Escuela Superior Politécnica del Litoral

Facultad de Ingeniería en Electricidad y Computación

Análisis de brecha basado en la norma ISO 27001 aplicado a una empresa de vigilancia, alerta y control aéreo.

Proyecto de Titulación

Previo a la obtención del título de:

Magister en Seguridad Informática

Presentado por:

Jairo Wladimir Jhayya Perlaza

Guayaquil - Ecuador
Año: 2026

Agradecimiento

Agradezco a Dios por permitirme lograr un objetivo más en la vida, y a mi tutor M.Sc. Lenin Freire Cobo, con sus conocimientos y apoyo, me guió en cada etapa de este trabajo de titulación. Él me ayudó a alcanzar los resultados que buscaba. También quiero agradecer a la Escuela Superior Politécnica del Litoral por brindarme todos los recursos y herramientas necesarios para llevar a cabo la investigación. Quiero agradecer a toda mi familia y compañeros por apoyarme incluso cuando mis ánimos decaían. En especial, agradezco a mis padres, que siempre estuvieron ahí para darme palabras de aliento y un abrazo reconfortante para renovar energías.

Ing. Jairo Wladimir Jhayya Perlaza

Dedicatoria

Dedico este trabajo de titulación a Dios, a mis padres e hijos. A Dios, porque ha guiado mis pasos, me ha enseñado que con fe y sacrificio se puede lograr cualquier objetivo propuesto. Mis padres, con su amor y apoyo incondicional, nunca dejaron de creer en mí. Faltarían palabras de consideración y estima para expresar el cariño de estos seres tan maravillosos. A mis hermanos, que siempre están cuando los necesito. A mi compañera de vida, EHMM, que invariablemente estuvo en los momentos más arduos.

Ing. Jairo Wladimir Jhayya Perlaza

Declaración expresa

Yo Jairo Wladimir Jhayya Perlaza acuerdo y reconozco que:

La titularidad de los derechos patrimoniales de autor del proyecto de graduación corresponderá al autor o autores, sin perjuicio de lo cual la ESPOL recibe en este acto una licencia gratuita de plazo indefinido para el uso no comercial y comercial de la obra con facultad de sublicenciar, incluyendo la autorización para su divulgación, así como para la creación y uso de obras derivadas. En el caso de usos comerciales se respetará el porcentaje de participación en beneficios que corresponda a favor del autor o autores.

La titularidad total y exclusiva sobre los derechos patrimoniales de patente de invención, modelo de utilidad, diseño industrial, secreto industrial, software o información no divulgada que corresponda o pueda corresponder respecto de cualquier investigación, desarrollo tecnológico o invención realizada por mí durante el desarrollo del proyecto de graduación, pertenecerán de forma total, exclusiva e indivisible a la ESPOL, sin perjuicio del porcentaje que me corresponda de los beneficios económicos que la ESPOL reciba por la explotación de mi innovación, de ser el caso.

En los casos donde la Oficina de Transferencia de Resultados de Investigación (OTRI) de la ESPOL comunique al autor que existe una innovación potencialmente patentable sobre los resultados del proyecto de graduación, no se realizará publicación o divulgación alguna, sin la autorización expresa y previa de la ESPOL.

Guayaquil, 19 de enero de 2026.

Firmado electrónicamente por:
JAIRO WLADIMIR
JHAYYA PERLAZA
Validar únicamente con FirmaEC

Ing. Jairo Wladimir Jhayya Perlaza

Evaluadores

Firmado electrónicamente por:
LENIN EDUARDO FREIRE COBO
Validar únicamente con FirmaEC

MSc. Lenin Eduardo Freire Cobo
Tutor

Firmado electrónicamente por:
JUAN CARLOS GARCIA PLUA
Validar únicamente con FirmaEC

MSc. Juan Carlos García Plúa
Revisor

Resumen

Este documento analiza la brecha según la norma ISO-27001 en una empresa de vigilancia, alerta y control aéreo. Este trabajo de titulación tiene como objetivo diseñar un plan actualizado para implementar la norma ISO-27001 en la empresa de vigilancia, alerta y control aéreo.

La empresa Vigalco, que forma parte de este estudio, realiza la vigilancia, alerta y control del espacio aéreo en el Ecuador. Para poder cumplir con la misión encomendada, la parte operativa se apoya en tres componentes críticos: comunicaciones, mando y control, y vigilancia aérea.

Este trabajo se enfoca en el componente crítico de comunicaciones porque la alta gerencia de Vigalco está preocupada por mantener segura toda la información generada, ya que constantemente adquieren más activos de información.

La solución propuesta será diseñar un plan de implementación construido a partir de las brechas existentes. Esto permitirá determinar el cumplimiento de los requisitos y controles de la norma ISO-27001, y satisfacer el diseño propuesto. Se utilizará como punto de referencia un modelo de evaluación con las medidas implantadas en la empresa.

Palabras clave: ISO/IEC 27001, modelo de evaluación, amenazas, controles ISO 27001

Abstract

This document analyzes the gap assessment based on the ISO/IEC 27001 standard in an air surveillance, alert, and control company. This degree project aims to design an updated plan to implement the ISO-27001 standard in the air surveillance, alert, and control company.

The company Vigalco, which is the subject of this study, carries out the surveillance, alert, and control of Ecuadorian airspace. To fulfill its assigned mission, its operations rely on three critical components: communications, command and control, and aerial surveillance.

This work focuses on the critical communications component because Vigalco's senior management is concerned with safeguarding all generated information, as the company is constantly acquiring more information assets.

The proposed solution is to design an implementation plan based on the identified gaps. This will allow determining compliance with ISO-27001 requirements and controls, and ensuring alignment with the proposed design. An evaluation model, considering the measures already implemented in the company, will be used as a reference point.

Keywords: *ISO/IEC 27001, evaluation model, ISO 27001 controls.*

Índice general

Resumen ..... **I**

Abstract ..... **II**

Abreviaturas ..... **III**

Índice de figuras ..... **IV**

Índice de tablas ..... **V**

CAPÍTULO 1 ..... **1**

1. Introducción 2

1.1 Descripción del problema 3

1.2 Justificación del Problema 4

1.3 Objetivos 6

1.3.1 Objetivo general 6

1.3.2 Objetivos específicos 6

1.4 Marco teórico 6

CAPÍTULO 2: METODOLOGÍA **13**

2.1 Alcance y supuestos 14

2.2 Identificación y catalogación de activos 14

2.2.1 Objetivo del proceso 15

2.2.2 Metodología empleada 15

2.3 Clasificación de activos 16

2.4 Criterios de valoración y priorización 16

2.5 Valoración de activos 18

2.6 Identificación de activos 18

2.7 Criterios de valoración 19

2.8 Escalas de valoración 19

2.9 Resultados y análisis 20

2.10 Identificación de amenazas/vulnerabilidades 20

2.10.1 Metodología de identificación 21

2.10.11 Identificación de amenazas 22

2.11 Identificación de vulnerabilidades 22

2.11.1 Vulnerabilidades técnicas 23

2.11.2 Vulnerabilidades operativas 23

2.11.3 Vulnerabilidades humanas 23
2.11.4 Vulnerabilidades físicas 23
2.12 Relación entre amenazas, vulnerabilidades y activos 23
2.13 Importancia del proceso para el análisis de brecha 24
2.14 Estimación de impacto y cálculo de riesgo 24
2.14.1 Estimación del impacto 25
2.14.2 Estimación de la probabilidad 25
2.14.3 Cálculo del riesgo 26
2.14.4 Priorización del riesgo y toma de decisiones 27
2.15 Análisis de brecha 27
2.15.1 Enfoque metodológico del análisis de brecha 28
2.15.1 Herramienta de evaluación 28
2.15.2 Criterios de cómputo del nivel de cumplimiento 29
2.16 Resultados del análisis de brecha 31
2.16.1 Controles con brecha alta (nivel 0–1) 31
2.16.2 Controles con brecha media (nivel 2) 31
2.16.3 Controles con brecha baja (nivel 3–4) 32
2.17 Plan de tratamiento 32
2.17.1 Enfoque metodológico 33
2.17.2 Estrategias de tratamiento aplicadas 33
2.17.3 Priorización de medidas 34
2.18 Matriz de tratamiento de riesgos (ejemplo) 35
2.18.1 Seguimiento y revisión 36
2.19 Riesgo residual 36
2.19.1 Enfoque metodológico para la gestión del riesgo residual 37
2.19.2 Categorías de riesgo residual identificadas 37
2.19.3 Criterios de aceptación del riesgo residual 38
2.19.4 Acciones de seguimiento del riesgo residual 39
2.20 Validación experta 39
2.20.1 Selección de expertos 40
2.20.2 Método de validación empleado 41
2.20.3 Regla de aceptación y agregación de resultados 44
2.21 Instrumento utilizado para el levantamiento de activos 44
2.22 Ética y legalidad 48

CAPÍTULO 3: ANÁLISIS DE RIESGO DE LA EMPRESA 49
3.1 Inventario resumido de activos críticos 49
3.2 Mapa de riesgos 50
3.3 Metodología para la elaboración del mapa de riesgos 52
3.4 Valoración de impacto y probabilidad: 52
3.5 Interpretación del mapa de riesgos 53
3.6 Brechas por control 53
3.6.1 Controles organizacionales (A.5) 53
3.6.2 Controles relacionados con el personal (A.6) 54
3.6.3 Controles físicos (A.7) 55
3.6.4 Controles tecnológicos (A.8) 56
3.7 Gestión de sesgos y validación de datos 58
3.7.1 Triangulación de fuentes 58
3.7.2 Validación externa de información 59
3.7.3 Entrevistas a distintos niveles organizacionales 59
4. Análisis de contenido con criterios predefinidos 59
3.8 Amenazas a la validez del estudio 59
3.8.1 Validez interna 60
3.8.2 Validez externa 60
3.8.3 Validez de constructo 61
3.9 Riesgo residual en Vigalco 62
3.9.1 Conceptualización del riesgo residual 62
3.9.2 Evaluación del riesgo residual en Vigalco 63
3.10 Matriz general del riesgo residual 64
3.11 Interpretación de resultados 65
3.13 Cronograma de implementación 70
3.14 Comparación con trabajos previos e implicaciones prácticas 74
3.15 Limitaciones 78
CAPÍTULO 4 49
4.1 Conclusiones y recomendaciones 78
4.1.1 Conclusiones 78
4.1.2 Recomendaciones 79
Referencias Bibliográficas 78

APÉNDICES 83
Apéndice A Dominios y objetivos de control. 83
Apéndice B Amenazas detalladas por tipo. 86
Apéndice C Tipos de activos y amenazas. 88
Apéndice D Identificación de controles existentes. 95
Apéndice E Identificación de las vulnerabilidades. 102
Apéndice F Evaluación de las consecuencias. 113
Apéndice G Evaluación de la probabilidad. 125
Apéndice H Determinación del nivel de riesgo. 136
Apéndice I Gráfico de barras multifacético 147
Apéndice J Integral de activos, brechas, mejoras e indicadores. 148
Apéndice K Consolidada de validación experta del análisis de brecha ISO/IEC 27001 ... 151
Apéndice L Matriz de priorización de controles críticos 152
Apéndice M Diez (10) controles priorizados para comunicaciones 153

Abreviaturas

CM	Centros de mando
CMM	Modelo de madurez de las capacidades.
Emplazamiento	Sitio remoto de vigilancia del espacio aéreo.
FGE	Fiscalía General del Estado.
GES	Gestión: Área o personal técnico encargado de realizar el monitoreo y administración de varios servicios.
ISO	Organización Internacional de Estandarización.
MW	Microondas: Área encargada del mantenimiento de los enlaces y estaciones de microondas.
MyC	Área encargada de mantener operativos varios servidores y aplicaciones para la vigilancia y control aéreo.
NET	Redes: Área encargada del mantenimiento de redes de datos.
RAD	Radiocomunicaciones: Área encargada del mantenimiento de las radiocomunicaciones U/VHF-AM-FM, HF.
RRHH	Departamento de Recursos Humanos.
SAT	Satelital: Área encargada del mantenimiento de los enlaces satelitales.
SEG	Seguridad: Aérea encargada de la seguridad lógica de la empresa.
SGSI	Sistema de gestión de seguridad de la información.
SVR	Equipo servidor: hardware.
Vigalco	Vigilancia, alerta y control.

Índice de figuras

FIGURA 1 RELACIÓN ENTRE TIPO DE ACTIVO, CRITICIDAD Y RIESGOS ASOCIADOS. **17**
FIGURA 2 RIESGO RESIDUAL **66**

Índice de tablas

TABLA 1 ANÁLISIS COMPARATIVO DE CASOS RELEVANTES EN AMÉRICA LATINA. **9**

TABLA 2 EXTRACTO DE LA MATRIZ DE CATALOGACIÓN DE ACTIVOS. **17**

TABLA 3 CUANTIFICACIÓN DE LOS ACTIVOS. **19**

TABLA 4 ANÁLISIS DE ACTIVOS, AMENAZAS, VULNERABILIDADES Y NIVELES DE RIESGO. **26**

TABLA 5 NIVEL DE MADUREZ DE LOS CONTROLES DE SEGURIDAD **28**

TABLA 6 CONTROLES APLICABLES (SOA SIMPLIFICADA) **30**

TABLA 7 IDENTIFICACIÓN DE RIESGOS POR ACTIVO Y CONTROLES ISO RECOMENDADOS. **35**

TABLA 8 NIVELES DE RIESGO Y SU CORRESPONDIENTE DESCRIPCIÓN. **50**

TABLA 9 RIESGOS ASOCIADOS A ACTIVOS CRÍTICOS. **51**

TABLA 10 RIESGOS IDENTIFICADOS EN ACTIVOS CRÍTICOS. **52**

TABLA 11 PORCENTAJE DE CUMPLIMIENTO DE CONTROLES ISO/IEC 27001. **57**

TABLA 12 RESULTADOS DE LOS INDICADORES DE CUMPLIMIENTO ISO/IEC 27001 EN VIGALCO. **57**

TABLA 13 CLASIFICACIÓN DEL NIVEL DE RIESGOS RESIDUAL. **64**

TABLA 14 MATRIZ DE PRIORIZACIÓN DE CONTROLES CRÍTICOS **68**

TABLA 15 TOP 10 CONTROLES PRIORIZADOS PARA COMUNICACIONES **69**

TABLA 16 PLAN DE MEJORAS Y SEGUIMIENTOS DE CONTROLES ISO/IEC 27001. **70**

TABLA 17 PLAN DE ACCIÓN DERIVADO DEL ANÁLISIS DE BRECHA **71**

TABLA 18 MATRIZ DE BRECHAS, MEJORAS Y RESULTADOS. **72**

TABLA 19 TABLA INTEGRADA DE CUMPLIMIENTO DE CONTROLES Y EXPOSICIÓN AL RIESGO **74**

TABLA 20 INDICADORES UTILIZADOS EN LA EVALUACIÓN PILOTO **77**

CAPÍTULO 1

1. Introducción

La tecnología avanza tan rápido que las personas naturales o jurídicas adquieren diariamente cualquier tipo de información. Independientemente de la información obtenida, al final se convertirá en un activo de suma importancia para las partes mencionadas.

En ese contexto, existen un sinnúmero de organizaciones que, ya sea por falta de conocimiento, presupuesto u otras razones, no aplican los principios de disponibilidad, confidencialidad e integridad de la información. Esto las hace vulnerables a cualquier tipo de incidentes y tardan mucho tiempo en la recuperación o continuidad del negocio.

La empresa Vigalco presta servicios de vigilancia, alerta y control del espacio aéreo en Ecuador. Internamente, ha implementado procedimientos y controles para mantener la seguridad de la información. Los directivos, incluida la gerencia, necesitan saber si estos procedimientos y controles cumplen con la norma ISO/IEC 27001, una de las más extendidas en seguridad de la información. Varias organizaciones la utilizan como base para sus operaciones de seguridad de la información; además, es necesaria para certificar un Sistema de Gestión de la Seguridad de la Información (SGSI) *[1]*.

A pesar de que la empresa cuenta con alta disponibilidad en sus redes de comunicaciones, en ocasiones se producen puntos de fallo. Esto ocasiona malestar en los componentes de mando, control y vigilancia aérea. Además, se aplican procedimientos que no son estándar y, por ende, impiden una mejora continua.

Uno de los recursos más preciados de la empresa Vigalco es la información. Para mantener disponible este recurso, desde el año 2016, la empresa cuenta con dos manuales como propuesta: el manual de SGSI (Sistema de Gestión de la Seguridad de la Información) y el manual de análisis de riesgo. El objetivo es poder certificarse en el futuro con la norma o estándar UNE-ISO/IEC-27001. Cabe indicar que los manuales no los realizó con una entidad certificadora acreditada, sino que lo hizo de forma interna *[2]*.

Por ello, este trabajo se enfoca en diseñar un plan actualizado para implementar la norma ISO/IEC 27001 en la empresa de vigilancia, alerta y control aéreo.

Esta tesis está dividida en cuatro capítulos; cada uno de ellos contribuye a una respuesta integral a las interrogantes de investigación. El capítulo uno realiza una introducción al problema de estudio, las metas propuestas y el marco general en que se desarrollará el estudio. El capítulo dos ofrece una revisión teórica sobre la norma ISO/IEC 27001, el análisis de brecha, el análisis de riesgo y la metodología MAGERIT v3. El capítulo tres realiza una revisión del estado actual de la empresa, la determinación de las amenazas, los niveles de vulnerabilidades y riesgos.

El capítulo cuatro presenta un diseño para evaluar el estado de la empresa en seguridad de la información. También determina qué proyectos son necesarios para cerrar la brecha.

Para validar el diseño propuesto, se toman en cuenta los criterios de validación obtenidos previamente. Estos criterios se plasman en una prueba de concepto que evidencia la utilidad de implementar esta metodología en ambientes reales. Este trabajo resume los criterios básicos que una consultoría estratégica debe tener en cuenta para las entidades aéreas que quieren usar un método para evaluar los riesgos en la seguridad de la información. También incluye propuestas para futuras investigaciones y aplicaciones.

1.1 Descripción del problema

La empresa Vigalco forma parte de este estudio y pertenece al sector de servicios. Su actividad se centra en vigilar, alertar y controlar el espacio aéreo. Para cumplir con sus objetivos institucionales, cuenta con 6 instalaciones físicas y alrededor de 700 empleados.

La empresa Vigalco, para mantener el servicio de vigilancia, alerta y control del espacio aéreo, realiza sus procesos con base en 3 componentes:

a. Componente Comunicaciones.

b. Componente mando y control.

c. Componente de vigilancia aérea.

Los 3 componentes son sumamente críticos; sin embargo, el componente comunicaciones es el que tiene mayor criticidad y se lo considera como principal. La parte operativa de la empresa depende del mencionado componente.

Las afectaciones por delitos o ataques informáticos, según el Foro Económico Mundial, en el primer semestre del 2021, las pérdidas económicas ascienden a US$6 billones de dólares *[3]*. Según la fiscalía general del Estado, desde el año 2017 al 2021, en el Ecuador se han registrado más de 463 denuncias por ataques dirigidos contra la estabilidad y correcto funcionamiento de sistemas informáticos *[4]*. Como parte de su política de seguridad, y con la finalidad de mantener la disponibilidad, confidencialidad e integridad de la información, la empresa prohíbe que los componentes críticos tengan acceso al servicio de internet.

En su debido momento se llevó a cabo un estudio sobre la seguridad de la información. Sin embargo, la alta gerencia está preocupada por mantener segura toda la información que genera, su equipamiento y establecer un proceso de mejora continua. Por lo tanto, necesita conocer cómo se encuentra actualmente la empresa en el tema de seguridad de la información.

1.2 Justificación del Problema

El problema científico que se revela es: ¿Cuál es la brecha existente entre la situación actual de la empresa Vigalco y los requisitos de la norma ISO/IEC 27001, evaluada mediante indicadores medibles de cumplimiento de controles, madurez del SGSI y nivel de riesgo de los activos de información?

Entre las causas que contribuyeron a este problema se encuentran, por ejemplo, la determinación del porcentaje de cumplimiento de los controles ISO/IEC 27001, la cuantificación del número y tipo de brechas existentes en los dominios organizacional,

humano, físico y tecnológico. Identificar el número de activos de información en riesgo alto y su posible reducción mediante un plan de mejora y evaluar el nivel de madurez del SGSI en una escala estandarizada (1–5).

Es fundamental indicar que este problema es relevante debido a la importancia estratégica de la información y a la necesidad de protegerla adecuadamente. Esto garantiza la seguridad y efectividad de las operaciones de la empresa.

Vigalco es una empresa estratégica en Ecuador, encargada de gestionar y supervisar el espacio aéreo nacional. Garantiza su seguridad mediante sistemas de vigilancia, detección de amenazas y coordinación. Por tanto, debe seguir regulaciones nacionales e internacionales para la protección de datos de navegación aérea, como la norma ISO/IEC 27001 para sistemas de seguridad de la información.

La alta disponibilidad en las redes de comunicaciones de Vigalco es fundamental para garantizar la vigilancia aérea continua, el mando y control (C2) y la seguridad nacional. Sin embargo, puntos de fallo recurrentes y procedimientos no estandarizados generan problemas operativos que afectan la eficacia del sistema.

En resumen, la falta de herramientas sencillas de usar para identificar riesgos ha puesto de relieve la necesidad urgente de verificar si se están cumpliendo los requisitos y controles de la norma ISO/IEC 27001. Además, es necesario cumplir con el diseño propuesto para usarlo como punto de referencia en un modelo de evaluación con las medidas implantadas en la empresa. Dado el carácter crítico de la organización y las restricciones de acceso a ciertos entornos operativos, el alcance del análisis se centró en los activos y procesos más relevantes para la vigilancia, alerta y control aéreo, lo cual se reconoce como una limitación metodológica que podrá ser abordada en trabajos futuros con un inventario aún más exhaustivo.

1.3 Objetivos

1.3.1 *Objetivo general*

- Diseñar un plan de implementación actualizado de la norma ISO/IEC 27001 en la empresa de vigilancia, alerta y control aéreo, a partir del análisis de la brecha existente entre la situación actual de su SGSI y los requisitos de dicha norma.

1.3.2 *Objetivos específicos*

- Determinar el nivel de aplicación de las cláusulas y controles de seguridad establecidos en la norma ISO/27001 en una institución de vigilancia, alerta y control aéreo, mediante la elaboración de una Matriz de Cumplimiento que permita identificar el estado de implementación de cada requisito.
- Identificar las deficiencias de seguridad de la información y la distancia existente respecto al cumplimiento de los requisitos y controles de la norma ISO/27001, mediante la elaboración de una matriz de brechas que permita evidenciar los controles parciales o no implementados.
- Proponer un plan de mejora que permita cerrar las brechas identificadas y fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001, mediante la elaboración de una Matriz de Plan de Mejoras que priorice acciones en función de los requisitos y riesgos específicos de la institución de vigilancia, alerta y control aéreo.

1.4 Marco teórico

En el ámbito de la seguridad de la información, gran parte de la literatura coincide en que la protección de los activos más sensibles de una organización gira en torno a tres ejes: confidencialidad, integridad y disponibilidad, conocidos de forma clásica como la tríada CID *[5]*. Estos conceptos, lejos de ser estáticos, constituyen los objetivos primarios de cualquier

sistema de gestión de seguridad de la información (SGSI), según marcos normativos internacionales como la familia de normas ISO/IEC 27000 (ISO, 2022).

De acuerdo con la publicación especial 800-53 del Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST), la confidencialidad se refiere a garantizar que la información no quede expuesta ni sea accesible para personas, entidades o procesos que no cuenten con la autorización correspondiente *[6]*. Otros Autores enfatizan que este principio no solo aplica a datos digitales, sino a cualquier tipo de información sensible, como planes operativos, detalles de contratos o datos personales, cuyo acceso debe restringirse mediante mecanismos de control como cifrado, políticas de acceso y acuerdos de confidencialidad *[7]*.

La integridad, por su parte, se refiere a "la propiedad de salvaguardar la exactitud y completitud de los activos de información" (ISO/IEC 27000:2022). La literatura advierte que la violación de este principio, ya sea por error no intencional o por actos maliciosos, puede tener consecuencias catastróficas en entornos críticos *[8]*. En su análisis de seguridad en infraestructuras críticas, sostienen que garantizar la integridad implica proteger la información contra modificaciones no autorizadas, asegurando su fiabilidad y confiabilidad a lo largo de todo su ciclo de vida.

Finalmente, la disponibilidad asegura que "los activos de información sean accesibles y utilizables por las entidades o procesos autorizados cuando estos lo requieran". Este es un principio cardinal en operaciones de misión crítica, como los servicios aéreos. Los sistemas que toleran fallos están directamente relacionados con la disponibilidad y la continuidad del negocio. Esto significa que necesitan ser resistentes, tener planes para recuperarse de desastres y tomar medidas anticipadas para evitar amenazas que puedan causar interrupciones [9].

Autores y normativas internacionales coinciden en que su implementación es decisiva para organizaciones con activos sensibles y operaciones críticas. Estudios aplicados al sector

transporte y defensa destacan cómo amenazas contemporáneas (ciberataques, fallos sistémicos) atacan directamente estos principios.

Dentro del panorama actual de la ciberseguridad, la gestión de riesgos se erige como el proceso central para la protección de activos de información. Entre los marcos metodológicos más reconocidos a nivel internacional se encuentran la norma ISO/IEC 27005 y la guía NIST Special Publication (SP) 800-30. El primero, ISO/IEC 27005, da pautas generales para llevar a cabo un proceso de gestión de riesgos que esté en línea con lo que se exige en el Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO/IEC 27001. Es ampliamente adoptado por organizaciones que operan en mercados globales o que requieren demostrar cumplimiento regulatorio ante clientes y socios internacionales, gracias a su reconocimiento universal.

En contraste, el marco NIST SP 800-30, desarrollado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, presenta un proceso más detallado y prescriptivo, especialmente diseñado para alinearse con el Cybersecurity Framework (CSF) del NIST. Destaca por ofrecer un catálogo extenso y práctico de amenazas, vulnerabilidades, impactos y probabilidades, junto con matrices de riesgo cuantitativas y cualitativas predefinidas.

En los últimos años, la implementación de sistemas de gestión de seguridad de la información (SGSI) basados en ISO/IEC 27001 se ha convertido en una práctica recurrente en organizaciones de distintos sectores en América Latina. Esto se debe al creciente reconocimiento de los riesgos cibernéticos y la necesidad de proteger activos críticos.

No obstante, varios estudios señalan que muchas de estas organizaciones presentan brechas significativas en su cumplimiento normativo, lo que evidencia una "distancia" entre la situación real y los requisitos de la norma —resaltando la relevancia metodológica de un análisis de brecha (gap-analysis) como herramienta de diagnóstico.

Un ejemplo práctico se describe en un estudio realizado en una empresa privada peruana, donde se combinó el estándar ISO/IEC 27001 con la metodología MAGERIT para gestionar los riesgos sobre sus activos de información. En ese trabajo se emplearon encuestas, entrevistas y observación directa para detectar vulnerabilidades, y los resultados muestran que, después de aplicar las mejoras propuestas, el personal aumentó de forma significativa su comprensión sobre temas de seguridad, pasando de no registrar ningún nivel de conocimiento a alcanzar un 25% en la evaluación de control interno *[10]*.

Más allá de casos individuales, existen estudios con una visión panorámica de la región. Por ejemplo, la investigación La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas destaca que a nivel gubernamental y corporativo la región enfrenta un rezago significativo en capacidades de defensa, infraestructura, inversión en seguridad y adopción de buenas prácticas. Ese rezago se traduce en una vulnerabilidad incrementada frente a amenazas globales. *[11]*

Los estudios demuestran que, si bien hay conciencia sobre la seguridad de la información, la implementación práctica de controles normados suele ser parcial y desorganizada. Estudios de gap-analysis servidos por metodologías formales (como en los ejemplos mencionados) ofrecen una radiografía clara del estado real de cumplimiento, permitiendo elaborar planes de mejora bien fundamentados.

Tabla 1

Análisis comparativo de casos relevantes en América Latina.

Caso/Estudio	Alcance	Valoración de brechas	Herramientas/metodología
UPTC, Colombia	Sede seccional, cumplimiento ISO/IEC 27001	⚠ Parcial: infraestructura y controles con brechas críticas.	Matriz de cumplimiento ISO/IEC 27001, auditoría documental, entrevistas TI
Empresa Comercial, Perú	Sistema de ventas y procesos TI	⚠ Parcial: vulnerabilidades técnicas y humanas	Auditoría de seguridad, plan de mitigación ISO/IEC 27001, registro de incidentes
Institución educativa, México	SGSI completo (personal y	⚠ Parcial: capacitación y	Encuestas, entrevistas, revisión documental, matriz de riesgos.

	procesos administrativos)	gobernanza insuficientes	
Estudio regional LATAM	Departamentos de TI en múltiples sectores	⚠ Parcial / ❌ Deficiente: adopción de normas y madurez baja.	Cuestionarios, análisis comparativo de políticas y controles, reportes de cumplimiento ISO/IEC 27001.
Caso Vigalco	Sistema de vigilancia, alerta y control aéreo	⚠ Parcial: activos críticos identificados, riesgos operativos detectados.	Matriz de brechas ISO/IEC 27001, análisis de riesgos MAGERIT e ISO 27005, entrevistas con personal operativo.

Fuente: Elaborado por el autor.

✅ Cumplido / implementado

⚠ Parcial / en proceso de implementación.

❌ No implementado / crítico

La Tabla 1 muestra un análisis comparativo de varios casos de implementación de seguridad de la información en América Latina, indicando su alcance, nivel de brechas y métodos usados para evaluarlas. Resume cómo distintas organizaciones aplican (parcialmente o deficientemente) normas como ISO-27001 y qué herramientas emplean para identificar riesgos y controles.

Se medirán como variables de interés el aseguramiento de la calidad y los controles de seguridad, tal como los define la norma. En este trabajo, el aseguramiento de la información abarca todos los activos que la organización ha identificado como relevantes. Los controles de seguridad sobre esos activos se evaluarán utilizando un modelo de madurez de capacidades, de manera que sea posible medir su nivel de riesgo y ver cómo evolucionan en el tiempo.

En coherencia con el problema científico planteado, se determina la brecha existente entre la situación actual de Vigalco y los requisitos de la norma ISO/27001 en materia de seguridad de la información. Se formulan las siguientes **preguntas de investigación**, que permitirán evaluar de manera objetiva el grado de cumplimiento y madurez del Sistema de Gestión de Seguridad de la Información (SGSI):

1. ¿Cuál es el nivel de cumplimiento de los controles establecidos en el Anexo A de la norma ISO/27001 en la empresa Vigalco?

Indicadores (KPI):

KPI 1: Porcentaje de controles implementados:

(Controles implementados/Total de controles evaluados) × 100 (Controles implementados / Total de controles evaluados) × 100 (Controles implementados/Total de controles evaluados) × 100

KPI 2: Porcentaje de controles parcialmente implementados:

(Controles parcialmente implementados/Total) × 100 (Controles parcialmente implementados/Total) × 100 (Controles parcialmente implementados/Total) × 100

KPI 3: Porcentaje de controles no implementados (brecha):

(Controles no implementados/Total) × 100 (Controles no implementados/Total) × 100 (Controles no implementados/Total) × 100

2. ¿Qué brechas existen entre la situación actual del SGSI de Vigalco y los requisitos de la ISO/27001 en los dominios organizacional, físico y tecnológico?

Criterio de éxito asociado:

Determinar de manera estructurada todas las brechas por dominio, clasificadas como implementado, parcialmente implementado o no implementado.

Indicadores (KPI/KMI):

KPI 4 – Número total de brechas identificadas por dominio.

KPI 5 – Porcentaje de controles críticos con brechas.

KPI 6 – Clasificación de brechas por impacto operativo o de seguridad.

3. ¿ Qué nivel de riesgo presentan los activos de información más críticos de Vigalco, considerando el grado de cumplimiento actual de la norma ISO-27001?

Criterio de éxito asociado:

Evaluar el riesgo actual de todos los activos críticos mediante una metodología estandarizada, diferenciando riesgos inherentes y residuales.

Indicadores (KRI):

KRI 1 – Número de activos en riesgo alto.

KRI 2 – Nivel promedio de riesgo por dominio o categoría de activo.

4. ¿Qué nivel de madurez presenta el Sistema de Gestión de Seguridad de la Información (SGSI) de Vigalco en relación con las buenas prácticas establecidas por ISO/IEC 27001?

Criterio de éxito asociado:

Calcular el nivel de madurez de cada dominio del SGSI utilizando una escala estructurada (por ejemplo, 1 a 5), determinando tanto el nivel actual como la brecha respecto al nivel deseado.

Indicadores (KPI):

KPI 7 – Nivel de madurez promedio del SGSI.

KPI 8 – Brecha de madurez por dominio.

5. ¿En qué medida el cierre de brechas identificado puede contribuir a la reducción del riesgo y al fortalecimiento de la seguridad de la información en Vigalco?

Criterio de éxito asociado:

Proponer un plan de mejora que demuestre, de manera estimada o proyectada, una reducción del riesgo residual mediante el fortalecimiento de controles.

Indicadores (KRI/KPI):

KRI 4 – Reducción porcentual del riesgo estimada:

CAPÍTULO 2: METODOLOGÍA

En este capítulo se presentarán los fundamentos conceptuales que establecen el marco general de referencias para el estudio sobre el análisis de Brecha basado en la ISO-27001 en la empresa Vigalco. Se estudian los requisitos, controles, sistema de gestión de la seguridad de la información, análisis de riesgo, análisis de brecha.

2.1 Alcance y supuestos

El presente estudio se centró en la evaluación del nivel de aplicación de los controles de seguridad de la información establecidos en la norma ISO-27001 en la empresa Vigalco, dedicada a vigilancia, alerta y control aéreo. Se delimitó el análisis a los procesos y activos de información considerados críticos para la operación de la institución, así como al personal responsable de la gestión y supervisión de dichos sistemas.

El estudio incluyó la elaboración de la Matriz de Cumplimiento para determinar el estado de implementación de cada requisito, la construcción de la Matriz de Brechas para identificar deficiencias y la propuesta de un Plan de Mejoras priorizado según criticidad y riesgo.

En tanto que se asumió que la información que proporcionó el personal, así como la documentación institucional, fue veraz, completa y representativa de las operaciones de la organización durante el período de estudio.

2.2 Identificación y catalogación de activos

La identificación y catalogación de activos constituye un componente fundamental dentro del Sistema de Gestión de Seguridad de la Información (SGSI). Esto se debe a que permite establecer un inventario organizado de todos los recursos críticos de la organización, garantizando su protección conforme a los estándares de la norma ISO/IEC 27001.

En el presente estudio, este proceso se desarrolló en la empresa Vigalco, dedicada a vigilancia, alerta y control aéreo, con el objetivo de determinar cuáles activos requerían medidas de seguridad prioritarias y cómo estos se relacionaban con los riesgos identificados.

2.2.1 Objetivo del proceso

El objetivo principal de identificar y catalogar activos fue crear un inventario detallado de los recursos físicos, lógicos, humanos e informacionales que son importantes para el funcionamiento de la institución. También se establecieron criterios de importancia y valor para la seguridad de la información. Esta actividad permitió no solo reconocer los activos existentes, sino también comprender su importancia relativa dentro del flujo de información y los procesos operativos de vigilancia y control aéreo.

2.2.2 Metodología empleada

Para la identificación de activos se realizó una revisión exhaustiva de la documentación institucional, incluyendo organigramas, procedimientos internos, inventarios existentes y políticas de seguridad. Paralelamente, se llevaron a cabo entrevistas estructuradas con el personal clave responsable de la gestión de sistemas críticos, bases de datos operativas y plataformas de comunicación.

Cada activo identificado fue registrado en una **matriz de catalogación**, que incluyó los siguientes elementos:

- Nombre del activo
- Tipo de activo (hardware, software, información, recurso humano)
- Ubicación o dependencia operativa
- Responsable del activo
- Nivel de criticidad
- Riesgos asociados

La criticidad de cada activo se evaluó considerando su impacto en la confidencialidad, integridad y disponibilidad de la información, así como su relevancia para la continuidad operativa y la seguridad de las operaciones aéreas.

2.3 Clasificación de activos

Los activos se clasificaron en cuatro categorías principales:

- **Activos físicos:** Incluyeron servidores, estaciones de trabajo, dispositivos de comunicación, equipos de vigilancia y respaldo de información. Se consideró su ubicación, estado de conservación y protección física como factores determinantes de su criticidad.
- **Activos lógicos:** Comprendieron sistemas operativos, bases de datos, aplicaciones críticas, software de monitoreo y herramientas de control aéreo. Su relevancia se relacionó de forma directa con la capacidad de mantener operativos los procesos organizacionales y con la salvaguarda de los datos sensibles.
- **Activos informacionales:** Se incluyeron registros de vuelos, planes de operación, reportes de incidentes y documentación estratégica. Se evaluó su valor legal, operativo y estratégico para la empresa.

2.4 Criterios de valoración y priorización

La catalogación incluyó un análisis de riesgos preliminar, permitiendo asignar niveles de prioridad a los activos según su criticidad y vulnerabilidad. Se establecieron tres niveles de prioridad: alto, medio y bajo, basados en:

- Impacto potencial de la pérdida, alteración o divulgación de la información
- Frecuencia de uso y dependencia operativa
- Sensibilidad de la información contenida o procesada
- Exposición a amenazas internas y externas

Esta priorización facilitó la posterior elaboración de matrices de cumplimiento y de brechas, asegurando que los esfuerzos de seguridad se enfocaran en los activos más críticos.

La **Tabla 2** y la **Figura 1** presentan ejemplos representativos de los activos catalogados, mostrando su tipo, criticidad y riesgos asociados. Este inventario sirvió como

base para la evaluación de controles, el análisis de brechas y la planificación de mejoras, garantizando que los controles implementados guardaran correspondencia con la importancia de los activos involucrados y con los riesgos propios de la operación de vigilancia y control aéreo.

Tabla 2

Extracto de la matriz de catalogación de activos.

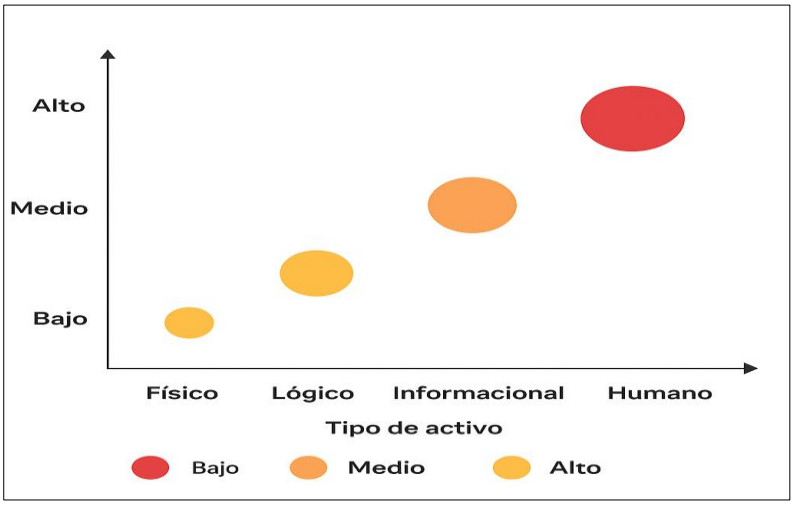
Activo	Tipo	Responsable	Criticidad	Riesgo asociado	Nivel de prioridad
Servidor de monitoreo aéreo	Físico	Jefe de TI	Alto	Interrupción de operaciones	Alto
Base de datos de vuelos	Lógico.	Administrador de BD	Alto	Perdida de información sensible	Alto
Planes operativos	Informacional	Coordinador operativo	Medio	Información desactualizada	Medio
Personal de control	Humano	Supervisor de control	Alto	Error humano	Alto
Estaciones de trabajo	Físico	Encargado de TI	Medio	Acceso no autorizado	Medio
Software de monitoreo	Lógico.	Administrador de sistemas	Alto	Fallos del sistema	Alto

Fuente: Elaboración propia del autor.

La tabla 2 muestra un extracto de la matriz de catalogación de activos del sistema, indicando para cada activo su tipo, responsable, criticidad, riesgo asociado y nivel de prioridad.

Figura 1

Relación entre tipo de activo, criticidad y riesgos asociados.



Fuente: Realizada por el autor.

La figura 1 representa la relación entre el tipo de activo y el nivel de criticidad/riesgo asociado. El eje horizontal muestra los tipos de activos: físico, lógico, informacional y humano. El eje vertical indica el nivel de criticidad o riesgo: bajo, medio y alto. Se observa una tendencia ascendente donde el activo humano aparece con el mayor tamaño y en nivel alto, indicando que concentra el riesgo/criticidad más elevada frente a los demás tipos.

2.5 Valoración de activos

La valoración de activos constituyó una etapa fundamental dentro del análisis de brecha de seguridad de la información en Vigalco. Este proceso permitió identificar, clasificar y priorizar los activos críticos para la operación de la empresa, considerando tanto los recursos físicos como los digitales, la información, el personal y los procedimientos operativos. La evaluación ayudó a definir criterios claros para identificar la importancia de cada activo y luego asignar controles de seguridad según la norma ISO/IEC 27001.

2.6 Identificación de activos

Se inició con la identificación exhaustiva de los activos que soportaban los procesos de vigilancia y control aéreo. Para ello, se elaboró un inventario que incluyó:

- **Activos de información:** bases de datos de vuelos, reportes de operadores, registros de seguridad y manuales de procedimientos.
- **Activos físicos:** estaciones de control aéreo, antenas de comunicación, servidores, equipos de cómputo y sistemas de respaldo energético.
- **Activos humanos**: personal operativo, ingenieros de sistemas, analistas de seguridad y personal administrativo vinculado a la gestión de información.

Cada activo fue registrado indicando su ubicación, responsable y función dentro del sistema de vigilancia y control aéreo, lo que permitió contar con una base sólida para evaluar su valor y determinar el impacto que tendría su pérdida, daño o divulgación no autorizada.

2.7 Criterios de valoración

Para determinar la criticidad de los activos, se establecieron criterios basados en los principios de confidencialidad, integridad y disponibilidad de la información, adaptados al contexto operativo de Vigalco. Los criterios fueron los siguientes:

- **Confidencialidad:** Se evaluó la sensibilidad de la información contenida en el activo y el daño que su divulgación no autorizada podría generar. Activos como la información de vuelos o procedimientos de seguridad recibieron puntajes altos en este criterio.
- **Integridad:** Se consideró la necesidad de mantener la exactitud y confiabilidad de los activos. Se evaluaron los efectos que tendría la alteración no autorizada de datos críticos, como los registros de control aéreo o los planes operativos.
- **Disponibilidad:** Se valoró la importancia de que el activo estuviera accesible cuando fuese requerido. Sistemas de monitoreo, comunicaciones y herramientas operativas en tiempo real fueron considerados críticos.

En cuanto al valor económico/funcional, se analizó el impacto financiero y operativo que ocasionaría la pérdida o indisponibilidad del activo, considerando costos de reemplazo y repercusiones en la continuidad operativa.

2.8 Escalas de valoración

Se implementó una escala ordinal para cuantificar la criticidad de los activos según cada criterio, utilizando un rango de 1 a 5, donde:

Tabla 3
Cuantificación de los activos.

Nivel	Descripción	Impacto esperado
1	Muy bajo.	Pérdida mínima de operación o seguridad
2	Bajo	Impacto limitado, requiere acciones menores.
3	Medio	Afecta parcialmente las operaciones; requiere medidas correctivas.

4	Alto	Provoca impactos significativos.
5	Muy alto.	Consecuencias graves para la seguridad, continuidad o reputación de la empresa.

Fuente: Elaboración hecha por el autor.

La tabla 3 explica, con una escala del 1 al 5, qué tan grave sería el impacto si un activo falla o se ve comprometido. Con esta escala se puede decidir a cuáles activos dar más atención, recursos y controles de seguridad, priorizando los niveles 4 y 5.

A partir de lo expuesto anteriormente, se pudo asumir que cada activo fue evaluado según los cuatro criterios mencionados, asignando un puntaje que permitió calcular un valor global de criticidad mediante la suma ponderada de cada criterio. Posteriormente, se clasificaron en categorías de riesgo bajo, medio y alto, permitiendo la priorización de controles y recursos de seguridad.

2.9 Resultados y análisis

La valoración de activos permitió evidenciar que los recursos vinculados con la información de vuelos y la comunicación en tiempo real eran los más críticos para la operación de Vigalco, presentando puntajes máximos en todos los criterios evaluados. Por otro lado, activos administrativos y documentos internos mostraron un nivel de criticidad medio, lo que implicó asignarles controles menos estrictos, aunque no nulos.

Referente a la utilización de criterios y escalas, permitió mantener consistencia y trazabilidad en el proceso de valoración, facilitando la toma de decisiones para la gestión de riesgos y la priorización de inversiones en seguridad de la información. Además, la clasificación objetiva de los activos sirvió como base para el análisis de brecha posterior.

2.10 Identificación de amenazas/vulnerabilidades

En el estudio, se otorgó un papel central a la identificación sistemática de amenazas y vulnerabilidades, entendida como una fase clave del enfoque metodológico empleado para realizar el análisis de brechas de la empresa Vigalco con referencia a la norma ISO/IEC

27001. Esta etapa hizo posible detectar situaciones de riesgo que podrían comprometer la protección de los activos de información más críticos y evidenciar las debilidades presentes en los procesos, en la infraestructura tecnológica y en los mecanismos de control implementados por la organización. El objetivo principal fue contar con una visión clara del panorama de riesgos al que se encontraba expuesta la empresa, especialmente considerando su rol estratégico en la vigilancia, alerta y control aéreo.

2.10.1 Metodología de identificación

La identificación de amenazas y vulnerabilidades se realizó siguiendo un proceso estructurado que integró técnicas documentales, entrevistas a personal clave y análisis técnico de la infraestructura tecnológica. El procedimiento se basó en las directrices establecidas por ISO/IEC 27001 e ISO 27005, adaptándolas a la realidad operativa de Vigalco.

El proceso se desarrolló en cuatro etapas:

- **Revisión documental:** Se analizaron políticas internas, registros de incidentes, auditorías previas, informes de mantenimiento y manuales de operación para identificar riesgos reportados.
- **Entrevistas y talleres:** se realizaron sesiones con operadores de control aéreo, personal técnico de TI, responsables de seguridad y jefes operativos, con el fin de recopilar información sobre fallos recurrentes, debilidades percibidas y amenazas propias del entorno aeronáutico.
- **Evaluación técnica:** Se revisaron sistemas, dispositivos y redes mediante inspecciones básicas, análisis de configuración y observación del funcionamiento de los controles existentes.
- **Clasificación y validación:** los hallazgos se organizaron en categorías y fueron validados con los responsables correspondientes.

2.10.11 Identificación de amenazas

Las amenazas se definieron como todos aquellos eventos, internos o externos, que podían causar daño a los activos de información o afectar la continuidad de las operaciones. Durante el análisis se identificaron amenazas tecnológicas, humanas, físicas y ambientales. Entre las principales amenazas identificadas se encontraron:

a) Amenazas tecnológicas

- Ataques informáticos dirigidos a la infraestructura crítica (malware, ransomware, intentos de intrusión).
- Interrupciones por fallas de software o errores de configuración.
- Saturación de sistemas de comunicaciones debido a sobrecarga o fallos en la red.

b) Amenazas humanas

- Errores operativos en la gestión de información de vuelos o reportes.
- Uso indebido de sistemas por desconocimiento o falta de capacitación.

c) Amenazas físicas

- Acceso no autorizado a áreas restringidas donde se encuentran equipos de control.
- Robo o pérdida de dispositivos móviles con información sensible.

d) Amenazas ambientales

- Inundaciones o humedad que afecten equipos sensibles.
- Tormentas eléctricas que pudieran dañar antenas y sistemas de comunicación.
- Fallos en la infraestructura externa de telecomunicaciones por eventos climáticos.

2.11 Identificación de vulnerabilidades

Las vulnerabilidades se definieron como las debilidades o deficiencias en los sistemas, procesos, personal o controles existentes que podían ser explotadas por una amenaza. La identificación se realizó mediante listas de verificación alineadas a los controles del Anexo A de ISO/IEC 27001, observaciones directas y entrevistas.

Las principales vulnerabilidades detectadas fueron:

2.11.1 Vulnerabilidades técnicas

- Configuraciones de seguridad incompletas o desactualizadas en servidores y equipos de red.
- Ausencia de autenticación multifactor para accesos críticos.
- Falta de segmentación adecuada en la red de comunicaciones.
- Sistemas legados sin actualizaciones de seguridad.

2.11.2 Vulnerabilidades operativas

- Procedimientos no documentados o desactualizados.
- Dependencia excesiva del conocimiento empírico de operadores.
- Falta de controles de cambio en la gestión de software y hardware.

2.11.3 Vulnerabilidades humanas

- Escasa capacitación del personal en seguridad de la información.
- Uso de contraseñas débiles o compartidas.
- Alto nivel de estrés operativo en el personal de control aéreo, lo que aumentaba la probabilidad de errores.

2.11.4 Vulnerabilidades físicas

- Espacios críticos sin control de acceso biométrico o tarjetas inteligentes.
- Equipos sensibles ubicados en áreas expuestas a humedad o variaciones térmicas.
- Insuficiente protección contra incendios en cuartos de servidores.

2.12 Relación entre amenazas, vulnerabilidades y activos

Una vez identificadas las amenazas y vulnerabilidades, se procedió a relacionarlas con los activos previamente valorados. Este cruce permitió determinar los riesgos específicos a

los que cada activo estaba expuesto y priorizar aquellos escenarios que podían comprometer gravemente la operación.

La **base de datos de vuelos**, clasificada como activo crítico, estaba expuesta a amenazas de ataques informáticos y errores de integridad, agravadas por vulnerabilidades como falta de controles robustos de acceso.

Los **sistemas de comunicación en tiempo real** presentaban amenazas ambientales y tecnológicas, sumadas a vulnerabilidades como hardware obsoleto o configuraciones inadecuadas. Este análisis permitió avanzar hacia la fase siguiente: la evaluación de riesgos y la posterior formulación del plan de acción.

2.13 Importancia del proceso para el análisis de brecha

La identificación de amenazas y vulnerabilidades resultó imprescindible para comprender el estado de la seguridad en Vigalco y determinar las brechas existentes respecto a los controles requeridos por ISO/IEC 27001. Gracias a este proceso fue posible:

- Reconocer los riesgos más relevantes para la continuidad operativa.
- Entender los puntos críticos donde se requerían mejoras inmediatas.
- Alinear los resultados con los requisitos del Anexo A de ISO/IEC 27001.

2.14 Estimación de impacto y cálculo de riesgo

En el estudio, la valoración del impacto y la estimación del riesgo ocupó un lugar clave dentro del enfoque metodológico adoptado para el análisis de brechas de Vigalco, tomando como referencia la norma ISO/IEC 27001. Esta fase hizo posible asignar un nivel de riesgo a cada activo de información, a partir de la combinación entre las amenazas identificadas, las vulnerabilidades detectadas y la importancia o criticidad de dichos activos para la operación de la organización. El propósito fue establecer una base objetiva para priorizar los controles de seguridad que debían implementarse dentro de la empresa.

El análisis de riesgos se realizó siguiendo los lineamientos de la norma ISO 27005, complementando las actividades de identificación de activos, amenazas y vulnerabilidades ya descritas. El proceso combinó técnicas cualitativas y cuantitativas, permitiendo obtener una medición del riesgo que fuera comprensible para los responsables operativos y suficientemente sólida para la toma de decisiones.

El procedimiento se desarrolló en cuatro pasos principales:

- Estimación de impacto
- Estimación de probabilidad
- Cálculo del nivel de riesgo
- Clasificación y priorización del riesgo

La integración de estos pasos permitió contar con una matriz de riesgos consistente y alineada con el contexto operativo de la empresa.

2.14.1 Estimación del impacto

La estimación del impacto se basó en los resultados obtenidos durante la valoración de activos. El impacto se entendió como el grado de daño que Vigalco podría sufrir si una amenaza se materializaba aprovechando una vulnerabilidad. Para ello, se evaluó cómo se verían afectados los atributos de confidencialidad, integridad y disponibilidad.

El impacto final asignado a cada escenario de riesgo se determinó tomando el mayor efecto previsto sobre cualquiera de los atributos de seguridad. Por ejemplo, para sistemas de comunicación en tiempo real, el impacto asociado a la disponibilidad se clasificó como **muy alto** por su rol crítico en la vigilancia aérea.

2.14.2 Estimación de la probabilidad

La probabilidad representó la posibilidad de que una amenaza lograra explotar una vulnerabilidad. La estimación se realizó evaluando factores como:

- Frecuencia histórica de incidentes.

- Estado del control existente (sólido, débil o inexistente).
- Exposición del activo al entorno operativo.
- Nivel de motivación o capacidad de agentes externos.

2.14.3 Cálculo del riesgo

El nivel de riesgo se obtuvo mediante la fórmula estándar recomendada por ISO 27005:

Riesgo = Probabilidad x Impacto

El valor resultante permitió clasificar el riesgo según su severidad. Como parte del análisis, varios escenarios de riesgo fueron evaluados. Un ejemplo ilustrativo se presenta a continuación:

Tabla 4

Análisis de activos, amenazas, vulnerabilidades y niveles de riesgo.

Activo	**Amenaza**	**Vulnerabilidad**	**Impacto**	**Probabilidad**	**Riesgo**	**Nivel**
Sistema de comunicación en tiempo real	Fallo técnico	Hardware obsoleto	5	4	20	Alto
Base de datos de vuelos	Intrusión externa	Controles débiles	5	3	15	Alto
Servidores administrativos	Malware	Falta de antivirus actualizado	3	3	9	Medio
Manuales internos	Acceso no autorizado	Documentación sin resguardo	2	2	4	Bajo

Fuente: Elaboración realizada por el autor.

La tabla 4 muestra, de forma sencilla, qué riesgos importantes afectan a cada activo y qué tan críticos son. El valor de riesgo se obtiene combinando ambos (normalmente multiplicando impacto por probabilidad) y se traduce en un nivel cualitativo: alto, medio o bajo, que sirve para priorizar qué riesgos atender primero. Este tipo de análisis permitió identificar claramente los riesgos que requerían atención inmediata debido a su nivel crítico.

2.14.4 Priorización del riesgo y toma de decisiones

Una vez obtenidos los valores de riesgo, se estableció un orden de priorización para definir los controles necesarios. Los riesgos altos fueron considerados inaceptables, lo que implicó evaluar medidas de mitigación urgentes, tales como:

- Actualización de equipos obsoletos.
- Endurecimiento de configuraciones de seguridad.
- Implementación de autenticación robusta.
- Fortalecimiento de políticas y capacitación del personal.

Los riesgos medios fueron considerados tolerables bajo monitoreo, pero sujetos a mejoras mediante controles adicionales. Finalmente, los riesgos bajos se mantuvieron bajo observación sin necesidad de intervenciones inmediatas.

El cálculo de riesgo permitió determinar las discrepancias entre la situación actual de Vigalco y los controles requeridos por ISO/IEC 27001. Gracias a esta estimación fue posible:

- Identificar los riesgos que amenazaban la continuidad del servicio de vigilancia aérea.
- Determinar dónde los controles eran insuficientes o inexistentes.
- Fundamentar la elaboración del plan de acción basado en evidencias técnicas.

2.15 Análisis de brecha

El análisis de brecha fue una parte clave de la metodología utilizada en el estudio. Este análisis permitió comparar cómo está la gestión de la seguridad de la información en Vigalco con los requisitos de la norma ISO/IEC 27001. Esta etapa hizo posible identificar las deficiencias existentes en controles, políticas, procesos y tecnologías, permitiendo evidenciar el nivel de madurez de la organización y los elementos que requerían atención inmediata para alcanzar el cumplimiento normativo.

2.15.1 Enfoque metodológico del análisis de brecha

El análisis de brecha se llevó a cabo mediante un procedimiento sistemático basado en la comparación directa entre:

- Los controles de seguridad requeridos por ISO/IEC 27001 (Anexo A).
- Los controles implementados y operativos en Vigalco.

Para realizar esta comparación se emplearon los siguientes insumos:

- Inventario y valoración de activos.
- Identificación de amenazas y vulnerabilidades.
- Resultados del cálculo de riesgos.
- Evidencia documental proporcionada por la empresa (procedimientos, registros, políticas).
- Entrevistas con personal clave sobre el funcionamiento real de los controles.

2.15.1 Herramienta de evaluación

Para el análisis se utilizó una matriz de cumplimiento, en la cual cada control del Anexo A se evaluó en función de su nivel de implementación, utilizando la siguiente escala:

Tabla 5
Nivel de madurez de los controles de seguridad

Nivel	Descripción	Interpretación
0	No implementado	El control no existe o no se aplica.
1	Parcialmente implementado.	Existe, pero es insuficiente o inefectivo.
2	Implementado	El control opera correctamente, pero sin evidencia formal.
3	Implementado y documentado.	El control se encuentra operativo y respaldado con documentación formal.
4	Optimizado	El control está comprobado, auditado y en mejora continua.

La tabla 5 presenta una escala de madurez de controles de seguridad con cinco niveles, del 0 al 4, esta escala permitió medir el nivel real de madurez en cada control de seguridad evaluado.

2.15.2 Criterios de cómputo del nivel de cumplimiento

Con el fin de garantizar la trazabilidad, consistencia y comparabilidad de los resultados obtenidos en el análisis de brecha del Sistema de Gestión de Seguridad de la Información (SGSI), se establecieron criterios explícitos para el cómputo del nivel de cumplimiento de la Norma ISO/IEC 27001, los cuales se detallan a continuación:

a. Universo de controles evaluados.

- Para la evaluación de los controles de seguridad de la información se consideró el Anexo A de la Norma ISO/IEC 27001, conformado por 93 controles en su versión vigente. A partir del análisis del contexto organizacional de VIGALCO y de la definición del alcance del SGSI, junto con la revisión de la Declaración de Aplicabilidad (SoA), se seleccionaron los controles que resultaban pertinentes para la empresa. En este proceso se descartaron aquellos controles que no aplicaban, dejando documentadas las razones de su exclusión.
- En consecuencia, el porcentaje de cumplimiento de controles se calcula únicamente sobre el universo de controles aplicables, y no sobre el total normativo, salvo que se indique expresamente lo contrario en tablas o figuras específicas.

b. Fecha y corte de evaluación.

- El análisis de brecha presentado en este estudio corresponde a una línea base, levantada mediante entrevistas, revisión documental y observación directa, con fecha de corte 12/2025.
- Los valores de cumplimiento reportados reflejan exclusivamente el estado actual del SGSI al momento del levantamiento de información, sin considerar la implementación de las acciones de mejora propuestas en el plan de implementación.
- Cuando se presentan escenarios prospectivos o estimaciones de cumplimiento posterior a la ejecución del plan de mejoras, estos se identifican explícitamente como escenario post-implementación y se reportan en secciones diferenciadas.

Las fuentes de información incluyeron: políticas y procedimientos institucionales, registros operativos, entrevistas con responsables de procesos, y revisión de sistemas tecnológicos en operación.

Del total de 93 controles definidos en el Anexo A de la Norma ISO/IEC 27001:2022, la totalidad de los controles fue considerada aplicable al alcance del SGSI de Vigalco. En consecuencia, el porcentaje de cumplimiento reportado en los resultados se calcula sobre el universo completo de 93 controles.

Tabla 6

Controles aplicables (SOA simplificada)

Control ISO/IEC 27001:2022	Descripción resumida	Aplicable (Sí/No)	Justificación de aplicabilidad / exclusión
A.5.1	Políticas de seguridad de la información	Si	Requerido para establecer el SGSI en VIGALCO
A.5.7	Inteligencias de amenazas	Si	Necesario por el entorno crítico aeronáutico
A.6.3	Formación en seguridad	Si	Aplica a todo el personal operativo
A.X.X	Control especifico excluido	No	No aplicable al alcance del SGSI definido, debido a [razón técnica/organizacional concreta]

Fuente: Elaboración propia

La tabla 6 presenta una SOA simplificada donde se identifican controles seleccionados de ISO-27001:2022 (p. ej., A.5.1, A.5.7, A.6.3), indicando su aplicabilidad al SGSI y la justificación correspondiente, así como un ejemplo de control no aplicable con su motivo de exclusión.

Para la evaluación del nivel de implementación de los controles de seguridad de la información se utilizó una escala ordinal unificada de cinco niveles (0–4), aplicada de manera consistente tanto en el checklist de levantamiento de información como en la matriz de cumplimiento y el análisis de brecha.

Esta escala permite medir el grado de madurez de cada control, desde su inexistencia hasta su optimización, y se encuentra alineada con enfoques de evaluación de madurez comúnmente utilizados en la implementación de Sistemas de Gestión de Seguridad de la Información basados en ISO/IEC 27001.

2.16 Resultados del análisis de brecha

Los resultados mostraron que Vigalco presentaba avances significativos en ciertos controles operativos, especialmente aquellos relacionados con la continuidad operativa y el manejo de equipos críticos. Sin embargo, también se evidenciaron brechas significativas en áreas estratégicas y administrativas, necesarias para cumplir con la norma ISO/IEC 27001. Entre los hallazgos principales se identificaron:

2.16.1 Controles con brecha alta (nivel 0–1)

Estos correspondieron a controles críticos que no estaban implementados o funcionaban de manera limitada. Las brechas más relevantes incluyeron:

- Falta de un sistema de gestión de seguridad de la información (SGSI) formalizado.
- Ausencia de políticas documentadas de seguridad revisadas periódicamente.
- Carencia de un proceso de gestión de incidentes estructurado.
- Debilidades en la clasificación de la información y control de activos.
- Controles insuficientes en **gestión de accesos**, incluyendo autenticación robusta.
- Estas brechas representaron un riesgo alto debido al impacto directo sobre los activos críticos identificados.

2.16.2 Controles con brecha media (nivel 2)

Incluyeron controles existentes, pero sin evidencia formal o con procedimientos que no se aplicaban de manera consistente. Entre los principales:

- Continuidad operativa con limitaciones en la formalización de procedimientos.
- Controles de respaldo de información sin pruebas periódicas documentadas.

- Gestión de proveedores sin evaluación sistemática de riesgos.
- Estos controles mostraban la necesidad de fortalecimiento documental y operativo.

2.16.3 Controles con brecha baja (nivel 3–4)

Se identificaron áreas donde la empresa ya aplicaba controles maduros:

- Gestión física de equipos en áreas restringidas.
- Monitoreo continuo de sistemas críticos de vigilancia y comunicaciones.
- Capacidades operativas estandarizadas en ambientes de control aéreo.
- Aunque operativos, algunos procesos carecían de evidencias de auditoría o de mejora continua.

El análisis de brecha se integró con los resultados del cálculo de riesgos, permitiendo establecer correspondencia entre:

- Riesgos altos no cubiertos por controles adecuados.
- Vulnerabilidades sin medidas de mitigación efectivas.
- Activos críticos sin protección suficiente.

El análisis de brecha permitió evidenciar que Vigalco debía fortalecer varios componentes esenciales para cumplir con los requisitos de ISO/IEC 27001, especialmente en cuanto a:

- Documentación formal del SGSI.
- Implementación de controles de acceso más robustos.
- Establecimiento de procesos de gestión de incidentes, riesgos y continuidad del negocio.
- Refuerzo de medidas de protección tecnológica y actualización de sistemas.
- Capacitación continua del personal en seguridad de la información.

2.17 Plan de tratamiento

El plan de tratamiento del riesgo constituyó la etapa final dentro del proceso de análisis aplicado en Vigalco, y permitió definir las acciones necesarias para mitigar, transferir, aceptar o evitar los riesgos identificados durante el análisis previo. Basándose en

los resultados de la evaluación de activos, la identificación de amenazas y debilidades, y el cálculo del nivel de riesgo, se establecieron acciones para reducir la probabilidad de que ocurran y el impacto de los riesgos que se consideran inaceptables.

2.17.1 Enfoque metodológico

Para la elaboración del plan se siguieron las directrices de la norma ISO 27005 e ISO/IEC 27001, las cuales recomiendan:

- Seleccionar los controles apropiados del Anexo A de ISO/IEC 27001 u otros marcos de referencia.
- Definir el tratamiento adecuado para cada riesgo (mitigar, evitar, transferir o aceptar).
- Asignar responsabilidades claras dentro de la organización.
- Establecer un cronograma realista para la implementación de medidas.
- Determinar indicadores de seguimiento que permitieran evaluar la eficacia del tratamiento.

Este enfoque permitió asegurar la coherencia del plan con los objetivos de la seguridad de la información y con las necesidades operativas de Vigalco.

2.17.2 Estrategias de tratamiento aplicadas

Cada riesgo identificado fue evaluado con base en su nivel de criticidad (bajo, medio o alto), aplicando una de las siguientes estrategias:

a) Mitigación

Consistió en aplicar acciones que redujeron la probabilidad o el impacto del riesgo. Esta estrategia se utilizó especialmente en riesgos altos asociados a la base de datos de vuelos, sistemas de comunicación y controles de acceso. Acciones típicas incluyeron:

- Actualización de hardware y software.
- Implementación de autenticación multifactor.
- Segmentación de redes y endurecimiento de configuraciones.

- Desarrollo o actualización de procedimientos operativos estándar.

b) Evitación

Se aplicó cuando la actividad generadora del riesgo podía ser eliminada o reemplazada.

Ejemplo:

- Eliminación del uso de equipos sin soporte técnico oficial.
- Descontinuación de procesos manuales que implicaban errores recurrentes.

c) Transferencia

Se utilizó para riesgos operativos o técnicos que podían ser gestionados parcialmente por terceros, como:

- Contratación de servicios externos de monitoreo o respaldo.
- Aseguramiento de equipos críticos mediante pólizas especializadas.

d) Aceptación

Se aplicó únicamente a riesgos bajos, cuando el costo de la mitigación superaba el beneficio o cuando la probabilidad de ocurrencia resultaba mínima. La aceptación se documentó formalmente para asegurar su trazabilidad.

2.17.3 Priorización de medidas

Las acciones del plan se priorizaron según:

- **Nivel de riesgo** (alto, medio, bajo).
- **Impacto sobre operaciones críticas** de vigilancia y control aéreo.
- **Recursos disponibles** y capacidad de implementación de Vigalco.
- **Dependencia tecnológica** de cada proceso.

Los riesgos altos fueron tratados de manera inmediata, destinando recursos prioritarios a la protección de activos como:

- Sistema de comunicación en tiempo real.
- Base de datos de vuelos.

- Plataformas de monitoreo y vigilancia aérea.

2.18 Matriz de tratamiento de riesgos (ejemplo)

La siguiente tabla resume el tipo de tratamiento propuesto para algunos de los riesgos representativos:

Tabla 7

Identificación de riesgos por activo y controles ISO recomendados.

Activo	**Riesgo identificado**	**Nivel**	**Tratamiento**	**Control ISO recomendado**	**Responsable**
Sistema de comunicación en tiempo real	Fallo crítico por hardware obsoleto	Alto	Mitigar	A.12.1.2, A.17.2.1	TI Seguridad
Base de datos de vuelos	Acceso no autorizado	Alto	Mitigar	A.9.2, A.10.1	TI Administración
Servidores administrativos	Malware	Medio	Mitigar	A.12.2.1	TI
Documentación interna	Acceso indebido	Bajo	Aceptar	A.8.2.2	Administración

Fuente: Elaborada por el autor.

La tabla 7 sintetiza la gestión de riesgos de cuatro activos de información, clasificando su impacto, tratamiento y controles ISO 27001 asociados. Prioriza la mitigación de riesgos altos y medios (fallo de hardware crítico, accesos no autorizados y malware) mediante controles de continuidad, control de acceso y seguridad de operaciones, mientras que el riesgo bajo de acceso a documentación interna se acepta de forma controlada, manteniendo responsables designados por activo.

Esta matriz sirvió de guía para la elaboración del plan final. Todos los riesgos y acciones definidas se documentaron en un **Plan de Tratamiento del Riesgo (PTR)**, el cual incluyó:

- Descripción del riesgo.
- Nivel asignado.
- Estrategia de tratamiento seleccionada.
- Controles de ISO/IEC 27001 aplicables.

- Acciones específicas a ejecutar.
- Responsables internos asignados.
- Recursos necesarios.
- Plazos de implementación
- Indicadores de evaluación.

El PTR fue presentado a la alta dirección de Vigalco para su aprobación, conforme al principio de responsabilidad y compromiso de ISO/IEC 27001.

2.18.1 Seguimiento y revisión

Finalmente, se establecieron mecanismos de seguimiento para garantizar el cumplimiento progresivo del plan:

- Reuniones mensuales de avance.
- Indicadores de desempeño del SGSI.
- Verificación documental de controles implementados.
- Ajustes y mejoras continuas.

Este proceso permitió asegurar que las acciones correctivas fueran implementadas de manera ordenada, verificable y alineada al análisis de brecha realizado.

2.19 Riesgo residual

El plan residual se elaboró con el objetivo de gestionar los riesgos que permanecieron después de la aplicación del plan de tratamiento correspondiente. A pesar de la implementación de controles técnicos, administrativos y operacionales, ciertos riesgos no pudieron eliminarse por completo, ya sea porque su mitigación total no resultó posible, porque existían limitaciones tecnológicas o porque el costo de reducirlos aún más superaba los beneficios esperados. Por eso, el plan residual ayudó a registrar, estudiar y aceptar oficialmente los riesgos que quedaron, garantizando una gestión continua y controlada según las normas de ISO/IEC 27001 e ISO 27005.

2.19.1 Enfoque metodológico para la gestión del riesgo residual

Para definir el riesgo residual, se siguió la metodología que se describe a continuación:

- Reevaluación del riesgo después del tratamiento.

  Se analizó nuevamente cada riesgo, considerando la reducción lograda en términos de probabilidad e impacto después de aplicar los controles seleccionados.

- Determinación del nivel residual.

  Se calculó el riesgo residual utilizando la misma metodología de valoración (matrices, escalas y criterios del análisis inicial), garantizando coherencia en la evaluación.

- Comparación con el nivel de riesgo aceptable de Vigalco.

  El nivel residual fue contrastado con la política de aceptación del riesgo definida en la organización, la cual establecía qué niveles podían ser tolerados sin medidas adicionales.

- Documentación formal del riesgo residual.

  Cada riesgo que permaneció se registró con detalle, incluyendo controles aplicados, causas de persistencia y justificación de aceptación.

- Aprobación por parte de la alta dirección.

  Según la ISO/IEC 27001, la responsabilidad final de aceptar riesgos recae en la dirección. Por ello, cada riesgo residual fue presentado para su validación formal.

Este enfoque permitió gestionar los riesgos de manera estructurada, transparente y trazable.

2.19.2 Categorías de riesgo residual identificadas

Durante el proceso se identificaron tres categorías principales de riesgo residual en Vigalco:

a) Riesgo residual tecnológico

- Incluyó riesgos derivados de:
- Limitaciones de infraestructura.
- Dependencia de equipos con soporte limitado.
- Amenazas persistentes como malware o ataques de fuerza bruta.

A pesar de controles instalados (antivirus, endurecimiento, monitoreo), siempre existió probabilidad residual debido a la naturaleza cambiante de las amenazas cibernéticas.

b) Riesgo residual humano

Relacionados con:

- Posibles errores operativos.
- Omisiones en el cumplimiento de procedimientos.
- Dependencia del factor humano en tareas críticas.

Incluso con capacitación y procedimientos formales, se consideró que los errores no podían eliminarse totalmente.

c) Riesgo residual organizacional

Vinculado a:

- Limitaciones presupuestarias para implementar controles más sofisticados.
- Procesos en mejora continua, aún en fase inicial.
- Dependencia de terceros o proveedores con niveles de seguridad variables.

Estos riesgos fueron gestionados mediante seguimiento constante.

2.19.3 Criterios de aceptación del riesgo residual

La aceptación del riesgo residual se basó en los siguientes criterios:

- El riesgo residual debía encontrarse en niveles **bajos o medios controlados**.
- Se requería una **justificación documentada**, especialmente cuando el riesgo residual era medio.
- Debía existir evidencia de que todas las acciones razonables de mitigación habían sido implementadas.
- El riesgo no debía comprometer operaciones críticas del servicio de vigilancia y control aéreo.
- Su aceptación debía ser aprobada explícitamente por la alta dirección de Vigalco.

2.19.4 Acciones de seguimiento del riesgo residual

Con el fin de asegurar que los riesgos residuales no evolucionaran hacia niveles inaceptables, se definieron acciones de seguimiento, tales como:

- Monitoreo periódico de controles tecnológicos.
- Revisión trimestral del plan residual.
- Reentrenamiento del personal en procesos críticos.
- Auditorías internas al SGSI.
- Actualización de políticas según cambios operativos o tecnológicos.

Estas actividades aseguraron que los riesgos no mitigados por completo permanecieran bajo vigilancia constante.

El plan residual proporcionó una visión clara y controlada de los riesgos que no pudieron ser eliminados totalmente, permitiendo a Vigalco gestionar de manera responsable aquellos elementos que, pese a las acciones de mitigación, continuaron representando una amenaza potencial. Asimismo, garantizó la conformidad con la ISO/IEC 27001, que exige la aceptación formal del riesgo residual como parte del proceso de establecimiento y mejora del SGSI.

El plan residual completó el ciclo metodológico del análisis de riesgos, asegurando que todas las decisiones quedaran documentadas, justificadas y alineadas con los objetivos de seguridad de la organización.

2.20 Validación experta

La validación por expertos fue la etapa final de la metodología utilizada en esta investigación. El propósito fue validar que el análisis de brecha realizado a la gestión de seguridad de la información de Vigalco resultara consistente con la realidad de la organización y útil para su implementación. Esta etapa permitió verificar que los hallazgos,

conclusiones y recomendaciones del estudio estuvieran alineados con las mejores prácticas del sector, así como con los requisitos establecidos en la norma ISO/IEC 27001.

El objetivo principal de la validación fue obtener la opinión fundamentada de profesionales con experiencia en:

- Implementación de Sistemas de Gestión de Seguridad de la Información (SGSI).
- Auditoría de estándares ISO/IEC 27001 y 27005.
- Gestión de riesgos en infraestructuras críticas y servicios de vigilancia y control aéreo.

El propósito consistió en asegurar que la metodología aplicada fuera técnicamente precisa y que los resultados obtenidos representaran una evaluación adecuada del estado de la seguridad de la información en Vigalco.

2.20.1 Selección de expertos

El proceso de validación se realizó mediante la participación de cinco (5) expertos, seleccionados bajo criterios de idoneidad técnica, experiencia profesional y conocimiento del contexto de seguridad de la información. El perfil resumido de los expertos fue el siguiente:

- Dos especialistas en Sistemas de Gestión de Seguridad de la Información (SGSI) con experiencia en implementación y auditoría de la Norma ISO/IEC 27001.
- Un profesional del **sector aeronáutico**, con experiencia en operaciones de vigilancia y control aéreo.
- Un especialista en ciberseguridad y gestión de riesgos tecnológicos, con énfasis en infraestructuras críticas.
- Un académico con experiencia en **investigación aplicada en** seguridad de la información.

Todos los expertos contaban con una experiencia profesional mínima de cinco años en sus respectivas áreas, lo que garantizó la calidad técnica de los juicios emitidos.

Los expertos fueron seleccionados mediante un muestreo intencional, priorizando criterios como:

- Certificaciones profesionales (ISO/IEC 27001 Lead Auditor, Lead Implementer, CISM, CISSP).
- Contar con al menos cinco años de trayectoria profesional en funciones relacionadas con la seguridad de la información.
- Poseer conocimientos demostrables en gestión de riesgos y/o en la realización de análisis de brechas de seguridad.
- Participación en proyectos similares dentro del ámbito aeronáutico o de comunicaciones críticas.

Este proceso permitió reunir un grupo representativo y con la capacidad técnica necesaria para evaluar los resultados del estudio.

2.20.2 Método de validación empleado

La validación se desarrolló mediante la técnica de juicio de expertos, utilizando un instrumento estructurado tipo checklist. Dicho instrumento evaluó las brechas y mejoras propuestas en función de criterios previamente definidos, tales como:

- Claridad de la brecha identificada
- Pertinencia del control propuesto frente a ISO/IEC 27001
- Viabilidad técnica y operativa
- Impacto esperado en la reducción del riesgo
- Coherencia con el contexto de la empresa Vigalco

Cada criterio fue evaluado mediante una **escala ordinal de cinco niveles (1–5)**, donde:

1 = Muy bajo

2 = Bajo

3 = Medio

4 = Alto

5 = Muy alto

La adopción de una escala de cinco niveles permitió una valoración homogénea y comparable entre los distintos criterios evaluados.

La validación se llevó a cabo mediante un método de juicio de expertos, el cual incluyó los siguientes pasos:

a) Presentación del informe técnico

- A cada experto se le proporcionó un documento que contenía:
- Inventario y valoración de activos.
- Identificación de amenazas y vulnerabilidades.
- Matriz de riesgos y riesgo residual.
- Análisis de brecha y plan de tratamiento del riesgo.
- Conclusiones preliminares.

b) Cuestionario estructurado

Se diseñó un instrumento de validación compuesto por criterios evaluativos como:

- Claridad y consistencia metodológica.
- Alineación con ISO/IEC 27001 y ISO 27005.
- Relevancia de las amenazas y vulnerabilidades identificadas.
- Pertinencia de los controles propuestos.
- Coherencia entre el riesgo calculado y el riesgo residual.
- Realismo y aplicabilidad del plan de tratamiento.

Cada criterio se evaluó mediante una escala tipo Likert de cinco niveles (Muy adecuado – Inadecuado).

c) Entrevistas de retroalimentación

Se llevaron a cabo entrevistas semiestructuradas con los expertos con el fin de profundizar en sus observaciones, aclarar dudas y obtener recomendaciones adicionales que fortalecieran los resultados del análisis. Los resultados generales del proceso indicaron que:

- La metodología aplicada se consideró técnicamente sólida y adecuada para el tipo de organización analizada.
- Los activos identificados fueron evaluados como correctamente clasificados y representativos del entorno operativo de Vigalco.
- La identificación de amenazas y vulnerabilidades fue valorada como **completa y coherente**, especialmente en lo referente a riesgos tecnológicos y operacionales.
- El cálculo del riesgo se calificó como **pertinente**, dado que utilizó criterios objetivos y escalas acordes a estándares internacionales.
- El plan de tratamiento fue considerado **realista y viable**, aunque los expertos recomendaron fortalecer algunas acciones relacionadas con monitoreo continuo y gestión de incidentes.
- El riesgo residual fue evaluado como **bien justificado**, documentando adecuadamente los motivos de aceptación.

En general, el nivel de conformidad obtenido se situó en rangos altos, lo que permitió validar el rigor metodológico y la confiabilidad de los resultados. Con base en la retroalimentación recibida, se realizaron los siguientes ajustes al estudio:

- Se ampliaron las descripciones de ciertos controles propuestos en el plan de tratamiento.
- Se reforzaron los criterios de aceptación del riesgo residual, añadiendo evidencia técnica y operativa.
- Se actualizó la matriz de brecha para incluir un mayor detalle en la valoración de documentaciones existentes.
- Se recomendó incorporar un plan de concientización anual para mitigar riesgos humanos residuales.

Estos ajustes permitieron mejorar la precisión del análisis y alinearlo aún más con los estándares internacionales.

2.20.3 Regla de aceptación y agregación de resultados

Para la interpretación de los resultados de la validación experta, se definió una **regla de aceptación explícita**. Se consideró que una brecha o mejora propuesta era **aceptada** cuando el **promedio de las calificaciones otorgadas por los expertos fue igual o superior a 4,0** en la escala de 1 a 5.

La agregación de los puntajes se realizó mediante el **promedio aritmético simple** de las valoraciones individuales de cada experto para cada criterio evaluado. Este enfoque permitió obtener un valor consolidado que reflejara el consenso general del panel de expertos.

En los casos en que el promedio obtenido fue inferior al umbral definido, la brecha o mejora fue clasificada como **requiere ajuste**, procediéndose a su revisión y reformulación antes de su inclusión definitiva en el plan de tratamiento.

El instrumento de validación utilizado, así como los resultados detallados de la evaluación por criterio y por experto, se presentan en los **anexos correspondientes**, a fin de garantizar la trazabilidad, transparencia y verificabilidad del proceso metodológico.

Los instrumentos utilizados y los resultados detallados de la validación experta se presentan en el Anexo Instrumentos y Resultados de la Validación experta, donde se documenta el proceso de evaluación por criterio, los puntajes individuales y los promedios consolidados.

2.21 Instrumento utilizado para el levantamiento de activos

Para la identificación y caracterización de los activos involucrados en los procesos de vigilancia, alerta y control aéreo de la empresa Vigalco, se empleó un **checklist estructurado**. Este fue desarrollado a partir de los lineamientos metodológicos de MAGERIT v3 y de los requisitos establecidos en el Anexo A de la Norma ISO/27001:2022.

Este instrumento permitió recopilar información sistemática, uniforme y verificable sobre los activos críticos relacionados con los servicios operacionales de la organización.

El checklist fue diseñado con el propósito de **identificar los activos esenciales**, determinar su nivel de criticidad y establecer su grado de protección actual. Se consideraron los parámetros de confidencialidad, integridad y disponibilidad (CID) definidos tanto por la normativa internacional como por la naturaleza altamente sensible de las operaciones aeronáuticas. Asimismo, el instrumento incorpora criterios de evaluación asociados a amenazas, vulnerabilidades y controles de seguridad existentes, lo que contribuyó a la construcción de una línea base para el análisis de riesgos y el análisis de brecha frente a ISO/IEC 27001.

El instrumento se organizó en tres secciones principales.

- **La primera** sección corresponde a la identificación de activos, en la cual se registraron datos como tipo de activo, propietario, ubicación, dependencias asociadas y valoración CID según una escala de 1 a 5 derivada de MAGERIT.
- **La segunda sección** aborda la identificación de amenazas y vulnerabilidades, permitiendo describir condiciones internas o externas que podrían comprometer el funcionamiento de los activos críticos.
- **La tercera sección** se centra en revisar y evaluar de manera inicial los controles, siguiendo los 93 controles del Anexo A de ISO/IEC 27001:2022 utilizando una escala de cumplimiento alineada con el modelo de madurez de controles definido en el numeral 2.15.1, con valores de 0 a 4.

La escala utilizada en el checklist se corresponde directamente con la escala de madurez empleada en el análisis de brecha, garantizando la consistencia metodológica y la comparabilidad de los resultados obtenidos.

La aplicación del instrumento se realizó mediante **entrevistas estructuradas**, **observación directa** y **revisión documental** en las áreas operativas, técnicas y administrativas de Vigalco. Su estructura facilitó la interacción con los responsables de cada proceso, lo que permitió obtener un inventario actualizado y contextualizado de los activos involucrados en las operaciones de vigilancia, alerta y control aéreo.

El checklist se aplicó de manera presencial en las instalaciones de la empresa, garantizando la verificación in situ de equipos, infraestructura tecnológica, sistemas de información y documentación relevante.

Este instrumento constituye la base para el análisis de riesgos desarrollado en el presente estudio, proporcionando una fuente primaria de información confiable, precisa y adaptada al entorno aeronáutico ecuatoriano. El formato completo del checklist se presenta en los Anexos de este documento.

En el contexto de Vigalco, el pilotaje se refiere a las habilidades y conocimientos necesarios para manejar y operar de forma segura y efectiva los equipos tecnológicos y operativos que apoyan las actividades de aviación. Este criterio adquiere especial relevancia debido a que la empresa trabaja con sistemas críticos —como consolas de control, radares, centros de monitoreo, equipos de telecomunicaciones y plataformas de procesamiento de datos aeronáuticos— cuya operación exige rigor técnico, precisión y cumplimiento normativo.

Para Vigalco, el pilotaje comprende los siguientes aspectos:

- Grado de intervención humana requerida para activar, supervisar o interpretar los sistemas de vigilancia y control aéreo.
- Complejidad de uso, tomando en cuenta la cantidad de procesos, comandos, protocolos o procedimientos necesarios para operar un activo de manera correcta.

- Sensibilidad del activo al error humano, considerando que una manipulación incorrecta puede afectar la capacidad de vigilancia del espacio aéreo o comprometer la comunicación operativa.
- Nivel de criticidad operativa, en función de su aporte directo a la seguridad operacional, toma de decisiones y gestión de eventos aéreos.

El criterio de pilotaje permitió clasificar activos según el esfuerzo técnico requerido para su operación, la necesidad de entrenamiento especializado y la relevancia que su manejo adecuado tiene en las actividades misionales de VIGALCO.

La confiabilidad se refiere a la habilidad de los activos tecnológicos, operativos e infraestructurales para realizar sus funciones de manera constante, estable y sin errores, asegurando la seguridad y la continuidad de las operaciones de vigilancia y control aéreo. Este criterio es especialmente crucial debido a que una interrupción en sistemas críticos —como radares, enlaces de comunicación, servidores o sensores— puede comprometer la capacidad de respuesta ante eventos aéreos, afectar la continuidad del servicio o generar riesgos operacionales.

En el contexto de la empresa, la confiabilidad se evalúa considerando:

- Historial de fallos, frecuencia de interrupciones o comportamientos anómalos en los activos.
- Estabilidad del desempeño, es decir, la capacidad del activo para mantener su operación bajo condiciones normales o exigentes.
- Disponibilidad operativa, medida en términos de su tiempo en servicio frente a su duración fuera de operación.
- Mantenibilidad del activo, incluyendo la facilidad de mantenimiento preventivo y correctivo, disponibilidad de repuestos y soporte técnico.

- Impacto del fallo, teniendo en cuenta cómo la interrupción del activo afecta los procesos de vigilancia, alerta y control del espacio aéreo.

2.22 Ética y legalidad

En el desarrollo de la presente investigación se adoptaron medidas de ética y legalidad para garantizar la recolección y manejo responsable de la información.

Se obtuvo consentimiento informado de los responsables de cada área, asegurando que la participación fuera voluntaria y que la información recopilada se utilizara exclusivamente con fines académicos y de análisis de riesgos. Todos los datos fueron tratados con confidencialidad**,** almacenados en medios seguros y codificados para proteger la identidad de los colaboradores y la integridad de los sistemas críticos de la empresa.

La investigación cumplió con la Ley Orgánica de Protección de Datos Personales (LOPD) de Ecuador, garantizando la privacidad de los datos personales recolectados durante entrevistas, observaciones y revisión documental. Asimismo, se respetaron las normativas de seguridad aeronáutica y los lineamientos de ISO/IEC 27001:2022, asegurando que el análisis de activos y controles no comprometiera la operación ni la seguridad de VIGALCO.

Se priorizó la **ética profesional**, evitando la manipulación de datos, respetando la confidencialidad de los participantes y asegurando que los resultados y recomendaciones se presentaran de manera objetiva y responsable. Finalmente, se documentaron las limitaciones derivadas del acceso restringido a información clasificada, garantizando que la investigación se desarrollara de manera segura y legal.

Aunque en el presente estudio no se dispuso de mediciones cuantitativas antes y después de la implementación de las mejoras, los expertos coincidieron en que los indicadores propuestos (KPI y KRI) permiten medir en el tiempo la reducción del riesgo y el incremento del cumplimiento de la norma ISO/IEC 27001, siempre que la organización continúe aplicando el plan de tratamiento definido.

CAPÍTULO 3: ANÁLISIS DE RIESGO DE LA EMPRESA

El presente capítulo abordará la identificación y el inventario de los activos críticos de la empresa, estableciendo su importancia y nivel de exposición. Se presentará un mapa de riesgos que permitirá visualizar amenazas, vulnerabilidades y su impacto potencial. También tendrá en cuenta las brechas existentes en los controles actuales para determinar su eficacia real, así como las mejoras propuestas para fortalecer la seguridad y reducir los riesgos identificados.

3.1 Inventario resumido de activos críticos

El inventario de activos críticos es crucial para el análisis de riesgos en VIGALCO. Este inventario ayuda a identificar los recursos que son esenciales para asegurar la continuidad y seguridad de las operaciones de vigilancia, alerta y control aéreo, cuidando su disponibilidad, integridad y confidencialidad. Con base en los criterios de confidencialidad, integridad y disponibilidad (CID), así como en las escalas de pilotaje y confiabilidad, se seleccionaron los **principales activos críticos** que requieren priorización en la gestión de riesgos.

Para determinar los activos incluidos en este inventario resumido, se aplicaron los siguientes criterios:

- **Valoración CID**: activos con puntajes altos en Confidencialidad, Integridad y Disponibilidad, indicando que su pérdida o fallo impactaría significativamente en las operaciones.
- **Nivel de pilotaje**: activos cuya operación requiere personal altamente capacitado o certificado, aumentando el riesgo operativo ante errores humanos.
- **Confiabilidad**: activos con baja confiabilidad o historial de fallos, cuya indisponibilidad podría afectar la continuidad de los servicios críticos.

- **Criticidad operacional**: activos cuya función está directamente relacionada con la vigilancia y control aéreo y cuya falla tendría repercusiones inmediatas en la seguridad de la operación.

El análisis del inventario revela que los activos Radar Primario y Servidor de datos aeronáuticos presentan la **mayor criticidad**, debido a su alto valor CID y dependencia operativa. También se nota que el personal que opera el radar es muy importante para que el servicio funcione sin problemas. Por eso, se sugiere dar prioridad a la capacitación y a las medidas para reducir los errores humanos.

El inventario consolidado permite a VIGALCO dirigir de manera prioritaria las actividades de gestión de riesgos, definición de controles y preparación de planes de respuesta hacia los activos que resultan más críticos para la seguridad y la continuidad del negocio.

3.2 Mapa de riesgos

Ejes del mapa:

- **Impacto (vertical):** Representa la criticidad del activo (CID y Pilotaje).
- **Probabilidad (horizontal):** Se basa en la confiabilidad del activo y en fallos históricos.

Definición de niveles:

Tabla 8
Niveles de riesgo y su correspondiente descripción.

Nivel	Impacto/Probabilidad	Descripción
Bajo	1-2	Riesgo menor, supervisión periódica.
Medio	3	Riesgo moderado, requiere mitigación planificada.
Alto	4	Riesgo relevante, acción correctiva inmediata
Crítico	5	Riesgo máximo, requiere medidas urgentes y controles redundantes.

Fuente: Elaborada por el autor.

La tabla 8 establece cuatro niveles de riesgo (bajo, medio, alto y crítico) que se diferencian por el valor numérico de impacto/probabilidad y por la urgencia de las acciones de control asociadas. En esencia, a medida que el valor se acerca a 5, el riesgo pasa de ser aceptable con simple seguimiento a exigir respuestas inmediatas y medidas reforzadas.

Tabla 9

Riesgos asociados a activos críticos.

Activo	Riesgo identificado	Impacto	Probabilidad	Nivel de riesgo
Radar primario	Fallo técnico durante operación	5	3	Alto
Servidor de datos aeronáuticos	Pérdida de información por fallo	5	2	Alto
Consola de control radar	Error humano en operación	4	3	Alto
Enlace de comunicación tierra-aire	Interrupción de comunicación	4	3	Alto
Personal operador de radar	Fatiga o error humano	4	3	Alto

Fuente: Elaborada por el autor.

La tabla 9 muestra que todos los activos críticos del sistema de vigilancia aérea presentan un nivel de riesgo alto, ya sea por fallos técnicos, errores humanos o interrupciones de comunicación. En general, los impactos asignados son muy elevados (4 y 5) y las probabilidades se sitúan en valores medios (2 y 3), lo que confirma que cualquier incidente en estos elementos podría afectar de forma seria la seguridad operacional.

El mapa de riesgos es una representación visual y resumida de los riesgos relacionados con los activos principales de VIGALCO. Este mapa tiene en cuenta su importancia en las operaciones, así como los niveles de Confidencialidad, Integridad y Disponibilidad (CID) y los criterios de Pilotaje y Confiabilidad. Este instrumento permite

priorizar las acciones de mitigación y la asignación de recursos según el impacto potencial y la probabilidad de ocurrencia de cada riesgo *[10]*.

3.3 Metodología para la elaboración del mapa de riesgos

Identificación de riesgos: Se derivan de los activos críticos identificados en el inventario resumido (Sección 3.1) y de la evaluación de los controles del Anexo A de ISO/27001.

3.4 Valoración de impacto y probabilidad:

- **Impacto:** Se calcula en función de la criticidad del activo (CID y Pilotaje).
- **Probabilidad:** Se estima según la confiabilidad del activo, historial de fallos y vulnerabilidades detectadas en los controles.
- **Asignación de niveles de riesgo:** Los riesgos se categorizan como ***bajo, medio, alto o crítico***, combinando el impacto y la probabilidad.

Se representa gráficamente con un diagrama de matriz de riesgos (Impacto vs. Probabilidad), destacando los activos que requieren atención prioritaria.

Tabla 10

Riesgos identificados en activos críticos.

Activo	Riesgo identificado	Impacto	Probabilidad	Nivel de riesgo	Observaciones
Servidor de datos aeronáuticos	Pérdida de información por fallo de hardware	Muy alto.	Bajo	Alto	Implementar backup y redundancia geográfica.
Consola de control de radar	Error humano en operación	Alto	Medio	Alto	Capacitación continua y protocolos de verificación
Enlace de comunicación tierra-aire	Interrupción de comunicación	Alto	Medio	Alto	Sistemas redundantes y monitoreo continuo
Personal operador de radar	Fatiga o error humano	Alto	Medio	Alto	Rotación de turnos y controles operativos

Fuente: Elaborada por el autor.

La tabla 10 detalla los riesgos más delicados de los activos críticos y propone cómo tratarlos, manteniendo en todos los casos un nivel de riesgo alto a pesar de las medidas

sugeridas. Se combinan impactos elevados con probabilidades bajas o medias, por lo que la intención es reducir la posibilidad de fallo sin perder de vista que las consecuencias seguirían siendo graves.

3.5 Interpretación del mapa de riesgos

Los activos con riesgo alto o crítico son prioritarios para la implementación de controles adicionales, planes de contingencia y medidas de mitigación. Los riesgos medios o bajos se monitorean periódicamente para evitar escalamiento. El mapa permite visualizar rápidamente la exposición de la empresa frente a amenazas internas y externas, facilitando la toma de decisiones estratégicas en la gestión de seguridad y continuidad operacional.

3.6 Brechas por control

El análisis de brechas por control se desarrolló tomando como referencia los requisitos del Anexo A de la Norma ISO-27001:2022, contrastando dichos lineamientos con el estado actual de los procesos, prácticas y controles implementados en Vigalco. Para cada uno de los controles evaluados se identificaron las evidencias disponibles, el grado de cumplimiento, la brecha existente, la severidad estimada del incumplimiento y una recomendación específica orientada a su mitigación. Los resultados presentados a continuación corresponden a los controles que evidenciaron desviaciones significativas con relación a los requerimientos de la norma.

3.6.1 Controles organizacionales (A.5)

A.5.1 Políticas para la seguridad de la información

Durante la revisión documental se constató que la política institucional de seguridad de la información fue emitida en el año 2019 y no registra actualizaciones posteriores. Además, no se identificó evidencia de revisiones periódicas ni de un mecanismo formal para mantenerla alineada a las necesidades de operación crítica de Vigalco.

Esta situación representa una brecha que impacta la consistencia y vigencia del marco normativo interno. La severidad se clasifica como **media**, debido a que la organización cuenta con lineamientos básicos, pero estos no se encuentran actualizados. Se recomienda actualizar la política conforme a ISO/IEC 27001:2022, incorporando elementos relativos a operaciones de vigilancia y control aéreo, así como establecer un proceso formal de revisión anual.

A.5.7 Seguridad en la gestión de proveedores

Se demostró que Vigalco no tiene un proceso formal para evaluar los riesgos de los proveedores que participan en actividades cruciales, como el mantenimiento de radares, las conexiones de comunicación y los servidores de procesamiento. La falta de controles para proveedores estratégicos constituye una brecha de alta relevancia, ya que compromete la integridad operativa de los servicios prestados. La severidad se determina como **alta**. Se recomienda establecer un proceso de gestión de proveedores que incluya criterios de evaluación de seguridad, cláusulas contractuales específicas y mecanismos de monitoreo continuo.

A.5.17 Continuidad del negocio

No se encontró evidencia de un análisis de impacto en el negocio (BIA) para los servicios de vigilancia y control aéreo, ni de un plan formal de continuidad que contemple situaciones de fallo total o parcial de los sistemas críticos. Esta brecha afecta directamente la capacidad de la organización para garantizar la disponibilidad operacional. La severidad se clasifica como **crítica**. Se recomienda desarrollar un BIA orientado a los servicios esenciales y, con base en ello, elaborar planes de continuidad y recuperación ante desastres.

3.6.2 Controles relacionados con el personal (A.6)

A.6.3 Capacitación en seguridad de la información

La capacitación en seguridad de la información se lleva a cabo de manera esporádica y no incluye contenidos especializados sobre amenazas a sistemas aeronáuticos ni gestión de incidentes operacionales. Esta brecha limita el nivel de preparación del personal ante riesgos emergentes. La severidad se determina como **media**. Se recomienda implementar un programa anual estructurado, con énfasis en ciberseguridad operacional y manejo de incidentes de alto impacto.

A.6.7 Acuerdos de confidencialidad

Los acuerdos de confidencialidad se aplican únicamente al personal administrativo, excluyendo a operadores de vigilancia, analistas tácticos y personal técnico con acceso a información operativa. Esto representa una brecha significativa en la protección de la información sensible. La severidad se clasifica como **alta**. Se recomienda formalizar acuerdos de confidencialidad para todos los roles con acceso a información crítica.

3.6.3 Controles físicos (A.7)

A.7.4 Control de acceso físico a áreas críticas

Se evidenció que el centro de monitoreo aéreo emplea tarjetas de acceso sin mecanismos de doble autenticación ni registro detallado bajo auditoría. Esta falta de seguridad física en áreas críticas representa una brecha de alto riesgo. La severidad se determina como crítica. Se recomienda la implementación de autenticación multifactor (tarjeta más biometría) y el uso de sistemas de registro automatizado de accesos.

A.7.8 Protección contra amenazas externas y ambientales

No se identificó redundancia energética ni sistemas UPS adecuados para proteger las consolas y equipos operacionales ante interrupciones eléctricas. Esta brecha incrementa la probabilidad de afectaciones operativas. La severidad se clasifica como **alta**. Se recomienda implementar sistemas UPS redundantes y establecer pruebas periódicas de respaldo energético.

3.6.4 Controles tecnológicos (A.8)

A.8.9 Gestión de la configuración

No existe un inventario completo y actualizado de hardware y software asociado a los sistemas radar, servidores de análisis y equipos de comunicaciones críticas. La falta de un control de configuración adecuado puede derivar en fallos no detectados o vulnerabilidades no tratadas. La severidad se determina como **alta**. Se recomienda establecer un inventario centralizado que incluya versiones, niveles de parche y responsables de mantenimiento.

A.8.16 Monitoreo de actividades

Se constató que los registros de auditoría generados por los sistemas de vigilancia no se revisan de forma periódica y que Vigalco no dispone de un sistema de monitoreo centralizado (SIEM). La ausencia de mecanismos efectivos de detección de incidentes constituye una brecha **crítica**. Se recomienda implementar un sistema SIEM, así como definir procedimientos de análisis y correlación de eventos.

A.8.28 Seguridad de las comunicaciones

Algunos enlaces de comunicación operativa carecen de cifrado de extremo a extremo, lo que expone la información a posibles interceptaciones o manipulación. Esta brecha se considera **crítica** debido al carácter sensible de la información transmitida. Se recomienda implementar cifrado robusto en los enlaces internos y externos, junto con el uso de redes privadas virtuales (VPN) y configuraciones de seguridad reforzada en equipos de red. (Ver anexo Brecha Vigalco 1).

Como resultado del análisis de brecha ISO-27001 realizado en la empresa Vigalco en Ecuador, se identificó que, mientras el 23.6 % evidencia un nivel de implementación parcial**.** Finalmente, el 46.2 % de los controles aún no se encuentran implementados**,** lo que refleja la necesidad de fortalecer el Sistema de Gestión de Seguridad de la Información mediante un plan estructurado de implementación y priorización.

Tabla 11

Porcentaje de cumplimiento de controles ISO/IEC 27001.

Estado del control	Cantidad	Porcentaje
Implementado	28	30.1%
Parcialmente implementado.	22	23.6%
No implementado	43	46.2%
Total	**93**	**100 %**

En la tabla 11 de describen el porcentaje de controles: en los implementados, se obtuvo un valor de **30.1 %,** correspondiente a 28 controles. El porcentaje de controles parcialmente implementados alcanzó **23.6 %,** equivalente a 22 controles. Finalmente, el porcentaje de controles no implementados fue de **46.2 %** (43 controles). Estos indicadores muestran un nivel de cumplimiento insuficiente y justifican la necesidad de diseñar un plan de implementación actualizado alineado con los requisitos de la norma ISO-27001.

- Implementados: 28
- Parcialmente implementados: 22
- No implementados: 43
- KPI 1 = 28 / 93 × 100 = **30.1 %**
- KPI 2 = 22 / 93 × 100 = **23.6 %**

Tabla 12

Resultados de los indicadores de cumplimiento ISO/IEC 27001 en Vigalco.

KPI	Descripción	Valor numérico
KPI 1	Porcentaje de controles implementados	**30.1%**
KPI 2	Porcentaje de controles parcialmente implementados	**23.6%**
KPI 3	Porcentaje de controles no implementados	**46.2%**

En la tabla 12 los indicadores muestran que la organización apenas ha dado los primeros pasos hacia un cumplimiento sólido de ISO-27001. Menos de un tercio de los controles se encuentra plenamente aplicado, casi una cuarta parte está a medio camino y cerca de la mitad ni siquiera se ha iniciado, lo que refleja un sistema de seguridad de la

información todavía inmaduro y con huecos importantes. El panorama que dibujan estos porcentajes es el de un proyecto de implementación en marcha, pero que necesita mayor prioridad, recursos y seguimiento para cerrar brechas y transformar los controles parcialmente implementados o inexistentes en prácticas efectivas y sostenidas.

La investigación se limitó a la empresa Vigalco debido a que, para enmarcar los hallazgos, se realizó una revisión documental contra los indicadores clave (operacionales, financieros, de satisfacción) de otras aerolíneas regionales de América Latina. También se puede compensar haciendo una triangulación con fuentes secundarias con datos del sector como: Informes de la Dirección General de Aviación Civil de Ecuador, Estadísticas de la Asociación de Líneas Aéreas Internacionales para la región andina.

En cuanto a la “muestra reducida”, se propone que no se busca representatividad estadística, sino profundidad y diversidad de perspectivas. Se aplicó el principio de saturación teórica en las entrevistas, asegurando la suficiencia de la información cualitativa. Se recomienda replicar este estudio con una muestra ampliada para probar la generalizabilidad de las conclusiones.

3.7 Gestión de sesgos y validación de datos

Para asegurar que el estudio sobre los procesos organizacionales y operativos de Vigalco sea riguroso y confiable, se utilizaron diferentes estrategias metodológicas para identificar, reducir y controlar los posibles sesgos en la información recolectada. Estas medidas buscan equilibrar posibles percepciones subjetivas, interpretaciones favorables de la empresa y limitaciones inherentes a las fuentes primarias y secundarias.

3.7.1 Triangulación de fuentes

Se utilizó un enfoque de triangulación metodológica que combina información proveniente de entrevistas, documentos internos de la empresa, reportes regulatorios, estadísticas sectoriales y observación directa. La convergencia de datos provenientes de

fuentes independientes permitió contrastar afirmaciones y reducir el riesgo de sesgos derivados de perspectivas individuales o institucionales.

3.7.2 Validación externa de información

Los datos proporcionados por la empresa fueron contrastados con información emitida por entidades regulatorias del sector aeronáutico ecuatoriano, tales como la Dirección General de Aviación Civil (DGAC) y el Ministerio de Transporte y Obras Públicas. Esta verificación permitió validar cifras, procedimientos y niveles de cumplimiento normativo, disminuyendo la posibilidad de que los procesos se presenten de manera excesivamente favorable.

3.7.3 Entrevistas a distintos niveles organizacionales

Se llevaron a cabo entrevistas semiestructuradas a actores de diferentes niveles jerárquicos de Vigalco (operativo, técnico, administrativo y directivo). Este enfoque permitió identificar coincidencias y divergencias en las percepciones sobre los procesos, facilitando la detección de posibles sesgos y la construcción de un análisis más equilibrado y objetivo.

4. Análisis de contenido con criterios predefinidos

La información cualitativa obtenida en entrevistas y documentos institucionales fue codificada mediante categorías analíticas previamente establecidas (eficiencia operativa, seguridad, cumplimiento normativo, tiempos de respuesta, entre otras). Esta codificación organizada disminuyó el impacto de opiniones personales y fortaleció la consistencia del análisis, mejorando el alcance y la fiabilidad de los resultados.

3.8 Amenazas a la validez del estudio

En toda investigación aplicada basada en estudios de caso y análisis de brecha normativa, es necesario reconocer las posibles amenazas a la validez de los resultados, así como las estrategias metodológicas adoptadas para mitigarlas. En este estudio, las amenazas a

la validez se analizaron considerando la validez interna, externa y de constructo, conforme a las buenas prácticas en investigación en sistemas de información y gestión de riesgos.

3.8.1 Validez interna

La validez interna se refiere al grado en que los resultados obtenidos reflejan de manera precisa la situación real de la seguridad de la información en la empresa Vigalco, sin distorsiones derivadas de sesgos del investigador, fuentes incompletas o interpretaciones subjetivas.

Amenazas identificadas:

- Dependencia parcial de información proporcionada por entrevistas al personal operativo y administrativo.
- Posible sesgo de deseabilidad organizacional en las respuestas de los entrevistados.
- Limitaciones en el acceso a información clasificada por razones de seguridad aeronáutica.

Medidas de mitigación:

- Aplicación de triangulación de fuentes, combinando entrevistas, revisión documental y observación directa.
- Contraste de la información obtenida con lineamientos y regulaciones de la DGAC (Dirección General de Aviación Civil) aplicables al entorno aeronáutico ecuatoriano.
- Validación cruzada de los hallazgos mediante juicio de expertos certificados en ISO/IEC 27001 y gestión de riesgos, reduciendo la influencia de interpretaciones individuales.

3.8.2 Validez externa

La validez externa hace referencia al grado en que los resultados del estudio pueden ser extrapolados o utilizados como referencia en organizaciones similares.

Amenazas identificadas:

- El estudio se desarrolló como un caso específico, centrado en una empresa dedicada a vigilancia, alerta y control aéreo.
- Las condiciones operativas, regulatorias y tecnológicas de Vigalco pueden diferir de otras organizaciones de distintos sectores.

Medidas de mitigación:

- Enfoque del análisis sobre controles y requisitos generales de la norma ISO/IEC 27001, de aplicación transversal a múltiples organizaciones.
- Descripción detallada del contexto organizacional y operativo, permitiendo que otros investigadores evalúen la transferibilidad de los resultados.
- Comparación de los hallazgos con trabajos previos y marcos normativos internacionales, fortaleciendo la utilidad del estudio como referencia metodológica más que como generalización estadística.

3.8.3 Validez de constructo

La validez de constructo se relaciona con el grado en que los instrumentos y métricas utilizados realmente miden los conceptos que se pretende evaluar, como nivel de cumplimiento, madurez de controles y riesgo residual.

Amenazas identificadas:

- Uso de escalas ordinales para la valoración de controles y riesgos.
- Ausencia de métricas cuantitativas post-implementación para medir directamente la reducción del riesgo residual.

Medidas de mitigación:

- Utilización de instrumentos alineados explícitamente con ISO/IEC 27001:2022, ISO 27005 y MAGERIT v3, garantizando coherencia conceptual.
- Definición clara de criterios de cómputo, escalas y reglas de aceptación, documentadas en la metodología.

- Incorporación de una mini-evaluación piloto pre–post mediante indicadores clave (KPIs y KRIs) propuestos, que permiten la medición futura del desempeño del SGSI, aun cuando su aplicación completa exceda el alcance temporal del presente estudio.

3.9 Riesgo residual en Vigalco

El riesgo residual corresponde al nivel de riesgo que permanece después de implementar los controles existentes en la organización. En el caso de Vigalco, que se encarga de la vigilancia, alerta y control aéreo, este tema es crucial porque sus servicios son esenciales. Si hay problemas como la falta de disponibilidad, cambios o filtraciones de información, esto puede poner en riesgo la seguridad aérea del país.

El análisis de riesgo residual se desarrolló tomando como referencia:

- Las brechas identificadas en los controles de la Norma ISO/27001:2022; los activos críticos asociados a la operación (radares, sistemas de comunicaciones, servidores analíticos, centro de monitoreo, infraestructura física y personal especializado); y la evaluación del nivel de exposición una vez considerados los controles actualmente implementados.

La aceptación formal de los riesgos residuales se documenta mediante un acta de aprobación institucional. El formato propuesto para dicha aceptación, incluyendo responsables, condiciones y periodicidad de revisión, se presenta en el Anexo 12.

3.9.1 Conceptualización del riesgo residual

En un SGSI, el riesgo residual se determina como:

Riesgo residual = Riesgo inherente – Efectividad de los controles existentes

Donde:

- El riesgo inherente representa el riesgo existente antes de aplicar cualquier control.
- La efectividad de los controles se basa en su diseño, implementación, evidencia y desempeño real.

- El riesgo residual es fundamental para la toma de decisiones en entornos operativos complejos como Vigalco, ya que permite identificar si los controles actuales son suficientes para mantener la seguridad operacional o si se requieren medidas adicionales.

3.9.2 Evaluación del riesgo residual en Vigalco

El análisis mostró que, aunque Vigalco tiene algunos controles operativos y tecnológicos básicos, aún hay altos y críticos riesgos residuales. Esto se debe a problemas estructurales, a la falta de controles más avanzados y a la inmadurez en los procesos formales de seguridad de la información.

Los riesgos residuales más significativos se agrupan en las siguientes áreas:

- **Riesgo residual en continuidad operativa**

  Vigalco no cuenta con un Análisis de Impacto en el Negocio (BIA) ni con planes formales de continuidad o recuperación ante desastres. Aunque existen soluciones técnicas aisladas (UPS básico, redundancia parcial), su cobertura es limitada.

  - Riesgo residual: Crítico
  - Impacto: Interrupción total o parcial de la capacidad de vigilancia aérea.
  - Motivo: Controles insuficientes para garantizar disponibilidad continua en sistemas de misión crítica.

- **Riesgo residual en comunicaciones y redes**

  Las brechas identificadas en cifrado, segmentación y monitoreo generan un riesgo residual significativo. Incluso con controles básicos (firewalls y antivirus), la falta de SIEM, IDS/IPS y cifrado intermedio deja expuestos sistemas de alto valor.

  - Riesgo residual: Crítico
  - Impacto: Intercepción de información operativa, ataques dirigidos, manipulación de datos.
  - Motivo: Controles tecnológicos avanzados no implementados.

- **Riesgo residual en ciberseguridad del personal**

  El personal operativo no recibe capacitación sistemática ni especializada en amenazas aeronáuticas, lo que disminuye la capacidad de respuesta frente a incidentes.

  - Riesgo residual: Alto
  - Impacto: Error humano, manipulación social, brechas no detectadas.
  - Motivo: Falta de formación continua y acuerdos de confidencialidad incompletos.

- **Riesgo residual en seguridad física**

  El centro de monitoreo aéreo cuenta con controles de acceso limitados (sin biometría ni registros auditables). Aunque existen cerramientos y CCTV, la correlación y supervisión son limitadas.

  - Riesgo residual: Alto
  - Impacto: Acceso no autorizado a áreas críticas.
  - Motivo: Insuficiencia de mecanismos de autenticación y trazabilidad.

- **Riesgo residual en gestión de proveedores**

  La falta de evaluación de riesgos y supervisión de proveedores que administran equipos sensibles mantiene un riesgo residual elevado, incluso cuando existen contratos de servicio.

  - Riesgo residual: Alto
  - Impacto: Dependencia vulnerable, manipulación o fallo en infraestructura crítica.
  - Motivo: Ausencia de controles de seguridad en relaciones contractuales.

3.10 Matriz general del riesgo residual

Tabla 13
Clasificación del nivel de riesgos residual.

Dominio evaluado	Riesgo inherente	Controles existentes	Riesgo residual
Continuidad del negocio	Muy alto.	Bajo	Crítico

Redes y comunicaciones	Alto	Moderado	Crítico
Seguridad del personal	Medio	Bajo	Alto
Seguridad física	Medio	Moderado	Alto
Proveedores	Alto	Bajo	Alto
Gestión documental	Medio	Moderado	Medio
Gestión de activos	Alto	Moderado	Alto

Fuente: Elaborado por el autor.

La tabla 13 muestra que, aun después de aplicar los controles actuales, varios dominios clave siguen quedando con un riesgo importante. En continuidad del negocio y en redes y comunicaciones, el riesgo residual se mantiene en nivel crítico, lo que evidencia que las medidas vigentes son insuficientes para compensar el riesgo inherente muy alto o alto de estos ámbitos. En áreas como seguridad del personal, seguridad física, proveedores y gestión de activos, el riesgo baja a “alto”, mientras que solo la gestión documental alcanza un riesgo residual medio, lo que sugiere que allí los controles son relativamente más efectivos y consistentes.

3.11 Interpretación de resultados

El riesgo residual persiste principalmente en aquellos procesos que involucran:

- Infraestructura crítica
- Operaciones continuas 24/7
- Dependencia de terceros
- Procesos no formalizados o no auditados
- Falta de monitoreo continuo

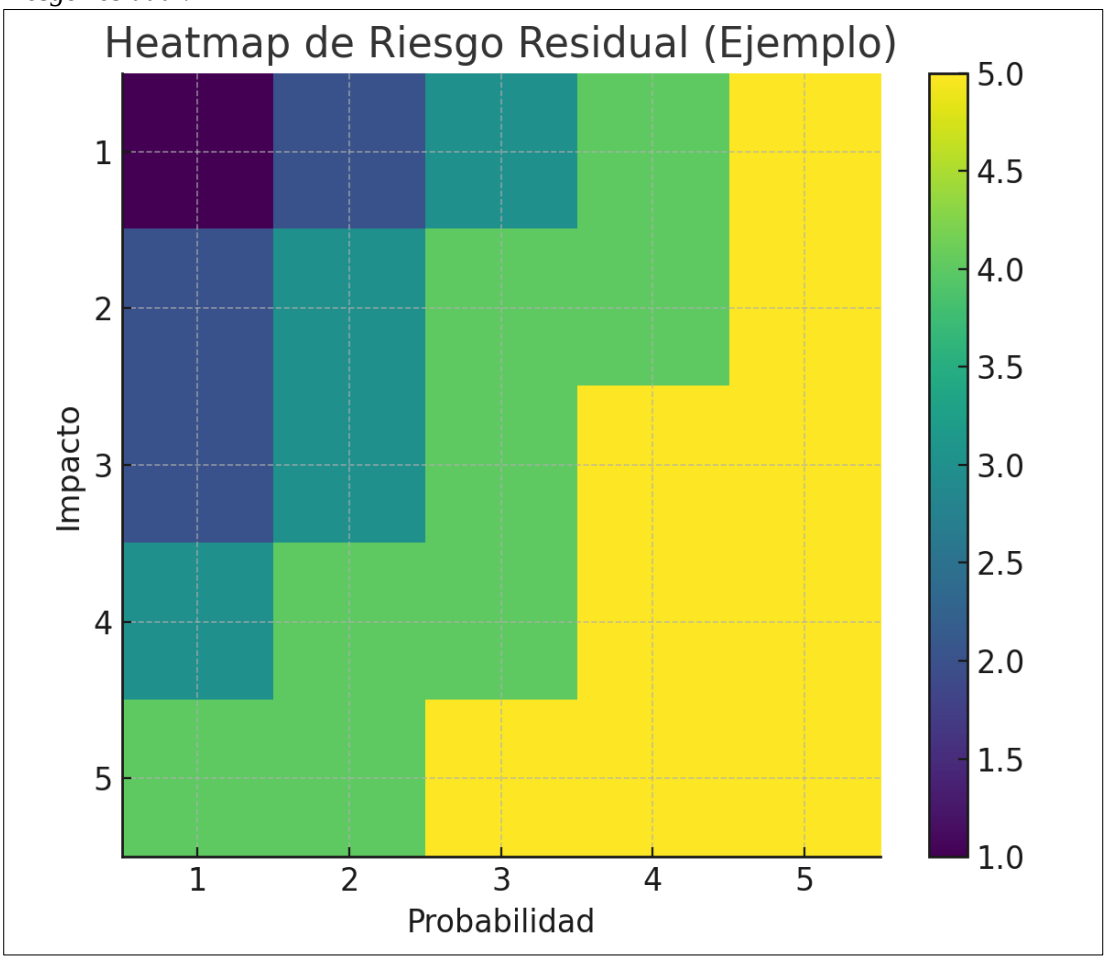
En este contexto, el riesgo residual refleja una madurez baja a media del SGSI, lo que justifica la necesidad de implementar un plan de tratamiento priorizado y orientado al fortalecimiento de controles tecnológicos, organizacionales y operativos.

- Relevancia para la toma de decisiones
- El análisis del riesgo residual permite a Vigalco:
- Priorizar inversiones en seguridad.
- Determinar qué controles son urgentes y cuáles pueden esperar.
- Evaluar la necesidad de fortalecer la protección de sistemas militares o aeronáuticos.
- Soportar auditorías internas y externas.
- Sustentar la futura certificación ISO/IEC 27001.

En resumen, la evaluación del riesgo residual muestra que Vigalco necesita mejorar mucho su seguridad, sobre todo en continuidad operativa, monitoreo, cifrado, gestión de proveedores y protección física en áreas cruciales.

Figura 2

Riesgo residual.



3.12 Validación de mejoras

La validación de mejoras constituye una etapa fundamental dentro del análisis de brechas, ya que permite verificar que las medidas correctivas implementadas para subsanar las deficiencias identificadas sean efectivas y cumplan con los requisitos de la Norma ISO/IEC 27001. Su objetivo principal es asegurar que los controles actualizados proporcionen la protección necesaria a la información crítica de la empresa y contribuyan al fortalecimiento de la seguridad de la información.

Para ello, se emplea una metodología basada en la revisión documental, la ejecución de pruebas de control, la realización de entrevistas o encuestas al personal responsable de los procesos, así como la medición de indicadores de desempeño relevantes, tales como el número de incidentes reportados, el tiempo de respuesta ante incidentes y el nivel de cumplimiento de los controles revisados. El procedimiento consiste en seleccionar las brechas críticas identificadas, aplicar las mejoras correspondientes, ejecutar pruebas de funcionamiento de los nuevos controles, registrar evidencias de cumplimiento y evaluar los resultados frente a los criterios establecidos por la ISO/IEC 27001.

Esta evaluación permite determinar la efectividad de cada medida y, en caso de detectar deficiencias, ajustar las acciones correctivas. Los resultados esperados incluyen la reducción de brechas críticas y moderadas, una mayor alineación con los requisitos de la norma y un incremento en la madurez de seguridad de la organización.

En resumen, validar las mejoras asegura que los controles no solo sigan las normas de seguridad, sino que también sean sostenibles, medibles y basados en pruebas. Esto ayuda en futuras auditorías y en tomar decisiones estratégicas sobre la seguridad de la información.

El análisis realizado con la Matriz de Brechas, Mejoras y Resultados mostró solo cuatro casos de validación (B01;B04). No incluyó un estudio cuantitativo que comparara el rendimiento antes y después de aplicar los controles sugeridos. Esto se debió a que, al

momento del estudio, no existían registros sistemáticos que permitieran establecer una línea base cuantitativa ni datos posteriores a la aplicación de las mejoras.

El inventario de activos utilizado fue limitado, incluyendo solo un subconjunto de los activos críticos de la empresa; aunque se identificaron y validaron mejoras para estas brechas, futuros estudios deberían ampliar el inventario para cubrir todas las instalaciones y recursos críticos, incluyendo hardware, software, infraestructura, servicios y personal clave.

En segundo lugar, no se contó con métricas de desempeño cuantitativas posteriores a la implementación de las mejoras, lo que impide evaluar objetivamente su efectividad y la reducción del riesgo residual. Se recomienda que futuras investigaciones adopten un esquema de medición pre-post mediante indicadores específicos para cada activo y brecha. Finalmente, el estudio no incluyó análisis estadístico para validar la significancia de los hallazgos; se sugiere aplicar pruebas estadísticas apropiadas, como t-test, chi-cuadrado o análisis de correlación, para determinar de manera cuantitativa el impacto de las mejoras y la efectividad de los controles implementados.

Tabla 14

Matriz de priorización de controles críticos

Control ISO 27001	Descripción resumida	Criticidad del activo	Nivel de riesgo	Dependencia operativa	Puntaje total	Prioridad
A.8.20	Seguridad de redes	Alta [3]	Alta [3]	Alta [3]	9	Muy alta
A.8.21	Seguridad de servicios de red	Alta [3]	Alta [3]	Media [2]	8	Muy alta
A.5.15	Control de accesos	Alta [3]	Media [2]	Alta [3]	8	Muy alta
A.5.24	Gestión de incidentes	Media [2]	Alta [3]	Alta [3]	8	Muy alta
A.8.16	Monitoreo de actividades	Media [2]	Alta [3]	Alta [3]	8	Muy alta
A.8.13	Respaldo de la información	Alta [3]	Media [2]	Media [2]	7	Alta

A.6.3	Concienciación y formación	Media [2]	Media [2]	Alta [3]	7	Alta
A.5.9	Inventario de información	Media [2]	Media [2]	Media [2]	6	Media
A.7.4	Protección física	Media [2]	Media [2]	Media [2]	6	Media
A.5.1	Políticas de seguridad	Media [2]	Baja [1]	Alta [3]	6	Media

La tabla 14 ordena los controles de ISO-27001 según la urgencia con la que deberían ser atendidos dentro de la organización. En la parte alta de la lista aparecen los controles de seguridad de redes, seguridad de servicios de red, control de accesos, gestión de incidentes y monitoreo de actividades, todos con puntajes elevados y prioridad “muy alta”, porque combinan activos críticos, riesgos significativos y una fuerte dependencia operativa de ellos. En un segundo plano quedan controles como respaldo de la información, concienciación y formación, inventario de información, protección física y políticas de seguridad, que, aunque siguen siendo importantes, se clasifican con prioridad “alta” o “media”, lo que indica que su implementación puede planificarse de forma escalonada una vez asegurados los controles más sensibles.

Tabla 15

Top 10 controles priorizados para comunicaciones

Control ISO	Iniciativa	Horizonte	Justificación
A.8.20	Fortalecer seguridad de red	Quick win	Alto impacto y baja complejidad técnica
A.5.15	Control de accesos	Quick win	Reduce riesgo inmediato de intrusión
A.5.24	Gestión de incidentes	Quick win	Mejora tiempos de respuesta
A.6.3	Capacitación del personal	Quick win	Bajo costo y alta efectividad
A.8.16	Monitoreo de eventos	Mediano plazo	Requiere herramientas especializadas
A.8.21	Seguridad de servicios de red	Mediano plazo	Ajustes técnicos y contractuales

A.8.13	Gestión de respaldos	Mediano plazo	Pruebas y automatización
A.5.9	Inventario de información	Mediano plazo	Requiere levantamiento detallado
A.7.4	Protección física	Mediano plazo	Inversión en infraestructura
A.5.1	Formalización de políticas	Mediano plazo	Aprobación institucional

La tabla 15 presenta de forma muy concreta, por dónde empezar a mejorar la seguridad en comunicaciones. Primero se propone ir a por los “golpes rápidos”: reforzar la seguridad de la red, ajustar mejor los accesos, pulir la gestión de incidentes y entrenar al personal, porque son cambios relativamente sencillos que reducen el riesgo de inmediato. Después, ya a mediano plazo, quedan las tareas más pesadas: montar un monitoreo más avanzado, robustecer los servicios de red, automatizar respaldos, levantar bien el inventario de información, mejorar la protección física y dejar las políticas formalmente aprobadas, todo ello exige más presupuesto, tecnología específica y el visto bueno de la organización.

3.13 Cronograma de implementación

Tabla 16

Plan de mejoras y seguimientos de controles ISO/IEC 27001.

Actividad/Mejora	Responsable	Fecha de inicio	Fecha de fin	Indicador de seguimiento
Selección de brechas críticas identificadas	Responsable de Seguridad de la Información	15/12/2025	20/12/2025	Lista de brechas priorizadas
Aplicación de mejoras y controles correspondientes.	Equipo de Seguridad de la Información / TI	21/12/2025	10/01/2026	% de controles implementados según plan
Ejecución de pruebas de funcionamiento de controles	Auditor interno / Responsable de procesos	11/01/2026	25/01/2026	Número de pruebas exitosas/fallidas
Registro de evidencias de cumplimiento	Responsable de Documentación / Seguridad de la Información	26/01/2026	30/01/2026	Evidencias documentadas y archivadas
Evaluación de resultados frente a criterios ISO/IEC 27001	Auditor interno / Responsable de seguridad	31/01/2026	05/02/2026	Informe de efectividad de controles

Ajuste de acciones correctivas según resultados	Equipo de Seguridad de la Información	06/02/2026	15/02/2026	Reducción de brechas críticas y moderadas
Medición de indicadores de desempeño (incidentes, tiempo de respuesta, cumplimiento de controles)	Responsable de Seguridad / Calidad	16/02/2026	28/02/2026	Reporte comparativo de indicadores postmejoras

La tabla 16 arma, prácticamente paso a paso, el plan para poner en marcha y revisar los controles ISO-27001 dentro de un periodo concreto de tiempo. Desde mediados de diciembre se parte por seleccionar las brechas críticas, aplicar las mejoras, probar que los controles realmente funcionan y dejar evidencia documentada de todo lo que se va haciendo. A continuación, ya a finales de enero y durante febrero, se analiza si los controles dieron resultado, se ajustan las acciones donde haga falta y se miden indicadores como incidentes o tiempos de respuesta, de modo que al final no solo se hayan aplicado cambios, sino que quede claro, con datos, cuánto mejoró la seguridad de la información.

Con base en los resultados del análisis de brecha respecto a la norma ISO27001:2022, se elaboró un plan de acción orientado a operacionalizar las iniciativas de mejora priorizadas. Este plan establece la relación entre cada iniciativa, el indicador de desempeño afectado, el responsable de su ejecución, el horizonte temporal y la evidencia objetiva esperada, permitiendo el seguimiento y control de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

Tabla 17

Plan de acción derivado del análisis de brecha

Iniciativa	Control ISO/IEC 27001	Indicador afectado (KPI/KRI)	Responsable	Fecha objetivo	Evidencia esperada
Formalización de la política de seguridad de la información	A.5.1	% de políticas aprobadas y comunicadas	Gerencia / Responsable SGSI	3 meses	Política aprobada, acta de difusión
Implementación de control de accesos lógicos	A.8.2	Nº de accesos no autorizados detectados	Área de TI	4 meses	Registros de acceso, bitácoras

Capacitación en seguridad de la información	A.6.3	% de personal capacitado	Talento humano	2 meses	Listas de asistencia, material
Gestión de respaldos y restauración	A.8.13	% de restauraciones exitosas	Área de TI	3 meses	Reportes de pruebas de backup
Gestión de incidentes de seguridad	A.5.24	Tiempo promedio de respuesta a incidentes	Responsable SGSI	4 meses	Registro de incidentes
Revisión periódica de riesgos	A.5.9	% de riesgos reevaluados	Comité SGSI	6 meses	Informes de revisión

La tabla 17 baja el análisis de brechas a un plan de trabajo muy concreto, con responsables claros y plazos definidos. En esencia, plantea formalizar la política de seguridad, mejorar el control de accesos lógicos, capacitar al personal, robustecer los respaldos, afinar la gestión de incidentes y revisar periódicamente los riesgos, todo con metas que van de tres a seis meses y con evidencias tangibles como políticas aprobadas, bitácoras de acceso, listas de asistencia, reportes de backup y actas de revisión.

Tabla 18

Matriz de brechas, mejoras y resultados.

ID de Brecha	Brecha identificada	Mejora implementada	Evidencia de validación	Resultado	Riesgo residual estimado
B01	Falta de control de acceso físico a la sala de servidores	Instalación de control de acceso con tarjeta magnética y registro de entradas	Fotos del sistema, registros de acceso durante 1 mes.	Validado: control funcionando y registros auditables.	Reducción estimada: 80-90% de accesos no autorizados mitigados
B02	No existe política de gestión de contraseñas.	Redacción e implementación de política de contraseñas según ISO/IEC 27001	Documento de política aprobado, capacitaciones realizadas.	Validado: personal capacitado y política aplicada	Reducción estimada: 70-85% de incidentes relacionados con contraseñas.
B03	Respaldo de información crítico no probado	Configuración de backup automático y pruebas mensuales de restauración	Reportes de pruebas de restauración exitosas	Validado: respaldo funcionando correctamente.	Reducción estimada: 75-90% riesgo de pérdida de información crítica.

B04	Falta de concienciación del personal sobre seguridad	Capacitación en seguridad de la información y campañas de sensibilización	Listas de asistencia, cuestionarios postcapacitación	Validado: respaldo funcionando correctamente.	Reducción estimada: 60-80% de errores humanos por falta de concienciación.
B05	Procedimientos de respuestas a Incidentes no documentados	Creación de procedimientos de gestión de incidentes y simulacros	Documento de procedimientos, registro de simulacros	Validado: procedimientos aplicables y personal entrenado	Reducción estimada: 65–85% del riesgo operativo por incidentes.

Fuente: Elaborada por el autor.

La tabla 18 muestra la Matriz de Brechas, Mejoras y Resultados ayudó a confirmar mejoras para las brechas B01 a B05 usando documentos y pruebas operativas, como registros de acceso, informes de respaldo, capacitaciones y procedimientos. Sin embargo, no hay métricas cuantitativas después de la implementación. Estas métricas no permiten evaluar objetivamente la efectividad de cada control ni la reducción del riesgo residual. Esto limita la posibilidad de verificar el impacto real de las mejoras en la operación de la empresa.

Es importante aclarar que los porcentajes de cumplimiento presentados corresponden a universos de evaluación distintos dentro de la Norma ISO-27001**.**

El 30,1 % de cumplimiento (28 de 93 controles) se refiere exclusivamente al nivel de implementación de los controles de seguridad de la información definidos en el Anexo A**,** aplicables al contexto de la empresa VIGALCO. Este resultado refleja el estado actual de los controles operativos y técnicos del SGSI al momento del levantamiento de información.

Por otro lado, el 76 % de cumplimiento presentado en la tabla integrada corresponde a la evaluación de los requisitos del cuerpo normativo de la ISO/IEC 27001 **(Cláusulas 4 a 10)**, los cuales abarcan aspectos de contexto organizacional, liderazgo, planificación, soporte, operación, evaluación del desempeño y mejora continua.

En consecuencia, ambos valores no representan un escenario de “antes y después”, sino dimensiones complementarias del nivel de madurez del SGSI**,** siendo el menor porcentaje un indicador de la brecha existente en la implementación de controles de

Tabla 19

Tabla integrada de cumplimiento de controles y exposición al riesgo

Indicador	Tipo	Meta/Umbral	Resultado 2024	Cumplimiento	Comentarios
KPI 1: % de controles implementados	KPI	≥ 80%	76%	Parcial	La brecha indica necesidad de fortalecer planeación y supervisión.
KPI 2: % de controles parcialmente implementados	KPI	≤ 15%	18%	No cumple.	La alta proporción refleja falta de madurez en implementación.
KRI 1: Activos con riesgo alto	KRI	≤ 10	14	No cumple.	Indica exposición significativa a incidentes operativos o de seguridad.
KRI 2: Nivel promedio de riesgo por dominio	KRI	≤ 3.0	3.4	No cumple.	Deben priorizarse dominios con mayor intensidad.

En la tabla 19 los resultados muestran que, aunque las mejoras implementadas ayudaron a mejorar un poco la gestión de controles, todavía hay diferencias significativas que dificultan la reducción del riesgo en la organización. El porcentaje de controles que se han implementado muestra progreso en comparación con la situación inicial. Sin embargo, el número de controles que se han implementado solo parcialmente sigue siendo alto, lo que indica que las acciones para mejorar no han sido completamente adoptadas en todos los procesos evaluados. Sobre los indicadores de riesgo, el número de activos con alto riesgo sigue siendo mayor de lo que se esperaba. Esto muestra que las acciones tomadas no han sido suficientes para reducir efectivamente la exposición al riesgo.

3.14 Comparación con trabajos previos e implicaciones prácticas

El presente estudio se distingue de investigaciones previas sobre la implementación de ISO/IEC 27001 en empresas del sector aeronáutico y de vigilancia por su enfoque en la empresa ecuatoriana Vigalco, dedicada a vigilancia, alerta y control aéreo. Al comparar los resultados con investigaciones previas, se nota que, al igual que en estudios de la región y del

mundo, las principales deficiencias están en la gestión de incidentes, la sensibilización del personal y el control de accesos cruciales.

Sin embargo, a diferencia de otros estudios que indican que implementar cambios puede ser muy costoso y tomar mucho tiempo, en Vigalco la adopción de mejoras ha mostrado un equilibrio bastante positivo entre la inversión, el tiempo y los resultados. Esto se debe a la forma en que está organizada la empresa y a la importancia que se les da a los controles esenciales.

Investigaciones sobre el tema evidencian que un SGSI basado en ISO/IEC 27001 resulta eficaz para estructurar la gestión de riesgos de información en organizaciones con dinámicas de riesgo elevadas *[12]*. Otro criterio utiliza un enfoque que combina métodos cualitativos y cuantitativos para evaluar la madurez del sistema. Esto ayuda a identificar cuán cerca está una organización de cumplir completamente y dónde tiene deficiencias [13].

Desde el punto de vista práctico, la aplicabilidad de los controles implementados se refleja en la capacidad de la empresa para reducir riesgos de seguridad de manera medible, fortaleciendo la confidencialidad, integridad y disponibilidad de la información. La evaluación de la madurez organizacional muestra que, aunque Vigalco ha cerrado varias brechas significativas, todavía necesita establecer procedimientos formales y asegurar que la capacitación del personal sea continua. Estos puntos coinciden con lo que se encontró en estudios anteriores de empresas similares.

Asimismo, el trabajo sobre la implementación de la norma ISO/IEC 27001 en Ecuador resulta relevante para esta tesis, ya que aborda la adopción de un SGSI en una organización con características similares a las de Vigalco *[14]*. Los autores destacan la identificación de activos críticos, la evaluación de riesgos y la aplicación de controles para garantizar la seguridad de la información, así como desafíos comunes como la capacitación del personal y la adaptación de procesos internos. Este trabajo permite contextualizar los

hallazgos de la presente investigación dentro de experiencias previas en el país, reforzando la factibilidad de aplicar controles ISO/IEC 27001 en entornos críticos de vigilancia aérea.

En términos de **coste**, las mejoras implementadas han requerido inversión en sistemas de control de acceso, herramientas de respaldo y capacitación, con un retorno en términos de reducción de riesgos y preparación para auditorías. Respecto al **tiempo**, las acciones correctivas se aplicaron de forma escalonada, priorizando controles de mayor criticidad, lo que permitió avances acelerados en áreas críticas sin afectar la operatividad de la empresa.

Al finalizar la evaluación de madurez, se observa que Vigalco está en un nivel intermedio de cumplimiento con ISO/IEC 27001. Esto es similar a otras organizaciones de su tamaño y sector. Además, tiene la posibilidad de mejorar continuamente a través de auditorías regulares y cambios en sus procesos de gestión de seguridad.

Al comparar los patrones de brecha identificados en Vigalco con los reportados en estudios previos sobre implementación de ISO/IEC 27001 en organizaciones críticas, se observa una coincidencia significativa en varias áreas clave. Las brechas más frecuentes se relacionan con la gestión de incidentes, el control de accesos críticos y la concienciación del personal sobre seguridad de la información.

Sin embargo, el análisis hecho en Vigalco proporciona pruebas específicas sobre el sector de vigilancia aérea en Ecuador. Muestra cómo estas deficiencias aparecen en un entorno de trabajo concreto, donde es muy importante mantener las operaciones y proteger información sensible.

Además, la verificación de las mejoras realizadas en la empresa muestra que es posible aplicar los controles de ISO/IEC 27001 de manera práctica, adaptándolos a las condiciones locales, como las restricciones de tiempo, recursos y el nivel de desarrollo de la organización. Este caso no solo confirma patrones que se han reportado antes, sino que también presenta algo nuevo al mostrar que las estrategias de mitigación son efectivas en un

contexto nacional y sectorial específico. Esto puede ser útil como referencia para futuras implementaciones en organizaciones parecidas.

Con el objetivo de complementar el análisis de brecha y validar de manera preliminar la viabilidad operativa del plan de implementación propuesto, se realizó una **mini-evaluación piloto pre–post** basada en un conjunto acotado de indicadores clave de desempeño (KPIs) del Sistema de Gestión de Seguridad de la Información.

Esta evaluación no tiene como finalidad medir la efectividad definitiva del SGSI ni la reducción concluyente del riesgo residual, sino **proporcionar evidencia inicial y objetiva** sobre la aplicabilidad de las medidas propuestas en un entorno controlado y en un periodo limitado.

Tabla 20

Indicadores utilizados en la evaluación piloto

KPI	Descripción	Método de recolección	Fuente	Periodicidad
Restauraciones exitosas (%)	Porcentaje de respaldos restaurados correctamente	Pruebas de restauración	Registros TI	Semanal
MTTR (horas)	Tiempo medio de respuesta a incidentes	Registro de incidentes	Mesa de ayuda	Mensual
Eventos de acceso no autorizado	Número de intentos fallidos o bloqueados	Logs de seguridad	SIEM / Firewall	Mensual
Cumplimiento de política de contraseñas (%)	Usuarios que cumplen política	Auditoría de credenciales	AD / RRHH	Mensual
Incidentes reportados	Incidentes de seguridad registrados	Reportes formales	SGSI	Mensual

Fuente: Elaboración propia.

La tabla 20 define los indicadores con los que se va a “tomar el pulso” a la seguridad durante la evaluación piloto. Se incluyen métricas sobre qué porcentaje de respaldos se restaura bien, cuánto tiempo se tarda en atender incidentes, cuántos intentos de acceso no autorizado se registran, qué tanto se cumple la política de contraseñas y cuántos incidentes de

seguridad llegan a reportarse formalmente. Cada KPI tiene claramente indicado de dónde salen los datos (pruebas de restauración, registros de incidentes, logs de seguridad, auditorías de credenciales y reportes del SGSI) y con qué frecuencia se revisan, combinando mediciones semanales y mensuales para mantener una vigilancia constante sin saturar al equipo.

3.15 Limitaciones

El presente estudio presenta limitaciones asociadas al alcance, la muestra y posibles sesgos, las cuales deben considerarse al interpretar los resultados. En cuanto al alcance, la investigación se centró únicamente en la empresa Vigalco, dedicada a vigilancia, alerta y control aéreo en Ecuador, lo que restringe la generalización de los hallazgos a otras organizaciones del sector o a contextos internacionales.

Respecto a la muestra, el análisis se basó en un conjunto limitado de procesos, áreas críticas y personal clave disponible durante el período de estudio, lo que pudo dejar fuera algunos aspectos operativos y tecnológicos relevantes para la seguridad de la información.

Finalmente, en relación con los sesgos, es posible que la información proporcionada por el personal y los registros internos estuvieran influenciados por percepciones subjetivas. También podrían estar influenciados por la intención de presentar los procesos de forma más favorable, así como por la experiencia previa de los investigadores en el área de seguridad de la información.

Reconocer estas limitaciones ayuda a entender los resultados con cuidado y resalta la necesidad de más investigaciones que amplíen el alcance, incluyan muestras más representativas y usen métodos que disminuyan los sesgos en la recolección de información.

CAPÍTULO 4

4.1 Conclusiones y recomendaciones

4.1.1 Conclusiones

Tras aplicar las fases necesarias de la propuesta, se obtienen las siguientes conclusiones primordiales:

1. En relación con el objetivo general, se logró analizar la brecha entre la situación actual de la empresa Vigalco y los requisitos de la norma ISO/IEC 27001, y a partir de ello se diseñó un plan de implementación actualizado que integra una matriz de cumplimiento, una matriz de brechas y una matriz de plan de mejoras priorizadas.
2. El primer objetivo específico se cumplió mediante la elaboración de la Matriz de Cumplimiento, donde se determinó el nivel de aplicación de las cláusulas y controles de la norma ISO/IEC 27001 en Vigalco. El segundo objetivo específico se alcanzó con la construcción de la Matriz de Brechas, que permitió identificar los controles parcialmente implementados o no implementados y la distancia respecto a los requisitos de la norma. El tercer objetivo específico se cumplió al proponer la Matriz de Plan de Mejoras, en la que se priorizan acciones concretas para cerrar las brechas identificadas y fortalecer el SGSI de la institución.
3. La evaluación realizada con la Matriz de Cumplimiento ayudó a ver cómo se están usando las cláusulas y controles de seguridad que establece la norma ISO/IEC 27001 en la institución responsable de la vigilancia, alerta y control aéreo. Los resultados evidenciados muestran que, si bien algunos controles están implementados de manera parcial o total, persisten brechas significativas en áreas críticas como la gestión de incidentes, control de accesos y concienciación del personal.
4. La creación de la Matriz de Brechas ayudó a identificar de manera clara las fallas en la seguridad de la información y cómo se está lejos de cumplir con los requisitos y controles de la norma ISO/IEC 27001.

5. La elaboración de la Matriz de Plan de Mejoras ayudó a sugerir varias acciones específicas para solucionar las diferencias identificadas y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) de la institución, cumpliendo con los requisitos de la norma ISO/IEC 27001.

4.1.2 Recomendaciones

Al culminar lo planificado en la propuesta, se obtienen las siguientes recomendaciones primordiales:

1. Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a ISO/IEC 27001, priorizando los controles del Anexo A aplicables a comunicaciones, acompañado de un proceso continuo de gestión de riesgos que incluya auditorías periódicas y actualizaciones frente a nuevas amenazas. Esta acción se considera un proyecto de mediano a largo plazo, debido a los recursos necesarios para la formalización del SGSI, la capacitación del personal, la adquisición de herramientas y la integración de procedimientos de monitoreo.
2. Los beneficios esperados incluyen la mejora integral de la seguridad de la información, la reducción de incidentes y vulnerabilidades, el cumplimiento con los requisitos de la norma y la preparación para auditorías o certificaciones externas.
3. Optimizar la infraestructura tecnológica y aprovechar la certificación ISO/IEC 27001 como elemento diferenciador en el mercado, mediante la inversión en sistemas de cifrado, segmentación de redes y monitoreo en tiempo real. Los beneficios esperados incluyen el fortalecimiento de la seguridad de la información, la reducción de riesgos asociados a accesos no autorizados y ataques cibernéticos, así como el aumento de la competitividad institucional al demostrar a clientes y autoridades regulatorias el compromiso con estándares internacionales de seguridad.

4. Las investigaciones futuras podrían enfocarse en un análisis exhaustivo del impacto que la digitalización, la inteligencia artificial y los sistemas avanzados de gestión aeronáutica generan en la eficiencia operativa, la seguridad y la optimización de recursos organizacionales. También sería pertinente profundizar en el desarrollo y evaluación de marcos técnicos y metodológicos orientados al fortalecimiento de la resiliencia institucional mediante la implementación de planes de contingencia, continuidad operacional y respuesta ante escenarios de crisis externas.
5. Como limitación de la investigación, se plantea que se enfocó esencialmente en Vigalco, sin incluir un análisis profundo del ecosistema aeronáutico ecuatoriano. Por consiguiente, se insta a que se desarrollen futuras investigaciones que puedan integrar datos de competidores, regulaciones, infraestructuras aeroportuarias y dinámicas del mercado nacional/internacional.
6. Aunque este estudio se centró en analizar los procesos internos de Vigalco, no examinó en detalle el ecosistema aeronáutico de Ecuador. Esto limita la capacidad de entender completamente los hallazgos en relación con las dinámicas del sector en el país. Esta restricción responde al alcance metodológico definido y a la priorización de la información disponible sobre la operación interna de la empresa.
7. Para superar esta limitación, en el futuro se podrán hacer estudios más amplios en diferentes sectores. Estos estudios incluirán diagnósticos de las reglas que rigen el sector, análisis del entorno general, comparaciones entre regiones y opiniones de expertos del sector. Además, crear indicadores que se midan a lo largo del tiempo y evaluar el impacto de las políticas públicas ayudará a entender mejor las condiciones que afectan a la industria aeronáutica en Ecuador y mejorará el análisis de empresas como Vigalco.

Referencias Bibliográficas

[1] E. Humphreys, An introduction to Information Security Management Systems, Reino Unido: BSI, 2022.

[2] A. G. Blokdyk, Redes de alta disponibilidad: una guía completa, Starcooks, 2020.

[3] «Informe del Foro Económico Mundial-Global Cybersecurity Outlook», 2022. [En línea]. Available: http://www.weforum.org/reports/global.

[4] «Fiscalía General del Estado de Ecuador», Informe estadístico de delitos informáticos 2017-2021, 2021.

[5] M. E. Whitman and H. J. Mattord, Principles of Information Security, 7th ed. Boston, MA: Cengage Learning, 2021.

[6] National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800-53, Revision 5. Gaithersburg, MD: NIST, 2020.

[7] C. P. Pfleeger and S. L. *Pfleeger, Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach*. Upper Saddle River, NJ: Pearson Education, 2015.

[8] M. Whitman y H. Mattord, «Principios de seguridad en infraestructuras críticas», 2012. [En línea]. Available: http://almuhammadi.com/sultan/sec_books/Whitman.pdf.

[9] A. Avizienis, J.-C. Laprie, B. Randell y C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Dependable Secur. Comput*., vol. 1, no. 1, pp. 11-33, Jan.-Mar. 2004, doi: 10.1109/TDSC.2004.2.

[10] M. Delgado y J.L. Vásquez, «Seguridad informática aplicando la norma ISO/IEC 27001 para la protección de activos de información*», Revista Científica Emprendimiento Científico Tecnológico,* no.1, pp.1-11, 2020 .

*[11] I. J.M. Aguilar, «*La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas», Revista *de Derecho, Globalización y Seguridad (RDGS), vol. 6*, no. 2, pp. 18-43, 2020.

[12] «Sistema Regional de Cooperación para la Vigilancia de la Seguridad Operacional, Sexta Reunion del Panel de Expertos», Lima, Perú, del 28 de mayo al 1ro de junio, 2021.

[13] J. G. Árevalo, R. A. Bayona y D. W. Rico, «Implantación de un sistema de gestión de seguridad de información bajo ISO/IEC 27001», Tecnura*, vol. 19, nº 46, pp. 123-134, 2015.*

[14] . Jevelin y A. Faza, «Evaluation the Information Security Management System: «A Path Towards ISO 27 001 Certification», Journal of Information Systems and Informatics, *vol. 5, nº 4, pp. 1240-1256, 2023.*

Apéndices

Apéndice A

Dominios y objetivos de control.

Capítulo Dominio	Descripción	Objetivo de control
A5	Políticas de seguridad de la información.	- Proporcionar seguridad y apoyar la gestión de la seguridad de la información según los requisitos, las leyes y las normas pertinentes.
A6	Organización de la seguridad de la información.	- Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información en la organización. - Garantizar la seguridad del teletrabajo y del uso de dispositivos móviles.
A7	Seguridad relativa a los recursos humanos.	- Asegurar que los empleados y contratistas entiendan sus responsabilidades y sean adecuados para las funciones para las que se consideran. - Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información. - Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo.
A8	Responsabilidad sobre los activos.	- Identificar los activos de la organización y definir las responsabilidades de protección adecuada. - Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización. - Evitar la revelación, modificación, eliminación o destrucción de la información almacenada en soportes.
A9	Control de acceso.	- Limitar el acceso a los recursos de tratamiento de información y a la información. - Garantizar el acceso de usuarios autorizados y evitar el acceso no permitido a los sistemas y servicios. - Hacer que los usuarios se hagan responsables de salvaguardar su información de autenticación. - Prevenir el acceso no autorizado a los sistemas y aplicaciones.

A10	Criptografía	- Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información.
A11	Seguridad física y del entorno.	- Prevenir el acceso físico no autorizado, así como los daños e interferencias a la información de la organización y a los recursos de tratamiento de la información. - Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.
A12	Seguridad de las operaciones.	- Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información. - Asegurar que los recursos de tratamiento de la información y la información están protegidos contra el malware. - Evitar la pérdida de datos. - Registrar eventos y generar evidencias. - Asegurar la integridad del software en explotación. - Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas. - Minimizar el impacto de las actividades de auditoría en los sistemas operativos.
A13	Seguridad de las comunicaciones.	- Asegurar la protección de la información en las redes y los recursos de tratamiento de la información. - Mantener la seguridad de la información que se transfiere dentro de una organización y con cualquier entidad externa.
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información.	- Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas. - Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de sistemas de información. - Asegurar la protección de los datos de prueba.
A15	Relación con proveedores.	- Asegurar la protección de los activos de la organización que sean accesibles a los proveedores. - Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores.

A16	Gestión de incidentes de seguridad de la información.	- Asegurar un enfoque coherente y eficaz para la gestión de incidentes, gestionar incidentes de seguridad de la información, incluyendo comunicar debilidades.
A17	Aspectos de seguridad de la información para la gestión de la continuidad del negocio.	- La continuidad de la seguridad de la información debería formar parte de los sistemas de continuidad de negocio de la organización. - Asegurar la disponibilidad de los recursos de tratamiento de la información.
A18	Cumplimiento.	- Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información.

Fuente: Elaboración propia.

Apéndice B

Amenazas detalladas por tipo.

Amenazas
N. Desastres naturales
N.º 1 Fuego
N.º 2 Daños por agua
N.º 3 Desastres naturales
I. Origen industrial
I.1 Fuego
I.2 Daños por agua
I.3 Contaminación mecánica
I.5 Avería de origen físico o lógico
I.6 Corte de suministro eléctrico
I.7 Condiciones inadecuadas de temperatura y humedad
I.8 Fallo de servicios de comunicaciones.
I.9 Interrupción de otros servicios y suministros esenciales.
I.10 Degradación de los soportes de almacenamiento de la información
I.11 Emanaciones electromagnéticas
E. Errores y fallos no intencionados
E.1 Errores de los usuarios
E.2 Errores del administrador
E.3 Errores de monitorización (log)
E.4 Errores de configuración
E.7 Deficiencias en la organización
E.8 Difusión de software dañino
E.9 Errores de redes
E10. Errores de secuencia
E.14. Escapes de información
E.15 Alteración accidental
E.18 Destrucción de información
E.19 Fugas de información
E.20 Vulnerabilidades de los programas (software)
E.21 Errores de mantenimiento/actualización de programas.
E.23 Errores de mantenimiento/actualización de equipos (hardware)
E.24 Caída del sistema por agotamiento de recursos
E.25 Pérdida de equipos
E.28 Indisponibilidad del personal
A. Ataques intencionados
A.3 Manipulación de los registros de actividad (log)
A.4 Manipulación de la configuración

A.5 Suplantación de la identidad del usuario
A.6 Abuso de privilegios de acceso
A.7 Uso no previsto
A.8 Difusión de software dañino
A.9 [Re]encaminamiento de mensajes
A.10 Alteración de secuencia
A.11 Acceso no autorizado
A.12 Análisis de tráfico
A.13 Repudio
A.14 Interceptación de información (escucha)
A.15 Modificación deliberada de la información
A.18 Destrucción de información
A.19 Divulgación de información
A.22 Manipulación de programas
A.23 Manipulación de los equipos
A.24 Denegación de servicios
A.25 Robo
A.26 Ataque destructivo
A.27 Ocupación enemiga
A.28 Indisponibilidad del personal
A.29 Extorsión
A.30 Ingeniería social (picaresca)

Fuente: Elaboración propia, basada en la metodología de Magerit.

Apéndice C

Tipos de activos y amenazas.

Código activo	Activo	Amenaza
[SW01]	Desarrollo propio - SRCO	Acceso no autorizado
[SW02]	Navegador web IE	Errores de mantenimiento/actualización de programas.
[SW03]	Navegador web Chrome	Errores de mantenimiento/actualización de programas.
[SW04]	Navegador web Mozilla	Errores de mantenimiento/actualización de programas.
[SW05]	Ofimática	Manipulación de programas
[SW06]	Servidor de ficheros	Errores del administrador Difusión de software dañino Errores de redes
[SW07]	SO Windows 7	Vulnerabilidades de los programas (software)
[SW09]	SO Linux	Caída del sistema por agotamiento de recursos
[SW10]	Windows Server 2003 R2	Vulnerabilidades de los programas (software)
[SW11]	Linux Red Hat	Caída del sistema por agotamiento de recursos
[SW12]	Linux Debian	Caída del sistema por agotamiento de recursos. Errores del administrador.
[SW13]	Windows Server 2012 R2	Vulnerabilidades de los programas (software).
[SW14]	Windows Embedded	Errores de mantenimiento/actualización de programas.
[SW15]	Servidor web CPI	Manipulación de la configuración
[SW16]	Servidor web Neptuno	Manipulación de la configuración
[SW17]	Servidor web CUCM	Manipulación de la configuración
[SW18]	Cisco ASDM-IDM	Acceso no autorizado
[SW19]	ArcSight Console	Acceso no autorizado
[SW20]	Provision Physical	Acceso no autorizado
[SW21]	Diagnostic Graphical Display	Acceso no autorizado
[SW22]	Marc Navigator	Manipulación de la configuración
[SW23]	Garex GAP	Manipulación de la configuración
[SW24]	RCMS II	Manipulación de la configuración
[SW25]	SkyWan	Manipulación de la configuración
[SW26]	VMware ESXi - NCS	Errores del administrador
[SW27]	VMware ESXi - Telefonía	Errores del administrador
[SW28]	VMware ESXi - Blade	Errores del administrador
[HW01]	Administración MyC	Errores de mantenimiento/actualización de equipos (hardware)
[HW02]	Supervisión de comunicaciones	Errores de mantenimiento/actualización de equipos (hardware)
[HW03]	Administración grabador E1	Errores de mantenimiento/actualización de equipos (hardware)
[HW04]	Operadores de tráfico aéreo	Indisponibilidad del personal
[HW05]	PDU Consola Garex	Errores del administrador
[HW06]	SVR Grabador de video	Acceso no autorizado Modificación deliberada de la información.
[HW07]	SVR Backup - Cintas	Acceso no autorizado. Modificación deliberada de la información.
[HW08]	SVR Cintas magnéticas	Acceso no autorizado. Modificación deliberada de la información.
[HW09]	SVR Grabador E1	Acceso no autorizado. Modificación deliberada de la información.
[HW10]	SVR Grabador VoIP	Acceso no autorizado. Modificación deliberada de la información.
[HW11]	SVR Virtualización Blade	Denegación de servicios. Indisponibilidad del personal.

[HW12]	SVR Cabina de discos respaldos.	Denegación de servicios. Indisponibilidad del personal. Acceso no autorizado. Modificación deliberada de la información.
[HW13]	SVR Mensajería - Gateway	Manipulación de la configuración Errores de redes.
[HW14]	SVR Seguridad SIEM	Manipulación de los registros de actividad. Acceso no autorizado. Manipulación de la configuración
[HW15]	Gestión KVM	Errores de redes. Avería de origen físico o lógico.
[HW16]	SVR Microondas	Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad.
[HW17]	SVR Sistema de Comunicación de Voz (SCV)	Errores del administrador. Fallo de servicios de comunicaciones Pérdida de equipos. Errores del administrador. Errores de configuración. Condiciones inadecuadas de temperatura y humedad.
[HW18]	SVR Radiocomunicaciones	Errores del administrador. Pérdida de equipos. Errores del administrador. Errores de configuración. Condiciones inadecuadas de temperatura y humedad.
[HW19]	Impresora en red	Manipulación de los equipos. Errores de redes. Errores de los usuarios.
[HW20]	Equipo router satelital	Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad.
[HW21]	Equipo router de redes	Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad. Errores de configuración. Errores de redes. Errores del administrador
[HW22]	Equipo switch de redes	Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad. Errores de configuración. Errores de redes. Errores del administrador

[HW23]	Equipo de seguridad de redes	Manipulación de los registros de actividad (log). Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad. Errores de configuración Errores de redes. Errores del administrador.
[HW24]	Equipo central telefónica	Manipulación de la configuración Acceso no autorizado Errores de configuración. Errores de redes.
[HW25]	Teléfonos IP	Errores de redes. Errores de configuración. Manipulación de los equipos.
[COM01]	Red telefónica PSTN	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Avería de origen físico o lógico.
[COM02]	Enlaces MW punto a punto	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.
[COM03]	Enlaces de radiocomunicaciones	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.
[COM04]	Enlaces vía satélite	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.
[COM05]	Red local	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Errores de redes. Errores de configuración. Manipulación de los equipos. Indisponibilidad del personal. Acceso no autorizado. Manipulación de los equipos.

		Ataque destructivo. Extorsión.
[COM06]	Servicio de internet	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Avería de origen físico o lógico. Errores de redes. Errores de configuración. Manipulación de los equipos.
[Media01]	Disco duro SATA	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.
[Media02]	Disco extraíble RDX	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.
[Media03]	Almacenamiento en red	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.
[Media04]	Cintas magnéticas	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.
[Media05]	Memorias USB	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.
[AUX01]	Fuentes de alimentación	Avería de origen físico o lógico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Ataque destructivo.
[AUX02]	UPS en data centers	Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Condiciones inadecuadas de temperatura y humedad.

		Fuego. Daños por agua.
[AUX03]	Generadores eléctricos	Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Condiciones inadecuadas de temperatura y humedad. Fuego. Daños por agua. Ataque destructivo.
[AUX04]	Equipos de climatización	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Fuego. Daños por agua. Ataque destructivo.
[AUX05]	Cableado eléctrico	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Fuego. Ataque destructivo.
[AUX06]	Fibra óptica	Ataque destructivo. Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Fuego.
[AUX07]	Mobiliario: mesas, sillas, etc.	Robo. Ataque destructivo. Daños por agua. Fuego. Desastres naturales.
[L01]	Sitios remotos de vigilancia aérea.	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones. Interrupción de otros servicios y suministros esenciales. Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.
[L02]	Edificio Centros de Mando.	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones.

		Interrupción de otros servicios y suministros esenciales. Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.
[L03]	Contenedores en los sitios remotos.	—Fuego. - Daños por agua. - Desastres naturales. - Corte de suministro eléctrico. - Fallo de servicios de comunicaciones. - Interrupción de otros servicios y suministros esenciales. - Indisponibilidad del personal. - Acceso no autorizado. - Robo. - Ataque destructivo. - Ocupación enemiga.
[P01]	Usuarios externos	- Fuga de información. - Divulgación de información. - Extorsión - Robo
[P02]	Usuarios internos	- Errores de los usuarios. - Fuga de información. - Indisponibilidad del personal.
[P03]	Operadores	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión
[P04]	Administradores de sistemas	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.
[P05]	Administradores de comunicaciones	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.
[P06]	Administradores de BBDD	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.
[P07]	Desarrolladores de software	- Difusión de software dañino. - Fugas de información. - Vulnerabilidades de los programas (software).
[P08]	Proveedores	- Fugas de información. - Divulgación de información.
[P09]	Administradores de SEG	- Errores de configuración.

		- Errores de mantenimiento/actualización de programas. - Errores de mantenimiento/actualización de equipos (hardware).

Fuente: Elaboración propia, basada en la metodología de Magerit v3.

Apéndice D

Identificación de controles existentes.

Código activo	Descripción	Responsable	Amenaza	Controles existentes
[SW01]	Desarrollo propio - SRCO	MyC	Acceso no autorizado	Control de acceso con usuario y contraseña de un solo factor. Instalación de antivirus.
[SW02]	Navegador web IE	MyC	Errores de mantenimiento/actualización de programas.	Ninguno.
[SW03]	Navegador web Chrome	MyC	Errores de mantenimiento/actualización de programas.	Ninguno.
[SW04]	Navegador web Mozilla	MyC	Errores de mantenimiento/actualización de programas.	Ninguno.
[SW05]	Ofimática	MyC	Manipulación de programas	Ninguno.
[SW06]	Servidor de ficheros	NET	Errores del administrador Difusión de software dañino. Errores de redes.	Control de acceso con usuario y contraseña de un solo factor.
[SW07]	SO Windows 7	NET	Vulnerabilidades de los programas (software)	Ninguno.
[SW09]	SO Linux	MyC	Caída del sistema por agotamiento de recursos	Ninguno.
[SW10]	Windows Server 2003 R2	NET	Vulnerabilidades de los programas (software)	Ninguno.
[SW11]	Linux Red Hat	MyC, NET	Caída del sistema por agotamiento de recursos	Ninguno.
[SW12]	Linux Debian	NET	Caída del sistema por agotamiento de recursos. Errores del administrador.	Ninguno.
[SW13]	Windows Server 2012 R2	MyC	Vulnerabilidades de los programas (software).	Ninguno.
[SW14]	Windows Embedded	GES	Errores de mantenimiento/actualización de programas.	Ninguno.
[SW15]	Servidor web CPI	NET	Manipulación de la configuración.	Certificado digital. Acceso con usuario y contraseña.
[SW16]	Servidor web Neptuno	NET	Manipulación de la configuración	Acceso con usuario y contraseña. El firewall permite acceder al usuario autorizado.
[SW17]	Servidor web CUCM	GES	Manipulación de la configuración	Acceso con usuario y contraseña. El firewall permite acceder al usuario autorizado.
[SW18]	Cisco ASDM-IDM	NET	Acceso no autorizado	Certificado digital. Acceso con usuario y contraseña.
[SW19]	ArcSight Console	MyC	Acceso no autorizado	Certificado digital. Acceso con usuario y contraseña.
[SW20]	Provision Physical	MW	Acceso no autorizado	Ninguno.
[SW21]	Diagnostic Graphical Display	GES	Acceso no autorizado	Ninguno.
[SW22]	Marc Navigator	RAD	Manipulación de la configuración	Acceso con usuario y contraseña.
[SW23]	Garex GAP	GES	Manipulación de la configuración	Ninguno.
[SW24]	RCMS II	RAD	Manipulación de la configuración	Acceso con usuario y contraseña.
[SW25]	SkyWan	SAT	Manipulación de la configuración	Acceso con usuario y contraseña.
[SW26]	VMware ESXi - NCS	NET	Errores del administrador	Acceso con usuario y contraseña.
[SW27]	VMware ESXi - Telefonía	NET	Errores del administrador	Acceso con usuario y contraseña.
[SW28]	VMware ESXi - Blade	MyC	Errores del administrador	Acceso con usuario y contraseña.

[HW01]	Administración MyC	MyC	Errores de mantenimiento/actualización de equipos (hardware)	Acceso con usuario y contraseña. Mantenimiento preventivo
[HW02]	Supervisión de comunicaciones	NET, MW, SAT, RAD, SEG.	Errores de mantenimiento/actualización de equipos (hardware)	Ninguno.
[HW03]	Administración grabador E1	GES	Errores de mantenimiento/actualización de equipos (hardware)	Acceso con usuario y contraseña.
[HW04]	Operadores de tráfico aéreo	MyC	Indisponibilidad del personal	Acceso con usuario y contraseña.
[HW05]	PDU Consola Garex	GES	Errores del administrador	Ninguno.
[HW06]	SVR grabador de vídeo.	MyC	Acceso no autorizado Modificación deliberada de la información.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.
[HW07]	SVR Backup - Cintas	MyC	Acceso no autorizado. Modificación deliberada de la información.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.
[HW08]	SVR Cintas magnéticas	MyC	Acceso no autorizado. Modificación deliberada de la información.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.
[HW09]	SVR Grabador E1	GES	Acceso no autorizado. Modificación deliberada de la información.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.
[HW10]	SVR Grabador VoIP	GES	Acceso no autorizado. Modificación deliberada de la información.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.
[HW11]	SVR Virtualización Blade	MyC	Denegación de servicios. Indisponibilidad del personal.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.
[HW12]	SVR Cabina de discos respaldos.	MyC	Denegación de servicios. Indisponibilidad del personal. Acceso no autorizado. Modificación deliberada de la información.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.
[HW13]	SVR Mensajería - Gateway	MyC	Manipulación de la configuración Errores de redes.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.
[HW14]	SVR Seguridad SIEM	SEG	Manipulación de los registros de actividad. Acceso no autorizado. Manipulación de la configuración	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña. Certificado digital.
[HW15]	Gestión KVM	GES	Errores de redes. Avería de origen físico o lógico.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.
[HW16]	SVR Microondas	GES	Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.
[HW17]	SVR Sistema de Comunicación de Voz (SCV)	GES	Errores del administrador. Fallo de servicios de comunicaciones Pérdida de equipos. Errores del administrador. Errores de configuración. Condiciones inadecuadas de temperatura y humedad.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.
[HW18]	SVR Radiocomunicaciones	RAD	Pérdida de equipos. Errores del administrador. Errores de configuración.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.

			Condiciones inadecuadas de temperatura y humedad.	
[HW19]	Impresora en red	MyC	Manipulación de los equipos. Errores de redes. Errores de los usuarios.	Ninguno.
[HW20]	Equipo router satelital	SAT	Errores del administrador. Errores de configuración. Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.
[HW21]	Equipo router de redes	NET	Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad. Errores de configuración. Errores de redes. Errores del administrador	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.
[HW22]	Equipo switch de redes	NET	Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad. Errores de configuración. Errores de redes. Errores del administrador	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.
[HW23]	Equipo de seguridad de redes	NET	Manipulación de los registros de actividad (log). Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad. Errores de configuración Errores de redes. Errores del administrador.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.
[HW24]	Equipo central telefónica	NET	Manipulación de la configuración Acceso no autorizado Errores de configuración. Errores de redes.	- Control de acceso biométrico. - Control de acceso lógico con usuario y contraseña.
[HW25]	Teléfonos IP	NET	Errores de redes. Errores de configuración. Manipulación de los equipos.	Ninguno.
[COM01]	Red telefónica PSTN	NET	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Avería de origen físico o lógico.	Ninguno.
[COM02]	Enlaces MW punto a punto	MW	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal.	Guardia física.

			Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.	
[COM03]	Enlaces de radiocomunicaciones	RAD	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.	Guardia física.
[COM04]	Enlaces vía satélite	SAT	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.	Guardia física.
[COM05]	Red local	NET	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Errores de redes. Errores de configuración. Manipulación de los equipos. Indisponibilidad del personal. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.	- Guardia física. - Control de acceso biométrico.
[COM06]	Servicio de internet	NET	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Avería de origen físico o lógico. Errores de redes. Errores de configuración. Manipulación de los equipos.	Equipo UTM controla el acceso a internet.
[Media01]	Disco duro SATA	MyC	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	Ninguno.
[Media02]	Disco extraíble RDX	MyC, NET	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información.	Ninguno.

			Difusión de software dañino.	
[Media03]	Almacenamiento en red.	MyC	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	Ninguno.
[Media04]	Cintas magnéticas.	MyC	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	Ninguno.
[Media05]	Memorias USB	NET, MW, SAT, RAD, SEG, GES, MyC	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	Ninguno.
[AUX01]	Fuentes de alimentación	MyC	Avería de origen físico o lógico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Ataque destructivo.	Ninguno.
[AUX02]	UPS en data centers	MyC	Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Condiciones inadecuadas de temperatura y humedad. Fuego. Daños por agua.	Control de acceso biométrico.
[AUX03]	Generadores eléctricos	MyC	Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Condiciones inadecuadas de temperatura y humedad. Fuego. Daños por agua. Ataque destructivo.	Ninguno.
[AUX04]	Equipos de climatización	MyC, RAD, MW	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Fuego. Daños por agua. Ataque destructivo.	Control de acceso biométrico.

[AUX05]	Cableado eléctrico	NET, MW, SAT, RAD, SEG, GES, MyC	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Fuego. Ataque destructivo.	Ninguno.
[AUX06]	Fibra óptica	NET	Ataque destructivo. Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Fuego.	Ninguno.
[AUX07]	Mobiliario: mesas, sillas, etc.	MyC	Robo. Ataque destructivo. Daños por agua. Fuego. Desastres naturales.	
[L01]	Sitios remotos de vigilancia aérea.	Jefes de sitios remotos	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones. Interrupción de otros servicios y suministros esenciales. Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.	Guardia física.
[L02]	Edificio Centros de Mando.	Jefes de centros de mando	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones. Interrupción de otros servicios y suministros esenciales. Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.	Guardia física. Control de acceso biométrico.
[L03]	Contenedores en los sitios remotos.	Jefes de sitios remotos	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones. Interrupción de otros servicios y suministros esenciales. Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.	Ninguno.
[P01]	Usuarios externos	RRHH	- Fuga de información. - Divulgación de información. - Extorsión - Robo	Ninguno.

[P02]	Usuarios internos	Jefes de sitios y CM	- Errores de los usuarios. - Fuga de información. - Indisponibilidad del personal.	Ninguno.
[P03]	Operadores	Jefes de sitios y CM	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión	- Procedimiento para la utilización de dispositivos electrónicos y medios extraíbles.
[P04]	Administradores de sistemas	NET, MW, SAT, RAD, SEG, GES, MyC	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.	- Manual de procedimientos técnicos.
[P05]	Administradores de comunicaciones	NET, MW, SAT, RAD	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.	- Manual de procedimientos.
[P06]	Administradores de BBDD	MyC	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.	- Procedimiento para la administración de BBDD.
[P07]	Desarrolladores de software	MyC	- Difusión de software dañino. - Fugas de información. - Vulnerabilidades de los programas (software).	Ninguno.
[P08]	Proveedores	RRHH, jefes CM	- Fugas de información. - Divulgación de información.	Ninguno.
[P09]	Administradores de SEG	SEG	- Errores de configuración. - Errores de mantenimiento/actualización de programas. - Errores de mantenimiento/actualización de equipos (hardware).	Manuales de procedimientos.

Fuente: elaboración propia, basada en la metodología de Magerit v3.

Apéndice E

Identificación de las vulnerabilidades.

Código activo	Descripción	Amenaza	Controles existentes	Vulnerabilidad
[SW01]	Desarrollo propio - SRCO	Acceso no autorizado	Control de acceso con usuario y contraseña de un solo factor. Instalación de antivirus.	Los usuarios utilizan la misma contraseña para ingresar a la aplicación.
[SW02]	Navegador web IE	Errores de mantenimiento/actualización de programas.	Ninguno.	Navegador desactualizado: utiliza versión del año 2017.
[SW03]	Navegador web Chrome	Errores de mantenimiento/actualización de programas.	Ninguno.	Navegador desactualizado: utiliza versión del año 2017.
[SW04]	Navegador web Mozilla	Errores de mantenimiento/actualización de programas.	Ninguno.	Navegador desactualizado: utiliza versión del año 2017.
[SW05]	Ofimática	Manipulación de programas	Ninguno.	Utiliza versiones ofimáticas sin licencia.
[SW06]	Servidor de ficheros	Errores del administrador Difusión de software dañino. Errores de redes.	Control de acceso con usuario y contraseña de un solo factor.	No existe un servidor de usuarios que autentique credenciales de clientes; lo hace directamente el servidor de ficheros.
[SW07]	SO Windows 7	Vulnerabilidades de los programas (software)	Ninguno.	- SO vulnerable, última actualización, año 2017. - SO sin hardening. - SO sin antivirus.
[SW09]	SO Linux	Caída del sistema por agotamiento de recursos	Ninguno.	- SO vulnerable, última actualización, año 2017. - SO sin hardening.
[SW10]	Windows Server 2003 R2	Vulnerabilidades de los programas (software)	Ninguno.	- SO vulnerable, última actualización, año 2017. - SO sin hardening.
[SW11]	Linux Red Hat	Caída del sistema por agotamiento de recursos	Ninguno.	- SO vulnerable, última actualización, año 2017. - SO sin hardening.
[SW12]	Linux Debian	Caída del sistema por agotamiento de recursos. Errores del administrador.	Ninguno.	- SO vulnerable, última actualización, año 2017. - SO sin hardening.
[SW13]	Windows Server 2012 R2	Vulnerabilidades de los programas (software).	Ninguno.	- SO vulnerable, última actualización, año 2017. - SO sin hardening.
[SW14]	Windows Embedded	Errores de mantenimiento/actualización de programas.	Ninguno.	- SO sin antivirus.
[SW15]	Servidor web CPI	Manipulación de la configuración.	Certificado digital. Acceso con usuario y contraseña.	- No existe un procedimiento para sacar respaldos cuando se llena la partición /var/log, provocando la caída del servidor.
[SW16]	Servidor web Neptuno	Manipulación de la configuración	Acceso con usuario y contraseña. El firewall permite acceder al usuario autorizado.	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.
[SW17]	Servidor web CUCM	Manipulación de la configuración	Acceso con usuario y contraseña. El firewall permite acceder al usuario autorizado.	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.

				- Existe un solo usuario y contraseña con privilegios de administrador.
[SW18]	Cisco ASDM-IDM	Acceso no autorizado	Certificado digital. Acceso con usuario y contraseña.	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.
[SW19]	ArcSight Console	Acceso no autorizado	Certificado digital. Acceso con usuario y contraseña.	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.
[SW20]	Provision Physical	Acceso no autorizado	Ninguno.	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.
[SW21]	Diagnostic Graphical Display	Acceso no autorizado	Ninguno.	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.
[SW22]	Marc Navigator	Manipulación de la configuración	Acceso con usuario y contraseña.	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.
[SW23]	Garex GAP	Manipulación de la configuración	Ninguno.	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.
[SW24]	RCMS II	Manipulación de la configuración	Acceso con usuario y contraseña.	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.
[SW25]	SkyWan	Manipulación de la configuración	Acceso con usuario y contraseña.	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.

				- Existe un solo usuario y contraseña con privilegios de administrador.
[SW26]	VMware ESXi - NCS	Errores del administrador	Acceso con usuario y contraseña.	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.
[SW27]	VMware ESXi - Telefonía	Errores del administrador	Acceso con usuario y contraseña.	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.
[SW28]	VMware ESXi - Blade	Errores del administrador	Acceso con usuario y contraseña.	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.
[HW01]	Administración MyC	Errores de mantenimiento/actualización de equipos (hardware)	Acceso con usuario y contraseña. Mantenimiento preventivo	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.
[HW02]	Supervisión de comunicaciones	Errores de mantenimiento/actualización de equipos (hardware)	Ninguno.	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.
[HW03]	Administración grabador E1	Errores de mantenimiento/actualización de equipos (hardware)	Acceso con usuario y contraseña.	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.
[HW04]	Operadores de tráfico aéreo	Indisponibilidad del personal	Acceso con usuario y contraseña.	- Falta de mantenimiento preventivo y hardening del SO.
[HW05]	PDU Consola Garex	Errores del administrador	Ninguno.	- Falta de mantenimiento preventivo.
[HW06]	SVR grabador de vídeo.	Acceso no autorizado Modificación deliberada de la información.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.	- Falta de mantenimiento preventivo y hardening del SO.
[HW07]	SVR Backup - Cintas	Acceso no autorizado. Modificación deliberada de la información.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.	- Falta de mantenimiento preventivo y hardening del SO.
[HW08]	SVR Cintas magnéticas	Acceso no autorizado. Modificación deliberada de la información.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.	- Falta de mantenimiento preventivo y hardening del SO.
[HW09]	SVR Grabador E1	Acceso no autorizado.	Control de acceso biométrico.	- Falta de mantenimiento preventivo y hardening del SO.

		Modificación deliberada de la información.	Control de acceso lógico con usuario y contraseña.	
[HW10]	SVR Grabador VoIP	Acceso no autorizado. Modificación deliberada de la información.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.	- Falta de mantenimiento preventivo y hardening del SO.
[HW11]	SVR Virtualización Blade	Denegación de servicios. Indisponibilidad del personal.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.	- Falta de mantenimiento preventivo y hardening del SO.
[HW12]	SVR Cabina de discos respaldos.	Denegación de servicios. Indisponibilidad del personal. Acceso no autorizado. Modificación deliberada de la información.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.	- Falta de mantenimiento preventivo y hardening del SO.
[HW13]	SVR Mensajería - Gateway	Manipulación de la configuración Errores de redes.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.	- Falta de mantenimiento preventivo y hardening del SO.
[HW14]	SVR Seguridad SIEM	Manipulación de los registros de actividad. Acceso no autorizado. Manipulación de la configuración	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña. Certificado digital.	- Falta de mantenimiento preventivo y hardening del SO.
[HW15]	Gestión KVM	Errores de redes. Avería de origen físico o lógico.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.	- Falta de mantenimiento preventivo y hardening del SO.
[HW16]	SVR Microondas	Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.	- Falta de mantenimiento preventivo y hardening del SO. - No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.
[HW17]	SVR Sistema de Comunicación de Voz (SCV)	Errores del administrador. Fallo de servicios de comunicaciones Pérdida de equipos. Errores del administrador. Errores de configuración. Condiciones inadecuadas de temperatura y humedad.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.	- Falta de mantenimiento preventivo y hardening del SO. - No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.
[HW18]	SVR Radiocomunicaciones	Pérdida de equipos. Errores del administrador. Errores de configuración. Condiciones inadecuadas de	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.	- Falta de mantenimiento preventivo y hardening del SO. - No existe un procedimiento para cambiar las credenciales periódicamente.

		temperatura y humedad.		- Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.
[HW19]	Impresora en red	Manipulación de los equipos. Errores de redes. Errores de los usuarios.	Ninguno.	- No existe un procedimiento o control; cualquier usuario que se encuentra en la misma red de la impresora puede imprimir.
[HW20]	Equipo router satelital	Errores del administrador. Errores de configuración. Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.	- Falta de entrenamiento o capacitación al personal técnico para que realice configuraciones avanzadas.
[HW21]	Equipo router de redes	Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad. Errores de configuración. Errores de redes. Errores del administrador	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.	Cualquier usuario que se encuentre en el mismo segmento de red de los routers, conociendo las credenciales, puede acceder vía SSH.
[HW22]	Equipo switch de redes	Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad. Errores de configuración. Errores de redes. Errores del administrador	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.	Cualquier usuario que se encuentre en el mismo segmento de red de los routers, conociendo las credenciales, puede acceder vía SSH.
[HW23]	Equipo de seguridad de redes	Manipulación de los registros de actividad (log). Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión.	Control de acceso biométrico. Control de acceso lógico con usuario y contraseña.	Cualquier usuario que se encuentre en el mismo segmento de red de los routers, conociendo las credenciales, puede acceder vía SSH.

		Condiciones inadecuadas de temperatura y humedad. Errores de configuración Errores de redes. Errores del administrador.		
[HW24]	Equipo central telefónica	Manipulación de la configuración Acceso no autorizado Errores de configuración. Errores de redes.	- Control de acceso biométrico. - Control de acceso lógico con usuario y contraseña.	- Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.
[HW25]	Teléfonos IP	Errores de redes. Errores de configuración. Manipulación de los equipos.	Ninguno.	Cualquier usuario puede acceder físicamente a los teléfonos IP y puede cambiar la configuración, dejando sin servicio el mencionado equipo. El equipo permite poner contraseña para impedir el acceso a la configuración, pero no existe un procedimiento para ello.
[COM01]	Red telefónica PSTN	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Avería de origen físico o lógico.	Ninguno.	El tendido de fibra óptica externa de la red PSTN se encuentra muy bajo; cualquier vehículo lo suficientemente alto puede romper la fibra óptica (ya ha sucedido).
[COM02]	Enlaces MW punto a punto	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.	Guardia física.	El personal de guardia física en las torres de MW no pertenece a la especialidad y no puede solucionar problemas técnicos en el sitio.
[COM03]	Enlaces de radiocomunicaciones	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.	Guardia física.	El personal técnico que se encuentra en los sitios remotos no está capacitado para realizar tareas de mantenimiento de primer, segundo y tercer escalón en radiocomunicaciones.
[COM04]	Enlaces vía satélite	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales.	Guardia física.	- Déficit de personal que realiza la guardia física en los sitios remotos. - El personal técnico que se encuentra en los sitios remotos no está capacitado para realizar tareas de mantenimiento de primer,

		Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.		segundo y tercer escalón en radiocomunicaciones.
[COM05]	Red local	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Errores de redes. Errores de configuración. Manipulación de los equipos. Indisponibilidad del personal. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.	- Guardia física. - Control de acceso biométrico.	No existen procedimientos para no manipular el cableado estructurado de la red o la electrónica de red.
[COM06]	Servicio de internet	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Avería de origen físico o lógico. Errores de redes. Errores de configuración. Manipulación de los equipos.	Equipo UTM controla el acceso a internet.	No existe procedimiento para el uso de internet; un equipo de seguridad controla los accesos a internet. Todos los usuarios a través de la red local disponen del servicio.
[Media01]	Disco duro SATA	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	Ninguno.	No existe una política o procedimiento de seguridad de la información para el almacenamiento y custodia de este tipo de dispositivo.
[Media02]	Disco extraíble RDX	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información.	Ninguno.	No existe una política o procedimiento de seguridad de la información para el almacenamiento y custodia de este tipo de dispositivo.

		Difusión de software dañino.		
[Media03]	Almacenamiento en red.	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	Ninguno.	No existe una política o procedimiento de seguridad de la información para el almacenamiento en la red.
[Media04]	Cintas magnéticas.	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	Ninguno.	No existe una política o procedimiento de seguridad de la información para el almacenamiento y custodia de este tipo de dispositivo.
[Media05]	Memorias USB	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	Ninguno.	No existe una política o procedimiento de seguridad de la información para el uso de este tipo de dispositivos.
[AUX01]	Fuentes de alimentación	Avería de origen físico o lógico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Ataque destructivo.	Ninguno.	No existen procedimientos para el uso, mantenimiento o reemplazo de los diferentes tipos de alimentación.
[AUX02]	UPS en data centers	Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Condiciones inadecuadas de	Control de acceso biométrico.	Falta de mantenimiento por falta de presupuesto.

		temperatura y humedad. Fuego. Daños por agua.		
[AUX03]	Generadores eléctricos	Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Condiciones inadecuadas de temperatura y humedad. Fuego. Daños por agua. Ataque destructivo.	Ninguno.	Falta de mantenimiento por falta de presupuesto.
[AUX04]	Equipos de climatización	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Fuego. Daños por agua. Ataque destructivo.	Control de acceso biométrico.	Falta de mantenimiento por falta de presupuesto.
[AUX05]	Cableado eléctrico	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Fuego. Ataque destructivo.	Ninguno.	Falta de mantenimiento por falta de presupuesto.
[AUX06]	Fibra óptica	Ataque destructivo. Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Fuego.	Ninguno.	- Falta de mantenimiento por falta de presupuesto. - Déficit de personal para brindar seguridad física.
[AUX07]	Mobiliario: mesas, sillas, etc.	Robo. Ataque destructivo. Daños por agua. Fuego. Desastres naturales.		Falta de mantenimiento por falta de presupuesto, depreciación de muebles de oficina.
[L01]	Sitios remotos de vigilancia aérea.	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones.	Guardia física.	Déficit de personal para la seguridad física de las instalaciones.

		Interrupción de otros servicios y suministros esenciales. Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.		
[L02]	Edificio Centros de Mando.	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones. Interrupción de otros servicios y suministros esenciales. Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.	Guardia física. Control de acceso biométrico.	Área muy extensa, déficit de personal para la seguridad física de las instalaciones.
[L03]	Contenedores en los sitios remotos.	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones. Interrupción de otros servicios y suministros esenciales. Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.	Ninguno.	Área muy extensa, déficit de personal para la seguridad física de las instalaciones.
[P01]	Usuarios externos	- Fuga de información. - Divulgación de información. - Extorsión - Robo	Ninguno.	- No existe VPN para conectarse remotamente a los sistemas y servidores de la empresa.
[P02]	Usuarios internos	- Errores de los usuarios. - Fuga de información. - Indisponibilidad del personal.	Ninguno.	- Falta de personal capacitado para cumplir con las tareas asignadas.
[P03]	Operadores	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión	- Procedimiento para la utilización de dispositivos electrónicos y medios extraíbles.	- Falta de personal capacitado para cumplir con las tareas asignadas. - Acuerdos de confidencialidad existentes.
[P04]	Administradores de sistemas	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información.	- Manual de procedimientos técnicos.	- Falta de procedimientos en los manuales de procedimientos.

		- Divulgación de información. - Extorsión - Errores del administrador.		
[P05]	Administradores de comunicaciones	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.	- Manual de procedimientos.	- Falta de procedimientos en los manuales de procedimientos.
[P06]	Administradores de BBDD	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.	- Procedimiento para la administración de BBDD.	- Falta de experiencia y capacitación del personal técnico en gestión de BBDD.
[P07]	Desarrolladores de software	- Difusión de software dañino. - Fugas de información. - Vulnerabilidades de los programas (software).	Ninguno.	- Falta de procedimientos para la introducción de software externo.
[P08]	Proveedores	- Fugas de información. - Divulgación de información.	Ninguno.	- Falta de contratos de confidencialidad.
[P09]	Administradores de SEG	- Errores de configuración. - Errores de mantenimiento/actualización de programas. - Errores de mantenimiento/actualización de equipos (hardware).	Manuales de procedimientos.	- Falta de personal capacitado para cumplir con las tareas asignadas.

Fuente: Elaboración propia, basada en la metodología de Magerit v3.

Apéndice F

Evaluación de las consecuencias.

EVALUACIÓN DE LAS CONSECUENCIAS				
Código activo	**Descripción**	**Amenaza**	**Vulnerabilidad**	**Consecuencias**
[SW01]	Desarrollo propio - SRCO	Acceso no autorizado	Los usuarios utilizan la misma contraseña para ingresar a la aplicación.	- Alteración de datos. - Pérdidas financieras.
[SW02]	Navegador web IE	Errores de mantenimiento/actualización de programas.	Navegador desactualizado: utiliza versión del año 2017.	- Inestabilidad en el funcionamiento de sistemas.
[SW03]	Navegador web Chrome	Errores de mantenimiento/actualización de programas.	Navegador desactualizado: utiliza versión del año 2017.	- Inestabilidad en el funcionamiento de sistemas.
[SW04]	Navegador web Mozilla	Errores de mantenimiento/actualización de programas.	Navegador desactualizado: utiliza versión del año 2017.	- Inestabilidad en el funcionamiento de sistemas.
[SW05]	Ofimática	Manipulación de programas	Utiliza versiones ofimáticas sin licencia.	- Pérdida de eficacia en el desarrollo administrativo.
[SW06]	Servidor de ficheros	Errores del administrador Difusión de software dañino. Errores de redes.	No existe un servidor de usuarios que autentique credenciales de clientes; lo hace directamente el servidor de ficheros.	- Pérdida de datos e información.
[SW07]	SO Windows 7	Vulnerabilidades de los programas (software)	- SO vulnerable, última actualización, año 2017. - SO sin hardening. - SO sin antivirus.	- Pérdida de datos e información. - Denegación de servicios.
[SW09]	SO Linux	Caída del sistema por agotamiento de recursos	- SO vulnerable, última actualización, año 2017. - SO sin hardening.	- Pérdida de datos e información. - Denegación de servicios.
[SW10]	Windows Server 2003 R2	Vulnerabilidades de los programas (software)	- SO vulnerable, última actualización, año 2017. - SO sin hardening.	- Pérdida de datos e información. - Denegación de servicios.
[SW11]	Linux Red Hat	Caída del sistema por agotamiento de recursos	- SO vulnerable, última actualización, año 2017. - SO sin hardening.	- Pérdida de datos e información. - Denegación de servicios.
[SW12]	Linux Debian	Caída del sistema por agotamiento de recursos. Errores del administrador.	- SO vulnerable, última actualización, año 2017. - SO sin hardening.	- Pérdida de datos e información. - Denegación de servicios.
[SW13]	Windows Server 2012 R2	Vulnerabilidades de los programas (software).	- SO vulnerable, última actualización, año 2017. - SO sin hardening.	- Pérdida de datos e información. - Denegación de servicios.
[SW14]	Windows Embedded	Errores de mantenimiento/actualización de programas.	- SO sin antivirus.	- Pérdida de datos e información. - Denegación de servicios.
[SW15]	Servidor web CPI	Manipulación de la configuración.	- No existe un procedimiento para sacar respaldos cuando se llena la partición /var/log, provocando la caída del servidor.	Denegación del servicio de monitoreo de la red de datos.
[SW16]	Servidor web Neptuno	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas,	- Pérdida de grabaciones de audio E1. - Imagen y reputación afectadas.

			visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	
[SW17]	Servidor web CUCM	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	- Denegación del servicio telefónico VoIP.
[SW18]	Cisco ASDM-IDM	Acceso no autorizado	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	- Denegación de servicios. - Pérdida del control de toda la red.
[SW19]	ArcSight Console	Acceso no autorizado	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	Pueden ingresar con las credenciales de administrador y cambiar la configuración o hacer una denegación de servicios.
[SW20]	Provision Physical	Acceso no autorizado	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	Pueden modificar o eliminar la configuración del sistema de microondas. También pueden denegar el servicio de vigilancia aérea desde los sitios remotos hacia los centros de mando.
[SW21]	Diagnostic Graphical Display	Acceso no autorizado	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.	Pueden modificar o eliminar la configuración del sistema de comunicación de voz, denegar el acceso a los operadores de vigilancia aérea.

[SW22]	Marc Navigator	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	Pueden modificar o eliminar la configuración del sistema de radiocomunicaciones, denegar el acceso a los operadores de vigilancia aérea.
[SW23]	Garex GAP	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	Pueden denegar la gestión del sistema de comunicación de voz.
[SW24]	RCMS II	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	Se puede cambiar la configuración de las radios HF de los sitios remotos.
[SW25]	SkyWan	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	Pueden modificar o eliminar la configuración del sistema satelital. También pueden denegar los servicios entre los sitios remotos y los centros de mando.
[SW26]	VMware ESXi - NCS	Errores del administrador	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.	Pueden eliminar la configuración de máquinas virtuales y denegar la gestión de la red de datos.
[SW27]	VMware ESXi - Telefonía	Errores del administrador	- No existe un procedimiento para cambiar las credenciales periódicamente.	Pueden eliminar la configuración de máquinas virtuales y denegar la gestión del sistema de telefonía.

			- Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.	
[SW28]	VMware ESXi - Blade	Errores del administrador	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.	Pueden eliminar la configuración de máquinas virtuales, crear otras y denegar la gestión de usuarios.
[HW01]	Administración MyC	Errores de mantenimiento/actualización de equipos (hardware)	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	Se puede eliminar o modificar la gestión de todos los servicios de vigilancia aérea.
[HW02]	Supervisión de comunicaciones	Errores de mantenimiento/actualización de equipos (hardware)	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	Se pueden denegar servicios, ser manipulados con facilidad.
[HW03]	Administración grabador E1	Errores de mantenimiento/actualización de equipos (hardware)	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	Pérdida de las grabaciones de radiocomunicaciones.
[HW04]	Operadores de tráfico aéreo	Indisponibilidad del personal	- Falta de mantenimiento preventivo y hardening del SO.	Inestabilidad en el funcionamiento de los sistemas.
[HW05]	PDU Consola Garex	Errores del administrador	- Falta de mantenimiento preventivo.	Inestabilidad en el funcionamiento de los sistemas.
[HW06]	SVR grabador de vídeo.	Acceso no autorizado	- Falta de mantenimiento	Inestabilidad en el funcionamiento de los sistemas.

		Modificación deliberada de la información.	preventivo y hardening del SO.	La pérdida de datos e información.
[HW07]	SVR Backup - Cintas	Acceso no autorizado. Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	- La pérdida de datos e información. - La pérdida de eficacia en el funcionamiento operacional de los sistemas.
[HW08]	SVR Cintas magnéticas	Acceso no autorizado. Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	- La pérdida de datos e información. - La pérdida de eficacia en el funcionamiento operacional de los sistemas.
[HW09]	SVR Grabador E1	Acceso no autorizado. Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	Deterioro del equipo e inestabilidad en el funcionamiento de los sistemas.
[HW10]	SVR Grabador VoIP	Acceso no autorizado. Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	Deterioro del equipo e inestabilidad en el funcionamiento de los sistemas.
[HW11]	SVR Virtualización Blade	Denegación de servicios. Indisponibilidad del personal.	- Falta de mantenimiento preventivo y hardening del SO.	Deterioro del equipo e inestabilidad en el funcionamiento de los sistemas.
[HW12]	SVR Cabina de discos respaldos.	Denegación de servicios. Indisponibilidad del personal. Acceso no autorizado. Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	Deterioro del equipo e inestabilidad en el funcionamiento de los sistemas.
[HW13]	SVR Mensajería - Gateway	Manipulación de la configuración Errores de redes.	- Falta de mantenimiento preventivo y hardening del SO.	Deterioro del equipo e inestabilidad en el funcionamiento de los sistemas.
[HW14]	SVR Seguridad SIEM	Manipulación de los registros de actividad. Acceso no autorizado. Manipulación de la configuración	- Falta de mantenimiento preventivo y hardening del SO.	Deterioro del equipo e inestabilidad en el funcionamiento de los sistemas.
[HW15]	Gestión KVM	Errores de redes. Avería de origen físico o lógico.	- Falta de mantenimiento preventivo y hardening del SO.	Deterioro del equipo e inestabilidad en el funcionamiento de los sistemas. Pérdida de gestión de los servidores.
[HW16]	SVR Microondas	Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad.	- Falta de mantenimiento preventivo y hardening del SO. - No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	- Deterioro del equipo e inestabilidad en el funcionamiento de los sistemas. - Pérdida de gestión del sistema de microondas.
[HW17]	SVR Sistema de Comunicación de Voz (SCV)	Errores del administrador. Fallo de servicios de comunicaciones Pérdida de equipos. Errores del administrador. Errores de configuración.	- Falta de mantenimiento preventivo y hardening del SO. - No existe un procedimiento para cambiar las	- Deterioro del equipo e inestabilidad en el funcionamiento de los sistemas. - Pérdida de gestión del sistema de comunicación de voz.

		Condiciones inadecuadas de temperatura y humedad.	credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	- Pérdida de la gestión de las consolas de los operadores de vigilancia aérea.
[HW18]	SVR Radiocomunicaciones	Pérdida de equipos. Errores del administrador. Errores de configuración. Condiciones inadecuadas de temperatura y humedad.	- Falta de mantenimiento preventivo y hardening del SO. - No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	- Deterioro del equipo e inestabilidad en el funcionamiento de los sistemas. - Pérdida de gestión del sistema de radiocomunicaciones. - No se puede acceder a los equipos de radio VHF, HF.
[HW19]	Impresora en red	Manipulación de los equipos. Errores de redes. Errores de los usuarios.	- No existe un procedimiento o control; cualquier usuario que se encuentra en la misma red de la impresora puede imprimir.	- Denegación del servicio de impresión.
[HW20]	Equipo router satelital	Errores del administrador. Errores de configuración. Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad.	- Falta de entrenamiento o capacitación al personal técnico para que realice configuraciones avanzadas.	- Medio alterno fuera de servicio. - Pérdida financiera. - Imagen y reputación afectadas. - Violación de obligaciones reglamentarias.
[HW21]	Equipo router de redes	Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad. Errores de configuración. Errores de redes. Errores del administrador	Cualquier usuario que se encuentre en el mismo segmento de red de los routers, conociendo las credenciales, puede acceder vía SSH.	- Sin acceso a los sitios remotos de vigilancia aérea. - Pérdida financiera. - Imagen y reputación afectadas. - Violación de obligaciones reglamentarias.
[HW22]	Equipo switch de redes	Corte de suministro eléctrico. Pérdida de equipos.	Cualquier usuario que se encuentre en el mismo segmento de red de los routers, conociendo las	Fuera de servicio la red LAN de los centros de mando o de sitios remotos.

		Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad. Errores de configuración. Errores de redes. Errores del administrador	credenciales, puede acceder vía SSH.	
[HW23]	Equipo de seguridad de redes	Manipulación de los registros de actividad (log). Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad. Errores de configuración Errores de redes. Errores del administrador.	Cualquier usuario que se encuentre en el mismo segmento de red de los routers, conociendo las credenciales, puede acceder vía SSH.	- Sin acceso a los sitios remotos de vigilancia aérea. - Pérdida financiera. - Imagen y reputación afectadas. - Violación de obligaciones reglamentarias.
[HW24]	Equipo central telefónica	Manipulación de la configuración Acceso no autorizado Errores de configuración. Errores de redes.	- Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	- Comunicaciones de voz fuera de servicio, VoIP, E1, PSTN, etc.
[HW25]	Teléfonos IP	Errores de redes. Errores de configuración. Manipulación de los equipos.	Cualquier usuario puede acceder físicamente a los teléfonos IP y puede cambiar la configuración, dejando sin servicio el mencionado equipo. El equipo permite poner contraseña para impedir el acceso a la configuración, pero no existe un procedimiento para ello.	- Denegación del servicio telefónico en el equipo manipulado.
[COM01]	Red telefónica PSTN	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Avería de origen físico o lógico.	El tendido de fibra óptica externa de la resta es muy bajo. Cualquier vehículo alto puede romper la fibra óptica, lo que ya ha sucedido.	- Denegación del servicio telefónico contratado. - Pérdida de competitividad.
[COM02]	Enlaces MW punto a punto	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración.	El personal de guardia física en las torres de MW no pertenece a la especialidad y no puede solucionar problemas técnicos en el sitio.	- Pérdida de datos e información. - Disponibilidad de los servicios afectada.

		Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.		
[COM03]	Enlaces de radiocomunicaciones	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.	El personal técnico que se encuentra en los sitios remotos no está capacitado para realizar tareas de mantenimiento de primer, segundo y tercer escalón en radiocomunicaciones.	- Señal de radiocomunicaciones fuera de servicio; afecta a las operaciones.
[COM04]	Enlaces vía satélite	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.	- Déficit de personal que realiza la guardia física en los sitios remotos. - El personal técnico que se encuentra en los sitios remotos no está capacitado para realizar tareas de mantenimiento de primer, segundo y tercer escalón en radiocomunicaciones.	
[COM05]	Red local	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Errores de redes. Errores de configuración. Manipulación de los equipos. Indisponibilidad del personal. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.	No existen procedimientos para no manipular el cableado estructurado de la red o la electrónica de red.	Red LAN fuera de servicio; afecta a las operaciones de los sitios remotos y en los centros de mando y control.
[COM06]	Servicio de internet	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Avería de origen físico o lógico. Errores de redes. Errores de configuración. Manipulación de los equipos.	No existe procedimiento para el uso de internet; un equipo de seguridad controla los accesos a internet. Todos los usuarios a través de la red local disponen del servicio.	- Pérdida de información, ataque a la red, denegación de servicios, ransomware.
[Media01]	Disco duro SATA	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de	No existe una política o procedimiento de seguridad de la información para el almacenamiento y	- Pérdida de datos e información. - Pérdida financiera. - Imagen y reputación afectadas.

		almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	custodia de este tipo de dispositivo.	
[Media02]	Disco extraíble RDX	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	No existe una política o procedimiento de seguridad de la información para el almacenamiento y custodia de este tipo de dispositivo.	- Pérdida de datos e información. - Pérdida financiera. - Imagen y reputación afectadas.
[Media03]	Almacenamiento en red.	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	No existe una política o procedimiento de seguridad de la información para el almacenamiento en la red.	- Pérdida de espacio en disco; se puede almacenar cualquier tipo de archivo.
[Media04]	Cintas magnéticas.	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	No existe una política o procedimiento de seguridad de la información para el almacenamiento y custodia de este tipo de dispositivo.	- Pérdida de datos e información. - Pérdida financiera. - Imagen y reputación afectadas.
[Media05]	Memorias USB	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	No existe una política o procedimiento de seguridad de la información para el uso de este tipo de dispositivos.	- Pérdida de datos e información. - Pérdida financiera. - Imagen y reputación afectadas.
[AUX01]	Fuentes de alimentación	Avería de origen físico o lógico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal.	No existen procedimientos para el uso, mantenimiento o reemplazo de los diferentes tipos de alimentación.	- Equipos hardware fuera de servicio, disponibilidad del sistema afectada.

		Manipulación de los equipos. Ataque destructivo.		
[AUX02]	UPS en data centers	Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Condiciones inadecuadas de temperatura y humedad. Fuego. Daños por agua.	Falta de mantenimiento por falta de presupuesto.	- Falla energía comercial: Todos los equipos del sistema se apagan. - Pérdida financiera. - Pérdida de datos e información. - Imagen y reputación afectadas. - Sitios remotos y centros de mando fuera de servicio.
[AUX03]	Generadores eléctricos	Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Condiciones inadecuadas de temperatura y humedad. Fuego. Daños por agua. Ataque destructivo.	Falta de mantenimiento por falta de presupuesto.	- Todos los equipos del sistema se apagan. - Pérdida financiera. - Pérdida de datos e información. - Imagen y reputación afectadas. - Sitios remotos y centros de mando fuera de servicio.
[AUX04]	Equipos de climatización	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Fuego. Daños por agua. Ataque destructivo.	Falta de mantenimiento por falta de presupuesto.	- Todos los equipos del sistema se apagan por sobrecalentamiento. - Pérdida financiera. - Pérdida de datos e información. - Imagen y reputación afectadas. - Sitios remotos y centros de mando fuera de servicio.
[AUX05]	Cableado eléctrico	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Fuego. Ataque destructivo.	Falta de mantenimiento por falta de presupuesto.	- Degradación de servicios.
[AUX06]	Fibra óptica	Ataque destructivo. Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Fuego.	- Falta de mantenimiento por falta de presupuesto. - Déficit de personal para brindar seguridad física.	- Disponibilidad de servicios afectada; no existe comunicación entre los centros remotos y los sitios de vigilancia aérea.
[AUX07]	Mobiliario: mesas, sillas, etc.	Robo. Ataque destructivo. Daños por agua.	Falta de mantenimiento por falta de presupuesto,	- Condiciones adversas de operación.

		Fuego. Desastres naturales.	depreciación de muebles de oficina.	
[L01]	Sitios remotos de vigilancia aérea.	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones. Interrupción de otros servicios y suministros esenciales. Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.	Déficit de personal para la seguridad física de las instalaciones.	- Pérdidas de vidas humanas. - Pérdidas financieras. - Imagen y reputación afectadas.
[L02]	Edificio Centros de Mando.	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones. Interrupción de otros servicios y suministros esenciales. Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.	Área muy extensa, déficit de personal para la seguridad física de las instalaciones.	Pérdidas de vidas humanas. - Pérdidas financieras. - Imagen y reputación afectadas.
[L03]	Contenedores en los sitios remotos.	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones. Interrupción de otros servicios y suministros esenciales. Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.	Área muy extensa, déficit de personal para la seguridad física de las instalaciones.	Pérdidas de vidas humanas. - Pérdidas financieras. - Imagen y reputación afectadas.
[P01]	Usuarios externos	- Fuga de información. - Divulgación de información. - Extorsión - Robo	- No existe VPN para conectarse remotamente a los sistemas y servidores de la empresa.	- Pérdida de datos e información. - Pérdidas financieras. - Pérdida de competitividad.
[P02]	Usuarios internos	- Errores de los usuarios. - Fuga de información. - Indisponibilidad del personal.	- Falta de personal capacitado para cumplir con las tareas asignadas.	- La pérdida de eficacia en el funcionamiento operacional de los sistemas.
[P03]	Operadores	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información.	- Falta de personal capacitado para cumplir con las tareas asignadas.	- Pérdida de datos e información. - Pérdidas financieras. - Imagen y reputación afectadas.

		- Extorsión	- Acuerdos de confidencialidad existentes.	
[P04]	Administradores de sistemas	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.	- Falta de procedimientos en los manuales.	- La pérdida de eficacia en el funcionamiento operacional de los sistemas.
[P05]	Administradores de comunicaciones	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.	- Falta de procedimientos en los manuales.	- La pérdida de eficacia en el funcionamiento operacional de los sistemas. - Inestabilidad en el funcionamiento de sistemas.
[P06]	Administradores de BBDD	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.	- Falta de experiencia y capacitación del personal técnico en gestión de BBDD.	- La pérdida de eficacia en el funcionamiento operacional de los sistemas. - Inestabilidad en el funcionamiento de sistemas. - Pérdida de datos e información.
[P07]	Desarrolladores de software	- Difusión de software dañino. - Fugas de información. - Vulnerabilidades de los programas (software).	- Falta de procedimientos para la introducción de software externo.	- Inestabilidad en el funcionamiento de sistemas. - Pérdida de datos e información.
[P08]	Proveedores	- Fugas de información. - Divulgación de información.	- Falta de contratos de confidencialidad.	- Imagen y reputación afectadas. - Pérdida de datos e información.
[P09]	Administradores de SEG	- Errores de configuración. - Errores de mantenimiento/actualización de programas. - Errores de mantenimiento/actualización de equipos (hardware).	- Falta de personal capacitado para cumplir con las tareas asignadas.	- La pérdida de eficacia en el funcionamiento operacional de los sistemas. - Inestabilidad en el funcionamiento de sistemas.

Fuente: Elaboración propia, basada en la metodología de Magerit v3.

Apéndice G

Evaluación de la probabilidad.

EVALUACIÓN DE LA PROBABILIDAD						
Código activo	**Descripción**	**Responsable**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**
[SW01]	Desarrollo propio – SRCO	MyC	Acceso no autorizado	Los usuarios utilizan la misma contraseña para ingresar a la aplicación.	3	1
[SW02]	Navegador web IE	MyC	Errores de mantenimiento/actualización de programas.	Navegador desactualizado: utiliza versión del año 2017.	1	1
[SW03]	Navegador web Chrome	MyC	Errores de mantenimiento/actualización de programas.	Navegador desactualizado: utiliza versión del año 2017.	1	1
[SW04]	Navegador web Mozilla	MyC	Errores de mantenimiento/actualización de programas.	Navegador desactualizado: utiliza versión del año 2017.	1	1
[SW05]	Ofimática	MyC	Manipulación de programas	Utiliza versiones ofimáticas sin licencia.	3	1
[SW06]	Servidor de ficheros	NET	Errores del administrador Difusión de software dañino. Errores de redes.	No existe un servidor de usuarios que autentique credenciales de clientes; lo hace directamente el servidor de ficheros.	3	2
[SW07]	SO Windows 7	NET	Vulnerabilidades de los programas (software)	- SO vulnerable, última actualización, año 2017. - SO sin hardening. - SO sin antivirus.	2	1
[SW09]	SO Linux	MyC	Caída del sistema por agotamiento de recursos	- SO vulnerable, última actualización, año 2017. - SO sin hardening.	2	1
[SW10]	Windows Server 2003 R2	NET	Vulnerabilidades de los programas (software)	- SO vulnerable, última actualización, año 2017. - SO sin hardening.	2	1
[SW11]	Linux Red Hat	MyC, NET	Caída del sistema por agotamiento de recursos	- SO vulnerable, última actualización, año 2017. - SO sin hardening.	2	1
[SW12]	Linux Debian	NET	Caída del sistema por agotamiento de recursos. Errores del administrador.	- SO vulnerable, última actualización, año 2017. - SO sin hardening.	2	1
[SW13]	Windows Server 2012 R2	MyC	Vulnerabilidades de los programas (software).	- SO vulnerable, última actualización, año 2017. - SO sin hardening.	2	1
[SW14]	Windows Embedded	GES	Errores de mantenimiento/actualización de programas.	- SO sin antivirus.	2	1
[SW15]	Servidor web CPI	NET	Manipulación de la configuración.	- No existe un procedimiento para sacar respaldos cuando se llena la partición /var/log, provocando la caída del servidor.	2	1
[SW16]	Servidor web Neptuno	NET	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.	3	1

				- Existe un solo usuario y contraseña con privilegios de administrador.		
[SW17]	Servidor web CUCM	GES	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	3	1
[SW18]	Cisco ASDM-IDM	NET	Acceso no autorizado	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	3	2
[SW19]	ArcSight Console	MyC	Acceso no autorizado	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	3	2
[SW20]	Provision Physical	MW	Acceso no autorizado	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	3	2
[SW21]	Diagnostic Graphical Display	GES	Acceso no autorizado	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.	3	1
[SW22]	Marc Navigator	RAD	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	3	2
[SW23]	Garex GAP	GES	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	3	1

[SW24]	RCMS II	RAD	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	3	1
[SW25]	SkyWan	SAT	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	3	2
[SW26]	VMware ESXi - NCS	NET	Errores del administrador	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.	2	1
[SW27]	VMware ESXi – Telefonía	NET	Errores del administrador	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.	2	1
[SW28]	VMware ESXi - Blade	MyC	Errores del administrador	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.	2	1
[HW01]	Administración MyC	MyC	Errores de mantenimiento/actualización de equipos (hardware)	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	3	1
[HW02]	Supervisión de comunicaciones	NET, MW, SAT, RAD, SEG.	Errores de mantenimiento/actualización de equipos (hardware)	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	2	1
[HW03]	Administración grabador E1	GES	Errores de mantenimiento/actualización de equipos (hardware)	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	2	1

[HW04]	Operadores de tráfico aéreo	MyC	Indisponibilidad del personal	- Falta de mantenimiento preventivo y hardening del SO.	3	1
[HW05]	PDU Consola Garex	GES	Errores del administrador	- Falta de mantenimiento preventivo.		
[HW06]	SVR grabador de vídeo.	MyC	Acceso no autorizado Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	3	1
[HW07]	SVR Backup - Cintas	MyC	Acceso no autorizado. Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	3	1
[HW08]	SVR Cintas magnéticas	MyC	Acceso no autorizado. Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	3	1
[HW09]	SVR Grabador E1	GES	Acceso no autorizado. Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	3	3
[HW10]	SVR Grabador VoIP	GES	Acceso no autorizado. Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	3	1
[HW11]	SVR Virtualización Blade	MyC	Denegación de servicios. Indisponibilidad del personal.	- Falta de mantenimiento preventivo y hardening del SO.	3	3
[HW12]	SVR Cabina de discos respaldos.	MyC	Denegación de servicios. Indisponibilidad del personal. Acceso no autorizado. Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	3	2
[HW13]	SVR Mensajería – Gateway	MyC	Manipulación de la configuración Errores de redes.	- Falta de mantenimiento preventivo y hardening del SO.	3	1
[HW14]	SVR Seguridad SIEM	SEG	Manipulación de los registros de actividad. Acceso no autorizado. Manipulación de la configuración	- Falta de mantenimiento preventivo y hardening del SO.	3	1
[HW15]	Gestión KVM	GES	Errores de redes. Avería de origen físico o lógico.	- Falta de mantenimiento preventivo y hardening del SO.	2	1
[HW16]	SVR Microondas	GES	Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad.	- Falta de mantenimiento preventivo y hardening del SO. - No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	3	1
[HW17]	SVR Sistema de Comunicación de Voz (SCV)	GES	Errores del administrador. Fallo de servicios de comunicaciones Pérdida de equipos. Errores del administrador. Errores de configuración.	- Falta de mantenimiento preventivo y hardening del SO. - No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	3	1

			Condiciones inadecuadas de temperatura y humedad.			
[HW18]	SVR Radiocomunicaciones	RAD	Pérdida de equipos. Errores del administrador. Errores de configuración. Condiciones inadecuadas de temperatura y humedad.	- Falta de mantenimiento preventivo y hardening del SO. - No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	3	2
[HW19]	Impresora en red	MyC	Manipulación de los equipos. Errores de redes. Errores de los usuarios.	- No existe un procedimiento o control; cualquier usuario que se encuentra en la misma red de la impresora puede imprimir.	1	1
[HW20]	Equipo router satelital	SAT	Errores del administrador. Errores de configuración. Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad.	- Falta de entrenamiento o capacitación al personal técnico para que realice configuraciones avanzadas.	3	2
[HW21]	Equipo router de redes	NET	Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad. Errores de configuración. Errores de redes. Errores del administrador	Cualquier usuario que se encuentre en el mismo segmento de red de los routers, conociendo las credenciales, puede acceder vía SSH.	3	3
[HW22]	Equipo switch de redes	NET	Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad. Errores de configuración. Errores de redes. Errores del administrador	Cualquier usuario que se encuentre en el mismo segmento de red de los routers, conociendo las credenciales, puede acceder vía SSH.	3	3

[HW23]	Equipo de seguridad de redes	NET	Manipulación de los registros de actividad (log). Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad. Errores de configuración Errores de redes. Errores del administrador.	Cualquier usuario que se encuentre en el mismo segmento de red de los routers, conociendo las credenciales, puede acceder vía SSH.	3	3
[HW24]	Equipo central telefónica	NET	Manipulación de la configuración Acceso no autorizado Errores de configuración. Errores de redes.	- Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	2	1
[HW25]	Teléfonos IP	NET	Errores de redes. Errores de configuración. Manipulación de los equipos.	Cualquier usuario puede acceder físicamente a los teléfonos IP y puede cambiar la configuración, dejando sin servicio el mencionado equipo. El equipo permite poner contraseña para impedir el acceso a la configuración, pero no existe un procedimiento para ello.	3	1
[COM01]	Red telefónica PSTN	NET	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Avería de origen físico o lógico.	El tendido de fibra óptica externa de la red PSTN se encuentra muy bajo; cualquier vehículo lo suficientemente alto puede romper la fibra óptica (ya ha sucedido).	3	1
[COM02]	Enlaces MW punto a punto	MW	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.	El personal de guardia física en las torres de MW no pertenece a la especialidad y no puede solucionar problemas técnicos en el sitio.	3	2
[COM03]	Enlaces de radiocomunicaciones	RAD	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo.	El personal técnico que se encuentra en los sitios remotos no está capacitado para realizar tareas de mantenimiento de primer, segundo y tercer escalón en radiocomunicaciones.	3	3

			Extorsión.			
[COM04]	Enlaces vía satélite	SAT	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.	- Déficit de personal que realiza la guardia física en los sitios remotos. - El personal técnico que se encuentra en los sitios remotos no está capacitado para realizar tareas de mantenimiento de primer, segundo y tercer escalón en radiocomunicaciones.	3	3
[COM05]	Red local	NET	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Errores de redes. Errores de configuración. Manipulación de los equipos. Indisponibilidad del personal. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.	No existen procedimientos para no manipular el cableado estructurado de la red o la electrónica de red.	3	2
[COM06]	Servicio de internet	NET	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Avería de origen físico o lógico. Errores de redes. Errores de configuración. Manipulación de los equipos.	No existe procedimiento para el uso de internet; un equipo de seguridad controla los accesos a internet. Todos los usuarios a través de la red local disponen del servicio.	3	1
[Media01]	Disco duro SATA	MyC	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	No existe una política o procedimiento de seguridad de la información para el almacenamiento y custodia de este tipo de dispositivo.	3	1
[Media02]	Disco extraíble RDX	MyC, NET	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información.	No existe una política o procedimiento de seguridad de la información para el almacenamiento y custodia de este tipo de dispositivo.	3	1

			Escapes de información. Difusión de software dañino.			
[Media03]	Almacenamiento en red.	MyC	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	No existe una política o procedimiento de seguridad de la información para el almacenamiento en la red.	3	1
[Media04]	Cintas magnéticas.	MyC	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	No existe una política o procedimiento de seguridad de la información para el almacenamiento y custodia de este tipo de dispositivo.	3	1
[Media05]	Memorias USB	NET, MW, SAT, RAD, SEG, GES, MyC	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	No existe una política o procedimiento de seguridad de la información para el uso de este tipo de dispositivos.	3	1
[AUX01]	Fuentes de alimentación	MyC	Avería de origen físico o lógico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Ataque destructivo.	No existen procedimientos para el uso, mantenimiento o reemplazo de los diferentes tipos de alimentación.	3	2
[AUX02]	UPS en data centers	MyC	Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Condiciones inadecuadas de temperatura y humedad. Fuego.	Falta de mantenimiento por falta de presupuesto.	3	3

			Daños por agua.			
[AUX03]	Generadores eléctricos	MyC	Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Condiciones inadecuadas de temperatura y humedad. Fuego. Daños por agua. Ataque destructivo.	Falta de mantenimiento por falta de presupuesto.	3	3
[AUX04]	Equipos de climatización	MyC, RAD, MW	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Fuego. Daños por agua. Ataque destructivo.	Falta de mantenimiento por falta de presupuesto.	3	3
[AUX05]	Cableado eléctrico	NET, MW, SAT, RAD, SEG, GES, MyC	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Fuego. Ataque destructivo.	Falta de mantenimiento por falta de presupuesto.	3	1
[AUX06]	Fibra óptica	NET	Ataque destructivo. Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Fuego.	- Falta de mantenimiento por falta de presupuesto. - Déficit de personal para brindar seguridad física.	3	3
[AUX07]	Mobiliario: mesas, sillas, etc.	MyC	Robo. Ataque destructivo. Daños por agua. Fuego. Desastres naturales.	Falta de mantenimiento por falta de presupuesto, depreciación de muebles de oficina.	2	1

[L01]	Sitios remotos de vigilancia aérea.	Jefes de sitios remotos	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones. Interrupción de otros servicios y suministros esenciales. Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.	Déficit de personal para la seguridad física de las instalaciones.	3	1
[L02]	Edificio Centros de Mando.	Jefes de Centros de Mando	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones. Interrupción de otros servicios y suministros esenciales. Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.	Área muy extensa, déficit de personal para la seguridad física de las instalaciones.	3	1
[L03]	Contenedores en los sitios remotos.	Jefes de sitios remotos	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones. Interrupción de otros servicios y suministros esenciales. Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.	Área muy extensa, déficit de personal para la seguridad física de las instalaciones.	3	1
[P01]	Usuarios externos	RRHH	- Fuga de información. - Divulgación de información. - Extorsión - Robo	- No existe VPN para conectarse remotamente a los sistemas y servidores de la empresa.	3	2

[P02]	Usuarios internos	Jefes de sitios y CM	- Errores de los usuarios. - Fuga de información. - Indisponibilidad del personal.	- Falta de personal capacitado para cumplir con las tareas asignadas.	3	1
[P03]	Operadores	Jefes de sitios y CM	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión	- Falta de personal capacitado para cumplir con las tareas asignadas. - Acuerdos de confidencialidad existentes.	3	1
[P04]	Administradores de sistemas	NET, MW, SAT, RAD, SEG, GES, MyC	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.	- Falta de procedimientos en los manuales de procedimientos.	3	1
[P05]	Administradores de comunicaciones	NET, MW, SAT, RAD	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.	- Falta de procedimientos en los manuales de procedimientos.	3	1
[P06]	Administradores de BBDD	MyC	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.	- Falta de experiencia y capacitación del personal técnico en gestión de BBDD.	3	1
[P07]	Desarrolladores de software	MyC	- Difusión de software dañino. - Fugas de información. - Vulnerabilidades de los programas (software).	- Falta de procedimientos para la introducción de software externo.	3	1
[P08]	Proveedores	RRHH, jefes CM	- Fugas de información. - Divulgación de información.	- Falta de contratos de confidencialidad.	3	1
[P09]	Administradores de SEG	SEG	- Errores de configuración. - Errores de mantenimiento/actualización de programas. - Errores de mantenimiento/actualización de equipos (hardware).	- Falta de personal capacitado para cumplir con las tareas asignadas.	3	1

Fuente: Elaboración propia, basada en la metodología de Magerit.

Apéndice H

Determinación del nivel de riesgo.

DETERMINACIÓN DEL NIVEL DE RIESGO							
Código activo	**Descripción**	**Responsable**	**Amenaza**	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Riesgo**
[HW11]	SVR Virtualización Blade	MyC	Denegación de servicios. Indisponibilidad del personal.	- Falta de mantenimiento preventivo y hardening del SO.	3	3	9
[COM03]	Enlaces de radiocomunicaciones	RAD	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.	El personal técnico que se encuentra en los sitios remotos no está capacitado para realizar tareas de mantenimiento de primer, segundo y tercer escalón en radiocomunicaciones.	3	3	9
[COM04]	Enlaces vía satélite	SAT	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.	- Déficit de personal que realiza la guardia física en los sitios remotos. - El personal técnico que se encuentra en los sitios remotos no está capacitado para realizar tareas de mantenimiento de primer, segundo y tercer escalón en radiocomunicaciones.	3	3	9
[AUX02]	UPS en data centers	MyC	Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Condiciones inadecuadas de temperatura y humedad. Fuego. Daños por agua.	Falta de mantenimiento por falta de presupuesto.	3	3	9
[AUX03]	Generadores eléctricos	MyC	Interrupción de otros servicios y suministros esenciales.	Falta de mantenimiento por falta de presupuesto.	3	3	9

			Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Condiciones inadecuadas de temperatura y humedad. Fuego. Daños por agua. Ataque destructivo.				
[AUX04]	Equipos de climatización	MyC, RAD, MW	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Fuego. Daños por agua. Ataque destructivo.	Falta de mantenimiento por falta de presupuesto.	3	3	9
[AUX06]	Fibra óptica	NET	Ataque destructivo. Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Fuego.	- Falta de mantenimiento por falta de presupuesto. - Déficit de personal para brindar seguridad física.	3	3	9
[SW06]	Servidor de ficheros	NET	Errores del administrador Difusión de software dañino. Errores de redes.	No existe un servidor de usuarios que autentique credenciales de clientes; lo hace directamente el servidor de ficheros.	3	2	6
[SW18]	Cisco ASDM-IDM	NET	Acceso no autorizado	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	3	2	6
[SW19]	ArcSight Console	MyC	Acceso no autorizado	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	3	2	6
[SW20]	Provision Physical	MW	Acceso no autorizado	- No existe un procedimiento para cambiar las credenciales periódicamente.	3	2	6

				- Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.			
[SW22]	Marc Navigator	RAD	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	3	2	6
[SW25]	SkyWan	SAT	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	3	2	6
[HW12]	SVR Cabina de discos respaldos.	MyC	Denegación de servicios. Indisponibilidad del personal. Acceso no autorizado. Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	3	2	6
[HW18]	SVR Radiocomunicaciones	RAD	Pérdida de equipos. Errores del administrador. Errores de configuración. Condiciones inadecuadas de temperatura y humedad.	- Falta de mantenimiento preventivo y hardening del SO. - No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	3	2	6
[COM02]	Enlaces MW punto a punto	MW	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Caída del sistema por agotamiento de recursos. Indisponibilidad del personal. Manipulación de la configuración. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.	El personal que se encuentra de guardia física en las torres de MW es ajeno a la especialidad y no puede solucionar problemas técnicos en sitio.	3	2	6
[COM05]	Red local	NET	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Errores de redes.	No existen procedimientos para no manipular el cableado estructurado de la red o la electrónica de red.	3	2	6

			Errores de configuración. Manipulación de los equipos. Indisponibilidad del personal. Acceso no autorizado. Manipulación de los equipos. Ataque destructivo. Extorsión.				
[AUX01]	Fuentes de alimentación	MyC	Avería de origen físico o lógico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Manipulación de los equipos. Ataque destructivo.	No existen procedimientos para el uso, mantenimiento o reemplazo de los diferentes tipos de alimentación.	3	2	6
[SW01]	Desarrollo propio – SRCO	MyC	Acceso no autorizado	Los usuarios utilizan la misma contraseña para ingresar a la aplicación.	3	1	3
[SW05]	Ofimática	MyC	Manipulación de programas	Utiliza versiones ofimáticas sin licencia.	3	1	3
[SW16]	Servidor web Neptuno	NET	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	3	1	3
[SW17]	Servidor web CUCM	GES	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	3	1	3
[SW21]	Diagnostic Graphical Display	GES	Acceso no autorizado	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.	3	1	3
[SW23]	Garex GAP	GES	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.	3	1	3
[SW24]	RCMS II	RAD	Manipulación de la configuración	- No existe un procedimiento para cambiar las credenciales periódicamente.	3	1	3

				- Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - Existe un solo usuario y contraseña con privilegios de administrador.			
[HW01]	Administración MyC	MyC	Errores de mantenimiento/actualización de equipos (hardware)	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	3	1	3
[HW04]	Operadores de tráfico aéreo	MyC	Indisponibilidad del personal	- Falta de mantenimiento preventivo y hardening del SO.	3	1	3
[HW05]	PDU Consola Garex	GES	Errores del administrador	- Falta de mantenimiento preventivo.	3	1	3
[HW06]	SVR grabador de vídeo.	MyC	Acceso no autorizado Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	3	1	3
[HW07]	SVR Backup – Cintas	MyC	Acceso no autorizado. Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	3	1	3
[HW08]	SVR Cintas magnéticas	MyC	Acceso no autorizado. Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	3	1	3
[HW09]	SVR Grabador E1	GES	Acceso no autorizado. Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	3	1	3
[HW10]	SVR Grabador VoIP	GES	Acceso no autorizado. Modificación deliberada de la información.	- Falta de mantenimiento preventivo y hardening del SO.	3	1	3
[HW13]	SVR Mensajería – Gateway	MyC	Manipulación de la configuración Errores de redes.	- Falta de mantenimiento preventivo y hardening del SO.	3	1	3
[HW14]	SVR Seguridad SIEM	SEG	Manipulación de los registros de actividad. Acceso no autorizado. Manipulación de la configuración	- Falta de mantenimiento preventivo y hardening del SO.	3	1	3
[HW16]	SVR Microondas	GES	Corte de suministro eléctrico. Pérdida de equipos. Manipulación de los equipos. Ataque destructivo. Extorsión. Condiciones inadecuadas de temperatura y humedad.	- Falta de mantenimiento preventivo y hardening del SO. - No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	3	1	3
[HW17]	SVR Sistema Comunicación de Voz (SCV)	GES	Errores del administrador. Fallo de servicios de comunicaciones Pérdida de equipos.	- Falta de mantenimiento preventivo y hardening del SO.	3	1	3

			Errores del administrador. Errores de configuración. Condiciones inadecuadas de temperatura y humedad.	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.			
[HW24]	Equipo central telefónica	NET	Manipulación de la configuración Acceso no autorizado Errores de configuración. Errores de redes.	- Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	3	1	3
[HW25]	Teléfonos IP	NET	Errores de redes. Errores de configuración. Manipulación de los equipos.	Cualquier usuario puede acceder físicamente a los teléfonos IP y puede cambiar la configuración, dejando sin servicio el mencionado equipo. El equipo permite poner contraseña para impedir el acceso a la configuración, pero no existe un procedimiento para ello.	3	1	3
[COM01]	Red telefónica PSTN	NET	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Avería de origen físico o lógico.	El tendido de fibra óptica externa de la red PSTN se encuentra muy bajo; cualquier vehículo lo suficientemente alto puede romper la fibra óptica (ya ha sucedido).	3	1	3
[COM06]	Servicio de internet	NET	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Avería de origen físico o lógico. Errores de redes. Errores de configuración. Manipulación de los equipos.	No existe procedimiento para el uso de internet; un equipo de seguridad controla los accesos a internet; todos los usuarios, a través de la red local, disponen del servicio.	3	1	3
[Media01]	Disco duro SATA	MyC	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	No existe una política o procedimiento de seguridad de la información para el almacenamiento y custodia de este tipo de dispositivo.	3	1	3
[Media02]	Disco extraíble RDX	MyC, NET	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información.	No existe una política o procedimiento de seguridad de la información para el almacenamiento y custodia de este tipo de dispositivo.	3	1	3

			Fugas de información. Escapes de información. Difusión de software dañino.				
[Media03]	Almacenamiento en red.	MyC	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	No existe una política o procedimiento de seguridad de la información para el almacenamiento en la red.	3	1	3
[Media04]	Cintas magnéticas.	MyC	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	No existe una política o procedimiento de seguridad de la información para el almacenamiento y custodia de este tipo de dispositivo.	3	1	3
[Media05]	Memorias USB	NET, MW, SAT, RAD, SEG, GES, MyC	Condiciones inadecuadas de temperatura y humedad. Degradación de los soportes de almacenamiento de la información. Destrucción de información. Fugas de información. Escapes de información. Difusión de software dañino.	No existe una política o procedimiento de seguridad de la información para el uso de este tipo de dispositivos.	3	1	3
[AUX05]	Cableado eléctrico	NET, MW, SAT, RAD, SEG, GES, MyC	Corte de suministro eléctrico. Interrupción de otros servicios y suministros esenciales. Pérdida de equipos. Indisponibilidad del personal. Fuego. Ataque destructivo.	Falta de mantenimiento por falta de presupuesto.	3	1	3
[L01]	Sitios remotos, vigilancia aérea.	Jefes de sitios remotos	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones. Interrupción de otros servicios y suministros esenciales.	Déficit de personal para la seguridad física de las instalaciones.	3	1	3

			Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.				
[L02]	Edificio Centros de Mando.	Jefes Centros de Mando	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones. Interrupción de otros servicios y suministros esenciales. Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.	Área muy extensa, déficit de personal para la seguridad física de las instalaciones.	3	1	3
[L03]	Contenedores en los sitios remotos.	Jefes de sitios remotos	Fuego. Daños por agua. Desastres naturales. Corte de suministro eléctrico. Fallo de servicios de comunicaciones. Interrupción de otros servicios y suministros esenciales. Indisponibilidad del personal. Acceso no autorizado. Robo. Ataque destructivo. Ocupación enemiga.	Área muy extensa, déficit de personal para la seguridad física de las instalaciones.	3	1	3
[P01]	Usuarios externos	RRHH	- Fuga de información. - Divulgación de información. - Extorsión - Robo	- No existe VPN para conectarse remotamente a los sistemas y servidores de la empresa.	3	1	3
[P02]	Usuarios internos	Jefes de sitios y CM	- Errores de los usuarios. - Fuga de información. - Indisponibilidad del personal.	- Falta de personal capacitado para cumplir con las tareas asignadas.	3	1	3
[P03]	Operadores	Jefes de sitios y CM	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información.	- Falta de personal capacitado para cumplir con las tareas asignadas. - Acuerdos de confidencialidad existentes.	3	1	3

			- Extorsión				
[P04]	Administradores de sistemas	NET, MW, SAT, RAD, SEG, GES, MyC	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.	- Falta de procedimientos en los manuales de procedimientos.	3	1	3
[P05]	Administradores de comunicaciones	NET, MW, SAT, RAD	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.	- Falta de procedimientos en los manuales de procedimientos.	3	1	3
[P06]	Administradores de BBDD	MyC	- Indisponibilidad del personal. - Errores de los usuarios. - Fuga de información. - Divulgación de información. - Extorsión - Errores del administrador.	- Falta de experiencia y capacitación del personal técnico en gestión de BBDD.	3	1	3
[P07]	Desarrolladores de software	MyC	- Difusión de software dañino. - Fugas de información. - Vulnerabilidades de los programas (software).	- Falta de procedimientos para la introducción de software externo.	3	1	3
[P08]	Proveedores	RRHH, jefes CM	- Fugas de información. - Divulgación de información.	- Falta de contratos de confidencialidad.	3	1	3
[P09]	Administradores de SEG	SEG	- Errores de configuración. - Errores de mantenimiento/actualización de programas. - Errores de mantenimiento/actualización de equipos (hardware).	- Falta de personal capacitado para cumplir con las tareas asignadas.	3	1	3
[SW07]	SO Windows 7	NET	Vulnerabilidades de los programas (software)	- SO vulnerable, última actualización año 2017. - SO sin hardening. - SO sin antivirus.	2	1	2
[SW09]	SO Linux	MyC	Caída del sistema por agotamiento de recursos	- SO vulnerable, última actualización año 2017. - SO sin hardening.	2	1	2
[SW10]	Windows Server 2003 R2	NET	Vulnerabilidades de los programas (software)	- SO vulnerable, última actualización año 2017. - SO sin hardening.	2	1	2

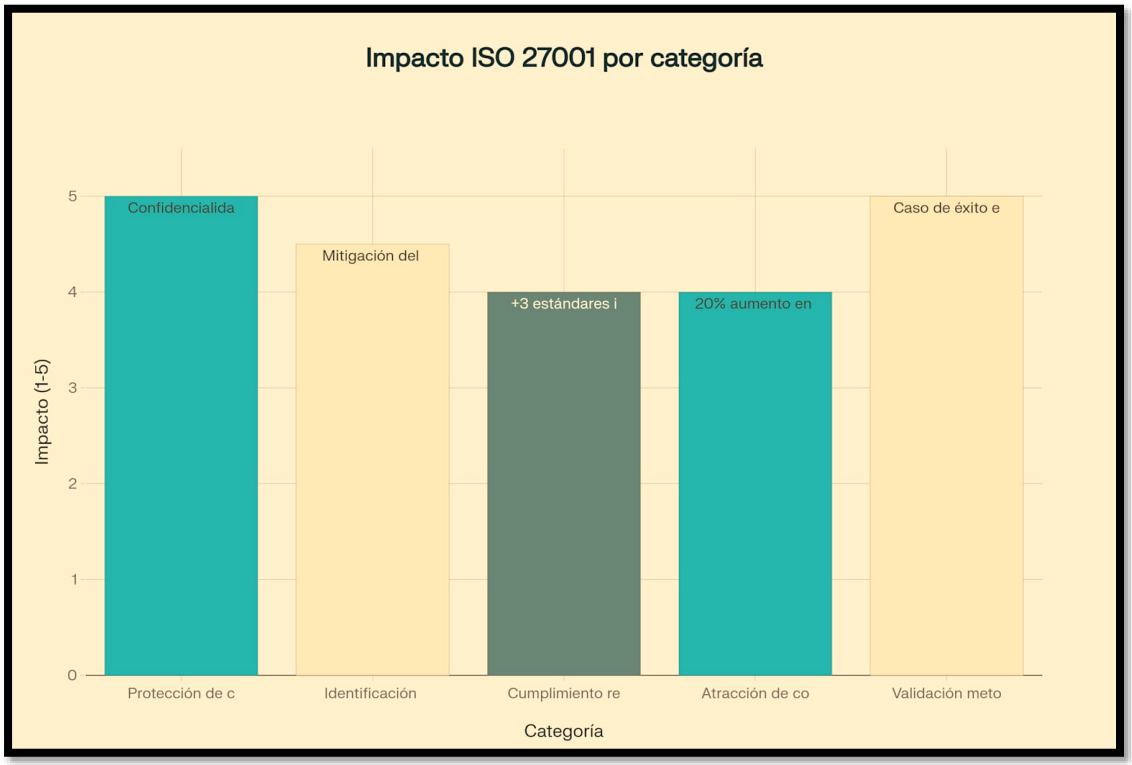
[SW11]	Linux Red Hat	MyC, NET	Caída del sistema por agotamiento de recursos	- SO vulnerable, última actualización año 2017. - SO sin hardening.	2	1	2
[SW12]	Linux Debian	NET	Caída del sistema por agotamiento de recursos. Errores del administrador.	- SO vulnerable, última actualización año 2017. - SO sin hardening.	2	1	2
[SW13]	Windows Server 2012 R2	MyC	Vulnerabilidades de los programas (software).	- SO vulnerable, última actualización año 2017. - SO sin hardening.	2	1	2
[SW14]	Windows Embedded	GES	Errores de mantenimiento/actualización de programas.	- SO sin antivirus.	2	1	2
[SW15]	Servidor web CPI	NET	Manipulación de la configuración.	- No existe un procedimiento para sacar respaldos cuando se llena la partición /var/log, provocando la caída del servidor.	2	1	2
[SW26]	VMware ESXi - NCS	NET	Errores del administrador	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.	2	1	2
[SW27]	VMware ESXi – Telefonía	NET	Errores del administrador	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.	2	1	2
[SW28]	VMware ESXi – Blade	MyC	Errores del administrador	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario.	2	1	2
[HW02]	Supervisión de comunicaciones	NET, MW, SAT, RAD, SEG.	Errores de mantenimiento/actualización de equipos (hardware)	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	2	1	2
[HW03]	Administración grabador E1	GES	Errores de mantenimiento/actualización de equipos (hardware)	- No existe un procedimiento para cambiar las credenciales periódicamente. - Credenciales de acceso registradas en carpetas físicas, visibles a cualquier usuario. - No existen procedimientos para utilizar las mejores prácticas (ITIL) para bloquear pantalla o escritorio.	2	1	2
[HW15]	Gestión KVM	GES	Errores de redes. Avería de origen físico o lógico.	- Falta de mantenimiento preventivo y hardening del SO.	2	1	2

[AUX07]	Mobiliario: mesas, sillas, etc.	MyC	Robo. Ataque destructivo. Daños por agua. Fuego. Desastres naturales.	Falta de mantenimiento por falta de presupuesto, depreciación de muebles de oficina.	2	1	2
[SW02]	Navegador web IE	MyC	Errores de mantenimiento/actualización de programas.	Navegador desactualizado: utiliza versión del año 2017.	1	1	1
[SW03]	Navegador web Chrome	MyC	Errores de mantenimiento/actualización de programas.	Navegador desactualizado: utiliza versión del año 2017.	1	1	1
[SW04]	Navegador web Mozilla	MyC	Errores de mantenimiento/actualización de programas.	Navegador desactualizado: utiliza versión del año 2017.	1	1	1
[HW19]	Impresora en red	MyC	Manipulación de los equipos. Errores de redes. Errores de los usuarios.	- No existe un procedimiento o control; cualquier usuario que se encuentra en la misma red de la impresora puede imprimir.	1	1	1

Fuente: Elaboración propia, basada en la metodología de Magerit.

Apéndice I

Gráfico de barras multifacético.



Nota: Muestra el impacto de la implementación de ISO/IEC 27001 en seguridad operacional.

Este gráfico sintetiza:

- Protección de comunicaciones críticas (confidencialidad, integridad y disponibilidad de datos).
- Identificación de riesgos específicos y mitigación de amenazas sectoriales.
- Cumplimiento regulatorio y alineación con estándares internacionales.
- Atracción de contratos internacionales como diferenciador competitivo.
- Validación metodológica en un entorno de vigilancia aérea.

Apéndice J

Integral de activos, brechas, mejoras e indicadores.

Ítem	Activo	Tipo	Ubicación	CID	Pilotaje	Confiabilidad	Brecha identificada	Mejora implementada	Riesgo residual estimado
1	Radar primario	HW	Torre	555	5	4	Falta de monitoreo continuo	Sistema de monitoreo 24/7	10%
2	Servidor de datos aeronáuticos	Infra	CPD	556	4	5	Backup no probado.	Backup automático y pruebas mensuales.	15%
3	Consola de control radar	SW	Torre	444	4	4	Procedimiento operativo no formal	Documentación y capacitación	12%
4	Personal operador de radar	Personal	Torre	344	5	4	Falta de concienciación	Capacitación y simulacros	20%
5	Enlace de comunicación tierra-aire	Serv	Torre	445	3	4	Fallas en redundancia	Enlace secundario	15%
6	Servidor de backup general	HW	CPD	557	4	5	Respaldos críticos no auditados	Auditorías periódicas	10%
7	Sistema de gestión de vuelos	SW	Oficina de Operaciones	558	4	4	Control de cambios no documentado	Procedimientos de control de cambios	12%
8	Red de comunicaciones internas	Infra	Todas	559	4	4	No hay monitoreo de tráfico.	Monitoreo continuo	15%
9	Sistema de energía de respaldo	Infra	Torre/CPD	560	4	5	Pruebas de energía no periódicas	Pruebas trimestrales	10%
10	Personal de mantenimiento de sistemas	Personal	CPD/Torre	345	5	4	Capacitación irregular	Plan anual de capacitación	15%
11	Documentación de procedimientos críticos	Infra	Archivo Central	561	3	5	Procedimientos desactualizados	Actualización anual	10%
12	Estación meteorológica	HW	Torre	562	3	4	Falta de mantenimiento	Mantenimiento preventivo	12%
13	Sistema ERP	SW	Oficina Administración	566	4	4	Accesos no controlados	Control de usuarios y roles	15%
14	Red Wi-Fi interna	Infra	Todas	567	3	4	Vulnerabilidades no parcheadas	Actualización y monitoreo	12%
15	Cámaras de seguridad	HW	Todas	568	4	4	Áreas no cubiertas	Instalación de cámaras adicionales	15%
16	Sistema de climatización crítica	Infra	CPD/Torre	569	3	5	Filtros y sensores no revisados	Mantenimiento programado	10%
17	Servidor de correos y comunicación	HW	CPD	565	3	4	No hay backups de correos.	Backup automático	12%
18	Terminales de trabajo para control de vuelos	HW	Torre	571	4	4	Procedimientos de uso seguro inexistentes	Manuales y capacitación	15%

19	Software de monitoreo de sistemas	SW	CPD	572	4	4	Alertas no parametrizadas	Configuración de alertas críticas	10%
20	Generadores de emergencia	Infra	CPD/Torre	573	4	5	Pruebas de carga no registradas	Simulaciones periódicas	12%
21	Personal de soporte IT	Personal	Todas	348	5	4	Falta de registro de intervenciones	Sistema de ticketing	15%
22	Sistema de control de accesos	HW/SW	Todas	574	4	4	Fallas en registro de accesos	Auditorías periódicas	10%
23	Servidor de base de datos de vuelos	HW	CPD	575	5	5	Backup incompleto	Plan de respaldo completo	10%
24	Sistema de comunicaciones satelitales	Serv	Torre/CPD	576	4	5	No hay redundancia.	Implementación de enlace secundario	12%
25	Sistema de control de alarmas	SW	CPD	577	3	4	No hay registro de eventos.	Registro automático de incidentes	15%
26	Servidor de aplicaciones financieras	HW	Oficina Administración	578	4	4	Control de acceso privilegiado inexistente	Políticas de control de accesos	12%
27	Sistema de gestión de inventarios	SW	Oficina Administración	563	3	4	Inventario incompleto	Inventario completo y actualizado.	10%
28	Servidores de respaldo de comunicaciones	HW	CPD	570	4	5	No hay pruebas periódicas.	Pruebas trimestrales	12%
29	Personal de operaciones administrativas	Personal	Todas	347	3	4	Procedimientos no formalizados	Manuales y capacitación	15%
30	Servidores de aplicaciones críticas	HW	CPD	579	5	5	Monitorización limitada	Sistema de monitoreo	10%
31	Equipos de telecomunicaciones	HW	Torre/CPD	580	4	4	No hay redundancia.	Implementación de redundancia	12%
32	Sistema de gestión documental	SW	Oficina Administración	581	3	4	Documentos críticos no digitalizados	Digitalización y control de versiones	10%
33	Personal de seguridad cibernética	Personal	CPD	349	5	5	Falta de monitoreo de amenazas	Implementación de SOC interno	12%
34	Servidores de bases de datos de clientes	HW	CPD	582	5	5	Backup parcial	Backup completo y pruebas	10%
35	Software de control de mantenimiento	SW	Oficina de Mantenimiento	583	3	4	Registro de actividades incompleto	Registro completo y seguimiento	12%
36	Sistema de GPS aeronáutico	HW	Torre/hangar	584	5	5	Monitorización limitada	Implementación de alertas automáticas	10%
37	Servidores de comunicaciones internas	HW	CPD	585	4	5	Sin redundancia.	Redundancia y monitoreo	12%

38	Sistemas de ventilación crítica	Infra	CPD/Torre	586	3	4	Mantenimiento no registrado	Plan de mantenimiento preventivo	10%
39	Personal de atención a clientes	Personal	Oficina Comercial	350	3	4	Capacitación irregular	Programa de capacitación	15%
40	Software de planificación de vuelos	SW	Oficina de Operaciones	587	4	4	Cambios no controlados	Procedimientos de control de cambios	12%
41	Servidor de registros administrativos	HW	CPD	588	4	5	Backup no probado.	Pruebas de restauración periódicas	10%
42	Sistema de comunicación interna	Serv	Todas	589	3	4	Fallas de disponibilidad	Monitoreo y redundancia	12%
43	Sistema de reportes operacionales	SW	Oficina de Operaciones	590	4	4	Datos incompletos	Integración y validación	10%
44	Servidores de correo interno	HW	CPD	591	4	4	Backup parcial	Backup completo y pruebas	12%
45	Sistema de control de incendios	HW	Todas	592	3	5	Pruebas no periódicas	Simulacros y pruebas trimestrales	10%
46	Personal de auditoría interna	Personal	Oficina de Auditoría	351	4	5	Procedimientos no estandarizados	Manuales y capacitación	12%
47	Sistema de gestión de riesgos	SW	Oficina Riesgos	593	4	5	Indicadores incompletos	Desarrollo de KPIs completos	10%
48	Servidores de aplicaciones de entrenamiento	HW	Simuladores	594	5	5	Monitoreo limitado	Sistema de monitoreo y alertas	10%
49	Equipos de simulación	HW	Simuladores	595	5	5	No hay registros de uso.	Registro y control de sesiones	12%
50	Personal de control de calidad	Personal	Todas	352	4	4	Capacitación irregular	Programa de capacitación	12%

Apéndice K

Consolidada de validación experta del análisis de brecha ISO/IEC 27001

ID Brecha	Perfil del experto	Años exp.	Certificación principal	Criterio evaluado	Puntaje (1–5)
B01	Auditor ISO 27001	8	Lead Auditor ISO/IEC 27001	Claridad de la brecha	4
B01	Consultor SGSI	10	Lead Implementer ISO 27001	Claridad de la brecha	5
B01	Especialista en riesgos	7	CISM	Claridad de la brecha	4
B01	Ingeniero en seguridad	6	CISSP	Claridad de la brecha	4
B01	Auditor externo	9	ISO 27005	Claridad de la brecha	5
B01	—	—	—	Promedio claridad	4,4
B01	—	—	—	Promedio global	4,5
B01	—	—	—	Decisión final	Aceptada

Apéndice L

Matriz de priorización de controles críticos

Control ISO 27001	Descripción resumida	Criticidad del activo	Nivel de riesgo	Dependencia operativa	Puntaje total	Prioridad
A.8.20	Seguridad de redes	Alta (3)	Alta (3)	Alta (3)	9	Muy alta
A.8.21	Seguridad de servicios de red	Alta (3)	Alta (3)	Media (2)	8	Muy alta
A.5.15	Control de accesos	Alta (3)	Media (2)	Alta (3)	8	Muy alta
A.5.24	Gestión de incidentes	Media (2)	Alta (3)	Alta (3)	8	Muy alta
A.8.16	Monitoreo de actividades	Media (2)	Alta (3)	Alta (3)	8	Muy alta
A.8.13	Respaldo de la información	Alta (3)	Media (2)	Media (2)	7	Alta
A.6.3	Concienciación y formación	Media (2)	Media (2)	Alta (3)	7	Alta
A.5.9	Inventario de información	Media (2)	Media (2)	Media (2)	6	Media
A.7.4	Protección física	Media (2)	Media (2)	Media (2)	6	Media
A.5.1	Políticas de seguridad	Media (2)	Baja (1)	Alta (3)	6	Media

Apéndice M

Diez (10) controles priorizados para comunicaciones

Control ISO	Iniciativa	Horizonte	Justificación
A.8.20	Fortalecer seguridad de red	Quick win	Alto impacto y baja complejidad técnica
A.5.15	Control de accesos	Quick win	Reduce riesgo inmediato de intrusión
A.5.24	Gestión de incidentes	Quick win	Mejora tiempos de respuesta
A.6.3	Capacitación del personal	Quick win	Bajo costo y alta efectividad
A.8.16	Monitoreo de eventos	Mediano plazo	Requiere herramientas especializadas
A.8.21	Seguridad de servicios de red	Mediano plazo	Ajustes técnicos y contractuales
A.8.13	Gestión de respaldos	Mediano plazo	Pruebas y automatización
A.5.9	Inventario de información	Mediano plazo	Requiere levantamiento detallado
A.7.4	Protección física	Mediano plazo	Inversión en infraestructura
A.5.1	Formalización de políticas	Mediano plazo	Aprobación institucional