



UNIREMINGTON®
CORPORACIÓN UNIVERSITARIA REMINGTON
RES. 2661 MEN JUNIO 21 DE 1996

CORPORACIÓN UNIVERSITARIA UNIREMINGTON

TRABAJO DE GRADO

Diseño y ejecución de una auditoría interna al Sistema Integrado de Gestión

Área de Tecnología y Central de Operaciones

SJ Seguridad Privada Ltda.

Docente: Cristina López Alzate

Alumno: José Arley Ramírez

Santiago de Cali

2026



TABLA DE CONTENIDO

i. Introducción.....	4
1. Descripción de la organización.....	5
2. Alcance del Sistema Integrado de Gestión.....	10
3. Contexto organizacional.....	12
3.1 Análisis DOFA.....	13
3.2 Análisis PESTEL.....	16
3.3 Cinco Fuerzas de Porter.....	17
3.4 Matriz de competitividad.....	18
3.5 Partes interesadas.....	19
3.6 Caracterización del proceso misional o productivo.....	20
4. Identificación de requisitos legales aplicables.....	26
4.1 Identificación de peligros y controles.....	26
4.2 Aspectos e impactos ambientales.....	29
5. Plan de auditoría.....	31
6. Lista de verificación (ISO 9001, ISO 14001 e ISO 45001)	37
7. Ejecución de la auditoría.....	43
7.1 Preparar la auditoría.....	41
7.2 Realizar entrevistas.....	45



7.3 Solicitar evidencias.....	46
7.4 Redactar hallazgos.....	47
7.5 Presentar conclusiones.....	45
8. Hallazgos.....	47
8.1 Aspectos relevantes o fortalezas.....	47
8.2 Oportunidades de mejora.....	53
8.3 No conformidades.....	55
9. Plan de acciones correctivas.....	57
9.1 Análisis de causas.....	58
9.2 Plan de acción.....	61
10. Conclusiones.....	63
11. Referencias.....	64
12. Anexos.....	66
13. Reunión de cierre.....	65
14. Conclusión de la ejecución de la auditoría.....	65
15. Consolidado de aspecto ambiental.....	68



Introducción

En la actualidad, las organizaciones enfrentan el reto de ofrecer servicios con altos estándares de calidad, garantizando al mismo tiempo la protección del medio ambiente y la seguridad de sus colaboradores. Por esta razón, la implementación de un Sistema Integrado de Gestión se ha convertido en una herramienta fundamental para mejorar el desempeño de los procesos, fortalecer la toma de decisiones y promover la mejora continua.

El presente trabajo de grado tiene como propósito analizar el Área de Tecnología y Central de Operaciones de **SJ Seguridad Privada Ltda.**, un proceso estratégico para la organización, ya que desde allí se administran los servicios de monitoreo de alarmas, videovigilancia, control de acceso, infraestructura tecnológica y soporte operativo que respaldan la prestación de los servicios de seguridad privada.

A lo largo del desarrollo del trabajo se realiza una caracterización del proceso, el análisis del contexto organizacional, la identificación de requisitos legales, peligros, riesgos, aspectos e impactos ambientales, así como la planificación y ejecución de una auditoría interna basada en las normas **ISO 9001:2015**, **ISO 14001:2015** e **ISO 45001:2018**. Este ejercicio permite evaluar el nivel de cumplimiento de los requisitos de cada norma, identificar fortalezas, oportunidades de mejora y no conformidades, y proponer acciones que contribuyan al fortalecimiento del Sistema Integrado de Gestión.

Finalmente, este trabajo busca evidenciar la importancia de integrar la gestión de la calidad, la gestión ambiental y la seguridad y salud en el trabajo dentro de un proceso altamente tecnológico, demostrando cómo estas herramientas contribuyen a incrementar la eficiencia operativa, la satisfacción de los clientes, el cumplimiento de la normativa vigente y la sostenibilidad de la organización.



1. Descripción de la organización

1.1 Información general

SJ Seguridad Privada Ltda. es una empresa colombiana dedicada a la prestación de servicios integrales de vigilancia y seguridad privada, orientada a proteger personas, bienes e información mediante la integración de talento humano altamente capacitado y soluciones tecnológicas de última generación. La organización desarrolla sus actividades bajo los principios de legalidad, confiabilidad, innovación, mejora continua y satisfacción del cliente, ofreciendo servicios ajustados a las necesidades de los diferentes sectores económicos.

La empresa se encuentra legalmente constituida y opera de conformidad con la normatividad vigente que regula el sector de la vigilancia y seguridad privada en Colombia, prestando servicios tanto de vigilancia física como de seguridad electrónica. Su portafolio está dirigido a clientes del sector residencial, comercial, industrial, financiero, institucional y de servicios, proporcionando soluciones que permiten reducir riesgos y fortalecer la protección de sus instalaciones.

1.2 Actividad económica

SJ Seguridad Privada Ltda. desarrolla actividades relacionadas con la prestación de servicios de vigilancia y seguridad privada, entre las cuales se destacan:

- Vigilancia física fija y móvil.
- Monitoreo electrónico de alarmas las 24 horas del día.
- Monitoreo de sistemas de circuito cerrado de televisión (CCTV).
- Control de acceso mediante sistemas biométricos, tarjetas de proximidad y reconocimiento facial.
- Vigilancia remota asistida.
- Custodia y administración de llaves.
- Instalación, configuración y mantenimiento de sistemas electrónicos de seguridad.
- Administración de plataformas tecnológicas para la gestión de eventos de seguridad.
- Soporte técnico especializado para infraestructura tecnológica de seguridad.

1.3 Estructura organizacional

La organización cuenta con una estructura administrativa y operativa que permite garantizar la prestación continua de los servicios ofrecidos. La dirección establece los lineamientos estratégicos y coordina las diferentes áreas responsables de la operación, entre ellas operaciones, comercial, gestión humana, financiera, calidad y tecnología.

El presente trabajo se desarrolla específicamente sobre el Área de Tecnología y Central de Operaciones, debido a que constituye el eje tecnológico que soporta la prestación de los servicios de monitoreo electrónico y garantiza la continuidad operacional de la organización.

Organigrama



Imagen tomada desde Gemini.

1.4 Área de Tecnología y Central de Operaciones

El Área de Tecnología y Central de Operaciones tiene la responsabilidad de administrar, mantener y asegurar el funcionamiento de toda la infraestructura tecnológica utilizada para la prestación de los servicios de seguridad electrónica. Su operación es permanente, funcionando las veinticuatro (24) horas del día durante los siete (7) días de la semana, con el propósito de garantizar la atención inmediata de los eventos reportados por los sistemas instalados en los clientes.



Entre sus principales responsabilidades se encuentran:

- Administración de la Central de Monitoreo.
- Gestión de la infraestructura de servidores.
- Administración de redes y telecomunicaciones.
- Administración de plataformas de monitoreo.
- Gestión de sistemas de control de acceso.
- Administración del sistema de video vigilancia.
- Soporte técnico interno.
- Gestión de continuidad del negocio.
- Administración de bases de datos y respaldos.
- Gestión de usuarios y permisos.
- Implementación de proyectos tecnológicos.
- Seguimiento de indicadores operacionales.

1.5 Infraestructura tecnológica

La Central de Operaciones dispone de una infraestructura tecnológica diseñada para garantizar alta disponibilidad y continuidad del servicio. Entre los principales recursos tecnológicos se encuentran:

- Servidores dedicados para las plataformas de monitoreo y administración.
- Sistema de recepción de señales de alarmas **Kronos**.
- Plataforma **Dynamic Codes** para la administración de cerraduras electrónicas y control de acceso.
- Plataforma **DSS (Dahua Security Software)** para la administración y supervisión del sistema de video vigilancia.
- Plataforma **TalkPlus** para comunicaciones Push To Talk (PTT).
- Plataforma **ORS Orbitand** para aplicaciones móviles y gestión operativa.
- Sistemas de almacenamiento para video y respaldo de información.



- Equipos de red administrables.
- Sistemas UPS para respaldo eléctrico.
- Planta eléctrica de emergencia.
- Videowall conformado por monitores industriales para la supervisión permanente de eventos.
- Estaciones de trabajo destinadas a los operadores de monitoreo.

Esta infraestructura permite garantizar la disponibilidad de los servicios críticos y disminuir el impacto ante posibles fallas técnicas o interrupciones del suministro eléctrico.

1.6 Proceso de monitoreo

La Central de Operaciones recibe de manera permanente señales provenientes de sistemas de alarma, cámaras de seguridad, controles de acceso y demás dispositivos electrónicos instalados en las instalaciones de los clientes.

Una vez recibido un evento, el operador realiza el análisis correspondiente siguiendo los protocolos establecidos por la organización, verifica la información disponible y ejecuta las acciones definidas para cada tipo de incidente, tales como contacto con el cliente, activación de protocolos internos o notificación a las autoridades competentes cuando sea necesario.

Todo el proceso queda registrado en las plataformas de monitoreo, permitiendo la trazabilidad de cada evento y facilitando la generación de informes e indicadores de gestión.

1.7 Clientes

SJ Seguridad Privada Ltda. presta sus servicios a organizaciones pertenecientes a diversos sectores económicos, entre ellos:

- Sector residencial.
- Sector comercial.
- Sector industrial.
- Sector salud.
- Sector financiero.
- Instituciones educativas.



- Entidades públicas y privadas.
- Empresas de servicios.

La organización adapta sus soluciones tecnológicas a las necesidades particulares de cada cliente, buscando incrementar los niveles de seguridad y confiabilidad.

1.8 Compromiso con la calidad, el ambiente y la seguridad y salud en el trabajo

La empresa orienta sus actividades hacia la mejora continua de sus procesos mediante la implementación de un Sistema Integrado de Gestión basado en los requisitos de las normas ISO 9001:2015, ISO 14001:2015 e ISO 45001:2018.

En el Área de Tecnología y Central de Operaciones este compromiso se refleja en la estandarización de procedimientos, la gestión de riesgos operacionales, la protección de la información, la prevención de incidentes de seguridad y salud en el trabajo, el manejo adecuado de residuos de aparatos eléctricos y electrónicos (RAEE), la optimización del consumo energético y el cumplimiento de la legislación aplicable.

La integración de estos sistemas permite garantizar la satisfacción del cliente, la continuidad del servicio, la protección de los trabajadores y la minimización de los impactos ambientales derivados de la operación tecnológica de la empresa.



2. Alcance del Sistema Integrado de Gestión

2.1 Alcance

El Sistema Integrado de Gestión (SIG) de SJ Seguridad Privada Ltda. comprende los procesos estratégicos, misionales y de apoyo relacionados con la prestación de servicios de vigilancia y seguridad privada, integrando los requisitos establecidos en las normas ISO 9001:2015 (Sistema de Gestión de la Calidad), ISO 14001:2015 (Sistema de Gestión Ambiental) e ISO 45001:2018 (Sistema de Gestión de Seguridad y Salud en el Trabajo).

Para el presente trabajo de grado, el alcance se encuentra delimitado al Área de Tecnología y Central de Operaciones, debido a que constituye el proceso responsable de garantizar la continuidad operativa de los servicios tecnológicos que soportan la prestación del servicio de seguridad electrónica ofrecido por la organización.

El alcance incluye todas las actividades desarrolladas desde la Central de Operaciones relacionadas con la administración, monitoreo y mantenimiento de la infraestructura tecnológica utilizada para la prestación de los servicios de seguridad, así como la gestión de los riesgos asociados a la calidad del servicio, los aspectos ambientales y los peligros para la seguridad y salud en el trabajo.

Dentro del alcance se incluyen las siguientes actividades:

- Administración y operación de la Central de Monitoreo las veinticuatro (24) horas del día.
- Recepción, análisis y atención de señales provenientes de sistemas de alarmas.
- Supervisión de sistemas de circuito cerrado de televisión (CCTV).
- Administración de plataformas de monitoreo y gestión de eventos.
- Administración de sistemas de control de acceso y cerraduras electrónicas.
- Gestión de servidores, redes, telecomunicaciones y bases de datos.
- Gestión de respaldos y continuidad de la operación tecnológica.
- Mantenimiento preventivo y correctivo de los equipos tecnológicos.
- Soporte técnico a usuarios internos y clientes.



- Gestión de incidentes tecnológicos y eventos críticos.
- Administración de usuarios, perfiles y permisos de acceso a las plataformas.
- Implementación de proyectos de innovación tecnológica.
- Seguimiento a indicadores de desempeño del proceso.
- Gestión documental asociada al proceso.
- Cumplimiento de requisitos legales aplicables al Sistema Integrado de Gestión.

2.2 Límites del alcance

El presente trabajo se limita al análisis de los procesos ejecutados por el Área de Tecnología y Central de Operaciones y no contempla la evaluación detallada de otros procesos organizacionales como Gestión Humana, Gestión Financiera, Comercial, Compras o Vigilancia Física, salvo cuando exista interacción directa con el proceso tecnológico.

Asimismo, el estudio comprende únicamente las actividades desarrolladas dentro de la infraestructura tecnológica administrada por SJ Seguridad Privada Ltda., incluyendo servidores, plataformas de monitoreo, redes de comunicaciones, sistemas de video vigilancia, control de acceso, almacenamiento de información y equipos utilizados para la operación continua del servicio.

2.3 Exclusiones

Considerando la naturaleza de las actividades evaluadas, el alcance del presente trabajo excluye:

- Procesos administrativos que no intervienen directamente en la operación tecnológica.
- Auditorías financieras y contables.
- Evaluaciones de desempeño del personal ajenas al Sistema Integrado de Gestión.
- Procesos constructivos o de infraestructura civil.
- Actividades desarrolladas por contratistas externos que no tengan relación con la operación tecnológica de la organización.

3. Contexto organizacional

De acuerdo con las normas ISO 9001:2015, ISO 14001:2015 e ISO 45001:2018, la organización debe determinar las cuestiones internas y externas que pueden afectar su capacidad para alcanzar los resultados previstos del Sistema Integrado de Gestión (SIG).

En SJ Seguridad Privada Ltda., el Área de Tecnología y Central de Operaciones constituye uno de los procesos misionales de mayor importancia, ya que soporta la prestación continua de los servicios de monitoreo de alarmas, videovigilancia, control de acceso y administración de plataformas tecnológicas. Debido a la naturaleza crítica de sus operaciones, este proceso requiere garantizar altos niveles de disponibilidad, confiabilidad, seguridad de la información, cumplimiento legal y mejora continua.

El contexto organizacional permite identificar los factores internos y externos que pueden influir positiva o negativamente en el desempeño del proceso, facilitando la toma de decisiones estratégicas y la implementación de acciones preventivas y correctivas.



Imagen tomada desde Gemini.



3.1 Análisis DOFA. Tabla 1

Matriz DOFA del Área de Tecnología y Central de Operaciones

Fortalezas	Debilidades
Central de monitoreo operando 24 horas al día, los 365 días del año.	Dependencia de algunos proveedores tecnológicos para soporte especializado.
Personal con experiencia en monitoreo y administración de plataformas de seguridad electrónica.	Algunos procedimientos requieren mayor automatización.
Infraestructura tecnológica con servidores, UPS y planta eléctrica para garantizar continuidad del servicio.	Actualización permanente de licencias y equipos genera altos costos operativos.
Plataformas tecnológicas especializadas para monitoreo, CCTV y control de acceso.	La documentación técnica requiere actualización periódica.
Alta disponibilidad de los servicios tecnológicos.	Dependencia del suministro de energía y conectividad a Internet.
Oportunidades	Amenazas
Implementación de Inteligencia Artificial para análisis de eventos.	Incremento de ataques informáticos y ciber amenazas.
Automatización de procesos mediante nuevas plataformas.	Cambios frecuentes en la normatividad del sector.
Crecimiento del mercado de seguridad electrónica.	Competencia con empresas nacionales e internacionales.
Integración de soluciones en la nube.	Obsolescencia tecnológica acelerada.
Expansión del portafolio de servicios tecnológicos.	Incremento de costos de equipos tecnológicos importados.



Tipo de Estrategia	Estrategia	Objetivo
FO (Fortalezas - Oportunidades)	Implementar soluciones de Inteligencia Artificial aprovechando la infraestructura tecnológica y la operación 24/7 para optimizar el análisis de eventos y reducir falsas alarmas.	Innovar y mejorar la eficiencia del monitoreo.
FO	Integrar las plataformas de monitoreo, CCTV y control de acceso con soluciones en la nube para ampliar el portafolio de servicios tecnológicos.	Incrementar la competitividad y diversificar los servicios.
FO	Aprovechar la experiencia del personal para liderar proyectos de automatización de procesos mediante nuevas tecnologías.	Mejorar la productividad y reducir tiempos operativos.
FO	Fortalecer la oferta de servicios tecnológicos mediante soluciones inteligentes de monitoreo y analítica de video.	Aprovechar el crecimiento del mercado de seguridad electrónica.
DO (Debilidades - Oportunidades)	Automatizar los procesos operativos que actualmente son manuales mediante nuevas plataformas tecnológicas.	Reducir errores y aumentar la eficiencia.
DO	Implementar un sistema de gestión documental para mantener actualizada la documentación técnica.	Mejorar el control documental y facilitar las auditorías.
DO	Elaborar un plan de renovación tecnológica que optimice la inversión en equipos y licencias.	Disminuir los costos operativos a largo plazo.
DO	Migrar gradualmente algunos servicios hacia plataformas en la nube para reducir costos de infraestructura.	Modernizar la operación tecnológica.
FA (Fortalezas - Amenazas)	Reforzar la ciberseguridad mediante controles de acceso, monitoreo continuo y respaldos de información.	Minimizar los riesgos por ciberataques.



Tipo de Estrategia	Estrategia	Objetivo
FA	Aprovechar la infraestructura redundante (servidores, UPS y planta eléctrica) para garantizar la continuidad del servicio.	Reducir el impacto de interrupciones operativas.
FA	Capacitar permanentemente al personal sobre nuevas amenazas tecnológicas y cambios normativos.	Mantener el cumplimiento legal y fortalecer la seguridad.
FA	Diferenciar la empresa mediante altos niveles de disponibilidad y calidad en los servicios tecnológicos.	Incrementar la competitividad frente al mercado.
DA (Debilidades - Amenazas)	Diversificar los proveedores tecnológicos para reducir la dependencia de un solo fabricante o proveedor.	Disminuir los riesgos de continuidad del servicio.
DA	Implementar un plan de gestión del ciclo de vida de los equipos tecnológicos.	Reducir el impacto de la obsolescencia tecnológica.
DA	Desarrollar planes de contingencia para garantizar la continuidad del servicio ante fallas de energía, Internet o ciberataques.	Minimizar el impacto de incidentes críticos.
DA	Actualizar periódicamente los procedimientos y la documentación técnica conforme a los cambios normativos y tecnológicos.	Garantizar el cumplimiento y la mejora continua.

Análisis DOFA

La organización presenta fortalezas relacionadas con su infraestructura tecnológica, experiencia del personal y continuidad operacional. Sin embargo, enfrenta desafíos asociados a la actualización tecnológica, dependencia de proveedores y amenazas derivadas del crecimiento de los riesgos cibernéticos. El análisis evidencia la necesidad de fortalecer la innovación tecnológica y la gestión documental para mantener la competitividad.

3.2 Análisis PESTEL Tabla 2.

Factor	Impacto sobre la organización
Político	Regulación del sector por la Superintendencia de Vigilancia y Seguridad Privada.
Económico	Variación del dólar, inflación y costos de importación de equipos tecnológicos.
Social	Mayor percepción de inseguridad incrementa la demanda de servicios tecnológicos.
Tecnológico	Avances en inteligencia artificial, analítica de video, ciberseguridad y computación en la nube.
Ambiental	Gestión adecuada de residuos electrónicos, baterías y consumo energético de los centros de datos.
Legal	Cumplimiento de normas ISO, legislación laboral, ambiental, de SST y protección de datos personales.

Análisis PESTEL

Los factores tecnológicos y legales representan los elementos de mayor influencia para el Área de Tecnología y Central de Operaciones. La constante evolución de las tecnologías de seguridad obliga a la organización a mantener procesos de actualización permanente, mientras que el cumplimiento normativo constituye un requisito indispensable para garantizar la continuidad del negocio.



3.3 Análisis de las Cinco Fuerzas de Porter Tabla 3.

Cinco Fuerzas de Porter

Fuerza	Nivel	Justificación
Rivalidad entre competidores	Alto	Existen numerosas empresas de vigilancia y seguridad electrónica con servicios similares.
Poder de negociación de los clientes	Alto	Los clientes comparan precio, calidad, tecnología y tiempos de respuesta.
Poder de negociación de proveedores	Medio	Algunos proveedores suministran tecnologías especializadas difíciles de reemplazar.
Amenaza de nuevos competidores	Media	El crecimiento del mercado favorece el ingreso de nuevas empresas tecnológicas.
Amenaza de productos sustitutos	Baja	Los servicios de monitoreo profesional continúan siendo esenciales para clientes corporativos.

Análisis

La principal presión competitiva proviene de la rivalidad entre empresas del sector y de la creciente exigencia de los clientes. Esto obliga a SJ Seguridad Privada Ltda. a mantener altos estándares de calidad, innovación tecnológica y servicio al cliente.



3.4 Matriz de Competitividad Tabla 4.

Comparación competitiva

Criterio	SJ Seguridad	Competidor A	Competidor B
Calidad del servicio	Alta	Alta	Media
Tecnología	Alta	Alta	Media
Atención al cliente	Alta	Media	Media
Innovación	Alta	Alta	Media
Tiempo de respuesta	Alto	Medio	Medio
Personal especializado	Alto	Alto	Medio

Análisis

SJ Seguridad Privada Ltda. presenta ventajas competitivas relacionadas con la atención personalizada, la integración de plataformas tecnológicas y la capacidad de respuesta desde su Central de Operaciones. No obstante, debe continuar fortaleciendo sus procesos de innovación para mantener una posición competitiva en el mercado.



3.5 Partes interesadas Tabla 5.

Identificación de partes interesadas

Parte interesada	Necesidades	Expectativas
Clientes	Servicio confiable y continuo.	Atención oportuna y disponibilidad 24/7.
Colaboradores	Condiciones laborales seguras.	Capacitación y bienestar.
Alta Dirección	Cumplimiento de objetivos estratégicos.	Rentabilidad y mejora continua.
Proveedores	Relaciones comerciales estables.	Pagos oportunos y comunicación efectiva.
Autoridades	Cumplimiento legal.	Evidencias y registros actualizados.
Comunidad	Protección ambiental y responsabilidad social.	Operación responsable.

Análisis

La satisfacción de las partes interesadas depende del cumplimiento de los requisitos legales, la calidad del servicio, la seguridad de la información y la mejora continua del Sistema Integrado de Gestión.



3.6 Caracterización del proceso misional

Nombre del proceso:

Tecnología y Central de Operaciones.

Objetivo

Garantizar la operación continua de la infraestructura tecnológica y la atención oportuna de los eventos de seguridad electrónica, asegurando la satisfacción del cliente y el cumplimiento de los requisitos legales, ambientales y de seguridad y salud en el trabajo.

Entradas

- Contratos de prestación del servicio.
- Requerimientos de los clientes.
- Plataformas tecnológicas.
- Equipos electrónicos.
- Redes de comunicaciones.
- Energía eléctrica.
- Personal operativo.

Actividades principales

- Recepción de señales de alarmas.
- Monitoreo de CCTV.
- Administración de plataformas tecnológicas.
- Gestión de servidores y bases de datos.
- Atención de eventos críticos.
- Soporte técnico.
- Gestión de respaldos.
- Administración de usuarios.
- Mantenimiento preventivo y correctivo.
- Elaboración de informes operacionales.



Salidas

- Eventos gestionados.
- Alarmas atendidas.
- Reportes operacionales.
- Servicios tecnológicos disponibles.
- Clientes atendidos.
- Información respaldada.

Indicadores

- Disponibilidad de la plataforma (%).
- Tiempo promedio de atención de eventos.
- Incidentes tecnológicos resueltos.
- Cumplimiento del mantenimiento preventivo.
- Nivel de satisfacción del cliente.
- Cumplimiento de acuerdos de nivel de servicio (SLA).

Recursos

- Servidores.
- Sistemas UPS.
- Planta eléctrica.
- Plataformas de monitoreo.
- Redes y telecomunicaciones.
- Software especializado.
- Personal técnico y operadores.
- Procedimientos documentados.



Riesgos

- Fallas de energía.
- Ciberataques.
- Caída de servidores.
- Interrupción de Internet.
- Errores operacionales.
- Obsolescencia tecnológica.

Oportunidades

- Automatización de procesos.
- Implementación de inteligencia artificial.
- Analítica avanzada de video.
- Migración de servicios a la nube.
- Integración de nuevas tecnologías de monitoreo.



		CARACTERIZACIÓN PROCESO TECNOLOGIA		
TIPO DE PROCESO	Operativo o Misional			
RESPONSABLE	Coordinador de Tecnología y Central de Operaciones			
OBJETIVO	Garantizar la continuidad, disponibilidad, administración y mejora de los recursos tecnológicos de la organización mediante la destión de la centra de operaciones, las plataformas de monitoreo y gestión, el soporte técnico preventivo y correctivo. Contort de inventarios de los servicios tecnológicos recurrentes y administración de contratos con su facturación, asegurando la eficiencia operativa, la disponibilidad y el cumplimiento de los requisitos del negocio.			
ALCANCE	El proceso de tecnología inicia con la identificación de las necesidades tecnológicas de la organización y la planificación de la Central de operaciones, las plataformas de monitoreo y gestión, el soporte técnico preventivo y correctivo, la administración de inventarios tecnológicos, e control de servicios recurrentes y la gestión de contratos y facturación, asegurando la continuidad del negoico y la satisfacción del cliente.			
PROVEEDOR	ENTRADAS	ACTIVIDADES	SALIDAS	CLIENTES
PLANEAR				
Gerencia General	Plan Estratégico	Identificar necesidades tecnológicas	Plan de trabajo	Gerencia
Todas la áreas	Requirimientos tecnológicos	Definir presupuesto y recursos	Plan de inversiones	Áreas internas
Proveedores	Cotizaciones	Evaluar proveedores tecnológicos	Proveedores seleccionados	Compras
HACER				
Proveedores TIC y tecnología	Equipos y licencias	Administrar infraestructura tecnológica	Infraestructura operativa	Organización
Área de tecnología	Solucitudes de soporte	Atender soporte preventivo y correctivo	Incidente solucionado	Usuarios internos
Central Operaciones	Alarmas y eventos	Monitorear plataformas y servicios	Eventos atendidos	Clientes
Técnicos	Órdenes de Servicio	Controlar técnicos en campo mediante plataforma	Servicios ejecutados	Operación
Compras	Equipos adquiridos	Administrar inventario tecnológico	Inventario actualizado	Compras y tecnología
Operadores	Facturas de servicios	Controlar servicios recurrentes y facturación	Pagos controlados	Facturación y Tecnología
VERIFICAR				
Indicadores	Reportes	Medir cumplimiento de indicadores	Informe de gestión	Gerencia
Auditorias	Hallazgos	Revisar cumplimiento de procedimientos	Planes de Acción	Direcciones
Plataformas	Reportes disponibilidad	Analizar disponibilidad de servicios	Estadísticas	Clientes
ACTUAR				
Auditorias	Hallazgos	Implementar acciones correctivas	Mejoras implementadas	Organización
Indicadores	Resultados	Actualizar procedimientos	Procedimientos actualizados	Personal
Usuarios	Encuestas	Implementar oportunidades de mejora	Mayor Satisfacción	Clientes



RECURSOS HUMANOS	RECURSOS FISICOS
Coordinador de tecnología y central de operaciones	Servidores físicos y virtuales
Analista de TI	NVR, XVR o DSS
Asistente Técnico	Estaciones de monitoreo
Operadores de medios tecnológicos	Equipos de computo
Proveedor de Servicios	Swiches administrables, Routers
Contratistas externos	Firewalls, enlaces de internet con políticas
N/A	UPS, planta eléctrica
N/A	Plataformas de gestión para monitoreo
N/A	Contorl de inventarios, matrices de control
N/A	Herramientas y dotación para mantenimiento
DOCUMENTACIÓN ASOCIADA	REQUISITOS LEGALES
Manual del Sistema Integrado de Gestión (SIG).	Constitución Política de Colombia (artículos relacionados con el trabajo y el ambiente).
Caracterización del proceso de Tecnología y Central de Operaciones.	Ley 9 de 1979 – Código Sanitario Nacional.
Procedimiento de Monitoreo de Alarmas.	Ley 99 de 1993 – Sistema Nacional Ambiental.
Procedimiento de Atención de Incidentes Tecnológicos.	Ley 1562 de 2012 – Sistema General de Riesgos Laborales.
Procedimiento de Administración de Plataformas Tecnológicas.	Decreto 1072 de 2015 – Decreto Único Reglamentario del Sector Trabajo.
Procedimiento de Gestión de Cambios Tecnológicos	Resolución 0312 de 2019 – Estándares Mínimos del SG-SST.
Procedimiento de Mantenimiento Preventivo y Correctivo.	Ley 1581 de 2012 – Protección de Datos Personales.
Procedimiento de Gestión de Copias de Seguridad (Backups).	Decreto 1377 de 2013 – Reglamentación de la Ley 1581 de 2012.
Procedimiento de Seguridad de la Información y Control de Accesos.	Ley 1273 de 2009 – Delitos Informáticos.
Procedimiento de Gestión de Activos Tecnológicos.	Ley 594 de 2000 – Ley General de Archivos.
Procedimiento de Gestión de Incidentes de Ciberseguridad.	Resolución 1362 de 2007 – Registro de Generadores de Residuos Peligrosos (cuando aplique).
Plan de Continuidad del Negocio y Recuperación ante Desastres (BCP/DRP).	Resolución 851 de 2022 y demás normas aplicables para la gestión de Residuos de Aparatos Eléctricos y Electrónicos (RAEE).
Matriz de Identificación de Peligros, Evaluación y Valoración de Riesgos (IPER).	ISO 9001:2015 – Sistema de Gestión de la Calidad.
Matriz de Aspectos e Impactos Ambientales.	ISO 14001:2015 – Sistema de Gestión Ambiental.
Matriz de Requisitos Legales.	ISO 45001:2018 – Sistema de Gestión de Seguridad y Salud en el Trabajo.
Plan Anual de Mantenimiento Tecnológico.	Normatividad vigente emitida por la Superintendencia de Vigilancia y Seguridad Privada aplicable a la prestación del servicio.
Inventario de Equipos Tecnológicos.	N/A
Cronograma de Capacitaciones.	N/A
Registros de Mantenimiento.	N/A
Registros de Incidentes y Mesa de Servicio.	N/A
Registros de Monitoreo y Eventos.	N/A
Indicadores de Gestión del Proceso.	N/A
Plan de Auditorías Internas.	N/A
Plan de Acciones Correctivas, Preventivas y de Mejora.	N/A



INDICADORES				
NOMBRE DEL INDICADOR	COMO SE MIDE	QUIEN LO MIDE	FRECUENCIA	META
Cumplimiento de ANS	$(\text{Número de servicios atendidos dentro del ANS} \div \text{Total de servicios atendidos}) \times 100$	Coordinador de Tecnología y Central de Operaciones	Mensual	$\geq 98 \%$
Tiempo de atención de incidentes	Promedio del tiempo transcurrido entre la recepción del incidente y el inicio de su atención	Coordinador de Tecnología	Mensual	≤ 5 minutos para eventos críticos
Cumplimiento de mantenimiento	$(\text{Mantenimientos ejecutados} + \text{Mantenimientos programados}) \times 100$	Ingeniero o Analista de Tecnología	Mensual	100%
Disponibilidad de plataformas tecnológicas	$(\text{Horas de disponibilidad} \div \text{Horas programadas de operación}) \times 100$	Coordinador de Tecnología	Mensual	$\geq 99,8 \%$
Disponibilidad de servidores	$(\text{Tiempo de disponibilidad de servidores} \div \text{Tiempo total del período}) \times 100$	Administrador de Infraestructura (Ingeniero de TI)	Mensual	$\geq 99,9 \%$
Incidentes tecnológicos resueltos	$(\text{Incidentes solucionados} \div \text{Total de incidentes reportados}) \times 100$	Mesa de Servicio / Tecnología	Mensual	$\geq 95 \%$
Cumplimiento de respaldos (Backups)	$(\text{Copias de seguridad exitosas} + \text{Copias programadas}) \times 100$	Administrador de Servidores	Diario / Mensual	100%
Disponibilidad de comunicaciones	$(\text{Tiempo de disponibilidad de Internet y enlaces} \div \text{Tiempo total}) \times 100$	Coordinador de Tecnología	Mensual	$\geq 99,5 \%$
Cumplimiento de capacitaciones del personal	$(\text{Capacitaciones ejecutadas} + \text{Capacitaciones programadas}) \times 100$	Gestión Humana y Coordinador de Tecnología	Trimestral	100%
Satisfacción del cliente interno	Resultado promedio de encuestas de satisfacción	Coordinador de Tecnología	Semestral	$\geq 95 \%$
RIESGOS Y OPORTUNIDADES ASOCIADOS AL PROCESO				
RIESGOS		OPORTUNIDADES		
Interrupción del servicio por fallas eléctricas.		Implementar mayor redundancia eléctrica y monitoreo inteligente de energía.		
Caída de servidores o plataformas críticas.		Virtualización y alta disponibilidad de servidores.		
Ciberataques, malware o ransomware.		Fortalecer la ciberseguridad mediante EDR, firewalls y autenticación multifactor.		
Fallas en la conectividad de Internet.		Contratar enlaces redundantes con diferentes proveedores.		
Obsolescencia de equipos tecnológicos.		Plan anual de renovación tecnológica.		
Errores operativos durante la atención de eventos.		Automatizar procesos y fortalecer la capacitación continua.		
Pérdida de información por fallas en respaldos.		Implementar copias de seguridad automáticas y replicación en la nube.		
Incumplimiento de requisitos legales o normativos.		Mantener una matriz legal actualizada y realizar auditorías periódicas.		
Alta rotación de personal especializado.		Desarrollar planes de formación, retención y transferencia del conocimiento.		
Incremento de la demanda de servicios tecnológicos.		Ampliar el portafolio de soluciones de monitoreo, analítica de video e inteligencia artificial.		



4. Identificación de requisitos legales aplicables

4.1 Identificación de requisitos legales

Uno de los pilares fundamentales de un Sistema Integrado de Gestión (SIG) es garantizar el cumplimiento de los requisitos legales y reglamentarios aplicables a la organización. Las normas ISO 9001:2015, ISO 14001:2015 e ISO 45001:2018 establecen que las organizaciones deben identificar, mantener actualizados y evaluar periódicamente los requisitos legales relacionados con sus actividades, productos y servicios.

En el caso de SJ Seguridad Privada Ltda., específicamente en el Área de Tecnología y Central de Operaciones, la identificación de requisitos legales tiene como propósito asegurar que todas las actividades relacionadas con la prestación del servicio de monitoreo electrónico, administración de infraestructura tecnológica, gestión de información, mantenimiento de equipos y operación de plataformas de seguridad se desarrollen conforme a la legislación colombiana vigente.

El cumplimiento de estos requisitos permite minimizar riesgos legales, operacionales, ambientales y de seguridad y salud en el trabajo, garantizando además la continuidad del servicio y la satisfacción de los clientes.

4.1.2 Matriz de identificación de peligros y controles Tabla 6.

Actividad	Peligro	Riesgo	Controles existentes
Monitoreo permanente de alarmas y CCTV	Posturas prolongadas y movimientos repetitivos	Trastornos musculoesqueléticos	Puestos ergonómicos, pausas activas, sillas ergonómicas y capacitación en higiene postural.
Operación continua frente a monitores	Fatiga visual	Disminución de la capacidad visual, cefaleas y fatiga	Iluminación adecuada, filtros de pantalla, pausas visuales cada dos horas y valoración ocupacional.
Administración de servidores y equipos eléctricos	Contacto con energía eléctrica	Descarga eléctrica o quemaduras	Mantenimiento preventivo, procedimientos seguros de trabajo, uso de elementos de protección personal (EPP) y personal autorizado.
Instalación y mantenimiento de cámaras y equipos electrónicos	Trabajo en alturas (cuando aplique)	Caídas a diferente nivel	Uso de arnés certificado, inspección de equipos, capacitación y permiso de trabajo en alturas.
Cableado estructurado y redes	Herramientas manuales y elementos cortopunzantes	Cortes y lesiones en manos	Uso de guantes de protección y herramientas certificadas.
Manipulación de UPS y baterías	Manipulación de cargas	Lesiones lumbares y musculares	Ayudas mecánicas, trabajo en equipo y capacitación en levantamiento seguro de cargas.

Operación 24/7 de la Central	Riesgo psicosocial	Estrés laboral, fatiga mental y disminución del rendimiento	Rotación de turnos, pausas activas, seguimiento psicosocial y programas de bienestar.
Centros de datos y cuartos técnicos	Incendio por sobrecarga eléctrica	Lesiones personales y pérdida de infraestructura	Detectores de humo, extintores, sistemas de respaldo eléctrico y mantenimiento preventivo.
Desplazamientos para soporte técnico	Riesgo de tránsito	Accidentes de tránsito	Capacitación en conducción segura, mantenimiento de vehículos y cumplimiento de normas de tránsito.
Uso de equipos informáticos	Exposición a campos electromagnéticos de baja intensidad	Fatiga y molestias ocupacionales	Distancias adecuadas, mantenimiento de equipos y cumplimiento de especificaciones técnicas.

Conclusión

La identificación de los requisitos legales constituye una herramienta fundamental para garantizar que las actividades desarrolladas por el Área de Tecnología y Central de Operaciones de SJ Seguridad Privada Ltda. se ejecuten conforme a la legislación colombiana y a los requisitos de las normas ISO 9001:2015, ISO 14001:2015 e ISO 45001:2018. El cumplimiento de estas disposiciones fortalece la gestión del riesgo, protege la información, promueve condiciones de trabajo seguras, minimiza los impactos ambientales y contribuye a la mejora continua del Sistema Integrado de Gestión.

4.2 Aspectos e impactos ambientales

4.2.1 Identificación de aspectos e impactos ambientales

La identificación de aspectos e impactos ambientales constituye uno de los requisitos fundamentales de la **Norma ISO 14001:2015**, cuyo propósito es establecer controles que permitan prevenir la contaminación, proteger el medio ambiente y promover el uso eficiente de los recursos naturales.

En **SJ Seguridad Privada Ltda.**, específicamente en el Área de Tecnología y Central de Operaciones, las actividades desarrolladas generan diferentes aspectos ambientales asociados al consumo de recursos, la generación de residuos y el funcionamiento continuo de la infraestructura tecnológica. Aunque la organización presta servicios de seguridad y no realiza procesos industriales, su operación implica el uso permanente de equipos electrónicos, servidores, sistemas de respaldo energético, redes de comunicaciones y centros de datos, los cuales pueden generar impactos ambientales si no son gestionados adecuadamente.

La identificación de aspectos ambientales permite establecer controles para minimizar los efectos negativos sobre el medio ambiente y fortalecer el desempeño ambiental de la organización.

4.2.2 Matriz de aspectos e impactos ambientales Tabla 7

Actividad	Aspecto ambiental	Impacto ambiental	Controles implementados
Operación continua de servidores y equipos tecnológicos	Consumo de energía eléctrica	Incremento del consumo energético y emisiones indirectas de CO ₂	Uso de equipos de alta eficiencia, monitoreo del consumo y mantenimiento preventivo.
Funcionamiento de UPS y planta eléctrica	Consumo de combustible y energía	Emisiones atmosféricas y consumo de recursos naturales	Mantenimiento periódico, pruebas programadas y control del consumo de combustible.
Sustitución de equipos tecnológicos	Generación de residuos electrónicos (RAEE)	Contaminación del suelo y del agua por disposición inadecuada	Entrega a gestores autorizados y aplicación del programa de gestión de RAEE.
Cambio de baterías	Generación de	Contaminación por	Almacenamiento temporal



de UPS	residuos peligrosos	metales pesados y sustancias químicas	seguro y disposición mediante gestores autorizados.
Uso de impresoras	Consumo de papel y tóner	Aumento de residuos sólidos y consumo de recursos forestales	Digitalización de documentos e impresión únicamente cuando sea necesario.
Limpieza de equipos tecnológicos	Uso de productos químicos	Contaminación por residuos químicos	Utilización de productos biodegradables y disposición adecuada de envases.
Uso de aire acondicionado en centros de datos	Consumo de energía eléctrica	Incremento de la huella de carbono	Programas de mantenimiento y control eficiente de la temperatura.
Mantenimiento de infraestructura tecnológica	Generación de empaques, cables y residuos ordinarios	Incremento de residuos sólidos	Separación en la fuente y reciclaje de materiales aprovechables.
Operación administrativa	Consumo de agua	Uso de recursos naturales	Campañas de ahorro y dispositivos de bajo consumo.
Transporte para soporte técnico	Consumo de combustibles fósiles	Emisión de gases de efecto invernadero	Planeación de rutas, mantenimiento de vehículos y promoción de buenas prácticas de conducción.



5. Plan de auditoría

5.1 Objetivo de la auditoría

Verificar el grado de conformidad del Sistema Integrado de Gestión (SIG) implementado en el Área de Tecnología y Central de Operaciones de **SJ Seguridad Privada Ltda.**, evaluando el cumplimiento de los requisitos establecidos en las normas **ISO 9001:2015**, **ISO 14001:2015** e **ISO 45001:2018**, así como de la legislación colombiana aplicable y de los procedimientos internos de la organización, con el fin de identificar fortalezas, oportunidades de mejora y no conformidades que contribuyan al mejoramiento continuo del proceso.

5.2 Alcance de la auditoría

La auditoría comprende las actividades desarrolladas en el **Área de Tecnología y Central de Operaciones**, incluyendo:

- Monitoreo de alarmas 24/7.
- Monitoreo de CCTV.
- Administración de la plataforma Kronos.
- Administración de la plataforma DSS (Dahua Security Software).
- Administración de Dynamic Codes para control de acceso.
- Gestión de servidores y almacenamiento.
- Administración de redes y telecomunicaciones.
- Gestión de respaldos (Backups).
- Administración de usuarios y permisos.
- Soporte técnico interno.
- Mantenimiento preventivo y correctivo de la infraestructura tecnológica.
- Gestión documental del proceso.
- Seguimiento de indicadores.
- Gestión de riesgos, aspectos ambientales y peligros de SST.



5.3 Criterios de auditoría

La auditoría se realizará tomando como referencia los siguientes criterios:

- ISO 9001:2015 – Sistema de Gestión de la Calidad.
- ISO 14001:2015 – Sistema de Gestión Ambiental.
- ISO 45001:2018 – Sistema de Gestión de Seguridad y Salud en el Trabajo.
- Decreto 1072 de 2015.
- Resolución 0312 de 2019.
- Ley 1562 de 2012.
- Procedimientos internos de SJ Seguridad Privada Ltda.
- Políticas del Sistema Integrado de Gestión.
- Objetivos del proceso.
- Indicadores de gestión.
- Requisitos contractuales con los clientes.

5.4 Equipo auditor Tabla 8

Cargo	Responsabilidad
Auditor líder	Planificar, dirigir y coordinar la auditoría, elaborar el informe final y presentar las conclusiones.
Auditor interno	Ejecutar entrevistas, revisar documentos, recopilar evidencias y elaborar hallazgos.
Auditado	Atender la auditoría, suministrar información y presentar las evidencias solicitadas.

Proceso auditado: Tecnología y Central de Operaciones.

Responsable del proceso: Coordinador de Tecnología y Central de Operaciones.



5.5 Metodología de la auditoría

La auditoría se desarrollará siguiendo las directrices de la **ISO 19011:2018**, utilizando las siguientes técnicas:

- Revisión documental.
- Entrevistas al personal.
- Observación directa de las actividades.
- Recorrido por las instalaciones.
- Verificación de registros.
- Muestreo de documentos.
- Revisión de indicadores.
- Análisis de evidencias objetivas.

5.6 Recursos requeridos

Para el desarrollo de la auditoría se dispondrá de:

- Plan de auditoría.
- Lista de verificación.
- Manual del Sistema Integrado de Gestión.
- Procedimientos documentados.
- Matriz legal.
- Matriz de riesgos.
- Matriz de aspectos ambientales.
- Indicadores del proceso.
- Computador portátil.
- Acceso a las plataformas tecnológicas.
- Formatos para registro de hallazgos.



5.7 Cronograma de auditoría Tabla 9

Actividad	Responsable	Duración
Elaboración del plan de auditoría	Auditor líder	1 hora
Reunión de apertura	Auditor líder y auditado	30 minutos
Revisión documental	Equipo auditor	2 horas
Entrevistas al personal	Equipo auditor	2 horas
Recorrido por la Central de Operaciones	Equipo auditor	1 hora
Verificación de evidencias	Equipo auditor	2 horas
Consolidación de hallazgos	Equipo auditor	1 hora
Reunión de cierre	Auditor líder	30 minutos
Elaboración del informe final	Auditor líder	4 horas



5.8 Documentos objeto de revisión

Durante la auditoría se revisarán, entre otros, los siguientes documentos:

- Manual del Sistema Integrado de Gestión.
- Política Integrada.
- Caracterización del proceso.
- Procedimiento de monitoreo de alarmas.
- Procedimiento de administración de plataformas tecnológicas.
- Procedimiento de mantenimiento preventivo.
- Procedimiento de gestión de incidentes.
- Plan de continuidad del negocio.
- Inventario de activos tecnológicos.
- Registros de mantenimiento.
- Registros de respaldos (Backups).
- Registros de incidentes tecnológicos.
- Indicadores de gestión.
- Matriz de requisitos legales.
- Matriz de identificación de peligros.
- Matriz de aspectos e impactos ambientales.
- Registros de capacitación.
- Informes de auditorías anteriores.
- Acciones correctivas y de mejora.



5.9 Riesgos de la auditoría

Durante la ejecución de la auditoría podrían presentarse las siguientes situaciones:

- Disponibilidad limitada del personal operativo por la atención de eventos críticos.
- Acceso restringido a información confidencial.
- Interrupciones ocasionadas por incidentes tecnológicos.
- Cambios operacionales durante el desarrollo de la auditoría.
- Evidencias documentales incompletas o desactualizadas.

Para mitigar estos riesgos se coordinará previamente la agenda con el responsable del proceso, se garantizará la confidencialidad de la información y se utilizará un muestreo representativo de documentos y registros.

5.10 Resultados esperados

Con la ejecución de la auditoría se espera:

- Verificar el cumplimiento de los requisitos de las normas ISO 9001:2015, ISO 14001:2015 e ISO 45001:2018.
- Confirmar el cumplimiento de los requisitos legales aplicables.
- Identificar fortalezas del proceso.
- Detectar oportunidades de mejora.
- Identificar no conformidades y sus causas.
- Proponer acciones correctivas y preventivas.
- Fortalecer la cultura de mejora continua en el Área de Tecnología y Central de Operaciones.
- Incrementar la eficacia del Sistema Integrado de Gestión y contribuir a la satisfacción de los clientes.



6. Lista de verificación para la auditoría interna Tabla 10.

Proceso auditado: Tecnología y Central de Operaciones

Normas de referencia: ISO 9001:2015 – ISO 14001:2015 – ISO 45001:2018

Auditor: _____

Fecha: _____

Responsable del proceso: _____

Numeral ISO	Pregunta de verificación	Evidencia a revisar	Cumple	Observaciones
4.1	¿Se han identificado las cuestiones internas y externas que afectan el proceso?	Contexto organizacional		
4.2	¿Se identificaron las partes interesadas y sus necesidades?	Matriz de partes interesadas		
4.3	¿Está definido el alcance del Sistema Integrado de Gestión para el proceso?	Documento del alcance		
4.4	¿La caracterización del proceso se encuentra actualizada?	Caracterización del proceso		
5.1	¿La Alta Dirección demuestra liderazgo y compromiso con el SIG?	Política, actas, reuniones		
5.2	¿La política integrada es conocida por el personal?	Entrevistas		
5.3	¿Las responsabilidades y autoridades están definidas?	Manual de funciones		
6.1	¿Se identifican riesgos y oportunidades del proceso?	Matriz de riesgos		
6.1	¿Se identifican peligros de SST?	Matriz IPER		



6.1	¿Se identifican aspectos e impactos ambientales?	Matriz ambiental		
6.1	¿Se identifican requisitos legales aplicables?	Matriz legal		
6.2	¿Existen objetivos e indicadores del proceso?	Indicadores		
6.2	¿Los objetivos tienen seguimiento periódico?	Informes de indicadores		
7.1	¿Se cuenta con los recursos necesarios para operar?	Inventario tecnológico		
7.1	¿Existe infraestructura suficiente para la continuidad del servicio?	Servidores, UPS, planta		
7.1	¿Los recursos tecnológicos reciben mantenimiento?	Registros de mantenimiento		
7.2	¿El personal es competente para desempeñar sus funciones?	Hojas de vida y capacitaciones		
7.2	¿Existe evidencia de formación en SST?	Registros de capacitación		
7.3	¿El personal conoce la política integrada?	Entrevistas		
7.4	¿La comunicación interna es efectiva?	Correos, reuniones		
7.5	¿La información documentada está controlada?	Procedimientos y formatos		
8.1	¿Las actividades del proceso están planificadas y controladas?	Procedimientos		
8.1	¿Existen controles para los riesgos identificados?	Matriz de riesgos		



8.1	¿Se controlan los cambios tecnológicos?	Registros de cambios		
8.2	¿Se gestionan adecuadamente los requerimientos del cliente?	Solicitudes y tickets		
8.4	¿Se evalúan los proveedores tecnológicos?	Evaluación de proveedores		
8.5	¿Se ejecutan mantenimientos preventivos?	Cronograma y registros		
8.5	¿Se realizan copias de seguridad de la información?	Bitácoras de backup		
8.5	¿Se administra el acceso a las plataformas?	Registros de usuarios		
8.5	¿Se monitorea la disponibilidad de servidores?	Consola de monitoreo		
8.5	¿Existe control sobre incidentes tecnológicos?	Mesa de ayuda		
8.5	¿Los operadores siguen los protocolos de monitoreo?	Observación directa		
8.6	¿Se verifica la conformidad del servicio antes de su entrega?	Registros operativos		
8.7	¿Existe tratamiento para servicios no conformes?	Registros de incidentes		
9.1	¿Se realiza seguimiento a los indicadores?	Informes mensuales		
9.1	¿Se mide el cumplimiento de los ANS?	Reportes de SLA		
9.1	¿Se mide el tiempo de atención de incidentes?	Reportes Kronos		



9.1	¿Se controla la disponibilidad de la infraestructura?	Indicadores		
9.1	¿Se evalúa el desempeño ambiental?	Indicadores ambientales		
9.1	¿Se evalúa el desempeño del SG-SST?	Indicadores SST		
9.2	¿Se realizan auditorías internas?	Programa de auditorías		
9.3	¿La dirección revisa el desempeño del SIG?	Actas de revisión		
10.1	¿Se implementan acciones de mejora?	Planes de mejora		
10.2	¿Se gestionan acciones correctivas?	Formatos de acciones correctivas		
10.2	¿Se analiza la causa raíz de las no conformidades?	Análisis de causas		
10.3	¿Existe evidencia de mejora continua?	Informes y proyectos		
ISO 14001	¿Existe programa para el manejo de RAEE?	Programa ambiental		
ISO 14001	¿Los residuos electrónicos se entregan a un gestor autorizado?	Certificados		
ISO 14001	¿Se controla el consumo de energía?	Facturas e indicadores		
ISO 14001	¿Se promueve el ahorro de papel?	Evidencias		
ISO 14001	¿Se realiza separación de residuos en la fuente?	Inspección		



ISO 45001	¿Se realizan inspecciones de seguridad?	Registros		
ISO 45001	¿El personal utiliza los EPP requeridos?	Observación		
ISO 45001	¿Se investigan incidentes y accidentes?	Informes		
ISO 45001	¿Existe plan de emergencias?	Documento		
ISO 45001	¿Se realizan simulacros?	Actas		
ISO 45001	¿Los puestos de trabajo cumplen criterios ergonómicos?	Inspección		
ISO 45001	¿Se ejecutan pausas activas?	Registros		
ISO 45001	¿Se controlan los riesgos eléctricos?	Inspecciones		
ISO 45001	¿Se encuentra actualizada la matriz de peligros?	Matriz IPER		
Integrado	¿El proceso cumple los requisitos legales aplicables?	Matriz legal		
Integrado	¿Los documentos se encuentran vigentes y controlados?	Listado maestro		
Integrado	¿El proceso demuestra mejora continua?	Evidencias objetivas		



Resultado de la auditoría

- Total de preguntas evaluadas: _____
- Cumple: _____
- No cumple: _____
- No aplica: _____

Concepto del auditor

Firma del Auditor: _____

Firma del responsable del Proceso: _____



7. Ejecución de la auditoría

7.1 Preparación de la auditoría

La auditoría interna al Área de Tecnología y Central de Operaciones de SJ Seguridad Privada Ltda. se desarrolló de manera simulada siguiendo los lineamientos establecidos en la norma ISO 19011:2018, la cual proporciona las directrices para la planificación, ejecución, seguimiento y mejora de las auditorías a sistemas de gestión.

El objetivo de la auditoría fue verificar el grado de cumplimiento de los requisitos establecidos en las normas ISO 9001:2015, ISO 14001:2015 e ISO 45001:2018, así como evaluar la eficacia de los controles implementados en el proceso de Tecnología y Central de Operaciones.

La auditoría se llevó a cabo mediante la revisión documental, entrevistas al personal responsable, observación directa de las actividades y verificación de evidencias objetivas.

Antes del inicio de la auditoría se realizaron las siguientes actividades:

- Elaboración y aprobación del Plan de Auditoría.
- Definición del alcance, criterios y objetivos de la auditoría.
- Revisión de la caracterización del proceso.
- Revisión de la política integrada.
- Revisión de la matriz de requisitos legales.
- Revisión de la matriz de riesgos y oportunidades.
- Revisión de la matriz de peligros y controles.
- Revisión de la matriz de aspectos e impactos ambientales.
- Elaboración de la lista de verificación.
- Programación de entrevistas con el personal del proceso.
- Programación del recorrido por la Central de Operaciones.

La preparación permitió conocer previamente el funcionamiento del proceso y determinar las evidencias necesarias para evaluar el cumplimiento de los requisitos normativos.



7.1.1 Reunión de apertura

La auditoría inició con una reunión de apertura entre el auditor y el responsable del Área de Tecnología y Central de Operaciones.

Durante esta reunión se presentaron:

- Objetivo de la auditoría.
- Alcance.
- Criterios de evaluación.
- Cronograma.
- Metodología.
- Responsabilidades del auditor y del auditado.
- Mecanismos para el suministro de información.
- Confidencialidad de la información revisada.

El responsable del proceso manifestó su conformidad con el desarrollo de la auditoría y designó el personal encargado de suministrar la información requerida.

7.1.2 Recorrido por la Central de Operaciones

Posteriormente se realizó un recorrido por las instalaciones del Área de Tecnología y Central de Operaciones con el fin de observar directamente las condiciones operativas.

Durante la inspección se verificó:

- Estado de los puestos de trabajo.
- Condiciones ergonómicas.
- Organización del cuarto de servidores.
- Funcionamiento de los sistemas UPS.
- Disponibilidad de la planta eléctrica.
- Estado de los equipos de monitoreo.
- Condiciones locativas.



- Señalización.
- Equipos de emergencia.
- Control de acceso a áreas restringidas.
- Gestión de residuos electrónicos.
- Funcionamiento de las plataformas tecnológicas.

Se observó que la infraestructura tecnológica garantiza la continuidad del servicio y dispone de controles para minimizar la ocurrencia de incidentes.

7.2 Desarrollo de entrevistas

Se realizaron entrevistas al personal involucrado en el proceso con el propósito de verificar el conocimiento y la aplicación de los procedimientos establecidos.

Las entrevistas fueron dirigidas a:

- Coordinador de Tecnología y Central de Operaciones.
- Operadores de Monitoreo.
- Personal de Soporte Técnico.
- Administrador de Infraestructura Tecnológica.
- Responsable del Sistema Integrado de Gestión.

Durante las entrevistas se abordaron aspectos relacionados con:

- Política Integrada.
- Objetivos del proceso.
- Gestión de riesgos.
- Gestión ambiental.
- Seguridad y Salud en el Trabajo.
- Procedimientos operacionales.
- Atención de incidentes.
- Copias de seguridad.
- Gestión documental.



- Indicadores.
- Acciones correctivas.
- Continuidad del negocio.

El personal demostró conocimiento general sobre sus responsabilidades y sobre los procedimientos operacionales aplicables al proceso.

7.3 Solicitud y verificación de evidencias

Con el propósito de respaldar los resultados de la auditoría se solicitaron evidencias objetivas, entre ellas:

- Registros de mantenimiento preventivo.
- Cronogramas de mantenimiento.
- Reportes de disponibilidad de plataformas.
- Indicadores de gestión.
- Registros de capacitación.
- Actas de reuniones.
- Evidencias fotográficas.
- Certificados de disposición de residuos electrónicos.
- Reportes de respaldo de información.
- Registros de atención de incidentes.
- Informes de auditorías anteriores.
- Planes de acción.

Las evidencias fueron suficientes para verificar el grado de cumplimiento de la mayoría de los requisitos auditados.



7.4 Redacción de hallazgos

Con base en las evidencias recopiladas se identificaron fortalezas, oportunidades de mejora y no conformidades.

Los hallazgos fueron redactados de forma objetiva, indicando:

- Requisito evaluado.
- Evidencia encontrada.
- Situación observada.
- Criterio incumplido (cuando aplicó).
- Clasificación del hallazgo.

La redacción se realizó siguiendo los principios establecidos por la ISO 19011:2018, evitando apreciaciones subjetivas y sustentando cada hallazgo con evidencias verificables.

8. Hallazgos de la auditoría

Como resultado de la auditoría interna realizada al Área de Tecnología y Central de Operaciones de SJ Seguridad Privada Ltda., se identificaron fortalezas, oportunidades de mejora y no conformidades, las cuales fueron determinadas con base en las evidencias obtenidas durante la revisión documental, las entrevistas realizadas al personal, la observación de las actividades y la verificación del cumplimiento de los requisitos establecidos en las normas ISO 9001:2015, ISO 14001:2015 e ISO 45001:2018.

8.1 Aspectos relevantes o fortalezas

Hallazgo 1. Infraestructura tecnológica robusta

Norma: ISO 9001:2015 – Numeral 7.1 (Recursos).

Evidencia: Se verificó que la Central de Operaciones cuenta con servidores dedicados, sistemas UPS, planta eléctrica de respaldo, almacenamiento redundante y plataformas tecnológicas para garantizar la continuidad del servicio.

Resultado: Se asegura la disponibilidad de los servicios tecnológicos y la continuidad de la operación ante posibles fallas de energía o infraestructura.



Hallazgo 2. Alto cumplimiento de los Acuerdos de Nivel de Servicio (ANS)

Norma: ISO 9001:2015 – Numeral 9.1 (Seguimiento y medición).

Evidencia: Los indicadores del proceso muestran un cumplimiento promedio superior al 98 % en los tiempos de atención de alarmas e incidentes tecnológicos.

Resultado: El proceso mantiene un nivel elevado de satisfacción del cliente y cumple con los tiempos de respuesta establecidos.

Hallazgo 3. Personal competente y comprometido

Norma: ISO 9001:2015 – Numeral 7.2 (Competencia).

Evidencia: Durante las entrevistas se evidenció que los colaboradores conocen sus funciones, los procedimientos operativos y las plataformas tecnológicas utilizadas en la Central de Operaciones.

Resultado: El nivel de competencia del personal favorece la correcta prestación del servicio.

Hallazgo 4. Controles implementados para Seguridad y Salud en el Trabajo

Norma: ISO 45001:2018 – Numerales 6.1 y 8.1.

Evidencia: Se verificó la existencia de la matriz de peligros, programas de pausas activas, inspecciones de seguridad y elementos de protección personal para actividades técnicas.

Resultado: Se evidencian acciones preventivas orientadas a proteger la salud y seguridad de los trabajadores.

Hallazgo 5. Gestión de la información y continuidad del negocio

Norma: ISO 9001:2015 – Numeral 7.5.

Evidencia: Se verificó la ejecución de copias de seguridad periódicas, controles de acceso a plataformas y procedimientos para la recuperación de la información.

Resultado: La organización cuenta con mecanismos que fortalecen la disponibilidad y confidencialidad de la información.



8.2 Oportunidades de mejora

Hallazgo 6. Actualización de la documentación del proceso

Norma: ISO 9001:2015 – Numeral 7.5.

Evidencia: Se identificó que algunos procedimientos e instructivos presentan fechas de actualización superiores a un año y no reflejan completamente las herramientas tecnológicas actualmente utilizadas.

Oportunidad de mejora: Actualizar periódicamente la documentación para asegurar que refleje las actividades y tecnologías vigentes.

Hallazgo 7. Seguimiento a indicadores ambientales

Norma: ISO 14001:2015 – Numeral 9.1.

Evidencia: Aunque existen indicadores ambientales, no todos cuentan con análisis de tendencias ni con planes de acción asociados a sus resultados.

Oportunidad de mejora: Fortalecer el seguimiento de los indicadores ambientales mediante análisis periódicos y definición de acciones de mejora.

Hallazgo 8. Fortalecimiento del programa de capacitación

Norma: ISO 9001:2015 – Numeral 7.2.

Evidencia: Se evidenció capacitación en plataformas actuales; sin embargo, no existe un plan específico para nuevas tecnologías como inteligencia artificial aplicada al monitoreo y ciberseguridad.

Oportunidad de mejora: Diseñar un programa anual de formación en tecnologías emergentes y gestión de riesgos tecnológicos.

Hallazgo 9. Seguimiento a la evaluación de proveedores tecnológicos

Norma: ISO 9001:2015 – Numeral 8.4.

Evidencia: La evaluación de algunos proveedores se realiza únicamente al finalizar el contrato.



Oportunidad de mejora: Implementar evaluaciones periódicas que permitan monitorear el desempeño de los proveedores durante la ejecución del servicio.

Hallazgo 10. Automatización de reportes operacionales

Norma: ISO 9001:2015 – Numeral 10.3.

Evidencia: Algunos informes de gestión aún se consolidan manualmente, aumentando el tiempo de procesamiento y el riesgo de errores.

Oportunidad de mejora: Automatizar la generación de reportes mediante herramientas de inteligencia de negocios (Business Intelligence).

8.3 No conformidades

No conformidad 1. Documentación desactualizada

Norma incumplida: ISO 9001:2015 – Numeral 7.5.3 (Control de la información documentada).

Evidencia objetiva: Se evidenció que el procedimiento de Administración de Plataformas Tecnológicas no incorpora las actualizaciones correspondientes a las plataformas implementadas recientemente.

Descripción: La organización no garantiza que toda la información documentada se mantenga actualizada y disponible para su uso.

Clasificación: No conformidad menor.

No conformidad 2. Seguimiento insuficiente a indicadores ambientales

Norma incumplida: ISO 14001:2015 – Numeral 9.1.1 (Seguimiento, medición, análisis y evaluación).

Evidencia objetiva: Durante la revisión documental se observó que no se dispone de análisis de resultados para los indicadores de consumo de energía y gestión de residuos electrónicos correspondientes al último trimestre.

Descripción: No se demuestra un seguimiento sistemático al desempeño ambiental del proceso.

Clasificación: No conformidad menor.



No conformidad 3. Cierre extemporáneo de acciones correctivas

Norma incumplida: ISO 9001:2015 – Numeral 10.2 (No conformidad y acción correctiva).

Evidencia objetiva: Se verificó que algunas acciones correctivas derivadas de auditorías anteriores permanecen abiertas después del plazo establecido, sin evidencia de seguimiento o cierre formal.

Descripción: La organización no asegura el cierre oportuno de las acciones correctivas implementadas para eliminar las causas de las no conformidades identificadas.

Clasificación: No conformidad menor.

8.1 Aspectos relevantes o fortalezas

Durante la ejecución de la auditoría se identificaron diversas fortalezas que evidencian el compromiso de SJ Seguridad Privada Ltda. con la implementación y mantenimiento del Sistema Integrado de Gestión en el Área de Tecnología y Central de Operaciones. Estas fortalezas contribuyen al cumplimiento de los objetivos del proceso, la satisfacción de los clientes y la mejora continua de la organización.

Fortaleza 1. Infraestructura tecnológica que garantiza la continuidad del servicio

Norma de referencia: ISO 9001:2015 – Numeral 7.1 (Recursos).

Evidencia: Se verificó que la Central de Operaciones dispone de servidores dedicados, sistemas UPS, planta eléctrica de respaldo, almacenamiento seguro y plataformas tecnológicas especializadas para el monitoreo de alarmas, CCTV y control de acceso.

Aspecto relevante: La infraestructura tecnológica permite mantener la continuidad de la operación durante las 24 horas del día, minimizando el riesgo de interrupciones en la prestación del servicio.

Fortaleza 2. Cumplimiento de los Acuerdos de Nivel de Servicio (ANS)

Norma de referencia: ISO 9001:2015 – Numeral 9.1 (Seguimiento, medición, análisis y evaluación).

Evidencia: Los indicadores del proceso muestran un cumplimiento superior al 98 % en los tiempos de atención de eventos e incidentes tecnológicos, conforme a los compromisos establecidos con los clientes.



Aspecto relevante: El seguimiento permanente a los indicadores permite mantener altos niveles de desempeño y contribuir a la satisfacción del cliente.

Fortaleza 3. Personal competente y comprometido con el proceso

Norma de referencia: ISO 9001:2015 – Numeral 7.2 (Competencia).

Evidencia: Durante las entrevistas se evidenció que los colaboradores conocen sus responsabilidades, los procedimientos del proceso y el funcionamiento de las plataformas tecnológicas utilizadas en la operación.

Aspecto relevante: La experiencia y el compromiso del personal favorecen una atención eficiente de los eventos y una adecuada operación de la Central de Operaciones.

Fortaleza 4. Implementación de controles en Seguridad y Salud en el Trabajo

Norma de referencia: ISO 45001:2018 – Números 6.1 y 8.1.

Evidencia: Se verificó la implementación de la matriz de identificación de peligros, programas de pausas activas, inspecciones de seguridad, capacitaciones y controles para la prevención de riesgos eléctricos, ergonómicos y locativos.

Aspecto relevante: Los controles implementados contribuyen a proteger la salud y seguridad de los colaboradores, reduciendo la probabilidad de accidentes y enfermedades laborales.

Fortaleza 5. Gestión adecuada de la información y continuidad del negocio

Norma de referencia: ISO 9001:2015 – Numeral 7.5 (Información documentada).

Evidencia: Se evidenció la ejecución periódica de copias de seguridad (backups), el control de accesos a las plataformas tecnológicas, la administración de usuarios y la existencia de procedimientos para la recuperación de la información ante incidentes.

Aspecto relevante: La organización cuenta con mecanismos que fortalecen la seguridad de la información, garantizan la disponibilidad de los datos críticos y respaldan la continuidad de las operaciones.



8.2 Oportunidades de mejora

Como resultado de la auditoría interna realizada al Área de Tecnología y Central de Operaciones de SJ Seguridad Privada Ltda., se identificaron oportunidades de mejora que, aunque no representan incumplimientos de los requisitos de las normas ISO, permitirán fortalecer la eficacia del Sistema Integrado de Gestión y optimizar el desempeño del proceso.

Oportunidad de mejora 1. Actualización de la documentación del proceso

Norma de referencia: ISO 9001:2015 – Numeral 7.5 Información documentada.

Evidencia: Se evidenció que algunos procedimientos e instructivos del proceso no reflejan las últimas actualizaciones tecnológicas implementadas por la organización, como nuevas plataformas de monitoreo y mejoras en la infraestructura.

Recomendación: Establecer un cronograma de revisión y actualización documental, garantizando que los procedimientos, instructivos y formatos se mantengan alineados con la operación actual.

Oportunidad de mejora 2. Fortalecer el seguimiento a los indicadores ambientales

Norma de referencia: ISO 14001:2015 – Numeral 9.1 Seguimiento, medición, análisis y evaluación.

Evidencia: Aunque se realiza el registro del consumo de energía y la gestión de residuos electrónicos, no se evidencia un análisis periódico de tendencias ni la definición de acciones preventivas cuando se presentan desviaciones.

Recomendación: Implementar informes trimestrales de desempeño ambiental que permitan analizar el comportamiento de los indicadores y definir acciones orientadas al mejoramiento continuo.

Oportunidad de mejora 3. Capacitación en nuevas tecnologías y ciberseguridad

Norma de referencia: ISO 9001:2015 – Numeral 7.2 Competencia.

Evidencia: Se constató que el personal cuenta con formación en las plataformas actualmente utilizadas; sin embargo, se identificó la necesidad de ampliar los conocimientos en temas como inteligencia artificial aplicada al monitoreo, análisis de video, ciberseguridad y protección de infraestructuras críticas.



Recomendación: Diseñar un plan anual de capacitación enfocado en nuevas tecnologías, fortaleciendo las competencias técnicas del personal y la capacidad de respuesta frente a amenazas emergentes.

Oportunidad de mejora 4. Evaluación continua del desempeño de proveedores tecnológicos

Norma de referencia: ISO 9001:2015 – Numeral 8.4 Control de los procesos, productos y servicios suministrados externamente.

Evidencia: Se observó que la evaluación de algunos proveedores tecnológicos se realiza únicamente al finalizar el contrato, limitando la posibilidad de detectar oportunamente desviaciones en la prestación del servicio.

Recomendación: Implementar evaluaciones periódicas del desempeño de los proveedores mediante indicadores relacionados con tiempos de respuesta, calidad del soporte, cumplimiento de acuerdos de nivel de servicio y satisfacción del cliente interno.

Oportunidad de mejora 5. Automatización de reportes e indicadores de gestión

Norma de referencia: ISO 9001:2015 – Numeral 10.3 Mejora continua.

Evidencia: Parte de los informes operativos e indicadores del proceso se elaboran de forma manual, lo que incrementa el tiempo de procesamiento y la posibilidad de errores en la consolidación de la información.

Recomendación: Implementar herramientas de inteligencia de negocios (Business Intelligence) o tableros de control (Dashboards) que permitan visualizar en tiempo real los indicadores de gestión, facilitando la toma de decisiones y el seguimiento al desempeño del proceso.



8.3 No conformidades

Durante la auditoría interna se identificaron tres no conformidades de carácter menor. Estas corresponden a incumplimientos puntuales de algunos requisitos establecidos en las normas ISO 9001:2015 e ISO 14001:2015, los cuales no comprometen la capacidad del proceso para prestar el servicio, pero requieren la implementación de acciones correctivas para evitar su recurrencia y fortalecer el Sistema Integrado de Gestión.

No conformidad 1. Información documentada desactualizada

Norma: ISO 9001:2015 – Numeral 7.5.3 Control de la información documentada.

Hallazgo: Durante la revisión documental se evidenció que el procedimiento de administración de plataformas tecnológicas y algunos instructivos operativos no incorporan las actualizaciones relacionadas con las herramientas y plataformas implementadas recientemente en la Central de Operaciones.

Evidencia objetiva:

- Procedimientos con fechas de revisión vencidas.
- Instructivos que no incluyen las últimas funcionalidades de las plataformas tecnológicas utilizadas.
- Ausencia de registros que evidencien la revisión periódica de algunos documentos.

Impacto: El uso de documentación desactualizada puede generar diferencias en la ejecución de las actividades y afectar la estandarización del proceso.

Clasificación: No conformidad menor.

No conformidad 2. Seguimiento insuficiente a los indicadores ambientales

Norma: ISO 14001:2015 – Numeral 9.1.1 Seguimiento, medición, análisis y evaluación.

Hallazgo: Se evidenció que, aunque el proceso registra información relacionada con el consumo de energía eléctrica y la gestión de residuos de aparatos eléctricos y electrónicos (RAEE), no se realizan análisis periódicos de tendencias ni se documentan acciones de mejora derivadas de los resultados obtenidos.



Evidencia objetiva:

- Indicadores ambientales sin análisis comparativo de resultados.
- Falta de informes de seguimiento del último trimestre.
- Ausencia de planes de acción asociados a desviaciones detectadas.

Impacto: La falta de seguimiento limita la evaluación del desempeño ambiental y dificulta la toma de decisiones orientadas a la mejora continua.

Clasificación: No conformidad menor.

No conformidad 3. Acciones correctivas sin cierre oportuno

Norma: ISO 9001:2015 – Numeral 10.2 No conformidad y acción correctiva.

Hallazgo: Se identificó que algunas acciones correctivas derivadas de auditorías internas anteriores continúan abiertas después de la fecha establecida para su cierre, sin evidencia documental que demuestre su verificación o eficacia.

Evidencia objetiva:

- Planes de acción con actividades vencidas.
- Registros sin evidencia de seguimiento.
- Ausencia de cierre formal y evaluación de la eficacia de las acciones implementadas.

Impacto: El incumplimiento en el cierre de las acciones correctivas aumenta la probabilidad de que las causas de las no conformidades se repitan, afectando la eficacia del Sistema Integrado de Gestión.

Clasificación: No conformidad menor.



9. Plan de acciones correctivas

No conformidad 1. Información documentada desactualizada

Descripción de la no conformidad

Se evidenció que algunos procedimientos e instructivos del Área de Tecnología y Central de Operaciones no reflejan las actualizaciones realizadas a las plataformas y procesos tecnológicos.

Análisis de causa (5 Porqués) Tabla 11.

Pregunta	Respuesta
¿Por qué la documentación está desactualizada?	Porque algunos procedimientos no fueron revisados después de implementar cambios tecnológicos.
¿Por qué no fueron revisados?	Porque no existía un cronograma formal de revisión documental.
¿Por qué no existía dicho cronograma?	Porque la actualización documental dependía únicamente de la necesidad del proceso.
¿Por qué dependía de la necesidad?	Porque no se había asignado un seguimiento periódico a esta actividad.
¿Causa raíz?	Falta de un procedimiento formal para la revisión y actualización periódica de la información documentada.

Plan de acción Tabla 12.

Acción correctiva	Responsable	Plazo	Indicador
Actualizar todos los procedimientos e instructivos del proceso.	Coordinador de Tecnología	30 días	100 % de documentos actualizados.
Implementar un cronograma semestral de revisión documental.	Coordinador SIG	30 días	Cronograma implementado.
Socializar los cambios con el personal.	Coordinador de Tecnología	15 días posteriores a la actualización	100 % del personal capacitado.

No conformidad 2. Seguimiento insuficiente a los indicadores ambientales

Descripción de la no conformidad

No se evidenció un análisis periódico de los indicadores relacionados con el consumo de energía y la gestión de residuos electrónicos (RAEE).

Análisis de causa (5 Porqués) Tabla 13.

Pregunta	Respuesta
¿Por qué no se analizan los indicadores?	Porque únicamente se registran los datos mensualmente.
¿Por qué solo se registran?	Porque no existe un procedimiento para analizar tendencias.
¿Por qué no existe el procedimiento?	Porque no había sido definido dentro del proceso ambiental.
¿Por qué no fue definido?	Porque se priorizó el cumplimiento operativo sobre el análisis de resultados.
Causa raíz	Ausencia de un procedimiento para el análisis periódico del desempeño ambiental.

Plan de acción

Acción correctiva	Responsable	Plazo	Indicador
Diseñar el procedimiento para el análisis de indicadores ambientales.	Responsable SIG	20 días	Procedimiento aprobado.
Elaborar informes trimestrales de desempeño ambiental.	Coordinador de Tecnología	Trimestral	100 % de informes elaborados.
Definir acciones de mejora cuando existan desviaciones.	Responsable Ambiental	Permanente	100 % de desviaciones tratadas.

No conformidad 3. Acciones correctivas sin cierre oportuno

Descripción de la no conformidad

Se evidenció que algunas acciones correctivas derivadas de auditorías anteriores permanecen abiertas después del plazo establecido, sin evidencia de seguimiento ni verificación de eficacia.

Análisis de causa (5 Porqués) Tabla 14.

Pregunta	Respuesta
¿Por qué las acciones correctivas no se cerraron?	Porque no se realizó seguimiento periódico.
¿Por qué no hubo seguimiento?	Porque no existía un responsable claramente asignado.
¿Por qué no estaba asignado?	Porque el procedimiento no definía responsables específicos.
¿Por qué el procedimiento no los definía?	Porque no había sido actualizado.
Causa raíz	Deficiencia en la asignación de responsabilidades y seguimiento de las acciones correctivas.

Plan de acción

Acción correctiva	Responsable	Plazo	Indicador
Actualizar el procedimiento de acciones correctivas.	Coordinador SIG	30 días	Procedimiento actualizado.
Asignar responsables y fechas para cada acción correctiva.	Coordinador de Tecnología	Inmediato	100 % de acciones con responsable asignado.
Realizar seguimiento mensual al estado de las acciones.	Responsable SIG	Mensual	100 % de acciones revisadas.
Verificar la eficacia antes del cierre de cada acción.	Auditor Interno	Permanente	100 % de acciones verificadas.

Seguimiento al plan de acciones correctivas

Para asegurar la eficacia del presente plan, se realizarán reuniones mensuales de seguimiento entre el Coordinador de Tecnología y Central de Operaciones y el responsable del Sistema Integrado de Gestión. Durante estas reuniones se verificará el cumplimiento de las actividades programadas, el avance de las acciones implementadas y la efectividad de las medidas adoptadas.

El cierre de cada acción correctiva se realizará únicamente cuando exista evidencia objetiva que demuestre la eliminación de la causa raíz y la no recurrencia de la no conformidad identificada.

9.1 Análisis de causas

Con el fin de determinar el origen de las no conformidades identificadas durante la auditoría interna al Área de Tecnología y Central de Operaciones de **SJ Seguridad Privada Ltda.**, se aplicó la metodología de los **Cinco Porqués (5 Why's)**. Esta herramienta permite identificar la causa raíz de un problema mediante un análisis secuencial de las razones que lo originan, facilitando la definición de acciones correctivas eficaces que eviten su recurrencia.

Análisis de causa de la No conformidad 1 Tabla 15

No conformidad: Información documentada desactualizada.

Análisis (5 Porqués)	Respuesta
¿Por qué la documentación se encuentra desactualizada?	Porque algunos procedimientos no han sido revisados desde su última actualización.
¿Por qué no se han revisado?	Porque no existe un cronograma formal para la revisión periódica de la documentación.
¿Por qué no existe dicho cronograma?	Porque el proceso no tiene definido un responsable exclusivo para el control documental.
¿Por qué no se ha asignado un responsable?	Porque la actualización documental se realiza únicamente cuando se presenta un cambio importante en la operación.
¿Por qué se espera a que ocurra un cambio importante?	Porque no se cuenta con un procedimiento que establezca revisiones periódicas de la información documentada.

Causa raíz: Falta de un procedimiento formal y de un cronograma para la revisión y actualización periódica de la información documentada del proceso.

Análisis de causa de la No conformidad 2

No conformidad: Seguimiento insuficiente a los indicadores ambientales.

Análisis (5 Porqués)	Respuesta
¿Por qué no se realiza un análisis de los indicadores ambientales?	Porque únicamente se registra la información sin efectuar un análisis de resultados.
¿Por qué solo se registra la información?	Porque no existe un procedimiento que establezca la forma de analizar los indicadores.
¿Por qué no existe ese procedimiento?	Porque el seguimiento ambiental se ha enfocado principalmente en el cumplimiento legal.
¿Por qué el enfoque se limita al cumplimiento legal?	Porque no se han definido actividades específicas para evaluar el desempeño ambiental del proceso.
¿Por qué no se han definido esas actividades?	Porque no se ha integrado el análisis de indicadores ambientales dentro del plan de seguimiento del Sistema Integrado de Gestión.

Causa raíz: Ausencia de un procedimiento que establezca el análisis periódico de los indicadores ambientales y la implementación de acciones de mejora derivadas de sus resultados.

Análisis de causa de la No conformidad 3 Tabla 16.

No conformidad: Acciones correctivas sin cierre oportuno.

Análisis (5 Porqués)	Respuesta
¿Por qué existen acciones correctivas sin cerrar?	Porque no se realizó seguimiento dentro del tiempo establecido.
¿Por qué no se realizó el seguimiento?	Porque no existe un cronograma de verificación de las acciones correctivas.
¿Por qué no existe ese cronograma?	Porque el seguimiento depende exclusivamente del responsable del proceso.
¿Por qué depende de una sola persona?	Porque no se ha definido un mecanismo de control que involucre al Sistema Integrado de Gestión y a los líderes del proceso.
¿Por qué no existe ese mecanismo?	Porque no se implementó un sistema de seguimiento periódico para verificar el avance y la eficacia de las acciones correctivas.

Causa raíz: Deficiencia en el seguimiento y control del plan de acciones correctivas, ocasionada por la ausencia de un mecanismo formal para verificar el cumplimiento de los compromisos establecidos.

9.2 Plan de acción

Con base en las causas raíz identificadas durante el proceso de auditoría, se establece el siguiente plan de acción, cuyo propósito es eliminar las causas de las no conformidades detectadas, prevenir su recurrencia y fortalecer la eficacia del Sistema Integrado de Gestión del Área de Tecnología y Central de Operaciones de **SJ Seguridad Privada Ltda.**

No conformidad	Objetivo de la acción	Acción correctiva	Responsable	Plazo	Recursos requeridos	Indicador de seguimiento	Evidencia de cumplimiento
Información documentada desactualizada.	Garantizar que toda la información documentada se mantenga actualizada y disponible para el personal.	Revisar, actualizar y aprobar todos los procedimientos, instructivos y formatos del proceso. Implementar un cronograma anual de revisión documental y socializar los cambios con el	Coordinador de Tecnología y responsable del Sistema Integrado de Gestión	30 días	Personal del proceso, software documental y tiempo de revisión.	(Documentos actualizados ÷ Documentos programados) × 100	Procedimientos actualizados, listado maestro de documentos, registros de socialización y actas de aprobación.



		personal.					
Seguimiento insuficiente a los indicadores ambientales.	Fortalecer el control y evaluación del desempeño ambiental del proceso.	Diseñar un procedimiento para el análisis mensual de indicadores ambientales, asignar responsables, establecer metas y generar informes periódicos con acciones de mejora cuando existan desviaciones.	Coordinador de Tecnología y responsable Ambiental	45 días	Indicadores ambientales, registros de consumo, hojas de cálculo y software de seguimiento.	(Informes ambientales elaborados ÷ Informes programados) × 100	Informes mensuales, análisis de tendencias, planes de acción y actas de seguimiento.
Acciones correctivas sin cierre oportuno.	Asegurar el cierre oportuno y la verificación de la eficacia de las acciones correctivas.	Implementar una matriz de seguimiento con fechas de compromiso, responsables y estado de avance. Realizar reuniones mensuales para verificar el cumplimiento y documentar el cierre de cada acción.	Responsable del Sistema Integrado de Gestión y Coordinador de Tecnología	30 días	Matriz de seguimiento, cronograma de reuniones y registros de auditoría.	(Acciones correctivas cerradas dentro del plazo ÷ Total de acciones correctivas) × 100	Matriz de seguimiento actualizada, actas de reunión, registros de cierre y verificación de eficacia.

Seguimiento al plan de acción

El seguimiento al cumplimiento de este plan será responsabilidad del Coordinador de Tecnología y del responsable del Sistema Integrado de Gestión, quienes verificarán periódicamente el avance de cada actividad, el cumplimiento de los plazos establecidos y la eficacia de las acciones implementadas.



10. Conclusión general

El desarrollo del presente trabajo de grado permitió evaluar el Sistema Integrado de Gestión aplicado al Área de Tecnología y Central de Operaciones de **SJ Seguridad Privada Ltda.**, evidenciando la importancia de integrar la gestión de la calidad, la gestión ambiental y la seguridad y salud en el trabajo como herramientas para fortalecer el desempeño organizacional y garantizar la prestación eficiente de los servicios de seguridad privada.

A través del análisis del contexto organizacional, la identificación de requisitos legales, la evaluación de riesgos, peligros, aspectos e impactos ambientales y la ejecución de una auditoría interna basada en las normas **ISO 9001:2015, ISO 14001:2015 e ISO 45001:2018**, fue posible verificar que el proceso cuenta con una infraestructura tecnológica sólida, personal competente y controles operacionales que favorecen la continuidad del servicio, la satisfacción de los clientes y el cumplimiento de los objetivos estratégicos de la organización.

La auditoría simulada permitió identificar fortalezas que reflejan el compromiso del área con la mejora continua, así como oportunidades de mejora y no conformidades relacionadas principalmente con la actualización de la información documentada, el seguimiento de los indicadores ambientales y la gestión de las acciones correctivas. Aunque estos hallazgos no afectan de manera significativa la operación del proceso, representan oportunidades para fortalecer el Sistema Integrado de Gestión y aumentar su eficacia.

Finalmente, el plan de acciones correctivas propuesto constituye una herramienta que permitirá eliminar las causas de las no conformidades identificadas, optimizar la gestión documental, mejorar el seguimiento de los indicadores y consolidar una cultura de mejora continua. En conclusión, la implementación y fortalecimiento del Sistema Integrado de Gestión en el Área de Tecnología y Central de Operaciones aporta beneficios tanto para la organización como para sus colaboradores y clientes, contribuyendo al cumplimiento de la normativa vigente, al incremento de la eficiencia operativa y al posicionamiento de **SJ Seguridad Privada Ltda.** como una empresa comprometida con la calidad, la sostenibilidad y la seguridad en la prestación de sus servicios.



11. Referencias

Congreso de la República de Colombia. (2012). *Ley 1562 de 2012. Por la cual se modifica el Sistema de Riesgos Laborales y se dictan otras disposiciones en materia de Salud Ocupacional*. Diario Oficial No. 48.488.

Congreso de la República de Colombia. (1979). *Ley 9 de 1979. Por la cual se dictan medidas sanitarias*. Diario Oficial No. 35.308.

Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (2015). *NTC-ISO 9001:2015. Sistemas de gestión de la calidad. Requisitos*. ICONTEC.

Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (2015). *NTC-ISO 14001:2015. Sistemas de gestión ambiental. Requisitos con orientación para su uso*. ICONTEC.

Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (2018). *NTC-ISO 45001:2018. Sistemas de gestión de seguridad y salud en el trabajo. Requisitos con orientación para su uso*. ICONTEC.

Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (2018). *NTC-ISO 19011:2018. Directrices para la auditoría de los sistemas de gestión*. ICONTEC.

Ministerio de Ambiente y Desarrollo Sostenible. (2015). *Decreto 1076 de 2015. Decreto Único Reglamentario del Sector Ambiente y Desarrollo Sostenible*.

Ministerio del Trabajo. (2015). *Decreto 1072 de 2015. Decreto Único Reglamentario del Sector Trabajo*.

Ministerio del Trabajo. (2019). *Resolución 0312 de 2019. Por la cual se definen los estándares mínimos del Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST)*.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2022). *Política de Gobierno Digital*. <https://www.mintic.gov.co>

Organización Internacional de Normalización (ISO). (2015). *ISO 9001:2015. Quality management systems — Requirements*. ISO.

Organización Internacional de Normalización (ISO). (2015). *ISO 14001:2015. Environmental management systems — Requirements with guidance for use*. ISO.

Organización Internacional de Normalización (ISO). (2018). *ISO 45001:2018. Occupational health and safety management systems — Requirements with guidance for use*. ISO.



Organización Internacional de Normalización (ISO). (2018). *ISO 19011:2018. Guidelines for auditing management systems*. ISO.

SJ Seguridad Privada Ltda. (2026). *Manual del Sistema Integrado de Gestión*. Documento interno.

SJ Seguridad Privada Ltda. (2026). *Caracterización del proceso de Tecnología y Central de Operaciones*. Documento interno.

SJ Seguridad Privada Ltda. (2026). *Procedimientos e instructivos del Área de Tecnología y Central de Operaciones*. Documentos internos.

SJ Seguridad Privada Ltda. (2026). *Matriz de identificación de peligros, evaluación y valoración de riesgos (IPER)*. Documento interno.

SJ Seguridad Privada Ltda. (2026). *Matriz de aspectos e impactos ambientales*. Documento interno.

SJ Seguridad Privada Ltda. (2026). *Matriz de requisitos legales del Sistema Integrado de Gestión*. Documento interno.

12. Anexos Tabla 17.

Los anexos presentados a continuación contienen la documentación de soporte utilizada para el desarrollo del presente trabajo de grado y sirven como evidencia de la aplicación del Sistema Integrado de Gestión en el Área de Tecnología y Central de Operaciones de **SJ Seguridad Privada Ltda.**

Anexo	Nombre del anexo	Descripción
Anexo A	Organigrama de SJ Seguridad Privada Ltda.	Estructura organizacional donde se identifica la ubicación del Área de Tecnología y Central de Operaciones dentro de la empresa.
Anexo B	Caracterización del proceso	Documento que contiene el objetivo, alcance, entradas, actividades, salidas, clientes, proveedores, indicadores, riesgos y documentos asociados al proceso.
Anexo C	Matriz DOFA	Análisis de fortalezas, oportunidades, debilidades y amenazas del proceso de Tecnología y Central de Operaciones.
Anexo D	Análisis PESTEL	Evaluación de los factores políticos, económicos, sociales, tecnológicos, ambientales y legales que influyen en el proceso.
Anexo E	Matriz de las Cinco Fuerzas de Porter	Análisis del entorno competitivo del sector de la seguridad privada y los servicios tecnológicos.
Anexo F	Matriz de Competitividad	Comparación de SJ Seguridad Privada Ltda. con empresas del mismo sector mediante factores críticos de éxito.
Anexo G	Matriz de Partes Interesadas	Identificación de las partes interesadas, necesidades, expectativas y mecanismos de seguimiento.
Anexo H	Matriz de Riesgos y Oportunidades	Riesgos identificados en el proceso, controles implementados y oportunidades de mejora.
Anexo I	Matriz de Identificación de Peligros	Identificación de peligros, evaluación de riesgos y controles implementados conforme a la ISO 45001:2018.
Anexo J	Matriz de Aspectos e Impactos Ambientales	Identificación de aspectos ambientales, impactos asociados y controles implementados conforme a la ISO 14001:2015.
Anexo K	Matriz de Requisitos Legales	Normativa aplicable en materia de calidad, medio ambiente y seguridad y salud en el trabajo.
Anexo L	Plan de Auditoría	Objetivos, alcance, criterios, cronograma, metodología y responsables de la auditoría interna.
Anexo M	Lista de Verificación	Formato utilizado para verificar el cumplimiento de los requisitos de las normas ISO 9001:2015, ISO 14001:2015 e ISO 45001:2018.
Anexo N	Registro de Evidencias	Relación de documentos revisados, entrevistas, observaciones y demás evidencias obtenidas durante la auditoría.
Anexo O	Registro de Hallazgos	Consolidado de fortalezas, oportunidades de mejora y no conformidades identificadas durante la auditoría.
Anexo P	Plan de Acciones Correctivas	Análisis de causas, acciones correctivas, responsables, plazos e indicadores de seguimiento.
Anexo Q	Indicadores del proceso	Resultados de los indicadores de gestión del Área de Tecnología y Central de Operaciones.
Anexo R	Evidencias Fotográficas	Registro fotográfico de la Central de Operaciones, cuarto de servidores, infraestructura tecnológica, puestos de trabajo, UPS, planta eléctrica y demás evidencias de la auditoría (cuando aplique).



13. Reunión de cierre

Al finalizar la auditoría se realizó una reunión de cierre con el Coordinador de Tecnología y Central de Operaciones.

Durante la reunión se presentaron:

- Resumen del desarrollo de la auditoría.
- Resultados obtenidos.
- Fortalezas identificadas.
- Oportunidades de mejora.
- No conformidades detectadas.
- Recomendaciones generales.
- Próximas actividades relacionadas con la implementación de acciones correctivas.

El responsable del proceso manifestó conformidad con los resultados obtenidos y se comprometió a elaborar el respectivo plan de acciones correctivas para atender las no conformidades identificadas.

14. Conclusión de la ejecución de la auditoría

La auditoría permitió evidenciar que el Área de Tecnología y Central de Operaciones de SJ Seguridad Privada Ltda. cuenta con un adecuado nivel de implementación del Sistema Integrado de Gestión, evidenciando fortalezas en la continuidad operativa, la infraestructura tecnológica y el compromiso del personal.

No obstante, también se identificaron oportunidades de mejora relacionadas con la actualización de la documentación, el fortalecimiento del seguimiento a los indicadores ambientales y el cierre oportuno de acciones correctivas, aspectos que contribuirán al fortalecimiento del Sistema Integrado de Gestión y al cumplimiento de los requisitos de las normas ISO 9001:2015, ISO 14001:2015 e ISO 45001:2018.

15. Consolidado de aspecto ambiental Tabla 18.

Aspecto ambiental	Impacto ambiental
1. Consumo de energía eléctrica (servidores, monitores, UPS, equipos de comunicaciones y aire acondicionado)	Incremento en el consumo de recursos naturales y emisiones indirectas de CO ₂ por la generación de energía.
2. Generación de residuos electrónicos (RAEE) (equipos obsoletos, discos duros, cámaras, computadores, baterías)	Contaminación del suelo y del agua si los residuos no son gestionados mediante un gestor autorizado.
3. Consumo de papel y tóner	Mayor utilización de recursos forestales y generación de residuos sólidos.
4. Uso y disposición de baterías (UPS, paneles de alarma, radios, dispositivos electrónicos)	Riesgo de contaminación por metales pesados y sustancias químicas cuando no se disponen correctamente.
5. Mantenimiento de plantas eléctricas y equipos (uso de aceites, combustibles y lubricantes)	Posibles derrames que pueden contaminar el suelo, el agua y generar emisiones atmosféricas.

Controles recomendados

- Implementar programas de ahorro y uso eficiente de la energía.
- Entregar los RAEE y baterías únicamente a gestores ambientales autorizados.
- Promover la digitalización de documentos para reducir el consumo de papel.
- Realizar mantenimiento preventivo para evitar fugas de combustibles y aceites.
- Capacitar al personal en la correcta segregación y disposición de residuos.



Riesgo	Consecuencia	Controles
1. Riesgo eléctrico por manipulación de equipos energizados.	Descargas eléctricas, quemaduras o electrocución.	Desenergizar equipos antes de intervenirlos, uso de herramientas aisladas, inspecciones eléctricas y personal autorizado.
2. Riesgo ergonómico por trabajo prolongado frente al computador.	Fatiga visual, dolor lumbar, cervical y síndrome del túnel del carpo.	Puestos ergonómicos, pausas activas, sillas ajustables y capacitación en higiene postural.
3. Riesgo de incendio en el centro de monitoreo o datacenter.	Lesiones al personal, pérdida de información y daños en equipos.	Detectores de humo, extintores, mantenimiento eléctrico, plan de emergencias y simulacros.
4. Riesgo de ciberataques o pérdida de información.	Interrupción del servicio y pérdida de datos críticos.	Antivirus, firewall, copias de seguridad, autenticación multifactor y control de accesos.
5. Riesgo por caídas al mismo nivel durante recorridos técnicos.	Golpes, esguinces o fracturas.	Orden y aseo, señalización, canalización de cables y uso de calzado de seguridad cuando aplique.



Peligro	Control
1. Contacto con energía eléctrica en tableros, UPS y equipos electrónicos.	Bloqueo y etiquetado (LOTO), uso de EPP dieléctrico y mantenimiento preventivo.
2. Posturas estáticas prolongadas durante el monitoreo.	Pausas activas, mobiliario ergonómico y rotación de actividades.
3. Cables sueltos en pisos o áreas de trabajo.	Canaletas, organización del cableado e inspecciones periódicas.
4. Manipulación manual de equipos pesados (UPS, servidores, monitores).	Uso de ayudas mecánicas, trabajo en equipo y capacitación en levantamiento seguro de cargas.
5. Exposición a humo o fuego por cortocircuitos.	Sistema de detección y alarma, extintores adecuados, mantenimiento de instalaciones eléctricas y capacitación en emergencias.