Somos **calidad**,
somos **competitividad**,
somos **confianza**.

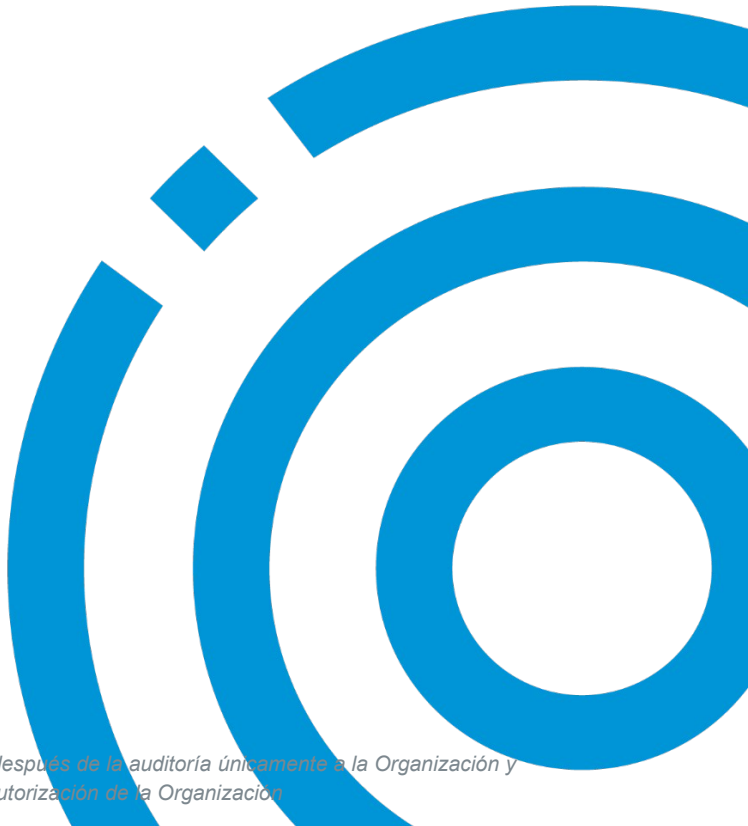
icontec

icontec

Huella de confianza.

icontec.org

INFORME DE AUDITORÍA DE SISTEMAS DE GESTIÓN



1. INFORMACIÓN GENERAL

1.1. ORGANIZACIÓN

INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR

1.2. SITIO WEB: www.icbf.gov.co

1.3 LOCALIZACIÓN DEL SITIO PERMANENTE PRINCIPAL:

ISO/IEC 27001:2022: Sede Nacional Avenida Carrera 68 No 64C 75 Bogotá D.C., Cundinamarca, Colombia

ISO/IEC 27001:2022 - SI-2002812

#Sitios permanentes adicionales	Número de certificado	Sedes y direcciones de los sitios permanentes	Localización (Ciudad-País)	Actividades del alcance del sistema de gestión, desarrollados en este sitio
1	SI-2002812	Sede Nacional Avenida Carrera 68 No 64C 75	Bogotá D.C., Cundinamarca, Colombia	Prestación de servicios orientados a la protección integral de los derechos de los niños, niñas, adolescentes y sus familias, en el marco de los programas misionales de la Entidad

1.3.1 LOCALIZACIÓN OTROS SITIO PERMANENTES:

1.4. ALCANCE DE LA CERTIFICACIÓN:

ISO/IEC 27001:2022 - SI-2002812

El sistema de gestión de seguridad de la información (SGSI) del Instituto Colombiano de Bienestar Familiar (ICBF) comprende la evaluación del diseño, implementación, mantenimiento y mejora continua de los controles de seguridad de la información aplicados a los procesos relacionados con la prestación de servicios orientados a la protección integral de los derechos de los niños, niñas, adolescentes y sus familias, en el marco de los programas misionales de la Entidad. Asimismo, el alcance incluye la verificación de las actividades de gestión de seguridad de la información asociadas a las Tecnologías de Información y Comunicaciones (TIC), con el fin de Propender por la confidencialidad, integridad y disponibilidad de la información. Declaración de Aplicabilidad A3.MS.DE, Versión 14 aprobada 2025-03-21
The information security management system (ISMS) of the Colombian Family Welfare Institute (ICBF) includes the evaluation of the design, implementation, maintenance, and continuous improvement of information security controls applied to processes related to the provision of services aimed at the comprehensive protection of the rights of children, adolescents, and their families, within the framework of the entity's mission programs. Likewise, the scope includes the verification of information security management activities associated with Information and Communication Technologies (ICT), in order to promote the confidentiality, integrity, and availability of information. Statement of Applicability A3.MS.DE, Versión 14 dated 2025-03-21

1.5. CÓDIGO IAF: , SI 4 ,SI 5

1.6. REQUISITOS DE SISTEMA DE GESTIÓN: ISO/IEC 27001:2022

1.7. REPRESENTANTE DE LA ORGANIZACIÓN:

Nombre:	MILTON FABIAN FORERO MELO
Cargo:	DIRECTOR DE PLANEACIACIÓN Y CONTROL DE GESTIÓN
Correo electrónico:	Milton.Forero@icbf.gov.co

1.8. TIPO DE AUDITORÍA: **Otorgamiento**

Es organización multisitio:	No
Auditoría Integral: No, Auditoría Combinada: No	X

1.9. Tiempo de auditoría	Fecha	Días de auditoría
Etapa 1 (Si aplica)	2025-10-21	1
Preparación de la auditoría y elaboración del plan	2025-10-22	1
Auditoria remota	N/A	0
Auditoria en sitio	2025-10-23	9.5

1.10. EQUIPO AUDITOR

Auditor líder	OSCAR FERNANDO RAMOS BENAVIDES Coordinador Lider ISO/IEC 27001:2022
Auditor	LIBARDO CHAVEZ ISO/IEC 27001:2022 JHOAN DAVID CORAL MEJIA ISO/IEC 27001:2022
Experto Técnico	N/A
Observador	N/A

1.11. DATOS DEL CERTIFICADO DE SISTEMA DE GESTIÓN

Código asignado por ICONTEC	SI-2002812
Fecha de aprobación inicial	N/A
Fecha de próximo vencimiento:	2028-12-23

2. OBJETIVOS DE LA AUDITORÍA

2.1. Determinar la conformidad del sistema de gestión con los requisitos de la norma de sistema de gestión.

2.2. Determinar la capacidad del sistema de gestión para asegurar que la Organización cumple los requisitos legales, reglamentarios y contractuales aplicables en el alcance del sistema de gestión y a la norma de requisitos de gestión

2.3. Determinar la eficacia del sistema de gestión para asegurar que la Organización puede tener expectativas razonables con relación al cumplimiento de los objetivos especificados.
2.4. Identificar áreas de mejora potencial del sistema de gestión.

3. ACTIVIDADES DESARROLLADAS

3.1. Los criterios de la auditoría incluyen la norma de requisitos de sistema de gestión, la información documentada del sistema de gestión establecida por la organización para cumplir los requisitos de la norma, otros requisitos aplicables que la organización suscriba y documentos de origen externo aplicables.
3.2. El alcance de la auditoría, las unidades organizacionales o procesos auditados se relacionan en el plan de auditoría, que hace parte de este informe.
3.3. La auditoría se realizó por toma de muestra de evidencias de las actividades y resultados de la Organización y por ello tiene asociada la incertidumbre, por no ser posible verificar toda la información documentada.
3.4. Se verificó la capacidad de cumplimiento de los requisitos legales o reglamentarios aplicables en el alcance del sistema de gestión, establecidos mediante su identificación, la planificación de su cumplimiento, la implementación y la verificación por parte de la Organización de su cumplimiento.
3.5. El equipo auditor manejó la información suministrada por la Organización en forma confidencial y la retornó a la Organización, en forma física o eliminó la entregada en otro medio, solicitada antes y durante el proceso de auditoría.
3.6. Al haberse ejecutado la auditoría de acuerdo con lo establecido en el plan de auditoría, se cumplieron los objetivos de ésta.

3.7..¿Se evidenciaron las acciones tomadas por la Organización para solucionar las áreas de preocupación, reportadas en el informe de la Etapa 1?
Si

3.8..Si se aplicó toma de muestra de múltiples sitios.

No

3.9..¿En el caso del Sistema de Gestión auditado están justificados los requisitos no aplicables acordes con lo requerido por el respectivo referencial?
NA

Todos los requisitos y controles de seguridad de la información del anexo A son aplicables

3.10..¿Se auditaron actividades en sitios temporales o fuera del sitio de acuerdo al listado de contratos o proyectos entregado por la Organización?
NA

3.11..Es una auditoría de ampliación o reducción de alcance de certificación o de cubrimiento de sitios permanentes
No

3.12..¿En el caso de los esquemas en los que es aplicable el requisito de diseño y desarrollo del producto o servicio (Por ejemplo, el numeral 8.3, de la norma ISO 9001:2015), este se incluye en el alcance del certificado?

No

3.13..¿Existen requisitos legales para el funcionamiento u operación de la Organización o los proyectos que realiza, por ejemplo, habilitación, registro sanitario, licencia de funcionamiento, licencia de construcción, licencia o permisos ambientales en los que la Organización sea responsable?
Si

- Decreto 1078 de 2015 principios de política de gobierno digital
- Decreto 1499 de 2017 Modelo de planeación integrado de planeación y gestión (MIPG)
- Decreto 1083 de 2015 Políticas de gestión y desempeño institucional (Decerto único reglamentario del setor de función pública
- Resolución 2710 de 2017 expedido por min Tic lineamientos para la adopción del protocolo IPV6.
- CONPES 3854 de 2016 – Establece la política nacional de seguridad digital.
- CONPES 3995 de 2020 – política nacional de confianza y seguridad digital.
- Resolución 500 de 2021 Lineamientos generales para la implementación del modelo de seguridad y privacidad de la información.

3.14..¿Se evidencian cambios significativos en la Organización, desde la anterior auditoría, por ejemplo, relacionados con alta dirección, estructura organizacional, sitios permanentes bajo el alcance de la certificación, cambios en el alcance de la certificación diferentes a ampliación o reducción, entre otros?
Si

El alcance solicitado fue ajustado, quedando "El sistema de gestión de seguridad de la información (SGSI) del Instituto Colombiano de Bienestar Familiar (ICBF) comprende la evaluación del diseño, implementación, mantenimiento y mejora continua de los controles de seguridad de la información aplicados a los procesos relacionados con la prestación de servicios orientados a la protección integral de los derechos de los niños, niñas, adolescentes y sus familias, en el marco de los programas misionales de la Entidad. Asimismo, el alcance incluye la verificación de las actividades de gestión de seguridad de la información asociadas a las Tecnologías de Información y Comunicaciones (TIC), con el fin de propender por la confidencialidad, integridad y disponibilidad de la información..

3.15..¿La organización consideró las cuestiones relativas al cambio climático dentro de la planificación del sistema de gestión?
Si

Se identifica dentro del contexto organizacional como fortaleza en cuanto a los lineamientos e implementaciones de prácticas de ahorro de energía, uso racional de recursos naturales, y como oportunidad en cuanto a la responsabilidad social.

3.16..¿Si la organización realiza actividades del alcance en turnos nocturnos que no pueden ser visitadas en el turno diurno, estas fueron auditadas en esta auditoría?
No

3.17..¿Se tienen actividades, productos y servicios declarados en el alcance del certificado que han sido tercerizados con proveedores o contratistas?
Si

3.17..¿En caso afirmativo, se encontraron controlados los proveedores o contratistas de estas actividades, productos y servicios?

Si

Actividades, productos y servicios incluidos en el alcance de certificación que son subcontratados:	Proveedor/Contratista:	Requisito legal para el funcionamiento u operación (en caso de ser aplicable)
Administración, gestión, monitoreo y control de TIC	UT - SERVICIOS GLOBAL TIC	N/A
Conectividad	Claro	N/A
Datacenter - Hosting de servicios de infraestructura – Operación global TIC	UT - SERVICIOS GLOBAL TIC	N/A

3.18..¿Se presentaron, durante la auditoría, cambios que hayan impedido cumplir con el plan de auditoría inicialmente acordado con la Organización?
NA

3.19..¿Existen aspectos o resultados significativos de esta auditoría, que incidan en el programa de auditoría del ciclo de certificación?
No

3.20..¿Quedaron puntos no resueltos en los casos en los cuales se presentaron diferencias de opinión sobre las NC identificadas durante la auditoría?
No

3.21..¿Aplica reactivación para este servicio?

No

3.22..Se verificó si la Organización implementó o no, el plan de acción establecido para solucionar las no conformidades menores pendientes de la auditoría anterior de ICONTEC y si fueron eficaces.
NA

3.23..Esta auditoría fue testificada por el Organismo de acreditación

No

4. HALLAZGOS DE LA AUDITORÍA

Como resultado de la auditoría, el equipo auditor declara la conformidad y eficacia del sistema de gestión auditado basados en el muestreo realizado. A continuación, se hace relación de los hallazgos de auditoría.

4.1. Hallazgos que apoyan la conformidad del sistema de gestión con los requisitos.

- Es destacable el conocimiento claro del marco legal, los responsables pueden tomar decisiones informadas sobre qué controles implementar, cómo clasificar la información, y cómo responder ante incidentes y en consecuancia blindar a la organziaicón en riegos de incumplimiento o sanciones legales.

- La competencia de los encargados de seguridad de la infroamción en cada procesos fortalece una postura sólida de seguridad, generando confianza entre los grupos de interes , lo cual es clave para la reputación y seguridad de la entidad.
- A aplicación del análisis de contexto Aspectos DOFA y definido bajo el procedimiento porque permite que su aplicación se estándar y la definición de planes de acción.
- La aplicación de formularios para recolectar la información asociada al DOFA a nivel organizacional sede, regional, y centro zonal.
- La información recolectada desde la regionales y centro zonal se consolida para retroalimentar los procesos.
- La definición de procedimiento para la gestión de las necesidades y expectativas de las partes interesadas en la medida que el resultado es confiable.
- La divulgación de la política y sus cambios a través de la website, por lo que permite a los interesados conocer los ajustes realizado e incrementar la conciencia de protección de la información.
- La definición de día de seguridad "Miércoles de ciberseguridad" donde se comparte información relacionada a la política de seguridad de la información con mensajes de seguridad de la información, aspectos de conciencia y cultura de seguridad de la información, todo ello incrementa la conciencia y sensibilización de protección de información.
- Integrar un comité de inteligencia de amenazas con el registro de las actas con el recorrido del análisis de la información, fortalece los propósitos de controles de ciberseguridad.
- La definición del servicio de evaluación de vulnerabilidades permanente dentro del servicio tercerizado, por tanto la oportunidad de aplicación oportuna de las remediaciones.
- El alcance de evaluación de vulnerabilidades de manera segmentada por servicios (DB, Aplicaciones Windows, Linux, Azure, Centro de Cómputo, asegura el conocimiento del estado de seguridad y la aplicación de controles necesarios
- El uso de servicios especializados por parte de proveedor para la gestión de seguridad de la información orientada sobre la infraestructura tecnológica, asegura monitora de eventos y actuaciones en cuanto a la implementación o mantenimiento de controles.
- La idónea definición de políticas de seguridad en servicios en la nube, red, administración de identidades, control de acceso privilegiado, protección de datos, administración de recursos, registro y atención de amenazas, copias de seguridad, alertas de seguridad, asegura la mejor elección del proveedor de servicios y la seguridad de la información en dichos servicios
- El uso de herramientas automáticas para realizar la gestión de capacidad, aseguran acciones oportunas para asegurar la disponibilidad permanente de los servicios tecnológicos.
- La práctica de anonimización de la información datos sensibles al momento de la restauración de bases de datos con datos personales (No. Documento, celular, dirección), asegura la confidencialidad de ellos.
- El uso de herramientas automáticas para la realización de pruebas de seguridad de los desarrollos, asegura altos niveles de protección de la información en los sistemas de información.

4.2. Oportunidades de mejora

- Redacción explícita y/o con detalles en las debilidades y oportunidades de modo tal permite identificar los planes de acciones orientados para su atención.

- Apropiar la gestión de activos y riesgos por parte de los integrantes del equipo del proceso que les permite fortalecer la postura de seguridad y minimizar los riesgos asociados.
- Es conveniente calificar de manera individual la efectividad de los controles identificados de manera que permita conocer qué controles son más débiles o menos efectivos, y así priorizar recursos y esfuerzos en mejorar los que representan mayor riesgo para la seguridad de la información.
- En el hablador que indica acerca de la política de tratamiento de datos en la recepción, incluir el derecho de revocación de la autorización y/o solicitud de la supresión de los datos personales.
- Revisar la pertinencia de hacer uso de herramienta manual o automática para el registro y control de los avances de los planes de remediación de las vulnerabilidad.
- Incluir como objetivo de toda prueba de continuidad de negocio el cumplimiento de los tiempos objetivos de recuperación y RPO, de esta manera se asegurará se satisface las necesidades de la entidad.
- Fortalecer el alcance de toma de evidencia de la ejecución de los mantenimientos de modo tal permita trazabilidad de todos los criterios definido.
- Revisar el resultado del BIA del proceso de Infancia ya indica en punto objetivo de recuperación no alineado con la frecuencia de la toma de respaldo de información de sistemas de información.
- Incluir vigencia de tiempo de la responsabilidad de compromiso de acuerdo de confidencialidad y no divulgación en los procesos de retiro o salida de personas, de mod tal se recuerde y/o referencie y se cumpla por parte de las personas.
- Presentar señalización asociada a la restricción de ingreso y uso de equipo videograbación o fotográfico, ello asegurará el cumplimiento.
- Revisar la pertinencia de incluir vigencia de la responsabilidad de confidencialidad de la información indefinida en el tiempo en los acuerdos de confidencialidad con los colaboradores.
- Incluir nota de socialización del cumplimiento de la política de tratamiento de datos personales en el formato Bitácora de Ingreso a Datacenter.

5. INFORMACIÓN RELACIONADA CON EL DESEMPEÑO Y LA EFICACIA DEL SISTEMA DE GESTIÓN

5.1.1. Incluir las reclamaciones o quejas válidas del cliente en los sistemas de gestión que aplique durante el último año.

Principales quejas o reclamaciones recurrentes	Principal causa	Acciones tomadas
0 quejas o reclamaciones	N/A	N/A

5.1.2. Incluir las solicitudes o comunicaciones de partes interesadas, por ejemplo, para ISO 14001, ISO 45001

N/A

5.1.3. Incluir las retiradas de producto del mercado para ISO 9001, NTC 5830, ISO 22000 y FSSC 22000

N/A

5.1.4. Incluir la ocurrencia de incidentes (accidentes o emergencias) en los sistemas de gestión que aplique y explique brevemente cómo fueron tratados

La organización cuenta con el protocolo definido y aprobado para atender incidentes de seguridad de la información, sin embargo, no se han presentado incidentes de seguridad de la información de impacto considerable

5.1.5. En los casos que aplique verificar que la Organización haya informado a ICONTEC durante los plazos especificados en el Reglamento R-PS-007 REGLAMENTO DE LA CERTIFICACIÓN ICONTEC DE SISTEMAS DE GESTIÓN, eventos que hayan afectado el desempeño del sistema de gestión certificado, relacionados con el alcance de certificación que sean de conocimiento público. El auditor verificará las acciones pertinentes tomadas por la Organización para evitar su recurrencia y describirá brevemente cómo fueron atendidas.

N/A

5.1.6. ¿Existen quejas de usuarios de la certificación recibidas por ICONTEC durante el último periodo evaluado?
No

5.1.7. ¿Se evidencia la capacidad del sistema de gestión para cumplir los requisitos aplicables y lograr los resultados esperados?
Si

5.1.8. ¿Se concluye que el alcance del sistema de gestión es apropiado frente a los requisitos que la Organización debe cumplir? (consultar E-PS-080 ALCANCE DE CERTIFICACIÓN DEL SISTEMA DE GESTION)
Si

Si

5.2. Relación de no conformidades detectadas durante el ciclo de certificación.

¿Se evidencia recurrencia de no conformidades detectadas en las auditorías de ICONTEC en el último ciclo de certificación?
Si

Auditoría	Número de no conformidades	Requisitos
Otorgamiento	3	A.5.9, A.8.13, A.8.9
1ª de seguimiento del ciclo	N/A	N/A
2ª de seguimiento del ciclo	N/A	N/A
Renovación	N/A	N/A
Auditorias especiales (Extraordinaria, reactivación)	N/A	N/A
Auditoría de ampliación	N/A	N/A

5.3. Análisis del proceso de auditoría interna

- La organización cuenta con un programa de auditoría interna para determinar los ciclos de auditoria que requiere la organización en función del estado de importancia, cambios y resultados de auditorías previas, incluida la de seguridad de la información. Se define objetivo, alcance, criterios y metodología.
- Se evidenció plan de auditoría para ejecución a partir del día 01 de agosto con fecha de cierre el 4 de septiembre de 2025 que incluye igualmente objetivo, alcance, criterios, metodología, fechas de ejecución y procesos; la auditoría fue llevada a cabo por parte de auditores internos.
- Se evidenció informe de auditoría por proceso, identificando hallazgos de no conformidad en cada uno de los procesos y por cada esquema ISO. El equipo auditor tanto interno como de personal externo asignados evidenciaron la competencia de acuerdo a lo definido por el procedimiento de auditoría. Se evidenció la toma de las correcciones y acciones correctivas las cuales se encuentran en etapa de implementación
- Se evidenció el desarrollo de la auditoría bajo el esquema de la ISO 19011

5.4. Análisis de la revisión del sistema por la dirección

Se evidenció informe de revisión por la dirección el 07 de octubre de 2025. Los informes incluyeron el análisis y la evaluación de todos los elementos de entrada requeridos por el esquema ISO/IEC 27001:2022. Al final de la revisión por la dirección se evidencia documento con la identificación de las conclusiones del estado de cada uno de los sistemas de gestión, entre ellas, la mejora continua.

6. USO DEL CERTIFICADO DE SISTEMA DE GESTIÓN Y DE LA MARCA O LOGO DE LA CERTIFICACIÓN

6.1. ¿El logo o la marca de conformidad de certificación de sistema de gestión de ICONTEC se usa en publicidad (página web, brochure, papelería, facturas, etc…)?

No

Se le informa a la Organización que el logo de certificación de ICONTEC y, solo podrá ser usado de acuerdo con lo establecido en el Manual de Aplicación E-GM-001, una vez ICONTEC notifique oficialmente la decisión de otorgar el certificado.

6.2. ¿La publicidad realizada por la Organización está de acuerdo con lo establecido en el reglamento R-PS-007 y el Manual de aplicación E-GM-001 USO DE LA MARCA DE CONFORMIDAD DE LA CERTIFICACIÓN ICONTEC PARA SISTEMAS DE GESTIÓN?

NA

6.3. ¿El logo o la marca de conformidad se usa sobre el producto o sobre el empaque o el envase o el embalaje del producto, o de cualquier otra forma que denote conformidad del producto?

NA

6.4. ¿Se evidencia la adecuación de la información contenida en el certificado (¿vigencia del certificado, logo de organismo de acreditación, razón social registrada en documentos de existencia y representación legal, direcciones de sitios permanentes cubiertos por la certificación, alcance, etc.?

NA

7. RESULTADO DE LA REVISIÓN DE LAS CORRECCIONES Y ACCIONES CORRECTIVAS PARA LAS NO CONFORMIDADES MAYORES DETECTADAS EN ESTA AUDITORÍA, MENORES QUE GENERARON COMPLEMENTARIA Y, MENORES DETECTADAS EN ESTA AUDITORÍA QUE POR SOLICITUD DEL CLIENTE FUERON REVISADAS

¿Se presentaron no conformidades mayores?

No.

¿Se presentaron no conformidades menores de la auditoria anterior que no pudieron ser cerradas en esta auditoría?

No.

¿Se presentaron no conformidades menores detectadas en esta auditoría que por solicitud del cliente fueron revisadas durante la complementaria?

No.

Fecha de la verificación complementaria

NA.

NC	Descripción de la no conformidad (se relaciona el numeral de la norma y la evidencia del incumplimiento)	Evidencia obtenida que soporta la solución	¿Fue eficaz la acción?
No conformidades mayores identificadas en esta auditoría			
No conformidades pendientes de la auditoría anterior que no se solucionaron			
No conformidades detectadas en esta auditoría que fueron cerradas			

8. RECOMENDACIÓN DEL EQUIPO AUDITOR DE ACUERDO CON EL R-PS-007

Se recomienda **Otorgar la Certificación**	ISO/IEC 27001:2022			
Nombre del auditor líder: OSCAR FERNANDO RAMOS BENAVIDES Coordinador Lider ISO/IEC 27001:2022	**Fecha:**	2025	12	17

9. ANEXOS QUE FORMAN PARTE DEL PRESENTE INFORME

Anexo 1	Correcciones, análisis de causa y acciones correctivas	X
Anexo 2	Información específica de esquemas de certificación de sistema de gestión (En caso de que no aplique indicar en el cuadro N/A)	X
Anexo 3	Plan de auditoría F-PS-530 PLAN DE AUDITORIA EN SITIO – SISTEMAS DE GESTIÓN (Adjuntar el plan a este formato y el F-PS-654 FORMATO DE PROYECTOS EJECUTADOS Y EN EJECUCIÓN, cuando aplique)	X
Anexo 4	Aceptación de los resultados de la auditoria firmada por la organización.	X

ANEXO 1 CORRECCIONES, CAUSAS Y ACCIONES CORRECTIVAS

- ✓ Se recibió la propuesta de correcciones, análisis de causas y acciones correctivas para la solución de no conformidades el 2025-11-18 y recibieron observaciones por parte del auditor líder.
- ✓ Las correcciones, análisis de causas y acciones correctivas propuestas por la organización, fueron aceptadas por el auditor líder el 2025-11-21.

SOLICITUD DE ACCIÓN CORRECTIVA		**No.** 1 de 3
[ ] No – Conformidad Mayor [X] No - Conformidad Menor	Norma(s): ISO/IEC 27001:2022	Requisito(s): A.8.9
Descripción de la no conformidad: No se establece, documenta, monitorea y revisa las configuraciones de seguridad de Hardware, Software, servicios y redes.		
Evidencia: No se provee evidencia asociada.		

Corrección	**Evidencia de Implementación**	**Fecha**
Revisar el alcance y propósito del control para	Sesión de trabajo	2025/12/19

definición de la estrategia de atención.		

Descripción de la (s) causas (s)

- No se cuenta con un procedimiento operativo que defina la frecuencia, responsables y herramientas para la revisión.
- No existe un instructivo ni checklist que defina parámetros seguros para hardware, software y redes.
- No se cuenta con controles automatizados para validar las configuraciones

CAUSA RAIZ: Ausencia de procedimiento específico y controles automatizados para validar configuraciones seguras.

Acción correctiva	Evidencia de Implementación	Fecha
Crear y aprobar guía para "Gestión de Configuraciones Seguras" (incluyendo frecuencia, responsables y herramientas).	Guía aprobada y publicada	2026/02/20
Crear formato de checklist con parámetros de seguridad para Hardware, Software y redes	Formato	2026/02/20
Socializar la guía para gestión de configuraciones seguras con parámetros de seguridad para hardware, software y redes	Acta de reunión	2026/06/30
Implementar controles automatizados para monitoreo periódico.	Reportes	2026/06/26
Llevar a cabo actividades de seguimiento y monitoreo al cumplimiento y eficacia de las acciones correctivas	Informe seguimiento/monitoreo	2026/07/31

SOLICITUD DE ACCIÓN CORRECTIVA	**No.** 2 de 3

	No – Conformidad Mayor	Norma(s): ISO/IEC 27001:2022	Requisito(s): A.5.9
X	No - Conformidad Menor		

Descripción de la no conformidad:
No se identifican todos los activos de información en el proceso Relación con el Ciudadano.

Evidencia:
El proceso de Atención al Ciudadano no incluyó en su inventario de activos de información, (1) El servicio gestionado por Operador de Centro de Contacto, (2) El Módulo de Atención al Ciudadano, como tampoco, (3) las personas o cargos asociados al proceso.

Corrección	Evidencia de Implementación	Fecha
Actualizar el inventario de activos del proceso de Relación con el Ciudadano, incluyendo: • Servicio del Operador de Centro de Contacto. • Roles de proceso dentro de la matriz de activos	Inventario actualizado	2026/02/20

Descripción de la (s) causas (s)

- Desconocimiento de que los servicios contratados deben hacer parte de los activos de información del proceso.
- Porque en la guía de activos actual no existe estandarizado que obligue a incluir servicios tercerizados, módulos y roles en el inventario.
- Porque el responsable del proceso desconoce los criterios del SGSI para la identificación de activos

CAUSA RAIZ: Falta de aplicación del procedimiento por desconocimiento y ausencia de control en la validación del inventario.

Acción correctiva	Evidencia de Implementación	Fecha
Actualizar la Guía para el desarrollo de inventario y clasificación de activos	Guía actualizada	2026/03/23
Actualizar formato para levantamiento de activos de información donde se adicione otras partes interesadas en la lista desplegable.	Formato actualizado	2026/03/23
Socializar la Guía para el desarrollo de inventario y clasificación de activos a los responsables de los procesos y regionales.	Presentación y Listado de asistencia	2026/04/06
Llevar a cabo actividades de seguimiento y monitoreo al cumplimiento y eficacia de las acciones correctivas	Informe de seguimiento/monitoreo	2026/04/30

SOLICITUD DE ACCIÓN CORRECTIVA	**No.** 3 de 3

	No – Conformidad Mayor	Norma(s): ISO/IEC 27001:2022	Requisito(s): A.8.13
X	No - Conformidad Menor		

Descripción de la no conformidad:
No se prueba la conformidad de las copias de seguridad de información.

Evidencia:
No se ha realizado pruebas de restauración de información de respaldo de bases de datos de, SIA (Gestión de proveedores), INSNSIR y, Rubonline (Sistema de Información Misional).

Corrección	Evidencia de Implementación	Fecha
La acción de corrección de orienta a restauración y pruebas de SIA, INSNSIR y Ruboline (sistema de información misional	Evidencia de resultados	2026/01/30

Descripción de la (s) causas (s)

- No se describe dentro de la G8.GTI Guía respaldo y restauración de copias de seguridad, realizar pruebas de restauración.
- Ausencia de un cronograma formal para ejecutar las pruebas periódicas de restauración.
- Ausencia de controles documentados, para realizar seguimiento a las pruebas de restauración.

CAUSA RAIZ: Falta de implementación de acciones y control para realizar pruebas de

restauración de copias de seguridad, derivado de ausencia de planificación y capacitación.		
Acción correctiva	**Evidencia de Implementación**	**Fecha**
Actualizar la G8.GTI Guía respaldo y restauración de copias de seguridad, incorporando la descripción, periodicidad, controles, formato y acta para la ejecución de pruebas de restauración de las copias de seguridad.	G8.GTI Guía respaldo y restauración de copias de seguridad actualizada y publicada.	2026/01/30
Definir un cronograma de pruebas de restauración que contemple: (Fecha / Sistema /Tipo de prueba /Responsable de la prueba / Evidencia de restauración)	Acta de reunión y cronograma	2026/01/30
Ejecutar las pruebas de restauración de acuerdo con lo establecido en la G8.GTI Guía respaldo y restauración de copias de seguridad y el cronograma definido.	Informe de pruebas con resultados y eventos.	2026/06/30
Verificar que la restauración se haya completado sin errores.	Informe de pruebas con resultados y eventos.	2026/06/30
Realizar actividades de seguimiento y monitoreo al cumplimiento y eficacia de las acciones correctivas	Informe mensual o correo electrónico	2026/06/30

Nota: Es importante que la organización realice un buen análisis de causa para evitar que la no conformidad se repita y el plan de acción sea devuelto por el equipo auditor, por lo cual les sugerimos consultar la guía para la solución de no conformidades, disponible en la página web de Icontec.

Consulte la *Guía para la solución de no conformidades* en la ruta https://www.icontec.org/%e2%80%8bdocumentos-servicios-icontec/ en el link Evaluación de la conformidad.

Ruta: www.icontec.org – Documentos servicios ICONTEC- Evaluación de la conformidad.

ANEXO 2
INFORMACIÓN ESPECÍFICA DE ESQUEMAS DE CERTIFICACIÓN DE SISTEMA DE GESTIÓN

ISO/IEC 27001:2022

Objetivos de la auditoría

Evaluar las implicaciones de los cambios en el SGSI/SGPI, iniciadas como consecuencia de cambios en la operación del cliente y cubrir al menos:

1. El sistema de mantenimiento de elementos tales como la evaluación y control de riesgos de seguridad de la información y privacidad, mantenimiento, auditorías internas del SGSI/SGPI, revisión por la dirección y las acciones correctivas;
2. Las comunicaciones de las partes externas como es requerido por la norma ISO/IEC 27001 e ISO/IEC 27701;
3. Los cambios en la documentación del SGSI/SGPI;
4. Las zonas sujetas a cambio;
5. Los requisitos de la norma ISO/IEC 27001 e ISO/IEC 27701 cuando sea aplicable.

Actividades desarrolladas

¿Cuál es sistema de gestión auditado?
ISO/IEC **27001**

.

- Si la auditoria se realizó totalmente remota, por favor confirme si la organización cuenta con sede física:

Si □ No X

La auditoría se llevó a cabo 100% presencial

Se verificó que la organización ha evaluado y realizado las adecuaciones internas y los procedimientos adoptados para asegurar que el SGSI se confiable.

Si X No □

La metodología de la auditoría fue verificación de registros físicos y electrónicos, interacción, observación y toma de muestreo.

¿Se modificó la declaración de aplicabilidad?
No

VERSIÓN VIGENTE:	JUSTIFICACIÓN DEL CAMBIO
Declaración de Aplicabilidad: A3.MS.DE Versión 14 2025-03-21	Es la versión asignada y aprobada para la auditoría de otorgamiento.

¿Los procedimientos adoptados por el cliente brindan confianza en el SGSI/ SGPI?
Si

.

.

Se revisaron los documentos concernientes a: Políticas de seguridad de la información, Registro de incidentes, Registro de revisiones de perfiles a colaboradores, Registro de vulnerabilidades, Revisión de cuentas desactivadas de usuarios retirados, Revisión física de equipos de cómputo, Roles de seguridad de la información, Manual de gestión de seguridad de la información y de gestión de servicios, capacitación de seguridad de la información y gestión de servicios, declaración de aplicabilidad, Formato identificación de perfiles a colaboradores, Gestión de vulnerabilidades, Identificación y análisis de riesgos de procesos, de seguridad de la información y de servicios, Identificación, clasificación y valoración de activos de información, Inventario de activos de información, Manual de servicios y plan de continuidad del negocio, Prueba de plan de continuidad del negocio,Informe de auditoría interna, Informe ethical hacking, Políticas de seguridad de la información y gestión de incidentes de seguridad de la información.

Análisis de la eficacia del sistema de gestión certificado

- El ejercicio de valoración de los riesgos realizado por la organización se soporta en lineamientos de metodología ISOIEC 27005.
- Los planes de acción para la implementación de controles (validados por la auditoria), satisfacen los requerimientos de la organización en el escenario de gestión del riesgo y sus objetivos, previamente definido por la entidad, proporcionando de esta manera un estado de aprobación por parte de los responsables de los riesgos y de la alta dirección.
- Así las cosas, los responsables del riesgo identifican los riesgos y registran la aprobación de los riesgos inherentes y el riesgo residual de manera estandarizada.
- La metodología de análisis de riesgos se destaca por su alcance, cobertura y por la constante participación de todos los líderes de los procesos.

ANEXO 3
Plan de auditoría F-PS-530 PLAN DE AUDITORIA EN SITIO – SISTEMAS DE GESTIÓN

Somos **calidad**,
somos **competitividad**,
somos **confianza**.

icontec

Huella de confianza.

icontec.org

EMPRESA:	INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR		
Dirección del sitio:	ISO/IEC 27001:2022 – Sede Nacional Avenida Carrera 68 No 64C 75 Bogotá D.C., Cundinamarca, Colombia		
Representante de la Organización:	MILTON FABIAN FORERO MELO		
Cargo:	DIRECTOR DE PLANEACIACIÓN Y CONTROL DE GESTIÓN	Correo electrónico:	Milton.Forero@icbf.gov.co

Alcance de la certificación:
ISO/IEC 27001:2022 –

El sistema de gestión de seguridad de la información (SGSI) del Instituto Colombiano de Bienestar Familiar (ICBF) comprende la evaluación del diseño, implementación, mantenimiento y mejora continua de los controles de seguridad de la información aplicados a los procesos relacionados con la prestación de servicios orientados a la protección integral de los derechos de los niños, niñas, adolescentes y sus familias, en el marco de los programas misionales de la Entidad. Asimismo, el alcance incluye la verificación de las actividades de gestión de seguridad de la información asociadas a las Tecnologías de Información y Comunicaciones (TIC), con el fin de Propender por la confidencialidad, integridad y disponibilidad de la información. Declaración de Aplicabilidad A3.MS.DE, Versión 14 aprobada 2025-03-21.

Alcance de la auditoria:

ISO/IEC 27001:2022 –

El sistema de gestión de seguridad de la información (SGSI) del Instituto Colombiano de Bienestar Familiar (ICBF) comprende la evaluación del diseño, implementación, mantenimiento y mejora continua de los controles de seguridad de la información aplicados a los procesos relacionados con la prestación de servicios orientados a la protección integral de los derechos de los niños, niñas, adolescentes y sus familias, en el marco de los programas misionales de la Entidad. Asimismo, el alcance incluye la verificación de las actividades de gestión de seguridad de la información asociadas a las Tecnologías de Información y Comunicaciones (TIC), con el fin de Propender por la confidencialidad, integridad y disponibilidad de la información. Declaración de Aplicabilidad A3.MS.DE, Versión 14 aprobada 2025-03-21.

Criterios de Auditoría:	ISO/IEC 27001:2022 + la documentación del Sistema de Gestión.
Tipo de auditoría: Otorgamiento	
Modalidad: XAuditoría en sitio □Auditoria parcialmente remota □Auditoría totalmente remota	
Aplica toma de muestra por multisitio:	NO ISO/IEC 27001:2022: No multisitio
Existen actividades/procesos que requieran ser auditadas en turno nocturno:	No

Con un cordial saludo, enviamos el plan de la auditoría que se realizará al Sistema de Gestión de su

organización. Por favor indicar en la columna correspondiente, el nombre y cargo de las personas que atenderán cada entrevista y devolverlo al correo electrónico del auditor líder. Así mismo, para la reunión de apertura de la auditoría le agradezco invitar a las personas del grupo de la alta dirección y de las áreas/procesos/actividades que serán auditadas.

Para la reunión de apertura le solicitamos disponer de un proyector para computador y sonido para video, si es necesario, (sólo para auditorías de certificación inicial y actualización).

En cuanto a las condiciones de seguridad y salud ocupacional aplicables a su organización, por favor informarlas previamente al inicio de la auditoría y disponer el suministro de los equipos de protección personal necesarios para el equipo auditor.

La información que se conozca por la ejecución de esta auditoría será tratada confidencialmente, por parte del equipo auditor de ICONTEC.

El idioma de la auditoría y su informe será el español.

Los objetivos de la auditoría son:

- Determinar la conformidad del sistema de gestión con los requisitos de la norma de sistema de gestión.
- Determinar la capacidad del sistema de gestión para asegurar que la organización cumple los requisitos legales, reglamentarios y contractuales aplicables al alcance del sistema de gestión y a la norma de requisitos de gestión.
- Determinar la eficacia del sistema de gestión para asegurar que la organización puede tener expectativas razonables con relación al cumplimiento de los objetivos especificados.
- Identificar áreas de mejora potencial del sistema de gestión.

Las condiciones de este servicio y las responsabilidades del equipo auditor se encuentran indicadas en el R-PS-0007 REGLAMENTO DE LA CERTIFICACIÓN ICONTEC DE SISTEMAS DE GESTIÓN.

Auditor Líder	OSCAR FERNANDO RAMOS BENAVIDES Coordinador Lider ISO/IEC 27001:2022	Correo electrónico	oramos@icontec.net
Auditor	LIBARDO CHAVEZ ISO/IEC 27001:2022 JHOAN DAVID CORAL MEJIA ISO/IEC 27001:2022		
Experto Técnico	N/A		
Observador-Profesional de Apoyo	N/A		

Fecha / Sitio (si hay más de uno)	Hora de inicio de la actividad de auditoría	Hora de finalización de la actividad de auditoría	PROCESO /REQUISITOS POR AUDITAR	EQUIPO AUDITOR	CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría)

2025-10-23 Sede Nacional Avenida Carrera 68 No 64C 75	08:00	08:30	REUNION DE APERTURA ISO/IEC 27001:2022 Act. Común	LIBARDO CHAVEZ OSCAR FERNANDO RAMOS BENAVIDES	Todos los Auditados
2025-10-23 Sede Nacional Avenida Carrera 68 No 64C 75	08:30	10:30	PRESTACION DEL SERVICIO. PROTECCION. RESPONSABILIDAD PENAL ADOLESCENTE ISO/IEC 27001:2022 7.1, 8.1, 8.2, 8.3, 9.1, A 5.8, A 5.9, A 5.10, A 5.11, A 5.12, A 5.13, A 5.14, A 5.15, A 5.16, A 5.17, A 5.18	LIBARDO CHAVEZ	Beatriz Adriana Tierradentro - Directora
2025-10-23 Sede Nacional Avenida Carrera 68 No 64C 75	08:30	10:30	DIRECCIONAMIENTO ESTRATEGICO ISO/IEC 27001:2022 4.1, 4.2, 4.3, 4.4, 5.2, 9.3.1, 9.3.2, 9.3.3	OSCAR FERNANDO RAMOS BENAVIDES	Beatriz Adriana Tierradentro - Directora
2025-10-23 Sede Nacional Avenida Carrera 68 No 64C 75	10:30	12:30	GESTION DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27001:2022 6.1.1, 6.1.2, 6.1.3, 8.2, 8.3, 9.2, 9.2.1, 9.2.2	OSCAR FERNANDO RAMOS BENAVIDES	Nayibe Pico
2025-10-23 Sede Nacional Avenida Carrera 68 No 64C 75	10:30	12:30	PRESTACION DEL SERVICIO. PROTECCION. RESTABLECIMIENTO DE DERECHOS ISO/IEC 27001:2022 7.1, 8.1, 8.2, 8.3, 9.1, A 5.8, A 5.9, A 5.10, A 5.11, A 5.12, A 5.13, A 5.14, A 5.15, A 5.16, A 5.17, A 5.18	LIBARDO CHAVEZ	Beatriz Adriana Tierradentro - Directora
2025-10-23 Sede Nacional Avenida Carrera 68 No 64C 75	13:30	15:00	PRESTACION DEL SERVICIO. PROTECCION. ADOPCIONES ISO/IEC 27001:2022 7.1, 8.1, 8.2, 8.3, 9.1, A 5.8, A 5.9, A 5.10, A 5.11, A 5.12, A 5.13, A 5.14, A 5.15, A 5.16, A 5.17, A 5.18	LIBARDO CHAVEZ	Carlos Arguello - EPICO
2025-10-23 Sede Nacional Avenida Carrera 68 No 64C 75	13:30	16:30	RELACION CON EL CIUDADANO ISO/IEC 27001:2022 7.1, 8.1, 8.2, 8.3, 9.1, A 5.8, A 5.9, A 5.10, A 5.11, A 5.12, A 5.13, A 5.14, A 5.15, A 5.16, A 5.17, A 5.18	OSCAR FERNANDO RAMOS BENAVIDES	Monica Jaime - EPICO
2025-10-23 Sede Nacional Avenida Carrera 68 No 64C 75	15:00	16:30	COORDINACION Y ARTICULACION DEL SNBF Y AGENTES ISO/IEC 27001:2022 7.1, 8.1, 8.2, 8.3, 9.1, A 5.8, A 5.9, A 5.10, A 5.11, A 5.12, A 5.13, A 5.14, A 5.15, A 5.16, A 5.17, A 5.18	LIBARDO CHAVEZ	Julian Moreno Parra - Director
2025-10-23	16:30	17:00	BALANCE DIARIO ISO/IEC 27001:2022	LIBARDO CHAVEZ	

Sede Nacional Avenida Carrera 68 No 64C 75			Act. Común	OSCAR FERNANDO RAMOS BENAVIDES	
2025-10-24 Sede Nacional Avenida Carrera 68 No 64C 75	08:00	10:00	CONTRATACION ISO/IEC 27001:2022 7.1, A 5.19, A 5.20, A 5.21, A 5.22	JHOAN DAVID CORAL MEJIA	Kerly Jazmin Agames - Directora
2025-10-24 Sede Nacional Avenida Carrera 68 No 64C 75	08:00	10:00	PROMOCION Y PREVENCION. ISO/IEC 27001:2022 7.1, 8.1, 8.2, 8.3, 9.1, A 5.8, A 5.9, A 5.10, A 5.11, A 5.12, A 5.13, A 5.14, A 5.15, A 5.16, A 5.17, A 5.18	LIBARDO CHAVEZ	Julie Pauline Trujillo V - Directora
2025-10-24 Sede Nacional Avenida Carrera 68 No 64C 75	08:00	10:00	GESTION DE TECNOLOGIA DE INFORMACION. EVENTOS DE SI / VULNERABILIDADES TECNICAS ISO/IEC 27001:2022 A 8.8, A 8.16	OSCAR FERNANDO RAMOS BENAVIDES	Amalia Peña Russi, Oscar Vivas, Nayive pico
2025-10-24 Sede Nacional Avenida Carrera 68 No 64C 75	10:00	12:00	INSPECCION, VIGILANCIA Y CONTROL ISO/IEC 27001:2022 7.1, 8.1, 8.2, 8.3, 9.1, A 5.8, A 5.9, A 5.10, A 5.11, A 5.12, A 5.13, A 5.14, A 5.15, A 5.16, A 5.17, A 5.18	JHOAN DAVID CORAL MEJIA	Jeason Ariel Cossio - Jefe Carlos Alberto Cuervo - EPICO
2025-10-24 Sede Nacional Avenida Carrera 68 No 64C 75	10:00	12:00	PROMOCION Y PREVENCION / FAMILIA Y COMUNIDADES ISO/IEC 27001:2022 7.1, 8.1, 8.2, 8.3, 9.1, A 5.8, A 5.9, A 5.10, A 5.11, A 5.12, A 5.13, A 5.14, A 5.15, A 5.16, A 5.17, A 5.18	LIBARDO CHAVEZ	Haidy Isabel Duque C - Directora Juana Hersilia Moya D - Subdirectora Juan Pablo Mongue - Subdirector Felipe Pedreros - EPICO
2025-10-24 Sede Nacional Avenida Carrera 68 No 64C 75	10:00	12:00	GESTION DE TECNOLOGIA DE INFORMACION. SEGURIDAD DE LA INFORMACION EN LA CONTINUIDAD DE NEGOCIO. ISO/IEC 27001:2022 A 5.29, A 5.30, A 8.14	OSCAR FERNANDO RAMOS BENAVIDES	Amalia Peña Russi, Oscar Vivas, Nayibe Pico
2025-10-24 Sede Nacional Avenida Carrera 68 No 64C 75	13:00	14:30	COOPERACION Y CONVENIOS ISO/IEC 27001:2022 7.1, 8.1, 8.2, 8.3, 9.1, A 5.8, A 5.9, A 5.10, A 5.11, A 5.12, A 5.13, A 5.14, A 5.15, A 5.16, A 5.17, A 5.18	JHOAN DAVID CORAL MEJIA	Diana Margarita Rivera - Jefe Oficina Christian Camilo Rodriguez - EPICO
2025-10-24 Sede Nacional Avenida Carrera 68	13:00	15:00	PROMOCION Y PREVENCION DE INFANCIA / ADOLESCENCIA Y JUVENTUD ISO/IEC 27001:2022 7.1, 8.1, 8.2, 8.3, 9.1, A 5.8, A 5.9, A 5.10, A 5.11, A 5.12, A 5.13, A 5.14, A 5.15, A 5.16,	LIBARDO CHAVEZ	Naya Gutiérrez P - Director Angela Fernanda Cabrera - Subdirectora Juan Leonardo Herrera G - EPICO

No 64C 75			A 5.17, A 5.18		
2025-10-24 Sede Nacional Avenida Carrera 68 No 64C 75	14:30	16:30	GESTION JURIDICA. ISO/IEC 27001:2022 A 5.31, A 5.32, A 5.33, A 5.34, A 5.35, A 5.36, A 5.37	JHOAN DAVID CORAL MEJIA	Jose Miguel Rueda - Jefe Juan Carlos Arias Alvarado - EPICO
2025-10-24 Sede Nacional Avenida Carrera 68 No 64C 75	15:00	16:30	PROMOCION Y PREVENCION NUTRICION ISO/IEC 27001:2022 7.1, 8.1, 8.2, 8.3, 9.1, A 5.8, A 5.9, A 5.10, A 5.11, A 5.12, A 5.13, A 5.14, A 5.15, A 5.16, A 5.17, A 5.18	LIBARDO CHAVEZ	Salvador Rincon Santos - Director
2025-10-24 Sede Nacional Avenida Carrera 68 No 64C 75	16:30	17:00	BALANCE DIARIO ISO/IEC 27001:2022 Act. Común	JHOAN DAVID CORAL MEJIA LIBARDO CHAVEZ	
2025-10-27 Sede Nacional Avenida Carrera 68 No 64C 75	08:00	10:00	GESTION DE TECNOLOGIA E INFORMACION. SEGURIDAD FISICA ISO/IEC 27001:2022 A 7.1, A 7.2, A 7.3, A 7.4, A 7.5, A 7.6, A 7.7, A 7.8, A 7.9, A 7.10, A 7.11, A 7.12, A 7.13, A 7.14	OSCAR FERNANDO RAMOS BENAVIDES	Amalia Peña Russi, Oscar Vivas, Nayibe Pico
2025-10-27 Sede Nacional Avenida Carrera 68 No 64C 75	10:00	12:00	GESTION DE TECNOLOGIA E INFORMACION. INCIDENTES DE SEGURIDAD DE LA INFORMACION ISO/IEC 27001:2022 A 5.24, A 5.25, A 5.26, A 5.27, A 5.28	OSCAR FERNANDO RAMOS BENAVIDES	Amalia Peña Russi, Oscar Vivas, Nayibe Pico
2025-10-27 Sede Nacional Avenida Carrera 68 No 64C 75	13:00	16:00	GESTION DE TECNOLOGIA E INFORMACION. CONTROLES ORGANIZACIONALES ISO/IEC 27001:2022 A 5.1, A 5.2, A 5.3, A 5.4, A 5.5, A 5.6, A 5.7, A 5.8, A 5.9, A 5.10, A 5.11, A 5.12, A 5.13, A 5.14, A 5.15, A 5.16, A 5.17, A 5.18, A 5.23	OSCAR FERNANDO RAMOS BENAVIDES	Amalia Peña Russi, Oscar Vivas, Nayibe Pico
2025-10-27 Sede Nacional Avenida Carrera 68 No 64C 75	16:00	17:00	BALANCE DIARIO. PREPARACION DE INFORME ISO/IEC 27001:2022 Act. Común	OSCAR FERNANDO RAMOS BENAVIDES	
2025-10-28 Sede Nacional Avenida Carrera 68 No 64C 75	08:00	12:00	GESTION DE TECNOLOGIA E INFORMACION. CONTROLES TECNOLOGICOS ISO/IEC 27001:2022 7.1, 8.1, 8.2, 8.3, 9.1, A 8.1, A 8.2, A 8.3, A 8.4, A 8.5, A 8.6, A 8.7, A 8.9, A 8.10, A 8.11, A 8.12, A 8.13, A 8.15	OSCAR FERNANDO RAMOS BENAVIDES	Amalia Peña Russi, Oscar Vivas, Nayibe Pico

2025-10-28 Sede Nacional Avenida Carrera 68 No 64C 75	13:00	16:00	GESTION DE TECNOLOGIA E INFORMACION ISO/IEC 27001:2022 A 8.17, A 8.18, A 8.19, A 8.20, A 8.21, A 8.22, A 8.23, A 8.24	OSCAR FERNANDO RAMOS BENAVIDES	Amalia Peña Russi, Oscar Vivas, Nayibe Pico
2025-10-28 Sede Nacional Avenida Carrera 68 No 64C 75	16:00	17:00	BALANCE DIARIO. PREPARACION DE INFORME ISO/IEC 27001:2022 Act. Común	OSCAR FERNANDO RAMOS BENAVIDES	
2025-10-29 Sede Nacional Avenida Carrera 68 No 64C 75	08:00	10:00	GESTION DE TECNOLOGIA E INFORMACION. DESARROLLO DE SOFTWARE ISO/IEC 27001:2022 A 8.25, A 8.26, A 8.27, A 8.28, A 8.29, A 8.30, A 8.31, A 8.32, A 8.33, A 8.34	OSCAR FERNANDO RAMOS BENAVIDES	Amalia Peña Russi, Oscar Vivas, Nayibe Pico
2025-10-29 Sede Nacional Avenida Carrera 68 No 64C 75	10:00	12:00	TALENTO HUMANO ISO/IEC 27001:2022 A 6.1, A 6.2, A 6.3, A 6.4, A 6.5, A 6.6, A 6.7, A 6.8	OSCAR FERNANDO RAMOS BENAVIDES	Nayibe Pico
2025-10-29 Sede Nacional Avenida Carrera 68 No 64C 75	13:00	16:00	PREPARACION DEL BALANCE GENERAL ISO/IEC 27001:2022 Act. Común	OSCAR FERNANDO RAMOS BENAVIDES	
2025-10-29 Sede Nacional Avenida Carrera 68 No 64C 75	16:00	17:00	REUNION DE CIERRE ISO/IEC 27001:2022 Act. Común	OSCAR FERNANDO RAMOS BENAVIDES	

Observaciones:

Especificar los requisitos comunes aplicables a los procesos y/o actividades del sistema de gestión que serán auditados por muestreo durante el desarrollo de las entrevistas del presente Plan de Auditoría:

ISO/IEC 27001:2022
10.1, 5.2, 6.2, 7.5.1, 7.5.2, 7.5.3, 8.1, 8.2, 8.3, 9.1

Verificación de uso del logo de ICONTEC.

Especificar cualquier aspecto logístico importante para el desarrollo de la auditoría, tal como traslado y regreso de los sitios donde se desarrollará la auditoría, transporte, entre otros, en caso de ser requerido.

Actividad	Horario	Ubicación

Indicar si esta auditoría es testificada por un Organismo de Acreditación. Indicar los nombres de las personas que conforman el equipo evaluador. Si □ No X
Para el balance diario de información del equipo auditor le agradecemos disponer de una oficina o sala, así como también de acceso a la documentación del sistema de gestión.

Fecha de emisión del plan de auditoría:	2025-10-22

ACEPTACIÓN DE LOS RESULTADOS DE LA AUDITORIA FIRMADA POR LA ORGANIZACIÓN: INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR
Número de no conformidades por esquema detectadas en esta auditoría: ISO/IEC 27001:2022 (0) Mayores (3) Menores Número de no conformidades pendientes que no se cerraron en esta auditoría: ( ) menores (X) N.A. Plazo para la entrega de propuesta de corrección y acción correctiva (de acuerdo con lo establecido en el R-PS-007) hasta: 2025-11-14 Fecha tentativa de verificación complementaria, cuando aplique NA
ACEPTACIÓN DE LA ORGANIZACIÓN: INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR
Declaro que los servicios previstos fueron integralmente ejecutados y soy consciente de los resultados obtenidos. La organización acepta la (s) no conformidad (es) reportada (s) en el presente informe y se compromete a presentar los planes de acción en los tiempos establecidos en el reglamento de certificación R-PS-007. En caso de no aceptarse alguna no conformidad relacione él número de la no conformidad ___N/A____ y el requisito al que fue reportada _N/A_. En este caso la organización deberá solicitar una reposición dirigida al Gerente de Certificación.
ACEPTACIÓN DE LA ORGANIZACIÓN DE RECIBIR AUDITORIAS TESTIFICADAS: N/A
Dando cumplimiento al requisito 4.7 del R-PS-007 la Organización se compromete a permitir la participación de equipos evaluadores de organismos de acreditación, en calidad de observadores, en las auditorías testificadas que dichos organismos seleccionen como parte de sus actividades de acreditación. Consulte el Reglamento de la certificación ICONTEC de Sistemas de Gestión mailto:https://www.icontec.org/wp-content/uploads/2021/07/Reglamento-de-la-certificaci%C3%B3n-ICONTEC-de-sistemas-de-gesti%C3%B3n.pdf

Nombre del Representante de la Organización:	Firma:
MILTON FABIÁN MORENO MELO **DIRECTOR DE PLANEACIÓN Y CONTROL DE GESTIÓN.**