



INFORME DE AUDITORÍA INTERNA

CÓDIGO	04.0-F06
VERSIÓN	1.0
FECHA APROBACIÓN	29/11/2016

Nombre del cliente:	AGENCIA PRESIDENCIAL DE COOPERACIÓN INTERNACIONAL
Dirección del sitio evaluado	Avenida Calle 10 # 97ª 13, Bogotá D.C.
Fecha de evaluación:	17, 18 y 19 de diciembre
Objetivo:	Realizar la auditoría interna al Sistema de Gestión de Seguridad de la información y de esta manera obtener una revisión de los procesos que intervienen en el alcance del Sistema, evaluando el cumplimiento de los requisitos de la Norma ISO/IEC 27001:2022.
Alcance de la auditoria (en término de procesos, áreas o proyectos):	La Agencia Presidencial de Cooperación Internacional de Colombia, APC -Colombia, adopta el Sistema de Gestión de la Seguridad y Privacidad de la Información (SGSPI), en el Sistema de Gestión Integral (SGI), con aplicación a catorce (14) procesos institucionales
Nombre y cargo de los auditados en el SGC	Jaime Gallego Profesional Especializado Dirección de Demanda José Héctor Mina Profesional Especializado con funciones de coordinación GIT Tecnologías de la información Gestión de Tecnologías de la información Jesús David Contratista Gestión de Tecnologías de la información Erika Marcela Quiñones Contratista Gestión de Tecnologías de la información Willy Vijalba Profesional especializado Gestión de Tecnologías de la información Julio Ignacio Profesional especializado Direccionamiento Estratégico y Planeación María Angelica Orozco Técnica Evaluación Control y Mejora Jennifer Paola Sierra Profesional especializado Gestión Contractual Edna Lorena León Profesional Especializado con funciones de coordinación GIT Contractual Gestión Contractual Andrés Felipe Ríos Profesional Especializado Gestión de Comunicaciones Yvette Araujo Profesional Especializado con funciones de coordinación Talento Humano Gestión de Talento Humano Luis Miguel Cayón Técnico Gestión Contractual

	Ángela Luisa Vargas Profesional universitario Gestión de Talento Humano
Auditor:	Elsa Marlen Baracaldo Huertas (Auditora Líder) Francia Rodríguez
Norma de referencia (criterio):	ISO/IEC 27001:2022
Recursos:	Computadores, internet.
Metodología:	Auditoría Presencial y remota

FORTALEZAS DEL SISTEMA EVALUADO

1. La organización demuestra una conciencia y compromiso claros con la seguridad de la información, lo que se refleja en la implementación de políticas y procedimientos para proteger la información.
2. La organización ha implementado controles de seguridad para proteger la información, como firewalls, antivirus y sistemas de detección de intrusos.
3. El personal de la organización ha recibido capacitación sobre la seguridad de la información y es consciente de sus responsabilidades en la protección de la información.

OBSERVACIONES DEL SISTEMA EVALUADO (Aspectos a reforzar)

Se identifican oportunidades de mejora en el fortalecimiento de la aplicación y consistencia de los controles definidos, así como en el seguimiento y documentación de las actividades del sistema.

CUMPLIMIENTO REQUISITOS (ISO 27001-1:2022)

4.1 Comprensión de la organización y contexto	La organización cuenta con la planeación estratégica documentada, liderada por la Directora General y el área de Planeación General, con un período de vigencia aprobado para 2023–2026. Adicionalmente, en el documento E-OT-003, Versión 13, “Manual del Sistema de Gestión Integral”, específicamente en el ítem 11 – Contexto Estratégico, se describe el panorama actual del entorno de la Agencia, así como sus capacidades internas, evidenciándose la revisión y actualización del contexto estratégico de la APC Colombia. Para la definición del contexto estratégico, la APC Colombia utiliza la matriz FODA como metodología, la cual integra factores internos y externos con el fin de identificar y analizar los aspectos positivos (fortalezas y oportunidades) y negativos (debilidades y amenazas), permitiendo una comprensión integral del contexto organizacional.
4.2. Comprensión de las necesidades y expectativa de las partes interesadas	Se evidencia el documento AOT084, Versión 5, correspondiente a la caracterización de las partes

	interesadas y grupos de valor de la organización. En dicho documento se identifican las partes interesadas relevantes, clasificadas en los siguientes grupos de valor: entidades del orden nacional, proveedores (personas naturales y jurídicas), aliados estratégicos (agencias de cooperación internacional), sector privado (empresas y cámaras de comercio), comunidad (poblaciones negras y afrocolombianas), sociedad (sindicatos y veedurías), y partes internas (servidores públicos, contratistas y procesos, entre otros). Asimismo, se identifican los contactos y responsables a nivel interno asociados a cada grupo de partes interesadas, tales como funcionario designado, representante legal o individuo responsable, lo que permite una adecuada gestión de la comunicación y el relacionamiento. Esta identificación constituye un insumo relevante para la determinación de requisitos aplicables al Sistema de Gestión de Seguridad de la Información (SGSI), en coherencia con las necesidades y expectativas de las partes interesadas.
4.3 Determinación del alcance del sistema de gestión	Se recomienda revisar y actualizar la definición del alcance del Sistema de Gestión de la Seguridad de la Información (SGSI), incorporando de manera explícita las cuestiones internas y externas del contexto organizacional, así como los requisitos y expectativas de las partes interesadas, conforme a lo establecido en el numeral 4.3 de la Norma ISO/IEC 27001:2022. La integración de estos elementos permitirá: - Asegurar que el alcance del SGSI refleje de forma clara y completa el propósito y la dirección estratégica de la organización. - Reducir la ambigüedad en la aplicación de controles y fortalecer la trazabilidad en la gestión de riesgos. - Mejorar la eficacia del SGSI y su alineación con los objetivos estratégicos institucionales. - Facilitar la evidencia de cumplimiento normativo y la coherencia en auditorías futuras.
4.4 Sistema de Gestión de Servicios y sus procesos	La Organización cuenta con un responsable del SGPSI aunque no se encuentra en un área independiente de tecnología. Por lo cual se genera una NC para que fortalezcan la gobernanza de la seguridad de la información y aseguren un enfoque integral que involucre a toda la organización y no solo a los aspectos tecnológicos.

	INFORME DE AUDITORÍA INTERNA	CÓDIGO	04.0-F06
		VERSIÓN	1.0
		FECHA APROBACIÓN	29/11/2016

5.1 Liderazgo y compromiso	La organización demuestra que tienen iniciativas que otorga al área presupuesto y personal para el SGSI, las cuales son medidos en el objetivo del plan de acción.
5.2 Política del SGS	La organización cuenta con el documento de la política general el 13 enero de 2025 por medio del comité institucional de gestión y desempeño. Se da cubrimiento Los procesos institucionales, identificarán, valorarán y documentarán la criticidad de los activos de información de la Agencia, de acuerdo con los pilares de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad), conforme a los procedimientos, instrumentos y demás lineamientos del SGPSI. Los procesos institucionales, identificarán, evaluarán y darán tratamiento a los riesgos del activo de información de la Agencia y los controles asociados, conforme al mapa de riesgos de seguridad de la información, los procedimientos, guías, instrumentos y demás lineamientos del SGPSI.
5.3 Roles responsabilidades y autoridades en la organización.	La organización cuenta con una POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Código: A-OT-011 Versión: 15 Fecha: enero 13 de 2025 ROLES Y RESPONSABILIDADES DEL SGPSI por medio de la Matriz RACI, cuenta con un cuadro donde se tienen varios procesos con responsabilidades dentro del documento se encuentran roles y responsabilidades
6.1 Acciones para tratar los riesgos y oportunidades	La organización dispone de documentos y una matriz; sin embargo, los procesos de identificación, valoración y tratamiento de riesgos requieren fortalecerse con el fin de mejorar la planificación. En todos los numerales que aplican
6.2 Objetivos de seguridad de la información y planes para lograrlos.	Se evidencia en el Plan de Acción Institucional 2025 de la APC Colombia la definición de objetivos relacionados con el Sistema de Gestión de Seguridad de la Información (SGSI). En dicho plan se establece como objetivo estratégico producir información de calidad, oportuna y pertinente para apoyar la toma de decisiones en materia de cooperación internacional al desarrollo, objetivo que se encuentra alineado con los principios de la seguridad de la información. Asimismo, se identifica como objetivo del SGSI establecer los lineamientos que conduzcan a la preservación de la confidencialidad, integridad y disponibilidad de la información, mediante la definición de políticas, controles y procedimientos, la promoción de la cultura de privacidad

	y seguridad, y la gestión de los riesgos de seguridad de la información, con el fin de brindar confianza a las partes interesadas y grupos de valor, y contribuir al logro de los objetivos estratégicos de la APC Colombia. Para el seguimiento de estos objetivos, se definen indicadores de desempeño, tales como el número de iniciativas implementadas durante la vigencia conforme a la hoja de ruta del PETI, así como el fortalecimiento y mantenimiento de las capacidades de los servicios tecnológicos para la transformación digital (TIC), lo cual permite evaluar el avance y la eficacia de los objetivos de seguridad de la información y los planes establecidos para su cumplimiento.
6.3 Planificación de los cambios	Se evidencia la planificación de los cambios del Sistema de Gestión de Seguridad de la Información (SGSI) mediante el documento A-FO-277 – Planificación de los cambios del SGSI, en el cual se identifican y gestionan tanto los cambios propios del SGSI como los cambios relevantes del sistema que pueden impactar la seguridad de la información. Dicho documento establece un marco para asegurar que los cambios se realicen de manera planificada, controlada y coherente, considerando su impacto en la confidencialidad, integridad y disponibilidad de la información.
7.1 Recursos	Se adopta ha designado recurso de recurso humano, infraestructura proyecto de inversión de fortalecimiento institucional de APC Colombia BPIN 202400000000116 inscrito en el DNP está hasta el 2028 el valor de los recursos al sistema so
7.2 Competencia	Cuentan con resoluciones para la designación del talento humano y aplicación a los requisitos como también para los contratistas
7.3 Toma de conciencia	Cuentas con documentos apoyado con comunicaciones y diferentes canales para la sensibilización y compromiso de la dirección
7.4 Comunicación	Por parte del sistema envía las comunicaciones y los canales como correo electrónico, pantallas internas piezas diapositivas y externa mente se publica por la página WEB y existe una matriz comunicaciones E_PO.045 y se encuentra una matriz E- OT 037 versión 04 plan estratégico de las comunicaciones, redes sociales de la entidad esquema de publicaciones.

	INFORME DE AUDITORÍA INTERNA	CÓDIGO	04.0-F06
		VERSIÓN	1.0
		FECHA APROBACIÓN	29/11/2016

7.5 Información Documentada	Cuentan con el apoyo de calidad quien imparte los lineamientos para la creación, actualización y aprobación de los documentos
8.1 Planificación y control operacional	Cuenta con documentos
8.2 valoración de riesgos de la seguridad de la información	Se cuenta con documentación
8.3 tratamiento de riesgos de la seguridad de la información	Se cuenta con documentación
9.1 Seguimiento, medición, análisis y evaluación.	Cuenta con la plataforma brújula del sistema integrado de gestión donde se encuentran documento del manual de operación MANUAL DE OPERACIÓN DEL SGSPI
9.2 Auditoría interna	Cuentan con el grupo de control interno quien apoya con las auditorias interna y externas en los tiempos planeado
9.3 Revisión por la dirección	Se evidencia la RXD del 2025: Presentación del contexto NTC ISO 27001: 9.3 Revisión por la dirección. Revisión SGSPI: Acciones provenientes de previas revisiones por la dirección, Cambios en cuestiones externas e internas pertinentes al SGSPI, Cambios en las necesidades y expectativas de las partes interesadas, retroalimentación del SGSPI: No conformidades y acciones correctivas, Resultados de seguimiento y medición, Resultados de las auditorias, Cumplimiento de los objetivos de seguridad de la información, Retroalimentación de las partes interesadas, Resultados de la evaluación de riesgos y estado del plan de tratamiento, Oportunidades de mejora.
10.1 No conformidad y acción correctiva	adopta el Sistema de Gestión de la Seguridad y Privacidad de la Información (SGSPI), en el Sistema de Gestión Integral (SGI), con aplicación a catorce (14) procesos
10.2 Mejora continua.	Se realizan las acciones correctivas como lo dicta calidad
A.5 Controles organizacionales	Se definen políticas, roles, responsabilidades y lineamientos organizacionales para la gestión de la seguridad de la información, orientados a asegurar el cumplimiento de los objetivos del SGSI y el control adecuado de los riesgos.
A.6 Controles personas	Se estable lineamientos para la gestión de personas, incluyendo roles, responsabilidades, sensibilización y formación en seguridad de la información, con el fin de reducir riesgos asociados al factor humano.
A.7. Controles físicos	Se ha implementado controles de seguridad física y ambiental para proteger instalaciones, equipos y activos de información, con el fin de prevenir accesos no autorizados, daños o interrupciones en la operación.

	INFORME DE AUDITORÍA INTERNA	CÓDIGO	04.0-F06
		VERSIÓN	1.0
		FECHA APROBACIÓN	29/11/2016

A.8 Controles Tecnológicos	Se implementa controles tecnológicos orientados a la protección de los activos de información, incluyendo gestión de accesos, uso de tecnologías de seguridad y medidas de protección de los sistemas de información, con el fin de mitigar riesgos tecnológicos.
-----------------------------------	---

Nota: El detalle de cada numeral se encuentra consolidado en el documento 04.0-F06 Lista de Chequeo ISO 27001-2022

NO CONFORMIDADES

No.	Numeral norma	NC	OBS	Descripción
1	6.1.1	x		Aunque la organización cuenta con documentación relacionada con la gestión y planificación de riesgos, la planificación no se encuentra correctamente implementada ni alineada con los requisitos del numeral 6.1. Durante la auditoría no se evidenció una identificación, análisis, evaluación y tratamiento de riesgos efectiva y consistente, ni su integración con los controles establecidos en distintos numerales del sistema de gestión. Adicionalmente, no se demostró la trazabilidad entre los riesgos identificados, los controles definidos y su aplicación real, lo que derivó en incumplimientos evidenciados en varios numerales relacionados con la gestión de la seguridad de la información. La falta de evidencia objetiva indica que la planificación de riesgos es parcial y no asegura el logro de los resultados previstos del sistema.
2	8.1	X		Durante la auditoría no se evidenció una planificación efectiva que permita asegurar la implementación de los controles definidos para los procesos, productos o servicios contratados externamente. Si bien la organización cuenta con documentación relacionada con proveedores y servicios externos, no se encontraron criterios claramente establecidos para la evaluación, selección, control y seguimiento de dichos procesos, productos o servicios. Asimismo, no se evidenció la aplicación de controles documentados ni registros que demuestren su implementación y seguimiento, lo que impide asegurar que los servicios externos cumplen con los requisitos

				definidos por la organización y con los objetivos del sistema de gestión.
3	8.3	X		Se evidencia que la organización cuenta con un plan de tratamiento de riesgos de seguridad de la información; sin embargo, no dispone de información documentada que evidencie los resultados del tratamiento de dichos riesgos, incumpliendo lo establecido en el numeral 8.3 de la norma ISO/IEC 27001. No se cuenta con información documentada de los resultados del tratamiento de los riesgos de seguridad de la información, en incumplimiento del numeral 8.3 de la norma ISO/IEC 27001.
4	A 5.30	X		Aunque la organización cuenta con un documento denominado “Estrategia de Continuidad del Negocio”, no se evidencia que dicho documento incluya un Plan de Continuidad del Negocio ni el Análisis de Impacto al Negocio (BIA). Además, no se ha demostrado que el alcance de la continuidad cubra todos los procesos críticos, ni se cuenta con evidencia de la realización de pruebas o simulacros para validar la continuidad del negocio. Esto incumple los requisitos del control 5.29 de la norma ISO/IEC 27001, que exige asegurar la seguridad de la información durante interrupciones mediante un Plan de Continuidad del Negocio documentado, con BIA y pruebas periódicas.
5	A 8.14	x		Se evidencia que la organización dispone únicamente de copias de seguridad (backup) como medida de protección, pero no se cuenta con evidencia de que la infraestructura on-premises cuente con mecanismos de redundancia que aseguren la disponibilidad continua de los sistemas críticos. Esta situación representa un incumplimiento de los requisitos para garantizar la continuidad y disponibilidad de la información, conforme a los controles aplicables de la norma ISO/IEC 27001.
6	A.8.17	X		Durante la auditoría se evidenció que el reloj del sistema de CCTV se encuentra desactualizado, presentando un desfase de 15 minutos respecto a la hora real (evidencia: hora actual 14:53; hora registrada en el sistema 14:38). Esta situación no es conforme con el control A.8.17 – Sincronización de relojes de la Norma ISO/IEC

				27001:2022, el cual establece que “los relojes de los sistemas de procesamiento de información utilizados por la organización deben sincronizarse con fuentes de tiempo aprobadas”. La falta de sincronización del reloj del sistema de CCTV puede afectar la integridad y confiabilidad de los registros de eventos, dificultar el análisis forense, la correlación de incidentes de seguridad de la información y el soporte a investigaciones internas o requerimientos legales.
7	A 8.17		X	Implementar y mantener mecanismos de sincronización automática de los relojes del sistema de CCTV (desfase de 15 min) con fuentes de tiempo aprobadas, conforme al control A.8.17 de la Norma ISO/IEC 27001:2022. La implementación de esta mejora permitirá: - Garantizar la integridad y confiabilidad de los registros de eventos generados por el sistema de CCTV. - Facilitar el análisis forense y la correlación precisa de incidentes de seguridad de la información. - Asegurar la disponibilidad de evidencia válida para investigaciones internas y requerimientos legales. - Reducir riesgos asociados a desfases de tiempo que puedan afectar la trazabilidad de los registros. - Fortalecer el cumplimiento normativo y la eficacia del SGSI en auditorías internas y externas.
8	5.3		X	Rol del Oficial de Seguridad / Responsable del MSPI – Resolución 02277 de 2025 Se identifica la oportunidad de formalizar y fortalecer el rol del responsable del MSPI, garantizando su independencia funcional dentro de la estructura organizacional. Actualmente, dicho rol se encuentra adscrito al área de Planeación, lo cual resulta adecuado desde el enfoque estratégico y de gobierno institucional, al permitir una visión transversal y alineada con los objetivos misionales de la entidad. No obstante, se recomienda reforzar la segregación de funciones, asegurando que el responsable del MSPI/SGSI no asuma responsabilidades operativas sobre la infraestructura tecnológica, ni participe en la administración directa de plataformas, redes, sistemas de información o usuarios con privilegios administrativos, con el fin de evitar posibles conflictos de interés y fortalecer los

				controles internos asociados a la seguridad y privacidad de la información. Así mismo, se sugiere formalizar el rol mediante acto administrativo, en caso de que no se encuentre explícitamente definido, estableciendo de manera clara sus funciones, responsabilidades y nivel de autoridad. Lo anterior incluye su participación con voz y voto en el Comité Institucional de Gestión y Desempeño, y con voz en el Comité de Control Interno, garantizando su intervención efectiva en la toma de decisiones relacionadas con el MSPI. Estas acciones contribuyen al fortalecimiento del modelo de seguridad y privacidad de la información, al cumplimiento de la Resolución 02277 de 2025, y a la alineación con buenas prácticas de control interno, gobierno de TI y estándares como ISO/IEC 27001, particularmente en lo relacionado con independencia, supervisión y gestión del riesgo.
9	6.1.3		X	Si bien la organización cuenta con una matriz de riesgos diligenciada, durante la auditoría no se evidenció la existencia ni la implementación de un plan de tratamiento de riesgos que permita gestionar adecuadamente los riesgos identificados. Asimismo, no se presentó evidencia de la realización de actividades de monitoreo y seguimiento a dichos riesgos, lo cual impide verificar la eficacia de los controles definidos. Adicionalmente, no se evidenció la aceptación formal del plan de tratamiento de riesgos ni de los riesgos residuales por parte de la autoridad correspondiente, lo que incumple el requisito de aprobación y toma de decisiones informadas sobre el nivel de riesgo aceptable para la organización. En relación con la Declaración de Aplicabilidad (SOA), se identificó que las justificaciones consignadas no guardan coherencia con los controles seleccionados, y en algunos casos no se evidencia la relación entre la implementación del control, su justificación y el riesgo tratado. Esta situación afecta la trazabilidad entre los riesgos identificados, los controles definidos y su aplicación real en el sistema de gestión.
10	A.5.13		X	Ampliar y consolidar la política “Políticas Específicas del Sistema de Gestión de Seguridad y Privacidad de la Información” (código A-OT-100, versión 05), así como su

				implementación en la herramienta HERMES, de manera que se logre una cobertura integral de los criterios de etiquetado y clasificación para la totalidad de la información y activos de la entidad. La implementación de esta mejora permitirá: - Definir de forma clara y homogénea los criterios de clasificación aplicables a todos los activos de información. - Reducir la ambigüedad en la aplicación de categorías y fortalecer la trazabilidad documental. - Garantizar que la clasificación de la información esté alineada con el nivel de sensibilidad y criticidad de cada activo.
11	A 5.17		X	Implementar mecanismos de autenticación de doble factor (MFA) en los servicios de intranet y sistemas internos de la organización, complementando el uso de credenciales básicas con un segundo nivel de verificación. La implementación de esta mejora permitirá: - Fortalecer los controles de acceso lógico definidos en el SGSI. - Reducir el riesgo de accesos no autorizados derivados de credenciales comprometidas. - Incrementar la confianza en la protección de los activos de información críticos. - Alinear la gestión de accesos con las buenas prácticas internacionales de seguridad de la información. - Facilitar la evidencia de cumplimiento normativo y la madurez del sistema de gestión en auditorías futuras. De esta manera, el hallazgo se convierte en una oportunidad para robustecer la seguridad de los sistemas internos, garantizando mayor protección y trazabilidad en el control de accesos. ¿Quieres que te prepare también un ejemplo de plan de implementación de MFA que pueda servir como guía práctica para la organización?
12	A 5.31		X	En esta auditoria se encontró que dentro de la documentación del Sistema de Gestión de Seguridad de la Información no se evidencia un documento que consolide la normatividad aplicable a la gestión y operación de la entidad, ni la actualización de las normas relacionadas con el SGSI. La ausencia de este insumo limita la identificación clara de los requisitos legales, reglamentarios y normativos vigentes que deben ser considerados en la implementación y operación del sistema

				La falta de un documento que identifique y mantenga actualizada la normatividad aplicable puede generar debilidades en el cumplimiento normativo y afectar la adecuada gestión del SGSI.
13	A 8.2		X	Diseñar y mantener una matriz formal que consolide y describa los derechos de acceso a la información y a la infraestructura tecnológica, incluyendo de manera clara los accesos privilegiados (como cuentas de administrador y accesos a sistemas críticos). La implementación de esta mejora permitirá: - Incrementar la trazabilidad y el control integral de los permisos otorgados. - Diferenciar y gestionar de forma adecuada los accesos privilegiados frente a los accesos estándar. - Fortalecer la gobernanza de la seguridad de la información mediante criterios homogéneos y documentados. - Facilitar la verificación del cumplimiento normativo y la evidencia objetiva en auditorías internas y externas.

OPORTUNIDADES DE MEJORA

No.	Numeral norma	NC	OM	Descripción
1	4.4		X	Organizar un área formalmente responsable del Sistema de Gestión de Seguridad de la Información (SGSI), independiente del área de tecnología, fortalece la gobernanza de la seguridad de la información y asegura un enfoque integral que involucre a toda la organización y no solo a los aspectos tecnológicos.
2	A5.5		X	El definir y documentar claramente el responsable de contactar a las autoridades competentes en una situación de emergencia es fundamental para garantizar una respuesta oportuna, coordinada y eficaz ante incidentes que puedan afectar la seguridad de la información y la continuidad del negocio.
3	6.1.2		X	Si bien la organización cuenta con documentación y una matriz de riesgos en las que se establece la identificación y valoración de riesgos, no se evidenció la trazabilidad entre los riesgos identificados, su valoración y los controles implementados. Durante la auditoría se identificaron inconsistencias entre la valoración asignada y los riesgos reales asociados a los procesos y activos, lo

				que demuestra que la metodología de evaluación de riesgos no se aplica de manera efectiva. Adicionalmente, la valoración de riesgos documentada no se encuentra alineada con la realidad operativa ni con los incumplimientos evidenciados en diversos numerales, lo que impide asegurar que la planificación de riesgos permita prevenir o mitigar adecuadamente los impactos sobre el sistema de gestión.
4	4.3		x	Revisar y actualizar la definición del alcance del Sistema de Gestión de la Seguridad de la Información (SGSI), incorporando de manera explícita las cuestiones internas y externas del contexto organizacional, así como los requisitos y expectativas de las partes interesadas, conforme a lo establecido en el numeral 4.3 de la Norma ISO/IEC 27001:2022. La integración de estos elementos permitirá: - Asegurar que el alcance del SGSI refleje de forma clara y completa el propósito y la dirección estratégica de la organización. - Reducir la ambigüedad en la aplicación de controles y fortalecer la trazabilidad en la gestión de riesgos. - Mejorar la eficacia del SGSI y su alineación con los objetivos estratégicos institucionales. - Facilitar la evidencia de cumplimiento normativo y la coherencia en auditorías futuras.
5	8.2		X	fortalecer el proceso de gestión de riesgos de seguridad de la información mediante la conservación de información documentada de los resultados de las evaluaciones realizadas ante cambios significativos, conforme a lo establecido en el numeral 8.2 de la Norma ISO/IEC 27001:2022. La implementación de esta mejora permitirá: - Evidenciar de manera objetiva la trazabilidad de las evaluaciones de riesgos realizadas. - Facilitar la verificación del cumplimiento normativo durante auditorías internas y externas. - Asegurar la disponibilidad de registros que respalden la toma de decisiones y la aplicación de controles. - Incrementar la eficacia del SGSI al contar con información histórica que apoye la gestión de riesgos y la mejora continua.

6	10.2		X	Establecer un mecanismo formal y documentado para la gestión de las acciones correctivas y oportunidades de mejora (ACOM) derivadas de auditorías internas y externas, asegurando su análisis, planificación, implementación, seguimiento y verificación de eficacia. La implementación de esta mejora permitirá: - Garantizar la trazabilidad y evidencia objetiva de la atención a hallazgos de auditoría. - Prevenir la reincidencia de no conformidades mediante un proceso estructurado de corrección y verificación. - Fortalecer la madurez del sistema de gestión y su alineación con el principio de mejora continua. - Asegurar la eficacia del SGSI al dar tratamiento oportuno a desviaciones previamente identificadas. - Facilitar la demostración de cumplimiento normativo y la confianza en la gestión durante auditorías futuras.
7	A.5.9		X	Revisar y actualizar el inventario de activos de información, asegurando que la clasificación de cada activo se realice conforme a los lineamientos definidos por la entidad y en coherencia con su uso real e impacto. La implementación de esta mejora permitirá: - Garantizar la correcta identificación del nivel de protección requerido para cada activo. - Evitar inconsistencias entre el tipo de activo y la clasificación asignada. - Eliminar clasificaciones genéricas o desactualizadas que dificultan la gestión de riesgos. - Aplicar de manera homogénea los criterios de clasificación definidos, fortaleciendo la trazabilidad y la confiabilidad del inventario. - Diferenciar adecuadamente los activos relevantes de aquellos de menor impacto, optimizando la asignación de controles de seguridad.
8	A.5.36		X	Revisar, establecer y documentar un procedimiento formal para la realización de revisiones periódicas al cumplimiento de la Política de Seguridad de la Información, las políticas específicas, las reglas y los estándares definidos por la organización. La implementación de esta mejora permitirá: - Contar con evidencia objetiva (actas, informes, matrices o registros) que respalde la ejecución y seguimiento de dichas previsiones. - Definir responsables y frecuencias claras para asegurar la continuidad y trazabilidad del control.

	INFORME DE AUDITORÍA INTERNA	CÓDIGO	04.0-F06
		VERSIÓN	1.0
		FECHA APROBACIÓN	29/11/2016

				- Fortalecer la gobernanza de la seguridad de la información y la alineación con los requisitos de la Norma ISO/IEC 27001:2022. - Incrementar la eficacia del SGSI al garantizar que las políticas y estándares se mantengan actualizados y aplicados de manera consistente. - Facilitar la verificación del cumplimiento normativo durante auditorías internas y externas.
--	--	--	--	---

CONCLUSIONES:

Conveniente:

La implementación del Sistema de Gestión de Seguridad de la Información en la organización resulta conveniente y pertinente, dado que permite establecer un marco para la protección de la información y el cumplimiento de los requisitos normativos aplicables. No obstante, los hallazgos identificados evidencian la necesidad de fortalecer algunos controles para mejorar el nivel de madurez del sistema.

Adecuado:

El diseño y la estructura del SGSI se consideran adecuados en términos generales, en cuanto a la definición de políticas, procedimientos y responsabilidades. Sin embargo, la presencia de no conformidades y observaciones refleja brechas en la documentación, implementación y seguimiento de ciertos procesos, lo que requiere la ejecución de acciones correctivas y de mejora.

Eficaz:

El SGSI presenta un nivel de eficacia parcial, debido a que si bien se han implementado controles orientados a la seguridad de la información, no en todos los casos se cuenta con evidencia suficiente que demuestre su correcta ejecución y evaluación. En consecuencia, se hace necesario atender las no conformidades, así como implementar las observaciones y oportunidades de mejora, para asegurar el cumplimiento de los objetivos del sistema.

De lo anterior, se resume el total de hallazgos encontrados para la auditoría realizada:

HALLAZGOS DE LA AUDITORIA	TOTAL
Fortalezas	3
Oportunidades de Mejora	8
No conformidades	6

FIN DEL DOCUMENTO