PRACTICAS ITIL Vr. 4 APLICADAS AL CUMPLIMIENTO DE LA ISO/IEC 27001:2022

Sistema de Gestión de Seguridad de la Información
Secretaría de Educación Del Distrito

Versión 1.0
Febrero 2026

Tabla de Contenido

Índice de Tablas

GLOSARIO

ACTIVOS: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

ACTIVO DE INFORMACIÓN: Bien de la entidad (representado en su información y datos) que tiene valor para los procesos de negocio, independientemente de su ubicación; puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil.

PIR (Post-Incident Review): Revisión Posterior a la Implementación (Post-Implementation Review).

SAST: Pruebas Estáticas de Seguridad de Aplicaciones

DAST: Pruebas Dinámicas de Seguridad de Aplicaciones

CISO (Chief Information Security Officer): director de Seguridad de la Información, un ejecutivo responsable de la estrategia de ciberseguridad y de proteger los activos digitales de una organización.

CAB Change Advisory Board: Consejo Asesor de Cambios, equipo responsable de evaluar y aprobar cambios en la infraestructura de TI.

SOP (Security Operations Center): Centro de Operaciones de Seguridad.

NOC (Network Operations Center): Centro de Operaciones de Red.

SGSI: Sistema de Gestión de Seguridad de la Información) es un marco estructurado que incluye políticas, procesos, tecnologías y recursos humanos para proteger la información de una organización contra accesos no autorizados, daños o interrupciones.

BIA (Business Impact Analysis): Análisis de Impacto en el Negocio, metodología para evaluar los efectos de interrupciones en procesos críticos.

RA (Risk Assessment): Evaluación de Riesgos, identifica amenazas y su probabilidad.

KPIs (Key Performance Indicators): métricas cuantificables que miden el rendimiento de un sistema, proyecto o departamento, y se utilizan para evaluar el progreso hacia objetivos específicos.

QA (Quality Assurance): Aseguramiento de la Calidad, es un conjunto de procesos y prácticas para garantizar que un producto de software cumpla con los estándares

y requisitos definidos antes de su lanzamiento.

RFC (Request For Change): solicitudes de cambio, propuesta formal para modificar la infraestructura o los servicios de TI.

SLA: Acuerdo de Nivel de Servicio, contrato en informática que define el nivel de servicio que un proveedor se compromete a ofrecer a un cliente.

Cis: Elementos de Configuración, cualquier componente que necesita ser gestionado para prestar un servicio de TI, y pueden incluir hardware, software, documentación y proveedores.

CMDB: Base de Datos de Gestión de la Configuración, repositorio centralizado que almacena información detallada sobre los activos de TI de una empresa, también llamados elementos de configuración (CIs)

CONTROL: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.

ISO 27001:2013: Norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

PROCEDIMIENTO: Los procedimientos, definen específicamente cómo las políticas, estándares, mejores prácticas y guías serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.

SENSIBILIDAD: Nivel de impacto que una divulgación no autorizada podría generar.

SERVICIO: Es cualquier acto o desempeño que una persona puede ofrecer a otra, que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

1. JUSTIFICACIÓN TÉCNICA

Desde la perspectiva técnica, ITIL 4 y la ISO/IEC 27001:2022 comparten un enfoque basado en procesos y mejora continua.

Las prácticas de gestión de ITIL 4 proporcionan la **infraestructura operativa, metodológica y documental** que la ISO requiere para demostrar conformidad con sus controles.

Cada práctica de ITIL actúa como un **mecanismo de implementación, seguimiento o evidencia técnica** de los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI).

Puntos clave de soporte técnico:

- **Control operacional:** ITIL establece procedimientos estandarizados para la gestión de incidentes, cambios, activos y configuraciones, lo que soporta controles ISO sobre disponibilidad, integridad y trazabilidad de la información.
- **Documentación y trazabilidad:** Las prácticas de conocimiento, mejora continua y medición permiten generar evidencias objetivas requeridas en las auditorías ISO.
- **Monitoreo y cumplimiento:** ITIL provee registros, métricas y dashboards que se alinean con la cláusula 9 de la ISO ("Evaluación del desempeño"), garantizando evidencia verificable.
- **Gestión de seguridad integrada:** Las prácticas de seguridad, continuidad y arquitectura técnica en ITIL habilitan la aplicación coherente de controles A.5 a A.9 de la norma.

En síntesis, ITIL 4 **operativiza los controles ISO/IEC 27001:2022** al proporcionar los mecanismos técnicos y de gestión necesarios para mantener un SGSI funcional, trazable y auditable.

2. JUSTIFICACIÓN TÁCTICA

A nivel táctico, la alineación ITIL–ISO se traduce en una **sinergia de gestión** que conecta los objetivos de gobierno institucional con la ejecución diaria de TI. La ISO define el *"qué se debe cumplir"* (requisitos, controles y objetivos de seguridad), mientras ITIL define el *"cómo se implementa"* mediante prácticas, roles y flujos operativos.

Puntos clave de soporte táctico:

- **Gobernanza y priorización:** Las prácticas ITIL de estrategia, riesgo y relación con el negocio permiten priorizar controles ISO conforme al contexto y apetito de riesgo institucional.
- **Coordinación operativa:** La gestión de incidentes, solicitudes y continuidad de ITIL traduce los requisitos ISO en rutinas diarias sostenibles, evitando duplicidad de procesos.

- **Madurez y mejora continua:** ITIL soporta la cláusula 10 de la ISO (“Mejora”) al establecer mecanismos de retroalimentación, lecciones aprendidas y optimización progresiva del SGSI.
- **Comunicación institucional:** A través de la gestión del conocimiento, relaciones y reportes, ITIL garantiza la trazabilidad y comunicación requerida para la eficacia del SGSI (cláusula 7).

En conjunto, la dimensión táctica de ITIL permite **operacionalizar la estrategia de seguridad**, convertir políticas ISO en prácticas concretas, y generar evidencia de cumplimiento sin alterar la estructura organizacional existente.

3. OBJETIVO

Establecer la alineación integral entre las prácticas de gestión de servicios de TI definidas por ITIL 4 y los controles de seguridad de la información contemplados en la norma ISO/IEC 27001:2022, con el propósito de fortalecer la gobernanza tecnológica institucional. Esta relación busca garantizar que los procesos, recursos y servicios tecnológicos operen bajo principios de mejora continua, control de riesgos, cumplimiento normativo y eficiencia operativa, permitiendo demostrar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) mediante la aplicación sistemática de las prácticas ITIL como marco operativo de soporte, control y evidencia de conformidad.

4. ALCANCE

Aplica a los procesos, servicios y funciones tecnológicas bajo el marco del SGSI institucional, incluyendo niveles estratégicos, tácticos y operativos.

5. CORRELACIÓN ESTRATÉGICA – VALOR DE LA INTEGRACIÓN

Tabla 1 Correlación Estratégica

Dimensión	Rol de ITIL 4	Requisito ISO/IEC 27001:2022 soportado	Resultado táctico
Gobernanza	Define prácticas estandarizadas de gestión y mejora	Cláusulas 4 y 5 (Contexto y Liderazgo)	Cohesión entre TI y objetivos institucionales
Riesgo y planificación	Identifica, evalúa y mitiga riesgos operativos	Cláusula 6 (Planificación)	SGSI adaptado al entorno operativo
Soporte y operación	Estructura procesos de gestión diaria de servicios	Cláusula 8 (Operación)	Procesos reproducibles y auditables

Dimensión	Rol de ITIL 4	Requisito ISO/IEC 27001:2022 soportado	Resultado táctico
Evaluación del desempeño	Proporciona métricas, indicadores y registros	Cláusula 9 (Evaluación del desempeño)	Evidencia verificable para auditorías
Mejora continua	Implementa mecanismos de revisión y optimización	Cláusula 10 (Mejora)	Retroalimentación permanente y madurez creciente
Seguridad y control técnico	Alinea controles A.5 a A.9 mediante prácticas TI	Anexo A (Controles)	Cumplimiento técnico y operativo sustentado

6. PRACTICAS Vr. ISO/IEC: 27001:2022

E → *Ejecutor (responsable directo de la operación o implementación de la práctica)*
T → *Táctico (responsable de coordinar, supervisar o garantizar cumplimiento de la práctica)*
O → *Operativo/Observador (Apoya o recibe los resultados; responsable del aseguramiento o verificación del cumplimiento)*

Tabla 2 Practicas Vr. Controles

N°	Nombre práctica	Controles ISO/IEC 27001:2022	Descripción Practica	Responsables	Responsabilidad por rol	Evidencias Esperadas	Descripción Técnica	Frecuencia
1	Gestión de la mejora continua	A.10.1, A.9.2	Establece un enfoque sistemático para revisar y optimizar continuamente los procesos, servicios. Identificar brechas, evaluar el rendimiento y proponer mejoras que aseguren la satisfacción de las partes interesadas.	**E:** Gestor de la mejora continua. **T**: Coordinador de calidad TI. **O:** Gestor de la mejora continua.	**E:** Documentar e implementar planes de mejora continua. **T:** Supervisar el ciclo de mejora (PDCA) del SGSI. **O:** Validar el cumplimiento de los planes de mejora.	Registros de no conformidades. Planes de acción. Informes de revisión de los planes de mejora continua.	Ciclo de vida de mejora continua (identificación, planificación, ejecución, revisión).	Periódica Semestral y Post-incidente o auditoría.

N°	Nombre práctica	Controles ISO/IEC 27001:2022	Descripción Practica	Responsables	Responsabilidad por rol	Evidencias Esperadas	Descripción Técnica	Frecuencia
2	Gestión del conocimiento	A.7.2, A.8.2	Garantiza la creación, preservación y difusión del conocimiento crítico para la operación segura y eficiente de los servicios TI. Evita la pérdida de información clave y fomenta la mejora continua basada en la experiencia institucional.	**E:** Gestor del conocimiento. **T:** Gestor del conocimiento, Oficial de seguridad de la información o Informática y especialistas seguridad perimetral. **O:** Oficial de Seguridad de la información o Informática.	**E:** Capturar, clasificar y mantener actualizada la base de conocimiento (KEDB). **T:** Definir la política de gestión del conocimiento del SGSI y alimentar la base de conocimiento. **O:** Verificar la accesibilidad y pertinencia de la información.	Base de conocimiento (KEDB). Procedimientos Manuales técnicos y de seguridad. Lecciones aprendidas.	Repositorio centralizado de documentación operativa y de seguridad.	Continua y en cada cierre de incidente o proyecto relacionado con seguridad de la información.
3	Gestión de activos de TI	A.5.9, A.5.10, A.8.1	Asegura que todos los activos tecnológicos sean identificados, inventariados, valorados y gestionados durante todo su ciclo de vida.	**E:** Gestor de activos de TI. **T:** Líder de infraestructura. **O:** Oficial de seguridad de la información o Informática.	**E:** Mantener actualizado el inventario de activos de TI y de información. **T:** Establecer la clasificación, etiquetado y gestión del ciclo de vida de los	Inventario de activos de hardware y software. Registro de clasificación. Valoración de la información	Mantenimiento y control de un inventario completo de activos de TI y de información, asignación de propietario y valoración de la criticidad y clasificación de la información que contienen.	Continua (para cambios), y verificación anual.

N°	Nombre práctica	Controles ISO/IEC 27001:2022	Descripción Practica	Responsables	Responsabilidad por rol	Evidencias Esperadas	Descripción Técnica	Frecuencia
					activos. **O:** Auditar el inventario y la valoración de los activos de información.	(activo de información).		
4	Gestión de la continuidad del servicio	A.5.29, A.5.30	Garantiza la disponibilidad y recuperación de los servicios de TI ante incidentes o desastres. Define estrategias de continuidad, planes de contingencia y pruebas periódicas que aseguren la resiliencia organizacional.	**E:** Gestor de continuidad del servicio. **T:** Comité de crisis. **O:** Oficial de Seguridad de la información o Informática.	**E:** Desarrollar, mantener y probar los planes de continuidad y recuperación. **T:** Autorizar la activación del plan de continuidad en caso de desastre. **O:** Evaluar la efectividad de los planes y el impacto de las pruebas.	Plan de Continuidad de Negocio (BCP). Plan de Recuperación ante Desastres (DRP). Informes de pruebas de continuidad.	Proceso de gestión de la resiliencia operativa y la recuperación de la infraestructura y servicios. pruebas de continuidad.	Anual (prueba completa) y semestral (pruebas de componentes).

N°	Nombre práctica	Controles ISO/IEC 27001:2022	Descripción Practica	Responsables	Responsabilidad por rol	Evidencias Esperadas	Descripción Técnica	Frecuencia
5	Gestión de problemas	A.8.16, A.8.23	Busca identificar las causas raíz de incidentes y prevenir su recurrencia. Permite mantener la estabilidad operativa del entorno tecnológico y minimizar el impacto de fallas recurrentes.	**E:** Gestor de problemas. **T:** Líder de infraestructura. **O:** Oficial de Seguridad de la información o Informática.	**E:** Realizar el análisis de la causa raíz de los problemas (RCA). **T:** Priorizar la resolución de problemas y asegurar la implementación de soluciones (workarounds/soluciones permanentes). **O:** Revisar los problemas críticos y su impacto en la seguridad.	Registro de problemas. Informes de Análisis de Causa Raíz (RCA). Soluciones y errores conocidos.	Gestión proactiva de fallas recurrentes para eliminar la causa raíz y mejorar la estabilidad del servicio.	Continuo y tras incidentes recurrentes de seguridad de la información.
6	Gestión del nivel de servicio	A.5.28, A.9.1	Establece, monitorea y revisa los acuerdos de nivel de servicio (SLA) para garantizar que los servicios TI cumplan los compromisos de disponibilidad, capacidad y seguridad establecidos.	**E:** Coordinador de calidad de TI. **T:** Líder de infraestructura. **O:** Gestor de nivel de servicio.	**E:** Monitorear el rendimiento contra los SLAs y reportar desviaciones. **T:** Negociar, documentar y revisar los SLAs con los clientes.	Anexo técnico con la definición de los acuerdos de Nivel de Servicio (SLAs). Informes de rendimiento de SLAs.	Medición, monitoreo y gestión del cumplimiento de los acuerdos de calidad y seguridad del servicio.	Mensual para monitoreo de SLAs.

N°	Nombre práctica	Controles ISO/IEC 27001:2022	Descripción Practica	Responsables	Responsabilidad por rol	Evidencias Esperadas	Descripción Técnica	Frecuencia
					O: Auditar el cumplimiento de los compromisos de seguridad en los SLAs.			
7	Gestión de la disponibilidad	A.5.29, A.8.16	Asegura que los servicios de TI estén disponibles según los objetivos acordados, mediante monitoreo proactivo, redundancia, mantenimiento planificado y gestión de riesgos operativos.	**E:** Ingeniero de infraestructura o administrador de sistemas/redes. **T:** Gestor de disponibilidad. **O:** Comité de TI, Oficial de Seguridad de la información o Informática.	**E:** Implementar controles de redundancia, monitoreo y respaldo. **T:** Desarrollar el plan de disponibilidad y asegurar el cumplimiento de los tiempos de actividad. **O:** Auditar los mecanismos de disponibilidad y los tiempos de inactividad.	Informes de disponibilidad de servicios. Plan de Disponibilidad. Registros de pruebas de fallas.	Planificación, diseño e implementación de la infraestructura para garantizar el acceso ininterrumpido a la información.	Continua (monitoreo) y mensual (informes).
8	Gestión de la capacidad y el rendimiento	A.5.29, A.8.13	Administra los recursos tecnológicos y la planificación de la capacidad para garantizar un rendimiento óptimo	**E:** Ingeniero de sistemas, redes o infraestructura. **T:** Gestor de capacidad.	**E:** Monitorear el consumo de capacidad y hacer	Informes de uso de capacidad. Plan de Capacidad, proyecciones de crecimiento.	Aseguramiento de que los recursos de TI son suficientes para cumplir los requisitos de rendimiento y disponibilidad.	Mensual (monitoreo) y semestral (planificación).

N°	Nombre práctica	Controles ISO/IEC 27001:2022	Descripción Practica	Responsables	Responsabilidad por rol	Evidencias Esperadas	Descripción Técnica	Frecuencia
			de los servicios sin comprometer la seguridad ni la disponibilidad	**O:** Comité de TI, Oficial de Seguridad de la información o Informática.	proyecciones. **T:** Desarrollar y mantener el Plan de Capacidad. **O:** Aprobar las inversiones de capacidad para mantener el nivel de servicio acordado.			
9	Mesa de Soluciones TIC	A.8.16, A.8.23	Actúa como punto único de contacto entre los usuarios y el área de TI. Atiende incidentes, solicitudes y consultas, asegurando trazabilidad, priorización y resolución conforme a los acuerdos de servicio.	**E:** Agente de Mesa de Soluciones TIC. **T:** Líder de mesa de servicio o gestor de servicios. **O:** Oficial de Seguridad de la información o Informática.	**E:** Registrar, clasificar y escalar incidentes y solicitudes de servicio. **T:** Supervisar el cumplimiento de los niveles de servicio y la calidad de la atención. **O:** Revisar el impacto de incidentes críticos de seguridad.	Registros de tickets (incidentes y solicitudes). Informes de cumplimiento de SLA de la Mesa de Servicio.	Punto de contacto centralizado para gestionar todas las interacciones de los usuarios con TI, incluyendo las de seguridad.	Quincenal (operación) y mensual (directivo).

N°	Nombre práctica	Controles ISO/IEC 27001:2022	Descripción Practica	Responsables	Responsabilidad por rol	Evidencias Esperadas	Descripción Técnica	Frecuencia
10	Gestión de incidentes	A.5.24, A.8.16, A.8.22	Gestiona los incidentes que afectan la operación normal de los servicios TI, asegurando su rápida restauración y el cumplimiento de los tiempos de respuesta definidos en los SLA.	**E:** Agente de Mesa de Mesa de Soluciones TIC/ Ingeniero especialistas de data center responsables técnicos de cada línea de servicio. **T:** Gestor de incidentes o líder de infraestructura **O:** Oficial de Seguridad, o Informática.	**E:** Detectar, registrar, diagnosticar y restaurar la operación del servicio. **T:** Coordinar la respuesta a incidentes mayores y asegurar la comunicación. **O:** Auditar el proceso de respuesta a incidentes de seguridad y los tiempos de resolución.	Registros detallados de incidentes. Informes de incidentes mayores. Análisis forense (si aplica).	Proceso para minimizar el impacto negativo de los incidentes restableciendo la operación normal tan pronto como sea posible	Continua (operación) y mensual (reporte).

N°	Nombre práctica	Controles ISO/IEC 27001:2022	Descripción Practica	Responsables	Responsabilidad por rol	Evidencias Esperadas	Descripción Técnica	Frecuencia
11	Gestión de solicitudes de servicio	A.8.16, A.8.23	Administra las solicitudes de los usuarios para servicios rutinarios y aprobados, garantizando un flujo controlado, documentado y trazable de atención.	**E:** Analista de soporte de primer nivel o técnico de TI. **T:** Líder de infraestructura o gestor de solicitudes. **O:** Oficial de Seguridad o Informática.	**E:** Procesar las solicitudes de servicio siguiendo los procedimientos establecidos. **T:** Asegurar la aprobación y el cumplimiento de los tiempos de entrega. **O:** Auditar el cumplimiento de los procedimientos de seguridad en la atención de solicitudes.	Registros de solicitudes de servicio. Flujos de trabajo de aprobación y cumplimiento.	Flujo de trabajo estandarizado para la entrega de servicios de bajo riesgo, como restablecimientos de contraseñas o provisión de acceso.	Quincenal (operación) y mensual (directivo).

N°	Nombre práctica	Controles ISO/IEC 27001:2022	Descripción Practica	Responsables	Responsabilidad por rol	Evidencias Esperadas	Descripción Técnica	Frecuencia
12	Habilitación del cambio	A.8.32, A.5.8	Controla los cambios en infraestructura, aplicaciones y servicios mediante un proceso formal de evaluación, autorización y comunicación para minimizar el riesgo de interrupciones o incidentes de seguridad.	**E:** Equipo técnico de data center y equipo de SI o responsable técnico del servicio. **T:** Gestor de cambios / Comité de Cambios (CAB). **O:** Oficial de Seguridad o Informática.	**E:** Registrar, clasificar y ejecutar los cambios autorizados. **T:** Evaluar el impacto de los cambios, especialmente en seguridad, y autorizar su despliegue. **O:** Auditar el proceso de gestión de cambios y la mitigación de riesgos.	Registro de cambios (RFCs). Actas de reunión del CAB. Informes de éxito/falla de cambios.	Proceso formal de control para la introducción de nuevos elementos o modificaciones a la línea base de los servicios.	Continua (operación) y semanal/quincenal (reuniones CAB).

N°	Nombre práctica	Controles ISO/IEC 27001:2022	Descripción Practica	Responsables	Responsabilidad por rol	Evidencias Esperadas	Descripción Técnica	Frecuencia
13	Gestión de la seguridad de la información	A.5, A.8, A.9	Implementa controles técnicos para proteger la infraestructura, redes, aplicaciones y datos frente a amenazas internas y externas. Garantiza la aplicación de mecanismos de cifrado, autenticación, monitoreo y respuesta ante incidentes.	**E:** Oficial de Seguridad Informática o administradores de seguridad perimetral. **T:** Oficial de Seguridad de la Información o informatica. **O:** Oficial de seguridad de la información o Informática, Alta Dirección.	**E:** Operar y mantener los sistemas de seguridad (firewalls, IDS, SIEM). **T:** Definir las políticas, estándares y controles de seguridad. **O:** Supervisar la efectividad de los controles y su alineación con los objetivos de la organización.	Políticas y estándares de seguridad. Informes de monitoreo de seguridad (SIEM). Registros de gestión de vulnerabilidades.	Aplicación de la estrategia de seguridad mediante la operación de controles, monitoreo y mitigación de amenazas.	Quincenal (operación) y mensual (directivo).

N°	Nombre práctica	Controles ISO/IEC 27001:2022	Descripción Practica	Responsables	Responsabilidad por rol	Evidencias Esperadas	Descripción Técnica	Frecuencia
14	Gestión de monitoreo y eventos	Cláusula 10 A.5.17, A.5.28, A.5.34, A.8.7, A.8.16, A.8.7, A.8.9 y A.8.16	Observa los servicios para identificar y registrar eventos de interés, así como los incidentes y cambios.	**E:** seguridad perimetral y conectividad. **T:** Gestor de monitoreo y eventos, Gestor de incidentes, Gestor de seguridad de la información. **O:** Gestor de monitoreo y eventos y Oficial seguridad de la información o Informática.	**E:** Configurar y operar las herramientas de monitoreo (registros, eventos, seguridad). **T:** Definir umbrales y escalamiento de eventos. **O:** Revisar los eventos críticos de seguridad y el rendimiento del monitoreo.	Registros de eventos, alertas automáticas. Informes de *uptime* y seguridad.	Detección de estados anormales o cambios en la operación de un servicio, sirviendo de base para la gestión de incidentes.	Continua (operación) y semanal (revisión de alertas).

Aprobado por: Milena del Pilar Sandoval Gómez
Jefe Oficina de Tecnologías de la Información y las Comunicaciones - OTIC

Elaborado: Juan Carlos Parra Moreno
Oficial Seguridad Informática – OTIC

Revisado: Henry Alexander Moyán Montenegro
Oficial Seguridad de la Información - OTIC

Revisado: Jasson Smith Castro
Profesional Especializado – OTIC

Revisado: Luz Dary Vargas
Profesional Especializado – OTIC

Revisado: César Ubaldo Báez
Profesional Especializado – OTIC

Revisado: Sandra Patricia Sánchez Ubaque
Contratista – OTIC