



UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
SEDE DE CONCEPCIÓN

“Propuesta de mejora para sistemas biométrico de control de acceso”

Trabajo para optar al Título de Ingeniero en Ejecución en
Gestión de la Calidad

Nombre: Ana Jenniffer Llafquen Cordova

Profesor Guía: Víctor Poblete

2025



CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☒ Memoria o trabajo de título; ☐ Tesis de Postgrado;

Título del trabajo: Propuesta de mejora para sistemas biométrico de control de acceso

Nombre del candidato(a): Ana Jenniffer Llafquen Cordova

Carrera / Grado: Ingeniería en Gestión de la Calidad **Campus:**

Concepción; **Departamento:** Química y Medioambiente.

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Víctor Poblete, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL

☒ El trabajo **NO contiene información que amerite confidencialidad** y puede ser publicado de inmediato en repositorio con acceso abierto.

☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (embargo) por:

☐ 6 meses; ☐ 12 meses; ☐ 2 años; ☐ 3 años; ☐ 5 años; ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 14-01-2026 ; **Firma:**

Estudiante o Candidato(a):

Fecha: 14-01-2026

Firma: Ana Llafquen

Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.

Resumen Ejecutivo

Los sistemas de control de acceso biométrico, mediante huella y tarjeta, son fundamentales en los recintos técnicos, ya que permiten restringir el ingreso solo a personal autorizado, proteger equipos e información crítica y mantener la trazabilidad de los accesos. Su implementación contribuye directamente a la seguridad física y a la continuidad operativa de la organización, evitando interrupciones y fortaleciendo el cumplimiento de las políticas de seguridad internas.

En este contexto este trabajo aborda una problemática en la empresa ACOM CONTROL es una compañía especializada en la instalación, mantenimiento y gestión de dispositivos biométricos de acceso. Con una sólida trayectoria de 20 años en el mercado, que la ha posicionado como un referente en el sector gracias a su compromiso con la calidad, innovación y la satisfacción de sus clientes.

Actualmente, ACOM CONTROL ha registrado un aumento significativo en los incidentes reportados por sus dos principales clientes, NORTE y SUR, que en conjunto suman más de 30 sucursales a nivel nacional. Ambos operan en sectores de alta exigencia en materia de seguridad, donde la confiabilidad y continuidad de los sistemas de control de acceso son fundamentales para su operación diaria.

En el presente trabajo se realizará un análisis estadístico de los registros evidencia un total de 192 fallas acumuladas, distribuidas principalmente en siete componentes del sistema.

Abreviaturas

DFD: Diagramas de Flujo de Datos.

FMAE: Análisis de Modos de Fallo y Efectos

HH: Horas Hombre

MTBF: Tiempo Promedio Entre Fallas.

MTTR: Tiempo Promedio de Reparación.

OKS: Sistema de liberación de respaldo.

PHVA: Planificar, Hacer, Verificar y Actuar

RCM: Mantenimiento Centrado en la Confiabilidad.

SGSI: Sistema de Gestión de Seguridad de la Información.



Contenido

CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO	2
2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS	2
3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL	2
4.- FIRMAS.....	2
Resumen Ejecutivo.....	3
Abreviaturas	4
Indicé de Imágenes.....	6
Indicé de Gráficos	6
Indicé de Tablas.....	6
Introducción.....	7
Capítulo 1 Antecedentes Generales	8
1.1 Justificación.....	8
1.2 Objetivos	9
1.2.1 Objetivos General.....	9
1.2.2 Objetivos Específicos	10
1.3 Alcance.....	10
1.4 Metodología	11
1.4.1 Etapa 1.....	11
1.4.2 Etapa 2.....	11
Capítulo 2 Estado del Arte	11
2.1 Antecedentes	11
2.2 Marco Teórico.....	14
2.2.1 Análisis de Modos y Efectos de Falla (FMEA).....	14
2.2.2 Diagrama de Ishikawa (Diagrama Causa–Efecto)	15
2.2.3 Indicadores de Desempeño Operacional y Acuerdos de Nivel de Servicio (SLA)	16
2.2.4 Ciclo PHVA	17
2.3 Propuesta Metodología.....	18
Capítulo 3 Desarrollo	19
3.1 Análisis.....	19
3.2 Verificar	20
3.3 Diagrama de Ishikawa.....	22
3.4 Análisis de FMEA.....	23
3.5 Análisis Costo	26
Conclusión.....	27
Bibliografía	28
Anexos	28



Indicé de Imagenes

IMAGEN 1. ARQUITECTURA ACTUAL DEL SISTEMA DE CONTROL BIOMÉTRICO DE ACCESO. 9

IMAGEN 2. DIAGRAMA DE ISHIKAWA. 23

IMAGEN 3. DISPOSITIVO OKS Y ARQUITECTURA DEL SISTEMA DE CONTROL DE ACCESO. 25

Indicé de Gráficos

GRÁFICO 1. DIAGRAMA DE PARETO POR NÚMERO DE FALLA. 9

GRÁFICO 2. NÚMEROS DE FALLAS POR EQUIPOS. 19

Indicé de Tablas

TABLA 1. ANÁLISIS MODAL DE FALLOS Y EFECTOS. 15

TABLA 2. CUMPLIMIENTO DE SLA (%) POR COMPONENTE. 17

TABLA 3. N° DE FALLAS, COSTOS UNITARIOS POR NÚMERO FALLAS, COSTO TOTAL POR FALLA, HH Y MULTAS. 20

TABLA 4. RESUMEN DE COSTOS TOTAL DE EQUIPOS, % DE COSTO Y % DE COSTO ACUMULADO. 21

TABLA 5. TASA DE REINCIDENCIA (%) POR AÑO. 21

TABLA 6. CUMPLIMIENTO DE SLA (%) POR COMPONENTE. 22

TABLA 7. ANÁLISIS MODAL DE FALLOS Y EFECTOS. 24

TABLA 8. TABLA DE O, S Y D. 24

TABLA 9. MATRIZ DE CRITICIDAD. 24

TABLA 10. PLAN DE ACCIÓN. 26

TABLA 11. COSTOS. 27

TABLA 12. BENEFICIOS PROYECTADOS. 27

TABLA 13. RETORNO (ROI)..... 27

Introducción

La presente memoria se enmarca en la empresa ACOM CONTROL, organización nacional dedicada a la instalación, mantenimiento y gestión de sistemas biométricos de control de acceso. Con más de veinte años de trayectoria en el ámbito de la seguridad tecnológica, la empresa se ha consolidado como un referente en la implementación de soluciones orientadas al resguardo y control de accesos en diversas instituciones del sector público y privado.

El desarrollo de este estudio responde a la necesidad de analizar y evaluar los procesos técnicos asociados a la gestión de sistemas biométricos, con el propósito de identificar fallas recurrentes, determinar sus costos asociados y proponer mejoras que contribuyan a optimizar la continuidad operativa. En este contexto, se abordan las principales actividades que ACOM CONTROL ejecuta, tales como la instalación, el mantenimiento preventivo y correctivo, y la asesoría técnica especializada, todas ellas fundamentales para garantizar la calidad y confiabilidad del servicio.

El trabajo busca aportar una perspectiva analítica que permita fortalecer la gestión técnica y operativa de los sistemas biométricos, promoviendo la eficiencia en el uso de los recursos y la sostenibilidad del servicio en el tiempo. Asimismo, se pretende generar un marco de referencia que sirva de apoyo para la toma de decisiones orientadas a la mejora continua dentro del área de mantenimiento y control tecnológico.

Capítulo 1 Antecedentes Generales

1.1 Justificación

Entre abril de 2024 y septiembre de 2025, ACOM CONTROL ha registrado variaciones en la cantidad de incidentes reportados en los sistemas de control de acceso. Durante este período, los registros indican que las fallas se concentran principalmente en determinados componentes, destacando incrementos del 19,8 % en bases de ventosa, 24 % en lectores biométricos y 27,15 % en ventosas, de acuerdo con los reportes de sus dos principales clientes, Norte y Sur, quienes en conjunto operan más de 30 sucursales a nivel nacional.

Los dos clientes pertenecen a sectores que necesitan la operación ininterrumpida de sistemas de control de acceso, los cuales son parte de sus rutinas normales de seguridad y gestión operativa.

El estudio estadístico de los registros acumulados abarca 192 fallas en total, repartidas entre siete componentes del sistema de control biométrico de acceso. De acuerdo con los contratos de nivel de servicio vigentes, la repetición de problemas en estos componentes ha llevado a que se impongan multas contractuales relacionadas con la reiteración de incidentes en el servicio.

Según el Diagrama de Pareto asociado, las fallas se concentran principalmente en tres componentes: ventosa (27,1 %), lector biométrico (23,9 %) y base de ventosa (19,8 %). En conjunto, estos elementos representan aproximadamente el 71 % del total de los incidentes registrados, de acuerdo con la trazabilidad disponible en los sistemas de la empresa.

La repetición de fallas en componentes críticos tiene un efecto directo sobre la continuidad operativa del cliente y, por ende, sobre su grado de satisfacción. Esto se debe a que reduce la fiabilidad del servicio, aumenta los tiempos de atención y coloca a la empresa ante sanciones contractuales. El presente trabajo ha sido elaborado con el objetivo de examinar las razones detrás de los errores más comunes y sugerir una mejora organizada para disminuir la frecuencia de incidentes, la calidad del servicio brindado por ACOM CONTROL y ayudar a mantener de manera constante los niveles de servicios acordados con sus clientes.

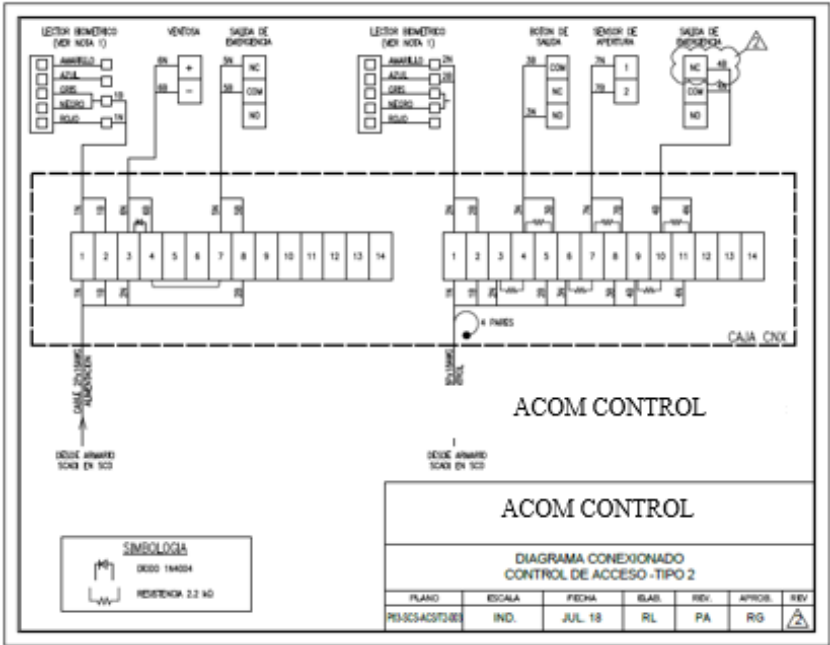


Imagen 1. Arquitectura actual del sistema de control biométrico de acceso.

Fuente: Elaboración Propia.

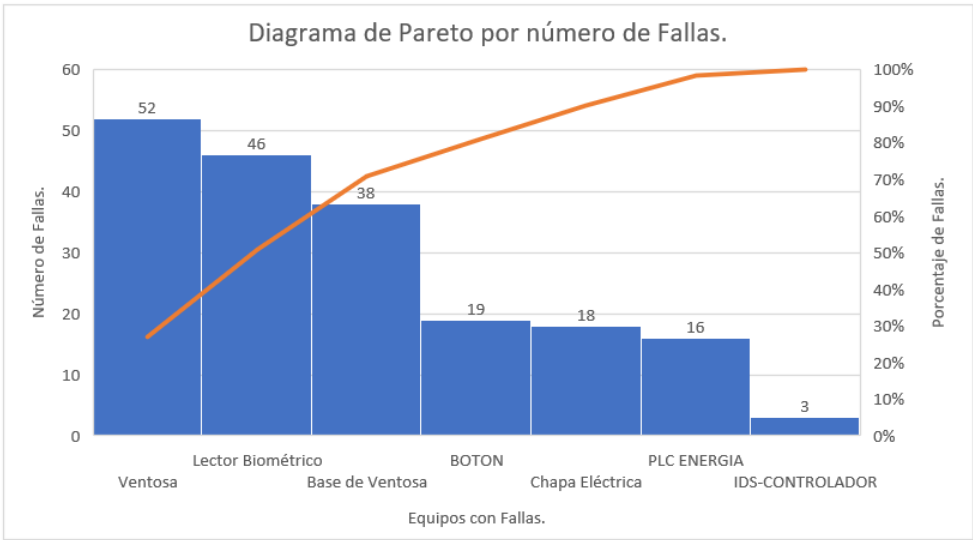


Gráfico 1. Diagrama de Pareto por número de falla.

Fuente: Elaboración Propia.

1.2 Objetivos

1.2.1 Objetivos General

Con el objetivo de reforzar la continuidad del servicio, se propone un proyecto de mejora centrado en reducir las fallas que ocurren en los sistemas y dispositivos biométricos de control de acceso de la compañía ACOM CONTROL. En un periodo de tres meses.

1.2.2 Objetivos Específicos

- Analizar los registros de fallas del sistema biométrico de control de acceso.
- Identificar los modos de falla mediante la aplicación del método FMEA (Failure Mode and Effects Analysis).
- Definir acciones de mejora asociadas a los modos de falla identificados.
- Estimar el impacto operativo y los costos asociados a las fallas del sistema.

1.3 Alcance

El presente estudio se enfoca en el análisis de los incidentes asociados al funcionamiento de los sistemas de control de acceso implementados por la empresa ACOM CONTROL en las sucursales de sus clientes Norte y Sur, quienes en conjunto operan más de 30 dependencias a nivel nacional.

El cliente Norte cuenta con 21 sucursales, distribuidas en las regiones de Arica y Parinacota, Tarapacá, Antofagasta, Atacama y Coquimbo. Por su parte, el cliente Sur dispone de 10 sucursales, ubicadas en las regiones de Biobío, La Araucanía, Los Ríos y Los Lagos.

El estudio se delimita temporalmente al período comprendido entre abril de 2024 y septiembre de 2025, tomando en cuenta solo los datos de fallas que sucedieron durante ese periodo. La finalidad del análisis se orienta a identificar las características de las fallas reportadas, así como su relación con factores operativos, de mantenimiento y componentes del sistema que inciden en la continuidad del servicio.

El alcance del proyecto se limita al análisis de las averías registradas en los sistemas de control de acceso de los clientes Norte y Sur durante el período definido. La información utilizada en el estudio mantiene carácter confidencial, motivo por el cual los datos han sido modificados, resguardando la identidad de los clientes y la integridad de la información contractual.

1.4 Metodología

1.4.1 Etapa 1

Caracterización Descriptiva de las Fallas

En esta etapa, el estudio se centra en describir las fallas reportadas en los sistemas de control de acceso instalados por ACOM CONTROL. El análisis considera la distribución, frecuencia y tipos de incidentes presentados en las sucursales de los clientes Norte y Sur, quienes operan más de 30 dependencias a nivel nacional. Para ello, se examinan los registros correspondientes al periodo comprendido entre abril del 2024 y septiembre del 2025, identificando el comportamiento de las fallas según región, local técnico y componente afectado.

1.4.2 Etapa 2

Análisis Correlacional de Incidencias y Factores Operativos

La segunda etapa incorpora un enfoque correlacional dirigido a explorar la relación entre la recurrencia de fallas y diversos factores operativos, de mantenimiento o administrativos que podrían incidir en la continuidad del servicio. Este análisis permite identificar patrones o asociaciones entre variables como tipo de componente, frecuencia de incidentes y condiciones de operación, sin pretender establecer causalidades directas.

Capítulo 2 Estado del Arte

2.1 Antecedentes

ACOM CONTROL es una empresa nacional dedicada a la instalación, mantenimiento y gestión de sistemas y dispositivos biométricos de control de acceso. Con más de veinte años de operación en el sector, la organización trabaja con tecnologías orientadas al control de ingreso y a la administración de accesos en diversas instalaciones.

La empresa cuenta con un equipo técnico y profesional conformado por aproximadamente 100 trabajadores, con formación en áreas como electrónica, tecnologías de la información y gestión de sistemas. Sus operaciones se desarrollan a nivel nacional y abarcan organizaciones del ámbito industrial, instituciones públicas, establecimientos educacionales, entidades de salud y empresas manufactureras.

Entre los principales servicios que ofrece la empresa se encuentran:

- Instalación de dispositivos biométricos: implementación de sistemas de control de acceso que utilizan mecanismos de identificación como huella digital, tarjeta de proximidad, entre otros.
- Mantenimiento preventivo y correctivo: actividades orientadas a mantener la continuidad operativa de los sistemas instalados y a resolver fallas notificadas por los clientes.
- Consultoría técnica: diagnósticos de infraestructura, diseño de soluciones de control de acceso y apoyo en la implementación de tecnologías de seguridad.

Estos servicios requieren la integración de hardware y software, conectividad con sistemas de red y cumplimiento de protocolos asociados a la gestión de datos, lo que implica procedimientos estandarizados de mantenimiento y soporte técnico.

El Área de Mantenimiento tiene como propósito asegurar la operatividad y trazabilidad de los sistemas instalados. Su estructura se organiza en tres zonas territoriales (Norte, Centro y Sur), coordinadas desde una plataforma central encargada de gestionar recursos, personal y prioridades de atención.

El área utiliza dos niveles de trabajo:

1. Mantenimiento preventivo: programado periódicamente e incluye inspección, limpieza y pruebas de funcionamiento.
2. Mantenimiento correctivo: realizado frente a fallas detectadas o reportadas, con énfasis en restablecer el funcionamiento del sistema.

Todas las actividades se gestionan mediante órdenes de trabajo digitalizadas, lo que permite mantener trazabilidad de las intervenciones, generar reportes y construir historiales por equipo o cliente.

El flujo de información relacionado con una avería se inicia cuando el cliente notifica el incidente a través de los canales disponibles. A partir de ello:

1. El departamento de soporte registra el caso y genera una orden de trabajo.
2. Se asigna un técnico para la atención en terreno.
3. El técnico realiza el diagnóstico, registra la causa y detalla las acciones ejecutadas y los repuestos utilizados.
4. La información es incorporada al sistema central de mantenimiento para su seguimiento.

ACOM CONTROL mantiene una base de datos histórica que consolida los registros de fallas y mantenimientos. A partir de esta información, la empresa obtiene indicadores técnicos como:

- Porcentaje de fallas por componente: identificar qué componentes concentran la mayor proporción de incidentes. En este punto según trazabilidad del periodo analizado se observan las mayores incidencias en los siguientes equipos: 52 fallas de Ventosa, 46 fallas de Lector biométrico y 38 fallas de Base de ventosa.
- Tasa de reincidencia de fallas: Este indicador muestra la frecuencia de fallas en un solo componente o equipo, según el registro anual disponible, lo que posibilita una evaluación inicial de la eficacia de las acciones correctivas implementadas.
- Porcentaje de fallas resueltas dentro del plazo (SLA): El valor que se obtiene para el año estudiado posibilita la medición del nivel de cumplimiento de los plazos de atención establecidos, lo cual puede servir como punto de referencia para comparaciones posteriores.
- Cumplimiento del mantenimiento preventivo programado: La ejecución del mantenimiento preventivo planificado, en términos de resultados anuales de este indicador, proporciona una base para el control y seguimiento en los períodos subsiguientes.

Los indicadores definidos permiten caracterizar el comportamiento del sistema de control de acceso desde una perspectiva operativa y de mantenimiento. El porcentaje de fallas por componente facilita la identificación de aquellos elementos que concentran una mayor proporción de incidentes, aportando información relevante para la priorización de análisis y acciones técnicas. Por su parte, la tasa de reincidencia de fallas permite identificar la repetición de incidentes en un mismo componente o equipo, entregando antecedentes sobre la recurrencia de fallas y su relación con la efectividad de las intervenciones realizadas.

El porcentaje de incidentes que se solucionan dentro del periodo establecido (SLA) ofrece una evaluación imparcial del rendimiento del proceso de atención y resolución de problemas, posibilitando examinar la realización de los plazos fijados y su efecto en la continuidad operativa del servicio. Además, el mantenimiento preventivo programado permite comprobar la realización de las actividades planificadas según las pautas establecidas, lo que brinda un marco relevante para analizar el rendimiento de las fallas y los resultados logrados.

Estos indicadores, en su totalidad, posibilitan la evaluación de tendencias, respaldan la planificación de mejoras y sustentan el proceso de toma de decisiones durante el mantenimiento. Las metodologías documentadas en la literatura técnica, como el análisis de modos y efectos de fallas (FMEA) y el mantenimiento centrado en la confiabilidad (RCM), que son frecuentemente utilizados en contextos donde se utilizan sistemas electrónicos y de automatización, son las que sirven como base para analizar el sistema. Investigaciones recientes (como las de Ben-Daya et al., 2021 y Sharma & Yadava, 2018) subrayan que estas metodologías hacen más fácil la detección de modos de falla importantes, el establecimiento

de prioridades para las intervenciones y la mejora de los planes de mantenimiento, lo cual es relevante en situaciones donde mantener operativos los sistemas de control de acceso es esencial para la administración cotidiana.

2.2 Marco Teórico

El presente marco teórico aborda los principales conceptos y herramientas utilizados para el análisis del desempeño operativo de los sistemas de control de acceso biométrico y la evaluación de sus fallas. Los contenidos desarrollados incluyen el Análisis de Modos y Efectos de Falla (FMEA), el Diagrama de Ishikawa, los principios de confiabilidad en sistemas técnicos y el uso de indicadores de desempeño operacional, particularmente aquellos asociados al cumplimiento de niveles de servicio (SLA).

Estas herramientas posibilitan estructurar el análisis de las fallas registradas, describir su comportamiento temporal y respaldar la evaluación objetiva del impacto que tiene en la operación el sistema, sin determinar relaciones directas de causalidad. Se exponen a continuación los fundamentos teóricos de cada componente, teniendo en cuenta su utilización, alcance y relevancia en situaciones donde son esenciales tanto la continuidad del servicio como la administración del mantenimiento.

2.2.1 Análisis de Modos y Efectos de Falla (FMEA)

El Análisis de Modos y Efectos de Falla (FMEA) es una metodología sistemática utilizada para identificar, evaluar y priorizar los posibles modos de falla en un sistema, equipo o proceso, considerando sus efectos sobre la operación y la seguridad. Su propósito principal es anticipar problemas antes de que ocurran, permitiendo implementar acciones preventivas y correctivas que reduzcan el impacto operativo y económico de las fallas.

Este enfoque constituye un pilar fundamental en la ingeniería de mantenimiento y en la gestión de la confiabilidad, especialmente en sistemas críticos donde la continuidad del servicio es esencial. El FMEA se basa en la identificación de tres factores clave: Ocurrencia (O), que mide la frecuencia con que se presenta la falla; Severidad (S), que evalúa la magnitud de sus consecuencias; y Detección (D), que estima la capacidad de identificar la falla antes de que afecte al sistema. La combinación de estos factores permite calcular el Número de Prioridad de Riesgo (RPN), indicador que orienta la toma de decisiones sobre qué fallas deben ser atendidas con mayor urgencia.

Entre los beneficios de aplicar FMEA se encuentran la posibilidad de priorizar recursos de mantenimiento, mejorar la confiabilidad de los equipos y establecer planes de acción más efectivos. Asimismo, facilita la comunicación entre áreas técnicas y de gestión, al proporcionar un lenguaje común para evaluar riesgos y definir estrategias de mejora.

En la Tabla se muestra, como ejemplo práctico, cómo se aplica la metodología FMEA a elementos cruciales de un sistema de control de acceso. En ella se reconocen los modos de falla más relevantes, sus consecuencias operativas, las posibles causas y la valoración de los elementos de Severidad (S), Ocurrencia (O) y Detección (D). El producto de estos tres factores determina el Número de Prioridad de Riesgo (NPR).

Los resultados permiten que se prioricen las fallas que tienen más impacto en la seguridad y la continuidad del servicio, como las asociadas al lector biométrico y a la ventosa, que son las que muestran los valores de NPR más altos. A partir de este análisis, se establecen acciones de seguimiento, preventivas y correctivas con el objetivo de disminuir la posibilidad de que sucedan y atenuar sus consecuencias.

ANÁLISIS MODAL DE FALLOS Y EFECTOS								
Componente conjunto	Modo de fallo	Efectos de fallo	Causa del fallo	Fallo				Recomendación, acciones correctoras y seguimiento
				O	S	D	NPR	
Ventosa	Ventosa no succiona / desprendimiento	Puerta no se abre o no queda bloqueada → interrupción acceso, reclamos, multas	Desgaste mecánico, suciedad, instalación incorrecta, repuesto de baja calidad	9	9	8	648	Mantenición preventiva; revisión de fijaciones; cambio oportuno; estandarizar repuestos; seguimiento MTTR.
Lector biométrico	No lectura / no responde / rechazo de usuarios	Imposibilidad de validar identidad → retrasos operativos y reclamos	Suciedad en lector, firmware desactualizado, fallas en alimentación o interfaz	9	8	8	576	Limpieza periódica; actualización de firmware; pruebas funcionales; stock de reemplazo; monitoreo de fallas.
Base de ventosa	Base fisurada / anclaje suelto	Ventosa no sujeta correctamente → falla de cierre	Corrosión, montaje incorrecto, vibraciones, piezas incompatibles	8	7	7	392	Inspección y ajuste de anclajes; reemplazo precoz; uso de repuestos homologados.
Chapa eléctrica	Chapa atascada / no energiza	Puerta no abre → bloqueo de acceso, riesgo operativo	Solenoides quemados, fallas en cableado, falta de tensión, contactos sucios	7	5	6	210	Verificación eléctrica; limpieza de contactos; reemplazo de solenoide; prueba post-mantenición.
Chapa eléctrica	Reinicio / pérdida IO / fallo control remoto	Pérdida de apertura remota o lógica de control → impacto crítico en operaciones	Variación de tensión/sobretensiones, firmware inestable, cableado defectuoso	7	4	6	168	Protección eléctrica; actualización de firmware; respaldo de programa; monitoreo de reinicios.
Botón emergencia	Pulsador atascado o mal funciona / activaciones falsas	Apertura/alarma no intencional o no funciona en emergencia → riesgo seguridad o paradas	Ingreso de suciedad, vandalismo, desgaste mecánico	5	3	4	60	Prueba funcional regular; limpieza; reemplazo inmediato si falla; protección antivandalismo.
IDS – Controlador	Alarmas falsas / pérdida de comunicación	Alarmas innecesarias o falta de alertas → sobrecarga operativa o falta de detección	Ingreso de suciedad, vandalismo, desgaste mecánico	6	2	4	48	Revisión de configuración; calibración; monitoreo de comunicación; pruebas periódicas.

Tabla 1. Análisis modal de fallos y efectos.

Fuente: Elaboración Propia.

2.2.2 Diagrama de Ishikawa (Diagrama Causa-Efecto)

El diagrama de Ishikawa, también denominado diagrama causa-efecto o de espina de pescado, es un instrumento analítico que se emplea para detectar y clasificar sistemáticamente las posibles causas que dan lugar a un efecto o problema específico. Se utiliza a menudo en la evaluación de procesos técnicos, el análisis de fallos y los estudios de calidad.

Esta técnica posibilita la categorización de las causas potenciales en grupos generales, típicamente vinculados con elementos como individuos, procedimientos, equipos, materiales, ambiente y gestión. Así se logra una perspectiva estructurada del problema estudiado. En contraste con las metodologías cuantitativas, el Diagrama de Ishikawa es fundamentalmente

descriptivo y exploratorio, y está diseñado para ayudar a entender el entorno donde ocurren los fallos.

Esta herramienta es beneficiosa para estructurar eventuales factores relacionados con el incumplimiento de SLA o con las fallas frecuentes en el análisis de sistemas de control de acceso, por ejemplo, problemas en la configuración, limitaciones operativas, defectos en los procedimientos de mantenimiento, condiciones ambientales desfavorables o fallas de componentes. Su utilización posibilita la adición a indicadores de rendimiento y métodos como el FMEA, brindando una perspectiva organizada sobre los elementos que podrían afectar el funcionamiento del sistema, sin sacar conclusiones causales definitivas.

2.2.3 Indicadores de Desempeño Operacional y Acuerdos de Nivel de Servicio (SLA)

Los indicadores de desempeño operacional son herramientas de medición que posibilitan el análisis del rendimiento de los procesos operativos y técnicos a través de variables que pueden ser cuantificadas. Estos indicadores simplifican la revisión de la conducta de las fallas, los periodos de respuesta y el desempeño de las actividades de mantenimiento dentro del marco de los sistemas para controlar el acceso.

En este contexto, los Acuerdos de Nivel de Servicio (SLA, por sus siglas en inglés) determinan estándares formales relacionados con los plazos máximos para la atención y solución de incidentes. Estos acuerdos se emplean como referencia para valorar el rendimiento del servicio, sin que esto implique necesariamente un análisis de responsabilidades o causas.

La capacidad de llevar a cabo evaluaciones objetivas, que se pueden comparar con el tiempo y que son beneficiosas para respaldar la toma de decisiones contractuales y operativas, está entre los principales beneficios de estos indicadores. Sin embargo, estos indicadores únicamente evalúan el desempeño del servicio y no tienen en cuenta directamente elementos técnicos, cualitativos o de contexto que pueden afectar los resultados.

Los hallazgos del periodo de análisis indican que diversos elementos esenciales tienen niveles de cumplimiento de SLA más bajos que la meta establecida. Mientras que algunos equipos llegan al 100 % de cumplimiento, otros, como el lector biométrico, la chapa eléctrica y la ventosa, muestran diferencias notables; esto afecta la continuidad operacional del sistema de control de acceso. Estos indicadores posibilitan la evaluación del rendimiento del servicio, sin embargo, por sí mismos no aclaran los elementos técnicos que causan el incumplimiento.

Equipo	SLA objetivo (%)	Resultado anual (%)	Estado de cumplimiento	Interpretación
Ventosa	95	71,2	No cumple	Alto impacto en continuidad del servicio
PLC Energía	95	87,5	No cumple	Riesgo operativo moderado
Base de Ventosa	95	86,8	No cumple	Requiere mejora en mantenimiento
Chapa Eléctrica	95	77,8	No cumple	Incumplimiento recurrente
Lector Biométrico	95	82,6	No cumple	Afecta tiempos de acceso
Botón	95	100	Cumple	Desempeño adecuado
IDS-Controlador	95	100	Cumple	Desempeño estable

Tabla 2. Cumplimiento de SLA (%) por componente.

Fuente: Elaboración Propia.

2.2.4 Ciclo PHVA

El ciclo PHVA (Planificar, Hacer, Verificar y Actuar) es un método de gestión enfocado en la mejora continua de los procesos, que se emplea con frecuencia en las áreas de calidad y mantenimiento. Su propósito es estructurar las actividades de manera sistemática para poder reconocer problemas, establecer acciones y evaluar los resultados.

Se utilizan métricas como el MTTR (Tiempo Medio de Reparación) y el MTBF (Tiempo Medio Entre Fallas) en la administración del mantenimiento. El MTTR, que hace referencia al tiempo medio de reparación y muestra la eficacia en la recuperación del servicio, contrasta con el MTBF, que mide el tiempo promedio de funcionamiento entre fallas y está relacionado con la confiabilidad de los equipos. El cumplimiento de los Acuerdos de Nivel de Servicio (SLA) se ve beneficiado directamente por ambos indicadores, pues un MTBF elevado disminuye la periodicidad de las averías y un MTTR bajo hace posible reestablecer el servicio en los plazos acordados.

Durante la fase de planificación, se examinan los datos históricos y se establecen metas de mejora tomando en cuenta el MTBF, el MTTR y el SLA. La fase de Hacer se refiere a la implementación de las acciones definidas, como el mantenimiento correctivo o preventivo. En la etapa de Verificación, se analizan los resultados a través del monitoreo de los indicadores, comparando las cifras logradas con las metas fijadas. Por último, en la fase Actuar se normalizan y adaptan las mejoras que se han puesto en marcha.

El ciclo PHVA permite que la toma de decisiones se base en indicadores y que haya una mejora constante; no obstante, para provocar impactos verdaderos, es necesario contar con información confiable y compromiso organizacional. Por esta razón, debe combinarse con metodologías como RCM o FMEA.

2.3 Propuesta Metodología

La metodología propuesta en esta investigación se basa en el ciclo PHVA (Planificar, Hacer, Verificar y Actuar) e incorpora instrumentos de análisis empleados en la ingeniería de mantenimiento y en la exploración de la fiabilidad de sistemas técnicos. En esta situación, se utilizan el Diagrama de Ishikawa, el análisis de modos y efectos de falla (FMEA) y los indicadores de desempeño operacional, acorde con los conceptos teóricos que se han desarrollado.

En la fase Planificar, se realiza el análisis de los registros históricos de fallas del sistema biométrico de control de acceso, considerando su frecuencia, distribución por componente y recurrencia. Esta etapa permite delimitar el alcance del análisis y establecer una base objetiva de información para el estudio.

El Diagrama de Ishikawa se utiliza en la etapa Hacer para clasificar y organizar los elementos que contribuyen a la ocurrencia de fallas, teniendo en cuenta las dimensiones operativas, técnicas y de gestión. El FMEA se emplea, además, para determinar los modos de fallo importantes del sistema y examinar sus impactos operativos, conservando una perspectiva estructurada y preventiva.

En la fase Verificar, se evalúa el desempeño del sistema mediante el análisis de indicadores operacionales, tales como la tasa de reincidencia de fallas, los tiempos de atención y resolución, el cumplimiento de los plazos establecidos en los acuerdos de nivel de servicio (SLA) y los indicadores de confiabilidad asociados. Esta etapa permite contrastar los resultados obtenidos y analizar su comportamiento en el período definido.

Por último, en la etapa Actuar se establecen medidas de mejora con el propósito de tratar los modos de fallo identificados, teniendo en cuenta los hallazgos del análisis FMEA y las métricas operativas. Estas acciones se proponen como insumos para la optimización de la mejora del rendimiento operativo del sistema de control de acceso y el proceso de mantenimiento.

Capítulo 3 Desarrollo

3.1 Análisis

Planificación: Estudio de los registros de fallas del sistema biométrico de control de acceso.

Durante la fase de planificación del ciclo PHVA, se lleva a cabo un análisis de los registros históricos de fallas en el sistema biométrico de control de acceso, que abarcan desde abril del 2024 hasta septiembre del 2025. El objetivo es describir cómo se comporta con el paso del tiempo.

La distribución del número de fallas registradas por tipo de equipo a lo largo de ese periodo se muestra en el siguiente gráfico. Esta información posibilita distinguir los componentes con más frecuencia de incidentes y sentar una base objetiva para definir y priorizar acciones técnicas en las etapas de mantenimiento.

Las fallas más frecuentes se concentran en los dispositivos electromecánicos y biométricos, componentes críticos para el correcto funcionamiento de los sistemas de control de acceso. Estas incidencias generan interrupciones en los puntos de acceso a los recintos, retrasos en la validación de identidad y afectan directamente la continuidad operacional del cliente.

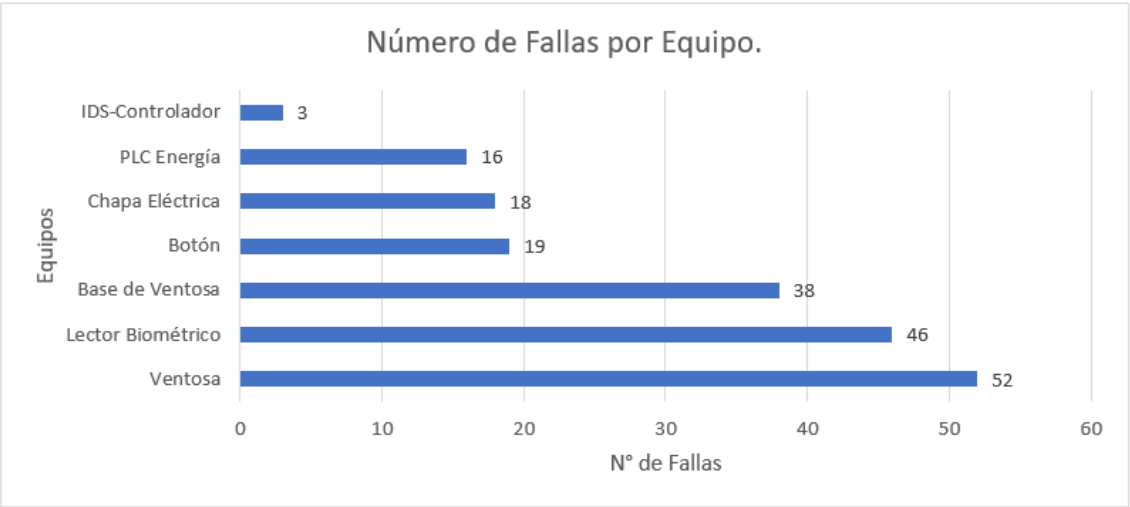


Gráfico 2. Números de Fallas por Equipos.

Fuente: Elaboración Propia.

3.2 Verificar

Evaluación del impacto operativo y de los costos asociados a las fallas del sistema.

A continuación, se presenta una tabla que consolida el análisis de fallas por tipo de equipo, detallando el número de incidencias, el costo unitario de reposición, el costo total por fallas acumuladas, el costo de horas hombre (HH) asociadas a la atención técnica, y las multas aplicadas por repetitividad, conforme a los compromisos establecidos en los SLA.

Para el cálculo del costo total por falla se consideró tanto el valor de reposición del componente afectado como el costo de la mano de obra requerida para su diagnóstico, traslado y reemplazo. El costo de HH fue estimado en función del tiempo promedio de intervención por tipo de equipo, multiplicado por la tarifa horaria vigente del personal técnico.

La información utilizada proviene de registros internos de planificación, hojas de servicio y tarifas operativas actualizadas del área de operaciones de ACOM CONTROL. Este enfoque permite cuantificar de manera integral el impacto económico de cada incidente, facilitando la evaluación del cumplimiento de los SLA y la identificación de oportunidades de mejora en la gestión de activos críticos.

Equipo	N° de Fallas	Costo Falla Uni.	Costo Total x Falla	Costo HH	Multas	Total
Ventosa	52	\$ 650.000	\$ 33.800.000	\$ 1.245.000	\$ 30.000.000	\$ 65.045.000
PLC Energía	16	\$ 1.300.000	\$ 20.800.000	\$ 540.000	\$ 4.000.000	\$ 25.340.000
Base de Ventosa	38	\$ 450.000	\$ 17.100.000	\$ 1.245.000	\$ 10.000.000	\$ 28.345.000
Chapa Eléctrica	18	\$ 800.000	\$ 14.400.000	\$ 585.000	\$ 8.000.000	\$ 22.985.000
Lector Biométrico	46	\$ 150.000	\$ 6.900.000	\$ 1.530.000	\$ 16.000.000	\$ 24.430.000
Botón	19	\$ 130.000	\$ 2.470.000	\$ 625.000	-	\$ 3.095.000
IDS-Controlador	3	\$ 80.000	\$ 240.000	\$ 90.000	-	\$ 330.000
Total	192	\$ 3.560.000	\$ 95.710.000	\$ 5.860.000	\$ 68.000.000	\$169.570.000

Tabla 3. N° de fallas, Costos unitarios por número fallas, Costo total por falla, HH y Multas.

Fuente: Elaboración Propia.

En la siguiente tabla se observa costo total por equipo, % costo y % costo acumulado, los datos pertenecen al periodo de abril 2024 a septiembre 2025.

Equipo	Costo Total	% Costo	% Costo Acumulado
Ventosa	\$ 65.045.000	38,4%	38,4%
PLC Energía	\$ 25.340.000	14,9%	53,3%
Base de Ventosa	\$ 28.345.000	16,7%	70,0%
Chapa Eléctrica	\$ 22.985.000	13,6%	83,6%
Lector Biométrico	\$ 24.430.000	14,4%	98,0%
Botón	\$ 3.095.000	1,8%	99,8%
IDS-Controlador	\$ 330.000	0,2%	100,0%
Total general	\$ 169.570.000		

Tabla 4. Resumen de costos total de equipos, % de costo y % de costo acumulado.

Fuente: Elaboración Propia.

La tasa anual de reincidencia de fallas por componente, que se calculó a partir del estudio de los registros históricos del sistema de control de acceso, se presenta en la tabla siguiente. Se clasificó como reincidente cualquier falla que se repitió en un mismo componente o equipo durante el lapso analizado. Esto posibilita una disminución de la variabilidad mensual y una interpretación más clara y comparable de los resultados.

Esta perspectiva a lo largo de un año ofrece una visión más constante del desempeño de los equipos, facilitando el reconocimiento de tendencias de deterioro, la valoración de la eficacia de las medidas correctivas aplicadas y el fortalecimiento del cumplimiento de los SLA a través de tácticas preventivas y predictivas.

Tasa de reincidencia (%) por año.		
Equipo	Reincidencia (%) 2024	Reincidencia (%) 2025
Ventosa	11,5	15,6
PLC Energía	3,1	5,2
Base de Ventosa	8,9	10,9
Chapa Eléctrica	4,2	5,2
Lector Biométrico	11,5	12,5
Botón	3,1	6,8
IDS-Controlador	1,6	0,0

Tabla 5. Tasa de reincidencia (%) por año.

Fuente: Elaboración Propia.

La tabla que sigue a continuación muestra el porcentaje de cumplimiento de los SLA por componente, determinado con base en la cantidad de fallas atendidas dentro del plazo acordado en relación con el total de incidentes reportados para cada equipo. Este indicador mide el nivel de cumplimiento con los estándares de servicio establecidos y la eficacia operacional.

Los hallazgos muestran variaciones en la magnitud de cumplimiento de los SLA entre los diferentes componentes, con cifras que fluctúan entre el 71,2 % y el 100 % durante el período examinado. El IDS-controlador y el botón alcanzaron un cumplimiento del 100 %, a

diferencia de la ventosa (71,2 %) y la chapa eléctrica (77,8 %), que tuvieron niveles más bajos.

Equipo	SLA objetivo (%)	Resultado anual (%)	Estado de cumplimiento	Interpretación
Ventosa	95	71,2	No cumple	Alto impacto en continuidad del servicio
PLC Energía	95	87,5	No cumple	Riesgo operativo moderado
Base de Ventosa	95	86,8	No cumple	Requiere mejora en mantenimiento
Chapa Eléctrica	95	77,8	No cumple	Incumplimiento recurrente
Lector Biométrico	95	82,6	No cumple	Afecta tiempos de acceso
Botón	95	100	Cumple	Desempeño adecuado
IDS-Controlador	95	100	Cumple	Desempeño estable

Tabla 6. Cumplimiento de SLA (%) por componente.

Fuente: Elaboración Propia.

Cumplimiento del mantenimiento preventivo programado: Según los registros existentes, se ha llevado a cabo el mantenimiento preventivo de acuerdo con el plan preestablecido, teniendo en cuenta las sugerencias del fabricante y las directrices fijadas por el departamento de ingeniería, basándose en la utilización de los equipos y en las observaciones técnicas documentadas.

3.3 Diagrama de Ishikawa

El análisis mediante el diagrama de Ishikawa permitió obtener una visión integral del problema, al reunir y relacionar de forma estructurada todas las causas que contribuyen a las fallas recurrentes de los sistemas biométricos de control de acceso. La información recopilada reflejó que el problema no se origina en un único factor, sino que es el resultado de la interacción entre fallas técnicas, deficiencias operativas, limitaciones de recursos y variabilidad en las condiciones de uso.

El estudio reveló patrones claros de recurrencia, especialmente en aspectos como, configuraciones inestables, desgaste natural de componentes, errores humanos en la operación y retrasos en la gestión de soporte. Asimismo, se detectaron factores críticos que afectan directamente el desempeño del sistema, entre ellos la ausencia de protocolos estandarizados, la limitada capacitación técnica del personal.

En conjunto, este análisis permitió comprender el problema de manera sistémica, visualizar cómo se conectan y potencian las causas entre sí y establecer una base objetiva para definir mejoras metodológicas. Esta visión integral resulta clave para orientar las decisiones correctivas, priorizar acciones y diseñar un proceso de gestión robusto que incremente la confiabilidad operativa de los dispositivos biométricos y mejore la satisfacción del cliente.

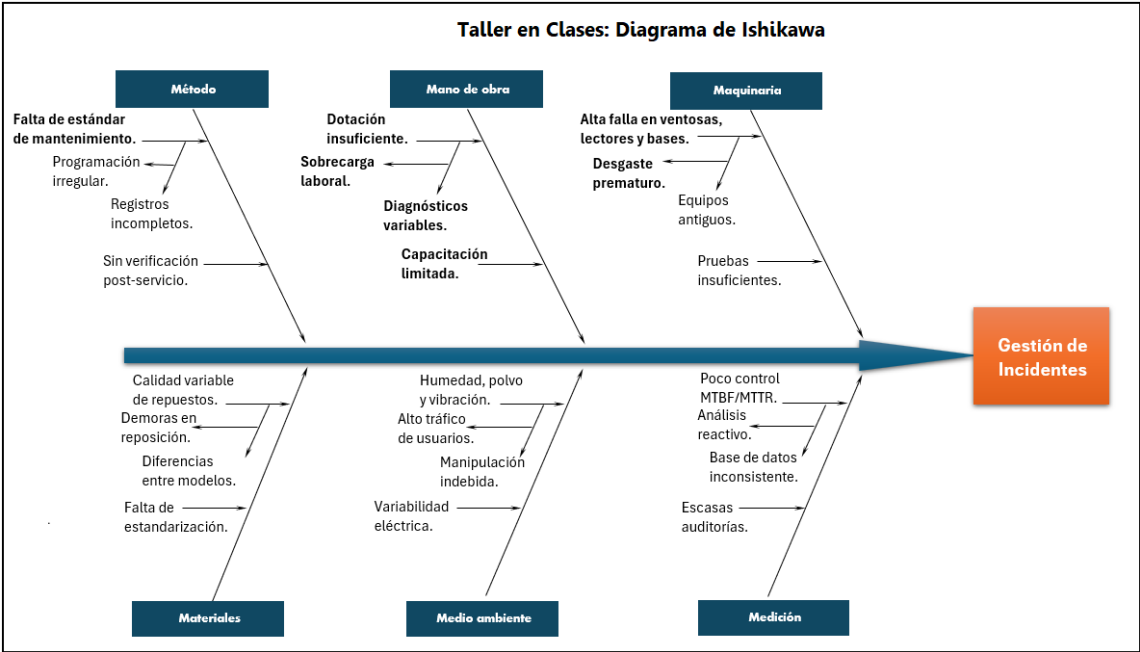


Imagen 2. Diagrama de Ishikawa.

Fuente: Elaboración Propia.

3.4 Análisis de FMEA

Identificación de los modos de falla mediante la aplicación del método FMEA.

El análisis FMEA permite identificar los modos de fallo más relevantes del sistema, destacando tres componentes con criticidad elevada debido a su impacto directo en la continuidad operativa y la seguridad. La Ventosa presentó el índice de riesgo más alto (RPN 648), ya que su fallo ocurre sin aviso previo y puede detener por completo la operación. El Lector Biométrico evidenció fallas intermitentes que afectan la validación de usuarios y generan retrasos significativos en los procesos. Por su parte, el Botón de Emergencia mostró una severidad crítica, dado que su mal funcionamiento compromete directamente la seguridad de los usuarios y dificulta una respuesta adecuada ante situaciones de riesgo.

Con base en estos resultados, se recomienda implementar un plan de mejoras prioritario enfocado en estos tres componentes. Entre las acciones más relevantes se encuentran el fortalecimiento del mantenimiento preventivo, la ejecución de pruebas funcionales sistemáticas, la actualización y calibración de equipos electrónicos, y el establecimiento de un programa de reemplazo preventivo para componentes de desgaste. Asimismo, se sugiere incorporar el enfoque FMEA de manera permanente en la gestión operativa, con el fin de anticipar fallas, reducir riesgos futuros y asegurar un funcionamiento continuo y confiable del sistema.

Este enfoque integrado permitirá a la organización aumentar la seguridad, mejorar la disponibilidad del sistema y minimizar la probabilidad de interrupciones críticas en sus operaciones.

A continuación, se muestra las siguientes tablas:



Análisis modal de fallos y efectos.

ANÁLISIS MODAL DE FALLOS Y EFECTOS								
Componente conjunto	Modo de fallo	Efectos de fallo	Causa del fallo	Fallo				Recomendación, acciones correctoras y seguimiento
				O	S	D	NPR	
Ventosa	Ventosa no succiona / desprendimiento	Puerta no se abre o no queda bloqueada → interrupción acceso, reclamos, multas	Desgaste mecánico, suciedad, instalación incorrecta, repuesto de baja calidad	9	9	8	648	Mantenimiento preventiva; revisión de fijaciones; cambio oportuno; estandarizar repuestos; seguimiento MTTR.
Lector biométrico	No lectura / no responde / rechazo de usuarios	Imposibilidad de validar identidad → retrasos operativos y reclamos	Suciedad en lector, firmware desactualizado, fallas en alimentación o interfaz	9	8	8	576	Limpieza periódica; actualización de firmware; pruebas funcionales; stock de reemplazo; monitoreo de fallas.
Base de ventosa	Base fisurada / anclaje suelto	Ventosa no sujeta correctamente → falla de cierre	Corrosión, montaje incorrecto, vibraciones, piezas incompatibles	8	7	7	392	Inspección y ajuste de anclajes; reemplazo precoz; uso de repuestos homologados.
Chapa eléctrica	Chapa atascada / no energiza	Puerta no abre → bloqueo de acceso, riesgo operativo	Solenoides quemado, fallas en cableado, falta de tensión, contactos sucios	7	5	6	210	Verificación eléctrica; limpieza de contactos; reemplazo de solenoides; prueba post-mantenión.
Chapa eléctrica	Reinicio / pérdida IO / fallo control remoto	Pérdida de apertura remota o lógica de control → impacto crítico en operaciones	Variación de tensión/sobretensiones, firmware inestable, cableado defectuoso	7	4	6	168	Protección eléctrica; actualización de firmware; respaldo de programa; monitoreo de reinicios.
Botón emergencia	Pulsador atascado o mal funciona / activaciones falsas	Apertura/alarma no intencional o no funciona en emergencia → riesgo seguridad o paradas	Ingreso de suciedad, vandalismo, desgaste mecánico	5	3	4	60	Prueba funcional regular; limpieza; reemplazo inmediato si falla; protección antivandalismo.
IDS – Controlador	Alarmas falsas / pérdida de comunicación	Alarmas innecesarias o falta de alertas → sobrecarga operativa o falta de detección	Ingreso de suciedad, vandalismo, desgaste mecánico	6	2	4	48	Revisión de configuración; calibración; monitoreo de comunicación; pruebas periódicas.

Tabla 7. Análisis modal de fallos y efectos.

Fuente: Elaboración Propia.

Tabla de O, S y D.

	Ocurrencia	Severidad	Detección
Ventosa	8-9. No da aviso / falla súbita	9-10.Paraliza la operación, genera multas, afecta continuidad	8-10. Casi imposible detectar antes de fallar
Lector biométrico	8-9. Falla sin patrón	7-8. Afecta funcionamiento normal, requiere intervención urgente	6-7. Difícil de detectar con inspecciones
Base de ventosa	7-8. Solo detectable al fallar	5-6. Provoca retrasos moderados	4-5. Detectable mediante mantenimiento regular
Chapa eléctrica	6-7. Se detecta al intentar abrir	3-4. Impacto menor	2-3. Fácil de detectar
PLC energía	6-7. Difícil sin monitoreo	1-2. No afecta operación	1. Siempre detectable

Tabla 8. Tabla de O, S y D.

Fuente: Elaboración Propia.

Tabla matriz de criticidad.

Matriz de Criticidad		
Color	RPN	Criticidad
	210+	Muy Alta
	72–209	Alta
	60–71	Media
	21–59	Baja
	<20	Muy Baja

Tabla 9. Matriz de criticidad.

Fuente: Elaboración Propia.

Como medida de mejora, se sugiere la puesta en marcha de programas de formación enfocados en el personal técnico, cuyo objetivo es aumentar las habilidades operativas, disminuir la recurrencia de fallos y optimizar la continuidad del servicio. El desarrollo de materiales técnicos, la contratación de oradores expertos, el uso de materiales auxiliares y la realización de jornadas de formación para todo el personal técnico de la compañía son tomados en cuenta en el costo aproximado de \$10,000,000. Esta cantidad es determinada tomando en cuenta el alcance del programa y los valores de referencia en el mercado para la formación técnica, y se considera una inversión preventiva ante los costos relacionados con errores que se repiten y reprocesos.

Además, se aconseja que el dispositivo OKS se instale como sistema de respaldo para garantizar la continuidad operacional en caso de que las ventosas fallen. Se ha determinado que las ventosas son uno de los elementos con más impacto en el servicio. No hay incompatibilidades entre la tecnología biométrica existente y la inclusión de este dispositivo. El costo aproximado de \$3.000.000 por dispositivo se basa en valores de referencia para comprar e instalar soluciones de respaldo con atributos parecidos. La implementación se planifica en diez sucursales de la región norte, escogidas según la cantidad de averías y el impacto en la continuidad operacional. Esto posibilita concentrar la inversión en las áreas más críticas.

A continuación, se presentan las imágenes del dispositivo OKS y su ubicación dentro de la arquitectura del sistema, lo que permite visualizar su integración y el aporte esperado en la confiabilidad del proceso de control de acceso.

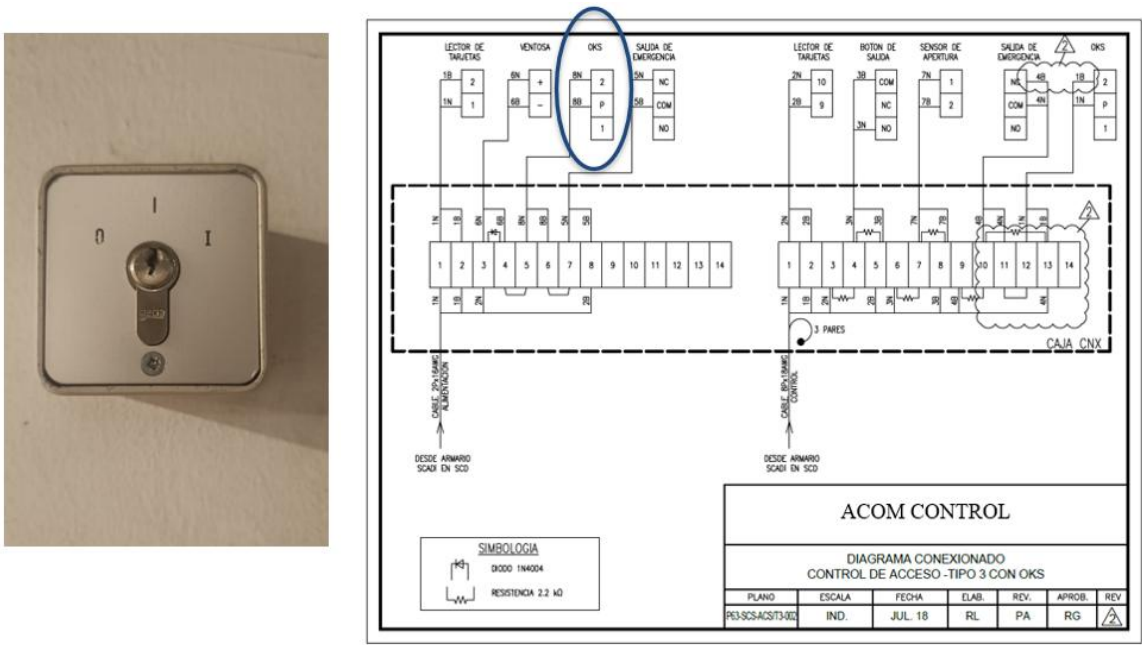


Imagen 3. Dispositivo OKS y arquitectura del sistema de control de acceso.

Fuente: Elaboración Propia.

A continuación, se presenta el siguiente plan de acción.

Acción	Por qué	Quién	Cuándo	Dónde	Cómo
Capacitación Técnica	Mejorar competencias técnicas para reducir reincidencia de fallas y cumplir SLA.	Área de RRHH junto con Jefes de Mantenimiento	Primer trimestre del plan de mejora	Sala de capacitación / plataforma online	Talleres prácticos, simulaciones de fallas, actualización en protocolos SLA y normativas de seguridad.
Instalación de Nuevos Dispositivos	Instalacion de nuevo componente OKS para mitigar las multas.	Equipo técnico especializado en biometría y electrónica	Segundo trimestre del plan de mejora	Sucursales clientes Norte y Sur	Sustitución progresiva de equipos, pruebas de funcionamiento, certificación de calidad y registro en sistema central.

Tabla 10. Plan de acción.

Fuente: Elaboración Propia.

3.5 Análisis Costo

Los costos relacionados con las fallas documentadas entre abril de 2024 y septiembre de 2025 son tenidos en cuenta por el análisis económico del sistema de control de acceso biométrico. Estos costos comprenden las horas-hombre que se emplean en trabajos de diagnóstico y reparación, la reposición de componentes y las multas impuestas por no cumplir con los acuerdos de nivel de servicio (SLA). Los datos que se usan son de los archivos financieros y operacionales internos de la compañía ACOM CONTROL, lo cual posibilita medir el efecto económico de los incidentes estudiados.

Se determinó una inversión con un enfoque preventivo, basada en los hallazgos del análisis técnico y operativo. Esta inversión se centra en las partes que más frecuentemente presentan fallas y que son más críticas. La propuesta incluye la formación del personal técnico y la implementación de sistemas de respaldo, tal como el equipo OKS, con el objetivo de reducir tanto la frecuencia de los incidentes como las consecuencias operativas que se relacionan con la interrupción del sistema de control de acceso.

Se calculan los beneficios económicos proyectados considerando la disminución pronosticada en la cantidad de fallas, la reducción de intervenciones correctivas no previstas y el cumplimiento más efectivo de los plazos establecidos en los SLA. Estos efectos se manifiestan en una reducción de las horas hombre necesarias, en la disminución de las multas por reincidencia de incidentes y en una menor necesidad de reponer componentes. La estimación se fundamenta en los supuestos establecidos para la ejecución de las medidas

planteadas y en los datos históricos analizados.

Se estimó el retorno de la inversión tomando en cuenta los costos de implementación del proyecto y las ganancias económicas esperadas a largo plazo. Los resultados señalan que, de acuerdo con las cifras proyectadas de disminución de costos operativos, la inversión inicial puede ser recuperada durante el periodo analizado. Esta evaluación hace posible determinar la relación entre los efectos económicos de la reducción de fallas del sistema y los recursos que se asignan a la mejora.

Costos implementación:

Costos	
Instalacion de OKS	\$ 30.000.000
Programa de capacitacion	\$ 10.000.000
Total	\$ 40.000.000

Tabla 11. Costos.

Fuente: Elaboración Propia.

Beneficios proyectados:

Reduccion de las Multas en 50%		Reduccion esp.	Ahorro anual
Costo anual	\$ 169.570.000	50%	\$ 84.785.000
Inversion inicial	\$ 40.000.000		
Beneficio	\$ 129.570.000		

Tabla 12. Beneficios proyectados.

Fuente: Elaboración Propia.

Retorno de la inversión (ROI):

Roi año 1	89%
Roi año 2	289%

Tabla 13. Retorno (ROI).

Fuente: Elaboración Propia.

Conclusión

Este proyecto examinó el desempeño de las fallas en los sistemas biométricos de control de acceso administrados por ACOM CONTROL durante el periodo comprendido entre abril del 2024 y septiembre del 2025, a través del uso de datos históricos. La investigación tuvo en cuenta la periodicidad de las fallas, los elementos implicados y las métricas operativas relacionadas con el mantenimiento y la ejecución de los acuerdos de nivel de servicio. Para llevar a cabo el análisis, se utilizaron técnicas específicas de gestión de la calidad e

ingeniería de mantenimiento, como el ciclo PHVA, el diagrama de Ishikawa y el análisis FMEA (de modos y efectos de falla). El uso de estas herramientas hizo posible organizar la información existente, reconocer maneras significativas de falla y establecer un orden de prioridad para los componentes basado en criterios técnicos y operativos.

Desde la perspectiva económica, el análisis permitió reconocer los costos relacionados con las averías del sistema, como la reposición de equipos, las horas hombre y las sanciones por no cumplir con los SLA. Con base en esta información, se calcularon los costos de llevar a cabo las medidas sugeridas y los beneficios financieros vinculados con la disminución de incidentes. Así fue posible determinar el retorno sobre la inversión durante el tiempo examinado.

En términos generales, el proyecto combina el análisis técnico, operativo y financiero de los sistemas de control de acceso biométrico, brindando datos organizados que pueden ser empleados para respaldar la administración del mantenimiento y las decisiones vinculadas con la continuidad del servicio. Además, la realización de la investigación hizo posible implementar instrumentos analíticos propios de los estudios en ingeniería de gestión de calidad.

Bibliografía

- Ben-Daya, M., Kumar, U., & Murthy, D. N. P. (2021). *Introduction to Maintenance Engineering: Modelling, Optimizarían and Management*. Springer.
- Ebeling, C. E. (2010). *An Introduction to Reliability and Maintainability Engineering*. Waveland Press.
- Sharma, A., & Yadava, G. S. (2018). *Reliability, Maintenance and Safety Engineering*. Springer.
- ISO/IEC 27001:2013. *Information technology — Security techniques — Information security management systems — Requirements*. International Organization for Standardization.
- ACOM CONTROL (2024–2025). *Registros internos de fallas y mantenimiento de sistemas biométricos de control de acceso*. Documentación interna.

Anexos

