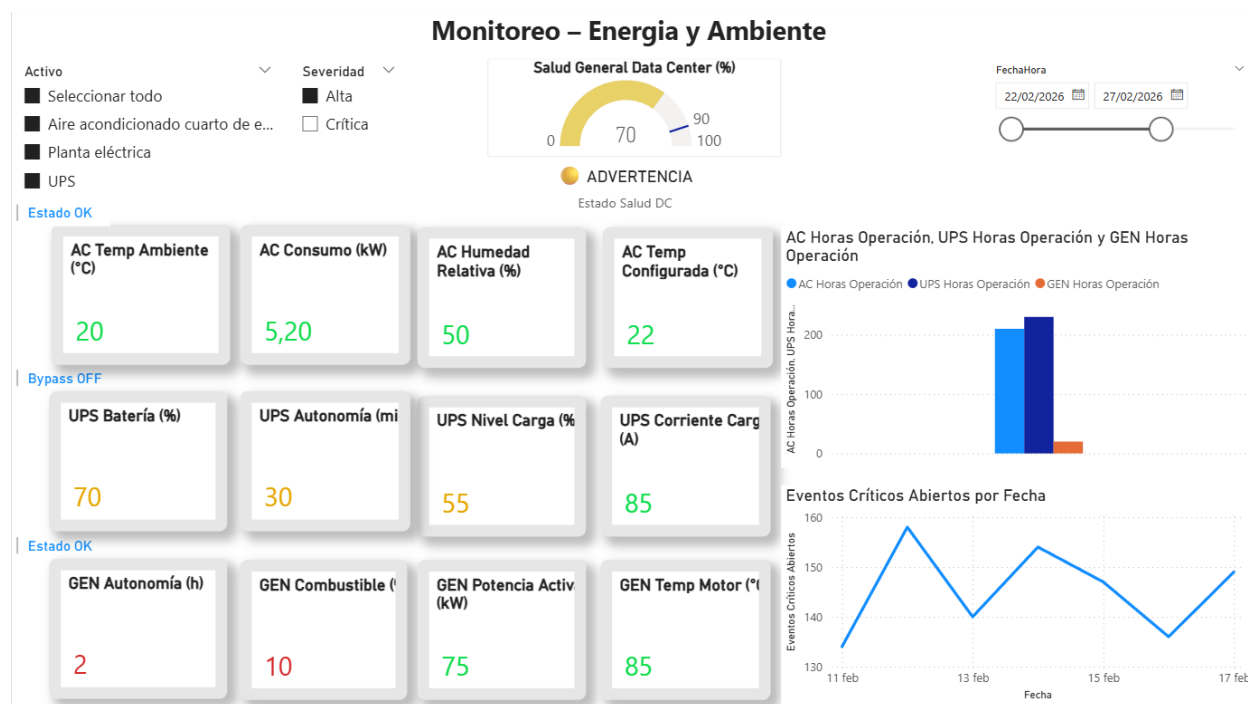
de riesgo de seguridad, que resume la condición actual del sistema de acuerdo con la severidad de las alertas detectadas.

Se incorporan gráficos que muestran la evolución de los eventos críticos en el tiempo, así como la distribución de eventos por activo y por nivel de severidad, lo que facilita identificar los componentes que presentan mayor cantidad de incidentes, sirviendo como una herramienta para el seguimiento de eventos de seguridad, la detección temprana de posibles amenazas y el apoyo en la toma de decisiones para fortalecer la protección de la infraestructura TI.

Diseño Dashboard Energía y Ambiente.

Figura 12

Dashboard de Monitoreo de Energía y Ambiente del Data Center de Transportes Gayco S.A.S.



Nota. Este dashboard fue desarrollado con el objetivo de supervisar las condiciones ambientales y el estado de los sistemas de energía que soportan la operación del data center

El dashboard de Monitoreo – Energía y Ambiente evidenciado en la figura 12, permite visualizar indicadores relacionados con el funcionamiento de equipos críticos como el aire acondicionado, la UPS y el generador eléctrico, los cuales son fundamentales para garantizar la continuidad del servicio.

En el panel se presentan métricas clave como temperatura ambiente, consumo energético del sistema de climatización, humedad relativa, estado de la batería de la UPS, autonomía, nivel de carga y parámetros operativos del generador, lo que permite evaluar el comportamiento de la infraestructura de soporte, incluyendo un indicador de salud general del data center, que resume el estado de los sistemas energéticos y ambientales.

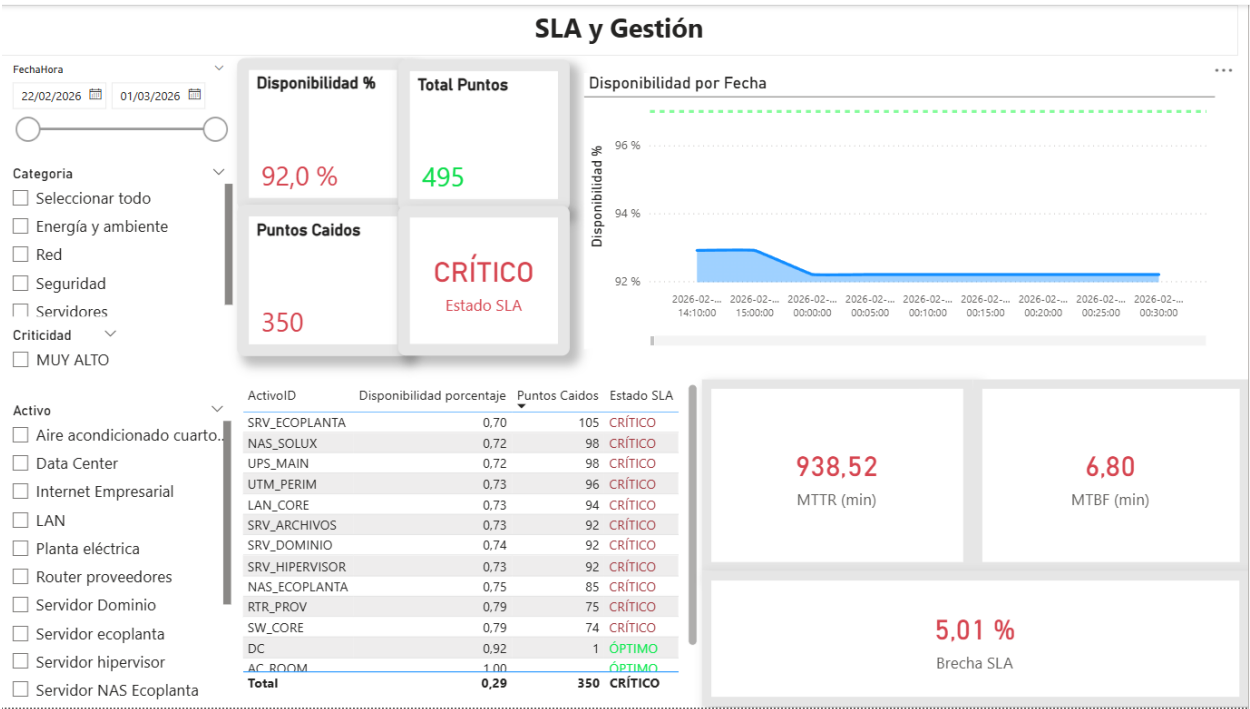
Por último, este dashboard incorpora gráficos que muestran las horas de operación de los equipos y la evolución de eventos críticos en el tiempo, permitiendo identificar posibles anomalías o condiciones que requieran intervención. De esta manera, este tablero sirve como una herramienta para el seguimiento de las condiciones ambientales y energéticas del cuarto de equipos, apoyando la detección temprana de fallas y la toma de decisiones para mantener la estabilidad de la infraestructura tecnológica de la empresa.

Diseño Dashboard SLA y Gestión de Disponibilidad.

Figura 13

SLA y Gestión de Disponibilidad del Sistema de Monitoreo del Data Center de Transportes

Gayco S.A.S.



Nota. Este dashboard fue desarrollado con el objetivo de evaluar el cumplimiento de los niveles de servicio (SLA) asociados a la infraestructura tecnológica del data center.

El dashboard de SLA y Gestión (figura 13) permite monitorear indicadores relacionados con la disponibilidad de los servicios y el impacto de las fallas en los diferentes activos tecnológicos.

En el panel se presentan métricas clave como el porcentaje de disponibilidad del sistema, el total de puntos monitoreados y la cantidad de puntos caídos y el estado general del SLA,

incluyendo un gráfico que muestra la evolución de la disponibilidad a lo largo del tiempo, permitiendo comparar el desempeño real con el nivel esperado de servicio.

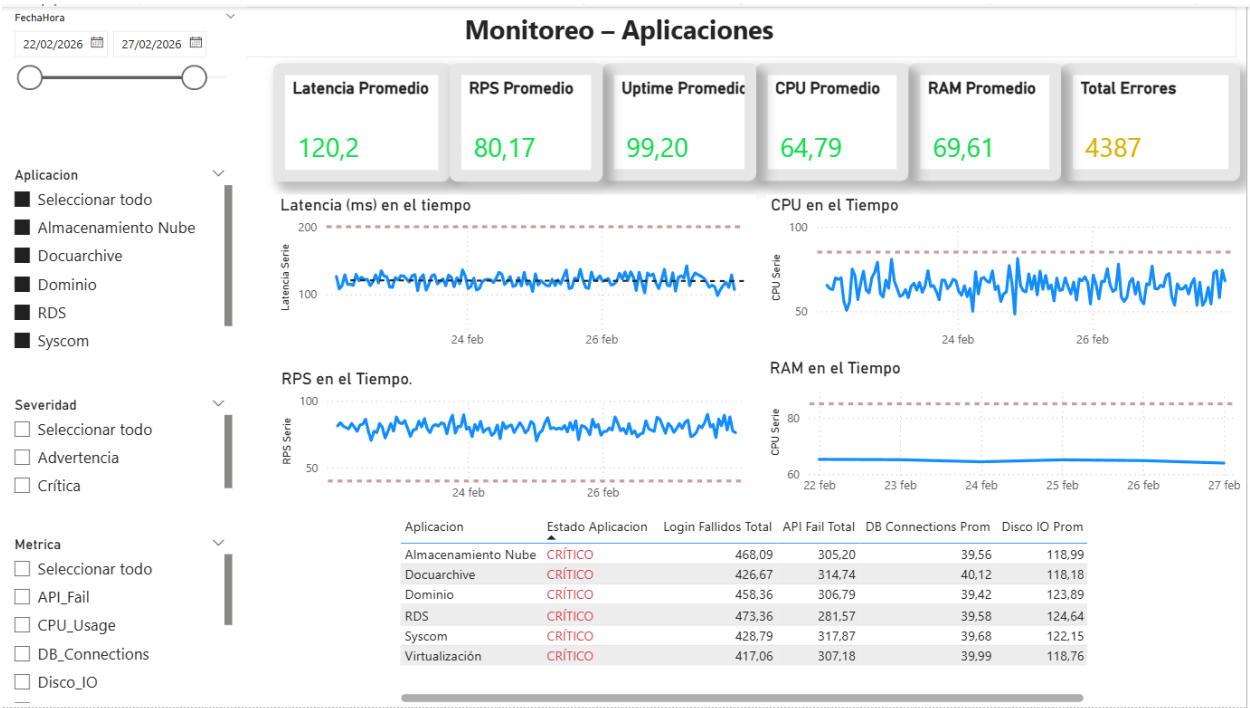
Este dashboard incorpora una tabla donde se visualiza el estado del SLA por cada activo monitoreado, identificando aquellos que presentan condiciones críticas, se presentan indicadores de gestión como el MTTR (tiempo medio de reparación), MTBF (tiempo medio entre fallas) y la brecha del SLA, los cuales facilitan el análisis del rendimiento operativo de la infraestructura.

Este tablero sirve como una herramienta para evaluar el cumplimiento de los acuerdos de nivel de servicio, identificar activos que afectan la disponibilidad y apoyar la toma de decisiones para mejorar la continuidad y confiabilidad de los servicios tecnológicos ofrecidos por el departamento de T.I de la organización.

Diseño Dashboard Monitoreo de Aplicaciones

Figura 14

Dashboard de Monitoreo de Aplicaciones del Data Center de Transportes Gayco S.A.S.



Nota. Este dashboard fue desarrollado con el objetivo de supervisar el desempeño y la disponibilidad de las aplicaciones que soportan los servicios tecnológicos del data center.

En la figura 14 se observa el dashboard de Monitoreo – Aplicaciones, el cual permite analizar el comportamiento de las aplicaciones y detectar posibles problemas que puedan afectar la operación de los sistemas.

En el panel se presentan indicadores clave como la latencia promedio, solicitudes por segundo (RPS), tiempo de disponibilidad (uptime), uso promedio de CPU y memoria RAM y el total de errores registrados, los cuales permiten evaluar el rendimiento general de las aplicaciones.

Además, se incluyen gráficos que muestran la evolución de la latencia, el consumo de CPU, el uso de memoria y el número de solicitudes en el tiempo, facilitando la identificación de variaciones o posibles degradaciones en el servicio.

Como último paso, este dashboard incorpora una tabla donde se visualiza el estado de cada aplicación monitoreada, junto con métricas relacionadas con intentos fallidos de acceso, fallos en la API, conexiones a la base de datos y operaciones de disco, sirviendo como una herramienta para el seguimiento del rendimiento de las aplicaciones, la detección temprana de errores y el apoyo en la gestión y mantenimiento de los servicios tecnológicos de la organización.

Impacto Esperado de la Estrategia de Monitoreo Integral

Antes de la propuesta de monitoreo integral, la empresa Transportes Gayco S.A.S. realizaba la supervisión de sus activos tecnológicos de manera fragmentada, utilizando diferentes herramientas independientes para servidores, redes y dispositivos auxiliares, mientras que algunos elementos críticos, como UPS, aire acondicionado y sistemas ambientales, no contaban

con algún tipo de monitoreo. Esta situación dificultaba la detección temprana de fallas, generando una gestión reactiva de incidentes, tiempos elevados de respuesta (MTTR), disminución en la disponibilidad de los servicios y riesgo de afectación a la continuidad operativa de la organización.

Con la estrategia propuesta, basada en una arquitectura centralizada de monitoreo apoyada en protocolos SNMP, Syslog y dashboards de visualización, se busca integrar en una única plataforma la supervisión de servidores, redes, dispositivos de seguridad, UPS, aire acondicionado, sensores ambientales y demás componentes del data center permitiendo así generar alertas automáticas en tiempo real, mejorar la capacidad de detección proactiva de incidentes y optimizar la toma de decisiones por parte del área de TI.

La implementación de la estrategia permitiría mejorar indicadores clave como el tiempo medio de reparación (MTTR), aumentar el tiempo medio entre fallas (MTBF) y fortalecer la disponibilidad de los activos críticos de la organización, permitiendo que la centralización de la información facilite el análisis de eventos, la correlación de fallas y el seguimiento del estado de la infraestructura tecnológica desde un enfoque preventivo y no únicamente correctivo.

La Tabla 93 a continuación presenta un análisis comparativo general entre el estado actual del monitoreo de infraestructura TI en la empresa Transportes Gayco S.A.S. y el escenario esperado después de la implementación de la estrategia de monitoreo integral propuesta, se evidencian mejoras relacionadas con la centralización del monitoreo, la automatización de alertas, la supervisión continua de los activos críticos y el fortalecimiento de la gestión proactiva de incidentes. Asimismo, la comparación permite identificar el impacto esperado de la estrategia sobre la disponibilidad de los servicios, la reducción en los tiempos de respuesta y la optimización de la toma de decisiones dentro del data center.

Tabla 93

Análisis Comparativo General del Estado del Monitoreo Antes y Después de la Implementación de la Estrategia Integral

Aspecto	Antes de la estrategia	Después de la estrategia
Monitoreo	Fragmentado	Centralizado
Gestión de incidentes	Reactiva	Proactiva
Alertas	Manuales o inexistentes	Automáticas en tiempo real
Visibilidad de infraestructura	Limitada	Integral
Monitoreo ambiental	Parcial	Continuo
Supervisión de UPS y energía	Ocasional	Permanente
Disponibilidad de servicios	Media	Alta
Tiempo de respuesta	Elevado	Reducido
Gestión de riesgos	Limitada	Basada en monitoreo continuo
Toma de decisiones	Correctiva	Preventiva

Nota. La tabla presenta una comparación general entre el estado actual del monitoreo de infraestructura TI en Transportes Gayco S.A.S. y el escenario esperado después de la implementación de la estrategia de monitoreo integral propuesta, evidenciando mejoras en centralización, disponibilidad, gestión proactiva y capacidad de respuesta ante incidentes.

Conclusiones

El análisis y evaluación de riesgos realizado mediante la metodología Magerit permitió identificar los activos críticos del data center de Transportes Gayco S.A.S., estableciendo de manera estructurada los componentes de infraestructura tecnológica susceptibles de monitoreo, incluyendo servidores, equipos de red, sistemas de energía y variables ambientales. Este proceso facilitó de manera estructurada priorizar los elementos más relevantes para la continuidad operativa de la organización y definir las métricas necesarias para su supervisión.

El análisis ROSI realizado evidencia que la implementación de la solución de monitoreo integral propuesta para Transportes Gayco S.A.S. resulta económicamente viable y justificable, debido a que la inversión estimada es significativamente inferior frente a las pérdidas potenciales asociadas a incidentes críticos en la infraestructura tecnológica, demostrando que el retorno obtenido permite la adopción de mecanismos de monitoreo proactivo contribuir a reducir el impacto operativo, mejorar la continuidad del negocio y fortalecer la disponibilidad de los servicios críticos de la organización.

El diseño de tableros de visualización desarrollados mediante la herramienta Power BI demostró la importancia de contar con aplicaciones de análisis que permitan centralizar y representar de forma clara las métricas del sistema de monitoreo integral, facilitando la interpretación del estado de la infraestructura TI, la detección temprana de incidentes y la toma de decisiones informadas para garantizar la disponibilidad, estabilidad y continuidad operativa del data center de la empresa Transportes Gayco S.A.S

Recomendaciones

Se recomienda a la empresa Transportes Gayco S.A.S. implementar progresivamente la estrategia de monitoreo propuesta, asegurando la correcta configuración de la plataforma Zabbix, la integración de los dispositivos mediante protocolos como SNMP y Modbus, y la definición de umbrales de alerta adecuados que permitan detectar de manera temprana fallas o comportamientos anómalos en los diferentes componentes de la infraestructura TI.

Se sugiere que, en futuros trabajos o fases de implementación, se incorporen técnicas de análisis predictivo y aprendizaje automático sobre los datos históricos recolectados por el sistema de monitoreo, con el propósito de anticipar posibles fallas en la infraestructura tecnológica y avanzar hacia un modelo de gestión más preventivo y basado en analítica de datos.

Se recomienda que la empresa Transportes Gayco S.A.S. fortalezca sus prácticas de gobernanza de tecnologías de la información, integrando la solución de monitoreo propuesta dentro de un marco de gestión alineado con buenas prácticas internacionales como COBIT, ISO 38500 e ITIL. Incorporando indicadores de desempeño y disponibilidad de los servicios TI para contribuir a mejorar la gestión de riesgos tecnológicos, la continuidad operativa y la alineación de los recursos tecnológicos con los objetivos estratégicos de la organización.

Referencias Bibliográficas

- ABB. (n.d.). *ABB AbilityTM Data Center Automation*. Retrieved September 21, 2025, from <https://new.abb.com/industrial-software/datacenter-automation>
- Abbasi, M., Shahraki, A., & Taherkordi, A. (2021). Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Survey. In *Computer Communications* (Vol. 170, pp. 19–41). Elsevier B.V. <https://doi.org/10.1016/j.comcom.2021.01.021>
- Abram, M. S. (2024). *Monitoreo de una infraestructura informática utilizando una estrategia guiada por medición y evaluación*.
- Abramov, A. G., & Porkhachev, V. A. (2022). Architecture and Key Components of the Improved Digital Center for Monitoring and Management of the National Research Computer Network of Russia. *Lobachevskii Journal of Mathematics*, 43(10), 2822–2832. <https://doi.org/10.1134/S1995080222130029>
- Al-Ashmoery, Y., Haider, H., Haider, A., Nasser, N., & Al-Sarem, M. (2021). Impact of IT Service Management and ITIL Framework on the Businesses. *International Conference of Modern Trends in ICT Industry: Towards the Excellence in the ICT Industries, MTICTI 2021*. <https://doi.org/10.1109/MTICTI53925.2021.9664763>
- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys and Tutorials*, 17(4), 2347–2376. <https://doi.org/10.1109/COMST.2015.2444095>
- Alhilali, A. H., Al Farawn, A., & Mjhool, A. Y. (2023). DESIGN AND IMPLEMENT A REAL-TIME NETWORK TRAFFIC MANAGEMENT SYSTEM USING SNMP

- PROTOCOL. *Eastern-European Journal of Enterprise Technologies*, 5(9(125)), 35–44. <https://doi.org/10.15587/1729-4061.2023.286528>
- Alsadhan, T., & Park, J. S. (2021). Leveraging Information Security Continuous Monitoring to Enhance Cybersecurity. *Proceedings - 2021 International Conference on Computational Science and Computational Intelligence, CSCI 2021*, 753–759. <https://doi.org/10.1109/CSCI54926.2021.00189>
- Andrés, C., Bermúdez, Ñ., Camilo, E., & Supelano, O. (2021). *Análisis de los riesgos y vulnerabilidades de un data center en Colombia para crear una matriz de riesgo acorde lo establecido en la norma ISO 27001: 2013*.
- Andrés Jiménez-Almeira, G., & López, D. E. (2023). *Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia*. <https://www.colcert.gov.co/800/w3-article-198657.html>
- Arman Kuzubasoglu, B. (2022). Recent Studies on the Humidity Sensor: A Mini Review. In *ACS Applied Electronic Materials* (Vol. 4, Number 10, pp. 4797–4807). American Chemical Society. <https://doi.org/10.1021/acsaelm.2c00721>
- Babel, W. (2022). Fieldbuses, Communication Protocols, User Interfaces, Hardware ASICs. In W. Babel (Ed.), *Industry 4.0, China 2025, IoT: The Hype Around the World of Automation* (pp. 149–329). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-37852-3_5
- Berk, M., Ay, I., Sari, S. S., Ayçiçek, Ö., Gonenc, S., & Tosun, S. (n.d.). *Telekomünikasyon Sistemleri İçin Çoklu Arızalarda Kaynak Tespit Yöntemi A Method for Source Detection in Multiple Faults for Telecommunication Systems*.

- Bezerra Jeronimo A. and Ibarra, J. E. and T. A. Q. and B. I. V. D. S. and C. V. and M. H. and L. M. and K. B. (2022). AmLight Real Time In-Band Telemetry Within the NoviFlow Switches. In K. Arai (Ed.), *Advances in Information and Communication* (pp. 644–655). Springer International Publishing.
- Burbank, J., & Kasch, W. (2010). *Network Time Protocol Version 4: Protocol and Algorithms Specification Abstract*. <http://www.rfc-editor.org/info/rfc5905>.
- Castaño Saldarriaga, J. D. (n.d.). *Sistema de Monitoreo para el Aseguramiento de la Calidad de la Red de Transmisión Óptica y los Aplicativos basados en Nube de los Servicios de TIGO-COLOMBIA ofrecidos a un Hospital de Tercer Nivel en Antioquia*.
- Cevallos Velásquez, O. A. Q. M. J. G. (2022). Evolución histórica de las normativas de diseño sismo resistente en América Latina. casos de estudio: Colombia, Ecuador, Perú y Chile. *Riobamba, Universidad Nacional de Chimborazo*.
- Chakian, & García. (2012). *Definición e implantación de un sistema de monitoreo y reporte de la seguridad lógica en un data center*.
- Chen, P. (2024). Data Acquisition System based on Serial Port. *Journal of Theory and Practice of Engineering Science*, 4(03), 87–98.
[https://doi.org/10.53469/jtpes.2024.04\(03\).09](https://doi.org/10.53469/jtpes.2024.04(03).09)
- Choi, B. (2024). Python Network Automation Labs: SNMP Discovery with Python. In B. Choi (Ed.), *Introduction to Python Network Automation Volume II: Stepping up: Beyond the Essentials for Success* (pp. 273–347). Apress.
https://doi.org/10.1007/979-8-8688-0391-8_5

- Choi, J., Narayanasamy, D., Ahn, B., Ahmad, S., Zeng, J., & Kim, T. (2021, June 28). A Real-Time Hardware-in-the-Loop (HIL) Cybersecurity Testbed for Power Electronics Devices and Systems in Cyber-Physical Environments. *Proceedings of the 2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems, PEDG 2021*.
<https://doi.org/10.1109/PEDG51384.2021.9494202>
- Choi, W. H., & Lewe, J. H. (2024). Advancing Fault Detection in Building Automation Systems through Deep Learning. *Buildings*, 14(1).
<https://doi.org/10.3390/buildings14010271>
- coordinación de contenidos, E., General de Modernización Administrativa, D., & Impulso de la Administración Electrónica, P. (2012). *Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*.
<http://administracionelectronica.gob.es/>
- Costa, B., Bachiega, J., Carvalho, L. R., Rosa, M., & Araujo, A. (2022). Monitoring fog computing: A review, taxonomy and open challenges. In *Computer Networks* (Vol. 215). Elsevier B.V. <https://doi.org/10.1016/j.comnet.2022.109189>
- D. Giannopoulos, P. P. C. T. and S. D. (2021). Monitoring as a Service over a 5G Network Slice. *Oint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*,.
- Dempsey, K., Pillitteri, V. Y., Baer, C., Niemeyer, R., Rudman, R., & Urban, S. (2020). *Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment*. <https://doi.org/10.6028/NIST.SP.800-137A>

DevOpsCube. (2023). *13 Best Open Source & Free Monitoring Tools in 2025*.

<https://devopscube.com/best-opensource-monitoring-tools/>

DevX Editorial Staff. (2024). *Microsoft System Center Operations Manager*.

<https://www.devx.com/terms/microsoft-system-center-operations-manager>

Dharshani, J., & Annamalai, S. (2023, November 23). Cloud based Effective Environmental Monitoring of Temperature, Humidity and Air Quality using IoT Sensors. *ACM International Conference Proceeding Series*.

<https://doi.org/10.1145/3647444.3647839>

Ekwonwune, E. N., & Enyinnaya, V. C. (2020). Design and Implementation of End to End Encrypted Short Message Service (SMS) Using Hybrid Cipher Algorithm. *Journal of Software Engineering and Applications*, 13(03), 25–40.

<https://doi.org/10.4236/jsea.2020.133003>

Enas Dhuhri Kusuma, T. F. A. , dan W. D. (2024). Implementasi Modbus TCP dalam Pengiriman Data Deteksi Objek ke PLC Schneider M221. *Journal of Applied Electrical Engineering*.

Faisal, M., Walter, T., & Montenegro, S. (2017). Power distribution unit (PDU) for a distributed computing network. *Conference of Open Innovation Association, FRUCT*. <https://doi.org/10.23919/FRUCT.2017.8250171>

Farah, E., & Shahrour, I. (2024). Water Leak Detection: A Comprehensive Review of Methods, Challenges, and Future Directions. In *Water (Switzerland)* (Vol. 16, Number 20). Multidisciplinary Digital Publishing Institute (MDPI).

<https://doi.org/10.3390/w16202975>

- Forti, S., Gaglianese, M., & Brogi, A. (2021). Lightweight self-organising distributed monitoring of Fog infrastructures. *Future Generation Computer Systems*, 114, 605–618. <https://doi.org/10.1016/j.future.2020.08.011>
- Fun, T. S., & Samsudin, A. (2021). Recent technologies, security countermeasure and ongoing challenges of industrial internet of things (IIoT): A survey. In *Sensors* (Vol. 21, Number 19). MDPI. <https://doi.org/10.3390/s21196647>
- Función Pública. (2012). *Ley 1581 de 2012*.
- García-Hernández, C. (2023). Monitoreo de servidores: una guía práctica. *Madrid, España: Anaya*.
- García-Hernández, C. , P.-M. J. , y G.-L. A. (2021). Elementos clave del monitoreo de aire acondicionado. *En XI Congreso Internacional de Comunicaciones y Tecnologías de La Información*.
- García-López, A. , G.-P. F. , & G.-G. J. (2023). Diseño e implementación de un sistema de monitoreo integral para datacenter. *Revista de Ingeniería Informática.*, 11–22.
- Gartner, Inc. (2022). *Top 10 Strategic Technology Trends for Data Centers in 2023*. 15.
- Gerhards R. (2009). *Network Working Group*. <http://trustee.ietf.org/license-info>
- Gómez-Rodríguez, J. R. , C.-S. E. F. A. , S.-A. R. , R.-A. V. I. , B. C. E. , L. G. , . . . & Á.-F. J. L. (2024). Evaluación de una herramienta para monitoreo de red, Teniendo énfasis en la verificación de conexión de equipo activo con protocolo ICMP. *Revista de Difusión Científica, Ingeniería y Tecnologías*, 15–23.
- González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, 21(14). <https://doi.org/10.3390/s21144759>

- Grafana Labs. (2023). *Grafana: The open observability platform*. <https://grafana.com>
- Grivin Mokodaser, W., Juan Mambu, J., Pop Koapaha, H., Lompoliu, E., Ilmu Komputer, F., Klabat, U., & Ekonomi dan Bisnis, F. (2024). Aligning IT Governance with Business Goals Using the COBIT 2019 Framework: A Case Study of an Innovation Consultancy Firm. *COGITO Smart Journal*, 10(2).
- Guo, D. (2022). Introduction of Data Center. In D. Guo (Ed.), *Data Center Networking: Network Topologies and Traffic Management in Large-Scale Data Centers* (pp. 3–24). Springer Nature Singapore. https://doi.org/10.1007/978-981-16-9368-7_1
- Hayes, T. (2018). The mega, modular data center is here and it's bigger than you thought. *Data Center Knowledge*.
- Howser, G. (2020). Simple Mail Transfer Protocol: Email. In *Computer Networks and the Internet* (pp. 385–417). Springer International Publishing. https://doi.org/10.1007/978-3-030-34496-2_22
- Icinga. (2023). *Icinga – Open Source & Scalable*. <https://icinga.com/solutions/network-monitoring/>
- Itaya, S., Ohori, F., Osuga, T., & Matsumura, T. (2023). Smart Monitoring of Wireless Environments with Real-Time Aggregation and Analysis. *Procedia Computer Science*, 220, 86–93. <https://doi.org/10.1016/j.procs.2023.03.014>
- Jaramillo, E. S. (n.d.). *El neutro en las instalaciones eléctricas de baja tensión: interrumpir y proteger*.
- Jayaweera, T. M., & Yu, H. Z. (2008). Scaling of fire cooling by water mist under low drop Reynolds number conditions. *Fire Safety Journal*, 43(1), 63–70. <https://doi.org/10.1016/J.FIRESAF.2007.01.004>

- Jin, C., Bai, X., Zhang, X., Xu, X., Tang, Y., & Zeng, C. (2022). A measurement-based power consumption model of a server by considering inlet air temperature. *Energy*, 261. <https://doi.org/10.1016/j.energy.2022.125126>
- Julian, M. (2017). *Practical Monitoring: Effective strategies for the real world*. O'Reilly Media, Inc.
- Kaganurmah, S., Cholli, N. G., & Anala, M. R. (2025). DLKS-MQTT: A Lightweight Key Sharing Protocol for Secure IoT Communications. *Engineering, Technology and Applied Science Research*, 15(2), 21532–21538. <https://doi.org/10.48084/etasr.10216>
- Katal, A., Dahiya, S., & Choudhury, T. (2023a). Energy efficiency in cloud computing data centers: a survey on software technologies. *Cluster Computing*, 26(3), 1845–1875. <https://doi.org/10.1007/s10586-022-03713-0>
- Katal, A., Dahiya, S., & Choudhury, T. (2023b). Energy efficiency in cloud computing data centers: a survey on software technologies. *Cluster Computing*, 26(3), 1845–1875. <https://doi.org/10.1007/s10586-022-03713-0>
- Khan, M. (2020). Small data centers: who needs them and why? *Network World*.
- Kirill Krinkin, Igor Kulikov, & Alexander Vodyaho. (2021). Architecture of Cloud Telecommunication Network Monitoring Platform Based on Knowledge Graphs. *IEEE International Conference on Communications*.
- Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability (Switzerland)*, 15(7). <https://doi.org/10.3390/su15075828>
- Knafllic, C. N. (2015). *Storytelling_with_Data*.

- Kulikov, I. and Z. S. and K. A. (2020). An Analytical Computing Infrastructure for Monitoring Dynamic Networks Based on Knowledge Graphs. *Springer*.
- La Republica. (2024). *Los ataques cibernéticos serán el principal riesgo global para las empresas en 2024*.
- Leclair, G. (2019). What is a medium data center? *Data Center Knowledge*.
- Ligus, S. (2013). *Effective_Monitoring_and_Alerting*.
- Liu, J., Gu, W., Chen, Z., Li, Y., Su, Y., & Lyu, M. R. (2024). *MTAD: Tools and Benchmarks for Multivariate Time Series Anomaly Detection*.
<http://arxiv.org/abs/2401.06175>
- Lonvick. C. (2006). *The Secure Shell (SSH) Protocol Architecture*.
- López, M. A., Rivera Fierro, D. G., Satizábal Echavarría, I. C., & Ortiz Sánchez, W. Y. (2024). Análisis comparativo de sensores de temperatura, humedad y luminosidad para su uso en sistemas de producción de lombricompost. *Entre Ciencia e Ingeniería*, 18(35), 32–40. <https://doi.org/10.31908/19098367.3045>
- Lopez Naranjo, J. A. , & S. G. E. R. (2021). *Gestor de eventos de seguridad para monitoreo de los servidores windows de la empresa mazars Colombia SAS*.
- Lowry, M. R., Lowry, P. B., Chatterjee, S., Moody, G. D., & Richardson, V. J. (2025). Achieving strategic alignment between business and information technology with information technology governance: the role of commitment to principles and Top Leadership Support. *European Journal of Information Systems*, 34(4), 610–635.
<https://doi.org/10.1080/0960085X.2024.2390998>

- Malek, D., Harun, A. N., Aliyah, F., & Ohshima, N. (2025). IoT and Sensor for Sustainable Buildings: Research Trends from 2019 to 2023. *Journal of Advanced Research Design*, 128(1), 144–162. <https://doi.org/10.37934/ard.128.1.144162>
- Marchionni, M. (2011). The role of material flow cost accounting in sustainable development. *Journal of Cleaner Production*.
- Mariño-García, J. F. (2020). *Propuesta de buenas prácticas de eventos a monitorear en un SIEM para cooperativas financieras en Colombia dando cumplimiento a la circular 007*.
- Maya Horowitz. (2024). *INTRODUCTION TO THE 2024 CYBER SECURITY REPORT*.
- McGrath, M. (2021). What is a large data center? *Data Center Knowledge*.
- Mejía, Á. D., Sierra, L. G., Molina, S. Z., Olaya, J. D. P., Durango, V. C., & Chaverra, M. C. (2022). Los heliostatos como alternativa energética en zonas tropicales colombianas. *Encuentro Internacional de Educación En Ingeniería*.
- Melnikov A. (2011). *RFC 6455 – The WebSocket Protocol*.
- Minea, M., Dumitrescu, C. M., & Minea, V. L. (2021). Intelligent network applications monitoring and diagnosis employing software sensing and machine learning solutions. *Sensors*, 21(15). <https://doi.org/10.3390/s21155036>
- Ministerio de Hacienda y Función Pública, G. de España. (2018). *MAGERIT v3: Método de análisis y gestión de riesgos de los sistemas de información*. 45–52.
- Misal, J. (n.d.). Automated monitoring systems in it infrastructure: a systematic analysis of detection, response, and optimization mechanisms. *Article ID: IJCET_15_06_091 International Journal of Computer Engineering and Technology*, 15(6), 1099. <https://doi.org/10.5281/zenodo.14287624>

- Moeyersons, J., Kerkhove, S., Wauters, T., De Turck, F., & Volckaert, B. (2022). Towards cloud-based unobtrusive monitoring in remote multi-vendor environments. *Software: Practice and Experience*, 52(2), 427–442.
<https://doi.org/https://doi.org/10.1002/spe.3029>
- Myrzatay, A. A. and R. L. G. (2020). Creation of Forecast Algorithm for Networking Hardware Malfunction in the context of small number of breakdowns. *International Journal of Engineering Research and Technology*.
- Nagano, M., Arai, Y., Fujihashi, T., Watanabe, T., & Saruwatari, S. (2021). Design and Implementation of Device Monitoring SaaS for DIY-IoT Systems. *Digest of Technical Papers - IEEE International Conference on Consumer Electronics, 2021-January*. <https://doi.org/10.1109/ICCE50685.2021.9427662>
- Nagios Enterprises. (2022). *Nagios Core*. <https://www.nagios.org>
- Omokere, O. K., Olubiwe, M., Olatomiwa, L. J., & Jack, K. E. (2023). Implementation of Smart Distribution Board for Domestic Energy Management and Regulatory System. *Electrica*, 23(3), 673–680. <https://doi.org/10.5152/electr.2023.22226>
- Opekunova L. A. and Opekunov, A. N. and K. I. N. and N. N. V. (2020). Modeling Enterprise Architecture Using Language ArchiMate. In M. and M. V. V. Ashmarina Svetlana Igorevna and Vochozka (Ed.), *Digital Age: Chances, Challenges and Future* (pp. 506–513). Springer International Publishing.
- Pacios, G. (2019). Data Centers Hoy. *Amazon*.
- Paessler AG. (n.d.). *PRTG Network Monitor*. Retrieved August 28, 2025, from <https://www.paessler.com/prtg>

- Paola A. Sánchez-Sánchez, J. R. G.-G. A. T. L. P.-C. (2021). Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. *Información Tecnológica*.
- Perdices, D., Garcia-Dorado, J. L., Ramos, J., De Pool, R., & Aracil, J. (2021). Towards the Automatic and Schedule-Aware Alerting of Internet Time Series. *IEEE Access*, 9, 61346–61358. <https://doi.org/10.1109/ACCESS.2021.3073598>
- Petrescu, I., Niculae, E., Vulturescu, V., Dimitrescu, A., & Ungureanu, L. M. (2025). Transport and Application Layer Protocols for IoT: Comprehensive Review. In *Technologies* (Vol. 13, Number 12). Multidisciplinary Digital Publishing Institute (MDPI). <https://doi.org/10.3390/technologies13120583>
- Presuhn, R. (2002). *Network Working Group*.
- Prometheus. (2023). *Prometheus - Monitoring system & time series database*. <https://prometheus.io/>
- Ramírez Fernández, E. R. (2023). Implementación de técnicas de observabilidad en el Centro de Monitoreo de la Red. *Cuadernos Técnicos Universitarios de La DGTIC*, 1(1). <https://doi.org/10.22201/dgtic.ctud.2023.1.1.17>
- Red Hat Documentation. (2025). *Monitoring and managing system status and performance*. *Red Hat Enterprise Linux 8*. Retrieved from Red Hat documentation.
- Rodas Mendoza, O. A. (2022). *Beneficio e impacto del monitoreo mediante el uso de telemetría en servidores web de alta demanda*.
- Rodríguez, G. D. L. C., Fernández, R. A. M., & Fernández, A. C. M. (2023). Seguridad de la información en el comercio electrónico basado en ISO 27001: Una revisión sistemática. *Innovación y software*. 4, 219–236.

- Roffia, P., & Dabić, M. (2024). The role of management control and integrated information systems for the resilience of SMEs. *Review of Managerial Science*, 18(5).
<https://doi.org/10.1007/s11846-023-00657-6>
- Rooted In Linux. (2024). *Enterprise Linux Labs Part 3: Monitoring and Optimization*.
Retrieved from Rooted in Linux blog.
- Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems* : <https://doi.org/10.6028/NIST.SP.800-160v2r1>
- Sahara, D. D., Sapri, A. :, & Akbar, S. (2024). The Design And Implementation Of Computer Network Monitoring And Security System Using Linux Ubuntu Server.
In *Jurnal Media Computer Science* (Vol. 3, Number 1). ARTICLE HISTORY.
- Savola, A. (2021). *Server virtualization with VMware*.
- Shvets, P. A., & Voevodin, V. V. (2021). ““Endless”” Workload Analysis of Large-Scale Supercomputers. *Lobachevskii Journal of Mathematics*, 42(1), 184–194.
<https://doi.org/10.1134/S1995080221010236>
- Sood, A. K. (2023). *Empirical Cloud Security: Practical Intelligence to Evaluate Risks and Attacks*.
- Suarez Valencia, P. (2025). Protección jurídica de los sistemas informáticos en Colombia: retos y necesidades de actualización de la Ley 1273 de 2009. (*Bachelor’s Thesis, Escuela de Derecho y Ciencias Políticas–Facultad de Derecho*).
- Trimetta Wintio, R., Widi Dionova, B., & Yusuf, A. (2025). *Validation of Pressure Transmitter Input/Output Loop Testing Based on Hybrid Analog and Digital HART Communication* (Vol. 21, Number 01). <https://jurnal.polines.ac.id/index.php/eksergi>

Uptime Institute. (2023). Five Data Center Predictions for 2023.

<https://Uptimeinstitute.Com/Resources/Research-and-Reports/Five-Data-Center-Predictions-for-2023>.

Usman, A., Zulkifli, N., Salim, M. R., Khairi, K., & Azmi, A. I. (2020). Optical link monitoring in fibre-to-the-x passive optical network (FTTx PON): A comprehensive survey. In *Optical Switching and Networking* (Vol. 39). Elsevier B.V.
<https://doi.org/10.1016/j.osn.2020.100596>

Wang, X., Liu, F., Feng, Y., & Zhao, J. (2021). A two-layer architecture for failure prediction based on high-dimension monitoring sequences. *Complexity*, 2021.
<https://doi.org/10.1155/2021/6623666>

Watanakesuntorn, W., Takahashi, K., Nakasan, C., Ichikawa, K., & Iida, H. (2022). Opimon: A Transparent, Low-Overhead Monitoring System for OpenFlow Networks. *IEICE Transactions on Communications*, E105B(4), 485–493.
<https://doi.org/10.1587/transcom.2021EBP3083>

Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.).

W.N.H. Ibrahim A.A. El-Sheikh M.A. El-Sherif M.A. El-Khodary M.A. Ibrahim M.S. Al-Sharawy. (2016). Recent Advances on Fog Computing: A Survey. *IEEE Communications Surveys & Tutorials*, 2535–2561.

Wu, H. Te. (2022). Establish a Digital Real-Time Learning System With Push Notifications. *Frontiers in Psychology*, 13.
<https://doi.org/10.3389/fpsyg.2022.767389>

Yin, J., Lang, X., Xu, H., & Duan, J. (2022). High-Performance Breaking and Intelligent of Miniature Circuit Breakers. *Sensors*, 22(16). <https://doi.org/10.3390/s22165990>

Zabbix LLC. (2023). *The enterprise-class open source observability solution*.

<https://www.zabbix.com/index>

Zanoni, M., Chiumeo, R., Tenti, L., & Volta, M. (2021). Automated tool based on deep learning to assess voltage dips validity: Integration in the QuEEN MV network monitoring system. *Renewable Energy and Power Quality Journal*, 19, 235–240.

<https://doi.org/10.24084/repqj19.265>

Zheng, C., Wang, L., McKee, S. A., Zhang, L., & Ye, H. (2019). *XOS: An Application-Defined Operating System for Data Center Servers*.

Apéndices

Apéndice A

Valoración Detallada de Amenazas de los Activos de Información de Transportes Gayco

TIPO DE ACTIVO	Cod. ACTIVO	DESCRIPCION	AMENZAS	FRECUENCIA	DEGRADACION	DAÑO/IMPACTO (VALOR)	DAÑO/IMPACTO CULAITATIVO
DATOS	[D]	Gestion Documental	5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
			5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO
			5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
			5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
			5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
			5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
			5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
			5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
			5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
			5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO
			5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
		Almacen	5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
			5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO

		5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
		5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
		5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
		5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
		5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
		5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
		5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO
		5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
	Compras	5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
		5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO
		5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
		5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
		5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
		5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
		5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
		5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
		5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO

	5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
Contabilidad	5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
	5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO
	5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
	5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
	5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
	5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
	5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
	5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
	5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO
	5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
Facturacion	5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
	5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO
	5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
	5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
	5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
	5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
	5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
	5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO

	5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO
	5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
Gerencia	5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
	5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO
	5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
	5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
	5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
	5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
	5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
	5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
	5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO
	5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
Gerencia 2021	5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
	5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO
	5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
	5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
	5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
	5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
	5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
	5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
	5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO

	5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
Gerencia Gayco	5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
	5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO
	5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
	5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
	5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
	5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
	5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
	5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
	5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO
	5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
Gestion Comercial	5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
	5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO
	5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
	5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
	5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
	5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
	5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
	5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
	5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO
	5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO

HSEQ	5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
	5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO
	5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
	5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
	5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
	5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
	5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
	5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
	5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO
	5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
Mantenimiento	5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
	5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO
	5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
	5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
	5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
	5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
	5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
	5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
	5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO
	5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
Operaciones	5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO

		5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO
		5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
		5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
		5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
		5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
		5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
		5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
		5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO
		5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
Proveedores 2022		5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
		5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO
		5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
		5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
		5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
		5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
		5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
		5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
		5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO
Seguridad Fisica		5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
		5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
		5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO

		5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
		5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
		5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
		5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
		5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
		5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
		5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO
		5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
	Sistema de Gestion	5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
		5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO
		5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
		5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
		5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
		5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
		5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
		5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
		5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO
		5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
	Talento Humano	5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
		5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO
		5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO

		5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
		5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
		5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
		5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
		5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
		5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO
		5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
	Tesoreria	5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
		5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO
		5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
		5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
		5.3.12. [E.19] Fugas de información	2	50%	3	BAJO
		5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
		5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
		5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
		5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO
		5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
	Vehiculos	5.3.1. [E.1] Errores de los usuarios	4	50%	5	MEDIO
		5.3.2. [E.2] Errores del administrador	1	50%	1	MUY BAJO
		5.3.10. [E.15] Alteración accidental de la información	2	50%	5	MEDIO
		5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
		5.3.12. [E.19] Fugas de información	2	50%	3	BAJO

			5.4.3. [A.5] Suplantación de la identidad del usuario	2	50%	3	BAJO
			5.4.4. [A.6] Abuso de privilegios de acceso	1	1%	3	MUY BAJO
			5.4.9. [A.11] Acceso no autorizado	1	100 %	5	ALTO
			5.4.13. [A.15] Modificación deliberada de la información	2	100 %	8	MUY ALTO
			5.4.14. [A.18] Destrucción de información	1	100 %	8	MUY ALTO
			5.4.15. [A.19] Divulgación de información	1	1%	1	MUY BAJO
CLAVES CRIPTOGRAFICAS	[K]	Bitlocker discos externos	5.3.1. [E.1] Errores de los usuarios	4	1%	5	BAJO
			5.3.2. [E.2] Errores del administrador	4	1%	5	BAJO
			5.3.10. [E.15] Alteración accidental de la información	4	50%	5	MEDIO
			5.3.11. [E.18] Destrucción de información	3	100 %	8	MUY ALTO
			5.3.12. [E.19] Fugas de información	4	1%	5	BAJO
			5.4.3. [A.5] Suplantación de la identidad del usuario	4	50%	5	MEDIO
			5.4.4. [A.6] Abuso de privilegios de acceso	3	50%	5	MEDIO
			5.4.9. [A.11] Acceso no autorizado	3	50%	5	MEDIO
			5.4.13. [A.15] Modificación deliberada de la información	3	50%	5	MEDIO
			5.4.14. [A.18] Destrucción de información	2	100 %	8	MUY ALTO
			5.4.15. [A.19] Divulgación de información	3	1%	5	BAJO
			HARDWARE	[HW]	Servidor ecoplanta	5.1.1. [N.1] Fuego	1
5.1.2. [N.2] Daños por agua	1	100 %				8	MUY ALTO
5.1.3. [N.*] Desastres naturales	1	100 %				8	MUY ALTO
5.2.1. [I.1] Fuego	1	100 %				8	MUY ALTO
5.2.2. [I.2] Daños por agua	1	100 %				8	MUY ALTO
5.2.3. [I.*] Desastres industriales	2	100 %				8	MUY ALTO
5.2.4. [I.3] Contaminación mecánica	3	50%				5	MEDIO

		5.2.5. [I.4] Contaminación electromagnética	3	50%	5	MEDIO
		5.2.6. [I.5] Avería de origen físico o lógico	3	50%	8	ALTO
		5.2.7. [I.6] Corte del suministro eléctrico	4	50%	8	ALTO
		5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	50%	8	ALTO
		5.2.12. [I.11] Emanaciones electromagnéticas	3	50%	5	MEDIO
		5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	50%	8	ALTO
		5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	50%	8	ALTO
		5.3.17. [E.25] Pérdida de equipos	1	100 %	8	MUY ALTO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	8	MEDIO
		5.4.5. [A.7] Uso no previsto	3	1%	8	MEDIO
		5.4.9. [A.11] Acceso no autorizado	3	1%	8	MEDIO
		5.4.17. [A.23] Manipulación de los equipos	3	50%	8	ALTO
		5.4.18. [A.24] Denegación de servicio	3	1%	8	MEDIO
		5.4.19. [A.25] Robo	1	100 %	8	MUY ALTO
		5.4.20. [A.26] Ataque destructivo	1	100 %	8	MUY ALTO
	Servidor hipervisor	5.1.1. [N.1] Fuego	1	100 %	8	MUY ALTO
		5.1.2. [N.2] Daños por agua	1	100 %	8	MUY ALTO
		5.1.3. [N.*] Desastres naturales	1	100 %	8	MUY ALTO
		5.2.1. [I.1] Fuego	1	100 %	8	MUY ALTO
		5.2.2. [I.2] Daños por agua	1	100 %	8	MUY ALTO
		5.2.3. [I.*] Desastres industriales	2	100 %	8	MUY ALTO
		5.2.4. [I.3] Contaminación mecánica	3	50%	5	MEDIO
		5.2.5. [I.4] Contaminación electromagnética	3	50%	5	MEDIO

		5.2.6. [I.5] Avería de origen físico o lógico	3	50%	8	ALTO
		5.2.7. [I.6] Corte del suministro eléctrico	4	50%	8	ALTO
		5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	50%	8	ALTO
		5.2.12. [I.11] Emanaciones electromagnéticas	3	50%	5	MEDIO
		5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	50%	8	ALTO
		5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	50%	8	ALTO
		5.3.17. [E.25] Pérdida de equipos	1	100 %	8	MUY ALTO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	8	MEDIO
		5.4.5. [A.7] Uso no previsto	3	1%	8	MEDIO
		5.4.9. [A.11] Acceso no autorizado	3	1%	8	MEDIO
		5.4.17. [A.23] Manipulación de los equipos	3	50%	8	ALTO
		5.4.18. [A.24] Denegación de servicio	3	1%	8	MEDIO
		5.4.19. [A.25] Robo	1	100 %	8	MUY ALTO
		5.4.20. [A.26] Ataque destructivo	1	100 %	8	MUY ALTO
	Servidor Dominio	5.1.1. [N.1] Fuego	1	100 %	8	MUY ALTO
		5.1.2. [N.2] Daños por agua	1	100 %	8	MUY ALTO
		5.1.3. [N.*] Desastres naturales	1	100 %	8	MUY ALTO
		5.2.1. [I.1] Fuego	1	100 %	8	MUY ALTO
		5.2.2. [I.2] Daños por agua	1	100 %	8	MUY ALTO
		5.2.3. [I.*] Desastres industriales	2	100 %	8	MUY ALTO
		5.2.4. [I.3] Contaminación mecánica	3	50%	5	MEDIO
		5.2.5. [I.4] Contaminación electromagnética	3	50%	5	MEDIO
		5.2.6. [I.5] Avería de origen físico o lógico	3	50%	8	ALTO

		5.2.7. [I.6] Corte del suministro eléctrico	4	50%	8	ALTO
		5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	50%	8	ALTO
		5.2.12. [I.11] Emanaciones electromagnéticas	3	50%	5	MEDIO
		5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	50%	8	ALTO
		5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	50%	8	ALTO
		5.3.17. [E.25] Pérdida de equipos	1	100 %	8	MUY ALTO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	8	MEDIO
		5.4.5. [A.7] Uso no previsto	3	1%	8	MEDIO
		5.4.9. [A.11] Acceso no autorizado	3	1%	8	MEDIO
		5.4.17. [A.23] Manipulación de los equipos	3	50%	8	ALTO
		5.4.18. [A.24] Denegación de servicio	3	1%	8	MEDIO
		5.4.19. [A.25] Robo	1	100 %	8	MUY ALTO
		5.4.20. [A.26] Ataque destructivo	1	100 %	8	MUY ALTO
	Servidores de archivos	5.1.1. [N.1] Fuego	1	100 %	8	MUY ALTO
		5.1.2. [N.2] Daños por agua	1	100 %	8	MUY ALTO
		5.1.3. [N.*] Desastres naturales	1	100 %	8	MUY ALTO
		5.2.1. [I.1] Fuego	1	100 %	8	MUY ALTO
		5.2.2. [I.2] Daños por agua	1	100 %	8	MUY ALTO
		5.2.3. [I.*] Desastres industriales	2	100 %	8	MUY ALTO
		5.2.4. [I.3] Contaminación mecánica	3	50%	5	MEDIO
		5.2.5. [I.4] Contaminación electromagnética	3	50%	5	MEDIO
		5.2.6. [I.5] Avería de origen físico o lógico	3	50%	8	ALTO
		5.2.7. [I.6] Corte del suministro eléctrico	4	50%	8	ALTO

		5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	50%	8	ALTO
		5.2.12. [I.11] Emanaciones electromagnéticas	3	50%	5	MEDIO
		5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	50%	8	ALTO
		5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	50%	8	ALTO
		5.3.17. [E.25] Pérdida de equipos	1	100 %	8	MUY ALTO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	8	MEDIO
		5.4.5. [A.7] Uso no previsto	3	1%	8	MEDIO
		5.4.9. [A.11] Acceso no autorizado	3	1%	8	MEDIO
		5.4.17. [A.23] Manipulación de los equipos	3	50%	8	ALTO
		5.4.18. [A.24] Denegación de servicio	3	1%	8	MEDIO
		5.4.19. [A.25] Robo	1	100 %	8	MUY ALTO
		5.4.20. [A.26] Ataque destructivo	1	100 %	8	MUY ALTO
	Servidor Solucionar	5.1.1. [N.1] Fuego	1	100 %	8	MUY ALTO
		5.1.2. [N.2] Daños por agua	1	100 %	8	MUY ALTO
		5.1.3. [N.*] Desastres naturales	1	100 %	8	MUY ALTO
		5.2.1. [I.1] Fuego	1	100 %	8	MUY ALTO
		5.2.2. [I.2] Daños por agua	1	100 %	8	MUY ALTO
		5.2.3. [I.*] Desastres industriales	2	100 %	8	MUY ALTO
		5.2.4. [I.3] Contaminación mecánica	3	50%	5	MEDIO
		5.2.5. [I.4] Contaminación electromagnética	3	50%	5	MEDIO
		5.2.6. [I.5] Avería de origen físico o lógico	3	50%	8	ALTO
		5.2.7. [I.6] Corte del suministro eléctrico	4	50%	8	ALTO
		5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	50%	8	ALTO

		5.2.12. [I.11] Emanaciones electromagnéticas	3	50%	5	MEDIO
		5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	50%	8	ALTO
		5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	50%	8	ALTO
		5.3.17. [E.25] Pérdida de equipos	1	100 %	8	MUY ALTO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	8	MEDIO
		5.4.5. [A.7] Uso no previsto	3	1%	8	MEDIO
		5.4.9. [A.11] Acceso no autorizado	3	1%	8	MEDIO
		5.4.17. [A.23] Manipulación de los equipos	3	50%	8	ALTO
		5.4.18. [A.24] Denegación de servicio	3	1%	8	MEDIO
		5.4.19. [A.25] Robo	1	100 %	8	MUY ALTO
		5.4.20. [A.26] Ataque destructivo	1	100 %	8	MUY ALTO
	Switch administrable	5.1.1. [N.1] Fuego	1	100 %	8	MUY ALTO
		5.1.2. [N.2] Daños por agua	1	100 %	8	MUY ALTO
		5.1.3. [N.*] Desastres naturales	1	100 %	8	MUY ALTO
		5.2.1. [I.1] Fuego	1	100 %	8	MUY ALTO
		5.2.2. [I.2] Daños por agua	1	100 %	8	MUY ALTO
		5.2.3. [I.*] Desastres industriales	2	100 %	8	MUY ALTO
		5.2.4. [I.3] Contaminación mecánica	3	50%	5	MEDIO
		5.2.5. [I.4] Contaminación electromagnética	3	50%	5	MEDIO
		5.2.6. [I.5] Avería de origen físico o lógico	3	50%	8	ALTO
		5.2.7. [I.6] Corte del suministro eléctrico	4	50%	8	ALTO
		5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	50%	8	ALTO
		5.2.12. [I.11] Emanaciones electromagnéticas	3	50%	5	MEDIO

		5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	50%	8	ALTO
		5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	50%	8	ALTO
		5.3.17. [E.25] Pérdida de equipos	1	100 %	8	MUY ALTO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	8	MEDIO
		5.4.5. [A.7] Uso no previsto	3	1%	8	MEDIO
		5.4.9. [A.11] Acceso no autorizado	3	1%	8	MEDIO
		5.4.17. [A.23] Manipulación de los equipos	3	50%	8	ALTO
		5.4.18. [A.24] Denegación de servicio	3	1%	8	MEDIO
		5.4.19. [A.25] Robo	1	100 %	8	MUY ALTO
		5.4.20. [A.26] Ataque destructivo	1	100 %	8	MUY ALTO
	Switch almacén	5.1.1. [N.1] Fuego	1	100 %	5	ALTO
		5.1.2. [N.2] Daños por agua	1	100 %	5	ALTO
		5.1.3. [N.*] Desastres naturales	1	100 %	5	ALTO
		5.2.1. [I.1] Fuego	1	100 %	5	ALTO
		5.2.2. [I.2] Daños por agua	1	100 %	5	ALTO
		5.2.3. [I.*] Desastres industriales	3	100 %	5	ALTO
		5.2.4. [I.3] Contaminación mecánica	4	50%	2	MUY BAJO
		5.2.5. [I.4] Contaminación electromagnética	3	50%	2	MUY BAJO
		5.2.6. [I.5] Avería de origen físico o lógico	3	50%	5	MEDIO
		5.2.7. [I.6] Corte del suministro eléctrico	4	50%	3	BAJO
		5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	4	50%	3	BAJO
		5.2.12. [I.11] Emanaciones electromagnéticas	3	50%	2	MUY BAJO

		5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	50%	3	BAJO
		5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	50%	5	MEDIO
		5.3.17. [E.25] Pérdida de equipos	1	100 %	5	ALTO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	2	MUY BAJO
		5.4.5. [A.7] Uso no previsto	3	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	3	1%	3	MUY BAJO
		5.4.17. [A.23] Manipulación de los equipos	3	50%	3	BAJO
		5.4.18. [A.24] Denegación de servicio	3	1%	5	BAJO
		5.4.19. [A.25] Robo	2	100 %	5	ALTO
		5.4.20. [A.26] Ataque destructivo	1	100 %	5	ALTO
	UTM	5.1.1. [N.1] Fuego	1	100 %	8	MUY ALTO
		5.1.2. [N.2] Daños por agua	1	100 %	8	MUY ALTO
		5.1.3. [N.*] Desastres naturales	1	100 %	8	MUY ALTO
		5.2.1. [I.1] Fuego	1	100 %	8	MUY ALTO
		5.2.2. [I.2] Daños por agua	1	100 %	8	MUY ALTO
		5.2.3. [I.*] Desastres industriales	2	100 %	8	MUY ALTO
		5.2.4. [I.3] Contaminación mecánica	3	50%	5	MEDIO
		5.2.5. [I.4] Contaminación electromagnética	3	50%	5	MEDIO
		5.2.6. [I.5] Avería de origen físico o lógico	3	50%	8	ALTO
		5.2.7. [I.6] Corte del suministro eléctrico	4	50%	8	ALTO
		5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	50%	8	ALTO
		5.2.12. [I.11] Emanaciones electromagnéticas	3	50%	5	MEDIO

		5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	50%	8	ALTO
		5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	50%	8	ALTO
		5.3.17. [E.25] Pérdida de equipos	1	100 %	8	MUY ALTO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	8	MEDIO
		5.4.5. [A.7] Uso no previsto	3	1%	8	MEDIO
		5.4.9. [A.11] Acceso no autorizado	3	1%	8	MEDIO
		5.4.17. [A.23] Manipulación de los equipos	3	50%	8	ALTO
		5.4.18. [A.24] Denegación de servicio	3	1%	8	MEDIO
		5.4.19. [A.25] Robo	1	100 %	8	MUY ALTO
		5.4.20. [A.26] Ataque destructivo	1	100 %	8	MUY ALTO
	Router proveedores	5.1.1. [N.1] Fuego	1	100 %	8	MUY ALTO
		5.1.2. [N.2] Daños por agua	1	100 %	8	MUY ALTO
		5.1.3. [N.*] Desastres naturales	1	100 %	8	MUY ALTO
		5.2.1. [I.1] Fuego	1	100 %	8	MUY ALTO
		5.2.2. [I.2] Daños por agua	1	100 %	8	MUY ALTO
		5.2.3. [I.*] Desastres industriales	2	100 %	8	MUY ALTO
		5.2.4. [I.3] Contaminación mecánica	3	50%	5	MEDIO
		5.2.5. [I.4] Contaminación electromagnética	3	50%	5	MEDIO
		5.2.6. [I.5] Avería de origen físico o lógico	3	50%	8	ALTO
		5.2.7. [I.6] Corte del suministro eléctrico	4	50%	8	ALTO
		5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	50%	8	ALTO
		5.2.12. [I.11] Emanaciones electromagnéticas	3	50%	5	MEDIO

		5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	50%	8	ALTO
		5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	50%	8	ALTO
		5.3.17. [E.25] Pérdida de equipos	1	100 %	8	MUY ALTO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	8	MEDIO
		5.4.5. [A.7] Uso no previsto	3	1%	8	MEDIO
		5.4.9. [A.11] Acceso no autorizado	3	1%	8	MEDIO
		5.4.17. [A.23] Manipulación de los equipos	3	50%	8	ALTO
		5.4.18. [A.24] Denegación de servicio	3	1%	8	MEDIO
		5.4.19. [A.25] Robo	1	100 %	8	MUY ALTO
		5.4.20. [A.26] Ataque destructivo	1	100 %	8	MUY ALTO
	Acces Point	5.1.1. [N.1] Fuego	1	100 %	5	ALTO
		5.1.2. [N.2] Daños por agua	1	100 %	5	ALTO
		5.1.3. [N.*] Desastres naturales	1	100 %	5	ALTO
		5.2.1. [I.1] Fuego	1	100 %	5	ALTO
		5.2.2. [I.2] Daños por agua	1	100 %	5	ALTO
		5.2.3. [I.*] Desastres industriales	2	100 %	5	ALTO
		5.2.4. [I.3] Contaminación mecánica	3	50%	2	MUY BAJO
		5.2.5. [I.4] Contaminación electromagnética	3	50%	5	MEDIO
		5.2.6. [I.5] Avería de origen físico o lógico	3	50%	5	MEDIO
		5.2.7. [I.6] Corte del suministro eléctrico	4	50%	3	BAJO
		5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	50%	3	BAJO
		5.2.12. [I.11] Emanaciones electromagnéticas	3	50%	5	MEDIO

		5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	50%	3	BAJO
		5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	50%	5	MEDIO
		5.3.17. [E.25] Pérdida de equipos	1	100 %	5	ALTO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	2	MUY BAJO
		5.4.5. [A.7] Uso no previsto	3	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	3	1%	3	MUY BAJO
		5.4.17. [A.23] Manipulación de los equipos	3	50%	3	BAJO
		5.4.18. [A.24] Denegación de servicio	3	1%	5	BAJO
		5.4.19. [A.25] Robo	1	100 %	5	ALTO
		5.4.20. [A.26] Ataque destructivo	1	100 %	5	ALTO
	Monitores	5.1.1. [N.1] Fuego	1	100 %	2	BAJO
		5.1.2. [N.2] Daños por agua	1	100 %	2	BAJO
		5.1.3. [N.*] Desastres naturales	1	100 %	2	BAJO
		5.2.1. [I.1] Fuego	1	100 %	2	BAJO
		5.2.2. [I.2] Daños por agua	1	100 %	2	BAJO
		5.2.3. [I.*] Desastres industriales	2	100 %	2	BAJO
		5.2.4. [I.3] Contaminación mecánica	3	50%	1	MUY BAJO
		5.2.5. [I.4] Contaminación electromagnética	3	50%	1	MUY BAJO
		5.2.6. [I.5] Avería de origen físico o lógico	3	50%	2	MUY BAJO
		5.2.7. [I.6] Corte del suministro eléctrico	4	50%	2	MUY BAJO
		5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	50%	1	MUY BAJO
		5.2.12. [I.11] Emanaciones electromagnéticas	3	50%	2	MUY BAJO

		5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	50%	1	MUY BAJO	
		5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	50%	1	MUY BAJO	
		5.3.17. [E.25] Pérdida de equipos	1	100 %	3	MEDIO	
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	1	MUY BAJO	
		5.4.5. [A.7] Uso no previsto	3	1%	2	MUY BAJO	
		5.4.9. [A.11] Acceso no autorizado	3	1%	3	MUY BAJO	
		5.4.17. [A.23] Manipulación de los equipos	3	50%	3	BAJO	
		5.4.18. [A.24] Denegación de servicio	3	1%	1	MUY BAJO	
		5.4.19. [A.25] Robo	1	100 %	3	MEDIO	
		5.4.20. [A.26] Ataque destructivo	1	100 %	3	MEDIO	
REDES DE COMUNICACIONES	[COM]	LAN	5.2.9. [I.8] Fallo de servicios de comunicaciones	3	50%	5	MEDIO
			5.3.2. [E.2] Errores del administrador	3	1%	3	MUY BAJO
			5.3.7. [E.9] Errores de [re-]encaminamiento	2	1%	3	MUY BAJO
			5.3.8. [E.10] Errores de secuencia	2	1%	3	MUY BAJO
			5.3.10. [E.15] Alteración accidental de la información	4	1%	3	MUY BAJO
			5.3.11. [E.18] Destrucción de información	3	50%	8	ALTO
			5.3.12. [E.19] Fugas de información	4	1%	5	BAJO
			5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	1%	8	MEDIO
			5.4.3. [A.5] Suplantación de la identidad del usuario	3	1%	5	BAJO
			5.4.4. [A.6] Abuso de privilegios de acceso	4	1%	5	BAJO
			5.4.5. [A.7] Uso no previsto	5	50%	5	MEDIO
			5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	1%	3	MUY BAJO
			5.4.8. [A.10] Alteración de secuencia	4	1%	3	MUY BAJO

			5.4.9. [A.11] Acceso no autorizado	3	1%	5	BAJO
			5.4.10. [A.12] Análisis de tráfico	3	1%	5	BAJO
			5.4.12. [A.14] Interceptación de información (escucha)	3	1%	5	BAJO
			5.4.13. [A.15] Modificación deliberada de la información	2	1%	8	MEDIO
			5.4.15. [A.19] Divulgación de información	3	1%	8	MEDIO
			5.4.18. [A.24] Denegación de servicio	3	1%	8	MEDIO
		Internet Empresarial Backup	5.2.9. [I.8] Fallo de servicios de comunicaciones	4	50%	8	ALTO
			5.3.2. [E.2] Errores del administrador	3	50%	5	MEDIO
			5.3.7. [E.9] Errores de [re-]encaminamiento	3	1%	5	BAJO
			5.3.8. [E.10] Errores de secuencia	3	1%	5	BAJO
			5.3.10. [E.15] Alteración accidental de la información	3	1%	5	BAJO
			5.3.11. [E.18] Destrucción de información	3	50%	5	MEDIO
			5.3.12. [E.19] Fugas de información	3	1%	8	MEDIO
			5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	50%	8	ALTO
			5.4.3. [A.5] Suplantación de la identidad del usuario	3	1%	8	MEDIO
			5.4.4. [A.6] Abuso de privilegios de acceso	2	1%	8	MEDIO
			5.4.5. [A.7] Uso no previsto	5	50%	8	ALTO
			5.4.7. [A.9] [Re-]encaminamiento de mensajes	4	1%	5	BAJO
			5.4.8. [A.10] Alteración de secuencia	3	1%	5	BAJO
			5.4.9. [A.11] Acceso no autorizado	3	1%	8	MEDIO
			5.4.10. [A.12] Análisis de tráfico	3	1%	5	BAJO
			5.4.12. [A.14] Interceptación de información (escucha)	3	50%	5	MEDIO
			5.4.13. [A.15] Modificación deliberada de la información	3	50%	8	ALTO
			5.4.15. [A.19] Divulgación de información	2	50%	8	ALTO
			5.4.18. [A.24] Denegación de servicio	3	50%	8	ALTO
		Internet Empresarial	5.2.9. [I.8] Fallo de servicios de comunicaciones	4	50%	8	ALTO
			5.3.2. [E.2] Errores del administrador	4	50%	5	MEDIO

		5.3.7. [E.9] Errores de [re- encaminamiento	4	1%	5	BAJO
		5.3.8. [E.10] Errores de secuencia	4	1%	5	BAJO
		5.3.10. [E.15] Alteración accidental de la información	4	1%	5	BAJO
		5.3.11. [E.18] Destrucción de información	3	50%	8	ALTO
		5.3.12. [E.19] Fugas de información	4	1%	5	BAJO
		5.3.16. [E.24] Caída del sistema por agotamiento de recursos	4	50%	8	ALTO
		5.4.3. [A.5] Suplantación de la identidad del usuario	4	1%	8	MEDIO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	5	BAJO
		5.4.5. [A.7] Uso no previsto	5	50%	5	MEDIO
		5.4.7. [A.9] [Re-]encaminamiento de mensajes	4	1%	5	BAJO
		5.4.8. [A.10] Alteración de secuencia	4	1%	5	BAJO
		5.4.9. [A.11] Acceso no autorizado	3	1%	8	MEDIO
		5.4.10. [A.12] Análisis de tráfico	3	1%	8	MEDIO
		5.4.12. [A.14] Interceptación de información (escucha)	3	50%	8	ALTO
		5.4.13. [A.15] Modificación deliberada de la información	3	50%	8	ALTO
		5.4.15. [A.19] Divulgación de información	3	50%	8	ALTO
		5.4.18. [A.24] Denegación de servicio	3	50%	8	ALTO
	Red Inalambrica	5.2.9. [I.8] Fallo de servicios de comunicaciones	4	50%	5	MEDIO
		5.3.2. [E.2] Errores del administrador	3	1%	3	MUY BAJO
		5.3.7. [E.9] Errores de [re- encaminamiento	3	1%	3	MUY BAJO
		5.3.8. [E.10] Errores de secuencia	3	1%	3	MUY BAJO
		5.3.10. [E.15] Alteración accidental de la información	4	1%	3	MUY BAJO
		5.3.11. [E.18] Destrucción de información	3	50%	8	ALTO
		5.3.12. [E.19] Fugas de información	4	1%	5	BAJO
		5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	1%	8	MEDIO

SOPORTES DE INFORMACIÓN	[MEDIA]	5.4.3. [A.5] Suplantación de la identidad del usuario	3	1%	5	BAJO
		5.4.4. [A.6] Abuso de privilegios de acceso	4	1%	5	BAJO
		5.4.5. [A.7] Uso no previsto	4	50%	5	MEDIO
		5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	1%	3	MUY BAJO
		5.4.8. [A.10] Alteración de secuencia	4	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	3	1%	5	BAJO
		5.4.10. [A.12] Análisis de tráfico	3	1%	5	BAJO
		5.4.12. [A.14] Interceptación de información (escucha)	3	1%	5	BAJO
		5.4.13. [A.15] Modificación deliberada de la información	2	1%	8	MEDIO
		5.4.15. [A.19] Divulgación de información	3	1%	8	MEDIO
		5.4.18. [A.24] Denegación de servicio	3	1%	8	MEDIO
	Disco Duro Externo	5.1.1. [N.1] Fuego	1	100 %	5	ALTO
		5.1.2. [N.2] Daños por agua	1	100 %	5	ALTO
		5.1.3. [N.*] Desastres naturales	1	100 %	5	ALTO
		5.2.1. [I.1] Fuego	1	100 %	5	ALTO
		5.2.2. [I.2] Daños por agua	1	100 %	5	ALTO
		5.2.3. [I.*] Desastres industriales	1	100 %	5	ALTO
		5.2.4. [I.3] Contaminación mecánica	3	50%	3	BAJO
		5.2.5. [I.4] Contaminación electromagnética	3	50%	3	BAJO
		5.2.6. [I.5] Avería de origen físico o lógico	3	50%	5	MEDIO
		5.2.7. [I.6] Corte del suministro eléctrico	4	1%	2	MUY BAJO
		5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	50%	2	MUY BAJO
		5.2.11. [I.10] Degradación de los soportes de almacenamiento de la información	3	100 %	5	ALTO

		5.2.12. [I.11] Emanaciones electromagnéticas	3	50%	3	BAJO
		5.3.1. [E.1] Errores de los usuarios	3	1%	3	MUY BAJO
		5.3.2. [E.2] Errores del administrador	3	1%	5	BAJO
		5.3.10. [E.15] Alteración accidental de la información	3	1%	5	BAJO
		5.3.11. [E.18] Destrucción de información	2	1%	5	BAJO
		5.3.12. [E.19] Fugas de información	3	1%	5	BAJO
		5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	50%	3	BAJO
		5.3.17. [E.25] Pérdida de equipos	3	100 %	5	ALTO
		5.4.5. [A.7] Uso no previsto	2	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	2	1%	3	MUY BAJO
		5.4.13. [A.15] Modificación deliberada de la información	2	1%	5	BAJO
		5.4.14. [A.18] Destrucción de información	2	1%	5	BAJO
		5.4.15. [A.19] Divulgación de información	2	1%	5	BAJO
		5.4.17. [A.23] Manipulación de los equipos	2	50%	3	BAJO
		5.4.19. [A.25] Robo	3	100 %	5	ALTO
		5.4.20. [A.26] Ataque destructivo	2	100 %	5	ALTO
	Servidor Nas Soluxionar	5.1.1. [N.1] Fuego	1	100 %	8	MUY ALTO
		5.1.2. [N.2] Daños por agua	1	100 %	8	MUY ALTO
		5.1.3. [N.*] Desastres naturales	1	100 %	8	MUY ALTO
		5.2.1. [I.1] Fuego	1	100 %	8	MUY ALTO
		5.2.2. [I.2] Daños por agua	1	100 %	8	MUY ALTO
		5.2.3. [I.*] Desastres industriales	1	100 %	8	MUY ALTO
		5.2.4. [I.3] Contaminación mecánica	3	50%	5	MEDIO

		5.2.5. [I.4] Contaminación electromagnética	3	50%	5	MEDIO
		5.2.6. [I.5] Avería de origen físico o lógico	3	50%	8	ALTO
		5.2.7. [I.6] Corte del suministro eléctrico	4	1%	5	BAJO
		5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	50%	3	BAJO
		5.2.11. [I.10] Degradación de los soportes de almacenamiento de la información	3	100 %	5	ALTO
		5.2.12. [I.11] Emanaciones electromagnéticas	3	50%	3	BAJO
		5.3.1. [E.1] Errores de los usuarios	5	1%	5	BAJO
		5.3.2. [E.2] Errores del administrador	4	1%	8	MEDIO
		5.3.10. [E.15] Alteración accidental de la información	4	1%	5	BAJO
		5.3.11. [E.18] Destrucción de información	2	1%	8	MEDIO
		5.3.12. [E.19] Fugas de información	4	1%	5	BAJO
		5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	50%	5	MEDIO
		5.3.17. [E.25] Pérdida de equipos	3	100 %	8	MUY ALTO
		5.4.5. [A.7] Uso no previsto	4	1%	5	BAJO
		5.4.9. [A.11] Acceso no autorizado	3	1%	5	BAJO
		5.4.13. [A.15] Modificación deliberada de la información	3	1%	8	MEDIO
		5.4.14. [A.18] Destrucción de información	2	1%	8	MEDIO
		5.4.15. [A.19] Divulgación de información	3	1%	8	MEDIO
		5.4.17. [A.23] Manipulación de los equipos	2	50%	5	MEDIO
		5.4.19. [A.25] Robo	2	100 %	8	MUY ALTO
		5.4.20. [A.26] Ataque destructivo	1	100 %	8	MUY ALTO
	Servidor NAS Ecoplanta	5.1.1. [N.1] Fuego	1	100 %	5	ALTO
		5.1.2. [N.2] Daños por agua	1	100 %	5	ALTO

		5.1.3. [N.*] Desastres naturales	1	100 %	5	ALTO
		5.2.1. [I.1] Fuego	1	100 %	5	ALTO
		5.2.2. [I.2] Daños por agua	1	100 %	5	ALTO
		5.2.3. [I.*] Desastres industriales	1	100 %	5	ALTO
		5.2.4. [I.3] Contaminación mecánica	3	50%	3	BAJO
		5.2.5. [I.4] Contaminación electromagnética	3	50%	3	BAJO
		5.2.6. [I.5] Avería de origen físico o lógico	3	50%	5	MEDIO
		5.2.7. [I.6] Corte del suministro eléctrico	4	1%	3	MUY BAJO
		5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	50%	3	BAJO
		5.2.11. [I.10] Degradación de los soportes de almacenamiento de la información	3	100 %	3	MEDIO
		5.2.12. [I.11] Emanaciones electromagnéticas	3	50%	3	BAJO
		5.3.1. [E.1] Errores de los usuarios	5	1%	3	MUY BAJO
		5.3.2. [E.2] Errores del administrador	4	1%	5	BAJO
		5.3.10. [E.15] Alteración accidental de la información	4	1%	3	MUY BAJO
		5.3.11. [E.18] Destrucción de información	2	1%	5	BAJO
		5.3.12. [E.19] Fugas de información	4	1%	3	MUY BAJO
		5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	50%	5	MEDIO
		5.3.17. [E.25] Pérdida de equipos	3	100 %	3	MEDIO
		5.4.5. [A.7] Uso no previsto	4	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	3	1%	3	MUY BAJO
		5.4.13. [A.15] Modificación deliberada de la información	3	1%	5	BAJO
		5.4.14. [A.18] Destrucción de información	2	1%	5	BAJO

SOFTWARE		5.4.15. [A.19] Divulgación de información	3	1%	5	BAJO
		5.4.17. [A.23] Manipulación de los equipos	2	50%	3	BAJO
		5.4.19. [A.25] Robo	2	100%	5	ALTO
		5.4.20. [A.26] Ataque destructivo	1	100%	5	ALTO
	Syscom	5.2.6. [I.5] Avería de origen físico o lógico	3	50%	8	ALTO
		5.3.1. [E.1] Errores de los usuarios	5	1%	5	BAJO
		5.3.2. [E.2] Errores del administrador	3	50%	8	ALTO
		5.3.6. [E.8] Difusión de software dañino	2	50%	8	ALTO
		5.3.7. [E.9] Errores de [re-]encaminamiento	2	1%	8	MEDIO
		5.3.8. [E.10] Errores de secuencia	2	1%	8	MEDIO
		5.3.10. [E.15] Alteración accidental de la información	4	1%	8	MEDIO
		5.3.11. [E.18] Destrucción de información	2	100%	8	MUY ALTO
		5.3.12. [E.19] Fugas de información	3	1%	5	BAJO
		5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	50%	8	ALTO
		5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	50%	8	ALTO
		5.4.3. [A.5] Suplantación de la identidad del usuario	3	1%	8	MEDIO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	8	MEDIO
		5.4.5. [A.7] Uso no previsto	3	1%	8	MEDIO
		5.4.6. [A.8] Difusión de software dañino	2	100%	8	MUY ALTO
		5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	1%	5	BAJO
		5.4.8. [A.10] Alteración de secuencia	3	1%	8	MEDIO
		5.4.9. [A.11] Acceso no autorizado	3	1%	8	MEDIO
		5.4.13. [A.15] Modificación deliberada de la información	2	1%	8	MEDIO
		5.4.14. [A.18] Destrucción de información	2	50%	8	ALTO
		5.4.15. [A.19] Divulgación de información	2	1%	5	BAJO

		5.4.16. [A.22] Manipulación de programas	2	50%	8	ALTO
	Docuarchive	5.2.6. [I.5] Avería de origen físico o lógico	3	50%	8	ALTO
		5.3.1. [E.1] Errores de los usuarios	5	1%	5	BAJO
		5.3.2. [E.2] Errores del administrador	3	50%	8	ALTO
		5.3.6. [E.8] Difusión de software dañino	2	50%	8	ALTO
		5.3.7. [E.9] Errores de [re-]encaminamiento	2	1%	8	MEDIO
		5.3.8. [E.10] Errores de secuencia	2	1%	8	MEDIO
		5.3.10. [E.15] Alteración accidental de la información	4	1%	8	MEDIO
		5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
		5.3.12. [E.19] Fugas de información	3	1%	5	BAJO
		5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	50%	8	ALTO
		5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	50%	8	ALTO
		5.4.3. [A.5] Suplantación de la identidad del usuario	3	1%	8	MEDIO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	8	MEDIO
		5.4.5. [A.7] Uso no previsto	3	1%	8	MEDIO
		5.4.6. [A.8] Difusión de software dañino	2	100 %	8	MUY ALTO
		5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	1%	5	BAJO
		5.4.8. [A.10] Alteración de secuencia	3	1%	8	MEDIO
		5.4.9. [A.11] Acceso no autorizado	3	1%	8	MEDIO
		5.4.13. [A.15] Modificación deliberada de la información	2	1%	8	MEDIO
		5.4.14. [A.18] Destrucción de información	2	50%	8	ALTO
		5.4.15. [A.19] Divulgación de información	2	1%	5	BAJO
		5.4.16. [A.22] Manipulación de programas	2	50%	8	ALTO
	Plataforma OCS Inventory	5.2.6. [I.5] Avería de origen físico o lógico	3	50%	5	MEDIO
		5.3.1. [E.1] Errores de los usuarios	5	1%	2	MUY BAJO

		5.3.2. [E.2] Errores del administrador	3	50%	5	MEDIO
		5.3.6. [E.8] Difusión de software dañino	2	50%	5	MEDIO
		5.3.7. [E.9] Errores de [re-]encaminamiento	2	1%	5	BAJO
		5.3.8. [E.10] Errores de secuencia	2	1%	3	MUY BAJO
		5.3.10. [E.15] Alteración accidental de la información	4	1%	5	BAJO
		5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
		5.3.12. [E.19] Fugas de información	3	1%	5	BAJO
		5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	50%	3	BAJO
		5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	50%	5	MEDIO
		5.4.3. [A.5] Suplantación de la identidad del usuario	3	1%	5	BAJO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	5	BAJO
		5.4.5. [A.7] Uso no previsto	3	1%	3	MUY BAJO
		5.4.6. [A.8] Difusión de software dañino	2	100 %	5	ALTO
		5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	1%	5	BAJO
		5.4.8. [A.10] Alteración de secuencia	3	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	3	1%	5	BAJO
		5.4.13. [A.15] Modificación deliberada de la información	2	1%	5	BAJO
		5.4.14. [A.18] Destrucción de información	2	50%	8	ALTO
		5.4.15. [A.19] Divulgación de información	2	1%	5	BAJO
		5.4.16. [A.22] Manipulación de programas	2	50%	5	MEDIO
	Plataforma GLPI	5.2.6. [I.5] Avería de origen físico o lógico	3	50%	3	BAJO
		5.3.1. [E.1] Errores de los usuarios	5	1%	2	MUY BAJO
		5.3.2. [E.2] Errores del administrador	3	50%	3	BAJO

		5.3.6. [E.8] Difusión de software dañino	2	50%	3	BAJO
		5.3.7. [E.9] Errores de [re-]encaminamiento	2	1%	3	MUY BAJO
		5.3.8. [E.10] Errores de secuencia	2	1%	3	MUY BAJO
		5.3.10. [E.15] Alteración accidental de la información	4	1%	3	MUY BAJO
		5.3.11. [E.18] Destrucción de información	2	100 %	5	ALTO
		5.3.12. [E.19] Fugas de información	3	1%	3	MUY BAJO
		5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	50%	3	BAJO
		5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	50%	3	BAJO
		5.4.3. [A.5] Suplantación de la identidad del usuario	3	1%	3	MUY BAJO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	3	MUY BAJO
		5.4.5. [A.7] Uso no previsto	3	1%	3	MUY BAJO
		5.4.6. [A.8] Difusión de software dañino	2	100 %	3	MEDIO
		5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	1%	3	MUY BAJO
		5.4.8. [A.10] Alteración de secuencia	3	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	3	1%	3	MUY BAJO
		5.4.13. [A.15] Modificación deliberada de la información	2	1%	3	MUY BAJO
		5.4.14. [A.18] Destrucción de información	2	50%	5	MEDIO
		5.4.15. [A.19] Divulgación de información	2	1%	3	MUY BAJO
		5.4.16. [A.22] Manipulación de programas	2	50%	3	BAJO
	VPN Sophos	5.2.6. [I.5] Avería de origen físico o lógico	3	50%	5	MEDIO
		5.3.1. [E.1] Errores de los usuarios	5	1%	2	MUY BAJO
		5.3.2. [E.2] Errores del administrador	3	50%	5	MEDIO

		5.3.6. [E.8] Difusión de software dañino	2	50%	5	MEDIO
		5.3.7. [E.9] Errores de [re-]encaminamiento	2	1%	5	BAJO
		5.3.8. [E.10] Errores de secuencia	2	1%	3	MUY BAJO
		5.3.10. [E.15] Alteración accidental de la información	4	1%	5	BAJO
		5.3.11. [E.18] Destrucción de información	2	100 %	8	MUY ALTO
		5.3.12. [E.19] Fugas de información	3	1%	5	BAJO
		5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	50%	3	BAJO
		5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	50%	5	MEDIO
		5.4.3. [A.5] Suplantación de la identidad del usuario	3	1%	5	BAJO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	1%	5	BAJO
		5.4.5. [A.7] Uso no previsto	3	1%	3	MUY BAJO
		5.4.6. [A.8] Difusión de software dañino	2	100 %	5	ALTO
		5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	1%	5	BAJO
		5.4.8. [A.10] Alteración de secuencia	3	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	3	1%	5	BAJO
		5.4.13. [A.15] Modificación deliberada de la información	2	1%	5	BAJO
		5.4.14. [A.18] Destrucción de información	2	50%	8	ALTO
		5.4.15. [A.19] Divulgación de información	2	1%	5	BAJO
		5.4.16. [A.22] Manipulación de programas	2	50%	5	MEDIO
	Antivirus Kaspersky Office Small	5.2.6. [I.5] Avería de origen físico o lógico	3	100 %	5	ALTO
		5.3.1. [E.1] Errores de los usuarios	5	50%	3	BAJO
		5.3.2. [E.2] Errores del administrador	3	50%	5	MEDIO
		5.3.6. [E.8] Difusión de software dañino	2	100 %	8	MUY ALTO

PERSONAL	[P]		5.3.7. [E.9] Errores de [re- encaminamiento	2	50%	3	BAJO
			5.3.8. [E.10] Errores de secuencia	2	50%	3	BAJO
			5.3.10. [E.15] Alteración accidental de la información	4	50%	5	MEDIO
			5.3.11. [E.18] Destrucción de información	2	100 %	5	ALTO
			5.3.12. [E.19] Fugas de información	3	1%	3	MUY BAJO
			5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	50%	5	MEDIO
			5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	50%	5	MEDIO
			5.4.3. [A.5] Suplantación de la identidad del usuario	3	50%	5	MEDIO
			5.4.4. [A.6] Abuso de privilegios de acceso	3	50%	5	MEDIO
			5.4.5. [A.7] Uso no previsto	3	50%	5	MEDIO
			5.4.6. [A.8] Difusión de software dañino	2	100 %	5	ALTO
			5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	50%	5	MEDIO
			5.4.8. [A.10] Alteración de secuencia	3	50%	3	BAJO
			5.4.9. [A.11] Acceso no autorizado	3	50%	5	MEDIO
			5.4.13. [A.15] Modificación deliberada de la información	2	1%	5	BAJO
			5.4.14. [A.18] Destrucción de información	2	50%	5	MEDIO
			5.4.15. [A.19] Divulgación de información	2	50%	5	MEDIO
			5.4.16. [A.22] Manipulación de programas	2	50%	5	MEDIO
		Director de T,I	5.3.5. [E.7] Deficiencias en la organización	4	50%	5	MEDIO
			5.3.18. [E.28] Indisponibilidad del personal	3	100 %	5	ALTO
			5.4.22. [A.28] Indisponibilidad del personal	2	100 %	5	ALTO
			5.4.23. [A.29] Extorsión	2	100 %	8	MUY ALTO
			5.4.24. [A.30] Ingeniería social (picaresca)	2	1%	8	MEDIO

SERVICIOS	[S]	Auxiliar de T.I	5.3.5. [E.7] Deficiencias en la organización	4	50%	3	BAJO
			5.3.18. [E.28] Indisponibilidad del personal	3	100 %	3	MEDIO
			5.4.22. [A.28] Indisponibilidad del personal	2	100 %	5	ALTO
			5.4.23. [A.29] Extorsión	2	100 %	5	ALTO
			5.4.24. [A.30] Ingeniería social (picaresca)	2	1%	8	MEDIO
		Consultor de T.I	5.3.5. [E.7] Deficiencias en la organización	5	50%	3	BAJO
			5.3.18. [E.28] Indisponibilidad del personal	2	100 %	3	MEDIO
			5.4.22. [A.28] Indisponibilidad del personal	2	100 %	3	MEDIO
			5.4.23. [A.29] Extorsión	1	1%	5	BAJO
			5.4.24. [A.30] Ingeniería social (picaresca)	2	1%	5	BAJO
		Gerencia	5.3.5. [E.7] Deficiencias en la organización	2	50%	8	ALTO
			5.3.18. [E.28] Indisponibilidad del personal	2	100 %	5	ALTO
			5.4.22. [A.28] Indisponibilidad del personal	2	100 %	5	ALTO
			5.4.23. [A.29] Extorsión	1	100 %	8	MUY ALTO
			5.4.24. [A.30] Ingeniería social (picaresca)	1	1%	5	BAJO
	[S]	Correo Microsoft Office 365	5.3.1. [E.1] Errores de los usuarios	5	1%	3	MUY BAJO
			5.3.2. [E.2] Errores del administrador	3	50%	5	MEDIO
			5.3.7. [E.9] Errores de [re-]encaminamiento	4	1%	3	MUY BAJO
			5.3.8. [E.10] Errores de secuencia	4	1%	3	MUY BAJO
			5.3.10. [E.15] Alteración accidental de la información	5	1%	3	MUY BAJO
			5.3.11. [E.18] Destrucción de información	4	50%	5	MEDIO
			5.3.12. [E.19] Fugas de información	4	1%	3	MUY BAJO
			5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	1%	5	BAJO

		5.4.3. [A.5] Suplantación de la identidad del usuario	3	1%	5	BAJO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	50%	5	MEDIO
		5.4.5. [A.7] Uso no previsto	4	1%	3	MUY BAJO
		5.4.7. [A.9] [Re-]encaminamiento de mensajes	4	1%	3	MUY BAJO
		5.4.8. [A.10] Alteración de secuencia	3	1%	3	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	3	1%	3	MUY BAJO
		5.4.11. [A.13] Repudio	3	1%	3	MUY BAJO
		5.4.13. [A.15] Modificación deliberada de la información	3	50%	5	MEDIO
		5.4.14. [A.18] Destrucción de información	3	50%	5	MEDIO
		5.4.15. [A.19] Divulgación de información	3	1%	3	MUY BAJO
		5.4.18. [A.24] Denegación de servicio	3	1%	5	BAJO
	Dominio	5.3.1. [E.1] Errores de los usuarios	5	1%	3	MUY BAJO
		5.3.2. [E.2] Errores del administrador	3	50%	8	ALTO
		5.3.7. [E.9] Errores de [re-]encaminamiento	4	1%	3	MUY BAJO
		5.3.8. [E.10] Errores de secuencia	4	1%	3	MUY BAJO
		5.3.10. [E.15] Alteración accidental de la información	4	1%	5	BAJO
		5.3.11. [E.18] Destrucción de información	4	100%	8	MUY ALTO
		5.3.12. [E.19] Fugas de información	4	1%	8	MEDIO
		5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	1%	8	MEDIO
		5.4.3. [A.5] Suplantación de la identidad del usuario	3	1%	8	MEDIO
		5.4.4. [A.6] Abuso de privilegios de acceso	3	50%	8	ALTO
		5.4.5. [A.7] Uso no previsto	4	1%	8	MEDIO
		5.4.7. [A.9] [Re-]encaminamiento de mensajes	4	1%	5	BAJO

			5.4.8. [A.10] Alteración de secuencia	3	1%	3	MUY BAJO
			5.4.9. [A.11] Acceso no autorizado	3	50%	5	MEDIO
			5.4.11. [A.13] Repudio	3	1%	8	MEDIO
			5.4.13. [A.15] Modificación deliberada de la información	3	50%	8	ALTO
			5.4.14. [A.18] Destrucción de información	3	100 %	8	MUY ALTO
			5.4.15. [A.19] Divulgación de información	3	50%	8	ALTO
			5.4.18. [A.24] Denegación de servicio	3	1%	8	MEDIO
		Hosting	5.3.1. [E.1] Errores de los usuarios	4	1%	3	MUY BAJO
			5.3.2. [E.2] Errores del administrador	3	50%	5	MEDIO
			5.3.7. [E.9] Errores de [re-]encaminamiento	3	1%	3	MUY BAJO
			5.3.8. [E.10] Errores de secuencia	3	1%	3	MUY BAJO
			5.3.10. [E.15] Alteración accidental de la información	4	1%	5	BAJO
			5.3.11. [E.18] Destrucción de información	4	100 %	5	ALTO
			5.3.12. [E.19] Fugas de información	3	1%	5	BAJO
			5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	1%	5	BAJO
			5.4.3. [A.5] Suplantación de la identidad del usuario	3	1%	5	BAJO
			5.4.4. [A.6] Abuso de privilegios de acceso	3	50%	5	MEDIO
			5.4.5. [A.7] Uso no previsto	3	1%	5	BAJO
			5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	1%	3	MUY BAJO
			5.4.8. [A.10] Alteración de secuencia	3	1%	3	MUY BAJO
			5.4.9. [A.11] Acceso no autorizado	3	50%	5	MEDIO
			5.4.11. [A.13] Repudio	3	1%	5	BAJO
			5.4.13. [A.15] Modificación deliberada de la información	3	50%	5	MEDIO
			5.4.14. [A.18] Destrucción de información	2	100 %	5	ALTO
			5.4.15. [A.19] Divulgación de información	3	50%	5	MEDIO

			5.4.18. [A.24] Denegación de servicio	3	1%	5	BAJO
			5.3.1. [E.1] Errores de los usuarios	5	1%	3	MUY BAJO
		Almacenamiento o Nube	5.3.2. [E.2] Errores del administrador	3	50%	5	MEDIO
			5.3.7. [E.9] Errores de [re-]encaminamiento	4	1%	3	MUY BAJO
			5.3.8. [E.10] Errores de secuencia	4	1%	3	MUY BAJO
			5.3.10. [E.15] Alteración accidental de la información	5	1%	3	MUY BAJO
			5.3.11. [E.18] Destrucción de información	4	50%	8	ALTO
			5.3.12. [E.19] Fugas de información	4	1%	3	MUY BAJO
			5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	1%	5	BAJO
			5.4.3. [A.5] Suplantación de la identidad del usuario	3	1%	8	MEDIO
			5.4.4. [A.6] Abuso de privilegios de acceso	3	50%	8	ALTO
			5.4.5. [A.7] Uso no previsto	4	1%	3	MUY BAJO
			5.4.7. [A.9] [Re-]encaminamiento de mensajes	4	1%	3	MUY BAJO
			5.4.8. [A.10] Alteración de secuencia	3	1%	3	MUY BAJO
			5.4.9. [A.11] Acceso no autorizado	3	1%	3	MUY BAJO
			5.4.11. [A.13] Repudio	3	1%	3	MUY BAJO
			5.4.13. [A.15] Modificación deliberada de la información	3	50%	5	MEDIO
			5.4.14. [A.18] Destrucción de información	3	50%	8	ALTO
			5.4.15. [A.19] Divulgación de información	3	1%	8	MEDIO
			5.4.18. [A.24] Denegación de servicio	3	1%	5	BAJO
		Virtualización	5.3.1. [E.1] Errores de los usuarios	4	1%	5	BAJO
			5.3.2. [E.2] Errores del administrador	4	50%	8	ALTO
			5.3.7. [E.9] Errores de [re-]encaminamiento	3	1%	5	BAJO
			5.3.8. [E.10] Errores de secuencia	3	1%	5	BAJO

		RDS	5.3.10. [E.15] Alteración accidental de la información	4	1%	8	MEDIO
			5.3.11. [E.18] Destrucción de información	4	100%	8	MUY ALTO
			5.3.12. [E.19] Fugas de información	3	50%	8	ALTO
			5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	50%	8	ALTO
			5.4.3. [A.5] Suplantación de la identidad del usuario	3	50%	8	ALTO
			5.4.4. [A.6] Abuso de privilegios de acceso	3	50%	8	ALTO
			5.4.5. [A.7] Uso no previsto	3	50%	8	ALTO
			5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	50%	5	MEDIO
			5.4.8. [A.10] Alteración de secuencia	3	50%	5	MEDIO
			5.4.9. [A.11] Acceso no autorizado	3	50%	8	ALTO
			5.4.11. [A.13] Repudio	3	50%	5	MEDIO
			5.4.13. [A.15] Modificación deliberada de la información	3	50%	8	ALTO
			5.4.14. [A.18] Destrucción de información	2	100%	8	MUY ALTO
			5.4.15. [A.19] Divulgación de información	3	50%	8	ALTO
			5.4.18. [A.24] Denegación de servicio	3	50%	8	ALTO
			5.3.1. [E.1] Errores de los usuarios	4	1%	5	BAJO
			5.3.2. [E.2] Errores del administrador	4	50%	8	ALTO
			5.3.7. [E.9] Errores de [re-]encaminamiento	3	1%	5	BAJO
			5.3.8. [E.10] Errores de secuencia	3	1%	5	BAJO
			5.3.10. [E.15] Alteración accidental de la información	4	1%	8	MEDIO
			5.3.11. [E.18] Destrucción de información	4	100%	8	MUY ALTO
			5.3.12. [E.19] Fugas de información	3	50%	8	ALTO
			5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	50%	8	ALTO
			5.4.3. [A.5] Suplantación de la identidad del usuario	3	50%	8	ALTO
			5.4.4. [A.6] Abuso de privilegios de acceso	3	50%	8	ALTO
			5.4.5. [A.7] Uso no previsto	3	50%	8	ALTO
			5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	50%	5	MEDIO

EQUIPAMIENTO AUXILIAR	AUX		5.4.8. [A.10] Alteración de secuencia	3	50%	5	MEDIO
			5.4.9. [A.11] Acceso no autorizado	3	50%	8	ALTO
			5.4.11. [A.13] Repudio	3	50%	5	MEDIO
			5.4.13. [A.15] Modificación deliberada de la información	3	50%	8	ALTO
			5.4.14. [A.18] Destrucción de información	2	100 %	8	MUY ALTO
			5.4.15. [A.19] Divulgación de información	3	50%	8	ALTO
			5.4.18. [A.24] Denegación de servicio	3	50%	8	ALTO
		Aire acondicionado Data Center.	5.1.1. [N.1] Fuego	1	100 %	8	MUY ALTO
			5.1.2. [N.2] Daños por agua	2	100 %	8	MUY ALTO
			5.1.3. [N.*] Desastres naturales	2	100 %	8	MUY ALTO
			5.2.1. [I.1] Fuego	2	100 %	8	MUY ALTO
			5.2.2. [I.2] Daños por agua	2	100 %	8	MUY ALTO
			5.2.3. [I.*] Desastres industriales	2	1%	8	MEDIO
			5.2.4. [I.3] Contaminación mecánica	3	1%	8	MEDIO
			5.2.5. [I.4] Contaminación electromagnética	3	1%	8	MEDIO
			5.2.6. [I.5] Avería de origen físico o lógico	4	50%	8	ALTO
			5.2.7. [I.6] Corte del suministro eléctrico	4	1%	8	MEDIO
			5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	1%	8	MEDIO
			5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	3	1%	8	MEDIO
			5.2.12. [I.11] Emanaciones electromagnéticas	3	1%	8	MEDIO
			5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	50%	8	ALTO
			5.3.17. [E.25] Pérdida de equipos	3	100 %	8	MUY ALTO
			5.4.5. [A.7] Uso no previsto	3	1%	1	MUY BAJO
			5.4.9. [A.11] Acceso no autorizado	3	1%	1	MUY BAJO

			5.4.17. [A.23] Manipulación de los equipos	3	100 %	8	MUY ALTO
			5.4.19. [A.25] Robo	3	100 %	8	MUY ALTO
			5.4.20. [A.26] Ataque destructivo	1	100 %	8	MUY ALTO
		UPS	5.1.1. [N.1] Fuego	2	100 %	8	MUY ALTO
			5.1.2. [N.2] Daños por agua	2	100 %	8	MUY ALTO
			5.1.3. [N.*] Desastres naturales	2	100 %	8	MUY ALTO
			5.2.1. [I.1] Fuego	2	100 %	8	MUY ALTO
			5.2.2. [I.2] Daños por agua	2	100 %	8	MUY ALTO
			5.2.3. [I.*] Desastres industriales	2	1%	8	MEDIO
			5.2.4. [I.3] Contaminación mecánica	4	1%	8	MEDIO
			5.2.5. [I.4] Contaminación electromagnética	4	1%	8	MEDIO
			5.2.6. [I.5] Avería de origen físico o lógico	3	50%	8	ALTO
			5.2.7. [I.6] Corte del suministro eléctrico	4	1%	8	MEDIO
			5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	1%	8	MEDIO
			5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	3	1%	8	MEDIO
			5.2.12. [I.11] Emanaciones electromagnéticas	3	1%	8	MEDIO
			5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	50%	8	ALTO
			5.3.17. [E.25] Pérdida de equipos	2	100 %	8	MUY ALTO
			5.4.5. [A.7] Uso no previsto	2	1%	8	MEDIO
			5.4.9. [A.11] Acceso no autorizado	3	1%	8	MEDIO
			5.4.17. [A.23] Manipulación de los equipos	3	100 %	8	MUY ALTO
			5.4.19. [A.25] Robo	2	100 %	8	MUY ALTO
			5.4.20. [A.26] Ataque destructivo	2	100 %	8	MUY ALTO

INSTALACION	L	Planta electrica	5.1.1. [N.1] Fuego	1	100 %	8	MUY ALTO
			5.1.2. [N.2] Daños por agua	2	100 %	8	MUY ALTO
			5.1.3. [N.*] Desastres naturales	2	100 %	8	MUY ALTO
			5.2.1. [I.1] Fuego	2	100 %	8	MUY ALTO
			5.2.2. [I.2] Daños por agua	2	100 %	8	MUY ALTO
			5.2.3. [I.*] Desastres industriales	2	1%	8	MEDIO
			5.2.4. [I.3] Contaminación mecánica	4	1%	8	MEDIO
			5.2.5. [I.4] Contaminación electromagnética	4	1%	8	MEDIO
			5.2.6. [I.5] Avería de origen físico o lógico	3	50%	8	ALTO
			5.2.7. [I.6] Corte del suministro eléctrico	3	1%	8	MEDIO
			5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	1%	8	MEDIO
			5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	3	1%	8	MEDIO
			5.2.12. [I.11] Emanaciones electromagnéticas	3	1%	8	MEDIO
			5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	50%	8	ALTO
			5.3.17. [E.25] Pérdida de equipos	2	100 %	8	MUY ALTO
			5.4.5. [A.7] Uso no previsto	3	50%	5	MEDIO
			5.4.9. [A.11] Acceso no autorizado	3	100 %	8	MUY ALTO
			5.4.17. [A.23] Manipulación de los equipos	3	100 %	8	MUY ALTO
			5.4.19. [A.25] Robo	3	100 %	8	MUY ALTO
			5.4.20. [A.26] Ataque destructivo	2	100 %	8	MUY ALTO
	L	Data Center	5.1.1. [N.1] Fuego	2	100 %	8	MUY ALTO
			5.1.2. [N.2] Daños por agua	2	100 %	8	MUY ALTO
			5.2.1. [I.1] Fuego	2	100 %	8	MUY ALTO

		5.2.2. [I.2] Daños por agua	2	100 %	8	MUY ALTO
		5.2.3. [I.*] Desastres industriales	2	50%	8	ALTO
		5.2.12. [I.11] Emanaciones electromagnéticas	3	1%	8	MEDIO
		5.3.10. [E.15] Alteración accidental de la información	3	100 %	8	MUY ALTO
		5.3.11. [E.18] Destrucción de información	3	100 %	8	MUY ALTO
		5.3.12. [E.19] Fugas de información	3	100 %	5	ALTO
		5.4.5. [A.7] Uso no previsto	3	50%	2	MUY BAJO
		5.4.9. [A.11] Acceso no autorizado	3	100 %	8	MUY ALTO
		5.4.13. [A.15] Modificación deliberada de la información	3	50%	5	MEDIO
		5.4.14. [A.18] Destrucción de información	2	100 %	8	MUY ALTO
		5.4.15. [A.19] Divulgación de información	3	50%	8	ALTO
		5.4.20. [A.26] Ataque destructivo	1	100 %	8	MUY ALTO
		5.4.21. [A.27] Ocupación enemiga	1	100 %	8	MUY ALTO

Apéndice B

Valoración de Riesgos Activos de Información Transportes Gayco

ACTIVO	AMENAZAS	FRECUENCIA	DAÑO/IMPACTO (VALOR)	RIESGO CUANTITATIVO	RIESGO CUALITATIVO
Gestion Documental	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
Almacen	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE

	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
Compras	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
Contabilidad	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO

	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
Facturacion	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
Gerencia	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
Gerencia 2021	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE

	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
Gerencia Gayco	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
Gestion Comercial	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE

	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
HSEQ	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
Mantenimiento	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE

	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
Operaciones	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
Proveedores 2022	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
Seguridad Física	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE

	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
Sistema de Gestion	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
Talento Humano	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE

	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
Tesoreria	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE
Vehiculos	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	1	1	1	ACEPTABLE
	5.3.10. [E.15] Alteración accidental de la información	2	5	10	INTOLERANTE
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	2	3	6	TOLERANTE
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	1	5	5	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	1	8	8	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	1	1	1	ACEPTABLE

Bitlocker discos externos	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	4	5	20	EXTREMO
	5.3.10. [E.15] Alteración accidental de la información	4	5	20	EXTREMO
	5.3.11. [E.18] Destrucción de información	3	8	24	EXTREMO
	5.3.12. [E.19] Fugas de información	4	5	20	EXTREMO
	5.4.3. [A.5] Suplantación de la identidad del usuario	4	5	20	EXTREMO
	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	15	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	5	15	EXTREMO
	5.4.13. [A.15] Modificación deliberada de la información	3	5	15	EXTREMO
	5.4.14. [A.18] Destrucción de información	2	8	16	EXTREMO
	5.4.15. [A.19] Divulgación de información	3	5	15	EXTREMO
Servidor ecoplanta	5.1.1. [N.1] Fuego	1	8	8	INTOLERANTE
	5.1.2. [N.2] Daños por agua	1	8	8	INTOLERANTE
	5.1.3. [N.*] Desastres naturales	1	8	8	INTOLERANTE
	5.2.1. [I.1] Fuego	1	8	8	INTOLERANTE
	5.2.2. [I.2] Daños por agua	1	8	8	INTOLERANTE
	5.2.3. [I.*] Desastres industriales	2	8	16	EXTREMO
	5.2.4. [I.3] Contaminación mecánica	3	5	15	EXTREMO
	5.2.5. [I.4] Contaminación electromagnética	3	5	15	EXTREMO
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24	EXTREMO
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32	EXTREMO
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24	EXTREMO
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15	EXTREMO
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	8	32	EXTREMO

	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	8	16	EXTREMO
	5.3.17. [E.25] Pérdida de equipos	1	8	8	INTOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	8	24	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.17. [A.23] Manipulación de los equipos	3	8	24	EXTREMO
	5.4.18. [A.24] Denegación de servicio	3	8	24	EXTREMO
	5.4.19. [A.25] Robo	1	8	8	INTOLERANTE
	5.4.20. [A.26] Ataque destructivo	1	8	8	INTOLERANTE
Servidor hipervisor	5.1.1. [N.1] Fuego	1	8	8	INTOLERANTE
	5.1.2. [N.2] Daños por agua	1	8	8	INTOLERANTE
	5.1.3. [N.*] Desastres naturales	1	8	8	INTOLERANTE
	5.2.1. [I.1] Fuego	1	8	8	INTOLERANTE
	5.2.2. [I.2] Daños por agua	1	8	8	INTOLERANTE
	5.2.3. [I.*] Desastres industriales	2	8	16	EXTREMO
	5.2.4. [I.3] Contaminación mecánica	3	5	15	EXTREMO
	5.2.5. [I.4] Contaminación electromagnética	3	5	15	EXTREMO
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24	EXTREMO
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32	EXTREMO
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24	EXTREMO
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15	EXTREMO
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	8	32	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	8	16	EXTREMO
	5.3.17. [E.25] Pérdida de equipos	1	8	8	INTOLERANTE

	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	8	24	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.17. [A.23] Manipulación de los equipos	3	8	24	EXTREMO
	5.4.18. [A.24] Denegación de servicio	3	8	24	EXTREMO
	5.4.19. [A.25] Robo	1	8	8	INTOLERANTE
	5.4.20. [A.26] Ataque destructivo	1	8	8	INTOLERANTE
Servidor Dominio	5.1.1. [N.1] Fuego	1	8	8	INTOLERANTE
	5.1.2. [N.2] Daños por agua	1	8	8	INTOLERANTE
	5.1.3. [N.*] Desastres naturales	1	8	8	INTOLERANTE
	5.2.1. [I.1] Fuego	1	8	8	INTOLERANTE
	5.2.2. [I.2] Daños por agua	1	8	8	INTOLERANTE
	5.2.3. [I.*] Desastres industriales	2	8	16	EXTREMO
	5.2.4. [I.3] Contaminación mecánica	3	5	15	EXTREMO
	5.2.5. [I.4] Contaminación electromagnética	3	5	15	EXTREMO
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24	EXTREMO
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32	EXTREMO
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24	EXTREMO
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15	EXTREMO
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	8	32	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	8	16	EXTREMO
	5.3.17. [E.25] Pérdida de equipos	1	8	8	INTOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	8	24	EXTREMO

	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.17. [A.23] Manipulación de los equipos	3	8	24	EXTREMO
	5.4.18. [A.24] Denegación de servicio	3	8	24	EXTREMO
	5.4.19. [A.25] Robo	1	8	8	INTOLERANTE
	5.4.20. [A.26] Ataque destructivo	1	8	8	INTOLERANTE
Servidores de archivos	5.1.1. [N.1] Fuego	1	8	8	INTOLERANTE
	5.1.2. [N.2] Daños por agua	1	8	8	INTOLERANTE
	5.1.3. [N.*] Desastres naturales	1	8	8	INTOLERANTE
	5.2.1. [I.1] Fuego	1	8	8	INTOLERANTE
	5.2.2. [I.2] Daños por agua	1	8	8	INTOLERANTE
	5.2.3. [I.*] Desastres industriales	2	8	16	EXTREMO
	5.2.4. [I.3] Contaminación mecánica	3	5	15	EXTREMO
	5.2.5. [I.4] Contaminación electromagnética	3	5	15	EXTREMO
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24	EXTREMO
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32	EXTREMO
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24	EXTREMO
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15	EXTREMO
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	8	32	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	8	16	EXTREMO
	5.3.17. [E.25] Pérdida de equipos	1	8	8	INTOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	8	24	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.17. [A.23] Manipulación de los equipos	3	8	24	EXTREMO
	5.4.18. [A.24] Denegación de servicio	3	8	24	EXTREMO

	5.4.19. [A.25] Robo	1	8	8	INTOLERANT E
	5.4.20. [A.26] Ataque destructivo	1	8	8	INTOLERANT E
Servidor Soluxionar	5.1.1. [N.1] Fuego	1	8	8	INTOLERANT E
	5.1.2. [N.2] Daños por agua	1	8	8	INTOLERANT E
	5.1.3. [N.*] Desastres naturales	1	8	8	INTOLERANT E
	5.2.1. [I.1] Fuego	1	8	8	INTOLERANT E
	5.2.2. [I.2] Daños por agua	1	8	8	INTOLERANT E
	5.2.3. [I.*] Desastres industriales	2	8	16	EXTREMO
	5.2.4. [I.3] Contaminación mecánica	3	5	15	EXTREMO
	5.2.5. [I.4] Contaminación electromagnética	3	5	15	EXTREMO
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24	EXTREMO
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32	EXTREMO
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24	EXTREMO
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15	EXTREMO
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	8	32	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	8	16	EXTREMO
	5.3.17. [E.25] Pérdida de equipos	1	8	8	INTOLERANT E
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	8	24	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.17. [A.23] Manipulación de los equipos	3	8	24	EXTREMO
	5.4.18. [A.24] Denegación de servicio	3	8	24	EXTREMO
	5.4.19. [A.25] Robo	1	8	8	INTOLERANT E

	5.4.20. [A.26] Ataque destructivo	1	8	8	INTOLERANT E
Switch administrable	5.1.1. [N.1] Fuego	1	8	8	INTOLERANT E
	5.1.2. [N.2] Daños por agua	1	8	8	INTOLERANT E
	5.1.3. [N.*] Desastres naturales	1	8	8	INTOLERANT E
	5.2.1. [I.1] Fuego	1	8	8	INTOLERANT E
	5.2.2. [I.2] Daños por agua	1	8	8	INTOLERANT E
	5.2.3. [I.*] Desastres industriales	2	8	16	EXTREMO
	5.2.4. [I.3] Contaminación mecánica	3	5	15	EXTREMO
	5.2.5. [I.4] Contaminación electromagnética	3	5	15	EXTREMO
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24	EXTREMO
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32	EXTREMO
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24	EXTREMO
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15	EXTREMO
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	8	32	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	8	16	EXTREMO
	5.3.17. [E.25] Pérdida de equipos	1	8	8	INTOLERANT E
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	8	24	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.17. [A.23] Manipulación de los equipos	3	8	24	EXTREMO
	5.4.18. [A.24] Denegación de servicio	3	8	24	EXTREMO
	5.4.19. [A.25] Robo	1	8	8	INTOLERANT E
	5.4.20. [A.26] Ataque destructivo	1	8	8	INTOLERANT E
Switch almacen	5.1.1. [N.1] Fuego	1	5	5	TOLERANTE

	5.1.2. [N.2] Daños por agua	1	5	5	TOLERANTE
	5.1.3. [N.*] Desastres naturales	1	5	5	TOLERANTE
	5.2.1. [I.1] Fuego	1	5	5	TOLERANTE
	5.2.2. [I.2] Daños por agua	1	5	5	TOLERANTE
	5.2.3. [I.*] Desastres industriales	3	5	15	EXTREMO
	5.2.4. [I.3] Contaminación mecánica	4	2	8	INTOLERANTE
	5.2.5. [I.4] Contaminación electromagnética	3	2	6	TOLERANTE
	5.2.6. [I.5] Avería de origen físico o lógico	3	5	15	EXTREMO
	5.2.7. [I.6] Corte del suministro eléctrico	4	3	12	EXTREMO
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	4	3	12	EXTREMO
	5.2.12. [I.11] Emanaciones electromagnéticas	3	2	6	TOLERANTE
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	3	12	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	5	10	INTOLERANTE
	5.3.17. [E.25] Pérdida de equipos	1	5	5	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	3	2	6	TOLERANTE
	5.4.5. [A.7] Uso no previsto	3	3	9	INTOLERANTE
	5.4.9. [A.11] Acceso no autorizado	3	3	9	INTOLERANTE
	5.4.17. [A.23] Manipulación de los equipos	3	3	9	INTOLERANTE
	5.4.18. [A.24] Denegación de servicio	3	5	15	EXTREMO
	5.4.19. [A.25] Robo	2	5	10	INTOLERANTE
	5.4.20. [A.26] Ataque destructivo	1	5	5	TOLERANTE
UTM	5.1.1. [N.1] Fuego	1	8	8	INTOLERANTE
	5.1.2. [N.2] Daños por agua	1	8	8	INTOLERANTE
	5.1.3. [N.*] Desastres naturales	1	8	8	INTOLERANTE
	5.2.1. [I.1] Fuego	1	8	8	INTOLERANTE

	5.2.2. [I.2] Daños por agua	1	8	8	INTOLERANT E
	5.2.3. [I.*] Desastres industriales	2	8	16	EXTREMO
	5.2.4. [I.3] Contaminación mecánica	3	5	15	EXTREMO
	5.2.5. [I.4] Contaminación electromagnética	3	5	15	EXTREMO
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24	EXTREMO
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32	EXTREMO
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24	EXTREMO
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15	EXTREMO
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	8	32	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	8	16	EXTREMO
	5.3.17. [E.25] Pérdida de equipos	1	8	8	INTOLERANT E
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	8	24	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.17. [A.23] Manipulación de los equipos	3	8	24	EXTREMO
	5.4.18. [A.24] Denegación de servicio	3	8	24	EXTREMO
	5.4.19. [A.25] Robo	1	8	8	INTOLERANT E
	5.4.20. [A.26] Ataque destructivo	1	8	8	INTOLERANT E
Router proveedores	5.1.1. [N.1] Fuego	1	8	8	INTOLERANT E
	5.1.2. [N.2] Daños por agua	1	8	8	INTOLERANT E
	5.1.3. [N.*] Desastres naturales	1	8	8	INTOLERANT E
	5.2.1. [I.1] Fuego	1	8	8	INTOLERANT E
	5.2.2. [I.2] Daños por agua	1	8	8	INTOLERANT E
	5.2.3. [I.*] Desastres industriales	2	8	16	EXTREMO

	5.2.4. [I.3] Contaminación mecánica	3	5	15	EXTREMO
	5.2.5. [I.4] Contaminación electromagnética	3	5	15	EXTREMO
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24	EXTREMO
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32	EXTREMO
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24	EXTREMO
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15	EXTREMO
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	8	32	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	8	16	EXTREMO
	5.3.17. [E.25] Pérdida de equipos	1	8	8	INTOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	8	24	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.17. [A.23] Manipulación de los equipos	3	8	24	EXTREMO
	5.4.18. [A.24] Denegación de servicio	3	8	24	EXTREMO
	5.4.19. [A.25] Robo	1	8	8	INTOLERANTE
	5.4.20. [A.26] Ataque destructivo	1	8	8	INTOLERANTE
Acces Point	5.1.1. [N.1] Fuego	1	5	5	TOLERANTE
	5.1.2. [N.2] Daños por agua	1	5	5	TOLERANTE
	5.1.3. [N.*] Desastres naturales	1	5	5	TOLERANTE
	5.2.1. [I.1] Fuego	1	5	5	TOLERANTE
	5.2.2. [I.2] Daños por agua	1	5	5	TOLERANTE
	5.2.3. [I.*] Desastres industriales	2	5	10	INTOLERANTE
	5.2.4. [I.3] Contaminación mecánica	3	2	6	TOLERANTE
	5.2.5. [I.4] Contaminación electromagnética	3	5	15	EXTREMO
	5.2.6. [I.5] Avería de origen físico o lógico	3	5	15	EXTREMO
	5.2.7. [I.6] Corte del suministro eléctrico	4	3	12	EXTREMO

	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	3	9	INTOLERANTE
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15	EXTREMO
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	3	12	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	5	10	INTOLERANTE
	5.3.17. [E.25] Pérdida de equipos	1	5	5	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	3	2	6	TOLERANTE
	5.4.5. [A.7] Uso no previsto	3	3	9	INTOLERANTE
	5.4.9. [A.11] Acceso no autorizado	3	3	9	INTOLERANTE
	5.4.17. [A.23] Manipulación de los equipos	3	3	9	INTOLERANTE
	5.4.18. [A.24] Denegación de servicio	3	5	15	EXTREMO
	5.4.19. [A.25] Robo	1	5	5	TOLERANTE
	5.4.20. [A.26] Ataque destructivo	1	5	5	TOLERANTE
Monitores	5.1.1. [N.1] Fuego	1	2	2	ACEPTABLE
	5.1.2. [N.2] Daños por agua	1	2	2	ACEPTABLE
	5.1.3. [N.*] Desastres naturales	1	2	2	ACEPTABLE
	5.2.1. [I.1] Fuego	1	2	2	ACEPTABLE
	5.2.2. [I.2] Daños por agua	1	2	2	ACEPTABLE
	5.2.3. [I.*] Desastres industriales	2	2	4	TOLERANTE
	5.2.4. [I.3] Contaminación mecánica	3	1	3	TOLERANTE
	5.2.5. [I.4] Contaminación electromagnética	3	1	3	TOLERANTE
	5.2.6. [I.5] Avería de origen físico o lógico	3	2	6	TOLERANTE
	5.2.7. [I.6] Corte del suministro eléctrico	4	2	8	INTOLERANTE
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	1	3	TOLERANTE
	5.2.12. [I.11] Emanaciones electromagnéticas	3	2	6	TOLERANTE
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	1	4	TOLERANTE

	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	1	2	ACEPTABLE
	5.3.17. [E.25] Pérdida de equipos	1	3	3	TOLERANTE
	5.4.4. [A.6] Abuso de privilegios de acceso	3	1	3	TOLERANTE
	5.4.5. [A.7] Uso no previsto	3	2	6	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	3	3	9	INTOLERANTE
	5.4.17. [A.23] Manipulación de los equipos	3	3	9	INTOLERANTE
	5.4.18. [A.24] Denegación de servicio	3	1	3	TOLERANTE
	5.4.19. [A.25] Robo	1	3	3	TOLERANTE
	5.4.20. [A.26] Ataque destructivo	1	3	3	TOLERANTE
LAN	5.2.9. [I.8] Fallo de servicios de comunicaciones	3	5	15	EXTREMO
	5.3.2. [E.2] Errores del administrador	3	3	9	INTOLERANTE
	5.3.7. [E.9] Errores de [re-]encaminamiento	2	3	6	TOLERANTE
	5.3.8. [E.10] Errores de secuencia	2	3	6	TOLERANTE
	5.3.10. [E.15] Alteración accidental de la información	4	3	12	EXTREMO
	5.3.11. [E.18] Destrucción de información	3	8	24	EXTREMO
	5.3.12. [E.19] Fugas de información	4	5	20	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	8	24	EXTREMO
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	15	EXTREMO
	5.4.4. [A.6] Abuso de privilegios de acceso	4	5	20	EXTREMO
	5.4.5. [A.7] Uso no previsto	5	5	25	EXTREMO
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	3	9	INTOLERANTE
	5.4.8. [A.10] Alteración de secuencia	4	3	12	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	5	15	EXTREMO
	5.4.10. [A.12] Análisis de tráfico	3	5	15	EXTREMO
	5.4.12. [A.14] Interceptación de información (escucha)	3	5	15	EXTREMO
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.15. [A.19] Divulgación de información	3	8	24	EXTREMO

	5.4.18. [A.24] Denegación de servicio	3	8	24	EXTREMO
Internet Empresarial Backup	5.2.9. [I.8] Fallo de servicios de comunicaciones	4	8	32	EXTREMO
	5.3.2. [E.2] Errores del administrador	3	5	15	EXTREMO
	5.3.7. [E.9] Errores de [re-]encaminamiento	3	5	15	EXTREMO
	5.3.8. [E.10] Errores de secuencia	3	5	15	EXTREMO
	5.3.10. [E.15] Alteración accidental de la información	3	5	15	EXTREMO
	5.3.11. [E.18] Destrucción de información	3	5	15	EXTREMO
	5.3.12. [E.19] Fugas de información	3	8	24	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	8	24	EXTREMO
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	8	24	EXTREMO
	5.4.4. [A.6] Abuso de privilegios de acceso	2	8	16	EXTREMO
	5.4.5. [A.7] Uso no previsto	5	8	40	EXTREMO
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	4	5	20	EXTREMO
	5.4.8. [A.10] Alteración de secuencia	3	5	15	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.10. [A.12] Análisis de tráfico	3	5	15	EXTREMO
	5.4.12. [A.14] Interceptación de información (escucha)	3	5	15	EXTREMO
	5.4.13. [A.15] Modificación deliberada de la información	3	8	24	EXTREMO
	5.4.15. [A.19] Divulgación de información	2	8	16	EXTREMO
	5.4.18. [A.24] Denegación de servicio	3	8	24	EXTREMO
Internet Empresarial	5.2.9. [I.8] Fallo de servicios de comunicaciones	4	8	32	EXTREMO
	5.3.2. [E.2] Errores del administrador	4	5	20	EXTREMO
	5.3.7. [E.9] Errores de [re-]encaminamiento	4	5	20	EXTREMO
	5.3.8. [E.10] Errores de secuencia	4	5	20	EXTREMO
	5.3.10. [E.15] Alteración accidental de la información	4	5	20	EXTREMO
	5.3.11. [E.18] Destrucción de información	3	8	24	EXTREMO
	5.3.12. [E.19] Fugas de información	4	5	20	EXTREMO

	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	4	8	32	EXTREMO
	5.4.3. [A.5] Suplantación de la identidad del usuario	4	8	32	EXTREMO
	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	15	EXTREMO
	5.4.5. [A.7] Uso no previsto	5	5	25	EXTREMO
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	4	5	20	EXTREMO
	5.4.8. [A.10] Alteración de secuencia	4	5	20	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.10. [A.12] Análisis de tráfico	3	8	24	EXTREMO
	5.4.12. [A.14] Interceptación de información (escucha)	3	8	24	EXTREMO
	5.4.13. [A.15] Modificación deliberada de la información	3	8	24	EXTREMO
	5.4.15. [A.19] Divulgación de información	3	8	24	EXTREMO
	5.4.18. [A.24] Denegación de servicio	3	8	24	EXTREMO
Red Inalambrica	5.2.9. [I.8] Fallo de servicios de comunicaciones	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	3	3	9	INTOLERANTE
	5.3.7. [E.9] Errores de [re-]encaminamiento	3	3	9	INTOLERANTE
	5.3.8. [E.10] Errores de secuencia	3	3	9	INTOLERANTE
	5.3.10. [E.15] Alteración accidental de la información	4	3	12	EXTREMO
	5.3.11. [E.18] Destrucción de información	3	8	24	EXTREMO
	5.3.12. [E.19] Fugas de información	4	5	20	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	8	24	EXTREMO
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	15	EXTREMO
	5.4.4. [A.6] Abuso de privilegios de acceso	4	5	20	EXTREMO
	5.4.5. [A.7] Uso no previsto	4	5	20	EXTREMO
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	3	9	INTOLERANTE
	5.4.8. [A.10] Alteración de secuencia	4	3	12	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	5	15	EXTREMO

	5.4.10. [A.12] Análisis de tráfico	3	5	15	EXTREMO
	5.4.12. [A.14] Interceptación de información (escucha)	3	5	15	EXTREMO
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.15. [A.19] Divulgación de información	3	8	24	EXTREMO
	5.4.18. [A.24] Denegación de servicio	3	8	24	EXTREMO
Disco Duro Externo	5.1.1. [N.1] Fuego	1	5	5	TOLERANTE
	5.1.2. [N.2] Daños por agua	1	5	5	TOLERANTE
	5.1.3. [N.*] Desastres naturales	1	5	5	TOLERANTE
	5.2.1. [I.1] Fuego	1	5	5	TOLERANTE
	5.2.2. [I.2] Daños por agua	1	5	5	TOLERANTE
	5.2.3. [I.*] Desastres industriales	1	5	5	TOLERANTE
	5.2.4. [I.3] Contaminación mecánica	3	3	9	INTOLERANTE
	5.2.5. [I.4] Contaminación electromagnética	3	3	9	INTOLERANTE
	5.2.6. [I.5] Avería de origen físico o lógico	3	5	15	EXTREMO
	5.2.7. [I.6] Corte del suministro eléctrico	4	2	8	INTOLERANTE
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	2	6	TOLERANTE
	5.2.11. [I.10] Degradación de los soportes de almacenamiento de la información	3	5	15	EXTREMO
	5.2.12. [I.11] Emanaciones electromagnéticas	3	3	9	INTOLERANTE
	5.3.1. [E.1] Errores de los usuarios	3	3	9	INTOLERANTE
	5.3.2. [E.2] Errores del administrador	3	5	15	EXTREMO
	5.3.10. [E.15] Alteración accidental de la información	3	5	15	EXTREMO
	5.3.11. [E.18] Destrucción de información	2	5	10	INTOLERANTE
	5.3.12. [E.19] Fugas de información	3	5	15	EXTREMO
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	3	6	TOLERANTE
	5.3.17. [E.25] Pérdida de equipos	3	5	15	EXTREMO
	5.4.5. [A.7] Uso no previsto	2	3	6	TOLERANTE

	5.4.9. [A.11] Acceso no autorizado	2	3	6	TOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	2	5	10	INTOLERANTE
	5.4.14. [A.18] Destrucción de información	2	5	10	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	2	5	10	INTOLERANTE
	5.4.17. [A.23] Manipulación de los equipos	2	3	6	TOLERANTE
	5.4.19. [A.25] Robo	3	5	15	EXTREMO
	5.4.20. [A.26] Ataque destructivo	2	5	10	INTOLERANTE
Servidor Nas Soluxionar	5.1.1. [N.1] Fuego	1	8	8	INTOLERANTE
	5.1.2. [N.2] Daños por agua	1	8	8	INTOLERANTE
	5.1.3. [N.*] Desastres naturales	1	8	8	INTOLERANTE
	5.2.1. [I.1] Fuego	1	8	8	INTOLERANTE
	5.2.2. [I.2] Daños por agua	1	8	8	INTOLERANTE
	5.2.3. [I.*] Desastres industriales	1	8	8	INTOLERANTE
	5.2.4. [I.3] Contaminación mecánica	3	5	15	EXTREMO
	5.2.5. [I.4] Contaminación electromagnética	3	5	15	EXTREMO
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24	EXTREMO
	5.2.7. [I.6] Corte del suministro eléctrico	4	5	20	EXTREMO
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	3	9	INTOLERANTE
	5.2.11. [I.10] Degradación de los soportes de almacenamiento de la información	3	5	15	EXTREMO
	5.2.12. [I.11] Emanaciones electromagnéticas	3	3	9	INTOLERANTE
	5.3.1. [E.1] Errores de los usuarios	5	5	25	EXTREMO
	5.3.2. [E.2] Errores del administrador	4	8	32	EXTREMO
	5.3.10. [E.15] Alteración accidental de la información	4	5	20	EXTREMO
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO

	5.3.12. [E.19] Fugas de información	4	5	20	EXTREMO
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	15	EXTREMO
	5.3.17. [E.25] Pérdida de equipos	3	8	24	EXTREMO
	5.4.5. [A.7] Uso no previsto	4	5	20	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	5	15	EXTREMO
	5.4.13. [A.15] Modificación deliberada de la información	3	8	24	EXTREMO
	5.4.14. [A.18] Destrucción de información	2	8	16	EXTREMO
	5.4.15. [A.19] Divulgación de información	3	8	24	EXTREMO
	5.4.17. [A.23] Manipulación de los equipos	2	5	10	INTOLERANTE
	5.4.19. [A.25] Robo	2	8	16	EXTREMO
	5.4.20. [A.26] Ataque destructivo	1	8	8	INTOLERANTE
Servidor NAS Ecoplanta	5.1.1. [N.1] Fuego	1	5	5	TOLERANTE
	5.1.2. [N.2] Daños por agua	1	5	5	TOLERANTE
	5.1.3. [N.*] Desastres naturales	1	5	5	TOLERANTE
	5.2.1. [I.1] Fuego	1	5	5	TOLERANTE
	5.2.2. [I.2] Daños por agua	1	5	5	TOLERANTE
	5.2.3. [I.*] Desastres industriales	1	5	5	TOLERANTE
	5.2.4. [I.3] Contaminación mecánica	3	3	9	INTOLERANTE
	5.2.5. [I.4] Contaminación electromagnética	3	3	9	INTOLERANTE
	5.2.6. [I.5] Avería de origen físico o lógico	3	5	15	EXTREMO
	5.2.7. [I.6] Corte del suministro eléctrico	4	3	12	EXTREMO
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	3	9	INTOLERANTE
	5.2.11. [I.10] Degradación de los soportes de almacenamiento de la información	3	3	9	INTOLERANTE
	5.2.12. [I.11] Emanaciones electromagnéticas	3	3	9	INTOLERANTE
	5.3.1. [E.1] Errores de los usuarios	5	3	15	EXTREMO
	5.3.2. [E.2] Errores del administrador	4	5	20	EXTREMO

	5.3.10. [E.15] Alteración accidental de la información	4	3	12	EXTREMO
	5.3.11. [E.18] Destrucción de información	2	5	10	INTOLERANTE
	5.3.12. [E.19] Fugas de información	4	3	12	EXTREMO
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	15	EXTREMO
	5.3.17. [E.25] Pérdida de equipos	3	3	9	INTOLERANTE
	5.4.5. [A.7] Uso no previsto	4	3	12	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	3	9	INTOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	3	5	15	EXTREMO
	5.4.14. [A.18] Destrucción de información	2	5	10	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	3	5	15	EXTREMO
	5.4.17. [A.23] Manipulación de los equipos	2	3	6	TOLERANTE
	5.4.19. [A.25] Robo	2	5	10	INTOLERANTE
Syscom	5.4.20. [A.26] Ataque destructivo	1	5	5	TOLERANTE
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24	EXTREMO
	5.3.1. [E.1] Errores de los usuarios	5	5	25	EXTREMO
	5.3.2. [E.2] Errores del administrador	3	8	24	EXTREMO
	5.3.6. [E.8] Difusión de software dañino	2	8	16	EXTREMO
	5.3.7. [E.9] Errores de [re-]encaminamiento	2	8	16	EXTREMO
	5.3.8. [E.10] Errores de secuencia	2	8	16	EXTREMO
	5.3.10. [E.15] Alteración accidental de la información	4	8	32	EXTREMO
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	3	5	15	EXTREMO
	5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	8	24	EXTREMO
	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	8	32	EXTREMO

	5.4.3. [A.5] Suplantación de la identidad del usuario	3	8	24	EXTREMO
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	8	24	EXTREMO
	5.4.6. [A.8] Difusión de software dañino	2	8	16	EXTREMO
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	5	15	EXTREMO
	5.4.8. [A.10] Alteración de secuencia	3	8	24	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	2	8	16	EXTREMO
	5.4.15. [A.19] Divulgación de información	2	5	10	INTOLERANTE
	5.4.16. [A.22] Manipulación de programas	2	8	16	EXTREMO
Docuarchive	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24	EXTREMO
	5.3.1. [E.1] Errores de los usuarios	5	5	25	EXTREMO
	5.3.2. [E.2] Errores del administrador	3	8	24	EXTREMO
	5.3.6. [E.8] Difusión de software dañino	2	8	16	EXTREMO
	5.3.7. [E.9] Errores de [re-]encaminamiento	2	8	16	EXTREMO
	5.3.8. [E.10] Errores de secuencia	2	8	16	EXTREMO
	5.3.10. [E.15] Alteración accidental de la información	4	8	32	EXTREMO
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	3	5	15	EXTREMO
	5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	8	24	EXTREMO
	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	8	32	EXTREMO
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	8	24	EXTREMO
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	8	24	EXTREMO

	5.4.6. [A.8] Difusión de software dañino	2	8	16	EXTREMO
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	5	15	EXTREMO
	5.4.8. [A.10] Alteración de secuencia	3	8	24	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16	EXTREMO
	5.4.14. [A.18] Destrucción de información	2	8	16	EXTREMO
	5.4.15. [A.19] Divulgación de información	2	5	10	INTOLERANTE
	5.4.16. [A.22] Manipulación de programas	2	8	16	EXTREMO
Plataforma OCS Inventory	5.2.6. [I.5] Avería de origen físico o lógico	3	5	15	EXTREMO
	5.3.1. [E.1] Errores de los usuarios	5	2	10	INTOLERANTE
	5.3.2. [E.2] Errores del administrador	3	5	15	EXTREMO
	5.3.6. [E.8] Difusión de software dañino	2	5	10	INTOLERANTE
	5.3.7. [E.9] Errores de [re-]encaminamiento	2	5	10	INTOLERANTE
	5.3.8. [E.10] Errores de secuencia	2	3	6	TOLERANTE
	5.3.10. [E.15] Alteración accidental de la información	4	5	20	EXTREMO
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	3	5	15	EXTREMO
	5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	3	9	INTOLERANTE
	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	5	20	EXTREMO
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	15	EXTREMO
	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	15	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	3	9	INTOLERANTE
	5.4.6. [A.8] Difusión de software dañino	2	5	10	INTOLERANTE
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	5	15	EXTREMO

	5.4.8. [A.10] Alteración de secuencia	3	3	9	INTOLERANT E
	5.4.9. [A.11] Acceso no autorizado	3	5	15	EXTREMO
	5.4.13. [A.15] Modificación deliberada de la información	2	5	10	INTOLERANT E
	5.4.14. [A.18] Destrucción de información	2	8	16	EXTREMO
	5.4.15. [A.19] Divulgación de información	2	5	10	INTOLERANT E
	5.4.16. [A.22] Manipulación de programas	2	5	10	INTOLERANT E
Plataforma GLPI	5.2.6. [I.5] Avería de origen físico o lógico	3	3	9	INTOLERANT E
	5.3.1. [E.1] Errores de los usuarios	5	2	10	INTOLERANT E
	5.3.2. [E.2] Errores del administrador	3	3	9	INTOLERANT E
	5.3.6. [E.8] Difusión de software dañino	2	3	6	TOLERANTE
	5.3.7. [E.9] Errores de [re-]encaminamiento	2	3	6	TOLERANTE
	5.3.8. [E.10] Errores de secuencia	2	3	6	TOLERANTE
	5.3.10. [E.15] Alteración accidental de la información	4	3	12	EXTREMO
	5.3.11. [E.18] Destrucción de información	2	5	10	INTOLERANT E
	5.3.12. [E.19] Fugas de información	3	3	9	INTOLERANT E
	5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	3	9	INTOLERANT E
	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	3	12	EXTREMO
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	9	INTOLERANT E
	5.4.4. [A.6] Abuso de privilegios de acceso	3	3	9	INTOLERANT E
	5.4.5. [A.7] Uso no previsto	3	3	9	INTOLERANT E
	5.4.6. [A.8] Difusión de software dañino	2	3	6	TOLERANTE
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	3	9	INTOLERANT E

	5.4.8. [A.10] Alteración de secuencia	3	3	9	INTOLERANT E
	5.4.9. [A.11] Acceso no autorizado	3	3	9	INTOLERANT E
	5.4.13. [A.15] Modificación deliberada de la información	2	3	6	TOLERANTE
	5.4.14. [A.18] Destrucción de información	2	5	10	INTOLERANT E
	5.4.15. [A.19] Divulgación de información	2	3	6	TOLERANTE
	5.4.16. [A.22] Manipulación de programas	2	3	6	TOLERANTE
VPN Sophos	5.2.6. [I.5] Avería de origen físico o lógico	3	5	15	EXTREMO
	5.3.1. [E.1] Errores de los usuarios	5	2	10	INTOLERANT E
	5.3.2. [E.2] Errores del administrador	3	5	15	EXTREMO
	5.3.6. [E.8] Difusión de software dañino	2	5	10	INTOLERANT E
	5.3.7. [E.9] Errores de [re-]encaminamiento	2	5	10	INTOLERANT E
	5.3.8. [E.10] Errores de secuencia	2	3	6	TOLERANTE
	5.3.10. [E.15] Alteración accidental de la información	4	5	20	EXTREMO
	5.3.11. [E.18] Destrucción de información	2	8	16	EXTREMO
	5.3.12. [E.19] Fugas de información	3	5	15	EXTREMO
	5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	3	9	INTOLERANT E
	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	5	20	EXTREMO
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	15	EXTREMO
	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	15	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	3	9	INTOLERANT E
	5.4.6. [A.8] Difusión de software dañino	2	5	10	INTOLERANT E
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	5	15	EXTREMO
	5.4.8. [A.10] Alteración de secuencia	3	3	9	INTOLERANT E

	5.4.9. [A.11] Acceso no autorizado	3	5	15	EXTREMO
	5.4.13. [A.15] Modificación deliberada de la información	2	5	10	INTOLERANTE
	5.4.14. [A.18] Destrucción de información	2	8	16	EXTREMO
	5.4.15. [A.19] Divulgación de información	2	5	10	INTOLERANTE
	5.4.16. [A.22] Manipulación de programas	2	5	10	INTOLERANTE
Antivirus Kaspersky Office Small	5.2.6. [I.5] Avería de origen físico o lógico	3	5	15	EXTREMO
	5.3.1. [E.1] Errores de los usuarios	5	3	15	EXTREMO
	5.3.2. [E.2] Errores del administrador	3	5	15	EXTREMO
	5.3.6. [E.8] Difusión de software dañino	2	8	16	EXTREMO
	5.3.7. [E.9] Errores de [re-]encaminamiento	2	3	6	TOLERANTE
	5.3.8. [E.10] Errores de secuencia	2	3	6	TOLERANTE
	5.3.10. [E.15] Alteración accidental de la información	4	5	20	EXTREMO
	5.3.11. [E.18] Destrucción de información	2	5	10	INTOLERANTE
	5.3.12. [E.19] Fugas de información	3	3	9	INTOLERANTE
	5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	5	15	EXTREMO
	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	5	20	EXTREMO
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	15	EXTREMO
	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	15	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	5	15	EXTREMO
	5.4.6. [A.8] Difusión de software dañino	2	5	10	INTOLERANTE
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	5	15	EXTREMO
	5.4.8. [A.10] Alteración de secuencia	3	3	9	INTOLERANTE
	5.4.9. [A.11] Acceso no autorizado	3	5	15	EXTREMO
	5.4.13. [A.15] Modificación deliberada de la información	2	5	10	INTOLERANTE

	5.4.14. [A.18] Destrucción de información	2	5	10	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	2	5	10	INTOLERANTE
	5.4.16. [A.22] Manipulación de programas	2	5	10	INTOLERANTE
Director de T,I	5.3.5. [E.7] Deficiencias en la organización	4	5	20	EXTREMO
	5.3.18. [E.28] Indisponibilidad del personal	3	5	15	EXTREMO
	5.4.22. [A.28] Indisponibilidad del personal	2	5	10	INTOLERANTE
	5.4.23. [A.29] Extorsión	2	8	16	EXTREMO
	5.4.24. [A.30] Ingeniería social (picaresca)	2	8	16	EXTREMO
Auxiliar de T,I	5.3.5. [E.7] Deficiencias en la organización	4	3	12	EXTREMO
	5.3.18. [E.28] Indisponibilidad del personal	3	3	9	INTOLERANTE
	5.4.22. [A.28] Indisponibilidad del personal	2	5	10	INTOLERANTE
	5.4.23. [A.29] Extorsión	2	5	10	INTOLERANTE
	5.4.24. [A.30] Ingeniería social (picaresca)	2	8	16	EXTREMO
Consultor de T.I	5.3.5. [E.7] Deficiencias en la organización	5	3	15	EXTREMO
	5.3.18. [E.28] Indisponibilidad del personal	2	3	6	TOLERANTE
	5.4.22. [A.28] Indisponibilidad del personal	2	3	6	TOLERANTE
	5.4.23. [A.29] Extorsión	1	5	5	TOLERANTE
	5.4.24. [A.30] Ingeniería social (picaresca)	2	5	10	INTOLERANTE
Gerencia	5.3.5. [E.7] Deficiencias en la organización	2	8	16	EXTREMO
	5.3.18. [E.28] Indisponibilidad del personal	2	5	10	INTOLERANTE
	5.4.22. [A.28] Indisponibilidad del personal	2	5	10	INTOLERANTE
	5.4.23. [A.29] Extorsión	1	8	8	INTOLERANTE
	5.4.24. [A.30] Ingeniería social (picaresca)	1	5	5	TOLERANTE

Correo Microsoft Office 365	5.3.1. [E.1] Errores de los usuarios	5	3	15	EXTREMO
	5.3.2. [E.2] Errores del administrador	3	5	15	EXTREMO
	5.3.7. [E.9] Errores de [re-]encaminamiento	4	3	12	EXTREMO
	5.3.8. [E.10] Errores de secuencia	4	3	12	EXTREMO
	5.3.10. [E.15] Alteración accidental de la información	5	3	15	EXTREMO
	5.3.11. [E.18] Destrucción de información	4	5	20	EXTREMO
	5.3.12. [E.19] Fugas de información	4	3	12	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	5	15	EXTREMO
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	15	EXTREMO
	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	15	EXTREMO
	5.4.5. [A.7] Uso no previsto	4	3	12	EXTREMO
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	4	3	12	EXTREMO
	5.4.8. [A.10] Alteración de secuencia	3	3	9	INTOLERANTE
	5.4.9. [A.11] Acceso no autorizado	3	3	9	INTOLERANTE
	5.4.11. [A.13] Repudio	3	3	9	INTOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	3	5	15	EXTREMO
	5.4.14. [A.18] Destrucción de información	3	5	15	EXTREMO
	5.4.15. [A.19] Divulgación de información	3	3	9	INTOLERANTE
	5.4.18. [A.24] Denegación de servicio	3	5	15	EXTREMO
Dominio	5.3.1. [E.1] Errores de los usuarios	5	3	15	EXTREMO
	5.3.2. [E.2] Errores del administrador	3	8	24	EXTREMO
	5.3.7. [E.9] Errores de [re-]encaminamiento	4	3	12	EXTREMO
	5.3.8. [E.10] Errores de secuencia	4	3	12	EXTREMO
	5.3.10. [E.15] Alteración accidental de la información	4	5	20	EXTREMO
	5.3.11. [E.18] Destrucción de información	4	8	32	EXTREMO
	5.3.12. [E.19] Fugas de información	4	8	32	EXTREMO

	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	8	24	EXTREMO
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	8	24	EXTREMO
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24	EXTREMO
	5.4.5. [A.7] Uso no previsto	4	8	32	EXTREMO
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	4	5	20	EXTREMO
	5.4.8. [A.10] Alteración de secuencia	3	3	9	INTOLERANTE
	5.4.9. [A.11] Acceso no autorizado	3	5	15	EXTREMO
	5.4.11. [A.13] Repudio	3	8	24	EXTREMO
	5.4.13. [A.15] Modificación deliberada de la información	3	8	24	EXTREMO
	5.4.14. [A.18] Destrucción de información	3	8	24	EXTREMO
	5.4.15. [A.19] Divulgación de información	3	8	24	EXTREMO
	5.4.18. [A.24] Denegación de servicio	3	8	24	EXTREMO
Hosting	5.3.1. [E.1] Errores de los usuarios	4	3	12	EXTREMO
	5.3.2. [E.2] Errores del administrador	3	5	15	EXTREMO
	5.3.7. [E.9] Errores de [re-]encaminamiento	3	3	9	INTOLERANTE
	5.3.8. [E.10] Errores de secuencia	3	3	9	INTOLERANTE
	5.3.10. [E.15] Alteración accidental de la información	4	5	20	EXTREMO
	5.3.11. [E.18] Destrucción de información	4	5	20	EXTREMO
	5.3.12. [E.19] Fugas de información	3	5	15	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	5	15	EXTREMO
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	15	EXTREMO
	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	15	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	5	15	EXTREMO
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	3	9	INTOLERANTE
	5.4.8. [A.10] Alteración de secuencia	3	3	9	INTOLERANTE
	5.4.9. [A.11] Acceso no autorizado	3	5	15	EXTREMO

	5.4.11. [A.13] Repudio	3	5	15	EXTREMO
	5.4.13. [A.15] Modificación deliberada de la información	3	5	15	EXTREMO
	5.4.14. [A.18] Destrucción de información	2	5	10	INTOLERANTE
	5.4.15. [A.19] Divulgación de información	3	5	15	EXTREMO
	5.4.18. [A.24] Denegación de servicio	3	5	15	EXTREMO
Almacenamiento Nube	5.3.1. [E.1] Errores de los usuarios	5	3	15	EXTREMO
	5.3.2. [E.2] Errores del administrador	3	5	15	EXTREMO
	5.3.7. [E.9] Errores de [re-]encaminamiento	4	3	12	EXTREMO
	5.3.8. [E.10] Errores de secuencia	4	3	12	EXTREMO
	5.3.10. [E.15] Alteración accidental de la información	5	3	15	EXTREMO
	5.3.11. [E.18] Destrucción de información	4	8	32	EXTREMO
	5.3.12. [E.19] Fugas de información	4	3	12	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	5	15	EXTREMO
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	8	24	EXTREMO
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24	EXTREMO
	5.4.5. [A.7] Uso no previsto	4	3	12	EXTREMO
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	4	3	12	EXTREMO
	5.4.8. [A.10] Alteración de secuencia	3	3	9	INTOLERANTE
	5.4.9. [A.11] Acceso no autorizado	3	3	9	INTOLERANTE
	5.4.11. [A.13] Repudio	3	3	9	INTOLERANTE
	5.4.13. [A.15] Modificación deliberada de la información	3	5	15	EXTREMO
	5.4.14. [A.18] Destrucción de información	3	8	24	EXTREMO
	5.4.15. [A.19] Divulgación de información	3	8	24	EXTREMO
	5.4.18. [A.24] Denegación de servicio	3	5	15	EXTREMO
Virtualización	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	4	8	32	EXTREMO

	5.3.7. [E.9] Errores de [re-]encaminamiento	3	5	15	EXTREMO
	5.3.8. [E.10] Errores de secuencia	3	5	15	EXTREMO
	5.3.10. [E.15] Alteración accidental de la información	4	8	32	EXTREMO
	5.3.11. [E.18] Destrucción de información	4	8	32	EXTREMO
	5.3.12. [E.19] Fugas de información	3	8	24	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	8	24	EXTREMO
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	8	24	EXTREMO
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	8	24	EXTREMO
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	5	15	EXTREMO
	5.4.8. [A.10] Alteración de secuencia	3	5	15	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.11. [A.13] Repudio	3	5	15	EXTREMO
	5.4.13. [A.15] Modificación deliberada de la información	3	8	24	EXTREMO
	5.4.14. [A.18] Destrucción de información	2	8	16	EXTREMO
	5.4.15. [A.19] Divulgación de información	3	8	24	EXTREMO
	5.4.18. [A.24] Denegación de servicio	3	8	24	EXTREMO
RDS	5.3.1. [E.1] Errores de los usuarios	4	5	20	EXTREMO
	5.3.2. [E.2] Errores del administrador	4	8	32	EXTREMO
	5.3.7. [E.9] Errores de [re-]encaminamiento	3	5	15	EXTREMO
	5.3.8. [E.10] Errores de secuencia	3	5	15	EXTREMO
	5.3.10. [E.15] Alteración accidental de la información	4	8	32	EXTREMO
	5.3.11. [E.18] Destrucción de información	4	8	32	EXTREMO
	5.3.12. [E.19] Fugas de información	3	8	24	EXTREMO
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	8	24	EXTREMO
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	8	24	EXTREMO

	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	8	24	EXTREMO
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	5	15	EXTREMO
	5.4.8. [A.10] Alteración de secuencia	3	5	15	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.11. [A.13] Repudio	3	5	15	EXTREMO
	5.4.13. [A.15] Modificación deliberada de la información	3	8	24	EXTREMO
	5.4.14. [A.18] Destrucción de información	2	8	16	EXTREMO
	5.4.15. [A.19] Divulgación de información	3	8	24	EXTREMO
	5.4.18. [A.24] Denegación de servicio	3	8	24	EXTREMO
AIRE ACONDICIONADO O CUARTO DE EQUIPOS.	5.1.1. [N.1] Fuego	1	8	8	INTOLERANTE
	5.1.2. [N.2] Daños por agua	2	8	16	EXTREMO
	5.1.3. [N.*] Desastres naturales	2	8	16	EXTREMO
	5.2.1. [I.1] Fuego	2	8	16	EXTREMO
	5.2.2. [I.2] Daños por agua	2	8	16	EXTREMO
	5.2.3. [I.*] Desastres industriales	2	8	16	EXTREMO
	5.2.4. [I.3] Contaminación mecánica	3	8	24	EXTREMO
	5.2.5. [I.4] Contaminación electromagnética	3	8	24	EXTREMO
	5.2.6. [I.5] Avería de origen físico o lógico	4	8	32	EXTREMO
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32	EXTREMO
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24	EXTREMO
	5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	3	8	24	EXTREMO
	5.2.12. [I.11] Emanaciones electromagnéticas	3	8	24	EXTREMO
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	8	24	EXTREMO
	5.3.17. [E.25] Pérdida de equipos	3	8	24	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	1	3	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	3	1	3	TOLERANTE

	5.4.17. [A.23] Manipulación de los equipos	3	8	24	EXTREMO
	5.4.19. [A.25] Robo	3	8	24	EXTREMO
	5.4.20. [A.26] Ataque destructivo	1	8	8	INTOLERANTE
UPS	5.1.1. [N.1] Fuego	2	8	16	EXTREMO
	5.1.2. [N.2] Daños por agua	2	8	16	EXTREMO
	5.1.3. [N.*] Desastres naturales	2	8	16	EXTREMO
	5.2.1. [I.1] Fuego	2	8	16	EXTREMO
	5.2.2. [I.2] Daños por agua	2	8	16	EXTREMO
	5.2.3. [I.*] Desastres industriales	2	8	16	EXTREMO
	5.2.4. [I.3] Contaminación mecánica	4	8	32	EXTREMO
	5.2.5. [I.4] Contaminación electromagnética	4	8	32	EXTREMO
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24	EXTREMO
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32	EXTREMO
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24	EXTREMO
	5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	3	8	24	EXTREMO
	5.2.12. [I.11] Emanaciones electromagnéticas	3	8	24	EXTREMO
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	8	24	EXTREMO
	5.3.17. [E.25] Pérdida de equipos	2	8	16	EXTREMO
	5.4.5. [A.7] Uso no previsto	2	8	16	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.17. [A.23] Manipulación de los equipos	3	8	24	EXTREMO
	5.4.19. [A.25] Robo	2	8	16	EXTREMO
	5.4.20. [A.26] Ataque destructivo	2	8	16	EXTREMO
PLANTA ELECTRICA	5.1.1. [N.1] Fuego	1	8	8	INTOLERANTE
	5.1.2. [N.2] Daños por agua	2	8	16	EXTREMO
	5.1.3. [N.*] Desastres naturales	2	8	16	EXTREMO
	5.2.1. [I.1] Fuego	2	8	16	EXTREMO
	5.2.2. [I.2] Daños por agua	2	8	16	EXTREMO
	5.2.3. [I.*] Desastres industriales	2	8	16	EXTREMO

	5.2.4. [I.3] Contaminación mecánica	4	8	32	EXTREMO
	5.2.5. [I.4] Contaminación electromagnética	4	8	32	EXTREMO
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24	EXTREMO
	5.2.7. [I.6] Corte del suministro eléctrico	3	8	24	EXTREMO
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24	EXTREMO
	5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	3	8	24	EXTREMO
	5.2.12. [I.11] Emanaciones electromagnéticas	3	8	24	EXTREMO
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	8	24	EXTREMO
	5.3.17. [E.25] Pérdida de equipos	2	8	16	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	5	15	EXTREMO
	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.17. [A.23] Manipulación de los equipos	3	8	24	EXTREMO
	5.4.19. [A.25] Robo	3	8	24	EXTREMO
	5.4.20. [A.26] Ataque destructivo	2	8	16	EXTREMO
Data Center	5.1.1. [N.1] Fuego	2	8	16	EXTREMO
	5.1.2. [N.2] Daños por agua	2	8	16	EXTREMO
	5.2.1. [I.1] Fuego	2	8	16	EXTREMO
	5.2.2. [I.2] Daños por agua	2	8	16	EXTREMO
	5.2.3. [I.*] Desastres industriales	2	8	16	EXTREMO
	5.2.12. [I.11] Emanaciones electromagnéticas	3	8	24	EXTREMO
	5.3.10. [E.15] Alteración accidental de la información	3	8	24	EXTREMO
	5.3.11. [E.18] Destrucción de información	3	8	24	EXTREMO
	5.3.12. [E.19] Fugas de información	3	5	15	EXTREMO
	5.4.5. [A.7] Uso no previsto	3	2	6	TOLERANTE
	5.4.9. [A.11] Acceso no autorizado	3	8	24	EXTREMO
	5.4.13. [A.15] Modificación deliberada de la información	3	5	15	EXTREMO
	5.4.14. [A.18] Destrucción de información	2	8	16	EXTREMO

	5.4.15. [A.19] Divulgación de información	3	8	24	EXTREMO
	5.4.20. [A.26] Ataque destructivo	1	8	8	INTOLERANTE
	5.4.21. [A.27] Ocupación enemiga	1	8	8	INTOLERANTE

Apéndice C

Activos Críticos Transportes Gayco

ACTIVO	AMENZAS	FRECUENCIA	DAÑO/IMPACTO (VALOR)	RIESGO CUANTITATIVO	TOTAL RIESGO CUANTITATIVO POR ACTIVO	TOTAL RIESGO CUALITATIVO POR ACTIVO
Gestion Documental	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE
	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		
Almacen	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE

	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		
Compras	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE
	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		

Contabilidad	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE
	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		
Facturacion	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE
	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		

	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		
Gerencia	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE
	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		
Gerencia 2021	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE
	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		

	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		
Gerencia Gayco	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE
	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		
Gestion Comercial	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE
	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		

	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		
HSEQ	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE
	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		
Mantenimiento	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE
	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		

	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		
Operaciones	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE
	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		
Proveedores 2022	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE

	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		
Seguridad Física	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE
	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		

	5.4.15. [A.19] Divulgación de información	1	1	1		
Sistema de Gestion	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE
	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		
Talento Humano	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE
	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		

	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		
Tesoreria	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE
	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		
	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		
Vehiculos	5.3.1. [E.1] Errores de los usuarios	4	5	20	92	TOLERANTE
	5.3.2. [E.2] Errores del administrador	1	1	1		
	5.3.10. [E.15] Alteración accidental de la información	2	5	10		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	2	3	6		
	5.4.3. [A.5] Suplantación de la identidad del usuario	2	3	6		

	5.4.4. [A.6] Abuso de privilegios de acceso	1	3	3		
	5.4.9. [A.11] Acceso no autorizado	1	5	5		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	1	8	8		
	5.4.15. [A.19] Divulgación de información	1	1	1		
Bitlocker discos externos	5.3.1. [E.1] Errores de los usuarios	4	5	20	200	INTOLERANTE
	5.3.2. [E.2] Errores del administrador	4	5	20		
	5.3.10. [E.15] Alteración accidental de la información	4	5	20		
	5.3.11. [E.18] Destrucción de información	3	8	24		
	5.3.12. [E.19] Fugas de información	4	5	20		
	5.4.3. [A.5] Suplantación de la identidad del usuario	4	5	20		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	15		
	5.4.9. [A.11] Acceso no autorizado	3	5	15		
	5.4.13. [A.15] Modificación deliberada de la información	3	5	15		
	5.4.14. [A.18] Destrucción de información	2	8	16		
	5.4.15. [A.19] Divulgación de información	3	5	15		
Servidor ecoplanta	5.1.1. [N.1] Fuego	1	8	8	373	EXTREMO
	5.1.2. [N.2] Daños por agua	1	8	8		
	5.1.3. [N.*] Desastres naturales	1	8	8		
	5.2.1. [I.1] Fuego	1	8	8		
	5.2.2. [I.2] Daños por agua	1	8	8		
	5.2.3. [I.*] Desastres industriales	2	8	16		

	5.2.4. [I.3] Contaminación mecánica	3	5	15		
	5.2.5. [I.4] Contaminación electromagnética	3	5	15		
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24		
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32		
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24		
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15		
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	8	32		
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	8	16		
	5.3.17. [E.25] Pérdida de equipos	1	8	8		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24		
	5.4.5. [A.7] Uso no previsto	3	8	24		
	5.4.9. [A.11] Acceso no autorizado	3	8	24		
	5.4.17. [A.23] Manipulación de los equipos	3	8	24		
	5.4.18. [A.24] Denegación de servicio	3	8	24		
	5.4.19. [A.25] Robo	1	8	8		
	5.4.20. [A.26] Ataque destructivo	1	8	8		
Servidor hipervisor	5.1.1. [N.1] Fuego	1	8	8	373	EXTREMO
	5.1.2. [N.2] Daños por agua	1	8	8		
	5.1.3. [N.*] Desastres naturales	1	8	8		
	5.2.1. [I.1] Fuego	1	8	8		
	5.2.2. [I.2] Daños por agua	1	8	8		

	5.2.3. [I.*] Desastres industriales	2	8	16		
	5.2.4. [I.3] Contaminación mecánica	3	5	15		
	5.2.5. [I.4] Contaminación electromagnética	3	5	15		
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24		
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32		
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24		
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15		
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	8	32		
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	8	16		
	5.3.17. [E.25] Pérdida de equipos	1	8	8		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24		
	5.4.5. [A.7] Uso no previsto	3	8	24		
	5.4.9. [A.11] Acceso no autorizado	3	8	24		
	5.4.17. [A.23] Manipulación de los equipos	3	8	24		
	5.4.18. [A.24] Denegación de servicio	3	8	24		
	5.4.19. [A.25] Robo	1	8	8		
	5.4.20. [A.26] Ataque destructivo	1	8	8		
Servidor Dominio	5.1.1. [N.1] Fuego	1	8	8	373	EXTREMO
	5.1.2. [N.2] Daños por agua	1	8	8		
	5.1.3. [N.*] Desastres naturales	1	8	8		
	5.2.1. [I.1] Fuego	1	8	8		
	5.2.2. [I.2] Daños por agua	1	8	8		

	5.2.3. [I.*] Desastres industriales	2	8	16		
	5.2.4. [I.3] Contaminación mecánica	3	5	15		
	5.2.5. [I.4] Contaminación electromagnética	3	5	15		
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24		
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32		
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24		
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15		
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	8	32		
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	8	16		
	5.3.17. [E.25] Pérdida de equipos	1	8	8		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24		
	5.4.5. [A.7] Uso no previsto	3	8	24		
	5.4.9. [A.11] Acceso no autorizado	3	8	24		
	5.4.17. [A.23] Manipulación de los equipos	3	8	24		
	5.4.18. [A.24] Denegación de servicio	3	8	24		
	5.4.19. [A.25] Robo	1	8	8		
	5.4.20. [A.26] Ataque destructivo	1	8	8		
Servidores de archivos	5.1.1. [N.1] Fuego	1	8	8	373	EXTREMO
	5.1.2. [N.2] Daños por agua	1	8	8		
	5.1.3. [N.*] Desastres naturales	1	8	8		
	5.2.1. [I.1] Fuego	1	8	8		
	5.2.2. [I.2] Daños por agua	1	8	8		

	5.2.3. [I.*] Desastres industriales	2	8	16		
	5.2.4. [I.3] Contaminación mecánica	3	5	15		
	5.2.5. [I.4] Contaminación electromagnética	3	5	15		
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24		
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32		
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24		
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15		
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	8	32		
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	8	16		
	5.3.17. [E.25] Pérdida de equipos	1	8	8		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24		
	5.4.5. [A.7] Uso no previsto	3	8	24		
	5.4.9. [A.11] Acceso no autorizado	3	8	24		
	5.4.17. [A.23] Manipulación de los equipos	3	8	24		
	5.4.18. [A.24] Denegación de servicio	3	8	24		
	5.4.19. [A.25] Robo	1	8	8		
	5.4.20. [A.26] Ataque destructivo	1	8	8		
Servidor Solucionar	5.1.1. [N.1] Fuego	1	8	8	373	EXTREMO
	5.1.2. [N.2] Daños por agua	1	8	8		
	5.1.3. [N.*] Desastres naturales	1	8	8		
	5.2.1. [I.1] Fuego	1	8	8		
	5.2.2. [I.2] Daños por agua	1	8	8		
	5.2.3. [I.*] Desastres industriales	2	8	16		

	5.2.4. [I.3] Contaminación mecánica	3	5	15		
	5.2.5. [I.4] Contaminación electromagnética	3	5	15		
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24		
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32		
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24		
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15		
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	8	32		
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	8	16		
	5.3.17. [E.25] Pérdida de equipos	1	8	8		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24		
	5.4.5. [A.7] Uso no previsto	3	8	24		
	5.4.9. [A.11] Acceso no autorizado	3	8	24		
	5.4.17. [A.23] Manipulación de los equipos	3	8	24		
	5.4.18. [A.24] Denegación de servicio	3	8	24		
	5.4.19. [A.25] Robo	1	8	8		
	5.4.20. [A.26] Ataque destructivo	1	8	8		
Switch administrable	5.1.1. [N.1] Fuego	1	8	8	373	EXTREMO
	5.1.2. [N.2] Daños por agua	1	8	8		
	5.1.3. [N.*] Desastres naturales	1	8	8		
	5.2.1. [I.1] Fuego	1	8	8		
	5.2.2. [I.2] Daños por agua	1	8	8		

	5.2.3. [I.*] Desastres industriales	2	8	16		
	5.2.4. [I.3] Contaminación mecánica	3	5	15		
	5.2.5. [I.4] Contaminación electromagnética	3	5	15		
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24		
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32		
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24		
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15		
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	8	32		
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	8	16		
	5.3.17. [E.25] Pérdida de equipos	1	8	8		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24		
	5.4.5. [A.7] Uso no previsto	3	8	24		
	5.4.9. [A.11] Acceso no autorizado	3	8	24		
	5.4.17. [A.23] Manipulación de los equipos	3	8	24		
	5.4.18. [A.24] Denegación de servicio	3	8	24		
	5.4.19. [A.25] Robo	1	8	8		
	5.4.20. [A.26] Ataque destructivo	1	8	8		
Switch almacén	5.1.1. [N.1] Fuego	1	5	5	189	INTOLERANTE
	5.1.2. [N.2] Daños por agua	1	5	5		
	5.1.3. [N.*] Desastres naturales	1	5	5		
	5.2.1. [I.1] Fuego	1	5	5		

	5.2.2. [I.2] Daños por agua	1	5	5		
	5.2.3. [I.*] Desastres industriales	3	5	15		
	5.2.4. [I.3] Contaminación mecánica	4	2	8		
	5.2.5. [I.4] Contaminación electromagnética	3	2	6		
	5.2.6. [I.5] Avería de origen físico o lógico	3	5	15		
	5.2.7. [I.6] Corte del suministro eléctrico	4	3	12		
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	4	3	12		
	5.2.12. [I.11] Emanaciones electromagnéticas	3	2	6		
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	3	12		
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	5	10		
	5.3.17. [E.25] Pérdida de equipos	1	5	5		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	2	6		
	5.4.5. [A.7] Uso no previsto	3	3	9		
	5.4.9. [A.11] Acceso no autorizado	3	3	9		
	5.4.17. [A.23] Manipulación de los equipos	3	3	9		
	5.4.18. [A.24] Denegación de servicio	3	5	15		
	5.4.19. [A.25] Robo	2	5	10		
	5.4.20. [A.26] Ataque destructivo	1	5	5		
UTM	5.1.1. [N.1] Fuego	1	8	8	373	EXTREMO
	5.1.2. [N.2] Daños por agua	1	8	8		
	5.1.3. [N.*] Desastres naturales	1	8	8		

	5.2.1. [I.1] Fuego	1	8	8		
	5.2.2. [I.2] Daños por agua	1	8	8		
	5.2.3. [I.*] Desastres industriales	2	8	16		
	5.2.4. [I.3] Contaminación mecánica	3	5	15		
	5.2.5. [I.4] Contaminación electromagnética	3	5	15		
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24		
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32		
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24		
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15		
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	8	32		
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	8	16		
	5.3.17. [E.25] Pérdida de equipos	1	8	8		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24		
	5.4.5. [A.7] Uso no previsto	3	8	24		
	5.4.9. [A.11] Acceso no autorizado	3	8	24		
	5.4.17. [A.23] Manipulación de los equipos	3	8	24		
	5.4.18. [A.24] Denegación de servicio	3	8	24		
	5.4.19. [A.25] Robo	1	8	8		
	5.4.20. [A.26] Ataque destructivo	1	8	8		
Router proveedores	5.1.1. [N.1] Fuego	1	8	8	373	EXTREMO
	5.1.2. [N.2] Daños por agua	1	8	8		

	5.1.3. [N.*] Desastres naturales	1	8	8		
	5.2.1. [I.1] Fuego	1	8	8		
	5.2.2. [I.2] Daños por agua	1	8	8		
	5.2.3. [I.*] Desastres industriales	2	8	16		
	5.2.4. [I.3] Contaminación mecánica	3	5	15		
	5.2.5. [I.4] Contaminación electromagnética	3	5	15		
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24		
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32		
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24		
	5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15		
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	8	32		
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	8	16		
	5.3.17. [E.25] Pérdida de equipos	1	8	8		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24		
	5.4.5. [A.7] Uso no previsto	3	8	24		
	5.4.9. [A.11] Acceso no autorizado	3	8	24		
	5.4.17. [A.23] Manipulación de los equipos	3	8	24		
	5.4.18. [A.24] Denegación de servicio	3	8	24		
	5.4.19. [A.25] Robo	1	8	8		
	5.4.20. [A.26] Ataque destructivo	1	8	8		
Acces Point	5.1.1. [N.1] Fuego	1	5	5	192	INTOLERANTE

5.1.2. [N.2] Daños por agua	1	5	5
5.1.3. [N.*] Desastres naturales	1	5	5
5.2.1. [I.1] Fuego	1	5	5
5.2.2. [I.2] Daños por agua	1	5	5
5.2.3. [I.*] Desastres industriales	2	5	10
5.2.4. [I.3] Contaminación mecánica	3	2	6
5.2.5. [I.4] Contaminación electromagnética	3	5	15
5.2.6. [I.5] Avería de origen físico o lógico	3	5	15
5.2.7. [I.6] Corte del suministro eléctrico	4	3	12
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	3	9
5.2.12. [I.11] Emanaciones electromagnéticas	3	5	15
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	3	12
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	5	10
5.3.17. [E.25] Pérdida de equipos	1	5	5
5.4.4. [A.6] Abuso de privilegios de acceso	3	2	6
5.4.5. [A.7] Uso no previsto	3	3	9
5.4.9. [A.11] Acceso no autorizado	3	3	9
5.4.17. [A.23] Manipulación de los equipos	3	3	9
5.4.18. [A.24] Denegación de servicio	3	5	15
5.4.19. [A.25] Robo	1	5	5
5.4.20. [A.26] Ataque destructivo	1	5	5

Monitores	5.1.1. [N.1] Fuego	1	2	2	88	TOLERANTE
	5.1.2. [N.2] Daños por agua	1	2	2		
	5.1.3. [N.*] Desastres naturales	1	2	2		
	5.2.1. [I.1] Fuego	1	2	2		
	5.2.2. [I.2] Daños por agua	1	2	2		
	5.2.3. [I.*] Desastres industriales	2	2	4		
	5.2.4. [I.3] Contaminación mecánica	3	1	3		
	5.2.5. [I.4] Contaminación electromagnética	3	1	3		
	5.2.6. [I.5] Avería de origen físico o lógico	3	2	6		
	5.2.7. [I.6] Corte del suministro eléctrico	4	2	8		
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	1	3		
	5.2.12. [I.11] Emanaciones electromagnéticas	3	2	6		
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	4	1	4		
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	1	2		
	5.3.17. [E.25] Pérdida de equipos	1	3	3		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	1	3		
	5.4.5. [A.7] Uso no previsto	3	2	6		
	5.4.9. [A.11] Acceso no autorizado	3	3	9		
	5.4.17. [A.23] Manipulación de los equipos	3	3	9		
	5.4.18. [A.24] Denegación de servicio	3	1	3		
	5.4.19. [A.25] Robo	1	3	3		

	5.4.20. [A.26] Ataque destructivo	1	3	3		
LAN	5.2.9. [I.8] Fallo de servicios de comunicaciones	3	5	15	306	EXTREMO
	5.3.2. [E.2] Errores del administrador	3	3	9		
	5.3.7. [E.9] Errores de [re-]encaminamiento	2	3	6		
	5.3.8. [E.10] Errores de secuencia	2	3	6		
	5.3.10. [E.15] Alteración accidental de la información	4	3	12		
	5.3.11. [E.18] Destrucción de información	3	8	24		
	5.3.12. [E.19] Fugas de información	4	5	20		
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	8	24		
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	15		
	5.4.4. [A.6] Abuso de privilegios de acceso	4	5	20		
	5.4.5. [A.7] Uso no previsto	5	5	25		
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	3	9		
	5.4.8. [A.10] Alteración de secuencia	4	3	12		
	5.4.9. [A.11] Acceso no autorizado	3	5	15		
	5.4.10. [A.12] Análisis de tráfico	3	5	15		
	5.4.12. [A.14] Interceptación de información (escucha)	3	5	15		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.15. [A.19] Divulgación de información	3	8	24		
	5.4.18. [A.24] Denegación de servicio	3	8	24		
Internet Empresarial Backup	5.2.9. [I.8] Fallo de servicios de comunicaciones	4	8	32	388	EXTREMO
	5.3.2. [E.2] Errores del administrador	3	5	15		

	5.3.7. [E.9] Errores de [re-]encaminamiento	3	5	15		
	5.3.8. [E.10] Errores de secuencia	3	5	15		
	5.3.10. [E.15] Alteración accidental de la información	3	5	15		
	5.3.11. [E.18] Destrucción de información	3	5	15		
	5.3.12. [E.19] Fugas de información	3	8	24		
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	8	24		
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	8	24		
	5.4.4. [A.6] Abuso de privilegios de acceso	2	8	16		
	5.4.5. [A.7] Uso no previsto	5	8	40		
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	4	5	20		
	5.4.8. [A.10] Alteración de secuencia	3	5	15		
	5.4.9. [A.11] Acceso no autorizado	3	8	24		
	5.4.10. [A.12] Análisis de tráfico	3	5	15		
	5.4.12. [A.14] Interceptación de información (escucha)	3	5	15		
	5.4.13. [A.15] Modificación deliberada de la información	3	8	24		
	5.4.15. [A.19] Divulgación de información	2	8	16		
	5.4.18. [A.24] Denegación de servicio	3	8	24		
Internet Empresarial	5.2.9. [I.8] Fallo de servicios de comunicaciones	4	8	32	444	EXTREMO
	5.3.2. [E.2] Errores del administrador	4	5	20		

	5.3.7. [E.9] Errores de [re-]encaminamiento	4	5	20		
	5.3.8. [E.10] Errores de secuencia	4	5	20		
	5.3.10. [E.15] Alteración accidental de la información	4	5	20		
	5.3.11. [E.18] Destrucción de información	3	8	24		
	5.3.12. [E.19] Fugas de información	4	5	20		
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	4	8	32		
	5.4.3. [A.5] Suplantación de la identidad del usuario	4	8	32		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	15		
	5.4.5. [A.7] Uso no previsto	5	5	25		
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	4	5	20		
	5.4.8. [A.10] Alteración de secuencia	4	5	20		
	5.4.9. [A.11] Acceso no autorizado	3	8	24		
	5.4.10. [A.12] Análisis de tráfico	3	8	24		
	5.4.12. [A.14] Interceptación de información (escucha)	3	8	24		
	5.4.13. [A.15] Modificación deliberada de la información	3	8	24		
	5.4.15. [A.19] Divulgación de información	3	8	24		
	5.4.18. [A.24] Denegación de servicio	3	8	24		
Red Inalambrica	5.2.9. [I.8] Fallo de servicios de comunicaciones	4	5	20	312	EXTREMO

	5.3.2. [E.2] Errores del administrador	3	3	9	259	INTOLERANTE
	5.3.7. [E.9] Errores de [re-]encaminamiento	3	3	9		
	5.3.8. [E.10] Errores de secuencia	3	3	9		
	5.3.10. [E.15] Alteración accidental de la información	4	3	12		
	5.3.11. [E.18] Destrucción de información	3	8	24		
	5.3.12. [E.19] Fugas de información	4	5	20		
	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	8	24		
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	15		
	5.4.4. [A.6] Abuso de privilegios de acceso	4	5	20		
	5.4.5. [A.7] Uso no previsto	4	5	20		
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	3	9		
	5.4.8. [A.10] Alteración de secuencia	4	3	12		
	5.4.9. [A.11] Acceso no autorizado	3	5	15		
	5.4.10. [A.12] Análisis de tráfico	3	5	15		
	5.4.12. [A.14] Interceptación de información (escucha)	3	5	15		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.15. [A.19] Divulgación de información	3	8	24		
	5.4.18. [A.24] Denegación de servicio	3	8	24		
Disco Duro Externo	5.1.1. [N.1] Fuego	1	5	5	259	INTOLERANTE

	5.1.2. [N.2] Daños por agua	1	5	5
	5.1.3. [N.*] Desastres naturales	1	5	5
	5.2.1. [I.1] Fuego	1	5	5
	5.2.2. [I.2] Daños por agua	1	5	5
	5.2.3. [I.*] Desastres industriales	1	5	5
	5.2.4. [I.3] Contaminación mecánica	3	3	9
	5.2.5. [I.4] Contaminación electromagnética	3	3	9
	5.2.6. [I.5] Avería de origen físico o lógico	3	5	15
	5.2.7. [I.6] Corte del suministro eléctrico	4	2	8
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	2	6
	5.2.11. [I.10] Degradación de los soportes de almacenamiento de la información	3	5	15
	5.2.12. [I.11] Emanaciones electromagnéticas	3	3	9
	5.3.1. [E.1] Errores de los usuarios	3	3	9
	5.3.2. [E.2] Errores del administrador	3	5	15
	5.3.10. [E.15] Alteración accidental de la información	3	5	15
	5.3.11. [E.18] Destrucción de información	2	5	10
	5.3.12. [E.19] Fugas de información	3	5	15
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	3	6
	5.3.17. [E.25] Pérdida de equipos	3	5	15
	5.4.5. [A.7] Uso no previsto	2	3	6
	5.4.9. [A.11] Acceso no autorizado	2	3	6
	5.4.13. [A.15] Modificación deliberada de la información	2	5	10

	5.4.14. [A.18] Destrucción de información	2	5	10		
	5.4.15. [A.19] Divulgación de información	2	5	10		
	5.4.17. [A.23] Manipulación de los equipos	2	3	6		
	5.4.19. [A.25] Robo	3	5	15		
	5.4.20. [A.26] Ataque destructivo	2	5	10		
Servidor Nas Soluxionar	5.1.1. [N.1] Fuego	1	8	8	440	EXTREMO
	5.1.2. [N.2] Daños por agua	1	8	8		
	5.1.3. [N.*] Desastres naturales	1	8	8		
	5.2.1. [I.1] Fuego	1	8	8		
	5.2.2. [I.2] Daños por agua	1	8	8		
	5.2.3. [I.*] Desastres industriales	1	8	8		
	5.2.4. [I.3] Contaminación mecánica	3	5	15		
	5.2.5. [I.4] Contaminación electromagnética	3	5	15		
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24		
	5.2.7. [I.6] Corte del suministro eléctrico	4	5	20		
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	3	9		
	5.2.11. [I.10] Degradación de los soportes de almacenamiento de la información	3	5	15		
	5.2.12. [I.11] Emanaciones electromagnéticas	3	3	9		
	5.3.1. [E.1] Errores de los usuarios	5	5	25		
	5.3.2. [E.2] Errores del administrador	4	8	32		
	5.3.10. [E.15] Alteración accidental de la información	4	5	20		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	4	5	20		

	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	15		
	5.3.17. [E.25] Pérdida de equipos	3	8	24		
	5.4.5. [A.7] Uso no previsto	4	5	20		
	5.4.9. [A.11] Acceso no autorizado	3	5	15		
	5.4.13. [A.15] Modificación deliberada de la información	3	8	24		
	5.4.14. [A.18] Destrucción de información	2	8	16		
	5.4.15. [A.19] Divulgación de información	3	8	24		
	5.4.17. [A.23] Manipulación de los equipos	2	5	10		
	5.4.19. [A.25] Robo	2	8	16		
	5.4.20. [A.26] Ataque destructivo	1	8	8		
Servidor NAS Ecoplanta	5.1.1. [N.1] Fuego	1	5	5	277	INTOLERANTE
	5.1.2. [N.2] Daños por agua	1	5	5		
	5.1.3. [N.*] Desastres naturales	1	5	5		
	5.2.1. [I.1] Fuego	1	5	5		
	5.2.2. [I.2] Daños por agua	1	5	5		
	5.2.3. [I.*] Desastres industriales	1	5	5		
	5.2.4. [I.3] Contaminación mecánica	3	3	9		
	5.2.5. [I.4] Contaminación electromagnética	3	3	9		
	5.2.6. [I.5] Avería de origen físico o lógico	3	5	15		
	5.2.7. [I.6] Corte del suministro eléctrico	4	3	12		
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	3	9		

	5.2.11. [I.10] Degradación de los soportes de almacenamiento de la información	3	3	9		
	5.2.12. [I.11] Emanaciones electromagnéticas	3	3	9		
	5.3.1. [E.1] Errores de los usuarios	5	3	15		
	5.3.2. [E.2] Errores del administrador	4	5	20		
	5.3.10. [E.15] Alteración accidental de la información	4	3	12		
	5.3.11. [E.18] Destrucción de información	2	5	10		
	5.3.12. [E.19] Fugas de información	4	3	12		
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	5	15		
	5.3.17. [E.25] Pérdida de equipos	3	3	9		
	5.4.5. [A.7] Uso no previsto	4	3	12		
	5.4.9. [A.11] Acceso no autorizado	3	3	9		
	5.4.13. [A.15] Modificación deliberada de la información	3	5	15		
	5.4.14. [A.18] Destrucción de información	2	5	10		
	5.4.15. [A.19] Divulgación de información	3	5	15		
	5.4.17. [A.23] Manipulación de los equipos	2	3	6		
	5.4.19. [A.25] Robo	2	5	10		
	5.4.20. [A.26] Ataque destructivo	1	5	5		
Syscom	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24	449	EXTREMO
	5.3.1. [E.1] Errores de los usuarios	5	5	25		

	5.3.2. [E.2] Errores del administrador	3	8	24		
	5.3.6. [E.8] Difusión de software dañino	2	8	16		
	5.3.7. [E.9] Errores de [re-]encaminamiento	2	8	16		
	5.3.8. [E.10] Errores de secuencia	2	8	16		
	5.3.10. [E.15] Alteración accidental de la información	4	8	32		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	3	5	15		
	5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	8	24		
	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	8	32		
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	8	24		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24		
	5.4.5. [A.7] Uso no previsto	3	8	24		
	5.4.6. [A.8] Difusión de software dañino	2	8	16		
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	5	15		
	5.4.8. [A.10] Alteración de secuencia	3	8	24		
	5.4.9. [A.11] Acceso no autorizado	3	8	24		
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16		
	5.4.14. [A.18] Destrucción de información	2	8	16		
	5.4.15. [A.19] Divulgación de información	2	5	10		
	5.4.16. [A.22] Manipulación de programas	2	8	16		
Docuarchive	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24	449	EXTREMO
	5.3.1. [E.1] Errores de los usuarios	5	5	25		

	5.3.2. [E.2] Errores del administrador	3	8	24
	5.3.6. [E.8] Difusión de software dañino	2	8	16
	5.3.7. [E.9] Errores de [re-]encaminamiento	2	8	16
	5.3.8. [E.10] Errores de secuencia	2	8	16
	5.3.10. [E.15] Alteración accidental de la información	4	8	32
	5.3.11. [E.18] Destrucción de información	2	8	16
	5.3.12. [E.19] Fugas de información	3	5	15
	5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	8	24
	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	8	32
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	8	24
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24
	5.4.5. [A.7] Uso no previsto	3	8	24
	5.4.6. [A.8] Difusión de software dañino	2	8	16
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	5	15
	5.4.8. [A.10] Alteración de secuencia	3	8	24
	5.4.9. [A.11] Acceso no autorizado	3	8	24
	5.4.13. [A.15] Modificación deliberada de la información	2	8	16
	5.4.14. [A.18] Destrucción de información	2	8	16
	5.4.15. [A.19] Divulgación de información	2	5	10

	5.4.16. [A.22] Manipulación de programas	2	8	16		
Plataforma OCS Inventory	5.2.6. [I.5] Avería de origen físico o lógico	3	5	15	280	INTOLERANTE
	5.3.1. [E.1] Errores de los usuarios	5	2	10		
	5.3.2. [E.2] Errores del administrador	3	5	15		
	5.3.6. [E.8] Difusión de software dañino	2	5	10		
	5.3.7. [E.9] Errores de [re-]encaminamiento	2	5	10		
	5.3.8. [E.10] Errores de secuencia	2	3	6		
	5.3.10. [E.15] Alteración accidental de la información	4	5	20		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	3	5	15		
	5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	3	9		
	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	5	20		
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	15		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	15		
	5.4.5. [A.7] Uso no previsto	3	3	9		
	5.4.6. [A.8] Difusión de software dañino	2	5	10		
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	5	15		
	5.4.8. [A.10] Alteración de secuencia	3	3	9		

	5.4.9. [A.11] Acceso no autorizado	3	5	15		
	5.4.13. [A.15] Modificación deliberada de la información	2	5	10		
	5.4.14. [A.18] Destrucción de información	2	8	16		
	5.4.15. [A.19] Divulgación de información	2	5	10		
	5.4.16. [A.22] Manipulación de programas	2	5	10		
Plataforma GLPI	5.2.6. [I.5] Avería de origen físico o lógico	3	3	9	186	INTOLERANTE
	5.3.1. [E.1] Errores de los usuarios	5	2	10		
	5.3.2. [E.2] Errores del administrador	3	3	9		
	5.3.6. [E.8] Difusión de software dañino	2	3	6		
	5.3.7. [E.9] Errores de [re-]encaminamiento	2	3	6		
	5.3.8. [E.10] Errores de secuencia	2	3	6		
	5.3.10. [E.15] Alteración accidental de la información	4	3	12		
	5.3.11. [E.18] Destrucción de información	2	5	10		
	5.3.12. [E.19] Fugas de información	3	3	9		
	5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	3	9		
	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	3	12		
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	3	9		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	3	9		
	5.4.5. [A.7] Uso no previsto	3	3	9		

	5.4.6. [A.8] Difusión de software dañino	2	3	6		
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	3	9		
	5.4.8. [A.10] Alteración de secuencia	3	3	9		
	5.4.9. [A.11] Acceso no autorizado	3	3	9		
	5.4.13. [A.15] Modificación deliberada de la información	2	3	6		
	5.4.14. [A.18] Destrucción de información	2	5	10		
	5.4.15. [A.19] Divulgación de información	2	3	6		
	5.4.16. [A.22] Manipulación de programas	2	3	6		
VPN Sophos	5.2.6. [I.5] Avería de origen físico o lógico	3	5	15	280	INTOLERANTE
	5.3.1. [E.1] Errores de los usuarios	5	2	10		
	5.3.2. [E.2] Errores del administrador	3	5	15		
	5.3.6. [E.8] Difusión de software dañino	2	5	10		
	5.3.7. [E.9] Errores de [re-]encaminamiento	2	5	10		
	5.3.8. [E.10] Errores de secuencia	2	3	6		
	5.3.10. [E.15] Alteración accidental de la información	4	5	20		
	5.3.11. [E.18] Destrucción de información	2	8	16		
	5.3.12. [E.19] Fugas de información	3	5	15		
	5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	3	9		

	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	5	20		
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	15		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	15		
	5.4.5. [A.7] Uso no previsto	3	3	9		
	5.4.6. [A.8] Difusión de software dañino	2	5	10		
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	5	15		
	5.4.8. [A.10] Alteración de secuencia	3	3	9		
	5.4.9. [A.11] Acceso no autorizado	3	5	15		
	5.4.13. [A.15] Modificación deliberada de la información	2	5	10		
	5.4.14. [A.18] Destrucción de información	2	8	16		
	5.4.15. [A.19] Divulgación de información	2	5	10		
	5.4.16. [A.22] Manipulación de programas	2	5	10		
Antivirus Kaspersky Office Small	5.2.6. [I.5] Avería de origen físico o lógico	3	5	15	281	INTOLERANTE
	5.3.1. [E.1] Errores de los usuarios	5	3	15		
	5.3.2. [E.2] Errores del administrador	3	5	15		
	5.3.6. [E.8] Difusión de software dañino	2	8	16		
	5.3.7. [E.9] Errores de [re-]encaminamiento	2	3	6		
	5.3.8. [E.10] Errores de secuencia	2	3	6		
	5.3.10. [E.15] Alteración accidental de la información	4	5	20		

	5.3.11. [E.18] Destrucción de información	2	5	10		
	5.3.12. [E.19] Fugas de información	3	3	9		
	5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	5	15		
	5.3.14. [E.21] Errores de mantenimiento / actualización de programas (software)	4	5	20		
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	15		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	15		
	5.4.5. [A.7] Uso no previsto	3	5	15		
	5.4.6. [A.8] Difusión de software dañino	2	5	10		
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	5	15		
	5.4.8. [A.10] Alteración de secuencia	3	3	9		
	5.4.9. [A.11] Acceso no autorizado	3	5	15		
	5.4.13. [A.15] Modificación deliberada de la información	2	5	10		
	5.4.14. [A.18] Destrucción de información	2	5	10		
	5.4.15. [A.19] Divulgación de información	2	5	10		
	5.4.16. [A.22] Manipulación de programas	2	5	10		
Director de T,I	5.3.5. [E.7] Deficiencias en la organización	4	5	20	77	TOLERANTE
	5.3.18. [E.28] Indisponibilidad del personal	3	5	15		
	5.4.22. [A.28] Indisponibilidad del personal	2	5	10		
	5.4.23. [A.29] Extorsión	2	8	16		

	5.4.24. [A.30] Ingeniería social (picaresca)	2	8	16		
Auxiliar de T,I	5.3.5. [E.7] Deficiencias en la organización	4	3	12	57	TOLERANTE
	5.3.18. [E.28] Indisponibilidad del personal	3	3	9		
	5.4.22. [A.28] Indisponibilidad del personal	2	5	10		
	5.4.23. [A.29] Extorsión	2	5	10		
	5.4.24. [A.30] Ingeniería social (picaresca)	2	8	16		
Consultor de T.I	5.3.5. [E.7] Deficiencias en la organización	5	3	15	42	ACEPTABLE
	5.3.18. [E.28] Indisponibilidad del personal	2	3	6		
	5.4.22. [A.28] Indisponibilidad del personal	2	3	6		
	5.4.23. [A.29] Extorsión	1	5	5		
	5.4.24. [A.30] Ingeniería social (picaresca)	2	5	10		
Gerencia	5.3.5. [E.7] Deficiencias en la organización	2	8	16	49	ACEPTABLE
	5.3.18. [E.28] Indisponibilidad del personal	2	5	10		
	5.4.22. [A.28] Indisponibilidad del personal	2	5	10		
	5.4.23. [A.29] Extorsión	1	8	8		
	5.4.24. [A.30] Ingeniería social (picaresca)	1	5	5		
Correo Microsoft Office 365	5.3.1. [E.1] Errores de los usuarios	5	3	15	251	INTOLERANTE
	5.3.2. [E.2] Errores del administrador	3	5	15		
	5.3.7. [E.9] Errores de [re-]encaminamiento	4	3	12		
	5.3.8. [E.10] Errores de secuencia	4	3	12		
	5.3.10. [E.15] Alteración accidental de la información	5	3	15		
	5.3.11. [E.18] Destrucción de información	4	5	20		
	5.3.12. [E.19] Fugas de información	4	3	12		

	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	5	15		
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	15		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	15		
	5.4.5. [A.7] Uso no previsto	4	3	12		
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	4	3	12		
	5.4.8. [A.10] Alteración de secuencia	3	3	9		
	5.4.9. [A.11] Acceso no autorizado	3	3	9		
	5.4.11. [A.13] Repudio	3	3	9		
	5.4.13. [A.15] Modificación deliberada de la información	3	5	15		
	5.4.14. [A.18] Destrucción de información	3	5	15		
	5.4.15. [A.19] Divulgación de información	3	3	9		
	5.4.18. [A.24] Denegación de servicio	3	5	15		
Dominio	5.3.1. [E.1] Errores de los usuarios	5	3	15	415	EXTREMO
	5.3.2. [E.2] Errores del administrador	3	8	24		
	5.3.7. [E.9] Errores de [re-]encaminamiento	4	3	12		
	5.3.8. [E.10] Errores de secuencia	4	3	12		
	5.3.10. [E.15] Alteración accidental de la información	4	5	20		
	5.3.11. [E.18] Destrucción de información	4	8	32		
	5.3.12. [E.19] Fugas de información	4	8	32		

	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	8	24		
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	8	24		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24		
	5.4.5. [A.7] Uso no previsto	4	8	32		
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	4	5	20		
	5.4.8. [A.10] Alteración de secuencia	3	3	9		
	5.4.9. [A.11] Acceso no autorizado	3	5	15		
	5.4.11. [A.13] Repudio	3	8	24		
	5.4.13. [A.15] Modificación deliberada de la información	3	8	24		
	5.4.14. [A.18] Destrucción de información	3	8	24		
	5.4.15. [A.19] Divulgación de información	3	8	24		
	5.4.18. [A.24] Denegación de servicio	3	8	24		
Hosting	5.3.1. [E.1] Errores de los usuarios	4	3	12	263	INTOLERANTE
	5.3.2. [E.2] Errores del administrador	3	5	15		
	5.3.7. [E.9] Errores de [re-]encaminamiento	3	3	9		
	5.3.8. [E.10] Errores de secuencia	3	3	9		
	5.3.10. [E.15] Alteración accidental de la información	4	5	20		
	5.3.11. [E.18] Destrucción de información	4	5	20		
	5.3.12. [E.19] Fugas de información	3	5	15		

	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	5	15		
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	5	15		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	5	15		
	5.4.5. [A.7] Uso no previsto	3	5	15		
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	3	9		
	5.4.8. [A.10] Alteración de secuencia	3	3	9		
	5.4.9. [A.11] Acceso no autorizado	3	5	15		
	5.4.11. [A.13] Repudio	3	5	15		
	5.4.13. [A.15] Modificación deliberada de la información	3	5	15		
	5.4.14. [A.18] Destrucción de información	2	5	10		
	5.4.15. [A.19] Divulgación de información	3	5	15		
	5.4.18. [A.24] Denegación de servicio	3	5	15		
Almacenamiento Nube	5.3.1. [E.1] Errores de los usuarios	5	3	15	305	EXTREMO
	5.3.2. [E.2] Errores del administrador	3	5	15		
	5.3.7. [E.9] Errores de [re-]encaminamiento	4	3	12		
	5.3.8. [E.10] Errores de secuencia	4	3	12		
	5.3.10. [E.15] Alteración accidental de la información	5	3	15		
	5.3.11. [E.18] Destrucción de información	4	8	32		
	5.3.12. [E.19] Fugas de información	4	3	12		

	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	5	15		
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	8	24		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24		
	5.4.5. [A.7] Uso no previsto	4	3	12		
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	4	3	12		
	5.4.8. [A.10] Alteración de secuencia	3	3	9		
	5.4.9. [A.11] Acceso no autorizado	3	3	9		
	5.4.11. [A.13] Repudio	3	3	9		
	5.4.13. [A.15] Modificación deliberada de la información	3	5	15		
	5.4.14. [A.18] Destrucción de información	3	8	24		
	5.4.15. [A.19] Divulgación de información	3	8	24		
	5.4.18. [A.24] Denegación de servicio	3	5	15		
Virtualización	5.3.1. [E.1] Errores de los usuarios	4	5	20	423	EXTREMO
	5.3.2. [E.2] Errores del administrador	4	8	32		
	5.3.7. [E.9] Errores de [re-]encaminamiento	3	5	15		
	5.3.8. [E.10] Errores de secuencia	3	5	15		
	5.3.10. [E.15] Alteración accidental de la información	4	8	32		
	5.3.11. [E.18] Destrucción de información	4	8	32		
	5.3.12. [E.19] Fugas de información	3	8	24		

	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	8	24		
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	8	24		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24		
	5.4.5. [A.7] Uso no previsto	3	8	24		
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	5	15		
	5.4.8. [A.10] Alteración de secuencia	3	5	15		
	5.4.9. [A.11] Acceso no autorizado	3	8	24		
	5.4.11. [A.13] Repudio	3	5	15		
	5.4.13. [A.15] Modificación deliberada de la información	3	8	24		
	5.4.14. [A.18] Destrucción de información	2	8	16		
	5.4.15. [A.19] Divulgación de información	3	8	24		
	5.4.18. [A.24] Denegación de servicio	3	8	24		
RDS	5.3.1. [E.1] Errores de los usuarios	4	5	20	423	EXTREMO
	5.3.2. [E.2] Errores del administrador	4	8	32		
	5.3.7. [E.9] Errores de [re-]encaminamiento	3	5	15		
	5.3.8. [E.10] Errores de secuencia	3	5	15		
	5.3.10. [E.15] Alteración accidental de la información	4	8	32		
	5.3.11. [E.18] Destrucción de información	4	8	32		
	5.3.12. [E.19] Fugas de información	3	8	24		

	5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	8	24		
	5.4.3. [A.5] Suplantación de la identidad del usuario	3	8	24		
	5.4.4. [A.6] Abuso de privilegios de acceso	3	8	24		
	5.4.5. [A.7] Uso no previsto	3	8	24		
	5.4.7. [A.9] [Re-]encaminamiento de mensajes	3	5	15		
	5.4.8. [A.10] Alteración de secuencia	3	5	15		
	5.4.9. [A.11] Acceso no autorizado	3	8	24		
	5.4.11. [A.13] Repudio	3	5	15		
	5.4.13. [A.15] Modificación deliberada de la información	3	8	24		
	5.4.14. [A.18] Destrucción de información	2	8	16		
	5.4.15. [A.19] Divulgación de información	3	8	24		
	5.4.18. [A.24] Denegación de servicio	3	8	24		
AIRE ACONDICIONADO CUARTO DE EQUIPOS.	5.1.1. [N.1] Fuego	1	8	8	382	EXTREMO
	5.1.2. [N.2] Daños por agua	2	8	16		
	5.1.3. [N.*] Desastres naturales	2	8	16		
	5.2.1. [I.1] Fuego	2	8	16		
	5.2.2. [I.2] Daños por agua	2	8	16		
	5.2.3. [I.*] Desastres industriales	2	8	16		
	5.2.4. [I.3] Contaminación mecánica	3	8	24		
	5.2.5. [I.4] Contaminación electromagnética	3	8	24		
	5.2.6. [I.5] Avería de origen físico o lógico	4	8	32		
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32		

	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24		
	5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	3	8	24		
	5.2.12. [I.11] Emanaciones electromagnéticas	3	8	24		
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	8	24		
	5.3.17. [E.25] Pérdida de equipos	3	8	24		
	5.4.5. [A.7] Uso no previsto	3	1	3		
	5.4.9. [A.11] Acceso no autorizado	3	1	3		
	5.4.17. [A.23] Manipulación de los equipos	3	8	24		
	5.4.19. [A.25] Robo	3	8	24		
	5.4.20. [A.26] Ataque destructivo	1	8	8		
UPS	5.1.1. [N.1] Fuego	2	8	16	424	EXTREMO
	5.1.2. [N.2] Daños por agua	2	8	16		
	5.1.3. [N.*] Desastres naturales	2	8	16		
	5.2.1. [I.1] Fuego	2	8	16		
	5.2.2. [I.2] Daños por agua	2	8	16		
	5.2.3. [I.*] Desastres industriales	2	8	16		
	5.2.4. [I.3] Contaminación mecánica	4	8	32		
	5.2.5. [I.4] Contaminación electromagnética	4	8	32		
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24		
	5.2.7. [I.6] Corte del suministro eléctrico	4	8	32		
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24		

	5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	3	8	24		
	5.2.12. [I.11] Emanaciones electromagnéticas	3	8	24		
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	8	24		
	5.3.17. [E.25] Pérdida de equipos	2	8	16		
	5.4.5. [A.7] Uso no previsto	2	8	16		
	5.4.9. [A.11] Acceso no autorizado	3	8	24		
	5.4.17. [A.23] Manipulación de los equipos	3	8	24		
	5.4.19. [A.25] Robo	2	8	16		
	5.4.20. [A.26] Ataque destructivo	2	8	16		
PLANTA ELECTRICA	5.1.1. [N.1] Fuego	1	8	8	415	EXTREMO
	5.1.2. [N.2] Daños por agua	2	8	16		
	5.1.3. [N.*] Desastres naturales	2	8	16		
	5.2.1. [I.1] Fuego	2	8	16		
	5.2.2. [I.2] Daños por agua	2	8	16		
	5.2.3. [I.*] Desastres industriales	2	8	16		
	5.2.4. [I.3] Contaminación mecánica	4	8	32		
	5.2.5. [I.4] Contaminación electromagnética	4	8	32		
	5.2.6. [I.5] Avería de origen físico o lógico	3	8	24		
	5.2.7. [I.6] Corte del suministro eléctrico	3	8	24		
	5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	3	8	24		

	5.2.10. [I.9] Interrupción de otros servicios y suministros esenciales	3	8	24		
	5.2.12. [I.11] Emanaciones electromagnéticas	3	8	24		
	5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	3	8	24		
	5.3.17. [E.25] Pérdida de equipos	2	8	16		
	5.4.5. [A.7] Uso no previsto	3	5	15		
	5.4.9. [A.11] Acceso no autorizado	3	8	24		
	5.4.17. [A.23] Manipulación de los equipos	3	8	24		
	5.4.19. [A.25] Robo	3	8	24		
	5.4.20. [A.26] Ataque destructivo	2	8	16		
Data Center	5.1.1. [N.1] Fuego	2	8	16	268	INTOLERANTE
	5.1.2. [N.2] Daños por agua	2	8	16		
	5.2.1. [I.1] Fuego	2	8	16		
	5.2.2. [I.2] Daños por agua	2	8	16		
	5.2.3. [I.*] Desastres industriales	2	8	16		
	5.2.12. [I.11] Emanaciones electromagnéticas	3	8	24		
	5.3.10. [E.15] Alteración accidental de la información	3	8	24		
	5.3.11. [E.18] Destrucción de información	3	8	24		
	5.3.12. [E.19] Fugas de información	3	5	15		
	5.4.5. [A.7] Uso no previsto	3	2	6		
	5.4.9. [A.11] Acceso no autorizado	3	8	24		
	5.4.13. [A.15] Modificación deliberada de la información	3	5	15		
	5.4.14. [A.18] Destrucción de información	2	8	16		
	5.4.15. [A.19] Divulgación de información	3	8	24		

	5.4.20. [A.26] Ataque destructivo	1	8	8		
	5.4.21. [A.27] Ocupación enemiga	1	8	8		

Apéndice D

Identificación de Elementos y Componentes a Monitorear en el Data Center

ACTIVO	Elementos importantes a monitorear por activo	Componentes
Servidores datacenter	Rendimiento de sistema	CPU: Uso porcentual, temperatura, procesos críticos.
		RAM: Consumo, intercambio (swap), fugas de memoria.
		Disco: Uso de almacenamiento, latencia, IOPS (operaciones de E/S por segundo).
		Red: Ancho de banda, paquetes perdidos, latencia.
	Uptime	Verificación de servicios críticos (HTTP, DNS, BD, etc.).
		Alertas ante reinicios inesperados o caídas
	Seguridad y vulnerabilidades	Intentos de acceso no autorizado (logs de autenticación).
		Detección de malware o actividades sospechosas.
		Actualizaciones
	Almacenamiento y backup	Espacio en disco
		Integridad de backup
	Temperatura y energía	Monitoreo térmico
		Consumo eléctrico
	Logs y auditoria	Detección de anomalías mediante IA/ML.
		Análisis centralizado de logs (syslog, eventos de Windows).
Servidor hipervisor	Rendimiento de sistema	CPU: Uso porcentual, temperatura, procesos críticos.
		RAM: Consumo, intercambio (swap), fugas de memoria.
		Disco: Uso de almacenamiento, latencia, IOPS (operaciones de E/S por segundo).
		Red: Ancho de banda, paquetes perdidos, latencia.

	Uptime	Verificación de servicios críticos (HTTP, DNS, BD, etc.).
		Alertas ante reinicios inesperados o caídas
	Seguridad y vulnerabilidades	Intentos de acceso no autorizado (logs de autenticación).
		Detección de malware o actividades sospechosas.
		Actualizaciones
	Almacenamiento y backup	Espacio en disco
		Integridad de backup
	Temperatura y energía	Monitoreo termico
		Consumo electrico
	Logs y auditoria	Detección de anomalías mediante IA/ML.
		Análisis centralizado de logs (syslog, eventos de Windows).
Servidor Dominio	Rendimiento de sistema	CPU: Uso porcentual, temperatura, procesos críticos.
		RAM: Consumo, intercambio (swap), fugas de memoria.
		Disco: Uso de almacenamiento, latencia, IOPS (operaciones de E/S por segundo).
		Red: Ancho de banda, paquetes perdidos, latencia.
	Uptime	Verificación de servicios críticos (HTTP, DNS, BD, etc.).
		Alertas ante reinicios inesperados o caídas
	Seguridad y vulnerabilidades	Intentos de acceso no autorizado (logs de autenticación).
		Detección de malware o actividades sospechosas.
		Actualizaciones
	Almacenamiento y backup	Espacio en disco
		Integridad de backup
	Temperatura y energía	Monitoreo termico
		Consumo electrico
	Logs y auditoria	Detección de anomalías mediante IA/ML.
		Análisis centralizado de logs (syslog, eventos de Windows).

Servidores de archivos	Rendimiento de sistema	CPU: Uso porcentual, temperatura, procesos críticos.
		RAM: Consumo, intercambio (swap), fugas de memoria.
		Disco: Uso de almacenamiento, latencia, IOPS (operaciones de E/S por segundo).
		Red: Ancho de banda, paquetes perdidos, latencia.
	Uptime	Verificación de servicios críticos (HTTP, DNS, BD, etc.).
		Alertas ante reinicios inesperados o caídas
	Seguridad y vulnerabilidades	Intentos de acceso no autorizado (logs de autenticación).
		Detección de malware o actividades sospechosas.
		Actualizaciones
	Almacenamiento y backup	Espacio en disco
		Integridad de backup
	Temperatura y energía	Monitoreo termico
		Consumo electrico
	Logs y auditoria	Detección de anomalías mediante IA/ML.
		Análisis centralizado de logs (syslog, eventos de Windows).
Servidor Soluxionar	Rendimiento de sistema	CPU: Uso porcentual, temperatura, procesos críticos.
		RAM: Consumo, intercambio (swap), fugas de memoria.
		Disco: Uso de almacenamiento, latencia, IOPS (operaciones de E/S por segundo).
		Red: Ancho de banda, paquetes perdidos, latencia.
	Uptime	Verificación de servicios críticos (HTTP, DNS, BD, etc.).
		Alertas ante reinicios inesperados o caídas
	Seguridad y vulnerabilidades	Intentos de acceso no autorizado (logs de autenticación).
		Detección de malware o actividades sospechosas.
		Actualizaciones

	Almacenamiento y backup	Espacio en disco
		Integridad de backup
	Temperatura y energía	Monitoreo termico
		Consumo electrico
	Logs y auditoria	Detección de anomalías mediante IA/ML.
		Análisis centralizado de logs (syslog, eventos de Windows).
Switch administrable	Uso de Ancho de Banda y Tráfico	Monitoreo del ancho de banda por puerto (in/out).
		Detección de congestión (drops, colisiones, errores CRC).
		Top Talkers (identificación de dispositivos que consumen más ancho de banda).
	Latencia y Jitter	Medición de latencia entre switches y routers.
		Monitoreo de jitter para aplicaciones sensibles (VoIP, videoconferencia).
	Tablas de Enrutamiento	Estado de las tablas ARP y MAC.
		Monitoreo de rutas estáticas/dinámicas (OSPF, BGP, EIGRP)
	Estado de Puertos (Up/Down)	Alertas por caídas de enlace (link flapping)
		Monitoreo de STP (Spanning Tree Protocol) para evitar bucles
	Uso de CPU y Memoria del Switch	Uso de CPU y Memoria del Switch
		Consumo de memoria del switch (evitar saturación).
	Intentos de Acceso No Autorizado	Monitoreo de SSH/Telnet/SNMP (accesos sospechosos).
		Detección de MAC spoofing y ARP poisoning.
	Monitoreo de Cambios en Configuración	Auditoría de cambios en VLANs, ACLs, rutas.
		Uso de Syslog y SNMP traps para registro de eventos.
UTM	Uso de Recursos (CPU, RAM, Almacenamiento)	Monitorear el uso de CPU y RAM para detectar sobrecargas que afecten el rendimiento
		Verificar el espacio en disco para logs y actualizaciones.

	Disponibilidad y Uptime	Verificar el tiempo de actividad (uptime) y reinicios inesperados
		Alertas por caídas de servicios críticos (VPN, filtrado web).
	Firewall y Reglas de Filtrado	Monitorear intentos de conexión bloqueados/permitidos.
		Alertas por cambios no autorizados en reglas de firewall.
	Prevención de Intrusiones (IPS/IDS)	Detección de ataques conocidos (escaneo de puertos, exploits).
		Alertas por comportamientos anómalos (tráfico inusual).
	Filtrado Web y Antivirus	Monitorear bloqueos de malware/URLs maliciosas.
		Alertas por archivos infectados detectados en tráfico HTTP/FTP.
	VPN y Acceso Remoto	Verificar conexiones VPN activas y posibles intrusiones.
		Alertas por intentos de acceso no autorizado.
	Análisis Centralizado de Logs	Recolectar y analizar logs de firewall, IPS, proxy.
		Detectar patrones de ataque mediante SIEM
	Cambios en Configuración	Auditoría de modificaciones en políticas de seguridad.
		Alertas por cambios no autorizados en configuraciones.
Router proveedores	Uso de CPU y Memoria	Monitorear el uso de CPU (procesos activos, picos de rendimiento).
		Verificar el consumo de memoria RAM para evitar saturación.
	Ancho de Banda y Tráfico	Monitorear el tráfico por interfaz (in/out) para detectar congestión.
		Alertas por drops de paquetes o errores CRC.
	Latencia y Jitter	Medir latencia en enlaces críticos (WAN/VPN).
		Monitorear jitter para aplicaciones sensibles (VoIP, videoconferencia).

	Estado de Interfaces (Up/Down)	Alertas por caídas de enlace (interfaces físicas y lógicas).
		Monitorear flapping (intermitencia en enlaces).
	Protocolos de Enrutamiento (BGP, OSPF, EIGRP)	Verificar vecinos BGP/OSPF (estado estable/activo).
		Alertas por cambios en rutas (reconvergencia no planificada).
	Tablas de Enrutamiento (Routing Tables)	Monitorear tamaño de tablas de enrutamiento (evitar saturación)
		Alertas por rutas inválidas o flapping
	Intentos de Acceso No Autorizado	Monitorear accesos SSH/Telnet/SNMP (brute force attacks).
		Alertas por logins fallidos.
	ACLs (Access Control Lists)	Verificar reglas de firewall aplicadas en el router.
		Alertas por intentos de bypass de ACLs.
	Cambios en Configuración	Auditoría de modificaciones en configuraciones (ej: VLANs, ACLs).
		Uso de Syslog y SNMP traps para registro de eventos
LAN	Ancho de Banda y Utilización	Monitorear el tráfico por puerto (in/out) en switches.
		Detectar congestión (drops de paquetes, colisiones).
	Latencia y Jitter	Medir latencia interna entre dispositivos.
		Monitorear jitter para aplicaciones sensibles (VoIP, videoconferencia).
	Uso de DHCP y DNS	Verificar disponibilidad de direcciones IP (agotamiento de DHCP).
		Monitorear tiempos de respuesta DNS.
	Detección de Dispositivos No Autorizados	Identificar dispositivos no reconocidos (Rogue DHCP).
		Monitorear cambios en topología (LLDP/CDP).
	Ataques Internos	Detectar MAC flooding (saturación de tablas MAC).
		Alertas por ataques MITM (Man-in-the-Middle).

	Cambios en Configuración	Auditoría de modificaciones en switches/routers.
		Uso de Syslog y SNMP traps para registro de eventos.
Internet Empresarial Backup	Uptime y Estado del Enlace	Verificar disponibilidad 24/7 (SLAs).
		Alertas por interrupciones no planificadas.
	Ancho de banda	Medir el tráfico bidireccional (Tx/Rx) en Gbps.
		Detectar congestión (pérdida de paquetes, jitter).
	Atenuación y Pérdida de Señal (dB)	Monitorear la pérdida de potencia óptica (OLT, ONT).
		Alertas por valores anómalos (cortes o degradación).
	Latencia y Jitter	Monitorear latencia de extremo a extremo (E2E).
		Controlar jitter para aplicaciones críticas (VoIP, VPN).
Internet Empresarial	Uptime y Estado del Enlace	Verificar disponibilidad 24/7 (SLAs).
		Alertas por interrupciones no planificadas.
	Ancho de banda	Medir el tráfico bidireccional (Tx/Rx) en Gbps.
		Detectar congestión (pérdida de paquetes, jitter).
	Atenuación y Pérdida de Señal (dB)	Monitorear la pérdida de potencia óptica (OLT, ONT).
		Alertas por valores anómalos (cortes o degradación).
	Latencia y Jitter	Monitorear latencia de extremo a extremo (E2E).
		Controlar jitter para aplicaciones críticas (VoIP, VPN).
Red Inalambrica	Intensidad de la Señal (RSSI) y Relación Señal-Ruido (SNR)	Monitorear RSSI (Received Signal Strength Indicator) en dBm.
		Verificar SNR (Signal-to-Noise Ratio) para calidad de conexión.

	Ancho de Banda y Utilización del Canal	Medir tráfico por AP (Access Point) en Mbps
		Detectar congestión de canales (interferencias).
	Latencia y Pérdida de Paquetes	Monitorear latencia para aplicaciones críticas (VoIP, VPN).
		Alertas por pérdida de paquetes (> 1% es crítico).
	Estado de los Access Points (APs)	Verificar uptime de APs (reinicios inesperados).
		Alertas por APs sobrecargados (múltiples clientes).
	Planificación de Canales y Interferencias	Detectar solapamiento de canales (2.4 GHz/5 GHz).
		Usar análisis de espectro para interferencias no Wi-Fi.
	Encriptación y Autenticación	Verificar WPA3/AES (evitar TKIP/WEP).
		Alertas por dispositivos con configuraciones vulnerables
Servidor Nas Soluxionar	Uso de CPU y Memoria	Monitorear el % de uso de CPU (procesos críticos como Samba/NFS).
		Verificar consumo de RAM (caché, buffers, swap).
	Uso de Almacenamiento	Monitorear espacio en disco (por volumen/partición).
		Alertas por inodes agotados (especialmente en sistemas con muchos archivos pequeños).
	Rendimiento de E/S (I/O)	Medir latencia de disco
		Monitorear throughput (MB/s de lectura/escritura).
	Estado de los Servicios NAS	Verificar que Samba (SMB/CIFS), NFS, o FTP estén activos.
		Alertas por caídas de servicios
	RAID y Salud de Discos	Monitorear estado del RAID (mdadm o ZFS).
		Alertas por discos fallando (SMART errors, sectores defectuosos).

	Uptime y Cargas del Sistema	Verificar tiempo de actividad (uptime).
		Alertas por cargas promedio altas (load average > núm. de núcleos)
	Autenticación y Accesos	Monitorear intentos de login fallidos (SSH, Samba).
		Alertas por accesos no autorizados
	Permisos de Archivos	Verificar cambios en permisos críticos (chmod/chown).
		Alertas por archivos sensibles con permisos abiertos
Syscom	Tiempo de Respuesta (Latencia)	Monitorear el tiempo de respuesta de la aplicación
		Alertas por latencia elevada
	Uso de Recursos (CPU, RAM, Disco)	Verificar el consumo de CPU y RAM por proceso de la aplicación.
		Monitorear E/S de disco (lecturas/escrituras) para bases de datos.
	Throughput y Solicitudes por Segundo (RPS)	Medir el número de solicitudes manejadas
		Alertas por cuellos de botella
	Tiempo de Actividad (Uptime)	Verificar que la aplicación esté activa y respondiendo
		Alertas por caídas no planificadas
	Dependencias Externas	Monitorear conexiones a bases de datos
		Alertas por fallos en APIs externas
	Logs de Errores	Recolectar y analizar logs de errores
		Alertas por errores recurrentes

	Autenticación y Accesos	Monitorear intentos de login fallidos
		Alertas por accesos no autorizados
Docuarchive	Tiempo de Respuesta (Latencia)	Monitorear el tiempo de respuesta de la aplicación
		Alertas por latencia elevada
	Uso de Recursos (CPU, RAM, Disco)	Verificar el consumo de CPU y RAM por proceso de la aplicación.
		Monitorear E/S de disco (lecturas/escrituras) para bases de datos.
	Throughput y Solicitudes por Segundo (RPS)	Medir el número de solicitudes manejadas
		Alertas por cuellos de botella
	Tiempo de Actividad (Uptime)	Verificar que la aplicación esté activa y respondiendo
		Alertas por caídas no planificadas
	Dependencias Externas	Monitorear conexiones a bases de datos
		Alertas por fallos en APIs externas
	Logs de Errores	Recolectar y analizar logs de errores
		Alertas por errores recurrentes
Dominio	Autenticación y Accesos	Monitorear intentos de login fallidos
		Alertas por accesos no autorizados
	Disponibilidad del DC	Monitorear tiempo de respuesta y replicación entre controladores de dominio.
	Autenticaciones	Alertar sobre intentos fallidos (ataques brute force) y bloqueos de cuentas.
Almacenamiento Nube	Sincronización de tiempo	Garantizar que NTP esté funcionando para evitar problemas de autenticación.
	Espacio en disco	Evitar saturación en volúmenes donde se almacenan bases de datos de dominio.
	Disponibilidad del servicio	Verificar acceso a APIs y latencia de respuesta.
	Uso de almacenamiento	Alertar antes de alcanzar límites de capacidad.
	Transferencia de datos	Monitorear ancho de banda consumido (especialmente en sync/backup).
	Integridad de datos	Verificar checksums y consistencia en archivos críticos.

Virtualización	Uso de recursos	CPU/RAM asignada vs. utilizada por VMs (evitar overprovisioning).
	Estado de VMs	Detectar VMs caídas o con alto consumo.
	Almacenamiento virtual	Latencia y throughput de discos virtuales (vSAN, iSCSI).
	Redes virtuales	Monitorear tráfico entre VMs y congestión en vSwitches.
RDS	Conexiones activas	Identificar sesiones huérfanas o no autorizadas.
	Rendimiento	Monitorear latencia y calidad gráfica (útil para usuarios remotos).
	Seguridad	Detectar intentos de acceso brute force (RDP es objetivo común de ataques).
	Uso de recursos	Consumo de CPU/GPU en servidores de terminales.
AIRE ACONDICIONADO CUARTO DE EQUIPOS.	Temperatura Ambiente	Rango óptimo: 18°C - 27°C (según ASHRAE TC 9.9).
		Alertas por temperaturas fuera de rango (riesgo para equipos IT).
	Humedad Relativa	Rango ideal: 40% - 60%.
		Evitar condensación (< 40%) o corrosión (> 60%).
	Consumo Energético (kW)	Medir eficiencia (PUE, Power Usage Effectiveness).
		Alertas por sobreconsumo
	Tiempo de Operación y Ciclos	Registrar horas de funcionamiento
		Alertas por ciclos demasiado frecuentes
	Alarmas del Sistema	Integrar notificaciones SNMP del equipo HVAC
		Alertas por fallos críticos
UPS	Voltaje de Entrada/Salida	Monitorear calidad del voltaje (rango aceptable: $\pm 10\%$ del nominal).
		Detectar fluctuaciones
	Corriente de Carga	Medir corriente consumida por los equipos conectados.
		Alertas por sobrecarga (>80% de capacidad nominal)
	Frecuencia	Verificar frecuencia de salida (50/60 Hz $\pm$ 0.5 Hz).

	Nivel de Carga	Monitorear % de carga restante
	Voltaje de Batería	Alertas por celdas defectuosas (desviación $> \pm 5\%$ entre celdas).
	Tiempo de Autonomía	Calcular tiempo restante de backup basado en carga actual
	Eficiencia del Inversor	Monitorear pérdidas de conversión (DC-AC).
	Temperatura del Inversor	Alertas por sobrecalentamiento ($> 60^{\circ}\text{C}$).
	Tiempos de Transferencia	Verificar tiempo de switch a batería
	Estado del Bypass Estático	Monitorear uso del bypass
PLANTA ELECTRICA	Voltaje (V) y Corriente (A)	Voltaje fase-neutro y fase-fase (desviaciones $> \pm 10\%$ son críticas).
		Corriente por fase (evitar desbalances $> 15\%$)
	Frecuencia (Hz)	Rango aceptable: $60\text{ Hz} \pm 0.5\text{ Hz}$ (o 50 Hz según región).
		Alertas por inestabilidad (riesgo para equipos críticos).
	Potencia Activa/Reactiva (kW/kVAR)	Potencia activa (kW) consumida por el datacenter.
		Factor de potencia (ideal: 0.95-1.0).
	Nivel de Combustible	Nivel de diésel
		Tiempo de autonomía estimado.
	Temperatura y Presión del Motor	Temperatura $> 90^{\circ}\text{C}$ (sobrecalentamiento).
		Presión de aceite $< 30\text{ psi}$ (fallo inminente).
	Horas de Operación	Registrar horómetro para mantenimiento predictivo.
	Tiempo de Transferencia	< 10 segundos (para cargas críticas).
	Transitorios y Microcortes	Detectar picos de voltaje ($> 110\%$ nominal) o dips ($< 80\%$).