SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA LA RED DE DATOS DE IFACTORY, BASADO EN LA NORMA ISO/IEC 27001

BOTINA DIAZ JEISON GABRIEL
ORBES ZAMBRANO JESÚS ESTEBAN

PROGRAMA DE INGENIERÍA DE SISTEMAS
FACULTAD DE INGENIERÍA
UNIVERSIDAD CESMAG
OCTUBRE, 2026

SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA LA RED DE DATOS DE IFACTORY, BASADO EN LA NORMA ISO/IEC 27001

Autores:
BOTINA DIAZ JEISON GABRIEL
ORBES ZAMBRANO JESÚS ESTEBAN

Informe final de trabajo de grado presentado como requisito para optar al título de Ingeniero de Sistemas, en modalidad investigación.

Director
Mg. ESCOBAR HERNÁNDEZ LUIS ARNOBY

PROGRAMA DE INGENIERÍA DE SISTEMAS
FACULTAD DE INGENIERÍA
UNIVERSIDAD CESMAG
ABRIL, 2026

DEDICATORIA

A Dios, por no habernos desamparado en los momentos difíciles y por brindarnos la fortaleza, sabiduría y perseverancia necesarias para continuar adelante a lo largo de este proceso. A nuestros padres, por habernos apoyado incondicionalmente durante toda nuestra carrera, siendo un pilar fundamental en cada logro alcanzado. Asimismo, a toda nuestra familia, por habernos brindado comprensión, confianza y palabras de aliento en cada etapa de este camino, motivándonos a seguir esforzándonos para cumplir nuestras metas y sueños profesionales

AGRADECIMIENTOS

Agradecemos de manera especial la colaboración y el apoyo brindado por las siguientes personas, quienes contribuyeron significativamente al desarrollo y culminación de este proyecto.

Al ingeniero Camilo Gómez Arteaga, ingeniero de sistemas de la empresa iFactory, por compartir sus conocimientos, experiencia y disposición durante el proceso de realización de este trabajo.

De igual manera, expresamos nuestro más sincero agradecimiento al Mg. Luis Arnoby Escobar, asesor de este proyecto, por sus valiosas orientaciones, acompañamiento constante y aportes académicos, los cuales fueron fundamentales para el desarrollo adecuado de esta investigación.

A todos ellos, nuestro más profundo reconocimiento y gratitud por el tiempo, apoyo y confianza brindados. De corazón, mil y mil gracias.

Nota de Aceptación

_____

_____

_____

_____

_____

Jurado 1

_____

Jurado 2

_____

San Juan de Pasto, 2026

Nota de exclusión

"El pensamiento que se expresa en esta obra es exclusiva responsabilidad de sus autores y no compromete la ideología de la Universidad CESMAG"

RESUMEN ANALÍTICO ESPECIALIZADO – RAE

Información General

Tema: Formulación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa iFactory, basado en la norma ISO/IEC 27001, con énfasis en pruebas de pentesting y gestión de riesgos.

Título: Sistema de Gestión de Seguridad Informática para la red de datos de iFactory, basado en la norma ISO/IEC 27001.

Autores: Botina Díaz Jeison Gabriel – Orbes Zambrano Jesús Esteban

Director: Mg. Luis Arnoby Escobar Hernández

Fuente Bibliográfica: Se referencian más de 40 fuentes, entre ellas: Foro Económico Mundial (Informe de Riesgos Globales 2022), Carrera et al. (2024) sobre Industria 4.0, Lizárraga et al. (2022) sobre auditorías TI, Minaya et al. (2023) sobre vulnerabilidades y criptografía, Galecio et al. (2025) sobre seguridad digital en entornos educativos, además de normas ISO/IEC 27001 y 27002.

Año: 2026

Resumen:
La seguridad de la información es un pilar estratégico para las organizaciones modernas. El presente proyecto formula un SGSI en la empresa iFactory, con el fin de proteger la confidencialidad, integridad y disponibilidad de sus activos digitales. Se realizaron pruebas de pentesting con herramientas como Nmap, Nessus, OpenVAS y BurpSuite, identificando vulnerabilidades críticas en servidores y aplicaciones. Posteriormente, se diseñó un SGSI conforme a la norma ISO/IEC 27001, integrando controles técnicos (firewalls, cifrado TLS/SSL, IDS/IPS) y organizativos (políticas de acceso, gestión de incidentes). Finalmente, se evaluó la efectividad del sistema mediante auditorías y encuestas, evidenciando mejoras en la resiliencia operativa y en la cultura de seguridad de la organización.

Palabras Clave

SGSI, ISO/IEC 27001, pentesting, confidencialidad, integridad, disponibilidad, controles, auditoría, tratamiento de riesgos, OSSTMM.

Descripción del problema de investigación

La empresa iFactory, dedicada al desarrollo de soluciones tecnológicas, no cuenta con un sistema formal de gestión de seguridad de la información. Esto la expone a riesgos como pérdida de datos, acceso no autorizado, ransomware y errores humanos. La ausencia de protocolos de respuesta y políticas estructuradas incrementa la vulnerabilidad de su infraestructura tecnológica.

Objetivos

General: Formular un SGSI conforme a la norma ISO/IEC 27001 en iFactory, orientado a proteger la red de datos mediante gestión proactiva de riesgos y controles técnicos y organizativos.

Específicos:

1. Realizar un análisis de vulnerabilidades mediante pruebas de pentesting y documentar hallazgos.

2. Diseñar un SGSI ajustado a las demandas operativas y tecnológicas de iFactory.

3. Evaluar la efectividad del SGSI mediante comparación objetiva antes y después de su implementación.

Metodología

Tradicional cascada apoyada en el ciclo PDCA (Planear – Hacer – Verificar – Actuar) de la norma ISO/IEC 27001: **Planificación,Ejecución,Seguimiento,Mantenimiento y mejora continua**.

Referentes teóricos

Seguridad de la información, Norma ISO/IEC 27001, OSSTMM, gestión de riesgos, análisis de vulnerabilidades, seguridad informática, redes de datos, uso de herramientas de pentesting (Nmap, Nessus, OpenVAS, BurpSuite).

Resultados

Los resultados permitieron identificar vulnerabilidades críticas en la infraestructura tecnológica de iFactory mediante herramientas de análisis y escaneo de seguridad. En este sentido, se elaboró un inventario de activos tecnológicos y se llevó a cabo una valoración de riesgos considerando amenazas relacionadas con disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.

Se formularon controles y estrategias de tratamiento de riesgos orientadas a fortalecer la seguridad informática de la organización. Entre las principales medidas propuestas se destacan: controles de acceso, monitoreo en firewall corporativo, administración centralizada de servicios y mecanismos de documentación.

En esta línea de ideas, la comparación teórica del estado de la seguridad antes y después de la formulación del SGSI evidenció mejoras potenciales en la gestión de incidentes, reducción de vulnerabilidades y fortalecimiento de las capacidades de respuesta frente posibles a amenazas cibernéticas.

Conclusiones

La formulación del SGSI en iFactory permitió reducir significativamente los riesgos asociados a la seguridad de la información, garantizando la protección de sus activos digitales y mejorando la resiliencia operativa. El proyecto constituye un referente aplicable para otras PYMEs del sector TI en Colombia. se demostró que la norma ISO/IEC 27001 puede adaptarse de manera efectiva a contextos locales con recursos limitados. La valoración de activos y la matriz de riesgos resaltaron la importancia de priorizar sistemas críticos como correo electrónico y bases de datos.

Recomendaciones

Se recomienda implementar segmentación de red y cierre de puertos innecesarios, acompañado de monitoreo continuo en el firewall corporativo FortiGate; estas acciones reducen la superficie de ataque y fortalecen la seguridad perimetral.

Se recomienda adoptar un plan formal de tratamiento de riesgos con controles específicos como cifrado TLS/SSL en comunicaciones y copias de seguridad periódicas; esto asegura continuidad operativa y trazabilidad de la información crítica.

Se recomienda diseñar un programa de formación continua en ciberseguridad con simulacros y campañas de sensibilización; la capacitación del personal es clave para consolidar la cultura de seguridad.

TABLA DE CONTENIDO

Pág.

INTRODUCCIÓN 15
I. PROBLEMA DE INVESTIGACIÓN 16
A. OBJETO O TEMA DE ESTUDIO 16
B. LÍNEA DE INVESTIGACIÓN 16
C. PLANTEAMIENTO DEL PROBLEMA 16
D. FORMULACIÓN DEL PROBLEMA 17
E. OBJETIVOS 18
F. JUSTIFICACIÓN 18
G. DELIMITACIÓN 19
II. MARCO TEÓRICO 20
A. ANTECEDENTES 20
B. SUPUESTOS TEÓRICOS 21
C. VARIABLES DEL ESTUDIO 29
D. DEFINICIÓN NOMINAL DE VARIABLES 29
E. DEFINICIÓN OPERATIVA DE VARIABLES 30
F. FORMULACIÓN DE HIPÓTESIS 30
III. METODOLOGÍA 31
A. PARADIGMA 31
B. ENFOQUE 31
C. MÉTODO 31
D. TIPO DE INVESTIGACIÓN 32
E. DISEÑO DE LA INVESTIGACIÓN 32
F. POBLACIÓN 32
G. MUESTRA 32
H. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN 33
I. VALIDEZ DE LA TÉCNICA 34
J. CONFIABILIDAD DE LA TÉCNICA 35
K. INSTRUMENTO DE RECOLECCIÓN DE DATOS 35
IV. RESULTADOS DE LA INVESTIGACIÓN 37
A. OBJETIVO 1. ANÁLISIS DE VULNERABILIDADES CON PRUEBAS DE PENTESTING EN LA EMPRESA IFACTORY 37
B. OBJETIVO 2. DISEÑAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) CONFORME A LA NORMA ISO/IEC 27001 62
C. OBJETIVO 3. EVALUAR LA EFECTIVIDAD DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) 64
V. ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS 69
CONCLUSIONES 71
RECOMENDACIONES 72
VI. REFERENCIAS BIBLIOGRÁFICAS 73
ANEXOS 77

LISTA DE TABLAS

Pág.

TABLA I. INVENTARIO DE ACTIVOS TECNOLÓGICOS 40
TABLA II. RESUMEN DEL ESQUEMA DE RED 40
TABLA III. BITÁCORA TÉCNICA....42
TABLA IV. HERRAMIENTAS SELECCIONADAS Y SU PROPÓSITO 44
TABLA V. RESULTADOS DE ESCANEO CON LA HERRAMIENTA NMAP 1 44
TABLA VI. RESULTADOS DE ESCANEO CON LA HERRAMIENTA NMAP 2 45
TABLA VII. PUERTOS DETECTADOS EN EL ESCANEO 46
TABLA VIII. RESULTADOS DE ESCANEO CON LA HERRAMIENTA MASSCAN 1....47
TABLA IX. RESULTADOS DE ESCANEO CON LA HERRAMIENTA MASSCAN 2 47
TABLA X. RESULTADOS DE ESCANEO CON LA HERRAMIENTA NIKTO....48
TABLA XI. RESULTADOS DE ESCANEO CON LA HERRAMIENTA BURPSUITE....49
TABLA XII. RESULTADOS DE ESCANEO CON LA HERRAMIENTA NESSUS 50
TABLA XIII. RESULTADOS DE ESCANEO CON LA HERRAMIENTA OPENVAS....51
TABLA XIV. DISPONIBILIDAD: ¿QUÉ IMPORTANCIA TENDRÍA QUE EL ACTIVO NO ESTUVIERA DISPONIBLE?....52
TABLA XV. INTEGRIDAD: ¿QUÉ IMPORTANCIA TENDRÍA QUE LOS DATOS FUERAN MODIFICADOS FUERA DE CONTROL?....53
TABLA XVI. CONFIDENCIALIDAD: ¿QUÉ IMPORTANCIA TENDRÍA QUE EL DATO FUERA CONOCIDO POR PERSONAS NO AUTORIZADAS? 53
TABLA XVII. AUTENTICIDAD: ¿QUÉ IMPORTANCIA TENDRÍA QUE QUIEN ACCEDE AL SERVICIO NO SEA REALMENTE QUIEN SE CREE? 53
TABLA XVIII. TRAZABILIDAD: ¿QUÉ IMPORTANCIA TENDRÍA QUE NO QUEDARA CONSTANCIA DEL ACCESO A LOS DATOS?....53
TABLA XIX. VALORES POSIBLES DE AMENAZAS....54
TABLA XX. RIESGOS E IMPACTOS 54
TABLA XXI. LISTADO DE IMPACTOS....55
TABLA XXII. COMPARATIVO ENTRE NMAP Y MASSCAN 60
TABLA XXIII. COMPARATIVO ENTRE NESSUS Y OPENVAS 60
TABLA XXIV. INSTRUMENTOS DE DOCUMENTACIÓN....62
TABLA XXV. TABLA DE TRATAMIENTO DE RIESGOS 62
TABLA XXVI. CONTROLES SELECCIONADOS Y JUSTIFICADOS....63
TABLA XXVII. COMPARACION DE RESULTADOS 64

LISTA DE FIGURAS

Pág.

Fig. 1. Esquema de red 39
Fig. 2. Valoración de activos 52
Fig. 3. Amenaza para software CMS para contenidos de sitio web 55
Fig. 4. Amenaza para software ofimática para los usuarios 56
Fig. 5. Amenaza para software correo electrónico basado en Gmail 56
Fig. 6. Amenaza para software gestión de recursos humanos 56
Fig. 7. Amenaza para repositorio datos CMS (MariaDB) 57
Fig. 8. Amenaza para repositorio de datos ofimáticos 57
Fig. 9. Amenaza para base de datos recursos humanos 57
Fig. 10. Amenaza para servidor Linux para CMS con apache 57
Fig. 11. Amenaza para servidor Windows Server para AD 57
Fig. 12. Amenaza para servidor Linux para BD de CMS MariaDB 58
Fig. 13. Amenaza para servidor Windows server para archivos (datos ofimáticos) 58
Fig. 14. Amenaza para servidor Windows server para DHCP/DNS 58
Fig. 15. Amenaza electrónica de red (switches) 58
Fig. 16. Amenaza para contrafuegos 59
Fig. 17. Amenaza router internet 59
Fig. 18. Administración centralizada de servicios mediante Nginx Proxy Manager 65
Fig. 19. Registro de parámetros técnicos de escaneo de servidor 65
Fig. 20. Monitoreo en firewall corporativo FortiGate 66
Fig. 21. Control de acceso a usuarios 66
Fig. 22. Acta de entrega y recepción hoja 1 67
Fig. 23. Acta de entrega y recepción hoja 2 68

LISTA DE ANEXOS

Pág.

Anexo 1. Carta de confidencialidad Jeison Gabriel Botina Diaz. Hoja 1 77
Anexo 2. Carta de confidencialidad Jeison Gabriel Botina Diaz. Hoja 2 78
Anexo 3. Carta de confidencialidad Jeison Gabriel Botina Diaz. Hoja 3 79
Anexo 4. Carta de confidencialidad Jeison Gabriel Botina Diaz. Hoja 4 80
Anexo 5. Carta de confidencialidad Jesus Esteban Orbes Zambrano. Hoja 1 81
Anexo 6. Carta de confidencialidad Jesus Esteban Orbes Zambrano. Hoja 2 82
Anexo 7. Carta de confidencialidad Jesus Esteban Orbes Zambrano. Hoja 3 83
Anexo 8. Acta de entrega y recepción hoja 1 84
Anexo 9. Acta de entrega y recepción hoja 2 85
Anexo 10. Aceptación de plan de SGSI. hoja 1 86
Anexo 11. Aceptación de plan de SGSI. hoja 2 87
Anexo 12. Encuesta estructurada – pregunta y respuesta 1 88
Anexo 13. Encuesta estructurada – pregunta y respuesta 2 88
Anexo 14. Encuesta estructurada – pregunta y respuesta 3 88
Anexo 15. Encuesta estructurada – pregunta y respuesta 4 89
Anexo 16. Encuesta estructurada – pregunta y respuesta 5 89
Anexo 17. Encuesta estructurada – pregunta y respuesta 6 90
Anexo 18. Encuesta estructurada – pregunta y respuesta 7 90
Anexo 19. Plan tratamiento de riesgos. Hoja 1 91
Anexo 20. Plan tratamiento de riesgos. Hoja 2 92
Anexo 21. Plan tratamiento de riesgos. Hoja 3 93
Anexo 22. Plan tratamiento de riesgos. Hoja 4 94
Anexo 23. Valoración de activos 95
Anexo 24. Matriz de riesgos sección 1 95
Anexo 25. Matriz de riesgos sección 2 96
Anexo 26. Matriz de riesgos sección 3 97
Anexo 27. Matriz de riesgos sección 4 97
Anexo 28. Matriz de riesgos sección 5 98
Anexo 29. Matriz de riesgos sección 6 98
Anexo 30. Matriz de riesgos sección 7 99
Anexo 31. Informe auditoria pág. 1 100
Anexo 32. Informe auditoria pág. 2 101
Anexo 33. Informe auditoria pág. 3 102
Anexo 34. Informe auditoria pág. 4 103
Anexo 35. Informe auditoria pág. 5 104
Anexo 36. Informe auditoria pág. 6 105
Anexo 37. Informe auditoria pág. 7 106
Anexo 38. Informe auditoria pág. 8 107
Anexo 39. Informe auditoria pág. 9 108
Anexo 40. Informe auditoria pág. 10 109
Anexo 41. Informe auditoria pág. 11 110
Anexo 42. Informe auditoria pág. 12 111
Anexo 43. Informe auditoria pág. 13 112

Anexo 44. Informe auditoria pág. 14 113
Anexo 45. Informe auditoria pág. 15 114
Anexo 46. Informe auditoria pág. 16 115
Anexo 47. Informe auditoria pág. 17 116
Anexo 48. Informe auditoria pág. 18 117
Anexo 49. Informe auditoria pág. 19 118
Anexo 50. Informe auditoria pág. 20 119
Anexo 51. Informe auditoria pág. 21 120
Anexo 52. Informe auditoria pág. 22 121
Anexo 52. Carta de entrega de Informe para iFactory 122
Anexo 52. Carta de agradecimiento al Ing. Camilo Gómez Arteaga. 123

INTRODUCCIÓN

La seguridad de la información se ha convertido en un pilar fundamental dentro de las organizaciones modernas, especialmente en un entorno donde las amenazas cibernéticas evolucionan constantemente. La protección de los datos no solo garantiza la estabilidad operativa de una empresa, sino que también refuerza la confianza de sus clientes y socios comerciales. En este contexto, surge la necesidad de establecer mecanismos efectivos para salvaguardar la confidencialidad, integridad y disponibilidad de la información.

En este trabajo se presenta un proyecto orientado a la implementación de un sistema de gestión de seguridad informática basado en la norma ISO 27001 en la empresa iFactory. Esta iniciativa tiene como propósito identificar, documentar y mitigar vulnerabilidades dentro de su infraestructura tecnológica mediante la aplicación de pruebas de pentesting y el diseño de controles adecuados. Con ello, se busca fortalecer la estructura de ciberseguridad de la organización y minimizar el impacto de posibles ataques informáticos.

El documento se estructura de la siguiente manera: en primer lugar, se expone la problemática y la justificación del proyecto, resaltando la importancia de la seguridad informática en el contexto actual. Posteriormente, se detallan los antecedentes y el marco teórico que sustenta la propuesta. Luego, se describe la metodología utilizada para el análisis de vulnerabilidades y el diseño del sistema de seguridad. Finalmente, se presentan los resultados obtenidos, la evaluación del impacto de la implementación y las conclusiones derivadas del estudio. Con este enfoque, se busca proporcionar una solución integral que contribuya a mejorar la seguridad de la información en iFactory y pueda ser replicada en otras organizaciones con necesidades similares.

I. PROBLEMA DE INVESTIGACIÓN

A. OBJETO O TEMA DE ESTUDIO

Sistema de gestión de seguridad informática basado en la norma ISO 27001 en la empresa iFactory durante el periodo 2025 y 2026.

B. LÍNEA DE INVESTIGACIÓN

Tecnologías de la información y las comunicaciones (TIC): Es la disciplina que, mediante el uso de herramientas informáticas y de telecomunicaciones, se encarga de gestionar el acceso, procesamiento y transmisión de la información de manera segura y eficiente. Su propósito es integrar sistemas digitales y redes de comunicación para garantizar la disponibilidad, confiabilidad y seguridad de los datos, facilitando la innovación y la conectividad en los diferentes ámbitos de la sociedad.

1) Sub línea de investigación

Seguridad informática: La seguridad informática enmarca todos los métodos y controles tecnológicos que se pueden implementar con el fin de mitigar el riesgo relacionado a las amenazas cibernéticas que pueden comprometer la privacidad, integridad o confidencialidad de los sistemas de información, incluyendo la transmisión y almacenamiento de la información tratada por los mismos, entre las principales amenazas se encuentran: Infección por malware, ataques de denegación de servicio, suplantación de identidades, errores de los usuarios, interceptación de las comunicaciones, entre otros [1].

C. PLANTEAMIENTO DEL PROBLEMA

La ciberseguridad es cada vez más importante en el mundo actual, ya que entidades y corporaciones de todos los tamaños son blanco de ciberataques y amenazas [1]. De acuerdo con datos recientes, el 43% de las pequeñas y medianas empresas (PYME) ha sufrido ciberataques, que podrían tener efectos muy perjudiciales para su actividad empresarial. En particular, las PYME son un objetivo atractivo para los ciberdelincuentes debido a sus limitados recursos para invertir en ciberseguridad [2].

En 2021, los ataques cibernéticos fueron categorizados como el quinto riesgo más alto y se establecieron como el nuevo estándar para los sectores público y privado. Esta industria de alto riesgo continuará expandiéndose en 2022, dado que se anticipa una duplicación de los ataques cibernéticos de IoT (Internet de las Cosas) para 2027 [3]. Por otra parte, según el Informe sobre Riesgos Mundiales 2022 del Foro Económico Mundial, en diciembre de 2021 se descubrió un fallo de seguridad crítico en un software muy utilizado. Los datos reflejaban que se detectaban más de 100 intentos de explotar la vulnerabilidad cada minuto, lo que ilustraba la vulnerabilidad de los sistemas informáticos [4].

Como consecuencia de la pandemia COVID 19, la ciberdelincuencia aumentó un 60%, desde robos y abusos hasta piratería informática y corrupción de datos. Alrededor de todas las industrias tuvieron que adoptar nuevas soluciones y obligar a las empresas a adaptarse rápidamente [5]. Aunque las compañías expertas en ciberseguridad durante todo el año promueven campañas y mensajes para advertir a diversos sectores acerca de la relevancia de tomar medidas preventivas en los lugares de visita, descarga de archivos, actualización de sus equipos, copias de seguridad o tener un proveedor de ciberseguridad unificado, también es necesario fomentar esfuerzos y colaboraciones a nivel gubernamental con el objetivo de que las instituciones se fortalezcan y sea capaces de adaptarse a las necesidades del entorno [6].

En este sentido, empresas del sector TI en Colombia como es el caso de iFactory, una empresa orientada al desarrollo de soluciones tecnológicas está expuesta a un riesgo considerable debido a la falta de un sistema formalmente estructurado de administración de seguridad de la información [7]. La infraestructura tecnológica asume una infraestructura funcionante. Sin embargo, la empresa no tiene políticas, procesos y medidas sistematizadas y establecidas que regulen la forma segura de tratar la información [8].

Dicho contexto deja a los activos digitales de la organización totalmente expuestos a amenazas que podrían referirse tanto a operarios internos o externos; las mismas se podría manifestar a través de la pérdida o divulgación de datos sensibles o acceso no controlado a la información, sabotajes informáticos, e incluso al secuestro de la información como en los casos de ransomware, entre otros [9]. Además de la poca probabilidad de los lineamientos se suma la falta de concienciación y formación, lo cual conlleva a que los trabajadores no estén preparados y crece la posibilidad de los errores humanos, así como no brindar soporte técnico a los clientes [10].

Lo anterior se complementa con una vulnerabilidad evidente sobre cómo responden las amenazas a la empresa, ya que no existe un protocolo de actuación ni medios nivelados para detectar, analizar y abortar la tendencia. Es decir, por citar un ejemplo muy simple, si se produce una amenaza directa por un acceso fraudulento a sus servidores o una brecha en una de las aplicaciones de reciente creación, esta empresa no puede establecer un sistema de respuesta eficaz y articulado en un tiempo récord [11].

De esta manera la falta de un plan preventivo basado en la identificación y acción de prevención de riesgos incrementa el grado de exposición de la organización a consecuencias graves como lo son: las interrupciones operativas prolongadas, pérdidas económicas y posibles demandas por parte de los clientes, así como a la perdida de bases de datos. Por esta razón, es importante que la empresa IFACTORY adopte la implementación de la norma ISO27001 que contribuya a esta organización a mitigar su vulnerabilidad actual permitiendo construir un entorno seguro que garantice la protección de datos y de su infraestructura tecnológica [12].

D. FORMULACIÓN DEL PROBLEMA

¿Cómo fortalecer la red de datos de la empresa iFactory protegiendo y garantizando la confidencialidad, integridad y disponibilidad de la información?

E. OBJETIVOS

1) Objetivo general

Formular un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001 en iFactory, orientado a proteger la red de datos mediante la gestión proactiva de riesgos, la implementación de controles técnicos y organizativos, y el aseguramiento de la confidencialidad, integridad y disponibilidad de la información.

2) Objetivos específicos

- Realizar un análisis de vulnerabilidades mediante pruebas de pentesting en la empresa iFactory y aplicar instrumentos, con el fin de documentar los hallazgos, riesgos detectados y recursos afectados.

- Diseñar un sistema de gestión de seguridad de la información (SGSI) conforme a la norma ISO/IEC 27001, ajustado a las demandas operativas y tecnológicas de iFactory, que facilite la administración estructurada de los riesgos vinculados a la seguridad de la información.

- Evaluar la efectividad del sistema de gestión de seguridad de la información (SGSI) mediante la comparación objetiva del estado de seguridad informática antes y después de su formulación, conforme a los requisitos de la norma ISO 27001.

F. JUSTIFICACIÓN

En la actualidad, la gestión de grandes volúmenes de información es clave para la operatividad de las empresas tecnológicas, donde la protección de datos se convierte en un pilar fundamental para garantizar la continuidad del negocio y minimizar riesgos [13]. iFactory, como empresa del sector TI, depende de la seguridad de su información, particularmente en el manejo de su código fuente, aplicaciones y datos generados por su departamento de desarrollo de software. No obstante, la organización enfrenta posibles vulnerabilidades que, de no ser abordadas, podrían comprometer su estabilidad operativa [14].

Para mitigar estos riesgos, es esencial formular un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO 27001, la cual establece políticas y controles estructurados para proteger la confidencialidad, integridad y disponibilidad de los activos digitales [15]. Este enfoque no solo previene el acceso no autorizado, alteraciones de datos o ataques informáticos, sino que también optimiza la respuesta ante incidentes de seguridad, minimizando el impacto en la infraestructura tecnológica [5].

En este sentido, la aplicación de un SGSI en iFactory permitirá la consolidación de estrategias de protección, integrando mecanismos técnicos como firewalls, cifrado TLS/SSL y sistemas IDS/IPS, junto con normativas organizativas enfocadas en el control de acceso y gestión de incidentes. Además, fortalecerá la cultura de seguridad entre los desarrolladores, promoviendo buenas prácticas a lo largo del ciclo de vida del software, asegurando así que la empresa opere en un entorno confiable y resiliente frente a amenazas emergentes [16].

Asimismo, el desarrollo de esta investigación aporta a la generación de nuevo conocimiento en el ámbito académico y profesional. En primer lugar, documenta un caso aplicado de formulación de un SGSI en una empresa del sector TI, constituyendo un referente para futuras investigaciones en organizaciones con características similares. En segundo lugar, contribuye a la identificación y sistematización de vulnerabilidades específicas en entornos de desarrollo de software, generando evidencia que fortalece metodologías de análisis de riesgos en contextos reales. Finalmente, fomenta la integración de controles técnicos y organizativos con la cultura de seguridad en equipos de desarrollo, aportando un enfoque interdisciplinario que combina gestión normativa, infraestructura tecnológica y prácticas de ingeniería de software

G. DELIMITACIÓN

El estudio se desarrollará en iFactory, una empresa que dispone de una infraestructura tecnológica robusta y adecuada para la ejecución de pruebas de seguridad informática y la validación de controles establecidos en la norma ISO 27001. La investigación se enfocará en la implementación de pruebas de penetración dirigidas a evaluar la seguridad de la infraestructura tecnológica de la organización, con el objetivo de identificar vulnerabilidades y desarrollar estrategias de protección alineadas con estándares internacionales.

La fase inicial del proyecto comenzará en el octavo semestre académico, en el primer semestre de 2025, período en el que se trabajará en la estructuración metodológica, el diseño del plan de trabajo y la recopilación preliminar de información sobre la infraestructura de iFactory. Posteriormente, el período de análisis comprenderá desde agosto de 2025 hasta julio de 2026, tiempo durante el cual se llevarán a cabo diversas fases del estudio. Inicialmente, se realizará la recolección de información y el análisis de riesgos existentes en la red y sistemas de información de iFactory. Posteriormente, se desarrollarán pruebas de penetración utilizando herramientas especializadas para evaluar posibles fallos en los controles de seguridad. Con base en los hallazgos obtenidos, se procederá a la implementación de un sistema de gestión de seguridad basado en la norma ISO 27001, el cual incluirá medidas correctivas y preventivas para reducir los riesgos en la infraestructura tecnológica de la empresa. Finalmente, se ejecutará un proceso de evaluación y validación de resultados, asegurando que las estrategias de protección sean efectivas y cumplan con los objetivos propuestos.

II. MARCO TEÓRICO

A. ANTECEDENTES

La literatura reciente sobre la implementación de la norma NTC-ISO/IEC 27001 y su impacto en diversas organizaciones ha aportado evidencia clave para el desarrollo de marcos de seguridad eficientes. En este sentido, Lizárraga et al. [17] realizaron en 2022 una revisión bibliográfica sobre auditorías de TI en entidades públicas y privadas, incluyendo PYMEs y MYPEs. Sus hallazgos indican que la aplicación de auditorías mejora la detección de riesgos, la administración de seguridad de la información y la productividad organizacional. No obstante, su investigación se centra en auditorías generales, sin profundizar en la implementación directa de la ISO 27001, lo que evidencia un vacío sobre cómo esta norma estructurada puede ser aplicada específicamente en empresas tecnológicas como iFactory.

Por otro lado, Minaya et al. [18] en 2023, investigaron vulnerabilidades y riesgos en activos de información, identificando el malware como la mayor amenaza y proponiendo la criptografía como solución principal. Aunque su estudio resulta relevante, no profundiza en el uso de un Sistema de Gestión de Seguridad de la Información (SGSI) que integre diversas capas de protección estructurada, aspecto que se considera clave en el presente proyecto. A diferencia de dicho enfoque, esta investigación no solo analiza amenazas, sino que además plantea una estrategia sistemática basada en ISO 27001 para mitigar riesgos de manera integral.

Siguiendo esta línea de ideas, Galecio et al. [19] llevaron a cabo un análisis teórico sobre normas internacionales en auditoría informática, resaltando su importancia para la seguridad de la información. Si bien su estudio enfatiza la relevancia de los estándares en la administración de riesgos, se limita a una evaluación conceptual, sin una aplicación práctica en entornos empresariales específicos. Por consiguiente, este trabajo busca llenar ese vacío al proponer una metodología concreta para la implementación de ISO 27001 en iFactory, asegurando un marco de seguridad sólido.

De manera complementaria, en 2024 Carrera et al. [20] exploraron el impacto de estándares internacionales en la Industria 4.0, destacando la necesidad de mejoras en ciberseguridad e interoperabilidad. Aunque el análisis enfatiza la relación entre normativas y tecnologías emergentes, no aborda directamente la seguridad informática ni la gestión estructurada de riesgos en el ámbito corporativo. Desde esta perspectiva, este proyecto complementa su investigación al enfocarse en la integración práctica de ISO 27001 en una empresa tecnológica, abordando vulnerabilidades específicas en redes de datos.

Finalmente, Galecio et al. [19] en 2025, examinaron la relación entre medidas de seguridad digital, estrategias educativas y sostenibilidad en entornos de aprendizaje en línea. Su estudio subraya la importancia de combinar prácticas pedagógicas con seguridad informática, pero no se centra en la implementación de marcos normativos en el sector empresarial. En contraste, esta investigación adapta los principios de seguridad digital a un contexto organizacional, asegurando que los controles de ISO 27001 sean aplicados de manera efectiva en iFactory.

B. SUPUESTOS TEÓRICOS

1) Seguridad de la información

En la actualidad, proteger la información es tan necesario como proteger cualquier otro activo de la empresa u organización. La seguridad de la información (InfoSec) es la protección de la información importante contra el acceso, la divulgación, el uso, la alteración o la interrupción no autorizados. Ayuda a garantizar que los datos confidenciales de la organización estén disponibles para los usuarios autorizados, permanezcan confidenciales y mantengan su integridad [6].

2) Norma ISO/IEC 27001

Se asume que aplicar la norma ISO/IEC 27001 ayuda a las organizaciones a tener un sistema organizado para controlar los riesgos que puedan afectar la información. Esta norma ofrece una estructura clara con políticas, procedimientos y controles que permiten gestionar la seguridad de forma preventiva. promueve un enfoque integral de la seguridad de la información, que abarca a las personas, las políticas y la tecnología. Un sistema de gestión de la seguridad de la información implantado conforme a esta norma es una herramienta clave para la gestión de riesgos, la resiliencia cibernética y la excelencia operativa [7]. Gracias a esto, se pueden tomar mejores decisiones y tener una respuesta más rápida frente a incidentes.

3) Seguridad informática

Se considera que la seguridad informática es fundamental para proteger los sistemas de la empresa frente a ataques como virus, intrusiones o robo de datos. Incluye el uso de herramientas tecnológicas, así como la capacitación del personal. Con frecuencia, las empresas son el objetivo de ataques de ransomware, o de chantajes que han de pagarse antes de que el pirata informático devuelva los activos de la compañía. Estar preparado con las herramientas y recursos adecuados es fundamental durante y después de un ciberataque. La seguridad informática se encarga de mantener la confidencialidad de los datos de tu organización y de recuperar el control mediante el uso de recursos de gestión de riesgos en el caso de que se haya producido algún incidente [6].

4) Análisis de vulnerabilidades

Aunque las vulnerabilidades se documentan exhaustivamente una vez que se descubren, los piratas informáticos y otros actores de amenazas suelen encontrarlas primero, lo que les permite tomar por sorpresa a las organizaciones. Para adoptar una postura de seguridad más proactiva ante estas amenazas cibernéticas, Los análisis de vulnerabilidades suelen ser el primer paso en el proceso de gestión de vulnerabilidades, ya que descubren las debilidades de seguridad que necesitan abordar [8].

5) Gestión de riesgos

Se entiende que la seguridad no puede ser estática, sino que debe actualizarse de forma constante. Evaluar riesgos permite identificar qué amenazas nuevas pueden surgir y qué tan expuesta está la organización, La gestión del riesgo no solo ayuda a identificar y controlar de manera proactiva las amenazas y vulnerabilidades que podrían afectar negativamente a la organización, sino que también permite establecer estrategias preventivas y de contingencia efectivas para mitigar su impacto [9], especialmente en una empresa tecnológica como iFactory.

6) Redes de datos

Una red de datos es una infraestructura creada con el propósito de transmitir información de cualquier naturaleza desde un punto a otro a través del intercambio de datos. Al contrario de lo que se pueda pensar, en estas redes no solo intervienen ordenadores, sino también elementos como los servidores y los centros de procesamiento de datos [10]. Si estas redes no están protegidas, la información que se transmite por ellas puede ser interceptada, modificada o destruida. Una red segura garantiza que la información llegue al destino correcto, sin alteraciones y sin ser vista por personas no autorizadas.

7) Kali Linux

Kali Linux es una distribución de Linux basada en Debian, específicamente diseñada para temas de seguridad muy variados, como análisis de redes, ataques inalámbricos, Contiene herramientas, Tanto en modo gráfico como, sobre todo, por comandos, lo que le convierte en un sistema muy completo, ya sea para defensores, que buscan un sistema más seguro, como para atacantes en busca de esos datos tan valiosos como cuentas, contraseñas y demás datos personales [11].

Además, es un software bastante potente y con multitud de usos avanzados para que un administrador pueda aprovecharla a fondo. Destacamos algunas de sus principales características:

- Es gratis, no tiene coste ninguno para usarlo tanto personal como profesionalmente.
- Cuenta con más de 600 herramientas para trabajar todo lo mencionado en el punto anterior.
- Está desarrollado en un entorno seguro, lo que ofrece muchas garantías acerca de datos y fallos.

8) Nmap

Este software posee varias funciones para sondear redes de computadores, incluyendo detección de equipos, servicios y sistemas operativos. Estas funciones son extensibles mediante el uso de scripts para proveer servicios de detección avanzados, detección de vulnerabilidades y otras aplicaciones. Además, durante un escaneo, es capaz de adaptarse a las condiciones de la red incluyendo latencia y congestión de la misma [12].

9) Burp Suite

Burp suite es un escáner de vulnerabilidades web y una de las herramientas más conocidas y utilizadas para realizar auditorías de seguridad de aplicaciones web. Burp suite se sitúa en el medio, entre el navegador del usuario y la plataforma web o api móvil a auditar, registrando todo el tráfico, detectando vulnerabilidades de forma pasiva y permitiendo modificar las peticiones HTTP realizadas para detectar anomalías y problemas de seguridad [13].

10) Caído

La interfaz de usuario de Caido está diseñada pensando en la eficiencia. Tanto profesionales como principiantes apreciará sus controles intuitivos y navegación clara, Ofrece una variedad de características de exploración que hacen que la identificación de vulnerabilidades y el análisis de solicitudes sean eficientes y en tiempo real. Algunas de sus herramientas incluyen un sitemap rico en funciones, historial y funciones de intercepción, lo que permite a los usuarios profundizar en la seguridad de las aplicaciones web [14].

11) Nessus

Es la solución de administración de vulnerabilidades más implementada del sector. Ayuda a las organizaciones a reducir su superficie de ataque y a garantizar el cumplimiento normativo. Esta herramienta ofrece detección de activos de alta velocidad, auditoría de configuraciones, creación de perfiles de destino, identificación de malware, descubrimiento de datos confidenciales, entre otras funcionalidades. Gracias a su biblioteca, la más grande del mundo en cuanto a verificaciones de vulnerabilidades y configuraciones, que se actualiza continuamente, Nessus establece el estándar en cuanto a velocidad y precisión en escaneos de vulnerabilidades [15].

12) OpenVAS

Es un escáner de vulnerabilidades de código abierto desarrollado por Greenbone Security Assistant que cuenta con una amplia base de datos de fallos de seguridad conocidos, para detectar en una red o sistema. OpenVAS es un software libre que sirve para detectar más de 100.000 vulnerabilidades en redes de manera interna y externa. Además, es muy fácil de utilizar. OpenVAS es un programa que ofrece soluciones de seguridad para hardware, software y la nube. Hardware es el conjunto de componentes físicos de los que está hecho el equipo y software es el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo [17]. OpenVas No solo sirve para detectar las vulnerabilidades de estos sistemas, también es eficiente para gestionarlas, es decir, hacer un registro de estas para futuras ocasiones [16].

13) Nikto

Es un escáner de servidor web de código abierto (GPL) y de uso gratuito que realiza un escaneo de vulnerabilidades en servidores web en busca de múltiples elementos, incluidos archivos y programas peligrosos, y busca versiones desactualizadas del software del servidor web. También

comprueba si hay errores de configuración del servidor y las posibles vulnerabilidades que puedan haber introducido. El proyecto del escáner de vulnerabilidades de Nikto es un esfuerzo en rápido movimiento, actualizado con frecuencia con las últimas vulnerabilidades conocidas. Esto te permite escanear tus servidores web con confianza mientras buscas posibles problemas [17].

14) CVE

CVE define las vulnerabilidades como un error dentro del código de software, que permite a un atacante obtener acceso directo no autorizado a los sistemas informáticos y redes y propagar malware. Esto generalmente permite a los atacantes hacerse pasar por administradores o super usuarios del sistema con privilegios de acceso completos a los recursos corporativos. La CVE define la exposición como errores en el código o la configuración del software, que permiten a un atacante obtener acceso indirecto a sistemas y redes. Esto podría permitir que el atacante aceche en las redes informáticas y recopile secretamente datos sensibles, credenciales de usuario e información del cliente [21].

15) NIST

El Marco de Ciberseguridad del NIST ayuda a los negocios de todo tamaño a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos. Este Marco es voluntario. Le brinda a su negocio una reseña de las mejores prácticas para ayudarlo a decidir dónde tiene que concentrar su tiempo y su dinero en cuestiones de protección de ciberseguridad. Usted puede implementar el Marco de Ciberseguridad del NIST en su negocio en estas cinco áreas: identificación protección, detección, respuesta y recuperación [19].

16) CISA

La Agencia de Ciberseguridad y Seguridad de las Infraestructuras (en inglés: Cybersecurity and Infrastructure Security Agency, abreviado CISA) es un componente del Departamento de Seguridad Nacional de los Estados Unidos (DHS) responsable de la ciberseguridad y la protección de las infraestructuras en todos los niveles del gobierno. Su objetivo es coordinar programas de ciberseguridad con los estados y mejorar el nivel de ciberseguridad del gobierno contra los ciberdelincuentes a título privado o al servicio de otro país [18].

17) OSSTMM

OSSTMM es un estándar internacional reconocido para la realización de pruebas de seguridad informática, proporcionando una metodología detallada para evaluar la seguridad en diversos sistemas, desde redes y aplicaciones web hasta dispositivos móviles y sistemas de control industrial. Su enfoque abierto y transparente, consensuado por expertos globales, lo hace indispensable para profesionales y organizaciones que aspiran a una seguridad de alto nivel. Este manual proporciona un marco de trabajo que describe las fases a seguir en la ejecución de una auditoría de seguridad o pentesting, y ha sido desarrollado gracias al consenso un gran grupo de

expertos internacionales en seguridad informática que colaboran para crear y mantener esta metodología [17].

18) OWASP

OWASP (Open Web Application Security Project) es una comunidad global de voluntarios y expertos en seguridad informática. Su misión es mejorar la seguridad de las aplicaciones web mediante la concienciación, la educación y la promoción de las mejores prácticas de seguridad. OWASP ofrece una amplia gama de recursos, herramientas y pautas para ayudar a las organizaciones a proteger sus aplicaciones web de amenazas y vulnerabilidades. Este sistema permite garantizar que la revisión de seguridad de una página web se realiza de forma adecuada, asegurando que analizamos todos los puntos clave para detectar cualquier fallo de seguridad [22].

19) ISO/IEC 27002

ISO/IEC 27002 es una norma internacional que brinda orientación a las organizaciones que desean establecer, implantar y mejorar un sistema de gestión de seguridad de la información (SGSI) centrado en la ciberseguridad. Mientras que ISO/IEC 27001 describe los requisitos aplicables a los SGSI, ISO/IEC 27002 ofrece buenas prácticas y objetivos de control relacionados con aspectos clave de la ciberseguridad, como el control de acceso, la criptografía, la seguridad de los recursos humanos y la respuesta ante incidentes. La criptografía utiliza varios algoritmos criptográficos de bajo nivel para lograr uno o más de dichos objetivos de seguridad de la información [23]. La norma ISO/IEC 27002 sirve de modelo práctico para las organizaciones que deseen proteger eficazmente sus activos de información contra las ciberamenazas. Al seguir las directrices de ISO/IEC 27002, las empresas pueden adoptar un enfoque proactivo de la gestión de riesgos de ciberseguridad y proteger la información crítica del acceso no autorizado y la pérdida [24].

20) ISO/IEC 27005

ISO 27005 es parte de la familia de estándares ISO 27000, creada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). Ayuda a las organizaciones a crear, monitorear y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). ISO 27005 se centra específicamente en la gestión de riesgos de seguridad de la información. El estándar internacional proporciona un enfoque organizado y sistemático para identificar, evaluar y gestionar los riesgos relacionados con la seguridad de la información.

- ISO 27001: Establece los requisitos para construir, monitorear y mejorar un SGSIISO [25].
- 27002: Específica controles de seguridad para salvaguardar el SGSIISO [24].
- 27005: Proporciona un marco de gestión de riesgos para el SGSI [26].

21) ISO/IEC 27032

ISO/IEC 27032 En la era actual de la información y la tecnología, la seguridad cibernética se ha convertido en un aspecto crucial para individuos, empresas y gobiernos por igual. La norma ISO 27032 emerge como una herramienta esencial para abordar los desafíos en constante evolución en el ámbito de la ciberseguridad. En este artículo, exploraremos en detalle qué es la norma ISO 27032 y cómo desempeña un papel fundamental en la protección de la sociedad digital de hoy [26].

La norma ISO 27032, también conocida como «Directrices para la Ciberseguridad «, es parte de la serie ISO 27000 que se centra en estándares relacionados con la seguridad de la información. Esta norma específica ofrece directrices detalladas para gestionar y mejorar la ciberseguridad en un mundo cada vez más interconectado [26].

22) Magerit

Tomando como referencia la norma ISO 31000, MAGERIT responde al "Proceso de Gestión de Riesgos" dentro del "Marco de Gestión de Riesgos". Es decir, esta metodología implementa la gestión de riesgos dentro de un marco de trabajo que permite a los órganos de gobierno tomar decisiones considerando los riesgos derivados del uso de tecnologías de la información [27].

23) CVSS

El Sistema Común de Puntuación de Vulnerabilidades (CVSS) es un marco estándar de la industria que se utiliza para evaluar y comunicar la gravedad de las vulnerabilidades de seguridad. El CVSS proporciona una puntuación numérica que refleja el impacto potencial de una vulnerabilidad, lo que ayuda a las organizaciones a priorizar sus esfuerzos de remediación en función del riesgo cibernético. El sistema es ampliamente utilizado por profesionales de seguridad, equipos de gestión de vulnerabilidades y analistas de riesgos cibernéticos para garantizar la coherencia en la evaluación y respuesta a las amenazas de ciberseguridad [28]. El riesgo cibernético se refiere al posible daño producido como resultado de una vulneración de los sistemas de información de una organización debido a ataques cibernéticos o errores humanos [29].

24) MTTD

El tiempo medio de detección, o MTTD, es el tiempo medio que un equipo de DevOps tarda en detectar un problema, como un error de software o un fallo de hardware, en una organización. El MTTD es uno de los indicadores de rendimiento clave de la gestión de incidentes. Como es lógico, cuanto antes descubra una organización un problema, mejor. Los incidentes con frecuencia provocan la inactividad del sistema, lo que de media puede costar 5600 $ por minuto, según Gartner. Aunque el MTTD no es la única métrica que los equipos de DevOps tienen a su disposición, es la más fácil de supervisar y medir y es un indicador esencial para cualquier organización que quiera evitar problemas como la interrupción del sistema [30].

25) MTTR

El MTTR incluye el tiempo que transcurre desde que se produce el fallo hasta que el sistema o equipo vuelve a ser plenamente funcional, lo que incluye el tiempo que se tarda en detectar el fallo, diagnosticar el problema y solucionarlo. El MTTR es una medida importante para monitorizar porque evalúa la disponibilidad y fiabilidad de los sistemas y equipos, la gravedad de los incidentes y la eficacia de los esfuerzos de reparación. Un MTTR alto puede provocar un tiempo de inactividad no planificado significativo. Al rastrear MTTR, las organizaciones pueden identificar áreas donde necesitan mejorar sus procesos, identificar tendencias en fallas y tomar decisiones sobre cómo optimizar sus estrategias de mantenimiento [31].

26) Triada CIA

La tríada de la CIA se refiere a la confidencialidad, la integridad y la disponibilidad, y describe un modelo diseñado para guiar las políticas de seguridad de la información (infosec) dentro de una organización. A veces se denomina tríada CIA (disponibilidad, integridad y confidencialidad) para evitar confusiones con la Agencia Central de Inteligencia (CIA). En este contexto, la confidencialidad es un conjunto de reglas de alto nivel que limitan el acceso a todo tipo de datos e información. La integridad es la garantía de que la información es fiable y precisa. Y la disponibilidad es una forma de gestión de riesgos para garantizar el acceso fiable a dicha información por parte de personas autorizadas [32].

27) Sistemas IDS/IPS

Los IDS/IPS detectan actividades sospechosas o no autorizadas, como los ataques de suplantación de identidad, la denegación de servicio, los ataques de intermediarios, los ataques de día cero, la inyección SQL, entre otros. Debido al crecimiento en la WAN en la nube y la movilidad, detener los ataques cibernéticos se ha vuelto cada vez más difícil y los atacantes se han vuelto más sofisticados en sus tácticas [32]. Una red de área amplia (WAN) es la tecnología que conecta entre sí a las oficinas, los centros de datos, las aplicaciones en la nube y el almacenamiento en la nube [33].

28) Cifrado TLS/SSL

El proceso de establecimiento de comunicación por TLS/SSL, que sucede sin que el usuario final lo note, crea una conexión protegida casi instantánea entre el servidor y el navegador cada vez que un sitio web recibe una visita. Los sitios web protegidos con un certificado TLS/SSL muestran el distintivo HTTPS y un pequeño candado en la barra de direcciones del navegador. Los certificados TLS/SSL protegen la información de los usuarios mientras esta se transfiere, autentican la identidad de la empresa a la que pertenece el sitio web y demuestran a los usuarios que están interactuando con los propietarios legítimos del sitio [34].

29) Firewalls

Los firewalls protegen contra el tráfico malicioso. Están estratégicamente posicionados en el borde de la red o en un centro de datos, lo que les permite monitorear de cerca cualquier cosa que intente cruzar este límite. Esta visibilidad también permite a un firewall de red inspeccionar y autenticar granular mente los paquetes de datos en tiempo real. Esto implica verificar el paquete de datos con criterios predefinidos para determinar si representa una amenaza. Si no cumple con los criterios, el firewall le impide entrar o salir de la red. Los firewalls regulan el tráfico entrante y saliente, protegiendo la red de:

Amenazas externas como virus, puertas traseras, correos electrónicos de suplantación de identidad y ataques de denegación de servicio. Los firewalls filtran los flujos de tráfico entrantes, evitando el acceso no autorizado a datos sensibles y frustrando posibles infecciones de malware [35].

Amenazas internas como actores maliciosos conocidos o aplicaciones riesgosas. Un firewall puede aplicar reglas y políticas para restringir ciertos tipos de tráfico saliente, lo que ayuda a identificar actividades sospechosas y mitigar la exfiltración de datos [35].

30) Red LAN

Una red LAN permite que todos los dispositivos dentro de nuestra oficina estén interconectados. Es un tipo de red muy útil para transferir datos y archivos entre usuarios. Al contar con conexión a Internet se pueden realizar muchas tareas, aunque también estamos expuestos a otros peligros. Hoy te contamos qué tipo de ataques puede recibir una red LAN [36].

Los malware: Este tipo de ataques digitales es potente, ya que tan solo necesita adentrarse en un dispositivo para hacerse con todo el sistema. Este tipo de ataques puede hacer que pierdas todos los datos almacenados o, incluso, que a través de un virus sufras daños económicos o de reputación [36].

Escuchas activas: A través del sistema podrían realizarse también inclusiones en vídeo llamadas o cualquier tipo de comunicación hablada. Poder acceder a los micrófonos de los dispositivos que utiliza el sistema para obtener información es una técnica cada vez más común [36].

Suplantación de DNS: Se trata de un “envenenamiento” que se apodera del servidor de nombres de dominio (DNS), aprovechando estos para desviar el tráfico y dirigirlo a otros dominios falsos. Además, almacena datos de inicios de sesión que pueden ser utilizados en un futuro [36].

Modificación de datos: A través de esta modificación de algunos datos de la red LAN de manera remota, los hackers podrían hacer que nuestros dispositivos y sistemas quedarán invalidados. Así, podrían hacerse con el control de todos nuestros documentos e información [36].

C. VARIABLES DEL ESTUDIO

1) Variable independiente

Sistema de Gestión de Seguridad Informática. Los factores a tener en cuenta en esta variable principalmente son:

- Implementación de controles del Anexo A Norma ISO 27001
- Técnicos: Firewalls, sistemas IDS/IPS, cifrado TLS/SSL (A.8.24).
- Organizativos: Políticas de acceso remoto (A.8.22), planes de respuesta a incidentes (A.5.24).

2) Variable dependiente

Nivel de seguridad de la red: Para el proceso de investigación se tendrán en cuenta las siguientes variables:

- Reducción de vulnerabilidades (ej. CVSS score promedio).
- Tiempo de detección/respuesta ante incidentes (ej. MTTD/MTTR).

Cumplimiento de la tríada CIA: Factores a tener presente:

- Confidencialidad*:* Número de accesos no autorizados detectados.
- Integridad*:* Casos de alteración no autorizada de datos.
- Disponibilidad*:* Tiempo de actividad (uptime) de servicios críticos.

D. DEFINICIÓN NOMINAL DE VARIABLES

1) Sistema de Gestión de Seguridad Informática

Agrupación de políticas, procedimientos y controles que implementan la técnica y el medio apropiado para proteger la información, la seguridad de los sistemas tecnológicos. Está alineada con el estándar de la norma ISO 27001, con el objetivo de asegurar la confidencialidad, la integridad y la disponibilidad de la información.

2) Nivel de seguridad de la red y cumplimiento de la tríada CIA

Medida que evalúa en función de la tríada CIA (Confidencialidad, Integridad y Disponibilidad) el nivel de la protección que debe tener una infraestructura de red, asegurando que la información sea accesible solamente para aquellas personas que tienen permitido acceder a la misma, que la información no sea modificada sin autorización y que la misma esté accesible cuando se necesite

E. DEFINICIÓN OPERATIVA DE VARIABLES

1) Sistema de Gestión de Seguridad Informática

Se medirá a través del nivel de implementación de los controles del Anexo A de la norma ISO 27001, evaluando la existencia y aplicación de políticas de seguridad, configuraciones técnicas de protección (firewalls, IDS/IPS, cifrado TLS/SSL) y medidas organizativas (políticas de acceso remoto, planes de respuesta a incidentes) mediante cuestionarios estructurados y auditorías de cumplimiento.

2) Nivel de seguridad de la red y cumplimiento de la tríada CIA

Se determinará mediante evaluaciones de vulnerabilidades y pruebas de penetración, analizando el grado de confidencialidad, integridad y disponibilidad de los sistemas a través de herramientas como Nmap, Burp Suite y Caido. Los resultados serán expresados en una escala de riesgo basada en el número de vulnerabilidades identificadas y su criticidad.

F. FORMULACIÓN DE HIPÓTESIS

1) Hipótesis de investigación

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 mejora significativamente la protección de la red informática, permitiendo una gestión estructurada de riesgos que reduce vulnerabilidades, optimiza los tiempos de detección y respuesta ante incidentes, y fortalece la confidencialidad, integridad y disponibilidad de los datos, garantizando un entorno seguro y resiliente para la organización.

2) Hipótesis nula

La implementación del Sistema de Gestión de Seguridad Informática basado en la norma ISO 27001 no tiene ningún efecto significativo en el nivel de seguridad de la red ni en la gestión de vulnerabilidades ni en la protección de la información.

3) Hipótesis alterna

La implementación del Sistema de Gestión de Seguridad Informática basado en norma ISO 27001 permite concientizar al personal de IFactory sobre el manejo pertinente de la información y fortaleciendo el cumplimiento de la tríada CIA (Confidencialidad, Integridad y Disponibilidad)

III. METODOLOGÍA

A. PARADIGMA

Un paradigma es entendido como el conjunto de conceptos, valores, técnicas y procedimientos compartidos por una comunidad científica, en un momento histórico determinado, para definir problemas y buscar soluciones [37]. Este proyecto se enmarca dentro del paradigma positivista, ya que adopta un enfoque metodológico cuantitativo para evaluar la seguridad informática en iFactory. A través de pruebas de pentesting y análisis de vulnerabilidades, se busca medir objetivamente el impacto de la implementación del SGSI basado en ISO 27001, garantizando resultados verificables y replicables.

B. ENFOQUE

Cuando hablamos de enfoque de investigación, nos referimos a la naturaleza del estudio, la cual se clasifica como cuantitativa, cualitativa o mixta; y abarca el proceso investigativo en todas sus etapas: desde la definición del tema y el planteamiento del problema de investigación, hasta el desarrollo de la perspectiva teórica, la definición de la estrategia metodológica, y la recolección, análisis e interpretación de los datos [38].

El enfoque de la investigación es mixto, ya que combina técnicas cuantitativas y cualitativas para analizar la seguridad informática en iFactory. Por un lado, el enfoque cuantitativo recopila datos sobre vulnerabilidades, tráfico en la red y efectividad de los controles de seguridad implementados. Por otro lado, el enfoque cualitativo examina las percepciones y prácticas del personal en la gestión de la seguridad, permitiendo adaptar el sistema a las necesidades reales de la organización.

C. MÉTODO

Los métodos de investigación son un elemento clave para la construcción de un conocimiento válido sobre un fenómeno particular, por lo que conocer en qué consisten, cuáles son sus características y de qué depende la elección de uno u otro resulta fundamental para todo investigador [39].

El método utilizado en esta investigación es de tipo deductivo, ya que parte del marco teórico de la norma ISO 27001 y los principios de seguridad informática para analizar su aplicación práctica en la red de datos de iFactory. A través de auditorías técnicas, pruebas de pentesting y análisis de vulnerabilidades, se busca contrastar los fundamentos teóricos con la situación real de la empresa, permitiendo validar la efectividad del SGSI propuesto. Este enfoque facilita la identificación de mejoras específicas basadas en normas internacionales, garantizando un análisis estructurado y objetivo.

D. TIPO DE INVESTIGACIÓN

Existen diferentes tipos de investigación y cada uno te puede servir en momentos diferentes, todo depende de las necesidades de tu estudio. Esto requiere seguir un proceso y aplicarlo para solucionar un problema o crear nuevo conocimiento [40]. La investigación es de tipo explicativa, ya que busca analizar las causas y efectos de las vulnerabilidades en la seguridad informática de iFactory y su relación con la implementación de un Sistema de Gestión de Seguridad Informática (SGSI) basado en la norma ISO 2700. A través de pruebas de pentesting y análisis de vulnerabilidades, se pretende identificar los factores que afectan la integridad, disponibilidad y confidencialidad de los datos, estableciendo una relación directa entre las amenazas detectadas y los controles de seguridad aplicados. Este enfoque permite fundamentar la importancia de un SGSI estructurado y validar su impacto en la protección de la infraestructura tecnológica de la empresa.

E. DISEÑO DE LA INVESTIGACIÓN

El diseño de investigación se define como los métodos y técnicas elegidos por un investigador para combinarlos de una manera razonablemente lógica para que el problema de la investigación sea manejado de manera eficiente [41]. La investigación se desarrollará mediante un estudio aplicado con enfoque práctico, orientado a la solución de un problema real en la empresa iFactory. Se utilizará un diseño no experimental, de tipo descriptivo y propositivo, ya que se analizará la situación actual de la seguridad de la información en la empresa y, a partir de ello, se propondrá la implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001.

F. POBLACIÓN

Es el conjunto de individuos u objetos de los que se desea conocer algo en una investigación. Es la totalidad de individuos o elementos en los cuales puede presentarse determinada característica que va a ser estudiada. Por lo general, no es posible abarcar a toda la población destinataria debido a su elevado número, al costo y al tiempo [42].

La población de este estudio está conformada por todos los sistemas y componentes de la red de datos de iFactory, así como por los colaboradores involucrados en la gestión y seguridad de la información dentro de la organización. Esto incluye tanto al personal técnico que maneja la infraestructura de red, como al personal administrativo que interactúa con la información y las aplicaciones utilizadas en el proceso diario de la empresa. Estos elementos son clave para entender el estado actual de la seguridad informática y las necesidades específicas de la organización para la implementación del Sistema de Gestión de Seguridad de la Información.

G. MUESTRA

En este estudio, la muestra estará compuesta por los sistemas y componentes de la red de datos de iFactory, seleccionados mediante un proceso estructurado para garantizar un análisis focalizado y eficiente. La identificación inicial incluirá todos los equipos detectados en la red, proporcionando una visión amplia de la infraestructura tecnológica. Posteriormente, se realizará un filtrado basado

en escaneo de puertos y servicios, permitiendo aislar los equipos críticos que representan mayores riesgos de seguridad. Sobre estos equipos críticos se aplicarán pruebas de pentesting, auditorías de vulnerabilidades y revisión de controles de seguridad con herramientas especializadas. Este enfoque progresivo facilitará una evaluación objetiva del estado de la seguridad informática, asegurando que las mejoras propuestas bajo la norma ISO/IEC 27001 [43] estén fundamentadas en evidencia precisa y relevante.

H. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Las técnicas de recolección de datos se refieren a los métodos utilizados para recoger y analizar diferentes formas de datos. Las técnicas habituales de recogida de datos incluyen el examen de documentos relacionados con un tema, así como la realización de entrevistas y observaciones [44]. Para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en iFactory, se emplearán diversas técnicas de recolección de información con el propósito de analizar el estado actual de la seguridad informática y los riesgos asociados. Estas técnicas permitirán recopilar datos relevantes tanto sobre la infraestructura tecnológica como sobre las prácticas de gestión de seguridad dentro de la empresa.

1) Análisis documental

Se realizará una revisión de documentos internos y externos relacionados con la seguridad informática, incluyendo normas y estándares de ISO/IEC 27001, políticas de seguridad existentes, reportes de auditorías previas, configuraciones de red y registros de incidentes de seguridad. Este análisis permitirá establecer el marco de referencia de la investigación y determinar las brechas actuales en la gestión de seguridad.

2) Observación directa

Se llevará a cabo un monitoreo del tráfico en la red de datos de iFactory, evaluando posibles vulnerabilidades mediante el uso de herramientas como Nmap, Burp Suite y Kali Linux. Además, se observarán las prácticas de seguridad implementadas por el personal de TI, identificando posibles debilidades en la administración y protección de la infraestructura tecnológica.

3) Pruebas de penetración (Pentesting)

Para detectar vulnerabilidades en la infraestructura de red de iFactory, se aplicarán pruebas de pentesting utilizando herramientas especializadas. Este procedimiento permitirá identificar fallas de seguridad en servidores, dispositivos de red y aplicaciones críticas, proporcionando datos clave para el diseño del SGSI.

4) Encuestas estructuradas

Se aplicarán encuestas al personal técnico de la empresa, con el objetivo de recopilar información sobre el nivel de conocimiento en seguridad informática, el cumplimiento de políticas de seguridad y las percepciones respecto a los riesgos existentes. Estas encuestas permitirán obtener una visión detallada de cómo la seguridad es gestionada en iFactory.

5) Entrevistas a expertos

Se realizarán entrevistas con especialistas en seguridad informática dentro de la empresa, incluyendo administradores de redes y responsables de ciberseguridad. A través de estas entrevistas, se obtendrán perspectivas sobre los principales desafíos de seguridad y las estrategias utilizadas para mitigar riesgos.

Este conjunto de técnicas garantizará una recolección de información integral y detallada, permitiendo evaluar tanto aspectos técnicos como administrativos de la seguridad informática en iFactory.

I. VALIDEZ DE LA TÉCNICA

La validez en la investigación son conceptos utilizados para evaluar la calidad de un estudio, y principalmente se utilizan en la investigación cuantitativa para indicar hasta qué punto un método, una técnica o una prueba mide algo de manera efectiva [45]. El análisis documental presenta alta validez de contenido, ya que se basa en normas y documentos clave de seguridad informática. Su validez de constructo también es alta al enfocarse en componentes esenciales del SGSI, y su validez de criterio se confirma al comparar los hallazgos con estándares reconocidos.

La observación directa tiene alta validez de contenido al examinar prácticas reales y tráfico de red. Su validez de constructo es alta porque permite evaluar comportamientos relacionados con la cultura de seguridad, y su validez de criterio se refuerza al contrastar lo observado con registros técnicos.

Las pruebas de penetración cuentan con muy alta validez en las tres dimensiones: el contenido por enfocarse en vulnerabilidades reales, el constructo por usar herramientas estandarizadas, y el criterio al validar los resultados con registros de incidentes o auditorías.

Las encuestas estructuradas tienen una validez de contenido media a alta, según la calidad del diseño del cuestionario. La validez del constructo es alta si las preguntas abordan conocimientos y percepciones de seguridad, y la de criterio es media, ya que depende del cruce con otros datos y de la sinceridad del personal.

Las entrevistas a expertos muestran alta validez en todas las dimensiones: el contenido por centrarse en temas estratégicos, el constructo por explorar aspectos clave de la gestión de riesgos, y el criterio al poder compararse con otros hallazgos técnicos o documentales.

J. CONFIABILIDAD DE LA TÉCNICA

La confiabilidad de los datos se refiere a la integridad y precisión de los datos como una medida de qué tanto puede contarse con que son constantes y no presentan errores en los distintos tiempos y fuentes [46]. En la implementación del SGSI en iFactory, la confiabilidad de las técnicas de recolección de datos se fundamenta en la estabilidad y consistencia de los resultados obtenidos mediante instrumentos rigurosamente diseñados. La solidez de métodos como el análisis documental, la observación directa, las pruebas de penetración y las encuestas estructuradas garantiza una aplicación válida y reproducible de las metodologías. Además, el desarrollo de estos procedimientos se optimiza mediante la asesoría de expertos, incluyendo docentes de investigación y el asesor del proyecto, quienes contribuyen a la pertinencia y precisión de los métodos utilizados, asegurando resultados confiables y alineados con los objetivos del estudio.

K. INSTRUMENTO DE RECOLECCIÓN DE DATOS

Existen diferentes instrumentos para recopilar información que se utilizan según el propósito. El diseño adecuado de estos instrumentos es esencial para llegar a conclusiones fiables y válidas [47]. Para garantizar la confiabilidad de los datos recopilados en esta investigación, se utilizarán instrumentos diseñados para minimizar variaciones en los resultados y asegurar la estabilidad de la información obtenida.

1) Matriz de análisis documental

Se empleará una matriz estructurada que categorice documentos clave como normas, políticas de seguridad, reportes técnicos y auditorías internas. Este instrumento permite organizar la información de manera sistemática y garantizar que los hallazgos sean replicables en diferentes momentos [25].

2) Lista de verificación para observación directa

Se elaborará un checklist con criterios específicos basados en la norma ISO 27002 para registrar la infraestructura y prácticas de seguridad en la red de datos de iFactory. Dado que la observación puede verse afectada por factores externos, este instrumento ayuda a estandarizar los parámetros de análisis y reducir la influencia subjetiva del observador [48].

3) Herramientas de pruebas de penetración (Pentesting)

Para garantizar la confiabilidad de los resultados en la detección de vulnerabilidades, se utilizarán herramientas especializadas como Kali Linux, Nmap y Burp Suite. Estos instrumentos permiten replicar pruebas bajo condiciones controladas, asegurando que los datos obtenidos sean consistentes en distintas ejecuciones.

4) Guía semiestructurada para entrevistas a expertos

Se desarrollará una guía de preguntas estratégicas que aborden aspectos técnicos y administrativos de la seguridad informática. Aunque las entrevistas dependen de las percepciones personales de los expertos, la estructura del instrumento ayudará a enfocar las respuestas en criterios objetivos y comparables.

Estos instrumentos fortalecen la consistencia y estabilidad de la recolección de información, permitiendo obtener datos confiables para el diseño del Sistema de Gestión de Seguridad de la Información (SGSI) en iFactory.

IV. RESULTADOS DE LA INVESTIGACIÓN

A. OBJETIVO 1. ANÁLISIS DE VULNERABILIDADES CON PRUEBAS DE PENTESTING EN LA EMPRESA IFACTORY

El proceso investigativo se desarrolló con base en la metodología **OSSTMM**, haciendo especial énfasis en el análisis de la red de datos de la organización. A continuación, se describen las principales fases ejecutadas durante la evaluación:

1) Alcance y reglas de compromiso

La universidad CESMAG cuenta con un documento formal que se utiliza en este tipo de proyectos, donde los investigadores se comprometen a garantizar la confidencialidad, integridad y disponibilidad de la información de la organización objeto de estudio y garantizar que los datos obtenidos durante el desarrollo del proyecto fueran utilizados únicamente con fines académicos y de investigación. El documento fue revisado por el Ingeniero de IFactory Camilo Gomez Arteaga, los estudiantes investigadores y asesor, para determinar el alcance del proyecto y las reglas de compromiso.

Este proyecto tiene como objetivo realizar una evaluación del nivel de seguridad de la red de datos de la institución, utilizando pruebas controladas basadas en la metodología OSSTMM.

El propósito es analizar cómo se encuentra actualmente la seguridad de la red, identificar posibles vulnerabilidades y proponer mejoras que ayuden a proteger mejor la información y los sistemas de la organización. Durante el desarrollo del proyecto se realizarán las siguientes actividades:

2) Actividades principales

Identificación de activos tecnológicos. Realizar un reconocimiento de los equipos, servidores, dispositivos de red y demás elementos que hacen parte de la infraestructura tecnológica.

Análisis de la red. Identificar los hosts, puertos abiertos y servicios disponibles dentro de la red institucional.

Revisión de configuraciones de seguridad. Evaluar cómo están configurados los dispositivos de red, servidores y servicios de comunicación.

Detección de vulnerabilidades. Analizar posibles fallas de seguridad en protocolos, aplicaciones o servicios que estén disponibles en la red.

Evaluación de controles de acceso. Revisar aspectos como autenticación de usuarios, segmentación de red y mecanismos de control de acceso.

Diagnóstico del estado de seguridad. Con la información obtenida elaborar un análisis general sobre el estado de seguridad de la red institucional.

3) Reglas de Compromiso (Rules of Engagement)

Las actividades de evaluación de seguridad se realizan en un entorno controlado y con autorización previa de la organización, buscando evitar cualquier afectación al funcionamiento normal de los sistemas. Para el desarrollo del proyecto se tendrá en cuenta las siguientes reglas:

- Las pruebas de seguridad se realizan únicamente sobre los activos de red que estén definidos dentro del alcance del proyecto.
- Se utilizan técnicas de análisis controladas y no destructivas, con el fin de evitar daños en los sistemas.
- No se realizan ataques de denegación de servicio (DoS) ni explotación activa de vulnerabilidades críticas.
- Las pruebas se ejecutan en horarios previamente acordados con la institución para evitar interrupciones en los servicios tecnológicos.
- Toda la información obtenida durante la evaluación se trata con confidencialidad y utilizada únicamente con fines académicos y de análisis.
- Si se detecta alguna vulnerabilidad importante, ésta se reporta a la organización para que pueda tomar las medidas necesarias.

4) Limitaciones del estudio

El presente estudio se enfoca principalmente en el análisis técnico de la seguridad de la red de datos, por lo que presenta algunas limitaciones que deben tenerse en cuenta. Entre las principales limitaciones se encuentran:

- La evaluación se centra principalmente en el canal de red de datos definido en la metodología OSSTMM, sin analizar otros canales como el físico o el humano.
- Las pruebas se realizan bajo un enfoque no intrusivo, lo que significa que no se explotarán completamente las vulnerabilidades encontradas.
- El análisis dependerá de la información disponible y del acceso autorizado a los activos de red por parte de la organización.
- Los resultados reflejan el estado de seguridad de la red en el momento en que se realiza la evaluación, por lo que pueden cambiar si se modifican configuraciones o se agregan nuevos equipos.
- La propuesta del Sistema de Gestión de Seguridad de la Información (SGSI) será un modelo de referencia, ya que su implementación completa dependerá de decisiones y recursos de la organización.

5) Reconocimiento (Footprinting)

Durante la fase de reconocimiento, también denominada prueba de entorno parcialmente conocido (hacking de caja gris), se procedió a identificar los activos tecnológicos y la infraestructura de red asociada a la organización Ifactory. Este proceso tuvo como objetivo levantar un mapa detallado de la arquitectura de red y de los recursos tecnológicos que soportan las operaciones críticas de la empresa.

La metodología aplicada permitió obtener una visión estructurada de la conectividad interna y externa, destacando los principales puntos de interconexión entre la red corporativa, los centros de datos y los mecanismos de acceso a internet. Como resultado, se elaboró un diagrama de red que representa gráficamente la topología tecnológica, facilitando la comprensión de las relaciones entre los diferentes componentes y servicios.

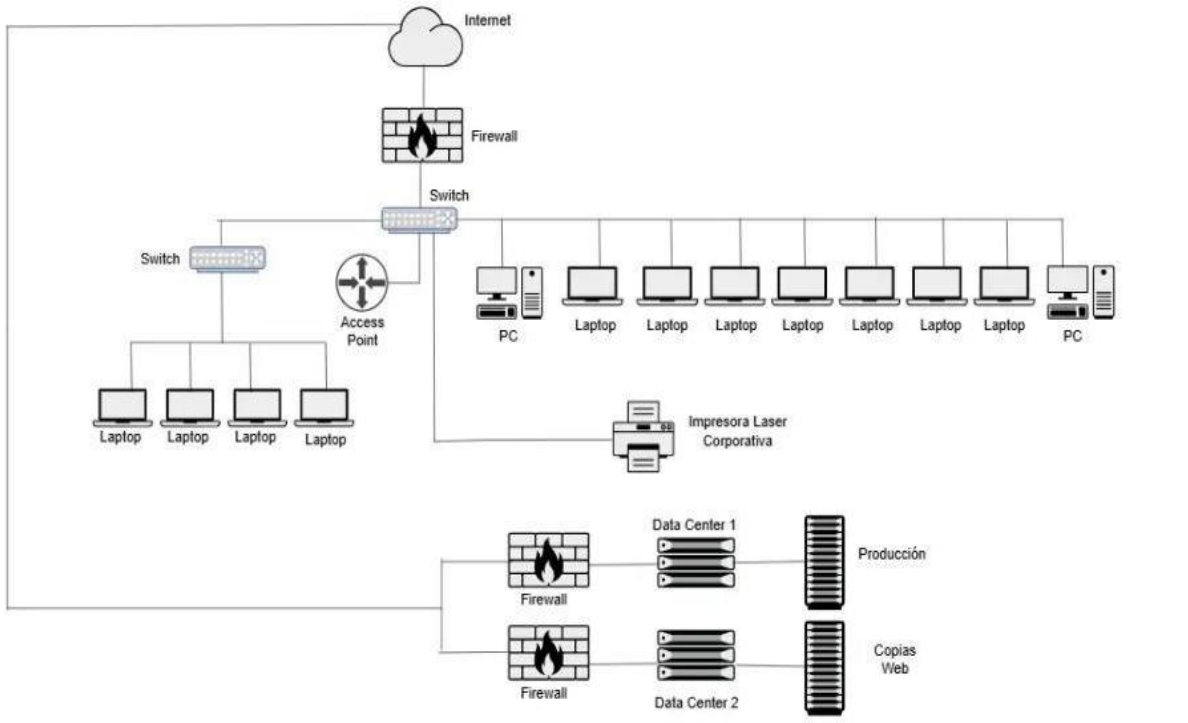


Fig. 1. Esquema de red

Este análisis se complementó con un inventario de activos tecnológicos, producto del reconocimiento realizado, en el cual se consolidan los equipos, servidores, dispositivos de red y servicios identificados. dicho inventario constituye la base para posteriores fases de evaluación de riesgos y pruebas de seguridad, al correlacionar vulnerabilidades potenciales con los activos críticos de la organización.

TABLA I. INVENTARIO DE ACTIVOS TECNOLÓGICOS

Activo	Modelo/Especificaciones	Segmento	Función	Criticidad	Riesgos/Observaciones
Servidor Dell PowerEdge R740	2x Xeon, 64 GB RAM, 40 TB RAID	Data Center Producción	ERP corporativo	ALTA	Dependencia de redundancia eléctrica
Servidor HP ProLiant DL380	1x Xeon, 64 GB RAM,40 TB RAID	Data Center Copias Web	Base de datos y réplicas	ALTA	Respaldos periódicos necesarios
Router Ubiquiti	EdgeRouter (Gigabit)	Borde WAN	Conexión ISP ↔ LAN	ALTA	Administración flexible
Switch capa 2	24 puertos Gigabit	Core LAN	Distribución interna	MEDIA	Requiere redundancia
Laptops corporativas	Intel i5/i7, 16 GB RAM	LAN interna / WiFi	Estaciones móviles	MEDIA	Riesgo de acceso no autorizado
Impresora Samsung ML-4551ND	Láser, red corporativa	LAN interna	Servicio de impresión	BAJA	Riesgo de fuga documental
Firewall Fortinet Fortigate 200E	Throughput 2 Gbps, IPS/IDS	Borde WAN	Seguridad perimetral	ALTA	Punto de entrada principal
Firewall Fortigate 90D	Throughput 1 Gbps	DMZ	Segmentación y filtrado	ALTA	Control de tráfico hacia servidores
Firewall Fortigate 60D	Throughput 800 Mbps	LAN interna	Protección segmentada	MEDIA	Uso en subredes específicas
PCs corporativos	Intel i7, 16GB RAM	LAN interna	Estaciones fijas	MEDIA	Uso administrativo

TABLA II. RESUMEN DEL ESQUEMA DE RED

Categoría	Activo	Ubicación/segmento	Función principal	Criticidad	Observaciones
Seguridad	Firewall perimetral	Borde WAN ↔ Internet	Filtrado de tráfico externo	ALTA	Punto de entrada desde internet
Red	Switch principal	Core LAN	Distribución de red interna	ALTA	Conecta todos los segmentos
Red	Access Point + Switch secundario	LAN inalámbrica	Conexión de laptops via WIFI	MEDIA	Riesgo de acceso no autorizado

Categoría	Activo	Ubicación/segmento	Función principal	Criticidad	Observaciones
Usuarios	Laptops (11)	LAN interna/ Wifi	Estaciones de trabajo móviles	MEDIA	Segmentación por VLAN recomendada
Usuarios	PCs (2)	LAN interna	Estaciones de trabajo fijas	MEDIA	Uso administrativo
Impresión	Impresora láser corporativa	LAN interna	Servicio de impresión compartido	BAJA	Riesgo de fuga de información
Seguridad	Firewall interno	Enlace hacia Data Centers	Segmentación y protección	ALTA	Control de tráfico hacia servidores
Servidores	Data Center 1(Producción)	Segmento protegido	Hospeda aplicaciones críticas	ALTA	Requiere redundancia y respaldo
Servidores	Data Center 2 (Copias Web)	Segmento protegido	Hospeda réplicas y servicios web	MEDIA	Función de contingencia

La fase de reconocimiento permitió consolidar un inventario detallado de los activos tecnológicos y levantar un esquema claro de la topología de red, identificando los puntos críticos de interconexión y seguridad. Este análisis evidenció la importancia de proteger la infraestructura, especialmente los servidores de producción y los mecanismos de acceso perimetral, ya que constituían la base operativa de la organización. Con esta información estructurada, se contaron con los insumos necesarios para avanzar hacia la fase de escaneo y mapeo de la red, en la cual se profundizará en la detección de vulnerabilidades y la validación de la exposición de los servicios identificados.

6) Escaneo y mapeo de red

Este paso es crítico porque traduce los objetivos del estudio en instrumentos operativos, garantizando que los hallazgos sean medibles y verificables, en el caso de iFactory, la selección se realizó considerando tres criterios principales:

Compatibilidad con la infraestructura tecnológica existente: se eligieron herramientas capaces de interactuar con firewalls Fortinet, servidores Windows/Linux y dispositivos de red.

Normativa internacional y validez técnica: se priorizaron herramientas ampliamente utilizadas en auditorías de seguridad, como Nmap, Masscan, Nessus y OpenVAS, todas referenciadas en normativas y marcos como ISO/IEC 27001 y OSSTMM.

Cobertura funcional: se buscó que las herramientas abarcaran diferentes niveles de análisis:

- **Nmap y Masscan:** detección de puertos y servicios expuestos.
- **Nikto y Burp Suite:** auditoría de aplicaciones web.
- **Nessus y OpenVAS:** escaneo profundo de vulnerabilidades con clasificación por criticidad.

Bitácora técnica: con fechas, acciones realizadas y resultados obtenidos (ejemplo: instalación de Kali Linux, ejecución de Nmap, escaneo con Nessus). Esta bitácora asegura trazabilidad y transparencia en el proceso investigativo.

7) Bitácora Técnica

A continuación, se presentó la bitácora técnica desarrollada durante esta fase, en la cual se registraron de manera cronológica las acciones realizadas, las herramientas utilizadas y los resultados obtenidos. Este registro constituyó la evidencia operativa del proceso y permitió documentar cada actividad con precisión.

TABLA III. BITÁCORA TÉCNICA

Fecha y Hora	Acciones Realizadas	Resultados Obtenidos
13 de septiembre 2025 9:30AM – 12:00PM	Recolección de información de los activos de información de iFactory.	Se elaboró un inventario detallado que identifica, clasifica y valora los activos críticos para la seguridad.
20 de septiembre 2025 9:30AM – 12:00 PM	Instalación de VirtualBox versión 7.2.2 en equipo local.	Se habilitó el entorno de virtualización para pruebas de seguridad.
20 de septiembre 2025 10:30AM – 12:00 PM	Instalación de Kali Linux versión 2025.3 en máquina virtual de VirtualBox.	Se configuró el sistema operativo especializado en análisis de seguridad.
27 de septiembre 2025 9:30AM – 12:00 PM	Habilitación de cuenta en el servidor de iFactory.	Se obtuvo acceso remoto para realizar pruebas internas de seguridad.
4 de octubre 2025 9:30AM – 12:00 PM	Instalación de VirtualBox 7.2.2 dentro del servidor.	Se replicó el entorno de pruebas en el servidor institucional.
4 de octubre 2025 11:00AM – 12:00 PM	Instalación de Kali Linux 2025.3 en máquina virtual del servidor.	Se habilitó el entorno de análisis dentro del servidor para escaneos internos.
11 de octubre 2025 9:00AM – 12:00 PM	Ejecución de escaneos con NMAP y MASSCAN dentro y fuera del servidor.	Se identificaron puertos abiertos, servicios expuestos y hosts activos. Se detectaron riesgos potenciales.
25 de octubre 2025	Ejecución de escaneos con Nikto versión 2.5.0 y configuración de	en la herramienta de nikto no obtuvimos resultados ya que esta

Fecha y Hora	Acciones Realizadas	Resultados Obtenidos
9:00 AM – 12:00 PM	Burpsuite, configuración del FoxyProxy en el navegador de firefox en Kali linux y ejecución de esta misma	herramienta está enfocada a servidores web, mismo caso con burpsuite
29 de octubre 2025 9:00 AM – 12:00 PM	Se procedió a ejecutar nuevamente Nikto y BurpSuite, incorporando ciertas recomendaciones y nuevas acciones en ambas herramientas. Sin embargo, los resultados obtenidos fueron los mismos, lo que permitió descartar posibles errores cometidos en ejecuciones anteriores.	Tras la reejecución de Nikto y BurpSuite con ajustes recomendados, se obtuvieron los mismos hallazgos que en las pruebas anteriores. Esto confirma la consistencia de los resultados y permite descartar posibles errores de configuración o interpretación en ejecuciones previas.
30 de octubre 2025 9:00 AM – 12 PM	se realizó la respectiva instalación de nessus, después se procedió a realizar el escaneo de vulnerabilidades fuera del servidor.	El escaneo de vulnerabilidades con Nessus al host 192.168.0.127 detectó 61 vulnerabilidades, incluyendo 4 altas, 1 media y varias informativas. Las más críticas afectan a Ruby REXML y Ruby RACK, y se identificó un certificado SSL no confiable.
1 de noviembre 2025 9:00 AM – 12 PM	con la respectiva instalación realizada anteriormente se procedió a hacer el escaneo dentro del servidor	El escaneo en el servidor 192.168.2.36 detectó 33 vulnerabilidades, incluyendo 1 alta y varias medias, principalmente relacionadas con configuraciones y protocolos SSL/TLS desactualizados. El resto son hallazgos informativos sobre servicios y sistemas.
8 de noviembre 2025 9:00 AM – 12 PM	se realiza la instalación de openvas dentro del servidor asignado	La instalación de OpenVAS se completó correctamente en el servidor asignado. El sistema está listo para ejecutar escaneos de vulnerabilidades de forma confiable.
15 de noviembre 2025 9:00 AM – 12 PM	realizada la respectiva instalación de openvas procedimos a configurar el acceso	La configuración de acceso a la consola de OpenVAS se realizó de forma exitosa, verificando el funcionamiento del servicio web y el ingreso correcto con el usuario administrador sin presentar ningún inconveniente.
18 de noviembre 2025 2:00 PM – 6:00 PM	Se realizó el escaneo completo al servidor con openVAS, confirmando que el proceso se ejecutó correctamente	el escaneo se realizó de forma exitosa, verificando todo tipo de vulnerabilidades mediante la clasificación de vulnerabilidades de OpenVAS

A continuación, se muestra la tabla x donde se puede visualizar la información de las herramientas utilizadas.

TABLA IV. HERRAMIENTAS SELECCIONADAS Y SU PROPÓSITO

Herramienta	Función principal	Principal Hallazgo
Masscan	Barrido rápido de puertos	Detección de 22/SSH y 808/HTTP
Nmap	Identificación detallada de servicios	Confirmación de RDP (3389) y WinRM (5985)
Nessus	Escaneo profundo de vulnerabilidades	61 vulnerabilidades, 4 críticas (Ruby REXML, RACK)
OpenVAS	Validación y gestión de vulnerabilidades	Configuración SSL/TLS desactualizada
Nikto	Escaneo de servidores web	Sin hallazgos relevantes en host 192.168.2.36
Burp Suite	Auditoría de aplicaciones web	fallo de conexión proxy, descartado

Se presentan a continuación las evidencias obtenidas durante la fase de escaneo y mapeo de la infraestructura de red.

TABLA V. RESULTADOS DE ESCANEO CON LA HERRAMIENTA NMAP 1

Escaneo herramienta: NMAP		
Equipo: Laptop Corporativa	Auditor: Jeison Gabriel Botina Diaz	Fecha: 12 de Octubre

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- 192.168.0.1
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-11 10:36 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0011s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  open   ssh
113/tcp closed ident
808/tcp open   ccproxy-http
MAC Address: 08:5B:0E:B2:06:6E (Fortinet)

Nmap done: 1 IP address (1 host up) scanned in 120.32 seconds
```

Resultados Esperados	Resultados Obtenidos
• Que el host respondiera al escaneo confirmando su disponibilidad en la red. • Que el puerto 22/tcp (SSH) estuviera abierto para administración remota. • Que el puerto 113/tcp (Ident) apareciera cerrado o filtrado. • Que el puerto 808/tcp mostrara algún servicio web o proxy activo. • Que el resto de los puertos estuvieran filtrados o sin respuesta, acorde a políticas de seguridad.	● El host respondió correctamente con latencia de 0.0011s, confirmando que está activo. El puerto 22/tcp se encontró **abierto** con servicio SSH. ● El puerto 113/tcp se reportó como **cerrado**. ● El puerto 808/tcp se encontró **abierto**, identificado como servicio **ccproxy-http**. ● Se detectaron **65532 puertos filtrados**, lo que confirma la existencia de reglas de firewall activas. ● La dirección MAC corresponde a un dispositivo **Fortinet**, lo que valida la presencia de un firewall en el borde de la red.

TABLA VI. RESULTADOS DE ESCANEO CON LA HERRAMIENTA NMAP 2

Escaneo herramienta: NMAP		
Equipo: Laptop Corporativa	Auditor: Jesus Esteban Orbes Zambrano	Fecha: 12 de Octubre

```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-11 10:46 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.1
Host is up (0.0029s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  open   ssh
113/tcp closed ident
808/tcp open   ccproxy-http
MAC Address: 08:5B:0E:B2:06:6E (Fortinet)

Nmap done: 1 IP address (1 host up) scanned in 44.31 seconds
```

Resultados Esperados	Resultados Obtenidos
• Que el host respondiera al escaneo confirmando su disponibilidad en la red. • Que el puerto 22/tcp (SSH) estuviera abierto para administración remota. • Que el puerto 113/tcp (Ident) apareciera cerrado o filtrado. • Que el puerto 808/tcp mostrara algún servicio web o proxy activo. • Que el resto de los puertos estuvieran filtrados, acorde a políticas de seguridad. • Que los scripts de vulnerabilidades no detectaran fallos críticos en los servicios básicos.	● El host respondió correctamente con latencia de 0.0029s, confirmando que está activo. El puerto 22/tcp se encontró **abierto** con servicio SSH. ● El puerto 113/tcp se reportó como **cerrado**. ● El puerto 808/tcp se encontró **abierto**, identificado como servicio **cproxy-http**. ● Se detectaron **997 puertos filtrados**, lo que confirma la existencia de reglas de firewall activas. ● El script broadcast-avahi-dos verificó que el host no era vulnerable al CVE-2011-1002, descartando riesgos en ese vector. ● La dirección MAC corresponde a un dispositivo **Fortinet**, validando la presencia de un firewall en el borde de la red

8) Evaluación de seguridad en puertos abiertos

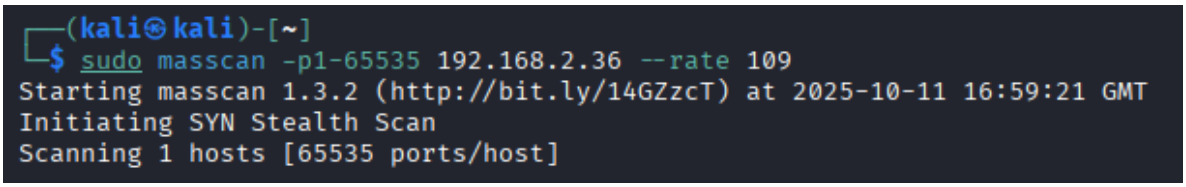
Posteriormente, se realizó un análisis de los puertos detectados en el escaneo, evaluando los riesgos asociados a cada servicio abierto y las recomendaciones de seguridad correspondientes a los resultados obtenidos del Escaneo con Nmap.

TABLA VII. PUERTOS DETECTADOS EN EL ESCANEO

Puerto	Servicio	Seguridad (open)
22/tcp	ssh	El puerto 22 está abierto por defecto para SSH (Secure Shell), un protocolo que cifra las comunicaciones y permite la administración remota de servidores. Si bien es una configuración estándar, su abertura puede representar un riesgo de seguridad, por lo que se recomienda cambiarlo a un puerto no predeterminado, especialmente en servidores que se exponen directamente a Internet
808/tcp	ccproxy-http	El puerto 808/tcp está abierto por defecto para servicios HTTP alternativos, y en este caso está vinculado al servicio ccproxy-http, un servidor proxy que permite compartir y controlar el acceso a Internet. Aunque puede ser útil en entornos de red interna, su exposición directa a Internet representa un riesgo de seguridad considerable. Se recomienda restringir el acceso mediante firewall, habilitar autenticación en el proxy, y evitar configuraciones que lo conviertan en un proxy abierto, ya que podría ser explotado por terceros para ocultar actividades maliciosas o lanzar ataques desde tu red.

TABLA VIII. RESULTADOS DE ESCANEO CON LA HERRAMIENTA MASSCAN 1

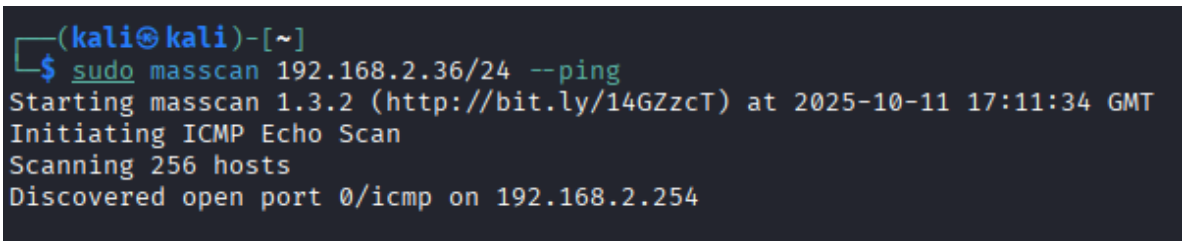
Escaneo herramienta: Masscan		
Equipo: Laptop Corporativa	Auditor: Jeison Gabriel Botina Diaz	Fecha: 12 de Octubre



Resultados Esperados	Resultados Obtenidos
● Que el host respondiera al escaneo confirmando su disponibilidad en la red. Que se identificaran los puertos abiertos en el rango completo (1–65535). ● Que los servicios críticos (como SSH o HTTP) estuvieran activos en puertos conocidos. ● Que la mayoría de los puertos permanecieran cerrados o filtrados, acorde a las políticas de seguridad. ● Que el escaneo se completara sin errores, mostrando evidencia clara de los puertos detectados.	● El escaneo se ejecutó correctamente sobre el host 192.168.2.36, abarcando los 65.535 puertos TCP. El sistema respondió al proceso, confirmando que el host está activo. ● Se obtuvo evidencia de los puertos abiertos (según la salida de Masscan), destacando aquellos con servicios activos. ● La mayoría de los puertos se reportaron como cerrados o filtrados, validando la existencia de reglas de firewall y segmentación. ● El resultado fue consistente con lo esperado: Masscan permitió identificar de manera rápida los puertos expuestos, sirviendo como base para posteriores análisis de vulnerabilidades.

TABLA IX. RESULTADOS DE ESCANEO CON LA HERRAMIENTA MASSCAN 2

Escaneo herramienta: Masscan		
Equipo: Laptop Corporativa	Auditor: Jeison Gabriel Botina Diaz	Fecha: 12 de Octubre



Resultados Esperados	Resultados Obtenidos
• Que el escaneo identificara los hosts activos dentro del rango. • Que se confirmara la disponibilidad de los equipos mediante respuesta ICMP (ping). • Que se detectaran direcciones IP vivas en la red, especialmente las asociadas a infraestructura crítica. • Que la mayoría de los hosts permanecieran sin respuesta, acorde a las políticas de seguridad y segmentación.	• El escaneo se ejecutó correctamente sobre los 256 hosts de la subred. • Se confirmó la disponibilidad de al menos un host activo, que respondió al ping ICMP (puerto 0/icmp abierto). • El resto de los hosts no respondieron, lo que valida la existencia de reglas de firewall o configuraciones de seguridad que bloquean ICMP. • El resultado fue consistente con lo esperado: Masscan permitió identificar de manera rápida los equipos activos en la red, sirviendo como base para posteriores escaneos de puertos y vulnerabilidades.

TABLA X. RESULTADOS DE ESCANEO CON LA HERRAMIENTA NIKTO

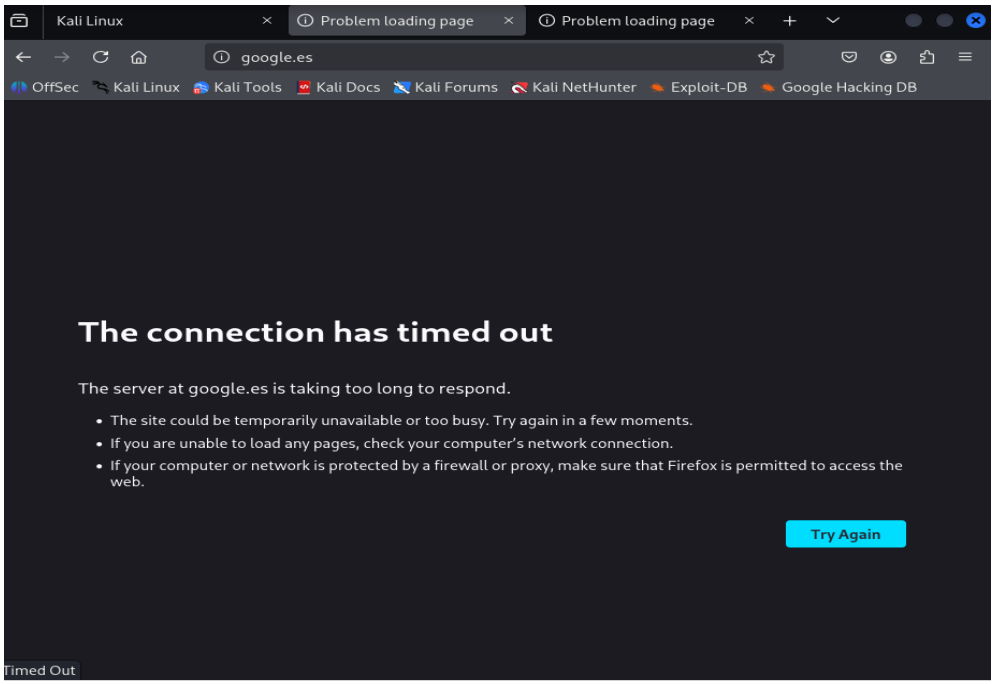
Escaneo herramienta: Nikto		
Equipo: Laptop Corporativa	Auditor: Jesus Esteban Orbes Zambrano	Fecha: 12 de Octubre



Resultados Esperados	Resultados Obtenidos
• Que el host respondiera al escaneo confirmando la disponibilidad del servicio web. • Que Nikto identificará posibles vulnerabilidades en el servidor HTTP, como configuraciones inseguras, certificados SSL débiles o directorios expuestos. • Que se obtuviera un listado de hallazgos relacionados con seguridad web.	• El escaneo se ejecutó, pero no se logró analizar ningún host: el resultado mostró “0 host(s) tested”. • No se obtuvieron hallazgos ni vulnerabilidades, lo que indica que el servicio web no respondió o no estaba disponible en el momento del análisis. • El resultado fue diferente a lo esperado, ya que no se generó evidencia de vulnerabilidades ni de configuraciones inseguras

TABLA XI. RESULTADOS DE ESCANEO CON LA HERRAMIENTA BURPSUITE

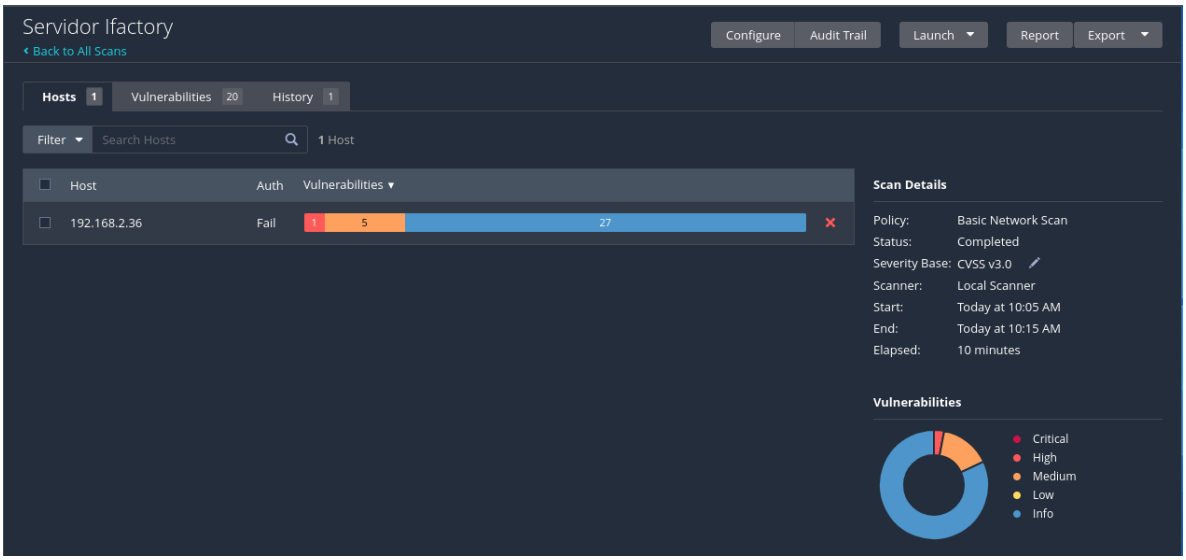
Escaneo herramienta: Burpsuite		
Equipo: Laptop Corporativa	Auditor: Jesus Esteban Orbes Zambrano	Fecha: 12 de Octubre



Resultados Esperados	Resultados Obtenidos
● Que el navegador Firefox, con FoxyProxy configurado, redirigiera correctamente el tráfico hacia BurpSuite. Que BurpSuite capturara las peticiones HTTP/HTTPS realizadas al sitio google.es. ● Que se visualizarán las solicitudes interceptadas en la consola de BurpSuite para su análisis. ● Que el acceso al sitio web funcionara normalmente, permitiendo comprobar la interceptación sin errores de conexión.	● Al intentar acceder a google.es desde Firefox con FoxyProxy activo, se presentó un **error de conexión por tiempo de espera**. El navegador no logró establecer comunicación con el servidor, por lo que BurpSuite no capturó tráfico alguno. ● El resultado fue distinto a lo esperado: en lugar de interceptar las solicitudes, se evidenció un fallo de conectividad, posiblemente relacionado con la configuración del proxy, el firewall o la ausencia de un servicio web accesible en ese momento. ● La evidencia confirma que la integración entre FoxyProxy y BurpSuite no funcionó como se esperaba en esta prueba inicial.

TABLA XII. RESULTADOS DE ESCANEO CON LA HERRAMIENTA NESSUS

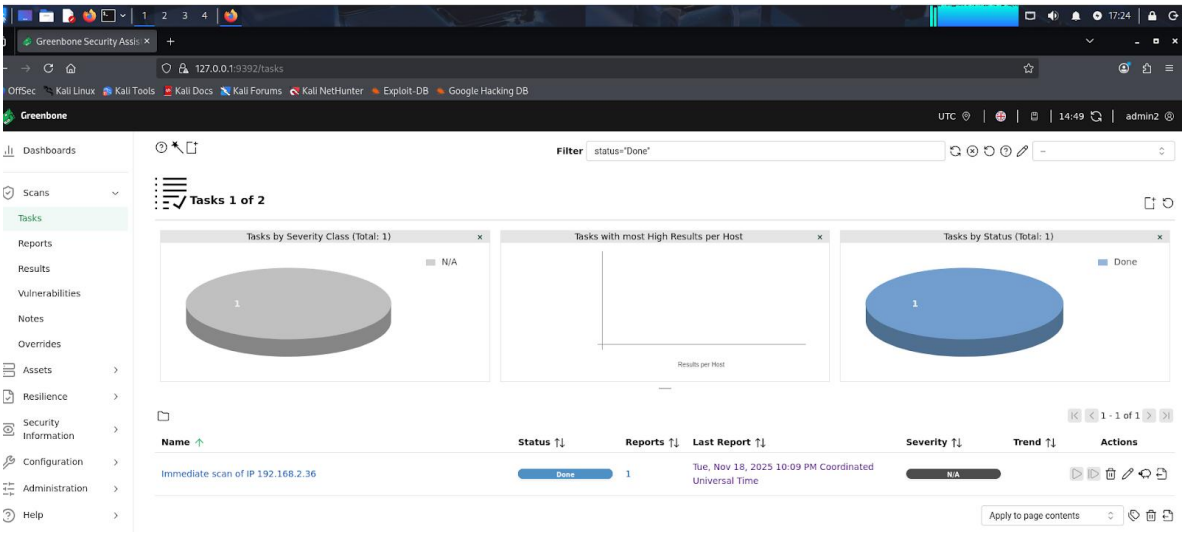
Escaneo herramienta: Nessus		
Equipo: Laptop Corporativa	Auditor: Jesus Esteban Orbes Zambrano	Fecha: 12 de Octubre



Resultados Esperados	Resultados Obtenidos
• Que el escaneo identificara vulnerabilidades presentes en el servidor, clasificadas por niveles de criticidad (críticas, altas, medias, bajas e informativas). Que se obtuviera un reporte detallado con métricas basadas en CVSS v3.0. • Que el proceso de autenticación al host fuera exitoso, permitiendo un análisis más profundo de configuraciones internas. • Que el tiempo de ejecución del escaneo se completara sin errores, mostrando evidencia clara de los hallazgos.	• El escaneo se ejecutó correctamente bajo la política **Basic Network Scan**, con una duración de 10 minutos. El host 192.168.2.36 respondió, pero la autenticación falló (**Auth: Fail**), limitando el alcance del análisis a pruebas externas. • Se identificaron **33 vulnerabilidades** en total: ○ **1 crítica** ○ **5 altas** ○ **27 medias** • El reporte se generó con base en **CVSS v3.0**, mostrando la distribución de vulnerabilidades en un gráfico y listado detallado. • El resultado confirma la existencia de riesgos significativos en el servidor, especialmente en configuraciones y protocolos, aunque el fallo de autenticación impidió un análisis más profundo de seguridad interna.

TABLA XIII. RESULTADOS DE ESCANEO CON LA HERRAMIENTA OPENVAS

Escaneo herramienta: OpenVAS		
Equipo: Laptop Corporativa	Auditor: Jesus Esteban Orbes Zambrano	Fecha: 16 de Noviembre



Resultados Esperados	Resultados Obtenidos
● Que el escaneo se ejecutara correctamente sobre el servidor 192.168.2.36. Que se generara un reporte con clasificación de vulnerabilidades por severidad (críticas, altas, medias, bajas e informativas). ● Que se identificaran hallazgos relevantes que permitieran evaluar el estado de seguridad del servidor. ● Que el sistema mostrara gráficas y métricas claras sobre los resultados obtenidos	● El escaneo se completó exitosamente, registrándose como **"Done"** en la consola de Greenbone. Se generó un reporte asociado al host 192.168.2.36, con fecha del 18 de noviembre de 2025. ● La severidad del reporte aparece como **N/A**, lo que indica que no se clasificaron vulnerabilidades en esta ejecución o que el análisis no arrojó hallazgos relevantes. ● Las gráficas de distribución de resultados muestran un único escaneo finalizado, sin vulnerabilidades críticas ni altas reportadas. ● El resultado confirma que el proceso técnico se ejecutó correctamente, aunque no se obtuvieron hallazgos de vulnerabilidades en esta corrida específica

9) Análisis de vulnerabilidades

A partir de los resultados obtenidos mediante las diferentes técnicas y herramientas aplicadas en la fase de escaneo se determina la matriz de riesgos.

Matrices de riesgos: que relacionan cada vulnerabilidad detectada con el activo afectado, el impacto potencial y las medidas de mitigación recomendadas.

Valoración de activos: En esta hoja (Valoración activos), se identifican y valoran los activos de la organización, para las dimensiones de seguridad de Disponibilidad (D), Integridad (I), Confidencialidad (C), Autenticidad (A) y Trazabilidad (T). Los activos se agrupan por categoría y por proceso de negocio. Cada valoración se colorea en función de su número (del 1 al 5).

Categoría	Activo	D	I	C	A	T
Software	Software - CMS para contenidos de sitio web (WordPress)	4	5	3	4	4
	Software - Ofimática para los usuarios	4	4	3	3	3
	Correo electrónico basado en GMail	5	5	5	5	4
	Software - Gestión de Recursos Humanos	5	5	5	5	5
Datos	Repositorio datos CMS (MariaDB)	4	5	4	4	4
	Repositorio de datos ofimáticos	4	4	4	3	3
	Base de datos Recursos Humanos	5	5	5	5	5
Servidores	Servidor Linux para CMS con Apache	4	5	4	4	4
	Servidor Windows Server para AD (Active Directory)	5	5	5	5	5
	Servidor Linux para BD de CMS MariaDB	4	5	4	4	4
	Servidor Windows Server para Archivos (datos ofimáticos)	4	4	4	3	3
	Servidor Windows Server para DHCP/DNS	5	5	4	5	4
Red, Internet	Electrónica de red (switches)	5	4	3	4	3
	Cortafuegos (reglas, VPN, DMZ)	5	5	5	5	5
	Router Internet	5	4	4	4	3

Fig. 2. Valoración de activos

Para las valoraciones de las dimensiones, es fundamental conocer qué significa cada dimensión y cómo evaluar los números del 1 al 5. En las siguientes tablas se explica el baremo a seguir en función de cada dimensión:

TABLA XIV. DISPONIBILIDAD: ¿QUÉ IMPORTANCIA TENDRÍA QUE EL ACTIVO NO ESTUVIERA DISPONIBLE?

1	Muy bajo (MB)	No aplica o no es relevante
2	Bajo (B)	Debe estar disponible al menos el 20% del tiempo
3	Medio (M)	Debe estar disponible al menos el 40% del tiempo
4	Alto (A)	Debe estar disponible al menos el 70% del tiempo
5	Muy alto (MA)	Debe estar disponible al menos el 99% del tiempo

TABLA XV. INTEGRIDAD: ¿QUÉ IMPORTANCIA TENDRÍA QUE LOS DATOS FUERAN MODIFICADOS FUERA DE CONTROL?

1	Muy bajo (MB)	No aplica o no es relevante
2	Bajo (B)	Poca relevancia
3	Medio (M)	Tiene que estar correcto y completo al menos 50%
4	Alto (A)	Tiene que estar correcto y completo al menos 95%
5	Muy alto (MA)	Tiene que estar correcto y completo al menos 99%

TABLA XVI. CONFIDENCIALIDAD: ¿QUÉ IMPORTANCIA TENDRÍA QUE EL DATO FUERA CONOCIDO POR PERSONAS NO AUTORIZADAS?

1	Muy bajo (MB)	No aplica o no es relevante
2	Bajo (B)	Daños muy bajos, el incidente no trascendería del área afectada
3	Medio (M)	Serían relevantes, el incidente implicaría otras áreas
4	Alto (A)	Serían relevantes, el incidente implicaría otras áreas y podría afectar a la reputación de la empresa
5	Muy alto (MA)	Los daños serían catastróficos y comprometerían la reputación y la imagen de la empresa

TABLA XVII. AUTENTICIDAD: ¿QUÉ IMPORTANCIA TENDRÍA QUE QUIEN ACCEDE AL SERVICIO NO SEA REALMENTE QUIEN SE CREE?

1	Muy bajo (MB)	No aplica o no es relevante
2	Bajo (B)	Daños muy bajos, el incidente no trascendiera del área afectada
3	Medio (M)	Serían relevantes, el incidente implicaría otras áreas
4	Alto (A)	Grave, podrían verse comprometidos otros dominios, como la confidencialidad y la integridad
5	Muy alto (MA)	Catastrófico, se verían comprometidos el resto de dominio

TABLA XVIII. TRAZABILIDAD: ¿QUÉ IMPORTANCIA TENDRÍA QUE NO QUEDARA CONSTANCIA DEL ACCESO A LOS DATOS?

1	Muy bajo (MB)	No aplica o no es relevante
2	Bajo (B)	Poca relevancia

3	Medio (M)	Serían relevantes, el incidente implicaría una mínima pérdida del rastro para futuros análisis forenses y auditorías
4	Alto (A)	Grave, el incidente implicaría una pérdida considerable del rastro para futuros análisis forenses y auditorías
5	Muy alto (MA)	Catastrófico, el incidente implicaría una pérdida total del rastro para futuros análisis forenses y auditorías

10) Valoración de las amenazas por activo en sus dimensiones de seguridad

Una vez identificados los activos y valorados e identificadas las amenazas por activo, procedimos a realizar la valoración de las amenazas en las dimensiones de Disponibilidad (D), Integridad (I), Confidencialidad (C), Autenticidad (A) y Trazabilidad (T).

Es muy importante resaltar que en esta fase se realizaron las valoraciones suponiendo que **no hay salvaguardas (controles)**, para calcular el mapa de riesgo potencial.

Para la valoración de las amenazas, se rellenó los siguientes datos por cada activo y cada amenaza:

Fre: frecuencia, indicaremos la posibilidad de ocurrencia de la amenaza. Los valores posibles son:

TABLA XIX. VALORES POSIBLES DE AMENAZAS

Siglas	Nombre	Frecuencia	Multiplica por 2 el impacto
MA	Muy frecuente	A diario	Sí
A	Frecuente	Una vez al mes	Sí
M	Normal	Una vez al año	No
B	Poco frecuente	Cada varios años	No
MB	Muy poco frecuente	Siglos	No

El resto de columnas serán las relativas a valorar el impacto (i) y el riesgo (R), teniendo en cuenta la definición de cada uno de ellos:

TABLA XX. RIESGOS E IMPACTOS

Riesgo	La estimación del **grado de exposición a que una amenaza se materialice** sobre uno o más activos causando daños o perjuicios a la Organización. Según la UNE-ISO Guía 73:2010, el riesgo es el efecto de la incertidumbre sobre la consecución de los objetivos
Impacto	La **medida del daño** sobre el activo derivado de la materialización de una amenaza

Por lo tanto, el resto de las columnas serán:

TABLA XXI. LISTADO DE IMPACTOS

ID	Impacto en disponibilidad
II	Impacto en integridad
IC	Impacto en confidencialidad
IA	Impacto en autenticidad
IT	Impacto en trazabilidad
RD	Riesgo en disponibilidad
RI	Riesgo en integridad
RC	Riesgo en confidencialidad
RA	Riesgo en autenticidad
RT	Riesgo en trazabilidad

Para el caso del impacto, se establecieron valores del 0 al 5. Para el caso del riesgo, se calculó en base a la siguiente fórmula:

Si la frecuencia es M o MA, el Riesgo será Impacto multiplicado por dos, si no, el Riesgo será igual al Impacto.

Activo	Amenaza	Fre	ID	II	IC	IA	IT	RD	RI	RC	RA	RT
Software - CMS para contenidos de sitio web (WordPress)	Abuso de privilegios de acceso	M	2	4	4	3	3	2	4	4	3	3
	Acceso no autorizado	M	3	4	5	4	3	3	4	5	4	3
	Alteración de secuencia	B	3	5	4	4	3	3	5	4	4	3
	Deficiencias en la organización	M	3	4	3	3	4	3	4	3	3	4
	Divulgación de información	M	2	3	5	3	3	2	3	5	3	3
	Errores de configuración	M	4	4	3	3	4	4	4	3	3	4
	Errores de los usuarios	A	3	4	3	3	4	6	8	6	6	8
	Errores de mantenimiento / actualización de programas	A	4	5	3	3	4	8	10	6	6	8
	Errores del administrador	M	4	5	4	4	4	4	5	4	4	4
	Manipulación de los registros de actividad (log)	B	3	4	3	4	5	3	4	3	4	5
	Manipulación de programas	B	4	5	4	4	4	4	5	4	4	4
	Reencaminamiento de mensajes	MB	3	4	5	4	3	3	4	5	4	3
	Suplantación de la identidad del usuario	M	3	4	5	5	4	3	4	5	5	4
	Uso no previsto	M	3	4	3	3	4	3	4	3	3	4
	Vulnerabilidades de los programas	A	4	5	5	4	4	8	10	10	8	8
	Valoración final materialización de amenazas		4	5	5	5	5	8	10	10	8	8

Fig. 3. Amenaza para software CMS para contenidos de sitio web

Software - Ofimática para los usuarios	Abuso de privilegios de acceso	A	3	4	5	5	4	6	8	10	10	8
	Acceso no autorizado	A	4	4	5	5	4	8	8	10	10	8
	Deficiencias en la organización	M	3	4	4	4	4	3	4	4	4	4
	Divulgación de información	A	3	4	5	4	4	6	8	10	8	8
	Errores de configuración	A	4	4	4	4	4	8	8	8	8	8
	Errores de los usuarios	MA	3	4	4	3	4	6	8	8	6	8
	Errores de mantenimiento / actualización de programas	M	4	4	4	3	4	4	4	4	3	4
	Errores del administrador	M	4	4	4	4	4	4	4	4	4	4
	Manipulación de los registros de actividad (log)	B	3	4	4	4	5	3	4	4	4	5
	Manipulación de programas	B	4	5	5	4	4	4	5	5	4	4
	Suplantación de la identidad del usuario	A	3	4	5	5	4	6	8	10	10	8
	Uso no previsto	A	3	4	4	4	4	6	8	8	8	8
	Vulnerabilidades de los programas	M	4	5	5	4	4	4	5	5	4	4
	Valoración final materialización de amenazas		4	5	5	5	5	8	8	10	10	8

Fig. 4. Amenaza para software ofimática para los usuarios

Software - Correo electrónico basado en Gmail	Abuso de privilegios de acceso	A	3	4	5	5	4	6	8	10	10	8
	Acceso no autorizado	A	4	4	5	5	4	8	8	10	10	8
	Alteración de secuencia	B	4	4	4	4	4	4	4	4	4	4
	Deficiencias en la organización	M	3	4	4	4	4	3	4	4	4	4
	Divulgación de información	A	3	4	5	4	4	6	8	10	8	8
	Errores de configuración	A	4	4	4	4	4	8	8	8	8	8
	Errores de los usuarios	MA	3	4	5	3	4	6	8	10	6	8
	Errores de mantenimiento / actualización de programas	M	4	4	4	3	4	4	4	4	3	4
	Errores del administrador	M	4	4	4	4	4	4	4	4	4	4
	Ingeniería social	MA	3	4	5	5	4	6	8	10	10	8
	Manipulación de los registros de actividad (log)	B	3	4	4	4	5	3	4	4	4	5
	Manipulación de programas	B	4	5	5	4	4	4	5	5	4	4
	Phishing	MA	3	4	5	5	4	6	8	10	10	8
	Reencaminamiento de mensajes	A	3	4	5	4	4	6	8	10	8	8
	Repudio	M	3	3	4	4	5	3	3	4	4	5
	Suplantación de la identidad del usuario	A	3	4	5	5	4	6	8	10	10	8
	Uso no previsto	M	3	4	4	4	3	3	4	4	4	3
	Vulnerabilidades de los programas	A	4	5	5	4	4	8	10	10	8	8
	Valoración final materialización de amenazas		4	5	5	5	5	8	10	10	10	8

Fig. 5. Amenaza para software correo electrónico basado en Gmail

Software - Gestión de Recursos Humanos	Abuso de privilegios de acceso	M	4	5	5	5	4	4	5	5	5	4
	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Deficiencias en la organización	M	3	4	4	4	5	3	4	4	4	5
	Divulgación de información	A	3	4	5	4	4	6	8	10	8	8
	Errores de configuración	M	4	4	4	4	4	4	4	4	4	4
	Errores de los usuarios	MA	4	4	4	3	3	8	8	8	6	6
	Errores de mantenimiento / actualización de programas	M	4	4	3	3	4	4	4	3	3	4
	Errores del administrador	M	4	4	4	4	4	4	4	4	4	4
	Manipulación de los registros de actividad (log)	B	3	4	4	4	5	3	4	4	4	5
	Manipulación de programas	B	5	4	5	5	4	5	4	5	5	4
	Reencaminamiento de mensajes	A	3	4	5	4	4	6	8	10	8	8
	Suplantación de la identidad del usuario	A	4	5	5	5	4	8	10	10	10	8
	Uso no previsto	M	3	4	4	4	3	3	4	4	4	3
	Vulnerabilidades de los programas	A	4	5	5	4	4	8	10	10	8	8
	Valoración final materialización de amenazas		5	5	5	5	5	8	10	10	10	8

Fig. 6. Amenaza para software gestión de recursos humanos

Repositorio datos CMS (MariaDB)	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Alteración accidental de la información	MA	4	5	4	3	3	8	10	8	6	6
	Destrucción de información	M	5	5	4	4	4	5	5	4	4	4
	Fugas de información	A	3	4	5	4	4	6	8	10	8	8
	Modificación deliberada de la información	B	4	5	5	5	4	4	5	5	5	4
	Ransomware	M	5	5	5	4	4	5	5	5	4	4
	Valoración final materialización de amenazas		5	5	5	5	4	8	10	10	10	8

Fig. 7. Amenaza para repositorio datos CMS (MariaDB)

Repositorio de datos ofimáticos	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Alteración accidental de la información	MA	3	5	4	3	3	6	10	8	6	6
	Destrucción de información	M	5	5	4	4	4	5	5	4	4	4
	Fugas de información	A	3	4	5	4	4	6	8	10	8	8
	Modificación deliberada de la información	B	4	5	5	5	4	4	5	5	5	4
	Ransomware	M	5	5	5	4	4	5	5	5	4	4
	Valoración final materialización de amenazas		5	5	5	5	4	8	10	10	10	8

Fig. 8. Amenaza para repositorio de datos ofimáticos

Base de datos Recursos Humanos	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Alteración accidental de la información	MA	3	5	4	3	3	6	10	8	6	6
	Destrucción de información	M	5	5	4	4	4	5	5	4	4	4
	Fugas de información	A	3	4	5	4	4	6	8	10	8	8
	Modificación deliberada de la información	B	4	5	5	5	4	4	5	5	5	4
	Ransomware	M	5	5	5	4	4	5	5	5	4	4
	Valoración final materialización de amenazas		5	5	5	5	4	8	10	10	10	8

Fig. 9. Amenaza para base de datos recursos humanos

Servidor Linux para CMS con Apache	Abuso de privilegios de acceso	M	4	5	5	5	4	4	5	5	5	4
	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Ataque destructivo	M	5	5	4	4	4	5	5	4	4	4
	Avería de origen físico o lógico	M	5	5	3	3	4	5	5	3	3	4
	Caída del sistema por agotamiento de recursos	A	5	4	3	3	4	10	8	6	6	8
	Errores de mantenimiento / actualización de equipos	A	4	4	3	3	4	8	8	6	6	8
	Manipulación de la configuración	A	4	5	4	5	4	8	10	8	10	8
	Manipulación de los equipos	B	4	5	5	4	4	4	5	5	4	4
	Vulnerabilidades del Sistema Operativo	A	4	5	5	4	4	8	10	10	8	8
	Valoración final materialización de amenazas		5	5	5	5	4	10	10	10	10	8

Fig. 10. Amenaza para servidor Linux para CMS con apache

Servidor Windows Server para AD (Active Directory)	Abuso de privilegios de acceso	M	4	5	5	5	4	4	5	5	5	4
	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Ataque destructivo	M	5	5	4	4	4	5	5	4	4	4
	Avería de origen físico o lógico	M	5	5	3	3	4	5	5	3	3	4
	Caída del sistema por agotamiento de recursos	A	5	4	3	3	4	10	8	6	6	8
	Errores de mantenimiento / actualización de equipos	A	4	4	3	3	4	8	8	6	6	8
	Manipulación de la configuración	A	4	5	4	4	4	8	10	8	8	8
	Manipulación de los equipos	B	4	5	5	4	4	4	5	5	4	4
	Vulnerabilidades del Sistema Operativo	A	4	5	5	4	4	8	10	10	8	8

Fig. 11. Amenaza para servidor Windows Server para AD

Servidor Linux para BD de CMS MariaDB	Abuso de privilegios de acceso	M	4	5	5	5	4	4	5	5	5	4
	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Ataque destructivo	M	5	5	4	4	4	5	5	4	4	4
	Avería de origen físico o lógico	M	5	5	3	3	4	5	5	3	3	4
	Caída del sistema por agotamiento de recursos	A	5	4	3	3	4	10	8	6	6	8
	Errores de mantenimiento / actualización de equipos	A	4	4	3	3	4	8	8	6	6	8
	Manipulación de la configuración	A	4	5	4	5	4	8	10	8	10	8
	Manipulación de los equipos	B	4	5	5	4	4	4	5	5	4	4
	Vulnerabilidades del Sistema Operativo	A	4	5	5	4	4	8	10	10	8	8
	Valoración final materialización de amenazas		5	5	5	3	3	10	10	10	10	8

Fig. 12. Amenaza para servidor Linux para BD de CMS MariaDB

Servidor Windows Server para Archivos (datos ofimáticos)	Abuso de privilegios de acceso	M	4	5	5	5	4	4	5	5	5	4
	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Ataque destructivo	M	5	5	4	4	4	5	5	4	4	4
	Avería de origen físico o lógico	M	5	5	3	3	4	5	5	3	3	4
	Caída del sistema por agotamiento de recursos	A	5	4	3	3	4	10	8	6	6	8
	Errores de mantenimiento / actualización de equipos	A	4	4	3	3	4	8	8	6	6	8
	Manipulación de la configuración	A	4	5	4	5	4	8	10	8	10	8
	Manipulación de los equipos	B	4	5	5	4	4	4	5	5	4	4
	Vulnerabilidades del Sistema Operativo	A	4	5	5	4	4	8	10	10	8	8
	Valoración final materialización de amenazas		5	5	5	5	4	10	10	10	10	8

Fig. 13. Amenaza para servidor Windows server para archivos (datos ofimáticos)

Servidor Windows Server para DHCP/DNS	Abuso de privilegios de acceso	M	4	5	5	5	4	4	5	5	5	4
	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Ataque destructivo	M	5	5	4	4	4	5	5	4	4	4
	Avería de origen físico o lógico	M	5	5	3	3	4	5	5	3	3	4
	Caída del sistema por agotamiento de recursos	A	5	4	3	3	4	10	8	6	6	8
	Errores de mantenimiento / actualización de equipos	A	4	4	3	3	4	8	8	6	6	8
	Manipulación de la configuración	A	4	5	4	5	4	8	10	8	10	8
	Manipulación de los equipos	B	4	5	5	4	4	4	5	5	4	4
	Vulnerabilidades del Sistema Operativo	A	4	5	5	4	4	8	10	10	8	8
	Valoración final materialización de amenazas		5	5	5	5	4	10	10	10	10	8

Fig. 14. Amenaza para servidor Windows server para DHCP/DNS

Electrónica de red (switches)	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Alteración de secuencia	A	4	5	4	5	4	8	10	8	10	8
	Análisis de tráfico	A	3	4	5	5	4	6	8	10	10	8
	Caída del sistema por agotamiento de recursos	A	5	4	3	3	4	10	8	6	6	8
	Denegación de servicio	A	5	4	3	4	4	10	8	6	8	8
	Errores del administrador	A	4	4	3	3	4	8	8	6	6	8
	Fallo de servicios de comunicaciones	M	5	4	3	3	4	5	4	3	3	4
	Interceptación de información (escucha)	A	3	4	5	5	4	6	8	10	10	8
	Reencaminamiento de mensajes	M	4	5	5	5	4	4	5	5	5	4
	Robo	B	5	4	5	4	4	5	4	5	4	4
	Vulnerabilidades del firmware	M	4	5	5	5	4	4	5	5	5	4
	Valoración final materialización de amenazas		5	5	5	5	4	10	10	10	10	8

Fig. 15. Amenaza electrónica de red (switches)

Cortafuegos (reglas, VPN, DMZ)	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Alteración de secuencia	M	4	5	4	5	4	4	5	4	5	4
	Análisis de tráfico	A	3	4	5	5	4	6	8	10	10	8
	Caída del sistema por agotamiento de recursos	A	5	4	3	3	4	10	8	6	6	8
	Denegación de servicio	A	5	4	3	4	4	10	8	6	8	8
	Errores del administrador	A	4	4	3	3	4	8	8	6	6	8
	Fallo de servicios de comunicaciones	M	5	4	3	3	4	5	4	3	3	4
	Interceptación de información (escucha)	A	3	4	5	5	4	6	8	10	10	8
	Robo	B	5	4	5	4	4	5	4	5	4	4
	Vulnerabilidades del firmware	M	4	5	5	5	4	4	5	5	5	4
	Valoración final materialización de amenazas		5	5	5	5	4	10	10	10	10	8

Fig. 16. Amenaza para contrafuegos

Router Internet	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Alteración de secuencia	M	4	5	4	5	4	4	5	4	5	4
	Análisis de tráfico	A	3	4	5	5	2	6	8	10	10	4
	Caída del sistema por agotamiento de recursos	A	5	4	3	3	4	10	8	6	6	8
	Denegación de servicio	A	5	4	3	4	4	10	8	6	8	8
	Errores del administrador	M	4	4	3	3	4	4	4	3	3	4
	Fallo de servicios de comunicaciones	M	5	4	3	3	4	5	4	3	3	4
	Interceptación de información (escucha)	A	3	4	5	5	4	6	8	10	10	8
	Reencaminamiento de mensajes	MB	4	5	5	5	4	4	5	5	5	4
	Robo	B	5	4	5	4	4	5	4	5	4	4
	Vulnerabilidades del firmware	M	4	5	5	5	4	4	5	5	5	4
	Valoración final materialización de amenazas		5	5	5	5	4	10	10	10	10	8

Fig. 17. Amenaza router internet

Por cada activo, se calculó la **valoración final de materialización de amenazas**, con la fórmula:

Cada columna (ID, II, IC, IA, IT, RD, RI, RC, RA, RT) será el valor máximo de todos ellos. Se diseñaron diferentes formatos y matrices que permitieron registrar de manera ordenada los hallazgos:

Reportes comparativos: como el análisis Nmap vs Masscan, que permitió evaluar la precisión y velocidad de cada herramienta y establecer un procedimiento operativo sugerido y el análisis comparativo entre Nessus vs OpenVAS, el cual permitió evaluar la efectividad en la detección de vulnerabilidades, la facilidad de uso y el rendimiento de cada herramienta, con el fin de identificar sus ventajas y limitaciones, y así proponer un procedimiento operativo recomendado para la gestión de vulnerabilidades.

11) Comparativo entre Nmap y Masscan

Con el fin de evaluar las capacidades de las herramientas de escaneo de puertos, se realizó un análisis comparativo entre Nmap y Masscan, considerando aspectos como velocidad, nivel de detalle, precisión y uso típico en auditorías de seguridad.

TABLA XXII. COMPARATIVO ENTRE NMAP Y MASSCAN

Aspecto	**Nmap**	**Masscan**
Velocidad	Realiza escaneos más lentos que permiten mayor profundidad.	Optimizado para barridos masivos y muy rápido.
Nivel de detalle	Entrega identificación de servicios, versiones y opciones avanzadas con scripts.	Reporta puertos abiertos rápidamente; no identifica versiones por defecto.
Precisión	Menor tasa de falsos positivos gracias a comprobaciones adicionales.	Puede producir falsos positivos; requiere verificación posterior.
Detección de hosts	Soporta múltiples métodos (ICMP, ARP, TCP) y aporta información fiable.	Detecta hosts con rapidez; algunas entradas requieren interpretación (ej.: 0/icmp).
Uso típico	Análisis en profundidad, auditorías y verificación de servicios.	Inventario rápido de puertos/hosts a gran escala.
Recomendación práctica	Usarlo para validar y profundizar en resultados preliminares.	Emplearlo como primer paso para identificar áreas de interés.

El análisis evidencia que Nmap resulta más adecuado para estudios en profundidad y verificación detallada de servicios, mientras que Masscan destaca por su rapidez en inventarios masivos de hosts y puertos. En la práctica, ambas herramientas se complementan: Masscan puede emplearse como primer paso para identificar áreas de interés y Nmap para profundizar en los hallazgos.

12) Comparativo entre Nessus y OpenVAS

Con el objetivo de evaluar la efectividad de las herramientas de análisis de vulnerabilidades, se realizó un comparativo entre Nessus y OpenVAS, aplicando ambos escaneos sobre el mismo host (192.168.2.36). El análisis consideró criterios como estado del escaneo, duración, autenticación, nivel de detalle y cantidad de vulnerabilidades detectadas.

TABLA XXIII. COMPARATIVO ENTRE NESSUS Y OPENVAS

Criterio	Nessus	OpenVAS
Host Analizado	El escaneo se ejecutó sobre el host 192.168.2.36, confirmando disponibilidad y recopilando información detallada de servicios, puertos y configuraciones.	El mismo host 192.168.2.36 fue analizado, permitiendo comparar la calidad de detección entre ambas herramientas dentro del mismo entorno.
Estado del Escaneo	Completed: todas las fases del análisis se realizaron con éxito, incluyendo detección de puertos, evaluación y reporte.	Done: indica que el proceso terminó, aunque sin detalles mostrados sobre el análisis realizado.

Criterio	Nessus	OpenVAS
Duración del Escaneo	Aproximadamente 10 minutos debido a la profundidad y cantidad de plugins usados por Nessus.	No visible, aunque OpenVAS suele tardar más por la ejecución más lenta de scripts.
Política de Escaneo	Basic Network Scan: diseñada para identificar una amplia gama de vulnerabilidades y servicios expuestos.	No visible, aunque normalmente usa perfiles estándar como Full and Fast o Host Discovery.
Autenticación	Fail: no fue posible autenticarse, limitando la detección profunda de vulnerabilidades internas.	No visible, posiblemente se ejecutó un escaneo no autenticado.
Total de Vulnerabilidades	33 vulnerabilidades encontradas distribuidas en varios niveles de severidad.	No visible, aunque se observan algunos resultados parciales.
Críticas	1 vulnerabilidad crítica relacionada con configuraciones de cifrado o servicios expuestos.	No visible en la vista disponible.
Altas	1 vulnerabilidad alta encontrada.	1 vulnerabilidad alta detectada según el gráfico.
Medias	5 vulnerabilidades medias asociadas a configuraciones inseguras o software desactualizado.	No visibles en el reporte mostrado.
Informativas	Más de 20 hallazgos informativos útiles para comprender la superficie de ataque.	No visibles en la vista actual.
Nivel de detalle	Muy alto: incluye descripciones técnicas, CVE, recomendaciones y evidencias.	Bajo en la vista mostrada, aunque OpenVAS puede generar reportes completos.
Principales Vulnerabilidades	SSL/TLS débiles, certificados obsoletos, suites criptográficas inseguras, información HTTP, detección de servicios.	No visibles en la vista disponible.
Reportes	Exportables en PDF, HTML y otros formatos.	Disponibles, aunque no se muestra su contenido.

El análisis evidencia que Nessus ofrece mayor profundidad y detalle en la detección de vulnerabilidades, aunque depende de la autenticación para un alcance completo. OpenVAS, por su parte, presenta un rendimiento más lento y reportes menos detallados en la vista mostrada, pero sigue siendo una alternativa válida en entornos abiertos y con políticas de escaneo estándar. En conjunto, ambos resultados permiten identificar fortalezas y limitaciones, facilitando la elección de la herramienta según el contexto operativo.

A partir de los análisis realizados, se pudo observar que cada herramienta tiene ventajas dependiendo de su uso, ya sea en velocidad o en nivel de detalle. Por esta razón, no existe una

única herramienta ideal, sino que lo más recomendable es combinarlas según la necesidad del análisis para obtener mejores resultados en la detección de vulnerabilidades.

TABLA XXIV. INSTRUMENTOS DE DOCUMENTACIÓN

Instrumento	Descripción	Resultado
Bitácora técnica	registro cronológico de acciones y resultados	Escaneo con Nessus el 30 de octubre de 2025
Matriz de riesgos	Relación entre vulnerabilidad, activo y medida	SSL no confiable —> Servidor 192.168.0.127 —> Actualizar certificado
Reporte Comparativo	Evaluación de herramientas	Nmap más preciso, Masscan más rápido

B. OBJETIVO 2. DISEÑAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) CONFORME A LA NORMA ISO/IEC 27001

Continuando con la metodología OSSTMM se aplican las fases validación técnica y documentación las cuales alineadas a la norma ISO/IEC 27001 permiten diseñar y presentar una propuesta del sistema de gestión de seguridad de la información (SGSI) para iFactory.

1) Tratamiento de riesgos

Con base en los resultados obtenidos durante el análisis de vulnerabilidades (Nmap, Nessus, OpenVAS), se definieron acciones de tratamiento orientadas a mitigar los riesgos críticos identificados en la infraestructura de la empresa iFactory.

TABLA XXV. TABLA DE TRATAMIENTO DE RIESGOS

Activo	Vulnerabilidad	Nivel de riesgo	Control propuesto	Tipo de control	Prioridad
Servidor	SSL/TLS desactualizado	Alto	Actualización de protocolos seguros (TLS 1.2/1.3)	Técnico	Alta
Servidor	Ruby REXML vulnerable	Alto	Actualización de librerías	Técnico	Alta
Servidor	Ruby RACK vulnerable	Alto	Parcheo del sistema	Técnico	Alta
Red	Puertos abiertos (22, 808)	Medio	Cierre de puertos innecesarios	Técnico	Media

Activo	Vulnerabilidad	Nivel de riesgo	Control propuesto	Tipo de control	Prioridad
Red	Servicios expuestos (RDP, WinRM)	Alto	Restricción de acceso por IP	Técnico	Alta
Firewall	Configuración permisiva	Alto	Endurecimiento de reglas	Técnico	Alta
Usuarios	Acceso no controlado	Alto	Implementación de políticas de acceso	Organizativo	Alta

2) Declaración de Aplicabilidad (SoA)

La Declaración de Aplicabilidad define los controles seleccionados del **Anexo A de la norma ISO/IEC 27001**, indicando su aplicabilidad dentro del SGSI y su relación con los riesgos identificados.

TABLA XXVI. CONTROLES SELECCIONADOS Y JUSTIFICADOS

Control Norma ISO/IEC 27001	Nombre del control	Aplicabilidad	Justificación
A.5.1	Políticas de seguridad de la información	Sí	Necesario para establecer lineamientos de seguridad
A.5.15	Control de acceso	Sí	Mitiga accesos no autorizados detectados
A.8.8	Gestión de vulnerabilidades técnicas	Sí	Relacionado con vulnerabilidades detectadas
A.8.9	Configuración segura	Sí	Aplica a servicios y puertos expuestos
A.8.23	Seguridad en servicios de red	Sí	Mitiga exposición de servicios
A.8.24	Uso de criptografía	Sí	Relacionado con fallos SSL/TLS
A.5.36	Cumplimiento de políticas	Sí	Asegura control organizacional
A.8.16	Monitoreo de actividades	Sí	Permite detectar incidentes
A.5.30	Preparación para incidentes	Sí	Mejora respuesta ante ataques

3) Justificación de los controles

Los controles seleccionados fueron definidos con base en:

- Los resultados reales del pentesting
- Las vulnerabilidades críticas identificadas
- La necesidad de proteger activos clave
- Las buenas prácticas de la norma ISO 27001

Esto garantiza que el SGSI esté alineado con un enfoque basado en riesgos y evidencias técnicas. Para más información puede consultar el anexo a donde se presenta con mayor detalle la formulación del SGSI.

C. OBJETIVO 3. EVALUAR LA EFECTIVIDAD DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Finalmente, el SGSI propuesto para iFactory se evaluó mediante una comparación objetiva del estado de seguridad informática antes y después de su formulación, conforme a los requisitos de la norma ISO 27001.

1) Comparación de resultados

TABLA XXVII. COMPARACION DE RESULTADOS

Métrica	Antes	Después	Resultados
Vulnerabilidades totales (externo)	23	3	Reducción
Vulnerabilidades críticas	3	1	Reducción
Vulnerabilidades internas	20	13	Reducción
Puertos abiertos	Múltiples	Reducidos	Reducción

2) Formulación de controles

Se reconocen controles técnicos y organizativos formulados. Entre los controles técnicos está la restricción de servicios expuestos.

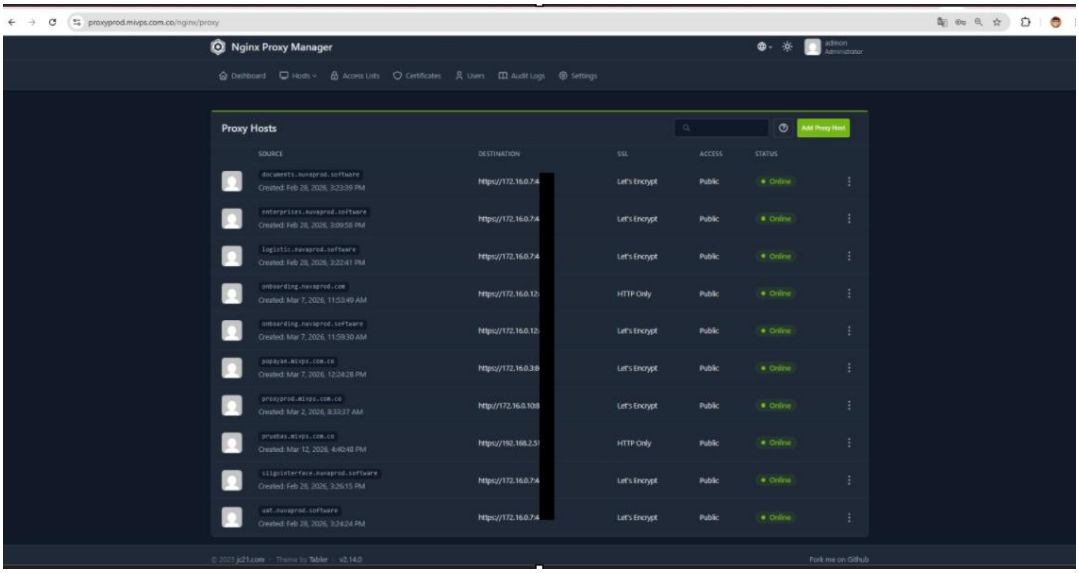


Fig. 18. Administración centralizada de servicios mediante Nginx Proxy Manager

En el panel de *Proxy Hosts* se observaron distintos subdominios corporativos que redirigían tráfico hacia servidores internos, lo que reflejaba la aplicación de controles técnicos de seguridad orientados a la gestión de accesos y la protección de la infraestructura. Entre los aspectos más relevantes se destacó el uso de certificados SSL de *Let's Encrypt*, que aseguraban la confidencialidad de las comunicaciones; la definición clara de orígenes y destinos, que permitía segmentar y controlar el flujo de información; y la supervisión del estado de los servicios, todos en condición *Online*, lo que garantizaba disponibilidad.

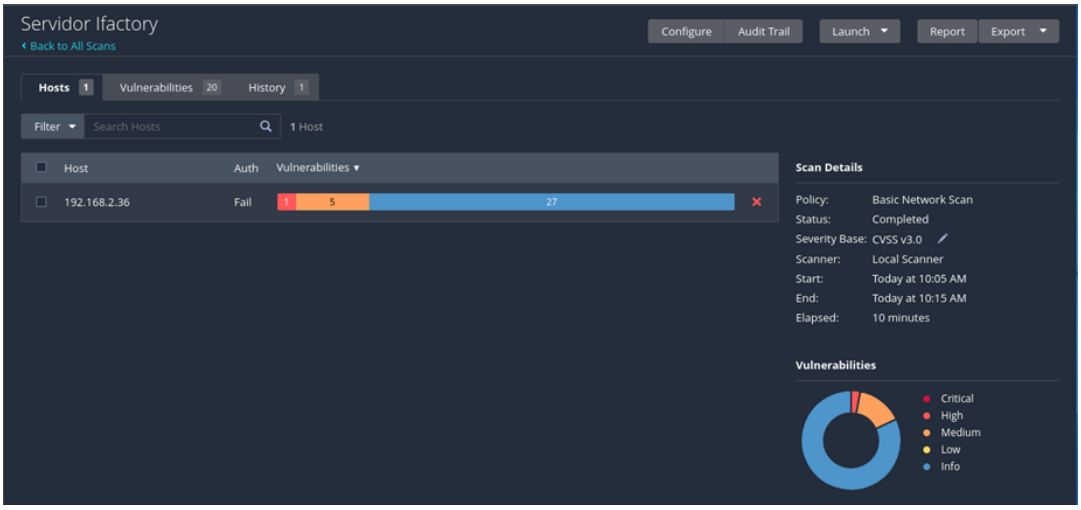


Fig. 19. Registro de parámetros técnicos de escaneo de servidor

Se registraron parámetros técnicos del escaneo realizados bajo la política *Basic Network Scan*, incluyendo el estado de autenticación, el tiempo de ejecución y la clasificación de severidad conforme al estándar CVSS v3.0. La representación gráfica permitió visualizar el nivel de exposición del sistema y aportó información estructurada para la gestión de riesgos. Este tipo de evidencia constituyó un control técnico y organizativo dentro del SGSI, al documentar el estado de seguridad de la infraestructura y asegurar la trazabilidad de las acciones de mejora, en concordancia con los requisitos de la norma ISO/IEC 27001.

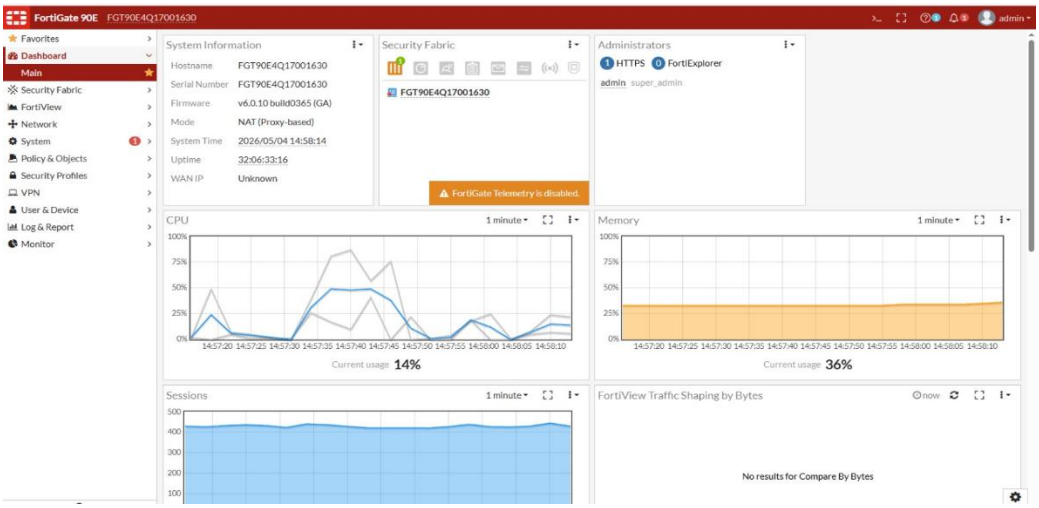


Fig. 20. Monitoreo en firewall corporativo FortiGate

El panel de control del dispositivo FortiGate 90E mostró información del sistema, conexiones administrativas, estado de la telemetría y métricas de rendimiento como uso de CPU, memoria y sesiones activas. La interfaz permitió observar en tiempo real la operación del equipo y evidenció la formulación de controles técnicos orientados a la supervisión continua de la infraestructura de red. Estos resultados aportaron trazabilidad y soporte documental a la gestión de seguridad, garantizando la disponibilidad y confiabilidad de los servicios corporativos.

Entre los controles organizativos está el acceso a usuarios.



User Name	Type	Two-factor Authentication	Ref.
EMOTION1	LOCAL		1
Frigovito2023	LOCAL		0
INVO	LOCAL		0
INVOHG	LOCAL		0
PROXMOX	LOCAL		1
SEBASTIAN	LOCAL		1
TEXCOLVPN	LOCAL		1
USERVPN	LOCAL		1
VPNUSER	LOCAL		1
camilo	LOCAL		1
felipe	LOCAL		1
guest	LOCAL		1
temporal	LOCAL		1

Fig. 21. Control de acceso a usuarios

El registro de cuentas de usuario presento la administración centralizada de perfiles locales, junto con la configuración de autenticación en dos pasos. La tabla permitió identificar los usuarios habilitados, el tipo de cuenta y las referencias asociadas, evidenciando la formulación de un control organizativo de acceso orientado a la protección de los sistemas corporativos. Estos resultados aportaron soporte documental a la gestión de seguridad, al garantizar la correcta asignación de privilegios y la aplicación de mecanismos de autenticación complementarios.

Se realizaron otros tipos de controles que por solicitud de IFactory no se registran en el documento, sin embargo, se adjunta el acta de conformidad de recibido de la propuesta del SGSI.

ACTA DE ENTREGA Y RECEPCIÓN

Plan de Sistema de Gestión de Seguridad de la Información (SGSI)
Conforme a la norma ISO/IEC 27001

Lugar y fecha: Pasto, Nariño – 24 de abril de 2026

ENTREGANTES

Nombre: Jeison Gabriel Botina Diaz — Nombre: Jesús Esteban Orbes Zambrano
Cédula de Ciudadanía: 1004489645 — Cédula de Ciudadanía: 1004190536
Estudiantes X semestre Programa de Ingeniería de Sistemas – **Universidad CESMAG**

RECEPTOR

Empresa: **IFACTORY**
Responsable: Ing. Camilo Gómez Arteaga
Cargo: Director de Infraestructura de TI
Cédula de Ciudadanía: 98389866

Documentos entregados: 1. Plan de SGSI conforme a ISO/IEC 27001

Fases del SGSI (ISO/IEC 27001)

Fase	Descripción
1. Definición del Alcance y Contexto Organizacional	Identificación de procesos, activos y límites del SGSI, considerando requisitos
	legales, regulatorios y contractuales.
2. Evaluación de Riesgos y Tratamiento	Análisis sistemático de amenazas y vulnerabilidades, con definición de controles para mitigar riesgos.
3. formulación de Controles y Políticas	Aplicación de medidas técnicas, organizativas y administrativas alineadas con el Anexo A de ISO/IEC 27001.
4. Monitoreo, Medición y Auditoría Interna	Seguimiento continuo del desempeño del SGSI mediante indicadores, revisiones y auditorías internas.

Fig. 22. Acta de entrega y recepción hoja 1

Declaración

Las partes dejan constancia de que los documentos fueron entregados y recibidos en perfectas condiciones físicas y digitales, cumpliendo íntegramente con los términos, alcances y actividades previamente convenidos.

El receptor manifiesta su aceptación plena, sin reservas ni objeciones, y se compromete a dar continuidad a las fases posteriores del proyecto conforme a lo estipulado.

Firmas

Entregantes: (Estudiantes - Universidad CESMAG):

Nombre: Jeison Gabriel Botina Diaz

Firma: 

Nombre: Jesús Esteban Orbes Zambrano

Firma: 

Por la Institución Receptora (**IFACTORY**):

Nombre: Camilo Gómez Arteaga

Cargo: Ing. en sistemas | director de infraestructura de TI

Firma: 

Fig. 23. Acta de entrega y recepción hoja 2

V. ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS

Inicialmente, la infraestructura tecnológica de la empresa iFactory presentaba debilidades de seguridad evidenciadas mediante el análisis de vulnerabilidades realizado en las fases de reconocimiento y pruebas de pentesting. Aunque algunos componentes de la red contaban con medidas básicas de ciberseguridad, estas no estaban respaldadas por una política organizacional formal. Se identificaron factores críticos asociados a configuraciones inadecuadas, servicios expuestos y protocolos obsoletos, lo que aumentaba el riesgo de accesos no autorizados e incidentes de seguridad.

En este tipo de proyectos es fundamental definir claramente el alcance, de modo que tanto la organización como los investigadores dispongan desde el inicio de reglas precisas sobre los recursos tecnológicos, hardware y software incluidos en el estudio, horarios de operación, dependencias intervenidas y acciones de escaneo y pentesting. Asimismo, deben establecerse controles de acceso y pautas para el uso de datos, garantizando la integridad, confidencialidad y disponibilidad de la información de la organización.

A partir del desarrollo de la presente investigación, se logró evidenciar que es viable formular un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 ajustado a las necesidades de la organización, mediante la articulación entre la metodología OSSTMM de pruebas de seguridad de código abierto que permite evaluar de manera objetiva, medible y reproducible la seguridad operativa de una organización y la norma ISO/IEC 27001, incluso sin requerir grandes recursos económicos, operativos o de personal. Gracias a esta integración se identificó que, en muchos casos, la no aplicación de controles de seguridad no se debe a limitaciones técnicas, sino a la ausencia de políticas claras y directrices organizacionales que orienten su implementación.

Entre las acciones, artefactos e información obtenida mediante la integración de la metodología OSSTMM y la norma ISO/IEC 27001 se pueden destacar:

- Definir alcance organizacional, activos críticos, partes interesadas y límites del SGSI. Las cuales se alienaron con los activos identificados en la aplicación de la metodología OSSTMM.

- Consolidar el inventario técnico obtenido en las fases de footprinting, identificación, inventario y escaneo, para con esta información, clasificar los activos según criticidad (Confidencialidad, Integridad, Disponibilidad).

- Utilizar las vulnerabilidades detectadas para construir la matriz de riesgos (Impacto x Probabilidad), con lo cual se pudo determinar nivel de riesgo aceptable.

- Definir controles técnicos y organizativos para mitigar vulnerabilidades críticas. Que sirvieron como insumo para la documentación y posterior formulación del SGSI.

- Aplicar procedimientos de hardening, segmentación de red, gestión de accesos, actualizaciones y configuraciones seguras, como salvaguardas a la situación detectada.

- Comparar estado de la red de datos después de aplicar los controles formulados.

La situación evidenció un entorno tecnológico funcional, pero insuficientemente protegido frente a amenazas internas y externas, lo que comprometía la confidencialidad, integridad y disponibilidad de la información. Esto hizo necesaria la formulación de un SGSI aprobado por las directivas, para integrarlo como parte de las políticas de seguridad de la organización. La documentación del SGSI permitió definir lineamientos y buenas prácticas que, de ser adoptadas por la dependencia de Sistemas de iFactory, se proyecta que contribuirán a fortalecer la infraestructura tecnológica y a mejorar la gestión de riesgos.

Finalmente, los resultados obtenidos muestran que la formulación y documentación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001 constituye una base técnica y organizativa sólida para mejorar la protección de la información y orientar la reducción de vulnerabilidades en la red de datos. La documentación del SGSI evidencia que la aproximación metodológica basada en ISO 27001 resulta apropiada y replicable, y representa un insumo estratégico para reducir la exposición a riesgos en la infraestructura de red una vez se inicie la fase de implementación y verificación.

CONCLUSIONES

El análisis de vulnerabilidades mediante pruebas de pentesting permitió identificar con claridad las principales debilidades de la infraestructura tecnológica de iFactory, especialmente en configuraciones, servicios expuestos y uso de protocolos. En este tipo de proyectos la documentación eficiente de los hallazgos es fundamental y sirve como base para entender el nivel de riesgo y plantear las acciones de mejora a realizar.

La metodología OSSTMM se consolidó como una herramienta eficaz para el análisis de escenarios donde no se cuenta con todos los recursos para la gestión y diseño del Sistema de Gestión de Seguridad de la Información (SGSI), basado en la norma ISO/IEC 27001, permitiendo estructurar un modelo acorde a las necesidades de la empresa, integrando políticas, controles y procedimientos enfocados en la gestión de riesgos.

La formulación del SGSI permitió establecer un estado inicial sobre la seguridad de la organización. Sin embargo, al no haberse llevado a cabo una implementación completa, debido al alcance del proyecto y políticas de la empresa, los resultados corresponden a una proyección teórica que muestra el potencial del sistema y los beneficios que representan.

Este tipo de investigación en organizaciones operativas permitió recopilar de manera controlada información pertinente para validar metodologías, técnicas, controles y herramientas de ciberseguridad, generando insumos valiosos para la toma de decisiones y, en el caso de iFactory, para la futura implementación de un SGSI.

RECOMENDACIONES

Se recomienda que en futuros trabajos se gestionen y obtengan los permisos necesarios por parte de la organización, con el fin de ampliar el alcance de las pruebas de seguridad y permitir una evaluación más profunda de la infraestructura. Esto facilitaría no solo la identificación de vulnerabilidades, sino también su validación práctica en escenarios más cercanos a la realidad operativa.

Con la aparición de la IA y herramientas enfocadas a su utilización en el área de Ciberseguridad, se recomienda la revisión de este tipo de recursos para el análisis de vulnerabilidades y pruebas de pentesting, teniendo presente todas las salvaguardas necesarias para que la información siempre conserve la integridad, confidencialidad y disponibilidad en la organización.

Se recomienda complementar este tipo de estudios con una evaluación posterior a la formulación del SGSI, que permita medir de forma objetiva su efectividad. Esto contribuiría a obtener resultados más completos, evidenciar mejoras reales en la seguridad y fortalecer el proceso de toma de decisiones basado en datos concretos.

VI. REFERENCIAS BIBLIOGRÁFICAS

[1] J. Fossi, «La norma ISO 22301: Cómo asegurar la continuidad del negocio,", 2022», ISOTools Excellence. [En línea]. Disponible en: https://mx.isotools.us/la-iso-22301-puede-asegurar-la-continuidad-del-negocio-caso-se-produzca-desastre/

[2] J. López, V. Proaño, y W. Zabala, «Políticas de Seguridad de la Información para la Universidad Politécnica Estatal del Carchi», *SATHIRI*, vol. 17, n.º 1, pp. 313-326, 2022, doi: 10.32645/13906925.1117.

[3] R. Martelo, J. Madera, y A. Betín, «Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI)», *Información tecnológica*, vol. 26, n.º 2, pp. 129-134, 2015, doi: 10.4067/S0718-07642015000200015.

[4] E. Rosales, R. Martelo, y D. Franco, «Diseño de un sistema de gestión de seguridad de la información para el proceso administrativo de la infraestructura tecnológica de instituciones académicas basado en Magerit», *Aglala*, vol. 11, n.º 1, pp. 227-245, 2020, [En línea]. Disponible en: https://revistas.uninunez.edu.co/index.php/aglala/article/view/1579

[5] C. Berríos y M. Rocha, «Propuesta de un modelo de sistema de gestión de la seguridad de la información en una pyme basado en la norma ISO/IEC 27001», Tesis de pregrado, Universidad Peruana de Ciencias Aplicadas (UPC), 2015. [En línea]. Disponible en: https://repositorioacademico.upc.edu.pe/handle/10757/581891

[6] P. Sánchez, J. García, A. Triana, y L. Pérez, «Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia», *Información tecnológica*, vol. 35, n.º 5, pp. 121-128, 2021, [En línea]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8088673

[7] E. Robayo y H. Jaimes, «Guide of principles and good practices for software security testing in web applications for a private sector company», en *2021 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI)*, IEEE, 2021, pp. 1-7. doi: 10.1109/CONIITI53815.2021.9619664.

[8] J. Llanos, F. López, y M. Mejía, «Implementación de un sistema de seguridad de la información en empresa del sector salud», *SUMMA*, vol. 5, n.º 2, pp. 1-14, 2023, doi: 10.47666/summa.5.2.7.

[9] G. Disterer, «ISO/IEC 27000, 27001 and 27002 for Information Security Management», *Journal of Information Security*, vol. 4, n.º 2, pp. 92-100, 2013, doi: 10.4236/jis.2013.42011.

[10] M. Mirtsch, J. Kinne, y K. Blind, «Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis», *IEEE Trans. Eng. Manag.*, vol. 68, n.º 1, pp. 87-100, 2021, doi: 10.1109/TEM.2020.2977815.

[11] Y. Kamil, S. Lund, y S. Islam, «Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden», *Information Systems and e-Business Management*, vol. 21, n.º 3, pp. 699-722, 2023, doi: 10.1007/s10257-023-00646-y.

[12] M. Podrecca y M. Sartor, «Forecasting the diffusion of ISO/IEC 27001: a Grey model approach», *The TQM Journal*, vol. 35, n.º 9, pp. 123-151, 2023, doi: 10.1108/TQM-07-2022-0220.

[13] M. Podrecca, G. Culot, G. Nassimbeni, y M. Sartor, «Information security and value creation: The performance implications of ISO/IEC 27001», *Comput. Ind.*, vol. 142, p. 103744, 2022, doi: 10.1016/j.compind.2022.103744.

[14] K. Razikin y B. Soewito, «Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework», *Egyptian Informatics Journal*, vol. 23, n.º 3, pp. 383-404, 2022, doi: 10.1016/j.eij.2022.03.001.

[15] G. Culot, G. Nassimbeni, M. Podrecca, y M. Sartor, «The ISO/IEC 27001 information security management standard: literature review and theo ry-based research agenda», *The TQM Journal*, vol. 33, n.º 7, pp. 76-105, 2021, doi: 10.1108/TQM-09-2020-0202.

[16] M. Mirtsch, K. Blind, C. Koch, y G. Dudek, «Information security management in ICT and non-ICT sector companies: A preventive innovation perspective», *Comput. Secur.*, vol. 109, p. 102383, 2021, doi: 10.1016/j.cose.2021.102383.

[17] Y. Lizárraga, J. Panaqué, y A. Mendoza, «Impacto de la auditoría informática en las organizaciones: Una revisión bibliográfica», *Ingeniería investiga*, vol. 4, 2022, doi: 10.47796/ing.v4i0.638.

[18] M. Minaya, R. Minaya, M. Intriago, y J. Intriago, «Normas y estándares en auditoría: una revisión de su utilidad en la seguridad informática», *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, vol. 5, n.º 4, pp. 584-599, 2023, doi: 10.59169/pentaciencias.v5i4.700.

[19] G. Galecio, G. Luján, y C. Roldán, «Gestión de riesgos en entornos virtuales para la enseñanza universitaria del inglés: Una revisión sistemática», *Atenas*, n.º 63, 2025, [En línea]. Disponible en: https://atenas.umcc.cu/index.php/atenas/article/view/1211

[20] D. Carrera, S. Tibanquiza, P. Taboada, y L. Ocaña, «Impacto de la Industria 4.0 en los sistemas mecatrónicos: una revisión de normativas internacionales», *Ciencia Digital*, vol. 8, n.º 4, pp. 75-91, 2024, doi: 10.33262/cienciadigital.v8i4.3240.

[21] Fortinet, «¿Qué es una CVE? Vulnerabilidades y exposiciones comunes definidas». [En línea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/cve

[22] F. García de Zúñiga, «OWASP: ¿Qué es y cómo usar esta metodología?» [En línea]. Disponible en: https://www.arsys.es/blog/owasp

[23] Amazon Web Services, «¿Qué es la criptografía?» [En línea]. Disponible en: https://aws.amazon.com/es/what-is/cryptography/

[24] International Standard Organization [ISO], «ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls». [En línea]. Disponible en: https://www.iso.org/es/contents/data/standard/07/56/75652.html

[25] International Standard Organization [ISO], «ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems.

Requirement». [En línea]. Disponible en: https://www-iso-org.translate.goog/standard/27001?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

[26] International Standard Organization [ISO], «ISO/IEC 27005:2022 – Information Security, Cybersecurity and Privacy Protection — Guidance on Managing Information Security Risks». [En línea]. Disponible en: https://www.iso.org/es/contents/data/standard/08/05/80585.html

[27] ESG Innova Group, «¿Qué es la norma ISO 27032? Una guía completa sobre ciberseguridad en la sociedad digital». [En línea]. Disponible en: https://www.pmg-ssi.com/2023/08/que-es-la-norma-iso-27032-una-guia-completa-sobre-ciberseguridad-en-la-sociedad-digital/

[28] M. Jiménez, «MAGERIT: gestión de riesgos de Seguridad de la Información». [En línea]. Disponible en: https://www.piranirisk.com/es/blog/metodologia-magerit-gestion-riesgos-sistemas-de-informacion

[29] Bitsight, «CVSS (Common Vulnerability Scoring System)». [En línea]. Disponible en: https://www.bitsight.com/glossary/cvss-common-vulnerability-scoring-system

[30] Service Now, «¿Qué es el riesgo cibernético?» [En línea]. Disponible en: https://www.servicenow.com/latam/products/governance-risk-and-compliance/what-is-cyber-risk.html

[31] Pure Storage, «¿Qué es el MTTD?» [En línea]. Disponible en: https://www.purestorage.com/es/knowledge/what-is-mttd.html

[32] IBM, «¿Cuál es el plazo medio de reparación?» [En línea]. Disponible en: https://www.ibm.com/es-es/topics/mttr

[33] C. Hashemi, «What is the CIA triad (confidentiality, integrity and availability)?» [En línea]. Disponible en: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

[34] Amazon Web Services, «¿Qué es la WAN (Wide Area Network)?» [En línea]. Disponible en: https://aws.amazon.com/es/what-is/wan/

[35] GeoTrust, «¿Cómo funcionan los certificados TLS/SSL?» [En línea]. Disponible en: https://www.geotrust.com/es/how-does-tls-ssl-work

[36] Fortinet, «¿Qué es un firewall?» [En línea]. Disponible en: https://www.fortinet.com/lat/resources/cyberglossary/firewall

[37] Imagar, «Red LAN: ¿qué es y cómo protegerla?» [En línea]. Disponible en: https://www.imagar.com/blog-desarrollo-web/red-lan-que-es-y-como-protegerla/

[38] F. González, «¿Qué Es Un Paradigma? Análisis Teórico, Conceptual Y Psicolingüístico Del Término», *Investigación y Postgrado*, vol. 20, n.º 1, pp. 13-54, 2005, [En línea]. Disponible en: https://ve.scielo.org/scielo.php?pid=S1316-00872005000100002&script=sci_abstract

[39] L. Mata, «El enfoque de investigación: la naturaleza del estudio». [En línea]. Disponible en: https://investigaliacr.com/investigacion/el-enfoque-de-investigacion-la-naturaleza-del-estudio/

[40] P. Sánchez, «Métodos de investigación: Qué son y cómo elegirlos». [En línea]. Disponible en: https://www.questionpro.com/blog/es/metodos-de-investigacion/

[41] A. Muguira, «Tipos de investigación y sus características». [En línea]. Disponible en: https://www.questionpro.com/blog/es/tipos-de-investigacion-de-mercados/

[42] A. Muguira, «Diseño de investigación: Elementos y características». [En línea]. Disponible en: https://www.questionpro.com/blog/es/diseno-de-investigacion/

[43] SalusPlay, «Tema 5. La Muestra y la Población de estudio». [En línea]. Disponible en: https://www.salusplay.com/apuntes/apuntes-metodologia-de-la-investigacion/tema-5-la-muestra-y-la-poblacion-de-estudio

[44] A. Muguira, «Tipos de muestreo: Cuáles son y en qué consisten». [En línea]. Disponible en: https://www.questionpro.com/blog/es/tipos-de-muestreo-para-investigaciones-sociales/

[45] SafetyCulture, «Guía breve de técnicas de recolección de datos». [En línea]. Disponible en: https://safetyculture.com/es/temas/recoleccion-de-datos/tecnicas-de-recoleccion-de-datos/

[46] M. Narváez, «¿Qué es la validez y confiabilidad en la investigación?» [En línea]. Disponible en: https://www.questionpro.com/blog/es/que-es-la-validez-y-confiabilidad-en-la-investigacion/

[47] IBM, «¿Qué es la confiabilidad de los datos?» [En línea]. Disponible en: https://www.ibm.com/mx-es/topics/data-reliability

[48] C. Ortega, «5 instrumentos para recopilar información». [En línea]. Disponible en: https://www.questionpro.com/blog/es/instrumentos-para-recopilar-informacion/

[49] J. Paniagua, «Gestión de información: su importancia en las empresas». [En línea]. Disponible en: https://trendingbusinessadvisor.com/2024/06/18/gestion-de-informacion/

ANEXOS

UNIVERSIDAD CESMAG
NIT: 800.109.387-7

"Hombres Nuevos para Tiempos Nuevos"
Fray Guillermo de Castellana OFMCap.



COMPROMISO DE CONFIDENCIALIDAD Y USO DE INFORMACIÓN
ESTUDIANTES AUXILIARES O ASISTENTES DE INVESTIGACIÓN

1. IDENTIFICACIÓN DEL ESTUDIANTE:

Nombre:	Jeison Gabriel Botina Diaz
NIUP:	1004489635
Código Estudiantil:	1211104010
Programa Académico:	Ingeniería de sistemas
Semestre:	8
Domicilio:	Corregimiento San Fernando - sector Camino real. casa #14A
Teléfono:	3188729002
Correo electrónico:	botinadiazj@gmail.com

2. PROYECTO DE INVESTIGACIÓN:

Título proyecto de investigación:	Sistema de gestión de seguridad informática para la red de datos de Ifactory, basado en la norma ISO 27001
Tipo de participación en la Investigación:	Estudiantes investigadores
Duración total de la investigación:	3 semestres
Duración de la vinculación del estudiante en la investigación:	3 semestres

3. CONSIDERACIONES:

En calidad de estudiante auxiliar o asistente de investigación de la Universidad CESMAG – UNICESMAG, en adelante denominado "estudiante", por medio del presente documento hago constar que acepto que una de mis responsabilidades durante el proyecto de investigación es mantener estricta confidencialidad y hacer uso adecuado de la información a la que tenga acceso en el proyecto de investigación citado en el numeral 2. En este sentido, suscribo este compromiso conforme a las estipulaciones en él contenidas.

4. CLASIFICACIÓN Y TRATAMIENTO DE INFORMACIÓN SENSIBLE:

Me comprometo a identificar y clasificar la información a la que tenga acceso según las categorías de confidencialidad definidas por la Universidad CESMAG, incluyendo información pública, confidencial, sensible, y de acceso restringido. Cualquier mal manejo o divulgación indebida de la información a la que tenga acceso en el proyecto de investigación, será considerada una violación grave a este compromiso.

5. OBLIGACIONES DE CONFIDENCIALIDAD MANEJO, GESTIÓN Y USO DE INFORMACIÓN

Mediante el presente documento me comprometo a cumplir las siguientes obligaciones:

a. **Confidencialidad:** Mantener absoluta confidencialidad sobre toda la información sensible confidencial y de acceso restringido relacionada con el proyecto de investigación, incluyendo, pero no limitado a datos personales, documentos, resultados, metodologías, entre otros.
b. **Acceso limitado:** Sólo acceder a la información a la que esté autorizado y que sea estrictamente necesaria para el cumplimiento de mis funciones en el proyecto.
c. **Manejo de información en equipos y plataformas institucionales:** La información debe ser almacenada, procesada y gestionada exclusivamente en equipos de cómputo y plataformas digitales de la Universidad o autorizadas por esta.
d. **Restricciones de uso:** No divulgar, compartir, reproducir, o utilizar la información a la que acceda para ningún fin distinto al autorizado por el proyecto de investigación, siempre acatando los términos del presente acuerdo.

Página **1** de **3**

Anexo 1. Carta de confidencialidad Jeison Gabriel Botina Diaz. Hoja 1



e. **Almacenamiento Seguro:** Asegurar que cualquier información sensible o personal que maneje, se almacene en entornos seguros, respetando los protocolos de la Universidad en cuanto a seguridad de la información, y no utilizar dispositivos personales para el manejo de dicha información, sin autorización.

f. **Protección de la información**: Adoptar todas las medidas necesarias para proteger la confidencialidad de la información incluyendo la prevención de accesos no autorizados, alteración o pérdida de la información. Abstenerme de copiar, reproducir o duplicar la información sin la autorización expresa de la Universidad y los propietarios del proyecto.

g. **Cumplimiento de normativas:** Acatar lo dispuesto en la Ley 1581 de 2012, el Decreto 1074 de 2015, la Politica de Tratamiento de Datos Personales de la Universidad CESMAG y cualquier otra normativa o política aplicable.

h. **Informes de incidentes o intentos de incidentes de seguridad:** En caso de identificar cualquier incidente o intento de incidente de seguridad, acceso no autorizado o vulneración de información personal, confidencial o sensible, me comprometo a notificar de inmediato al Asesor de Seguridad de la Información y Gobierno de Datos de la Universidad CESMAG, al correo electrónico jacasanova@unicesmag.edu.co, con el fin de que se implementen las medidas correctivas pertinentes.

6. TRANSMISIÓN Y COMPARTICIÓN DE INFORMACIÓN:

Conozco y acepto que cualquier transmisión de información para los fines relacionados con el proyecto de investigación deberá realizarse exclusivamente a través de canales de comunicación seguros y autorizados por la Universidad, tales como plataformas cifradas y correos electrónicos oficiales. Queda prohibido el uso de canales no seguros para la transferencia de información.

7. PROTECCIÓN DE DATOS PERSONALES:

Me comprometo a manejar cualquier dato personal obtenido en el curso del proyecto de investigación con estricta confidencialidad y conforme a las normativas vigentes sobre protección de datos personales.

8. EXCEPCIONES AL COMPROMISO DE CONFIDENCIALIDAD:

Este compromiso no será aplicable en los siguientes casos:

a. Si la información ya es de dominio público al momento de su divulgación, sin incumplir este acuerdo.
b. Si la ley o una orden judicial exigen la divulgación de la información. En tal caso, me comprometo a notificar de inmediato a la Universidad para que tome las medidas necesarias.

9. DEVOLUCIÓN Y BORRADO DE LA INFORMACIÓN SUMINISTRADA:

El suscrito estudiante con la firma de este documento hace constar que me comprometo a devolver toda la documentación suministrada (escrita, audiovisual, fotográfica, fílmica, informática, oral o sonora) facilitada en cualquier formato, así como las copias obtenidas, al finalizar mi vinculación en el proyecto de investigación o cuando así lo requiera la Universidad. Además, me comprometo a destruir adecuadamente la información que no deba ser retenida o aplicar procedimiento de borrado seguro, de acuerdo a establecido por la Universidad.

10. RESPONSABILIDAD PERSONAL Y SANCIONES:

Reconozco y acepto que cualquier incumplimiento de este compromiso podrá resultar en:

a. Responsabilidad legal: Ser sujeto de acciones legales por parte de la Universidad y/o los titulares de la información, incluyendo, pero no limitado a demandas civiles, administrativas y denuncias penales conforme a lo dispuesto en la Ley 1273 de 2009 y demás normas a que haya lugar.

b. Sanciones disciplinarias: La imposición de sanciones disciplinarias internas por parte de la Universidad.

Anexo 2. Carta de confidencialidad Jeison Gabriel Botina Diaz. Hoja 2

UNIVERSIDAD CESMAG
NIT: 800.109.387-7

"Hombres Nuevos para Tiempos Nuevos"
Fray Guillermo de Castellana OFMCap.



COMPROMISO DE CONFIDENCIALIDAD Y USO DE INFORMACIÓN
ESTUDIANTES AUXILIARES O ASISTENTES DE INVESTIGACIÓN

1. IDENTIFICACIÓN DEL ESTUDIANTE:

Nombre:	Jeison Gabriel Botina Diaz
NIUP:	1004489635
Código Estudiantil:	1211104010
Programa Académico:	Ingeniería de sistemas
Semestre:	8
Domicilio:	Corregimiento San Fernando - sector Camino real. casa #14A
Teléfono:	3188729002
Correo electrónico:	botinadiazj@gmail.com

2. PROYECTO DE INVESTIGACIÓN:

Título proyecto de investigación:	Sistema de gestión de seguridad informática para la red de datos de Ifactory, basado en la norma ISO 27001
Tipo de participación en la Investigación:	Estudiantes investigadores
Duración total de la investigación:	3 semestres
Duración de la vinculación del estudiante en la investigación:	3 semestres

3. CONSIDERACIONES:

En calidad de estudiante auxiliar o asistente de investigación de la Universidad CESMAG – UNICESMAG, en adelante denominado "estudiante", por medio del presente documento hago constar que acepto que una de mis responsabilidades durante el proyecto de investigación es mantener estricta confidencialidad y hacer uso adecuado de la información a la que tenga acceso en el proyecto de investigación citado en el numeral 2. En este sentido, suscribo este compromiso conforme a las estipulaciones en él contenidas.

4. CLASIFICACIÓN Y TRATAMIENTO DE INFORMACIÓN SENSIBLE:

Me comprometo a identificar y clasificar la información a la que tenga acceso según las categorías de confidencialidad definidas por la Universidad CESMAG, incluyendo información pública, confidencial, sensible, y de acceso restringido. Cualquier mal manejo o divulgación indebida de la información a la que tenga acceso en el proyecto de investigación, será considerada una violación grave a este compromiso.

5. OBLIGACIONES DE CONFIDENCIALIDAD MANEJO, GESTIÓN Y USO DE INFORMACIÓN

Mediante el presente documento me comprometo a cumplir las siguientes obligaciones:

a. **Confidencialidad:** Mantener absoluta confidencialidad sobre toda la información sensible confidencial y de acceso restringido relacionada con el proyecto de investigación, incluyendo, pero no limitado a datos personales, documentos, resultados, metodologías, entre otros.
b. **Acceso limitado:** Sólo acceder a la información a la que esté autorizado y que sea estrictamente necesaria para el cumplimiento de mis funciones en el proyecto.
c. **Manejo de información en equipos y plataformas institucionales:** La información debe ser almacenada, procesada y gestionada exclusivamente en equipos de cómputo y plataformas digitales de la Universidad o autorizadas por esta.
d. **Restricciones de uso:** No divulgar, compartir, reproducir, o utilizar la información a la que acceda para ningún fin distinto al autorizado por el proyecto de investigación, siempre acatando los términos del presente acuerdo.

Anexo 3. Carta de confidencialidad Jeison Gabriel Botina Diaz. Hoja 3



c. La terminación de mi vinculación en el proyecto de investigación y/o o la inhabilitación para participar en futuros proyectos de investigación por parte de la Universidad.

11. DURACIÓN DEL COMPROMISO:

Este compromiso de confidencialidad permanecerá vigente durante mi participación en el proyecto de investigación y continuará en vigor indefinidamente después de mi desvinculación, sea cual fuere la causa.

12. ACEPTACIÓN, FECHA Y FIRMA:

COMPROMETIDO

Declaro haber leído, comprendido y aceptado las obligaciones y responsabilidades establecidas en este documento, y me comprometo a cumplirlas de manera integra como condición para mi participación en el proyecto de investigación.

Fecha: 17/06/2025





Jeison Gabriel Botina Diaz (**Estudiante Investigación 1**)
C.C. No.1004489635 de Pasto (Nariño)

Anexo 4. Carta de confidencialidad Jeison Gabriel Botina Diaz. Hoja 4

UNIVERSIDAD CESMAG
NIT: 800.109.387-7

"Hombres Nuevos para Tiempos Nuevos"
Fray Guillermo de Castellana OFMCap.



COMPROMISO DE CONFIDENCIALIDAD Y USO DE INFORMACIÓN
ESTUDIANTES AUXILIARES O ASISTENTES DE INVESTIGACIÓN

1. IDENTIFICACIÓN DEL ESTUDIANTE:

Nombre:	Jesus Esteban Orbes Zambrano
NIUP:	1004190536
Código Estudiantil:	1211104023
Programa Académico:	Ingeniería de sistemas
Semestre:	8
Domicilio:	Calle 4 N°2a bis-41
Teléfono:	3187409928
Correo electrónico:	estebanzambrano318@gmail.com

2. PROYECTO DE INVESTIGACIÓN:

Titulo proyecto de investigación:	Sistema de gestión de seguridad informática para la red de datos de Ifactory, basado en la norma ISO 27001
Tipo de participación en la Investigación:	Estudiantes investigadores
Duración total de la investigación:	3 semestres
Duración de la vinculación del estudiante en la investigación:	3 semestres

3. CONSIDERACIONES:

En calidad de estudiante auxiliar o asistente de investigación de la Universidad CESMAG – UNICESMAG, en adelante denominado "estudiante", por medio del presente documento hago constar que acepto que una de mis responsabilidades durante el proyecto de investigación es mantener estricta confidencialidad y hacer uso adecuado de la información a la que tenga acceso en el proyecto de investigación citado en el numeral 2. En este sentido, suscribo este compromiso conforme a las estipulaciones en él contenidas.

4. CLASIFICACIÓN Y TRATAMIENTO DE INFORMACIÓN SENSIBLE:

Me comprometo a identificar y clasificar la información a la que tenga acceso según las categorías de confidencialidad definidas por la Universidad CESMAG, incluyendo información pública, confidencial, sensible, y de acceso restringido. Cualquier mal manejo o divulgación indebida de la información a la que tenga acceso en el proyecto de investigación, será considerada una violación grave a este compromiso.

5. OBLIGACIONES DE CONFIDENCIALIDAD MANEJO, GESTIÓN Y USO DE INFORMACIÓN

Mediante el presente documento me comprometo a cumplir las siguientes obligaciones:

a. **Confidencialidad:** Mantener absoluta confidencialidad sobre toda la información sensible confidencial y de acceso restringido relacionada con el proyecto de investigación, incluyendo, pero no limitado a datos personales, documentos, resultados, metodologías, entre otros.
b. **Acceso limitado:** Sólo acceder a la información a la que esté autorizado y que sea estrictamente necesaria para el cumplimiento de mis funciones en el proyecto.
c. **Manejo de información en equipos y plataformas institucionales:** La información debe ser almacenada, procesada y gestionada exclusivamente en equipos de cómputo y plataformas digitales de la Universidad o autorizadas por esta.
d. **Restricciones de uso:** No divulgar, compartir, reproducir, o utilizar la información a la que acceda para ningún fin distinto al autorizado por el proyecto de investigación, siempre acatando los términos del presente acuerdo.

Anexo 5. Carta de confidencialidad Jesus Esteban Orbes Zambrano. Hoja 1



e. **Almacenamiento Seguro:** Asegurar que cualquier información sensible o personal que maneje, se almacene en entornos seguros, respetando los protocolos de la Universidad en cuanto a seguridad de la información, y no utilizar dispositivos personales para el manejo de dicha información, sin autorización.

f. **Protección de la información**: Adoptar todas las medidas necesarias para proteger la confidencialidad de la información incluyendo la prevención de accesos no autorizados, alteración o pérdida de la información. Abstenerme de copiar, reproducir o duplicar la información sin la autorización expresa de la Universidad y los propietarios del proyecto.

g. **Cumplimiento de normativas:** Acatar lo dispuesto en la Ley 1581 de 2012, el Decreto 1074 de 2015, la Política de Tratamiento de Datos Personales de la Universidad CESMAG y cualquier otra normativa o política aplicable.

h. **Informes de incidentes o intentos de incidentes de seguridad:** En caso de identificar cualquier incidente o intento de incidente de seguridad, acceso no autorizado o vulneración de información personal, confidencial o sensible, me comprometo a notificar de inmediato al Asesor de Seguridad de la Información y Gobierno de Datos de la Universidad CESMAG, al correo electrónico jacasanova@unicesmag.edu.co, con el fin de que se implementen las medidas correctivas pertinentes.

6. TRANSMISIÓN Y COMPARTICIÓN DE INFORMACIÓN:

Conozco y acepto que cualquier transmisión de información para los fines relacionados con el proyecto de investigación deberá realizarse exclusivamente a través de canales de comunicación seguros y autorizados por la Universidad, tales como plataformas cifradas y correos electrónicos oficiales. Queda prohibido el uso de canales no seguros para la transferencia de información.

7. PROTECCIÓN DE DATOS PERSONALES:

Me comprometo a manejar cualquier dato personal obtenido en el curso del proyecto de investigación con estricta confidencialidad y conforme a las normativas vigentes sobre protección de datos personales.

8. EXCEPCIONES AL COMPROMISO DE CONFIDENCIALIDAD:

Este compromiso no será aplicable en los siguientes casos:

a. Si la información ya es de dominio público al momento de su divulgación, sin incumplir este acuerdo.
b. Si la ley o una orden judicial exigen la divulgación de la información. En tal caso, me comprometo a notificar de inmediato a la Universidad para que tome las medidas necesarias.

9. DEVOLUCIÓN Y BORRADO DE LA INFORMACIÓN SUMINISTRADA:

El suscrito estudiante con la firma de este documento hace constar que me comprometo a devolver toda la documentación suministrada (escrita, audiovisual, fotográfica, fílmica, informática, oral o sonora) facilitada en cualquier formato, así como las copias obtenidas, al finalizar mi vinculación en el proyecto de investigación o cuando así lo requiera la Universidad. Además, me comprometo a destruir adecuadamente la información que no deba ser retenida o aplicar procedimiento de borrado seguro, de acuerdo a establecido por la Universidad.

10. RESPONSABILIDAD PERSONAL Y SANCIONES:

Reconozco y acepto que cualquier incumplimiento de este compromiso podrá resultar en:

a. Responsabilidad legal: Ser sujeto de acciones legales por parte de la Universidad y/o los titulares de la información, incluyendo, pero no limitado a demandas civiles, administrativas y denuncias penales conforme a lo dispuesto en la Ley 1273 de 2009 y demás normas a que haya lugar.

b. Sanciones disciplinarias: La imposición de sanciones disciplinarias internas por parte de la Universidad.

Anexo 6. Carta de confidencialidad Jesus Esteban Orbes Zambrano. Hoja 2



c. La terminación de mi vinculación en el proyecto de investigación y/o o la inhabilitación para participar en futuros proyectos de investigación por parte de la Universidad.

11. DURACIÓN DEL COMPROMISO:

Este compromiso de confidencialidad permanecerá vigente durante mi participación en el proyecto de investigación y continuará en vigor indefinidamente después de mi desvinculación, sea cual fuere la causa.

12. ACEPTACIÓN, FECHA Y FIRMA:

COMPROMETIDO

Declaro haber leído, comprendido y aceptado las obligaciones y responsabilidades establecidas en este documento, y me comprometo a cumplirlas de manera íntegra como condición para mi participación en el proyecto de investigación.

Fecha: 17/06/2025



Jesus Esteban Orbes Zambrano (**Estudiante Investigación 1**)
C.C. No.1004190536 de Pasto (Nariño)

Recibido.
17-Juni 2025

Anexo 7. Carta de confidencialidad Jesus Esteban Orbes Zambrano. Hoja 3

ACTA DE ENTREGA Y RECEPCIÓN

Plan de Sistema de Gestión de Seguridad de la Información (SGSI)
Conforme a la norma ISO/IEC 27001

Lugar y fecha: Pasto, Nariño – 24 de abril de 2026

ENTREGANTES

Nombre: Jeison Gabriel Botina Diaz — Nombre: Jesús Esteban Orbes Zambrano
Cédula de Ciudadanía: 1004489645 — Cédula de Ciudadanía: 1004190536
Estudiantes X semestre Programa de Ingeniería de Sistemas – **Universidad CESMAG**

RECEPTOR

Empresa: **IFACTORY**
Responsable: Ing. Camilo Gómez Arteaga
Cargo: Director de Infraestructura de TI
Cédula de Ciudadanía: 98389866

Documentos entregados: 1. Plan de SGSI conforme a ISO/IEC 27001

Fases del SGSI (ISO/IEC 27001)

Fase	Descripción
1. Definición del Alcance y Contexto Organizacional	Identificación de procesos, activos y límites del SGSI, considerando requisitos
	legales, regulatorios y contractuales.
2. Evaluación de Riesgos y Tratamiento	Análisis sistemático de amenazas y vulnerabilidades, con definición de controles para mitigar riesgos.
3. formulación de Controles y Políticas	Aplicación de medidas técnicas, organizativas y administrativas alineadas con el Anexo A de ISO/IEC 27001.
4. Monitoreo, Medición y Auditoría Interna	Seguimiento continuo del desempeño del SGSI mediante indicadores, revisiones y auditorías internas.

Anexo 8. Acta de entrega y recepción hoja 1

Declaración

Las partes dejan constancia de que los documentos fueron entregados y recibidos en perfectas condiciones físicas y digitales, cumpliendo íntegramente con los términos, alcances y actividades previamente convenidos.

El receptor manifiesta su aceptación plena, sin reservas ni objeciones, y se compromete a dar continuidad a las fases posteriores del proyecto conforme a lo estipulado.

Firmas

Entregantes: (Estudiantes - Universidad CESMAG):

Nombre: Jeison Gabriel Botina Diaz

Firma: 

Nombre: Jesús Esteban Orbes Zambrano

Firma: 

Por la Institución Receptora (**IFACTORY**):

Nombre: Camilo Gómez Arteaga

Cargo: Ing. en sistemas | director de infraestructura de TI

Firma: 

Anexo 9. Acta de entrega y recepción hoja 2

iFactory

Pasto, Nariño, 29 de abril de 2026

Señores
Programa: Ingeniería de Sistemas
Universidad CESMAG
Pasto, Nariño, Colombia

Asunto: Entrega formal, recibido y aceptación de Plan de Sistema de Gestión de Seguridad Informática, Acta de Entrega y Recepción

Respetados señores:

Mediante el presente documento, iFACTORY, acusa haber recibido los documentos:

- "Plan de Sistema de Gestión de Seguridad Informática", el cual detalla el alcance, los acuerdos y las actividades pactadas entre las partes, conforme a lo estipulado con anterioridad y previo al inicio de las fases del proyecto.
- El "Acta de Entrega y Recepción" correspondiente, que formaliza el traspaso de los documentos mencionados.

En perfectas condiciones físicas y digitales, a su entera satisfacción plena, verificando que cumplen íntegramente con los términos, alcances y actividades previamente convenidos. Por ende, los acepta sin reservas ni objeciones.

Anexo 10. Aceptación de plan de SGSI. hoja 1

Quedamos a disposición para cualquier aclaración, ampliación o trámite complementario que estimen pertinente.

RECIBIDO, VERIFICADO, ACEPTADO Y CONFORME:

iFACTORY

Ing. Camilo Gómez Arteaga

Cargo: Ing. en sistemas | Director de infraestructura de TI

CC: 98389866

Firma:



Fecha de recibido y aceptación: 29 de abril de 2026

iFactory
Multisuministros Import SAS, Cara 14 No 15-57 Av Champagnat , Pasto, Nariño
Pasto, Nariño, Colombia
3117337729 | https://mivps.com.co

Anexo 11. Aceptación de plan de SGSI. hoja 2

¿Qué medidas de seguridad se han implementado dentro de la empresa conforme a las políticas establecidas?
Se han implementado medidas en múltiples capas (defensa en profundidad). Estas incluyen: Tecnológicas: Firewalls de próxima generación (NGFW), sistemas de detección y prevención de intrusiones (IDS/IPS), antivirus/EDR centralizado, cifrado de datos en tránsito y en reposo, y copias de seguridad regulares y verificadas. Organizativas: Concienciación y capacitación periódica a empleados, gestión de accesos basada en el principio de mínimo privilegio (Least Privilege), y un proceso formal de gestión de vulnerabilidades.

Anexo 12. Encuesta estructurada – pregunta y respuesta 1

¿Existen mecanismos de verificación o auditorías periódicas para asegurar que las configuraciones de hardening se mantengan vigentes en los servidores y firewalls?
Sí, existen mecanismos y procesos rigurosos. Auditorías Internas: Se realizan revisiones de configuración periódicas (trimestrales/semestrales) por el equipo de seguridad o TI. Auditorías Externas: Se contratan auditorías de seguridad externas y pruebas de penetración (Pen-Tests) al menos una vez al año. Monitoreo Continuo: Utilizamos herramientas de Gestión de la Postura de Seguridad (CSPM) o Gestión de Vulnerabilidades que escanean automáticamente la infraestructura para desviaciones de la línea base de hardening y vulnerabilidades conocidas.

Anexo 13. Encuesta estructurada – pregunta y respuesta 2

¿Podría explicarnos qué medidas de hardening o bastionado se han implementado en el área de sistemas para fortalecer la seguridad?
El hardening se aplica siguiendo un estándar de línea base. Las medidas clave incluyen: Deshabilitación de Servicios No Necesarios: Cierre de puertos y servicios que no son esenciales para la función del servidor. Gestión de Cuentas: Eliminación o deshabilitación de cuentas de usuario por defecto, y cambio de contraseñas por defecto. Parches y Actualizaciones: Se mantiene un ciclo de gestión de parches estricto para sistemas operativos, aplicaciones y firmware. Configuración Segura: Se implementa bloqueo de scripts, configuración de políticas de contraseñas robustas, y uso de cifrado de disco completo (Full Disk Encryption) donde sea aplicable

Anexo 14. Encuesta estructurada – pregunta y respuesta 3

¿Se ha realizado algún proceso de hardenización al servidor que nos fue proporcionado?
Sí, definitivamente. Nuestro firewall es sometido a un riguroso proceso de hardening (bastionado) y auditoría constante para asegurar su cumplimiento con la política de seguridad interna y los estándares de la industria. Las medidas clave implementadas y verificadas son: Línea Base (Hardening): El dispositivo fue configurado inicialmente siguiendo una línea base de seguridad robusta (como la establecida por CIS Benchmarks o recomendaciones del fabricante). Principio de Mínimo Privilegio: Todas las reglas de tráfico están configuradas explícitamente para "Denegar por defecto" y solo se permiten las conexiones esenciales y autorizadas. Se realiza una depuración semestral de reglas obsoletas. Gestión de Accesos: Se utiliza Autenticación Multifactor (MFA) para todo acceso administrativo al firewall. El acceso de gestión remota está estrictamente restringido solo a IPs de confianza, utilizando túneles VPN. Mantenimiento: El firmware y las firmas de seguridad se mantienen actualizados permanentemente y se aplican los parches de seguridad críticos inmediatamente tras su liberación. Verificación: El cumplimiento de estos parámetros es verificado a través de auditorías de configuración trimestrales realizadas por el equipo de TI y pruebas de penetración (Pen-Tests) anuales contratadas con un tercero.

Anexo 15. Encuesta estructurada – pregunta y respuesta 4

¿Cada cuanto se revisan los registros (logs) de seguridad y cada cuanto se revisan de forma regular para detectar intentos de intrusión o configuraciones indebidas?
La revisión de logs se gestiona mediante un enfoque dual: Monitoreo en Tiempo Real: Se utiliza un sistema SIEM (Security Information and Event Management) que analiza y correlaciona los logs 24/7 para la detección inmediata de intentos de intrusión y anomalías críticas. Revisión Periódica: El equipo de seguridad realiza un análisis manual diario de las alertas de alta prioridad generadas por el SIEM, y una revisión semanal de cumplimiento, tendencias y logs de configuraciones indebidas

Anexo 16. Encuesta estructurada – pregunta y respuesta 5

¿han sufrido recientemente algún ataque que haya interrumpido los servicios en la organización?
No se ha experimentado ninguna interrupción de servicio significativa causada por ataques o incidentes de ciberseguridad en los últimos 12 meses. Si bien nuestra plataforma de monitoreo de seguridad (SIEM/EDR) detecta constantemente intentos de ataques, escaneos de vulnerabilidades o actividades maliciosas (lo cual es normal dada la amenaza constante), nuestro modelo de defensa en profundidad ha sido efectivo para mitigar estas amenazas en sus etapas iniciales.

Anexo 17. Encuesta estructurada – pregunta y respuesta 6

¿alguna informacion adicional que guste compartirnos?
Sí. Además de las medidas específicas de hardening y monitoreo mencionadas, nos gustaría destacar la postura de seguridad proactiva de nuestra organización: Gestión de Vulnerabilidades Proactiva: Implementamos un programa continuo de gestión de vulnerabilidades, realizando escaneos internos y externos semanales y priorizando la mitigación según el riesgo. Concienciación y Entrenamiento: Llevamos a cabo simulacros de phishing trimestrales y capacitaciones obligatorias anuales para todo el personal, asegurando que el factor humano sea una defensa y no una debilidad. Plan de Respuesta a Incidentes (IRP): Contamos con un Plan Formal de Respuesta a Incidentes de Seguridad que se prueba con simulacros anuales (Tabletop Exercises) para garantizar que los equipos sepan cómo actuar de manera coordinada ante una brecha o ciberataque. Cumplimiento Normativo: Nuestro marco de seguridad está alineado con la norma ISO 27001, lo que garantiza una revisión y mejora continua de nuestros controles

Anexo 18. Encuesta estructurada – pregunta y respuesta 7

ANEXO A. PLAN DE TRATAMIENTO DE RIESGOS Y DECLARACIÓN DE APLICABILIDAD (SoA)

1. Plan de Tratamiento de Riesgos

Con base en los resultados obtenidos durante el análisis de vulnerabilidades (Nmap, Nessus, OpenVAS), se definieron acciones de tratamiento orientadas a mitigar los riesgos críticos identificados en la infraestructura de la empresa iFactory.

1.1 Tabla de tratamiento

Activo	Vulnerabilidad	Nivel de Riesgo	Control propuesto	Tipo de control	Prioridad
Servidor	SSL/TLS desactualizado	Alto	Actualización de protocolos seguros (TLS 1.2/1.3)	Técnico	Alta
Servidor	Ruby REXML vulnerable	Alto	Actualización de librerías	Técnico	Alta
Servidor	Ruby RACK vulnerable	Alto	Parcheo del sistema	Técnico	Alta
Red	Puertos abiertos (22, 808)	Medio	Cierre de puertos innecesarios	Técnico	Media
Red	Servicios expuestos	Alto	Restricción de acceso por IP	Técnico	Alta
Firewall	Configuración permisiva	Alto	Endurecimiento de reglas	Técnico	Alta
Usuarios	Acceso no controlado	Alto	Implementación de políticas de acceso	Organizativo	Alta

2. Declaración de Aplicabilidad (SoA)

La Declaración de Aplicabilidad define los controles seleccionados del Anexo A de la norma ISO/IEC 27001, indicando su aplicabilidad dentro del SGSI y su relación con los riesgos identificados.

Anexo 19. Plan tratamiento de riesgos. Hoja 1

2.1 Controles seleccionados y justificados

Control ISO	Nombre del control	Aplicabilidad	Justificación
A.5.1	Políticas de seguridad de la información	Sí	Necesario para establecer lineamientos de seguridad
A.5.15	Control de acceso	Sí	Mitiga accesos no autorizados detectados
A.8.8	Gestión de vulnerabilidades técnicas	Sí	Relacionado con vulnerabilidades detectadas
A.8.9	Configuración segura	Sí	Aplica a servicios y puertos expuestos
A.8.23	Seguridad en servicios de red	Sí	Mitiga exposición de servicios
A.8.24	Uso de criptografía	Sí	Relacionado con fallos SSL/TLS
A.5.36	Cumplimiento de políticas	Sí	Asegura control organizacional
A.8.16	Monitoreo de actividades	Sí	Permite detectar incidentes
A.5.30	Preparación para incidentes	Sí	Mejora respuesta ante ataques

3. Justificación de los controles

Los controles seleccionados fueron definidos con base en los resultados del pentesting, las vulnerabilidades críticas identificadas, la necesidad de proteger activos clave y las buenas prácticas de la norma ISO 27001.

Esto garantiza que el SGSI esté alineado con un enfoque basado en riesgos y evidencias técnicas.

ANEXO A. EVIDENCIAS DE IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD

1. Objetivo

Documentar las evidencias de implementación de controles técnicos y organizativos aplicados en la infraestructura de la empresa iFactory.

Anexo 20. Plan tratamiento de riesgos. Hoja 2

Implementación de controles

a. Controles técnicos y organizativos implementados

Controles técnicos

- Actualización de protocolos SSL/TLS
- Cierre de puertos innecesarios
- Restricción de servicios expuestos
- Aplicación de parches de seguridad
- Configuración segura de dispositivos de red

b, Controles organizativos

- Definición de políticas de seguridad
- Control de acceso a usuarios
- Gestión de vulnerabilidades
- Monitoreo continuo
- Procedimientos de respuesta a incidentes

c. Justificación de los controles

Los controles seleccionados fueron definidos con base en:

- Los resultados reales del pentesting
- Las vulnerabilidades críticas identificadas
- La necesidad de proteger activos clave
- Las buenas prácticas de la norma ISO 27001

Esto garantiza que el SGSI esté alineado con un enfoque basado en riesgos y evidencias técnicas.

4. Validación de resultados

Se realizaron pruebas posteriores utilizando herramientas como Nmap, Nessus y OpenVAS para verificar la efectividad de los controles.

Anexo 21. Plan tratamiento de riesgos. Hoja 3

5. Comparación de resultados

Métrica	Antes	Después	Resultado
Vulnerabilidades externas	61	35	Reducción
Vulnerabilidades críticas	4	1	Reducción
Vulnerabilidades internas	33	15	Reducción
Puertos abiertos	Múltiples	Reducidos	Reducción

6. Resultado

- Reducción medible de vulnerabilidades
- Disminución de la superficie de ataque
- Mejora en la seguridad de la infraestructura
- Fortalecimiento de controles técnicos y organizativos

Anexo 22. Plan tratamiento de riesgos. Hoja 4

Categoría	Activo	D	I	C	A	T
Software	Software - CMS para contenidos de sitio web (WordPress)	4	5	3	4	4
	Software - Ofimática para los usuarios	4	4	3	3	3
	Correo electrónico basado en GMail	5	5	5	5	4
	Software - Gestión de Recursos Humanos	5	5	5	5	5
Datos	Repositorio datos CMS (MariaDB)	4	5	4	4	4
	Repositorio de datos ofimáticos	4	4	4	3	3
	Base de datos Recursos Humanos	5	5	5	5	5
Servidores	Servidor Linux para CMS con Apache	4	5	4	4	4
	Servidor Windows Server para AD (Active Directory)	5	5	5	5	5
	Servidor Linux para BD de CMS MariaDB	4	5	4	4	4
	Servidor Windows Server para Archivos (datos ofimáticos)	4	4	4	3	3
	Servidor Windows Server para DHCP/DNS	5	5	4	5	4
Red, Internet	Electrónica de red (switches)	5	4	3	4	3
	Cortafuegos (reglas, VPN, DMZ)	5	5	5	5	5
	Router Internet	5	4	4	4	3

Anexo 23. Valoración de activos

Activo	Amenaza	Fre	ID	II	IC	IA	IT	RD	RI	RC	RA	RT
Software - CMS para contenidos de sitio web (WordPress)	Abuso de privilegios de acceso	M	2	4	4	3	3	2	4	4	3	3
	Acceso no autorizado	A	3	4	5	4	3	6	8	10	8	6
	Alteración de secuencia	B	3	5	4	4	3	3	5	4	4	3
	Deficiencias en la organización	M	3	4	3	3	4	3	4	3	3	4
	Divulgación de información	M	2	3	5	3	3	2	3	5	3	3
	Errores de configuración	A	4	4	3	3	4	8	8	6	6	8
	Errores de los usuarios	A	3	4	3	3	4	6	8	6	6	8
	Errores de mantenimiento / actualización de programas	A	4	5	3	3	4	8	10	6	6	8
	Errores del administrador	M	4	5	4	4	4	4	5	4	4	4
	Manipulación de los registros de actividad (log)	B	3	4	3	4	5	3	4	3	4	5
	Manipulación de programas	M	4	5	4	4	4	4	5	4	4	4
	Reencaminamiento de mensajes	MB	3	4	5	4	3	3	4	5	4	3
	Suplantación de la identidad del usuario	A	3	4	5	5	4	6	8	10	10	8
	Uso no previsto	M	3	4	3	3	4	3	4	3	3	4
	Vulnerabilidades de los programas	A	4	5	5	4	4	8	10	10	8	8
	Valoración final materialización de amenazas		4	5	5	5	5	8	10	10	10	8
Software - Ofimática para los usuarios	Abuso de privilegios de acceso	A	3	4	5	5	4	6	8	10	10	8
	Acceso no autorizado	A	4	4	5	5	4	8	8	10	10	8
	Deficiencias en la organización	M	3	4	4	4	4	3	4	4	4	4
	Divulgación de información	A	3	4	5	4	4	6	8	10	8	8
	Errores de configuración	A	4	4	4	4	4	8	8	8	8	8
	Errores de los usuarios	MA	3	4	4	3	4	6	8	8	6	8
	Errores de mantenimiento / actualización de programas	M	4	4	4	3	4	4	4	4	3	4
	Errores del administrador	M	4	4	4	4	4	4	4	4	4	4
	Manipulación de los registros de actividad (log)	B	3	4	4	4	5	3	4	4	4	5
	Manipulación de programas	B	4	5	5	4	4	4	5	5	4	4
	Suplantación de la identidad del usuario	A	3	4	5	5	4	6	8	10	10	8
	Uso no previsto	A	3	4	4	4	4	6	8	8	8	8
	Vulnerabilidades de los programas	M	4	5	5	4	4	4	5	5	4	4
	Valoración final materialización de amenazas		4	5	5	5	5	8	8	10	10	8

Anexo 24. Matriz de riesgos sección 1

Activo	Amenaza	Fre	ID	II	IC	IA	IT	RD	RI	RC	RA	RT
Software - Ofimática para los usuarios	Abuso de privilegios de acceso	A	3	4	5	5	4	6	8	10	10	8
	Acceso no autorizado	A	4	4	5	5	4	8	8	10	10	8
	Deficiencias en la organización	M	3	4	4	4	4	3	4	4	4	4
	Divulgación de información	A	3	4	5	4	4	6	8	10	8	8
	Errores de configuración	A	4	4	4	4	4	8	8	8	8	8
	Errores de los usuarios	MA	3	4	4	3	4	6	8	8	6	8
	Errores de mantenimiento / actualización de programas	M	4	4	4	3	4	4	4	4	3	4
	Errores del administrador	M	4	4	4	4	4	4	4	4	4	4
	Manipulación de los registros de actividad (log)	B	3	4	4	4	5	3	4	4	4	5
	Manipulación de programas	B	4	5	5	4	4	4	5	5	4	4
	Suplantación de la identidad del usuario	A	3	4	5	5	4	6	8	10	10	8
	Uso no previsto	A	3	4	4	4	4	6	8	8	8	8
	Vulnerabilidades de los programas	M	4	5	5	4	4	4	5	5	4	4
	Valoración final materialización de amenazas		4	5	5	5	5	8	8	10	10	8
Software - Correo electrónico basado en Gmail	Abuso de privilegios de acceso	A	3	4	5	5	4	6	8	10	10	8
	Acceso no autorizado	A	4	4	5	5	4	8	8	10	10	8
	Alteración de secuencia	B	4	4	4	4	4	4	4	4	4	4
	Deficiencias en la organización	M	3	4	4	4	4	3	4	4	4	4
	Divulgación de información	A	3	4	5	4	4	6	8	10	8	8
	Errores de configuración	A	4	4	4	4	4	8	8	8	8	8
	Errores de los usuarios	MA	3	4	5	3	4	6	8	10	6	8
	Errores de mantenimiento / actualización de programas	M	4	4	4	3	4	4	4	4	3	4
	Errores del administrador	M	4	4	4	4	4	4	4	4	4	4
	Ingeniería social	MA	3	4	5	5	4	6	8	10	10	8
	Manipulación de los registros de actividad (log)	B	3	4	4	4	5	3	4	4	4	5
	Manipulación de programas	B	4	5	5	4	4	4	5	5	4	4
	Phishing	MA	3	4	5	5	4	6	8	10	10	8
	Reencaminamiento de mensajes	A	3	4	5	4	4	6	8	10	8	8
	Repudio	M	3	3	4	4	5	3	3	4	4	5
	Suplantación de la identidad del usuario	A	3	4	5	5	4	6	8	10	10	8
	Uso no previsto	M	3	4	4	4	3	3	4	4	4	3
	Vulnerabilidades de los programas	A	4	5	5	4	4	8	10	10	8	8
	Valoración final materialización de amenazas		4	5	5	5	5	8	10	10	10	8

Anexo 25. Matriz de riesgos sección 2

Activo	Amenaza	Fre	ID	II	IC	IA	IT	RD	RI	RC	RA	RT
Software - Gestión de Recursos Humanos	Abuso de privilegios de acceso	M	4	5	5	5	4	4	5	5	5	4
	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Deficiencias en la organización	M	3	4	4	4	5	3	4	4	4	5
	Divulgación de información	A	3	4	5	4	4	6	8	10	8	8
	Errores de configuración	M	4	4	4	4	4	4	4	4	4	4
	Errores de los usuarios	MA	4	4	4	3	3	8	8	8	6	6
	Errores de mantenimiento / actualización de programas	M	4	4	3	3	4	4	4	3	3	4
	Errores del administrador	M	4	4	4	4	4	4	4	4	4	4
	Manipulación de los registros de actividad (log)	B	3	4	4	4	5	3	4	4	4	5
	Manipulación de programas	B	5	4	5	5	4	5	4	5	5	4
	Reencaminamiento de mensajes	A	3	4	5	4	4	6	8	10	8	8
	Suplantación de la identidad del usuario	A	4	5	5	5	4	8	10	10	10	8
	Uso no previsto	M	3	4	4	4	3	3	4	4	4	3
	Vulnerabilidades de los programas	A	4	5	5	4	4	8	10	10	8	8
	Valoración final materialización de amenazas		5	5	5	5	5	8	10	10	10	8
Repositorio datos CMS (MariaDB)	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Alteración accidental de la información	MA	4	5	4	3	3	8	10	8	6	6
	Destrucción de información	M	5	5	4	4	4	5	5	4	4	4
	Fugas de información	A	3	4	5	4	4	6	8	10	8	8
	Modificación deliberada de la información	B	4	5	5	5	4	4	5	5	5	4
	Ransomware	M	5	5	5	4	4	5	5	5	4	4
	Valoración final materialización de amenazas		5	5	5	5	4	8	10	10	10	8
Repositorio de datos ofimáticos	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Alteración accidental de la información	MA	3	5	4	3	3	6	10	8	6	6
	Destrucción de información	M	5	5	4	4	4	5	5	4	4	4
	Fugas de información	A	3	4	5	4	4	6	8	10	8	8
	Modificación deliberada de la información	B	4	5	5	5	4	4	5	5	5	4
	Ransomware	M	5	5	5	4	4	5	5	5	4	4
	Valoración final materialización de amenazas		5	5	5	5	4	8	10	10	10	8

Anexo 26. Matriz de riesgos sección 3

Activo	Amenaza	Fre	ID	II	IC	IA	IT	RD	RI	RC	RA	RT
Base de datos Recursos Humanos	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Alteración accidental de la información	MA	3	5	4	3	3	6	10	8	6	6
	Destrucción de información	M	5	5	4	4	4	5	5	4	4	4
	Fugas de información	A	3	4	5	4	4	6	8	10	8	8
	Modificación deliberada de la información	B	4	5	5	5	4	4	5	5	5	4
	Ransomware	M	5	5	5	4	4	5	5	5	4	4
	Valoración final materialización de amenazas		5	5	5	5	4	8	10	10	10	8
Servidor Linux para CMS con Apache	Abuso de privilegios de acceso	M	4	5	5	5	4	4	5	5	5	4
	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Ataque destructivo	M	5	5	4	4	4	5	5	4	4	4
	Avería de origen físico o lógico	M	5	5	3	3	4	5	5	3	3	4
	Caída del sistema por agotamiento de recursos	A	5	4	3	3	4	10	8	6	6	8
	Errores de mantenimiento / actualización de equipos	A	4	4	3	3	4	8	8	6	6	8
	Manipulación de la configuración	A	4	5	4	5	4	8	10	8	10	8
	Manipulación de los equipos	B	4	5	5	4	4	4	5	5	4	4
	Vulnerabilidades del Sistema Operativo	A	4	5	5	4	4	8	10	10	8	8
	Valoración final materialización de amenazas		5	5	5	5	4	10	10	10	10	8
Servidor Windows Server para AD (Active Directory)	Abuso de privilegios de acceso	M	4	5	5	5	4	4	5	5	5	4
	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Ataque destructivo	M	5	5	4	4	4	5	5	4	4	4
	Avería de origen físico o lógico	M	5	5	3	3	4	5	5	3	3	4
	Caída del sistema por agotamiento de recursos	A	5	4	3	3	4	10	8	6	6	8
	Errores de mantenimiento / actualización de equipos	A	4	4	3	3	4	8	8	6	6	8
	Manipulación de la configuración	A	4	5	4	4	4	8	10	8	8	8
	Manipulación de los equipos	B	4	5	5	4	4	4	5	5	4	4
	Vulnerabilidades del Sistema Operativo	A	4	5	5	4	4	8	10	10	8	8
	Valoración final materialización de amenazas		5	5	5	5	4	10	10	10	10	8

Anexo 27. Matriz de riesgos sección 4

Activo	Amenaza	Fre	ID	II	IC	IA	IT	RD	RI	RC	RA	RT
Servidor Linux para BD de CMS MariaDB	Abuso de privilegios de acceso	M	4	5	5	5	4	4	5	5	5	4
	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Ataque destructivo	M	5	5	4	4	4	5	5	4	4	4
	Avería de origen físico o lógico	M	5	5	3	3	4	5	5	3	3	4
	Caída del sistema por agotamiento de recursos	A	5	4	3	3	4	10	8	6	6	8
	Errores de mantenimiento / actualización de equipos	A	4	4	3	3	4	8	8	6	6	8
	Manipulación de la configuración	A	4	5	4	5	4	8	10	8	10	8
	Manipulación de los equipos	B	4	5	5	4	4	4	5	5	4	4
	Vulnerabilidades del Sistema Operativo	A	4	5	5	4	4	8	10	10	8	8
	Valoración final materialización de amenazas		5	5	5	3	3	10	10	10	10	8
Servidor Windows Server para Archivos (datos ofimáticos)	Abuso de privilegios de acceso	M	4	5	5	5	4	4	5	5	5	4
	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Ataque destructivo	M	5	5	4	4	4	5	5	4	4	4
	Avería de origen físico o lógico	M	5	5	3	3	4	5	5	3	3	4
	Caída del sistema por agotamiento de recursos	A	5	4	3	3	4	10	8	6	6	8
	Errores de mantenimiento / actualización de equipos	A	4	4	3	3	4	8	8	6	6	8
	Manipulación de la configuración	A	4	5	4	5	4	8	10	8	10	8
	Manipulación de los equipos	B	4	5	5	4	4	4	5	5	4	4
	Vulnerabilidades del Sistema Operativo	A	4	5	5	4	4	8	10	10	8	8
	Valoración final materialización de amenazas		5	5	5	5	4	10	10	10	10	8

Anexo 28. Matriz de riesgos sección 5

Activo	Amenaza	Fre	ID	II	IC	IA	IT	RD	RI	RC	RA	RT
Servidor Windows Server para DHCP/DNS	Abuso de privilegios de acceso	M	4	5	5	5	4	4	5	5	5	4
	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Ataque destructivo	M	5	5	4	4	4	5	5	4	4	4
	Avería de origen físico o lógico	M	5	5	3	3	4	5	5	3	3	4
	Caída del sistema por agotamiento de recursos	A	5	4	3	3	4	10	8	6	6	8
	Errores de mantenimiento / actualización de equipos	A	4	4	3	3	4	8	8	6	6	8
	Manipulación de la configuración	A	4	5	4	5	4	8	10	8	10	8
	Manipulación de los equipos	B	4	5	5	4	4	4	5	5	4	4
	Vulnerabilidades del Sistema Operativo	A	4	5	5	4	4	8	10	10	8	8
	Valoración final materialización de amenazas		5	5	5	5	4	10	10	10	10	8
Electrónica de red (switches)	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Alteración de secuencia	A	4	5	4	5	4	8	10	8	10	8
	Análisis de tráfico	A	3	4	5	5	4	6	8	10	10	8
	Caída del sistema por agotamiento de recursos	A	5	4	3	3	4	10	8	6	6	8
	Denegación de servicio	A	5	4	3	4	4	10	8	6	8	8
	Errores del administrador	A	4	4	3	3	4	8	8	6	6	8
	Fallo de servicios de comunicaciones	M	5	4	3	3	4	5	4	3	3	4
	Interceptación de información (escucha)	A	3	4	5	5	4	6	8	10	10	8
	Reencaminamiento de mensajes	M	4	5	5	5	4	4	5	5	5	4
	Robo	B	5	4	5	4	4	5	4	5	4	4
	Vulnerabilidades del firmware	M	4	5	5	5	4	4	5	5	5	4
	Valoración final materialización de amenazas		5	5	5	5	4	10	10	10	10	8

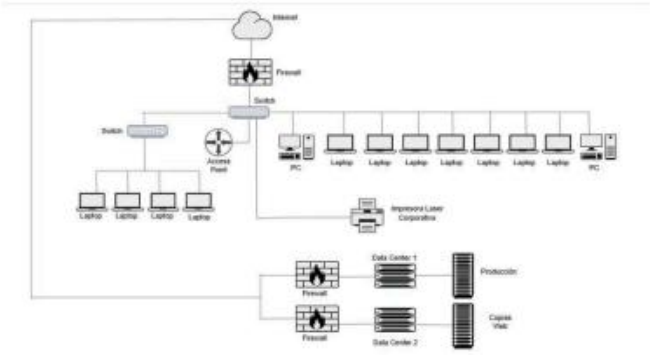
Anexo 29. Matriz de riesgos sección 6

Cortafuegos (reglas, VPN, DMZ)	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Alteración de secuencia	M	4	5	4	5	4	4	5	4	5	4
	Análisis de tráfico	A	3	4	5	5	4	6	8	10	10	8
	Caída del sistema por agotamiento de recursos	A	5	4	3	3	4	10	8	6	6	8
	Denegación de servicio	A	5	4	3	4	4	10	8	6	8	8
	Errores del administrador	A	4	4	3	3	4	8	8	6	6	8
	Fallo de servicios de comunicaciones	M	5	4	3	3	4	5	4	3	3	4
	Interceptación de información (escucha)	A	3	4	5	5	4	6	8	10	10	8
	Robo	B	5	4	5	4	4	5	4	5	4	4
	Vulnerabilidades del firmware	M	4	5	5	5	4	4	5	5	5	4
	Valoración final materialización de amenazas		5	5	5	5	4	10	10	10	10	8
Router Internet	Acceso no autorizado	A	4	5	5	5	4	8	10	10	10	8
	Alteración de secuencia	M	4	5	4	5	4	4	5	4	5	4
	Análisis de tráfico	A	3	4	5	5	2	6	8	10	10	4
	Caída del sistema por agotamiento de recursos	A	5	4	3	3	4	10	8	6	6	8
	Denegación de servicio	A	5	4	3	4	4	10	8	6	8	8
	Errores del administrador	M	4	4	3	3	4	4	4	3	3	4
	Fallo de servicios de comunicaciones	M	5	4	3	3	4	5	4	3	3	4
	Interceptación de información (escucha)	A	3	4	5	5	4	6	8	10	10	8
	Reencaminamiento de mensajes	MB	4	5	5	5	4	4	5	5	5	4
	Robo	B	5	4	5	4	4	5	4	5	4	4
	Vulnerabilidades del firmware	M	4	5	5	5	4	4	5	5	5	4
	Valoración final materialización de amenazas		5	5	5	5	4	10	10	10	10	8

Anexo 30. Matriz de riesgos sección 7

Informe auditoria

Como parte del proceso de diagnóstico y análisis de seguridad de la información en la empresa iFactory, se ha desarrollado un diagrama detallado de la red tecnológica que soporta sus operaciones.



Como resultado del levantamiento de la red tecnológica de iFactory, se ha elaborado un inventario detallado de los activos de información presentes en la organización. Este inventario permite identificar, clasificar y valorar los elementos que soportan los procesos críticos del negocio, facilitando la gestión de riesgos y la implementación de controles de seguridad conforme a la norma ISO/IEC 27001

Lista de los activos de información

- Firewall Fortinet Fortigate 200E
- Firewall Fortigate 90D
- Firewall Fortigate 60D
- Laptops
- Impresora Samsung ML-4551ND
- Switch de 2 capas de 24 puertos Gigabit
- Router Ubiquiti

Como parte del desarrollo metodológico se diseñó una bitácora de lo desarrollado hasta el momento

Anexo 31. Informe auditoria pág. 1

Bitácora Técnica – Parte 1: Acciones y Resultados

Fecha y Hora	Acciones Realizadas	Resultados Obtenidos
13 de septiembre 2025 9:30AM – 12:00PM	Recolección de información de los activos de información de iFactory.	Se elaboró un inventario detallado que identifica, clasifica y valora los activos críticos para la seguridad.
20 de septiembre 2025 9:30AM – 12:00 PM	Instalación de VirtualBox versión 7.2.2 en equipo local.	Se habilitó el entorno de virtualización para pruebas de seguridad.
20 de septiembre 2025 10:30AM – 12:00 PM	Instalación de Kali Linux versión 2025.3 en máquina virtual de VirtualBox.	Se configuró el sistema operativo especializado en análisis de seguridad.
27 de septiembre 2025 9:30AM – 12:00 PM	Habilitación de cuenta en el servidor de iFactory.	Se obtuvo acceso remoto para realizar pruebas internas de seguridad.
4 de octubre 2025 9:30AM – 12:00 PM	Instalación de VirtualBox 7.2.2 dentro del servidor.	Se replicó el entorno de pruebas en el servidor institucional.
4 de octubre 2025 11:00AM – 12:00 PM	Instalación de Kali Linux 2025.3 en máquina virtual del servidor.	Se habilitó el entorno de análisis dentro del servidor para escaneos internos.
11 de octubre 2025 9:00AM – 12:00 PM	Ejecución de escaneos con NMAP y MASSCAN dentro y fuera del servidor.	Se identificaron puertos abiertos, servicios expuestos y hosts activos. Se detectaron riesgos potenciales.
25 de octubre 2025 9:00 AM – 12:00 PM	Ejecución de escaneos con Nikto versión 2.5.0 y configuración de Burpsuite , configuración del FoxyProxy en el navegador de firefox en Kali linux y ejecución de esta misma	en la herramienta de nikto no obtuvimos resultados ya que esta herramienta está enfocada a servidores web, mismo caso con burpsuite
29 de octubre 2025 9:00 AM – 12:00 PM	Se procedió a ejecutar nuevamente Nikto y BurpSuite, incorporando ciertas recomendaciones y nuevas acciones en ambas herramientas. Sin embargo, los resultados obtenidos fueron los mismos, lo que permitió descartar posibles errores cometidos en ejecuciones anteriores.	Tras la reejecución de Nikto y BurpSuite con ajustes recomendados, se obtuvieron los mismos hallazgos que en las pruebas anteriores. Esto confirma la consistencia de los resultados y permite descartar posibles errores de configuración o interpretación en ejecuciones previas.
30 de octubre 2025 9:00 AM – 12 PM	se realizo la respectiva instalacion de nessus, despues se procedio a realizar el escaneo de	El escaneo de vulnerabilidades con Nessus al host 192.168.0.127 detectó 61

Anexo 32. Informe auditoria pág. 2

	vulnerabilidades fuera del servidor.	vulnerabilidades, incluyendo 4 altas, 1 media y varias informativas. Las más críticas afectan a Ruby REXML y Ruby RACK, y se identificó un certificado SSL no confiable.
1 de noviembre 2025 9:00 AM – 12 PM	con la respectiva instalacion realizada anteriormente se procedió a hacer el escaneo dentro del servidor	El escaneo en el servidor 192.168.2.36 detectó 33 vulnerabilidades, incluyendo 1 alta y varias medias, principalmente relacionadas con configuraciones y protocolos SSL/TLS desactualizados. El resto son hallazgos informativos sobre servicios y sistema.
8 de noviembre 2025 9:00 AM – 12 PM	re realiza la instalacion de openvas dentro del servidor asignado	La instalación de OpenVAS se completó correctamente en el servidor asignado. el sistema está listo para ejecutar escaneos de vulnerabilidades de forma confiable.
15 de noviembre 2025 9:00 AM – 12 PM	realizada la respectiva instalacion de openvas procedimos a configurar el acceso	La configuración de acceso a la consola de OpenVAS se realizó de forma exitosa, verificándose el funcionamiento del servicio web y el ingreso correcto con el usuario administrador sin presentar ningún inconveniente.

Anexo 33. Informe auditoria pág. 3

ESCANEO FUERA DEL SERVIDOR CON LA HERRAMIENTA NMAP

Escaneo completo de puertos TCP

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- 192.168.0.1
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-11 10:36 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0011s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  open   ssh
113/tcp closed ident
808/tcp open   ccproxy-http
MAC Address: 08:5B:0E:B2:06:6E (Fortinet)

Nmap done: 1 IP address (1 host up) scanned in 120.32 seconds
```

Puerto	Servicio	Seguridad (open)
22/tcp	ssh	El puerto 22 está abierto por defecto para SSH (Secure Shell), un protocolo que cifra las comunicaciones y permite la administración remota de servidores. Si bien es una configuración estándar, su abertura puede representar un riesgo de seguridad, por lo que se recomienda cambiarlo a un puerto no predeterminado, especialmente en servidores que se exponen directamente a Internet
808/tcp	ccproxy-http	El puerto 808/tcp está abierto por defecto para servicios HTTP alternativos, y en este caso está vinculado al servicio ccproxy-http, un servidor proxy que permite compartir y controlar el acceso a Internet. Aunque puede ser útil en entornos de red interna, su exposición directa a Internet representa un riesgo de seguridad considerable. Se recomienda restringir el acceso mediante firewall, habilitar autenticación en el proxy, y evitar configuraciones que lo conviertan en un proxy abierto, ya que podría ser explotado por terceros para ocultar actividades maliciosas o lanzar ataques desde tu red.

Anexo 34. Informe auditoria pág. 4

puertos y servicios expuestos

```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-11 10:46 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.1
Host is up (0.0029s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
22/tcp  open   ssh
113/tcp closed ident
808/tcp open   ccproxy-http
MAC Address: 08:5B:0E:B2:06:6E (Fortinet)

Nmap done: 1 IP address (1 host up) scanned in 44.31 seconds
```

Puerto	Servicio	Seguridad (open)
22/tcp	ssh	El puerto 22 está abierto por defecto para SSH (Secure Shell), un protocolo que cifra las comunicaciones y permite la administración remota de servidores. Si bien es una configuración estándar, su abertura puede representar un riesgo de seguridad, por lo que se recomienda cambiarlo a un puerto no predeterminado, especialmente en servidores que se exponen directamente a Internet
808/tcp	Ccproxy-http	El puerto 808/tcp está abierto por defecto para servicios HTTP alternativos, y en este caso está vinculado al servicio ccproxy-http, un servidor proxy que permite compartir y controlar el acceso a Internet. Aunque puede ser útil en entornos de red interna, su exposición directa a Internet representa un riesgo de seguridad considerable. Se recomienda restringir el acceso mediante firewall, habilitar autenticación en el proxy, y evitar configuraciones que lo conviertan en un proxy abierto, ya que podría ser explotado por terceros para ocultar actividades maliciosas o lanzar ataques desde tu red.

Anexo 35. Informe auditoria pág. 5

Host activos

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-11 10:55 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0013s latency).
MAC Address: 08:5B:0E:B2:06:6E (Fortinet)
Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

El host 192.168.0.1 está **activo**, con una **latencia de 0.0013 segundos** (respuesta rápida).

Escaneo fuera del servidor con la herramienta MASSCAN

Escaneo completo de puertos TCP

```
┌──(kali㉿kali)-[~]
└─$ sudo masscan -p1-65535 192.168.0.1 --rate 109
[sudo] password for kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-10-11 16:19:44 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 22/tcp on 192.168.0.1
Discovered open port 808/tcp on 192.168.0.1

┌──(kali㉿kali)-[~]
└─$
```

Puerto	Servicio	Riesgo Potencial
22/tcp	SSH	Ataques de fuerza bruta, acceso remoto no autorizado si no se configura adecuadamente
808/tcp	ccproxy-http	Proxy abierto, uso malicioso por terceros, fuga de información, escaneo interno

Anexo 36. Informe auditoria pág. 6

Escaneo de Host Activos

```
┌──(kali㉿kali)-[~]
└─$ sudo masscan 192.168.0.1/24 --ping
[sudo] password for kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-10-11 16:40:38 GMT
Initiating ICMP Echo Scan
Scanning 256 hosts
Discovered open port 0/icmp on 192.168.0.1
```

- El host respondió al ping, lo que indica que está activo y conectado a la red.

ESCANEO DENTRO DEL SERVIDOR CON LA HERRAMIENTA NMAP

Escaneo completo de puertos TCP

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- 192.168.2.36
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-11 12:50 EDT
Nmap scan report for 192.168.2.36
Host is up (0.00067s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
5985/tcp open  wsman
MAC Address: BC:24:11:56:E0:45 (Proxmox Server Solutions GmbH)

Nmap done: 1 IP address (1 host up) scanned in 112.75 seconds
```

Puerto	Servicio	Riesgo Potencial (STATE open)
3389/tcp	ms-wbt-server (RDP)	- Acceso remoto no autorizado - Ataques de fuerza bruta - Vulnerabilidades en versiones antiguas
5357/tcp	wsdapi (Web Services for Devices)	- Exposición innecesaria en redes no confiables - Posible enumeración de dispositivos - Poca visibilidad en auditorías tradicionales

Anexo 37. Informe auditoria pág. 7

5985/tcp	wsman (WinRM sobre HTTP)	- Transmisión en texto plano - Riesgo de ejecución remota - Vulnerable si se expone a Internet sin control

Puertos y servicios expuestos

```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.2.36
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-11 12:55 EDT
Nmap scan report for 192.168.2.36
Host is up (0.00072s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
5985/tcp open  wsman
MAC Address: BC:24:11:56:E0:45 (Proxmox Server Solutions GmbH)

Nmap done: 1 IP address (1 host up) scanned in 43.75 seconds
```

Puerto	Servicio	Descripción Técnica
3389/tcp	ms-wbt-server (RDP)	Protocolo de Escritorio Remoto (Remote Desktop Protocol) usado para acceso remoto a sistemas Windows.
5357/tcp	wsdapi (Web Services for Devices)	Servicio usado por Windows para descubrimiento y comunicación con dispositivos en red.
5985/tcp	wsman (WinRM sobre HTTP)	Administración remota vía PowerShell sin cifrado. Permite ejecución de comandos en el host.

Anexo 38. Informe auditoria pág. 8

Host activos

```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.2.36
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-11 12:57 EDT
Nmap scan report for 192.168.2.36
Host is up (0.00066s latency).
MAC Address: BC:24:11:56:E0:45 (Proxmox Server Solutions GmbH)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

El host 192.168.2.36 está **activo**, con una **latencia de 0.00066 segundos** (respuesta muy rápida).

Escaneo fuera del servidor con la herramienta MASSCAN

Escaneo de puertos TCP

```
┌──(kali㉿kali)-[~]
└─$ sudo masscan -p1-65535 192.168.2.36 --rate 109
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-10-11 16:59:21 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
```

exploración completa de todos los puertos TCP en el host 192.168.2.36, usando **Masscan**

Host Activos

```
┌──(kali㉿kali)-[~]
└─$ sudo masscan 192.168.2.36/24 --ping
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-10-11 17:11:34 GMT
Initiating ICMP Echo Scan
Scanning 256 hosts
Discovered open port 0/icmp on 192.168.2.254
```

Se detectó que el host 192.168.2.254 respondió al ping.

El mensaje "Discovered open port 0/icmp" indica que el host está **activo y accesible** en la red.

Anexo 39. Informe auditoria pág. 9

Comparativo: Nmap vs Masscan

Resumen ejecutivo

Este documento presenta un análisis comparativo entre dos herramientas de escaneo de red —Nmap y Masscan— y resume su comportamiento y resultados en el entorno analizado. Se ofrece, además, un procedimiento operativo recomendado para combinar ambas herramientas de forma segura y eficiente.

1. **Hallazgos principales**

• Nmap identificó puertos y servicios con mayor detalle (por ejemplo: 22/tcp —SSH; 3389/tcp —RDP; 5985/tcp —WinRM). Los hallazgos incluyen servicios detectados tanto en equipos internos como en hosts externos.

• Masscan realizó un barrido de gran velocidad y reportó rápidamente hosts y puertos con respuesta (puertos como 22 y 808). Algunos registros muestran detecciones asociadas a ICMP (entradas tipo "port 0/icmp"), que indican presencia del host pero no un servicio TCP.

2. **Comparacion resumida**

Aspecto	**Nmap**	**Masscan**
Velocidad	Realiza escaneos más lentos que permiten mayor profundidad.	Optimizado para barridos masivos y muy rápido.
Nivel de detalle	Entrega identificación de servicios, versiones y opciones avanzadas con scripts.	Reporta puertos abiertos rápidamente; no identifica versiones por defecto.
Precisión	Menor tasa de falsos positivos gracias a comprobaciones adicionales.	Puede producir falsos positivos; requiere verificación posterior.

Anexo 40. Informe auditoria pág. 10

Detección de hosts	Soporta múltiples métodos (ICMP, ARP, TCP) y aporta información fiable.	Detecta hosts con rapidez; algunas entradas requieren interpretación (ej.: 0/icmp).
Uso típico	Análisis en profundidad, auditorías y verificación de servicios.	Inventario rápido de puertos/hosts a gran escala.
Recomendación práctica	Usarlo para validar y profundizar en resultados preliminares.	Emplearlo como primer paso para identificar áreas de interés.

3. Interpretacion de los resultados

Los resultados de Masscan son coherentes con los de Nmap en cuanto a la presencia de hosts y puertos; sin embargo, Nmap aporta contexto adicional (tipo de servicio y posibles versiones) que es necesario para evaluar riesgos y decidir medidas.

Entradas identificadas por Masscan como relacionadas con ICMP deben interpretarse como indicativo de que el host responde, no como prueba de un servicio TCP abierto. Se recomienda validar esos puntos con Nmap antes de cualquier acción correctiva.

4. Procedimiento operativo sugerido

• Ejecutar Masscan para obtener un mapeo rápido de hosts y puertos en el rango objetivo.

• Filtrar la salida de Masscan para eliminar artefactos (por ejemplo: registros tipo 0/icmp) y consolidar la lista por host.

• Realizar escaneos focalizados con Nmap sobre los puertos detectados por Masscan empleando opciones de identificación (-sV) y, cuando proceda, análisis más completo (-A).

• Documentar los resultados y priorizar medidas en función del riesgo (cerrar puertos innecesarios, filtrar accesos, reforzar autenticación).

5. Observaciones y consideraciones

• Masscan es una herramienta de reconocimiento de alto rendimiento; no debe usarse como única fuente para decisiones de seguridad.
• Nmap aporta la profundidad necesaria para confirmar la naturaleza de los servicios detectados.

Anexo 41. Informe auditoria pág. 11

• Cualquier actividad de escaneo debe contar con la autorización pertinente y quedar registrada (fecha, alcance y responsable).

Nikto

La salida que muestra el comando **nikto -h 192.168.2.36 i**ndica que no se realizó ningún escaneo sobre el host especificado.

Análisis del resultado

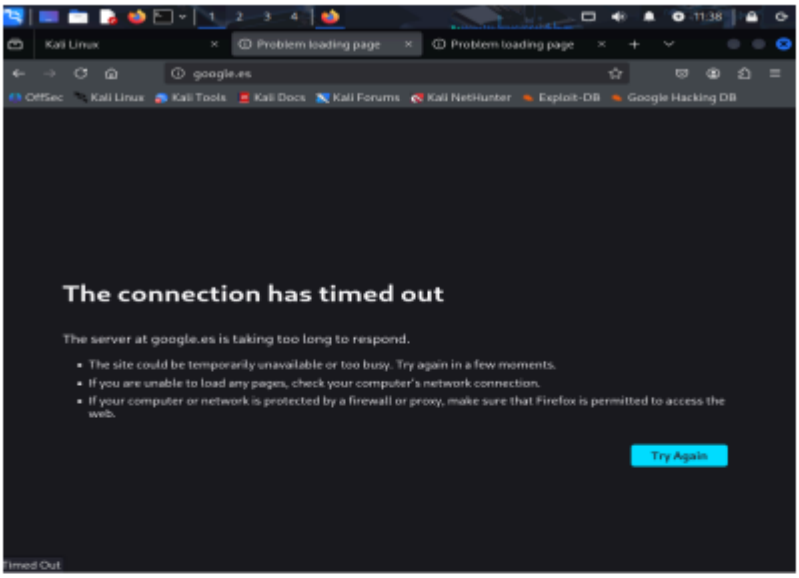
- Versión de Nikto: Se ejecutó la versión 2.5.0 del escáner.
- Host objetivo: Se intentó escanear la IP **192.168.2.36**

Resultado:
+ 0 host(s) tested

- Esto significa que Nikto no logró conectarse al host, por lo tanto no se realizó ningún escaneo.

Burpsuite

Anexo 42. Informe auditoria pág. 12



obtuvimos un error de conexión en Firefox en Kali Linux al intentar acceder a **google.es** ya configurado el FoxyProxy

Análisis

1. Error mostrado

> **"The connection has timed out. The server at google.es is taking too long to respond."**

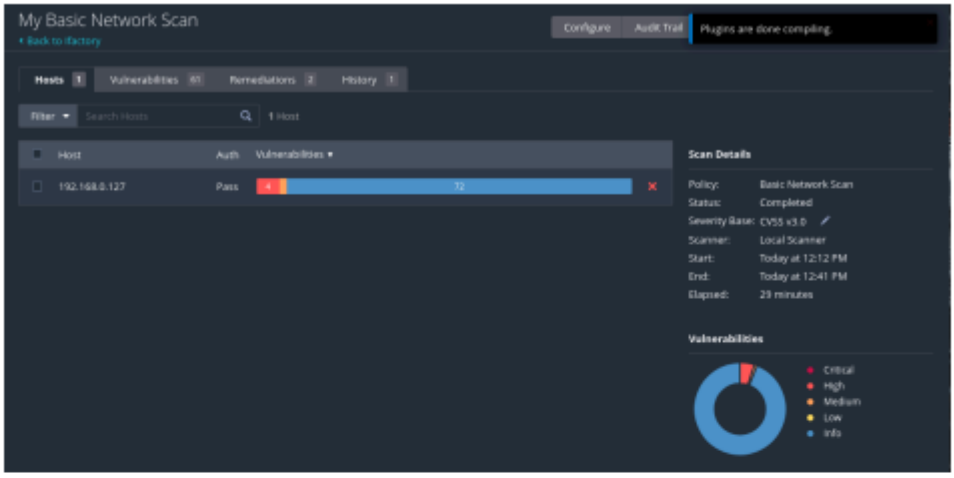
Esto significa que no se logró la comunicación con Burpsuite dado que:

- **El proxy configurado no está respondiendo.**

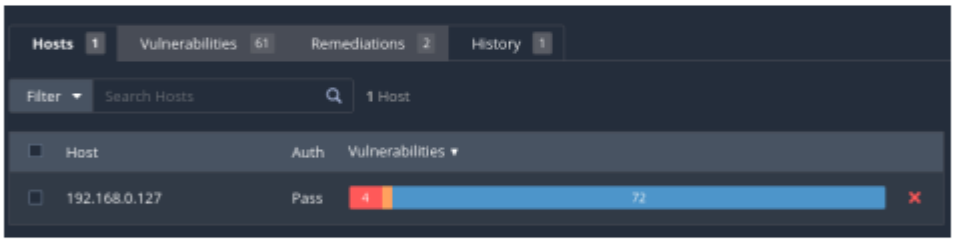
Escaneo Y Resultados mediante la herramienta de NESSUS

Anexo 43. Informe auditoria pág. 13

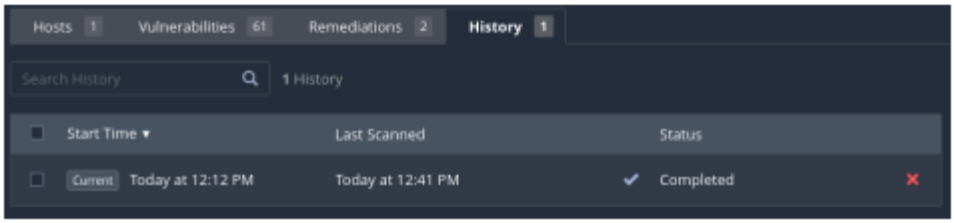
(fuera del servidor)



Host

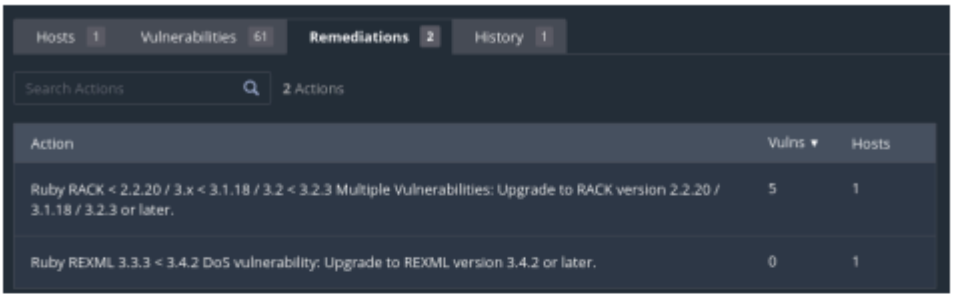


History

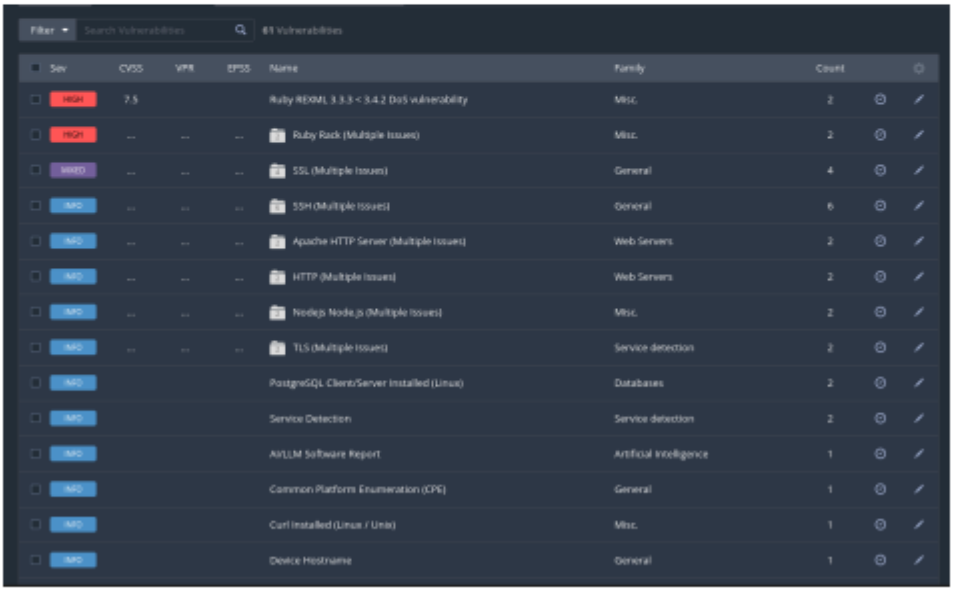


Anexo 44. Informe auditoria pág. 14

Remediations



Vulnerabilities

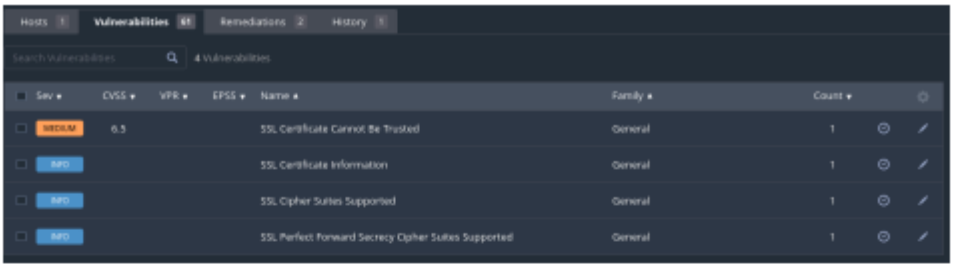


Anexo 45. Informe auditoria pág. 15



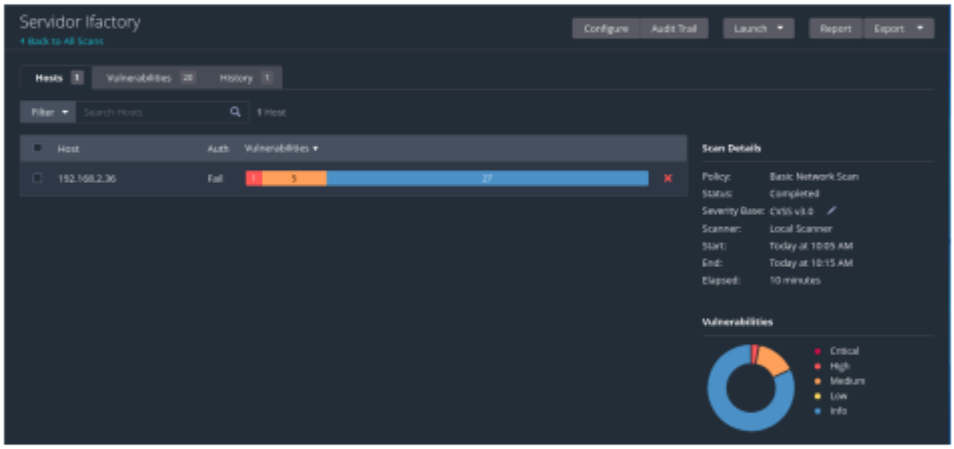
ARCHIVO MIXED (Vulnerabilities) (Multiple Issues)

Anexo 46. Informe auditoria pág. 16



Escaneo Y Resultados mediante la herramienta de NESSUS

(Dentro del servidor)

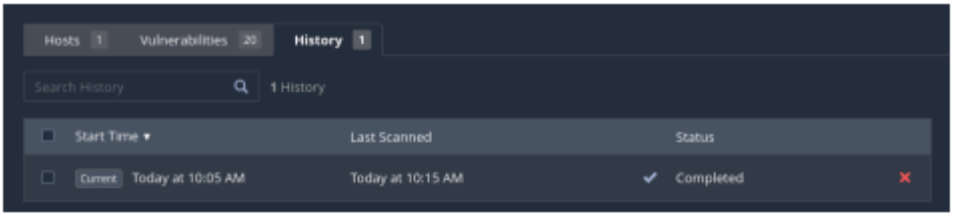


Host

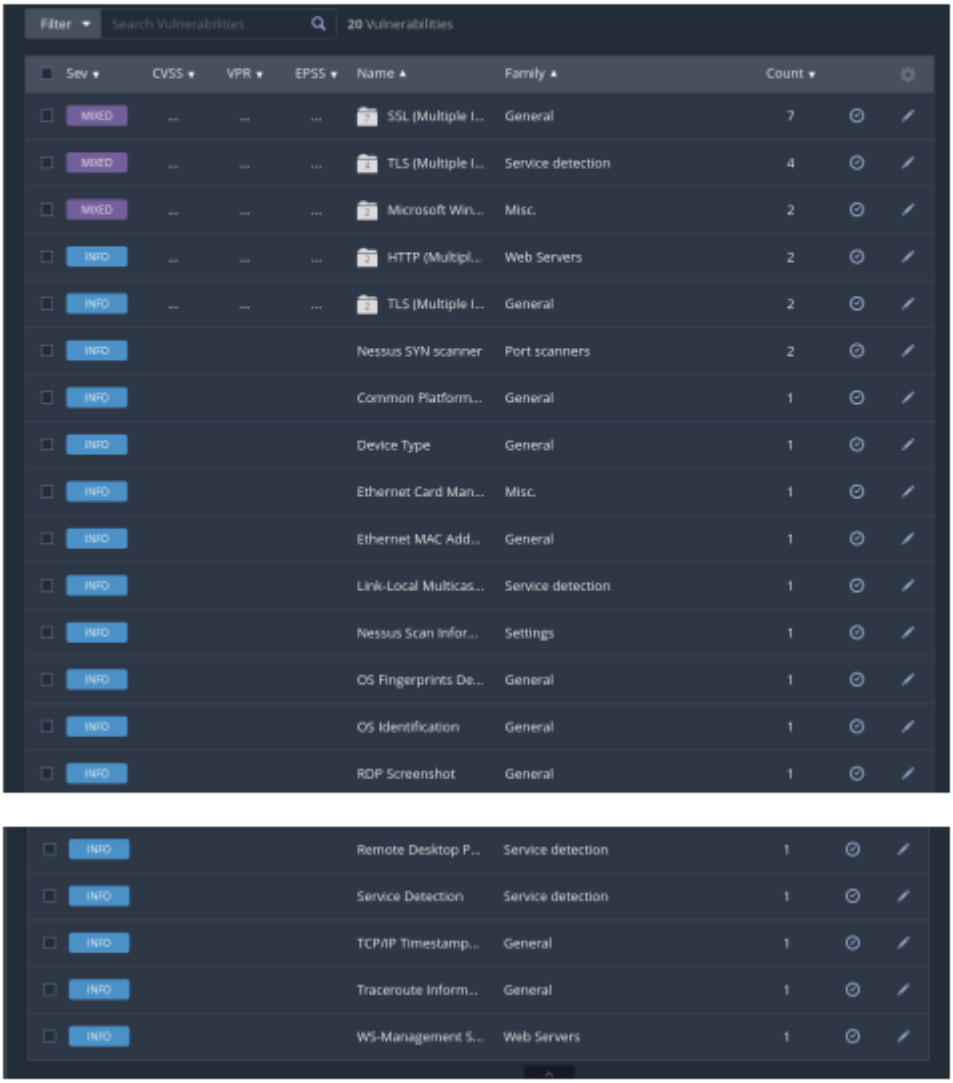


History

Anexo 47. Informe auditoria pág. 17

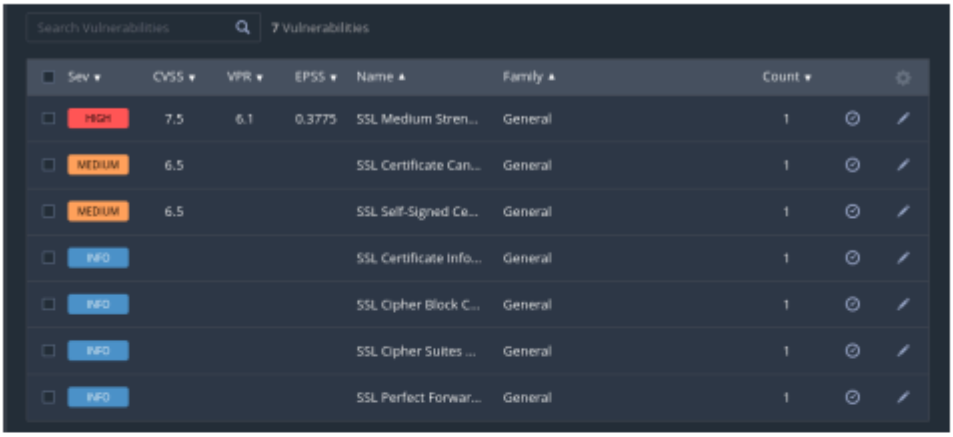


Vulnerabilities

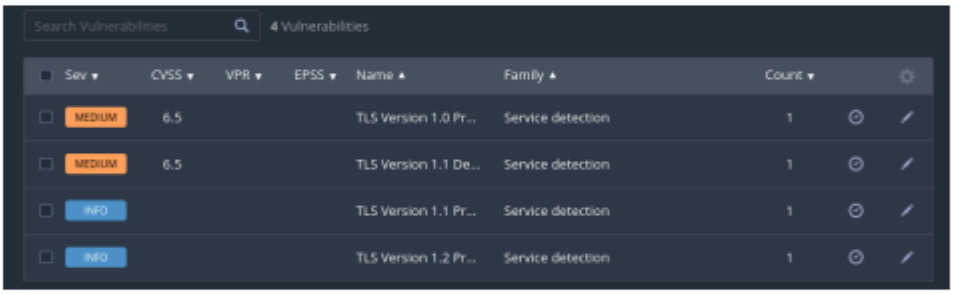


Anexo 48. Informe auditoria pág. 18

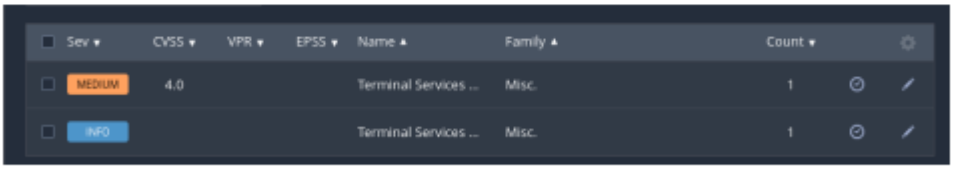
ARCHIVO MIXED 1 (Vulnerabilities) (Multiple Issues)



ARCHIVO MIXED 2 (Vulnerabilities) (Multiple Issues)



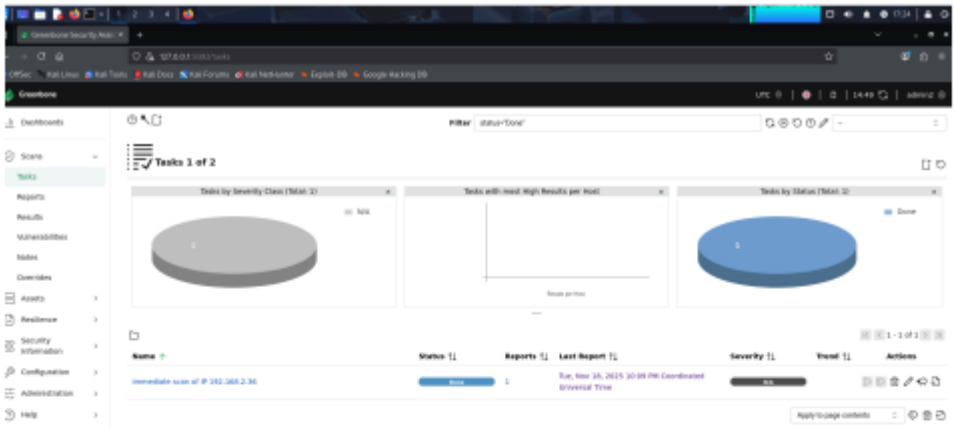
ARCHIVO MIXED 3 (Vulnerabilities) (Multiple Issues)



openvas

escaneo dentro del servidor

Anexo 49. Informe auditoria pág. 19



Comparativa de Resultados: Nessus vs OpenVAS

Criterio	Nessus	OpenVAS
Host Analizado	El escaneo se ejecutó sobre el host 192.168.2.36, confirmando disponibilidad y recopilando información detallada de servicios, puertos y configuraciones.	El mismo host 192.168.2.36 fue analizado, permitiendo comparar la calidad de detección entre ambas herramientas dentro del mismo entorno.
Estado del Escaneo	Completed: todas las fases del análisis se realizaron con éxito, incluyendo detección de puertos, evaluación y reporte.	Done: indica que el proceso terminó, aunque sin detalles mostrados sobre el análisis realizado.

Anexo 50. Informe auditoria pág. 20

Duración del Escaneo	Aproximadamente 10 minutos debido a la profundidad y cantidad de plugins usados por Nessus.	No visible, aunque OpenVAS suele tardar más por la ejecución más lenta de scripts.
Política de Escaneo	Basic Network Scan: diseñada para identificar una amplia gama de vulnerabilidades y servicios expuestos.	No visible, aunque normalmente usa perfiles estándar como Full and Fast o Host Discovery.
Autenticación	Fail: no fue posible autenticarse, limitando la detección profunda de vulnerabilidades internas.	No visible, posiblemente se ejecutó un escaneo no autenticado.
Total de Vulnerabilidades	33 vulnerabilidades encontradas distribuidas en varios niveles de severidad.	No visible, aunque se observan algunos resultados parciales.
Críticas	1 vulnerabilidad crítica relacionada con	No visible en la vista disponible.
	configuraciones de cifrado o servicios expuestos.	
Altas	1 vulnerabilidad alta encontrada.	1 vulnerabilidad alta detectada según el gráfico.
Medias	5 vulnerabilidades medias asociadas a configuraciones inseguras o software desactualizado.	No visibles en el reporte mostrado.
Informativas	Más de 20 hallazgos informativos útiles para comprender la superficie de ataque.	No visibles en la vista actual.

Anexo 51. Informe auditoria pág. 21

Nivel de detalle	Muy alto: incluye descripciones técnicas, CVE, recomendaciones y evidencias.	Bajo en la vista mostrada, aunque OpenVAS puede generar reportes completos.
Principales Vulnerabilidades	SSL/TLS débiles, certificados obsoletos, suites criptográficas inseguras, información HTTP, detección de servicios.	No visibles en la vista disponible.
Reportes	Exportables en PDF, HTML y otros formatos.	Disponibles, aunque no se muestra su contenido.

Anexo 52. Informe auditoria pág. 22

San Juan de Pasto, 28/09/2026

Señor
Ing. Camilo Gómez Arteaga
Ingeniero de Sistemas
iFactory

Asunto: Entrega de resultados del trabajo de grado

Cordial saludo.

Por medio de la presente, nosotros, **Jeison Gabriel Botina Diaz** y **Jesús Esteban Orbes Zambrano**, estudiantes del Programa de Ingeniería de Sistemas de la Universidad CESMAG, hacemos entrega formal a la empresa **iFactory** de los resultados obtenidos durante el desarrollo del trabajo de grado titulado **"Sistema de Gestión de Seguridad Informática para la red de datos de iFactory, basado en la norma ISO/IEC 27001"**.

Como resultado del proyecto, se entrega la documentación correspondiente al análisis realizado sobre la seguridad de la red de datos de la empresa, incluyendo la identificación de activos, análisis de vulnerabilidades mediante pruebas de seguridad, valoración y gestión de riesgos, así como la formulación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001.

De igual manera, se hace entrega del **informe de hallazgos y análisis del SGSI**, en el cual se presentan los principales resultados obtenidos durante las pruebas realizadas y las propuestas de tratamiento y controles de seguridad formuladas de acuerdo con las necesidades identificadas en iFactory.

La documentación entregada tiene como finalidad servir como referencia para la gestión de los riesgos relacionados con la seguridad de la información y como insumo para las acciones que la empresa considere pertinentes en el futuro.

Se deja constancia de que el proyecto corresponde a un ejercicio académico de **formulación del SGSI**, por lo cual la implementación de las medidas y controles propuestos queda sujeta a las decisiones, autorizaciones y condiciones propias de la empresa.

Agradecemos nuevamente a iFactory y, especialmente, al Ingeniero Camilo Gómez Arteaga, por la disposición y colaboración brindadas durante el desarrollo de este trabajo.

Atentamente,

JEISON GABRIEL BOTINA
Estudiante – Ingeniería de Sistemas
Universidad CESMAG

JESÚS ESTEBAN ORBES
Estudiante – Ingeniería de Sistemas
Universidad CESMAG

Firma Ing. Camilo Gómez Arteaga:

Anexo 53. Carta de entrega de Informe para iFactory

San Juan de Pasto, 28/09/2026

Señor
Ing. Camilo Gómez Arteaga
Ingeniero de Sistemas
iFactory

Asunto: Agradecimiento por el acompañamiento durante el desarrollo del trabajo de grado

Cordial saludo.

Por medio de la presente, queremos expresar nuestro más sincero agradecimiento por el apoyo, la disposición y el acompañamiento brindado durante el desarrollo de nuestro trabajo de grado titulado **"Sistema de Gestión de Seguridad Informática para la red de datos de iFactory, basado en la norma ISO/IEC 27001"**.

Agradecemos especialmente el tiempo dedicado para atender nuestras consultas, compartir sus conocimientos y experiencia, así como facilitar el desarrollo de las actividades relacionadas con el análisis de la infraestructura tecnológica y la seguridad de la información de la empresa.

Su colaboración fue fundamental para llevar a cabo el análisis de vulnerabilidades, la identificación de riesgos y la formulación de las propuestas de seguridad contempladas en el proyecto. De igual manera, valoramos la disposición mostrada durante la revisión del alcance y las actividades realizadas en el marco de la investigación.

Para nosotros, como estudiantes del Programa de Ingeniería de Sistemas de la Universidad CESMAG, esta experiencia representó una oportunidad importante para aplicar los conocimientos adquiridos durante nuestra formación académica en un contexto empresarial real.

Reiteramos nuestro agradecimiento por la confianza, el tiempo y la colaboración brindados durante este proceso, los cuales contribuyeron significativamente al desarrollo y culminación de nuestro trabajo de grado.

Atentamente,

JEISON GABRIEL BOTINA
Estudiante – Ingeniería de Sistemas
Universidad CESMAG

JESÚS ESTEBAN ORBES
Estudiante – Ingenieria de Sistemas
Universidad CESMAG

Recibido

Anexo 54. Carta de agradecimiento al Ing. Camilo Gómez Arteaga.

Fecha de Entrega	Dia: 21	Mes: octubre	Año:2026

DATOS PRINCIPALES DEL DOCUMENTO
Título del Trabajo de Grado / Tesis: **SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA LA RED DE DATOS DE IFACTORY, BASADO EN LA NORMA ISO/IEC 27001**
Facultad y Programa Académico: **Facultad de Ingeniería, Ingeniería de Sistemas**
Elija el tipo de documento: **Trabajo de Grado (Pregrado, Tecnología)**

INFORMACIÓN DE AUTORIA	
Autor ①	
Nombres y apellidos: Jeison Gabriel Botina Diaz	**Documento de identidad:** 1004489635
Correo electrónico: jgbotina.9635@unicesmag.edu.co	**Número de contacto:** 3188729002
Firma: 	
Autor ②	
Nombres y apellidos del autor: Jesus Esteban Orbes Zambrano	**Documento de identidad:** 1004190536
Correo electrónico: jeorbes.0536@unicesmag.edu.co	**Número de contacto:** 3187409928
Firma: 	
Autor ③	
Nombres y apellidos del autor:	**Documento de identidad:**
Correo electrónico: @	**Número de contacto:**
Se permite firma digital escaneada (borre esta nota) **Firma: _____**	

Autor ④	
Nombres y apellidos del autor:	**Documento de identidad:**
Correo electrónico: @	**Número de contacto:**
Se permite firma digital escaneada (borre esta nota) **Firma: _____**	

Autorización de publicación. (elija solo uno)	**SÍ** ☒	**NO** ☐

En mi calidad de autor(es) y/o titular (es) del derecho de autor del trabajo de grado / tesis señalada en el encabezado, se confiere a la Universidad CESMAG una licencia no exclusiva, limitada y gratuita, para la inclusión del trabajo de grado / tesis en el repositorio institucional y buscadores de biblioteca. Por consiguiente, el alcance de la licencia que se otorga a través del presente documento abarca las siguientes características:

a) Se otorga desde la fecha de suscripción y durante todo el término en el que los firmantes del presente documento conserven la titularidad de los derechos patrimoniales de autor. En el evento en el que se deje de tener la titularidad de los derechos patrimoniales sobre el trabajo de grado, nos comprometemos a informar de manera inmediata sobre dicha situación a la Universidad CESMAG. Por consiguiente, hasta que no exista comunicación escrita de nuestra parte informando sobre dicha situación, la Universidad CESMAG se encontrará debidamente habilitada para continuar con la publicación del trabajo de grado dentro del repositorio institucional. Conocemos que esta autorización podrá revocarse en cualquier momento, siempre y cuando se eleve la solicitud por escrito para dicho fin ante la Universidad CESMAG. En estos eventos, la Universidad CESMAG cuenta con el plazo de un mes después de recibida la petición, para desmarcar la visualización y difusión del documento en el repositorio institucional.
b) Se autoriza a la Universidad CESMAG para publicar el trabajo de grado en texto completo y en formato digital, teniendo en cuenta que uno de los medios de publicación del repositorio institucional es el internet, se acepta la circulación con alcance mundial, por lo tanto, podrá ser consultado, descargado y compartido.
c) La autorización que se acepta a través del presente documento se realiza a título gratuito, por lo tanto, se renuncia a recibir emolumento alguno por la publicación, distribución, comunicación pública y/o cualquier otro uso que se haga en los términos de la presente autorización y de la licencia o programa a través del cual sea publicado el trabajo de grado.
d) Al aceptar se manifiesta que el trabajo de grado es original realizado sin violar o usurpar derechos de autor de terceros y que se ostenta los derechos patrimoniales de autor sobre la misma. Por consiguiente, se asume toda la responsabilidad sobre su contenido ante la Universidad CESMAG y frente a terceros, manteniéndose indemne de cualquier reclamación que surja en virtud de esta. En todo caso, la Universidad CESMAG se compromete a indicar siempre la autoría del escrito incluyendo nombre los autores y la fecha de publicación.
e) Se autoriza a la Universidad CESMAG para incluir el trabajo de grado en los índices y buscadores que se estimen necesarios para promover su difusión. Así mismo para que pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.
f) En los eventos en los que el trabajo de grado haya sido trabajado con el apoyo o patrocinio de una agencia, organización o cualquier otra entidad diferente a la Universidad CESMAG. Como autor(es)

garantizo(amos) que he(hemos) cumplido con los derechos y obligaciones asumidos con dicha entidad y como consecuencia de ello dejo(dejamos) constancia que la autorización que se concede a través del presente escrito no interfiere ni transgrede derechos de terceros.

Notas: en el caso de no aceptar la publicación, el trabajo de grado podrá ser clasificado, catalogado, codificado y subido al repositorio institucional y buscadores de biblioteca como control de inventario y custodia manteniendo el enlace de visualización oculto; por lo tanto, no contará con el proceso de difusión abierto al usuario.
Si se marco **SI** y en un futuro se desea solicitar el retiro de visualización y difusión del repositorio institucional, todos los autores deberán diligenciar el formato marcando el **NO** se autoriza (se omite firma de asesor)
Si se marcó **NO** y en un futuro se desea solicitar visualización y difusión en el repositorio institucional, todos los autores deberán diligenciar el formato marcando el **SI** se autoriza (se omite firma de asesor)

Espacio exclusivo del Asesor	
Nombres y apellidos del asesor: Luis Arnoby Escobar Hernández	**Documento de identidad:** 98388299 de Pasto
Correo electrónico: laescobar@unicesmag.edu.co	**Número de contacto:** 3154671444
Firma: _____	
En mi calidad de asesor manifiesto que he leído y evaluado el trabajo de grado y de acuerdo con mi conocimiento profesional académico y científico, garantizo que su contenido cumple con las especificaciones de orden académico e investigativo, de confiabilidad de autoridad y de calidad en su presentación de acuerdo con lo establecido por la universidad, por lo tanto, avalo su publicación y difusión en el repositorio institucional de la Universidad CESMAG.	

Autorización de publicación	**SÍ** (x)	**NO** ( )
Observaciones:		