1. INFORMACIÓN GENERAL

1.1. ORGANIZACIÓN

INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR

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

1.3. LOCALIZACIÓN DEL SITIO PERMANENTE PRINCIPAL: Avenida carrera 68 No. 64 C 75, Bogotá, D.C. - Colombia

1.3.1 LOCALIZACION DE OTROS SITIOS PERMANENTES INCLUIDOS EN EL CERTIFICADO

Si la certificación de la organización registrada en el numeral 1.1 cubre más de un sitio permanente donde se realicen actividades del sistema de gestión, indique la localización de cada uno.

Dirección del sitio permanente	Localización (ciudad - país)	Actividades del sistema de gestión,desarrollados en este sitio, que estén cubiertas en el alcance
Sede nacional Av. Carrera 68 No. 64C- 75	Bogotá D.C., Cundinamarca,Colombia	Todas las actividades del alcance
Av. 68 # 75 a – 50 piso 3 Sede Metrópolis	Bogotá D.C., Cundinamarca,Colombia	Gestión de la Tecnologías de información y comunicaciones
Regional Amazonas: Carrera 4 No. 4 - 10	Leticia Amazonas, Colombia	Todas las actividades del alcance
Regional Antioquia: Calle 45 No. 79 - 141	Medellín, Antioquia, Colombia	Todas las actividades del alcance
Regional Arauca Calle 21 No. 1 - 24 Barrio Fundadores	Arauca, Arauca, Colombia	Todas las actividades del alcance
Regional Atlántico: Carrera 46 No. 61 – 15 Barrio Boston	Barranquilla, Atlántico, Colombia	Todas las actividades del alcance
Regional Bogotá: Carrera 50 No. 26 - 51 CAN	Bogotá D.C., Cundinamarca, Colombia	Todas las actividades del alcance
Regional Bolívar: Calle 32 No. 8 - 50 Piso 16 La Matuna, Centro Car	Cartagena, Bolívar, Colombia	Todas las actividades del alcance
Regional Boyacá: Carrera 6 No. 73 – 98 Barrio Palos Verdes	Tunja, Boyacá, Colombia	Todas las actividades del alcance
Regional Caldas:	Manizales, Caldas, Colombia	Todas las actividades del alcance

Avenida Santander Carrera 23 No. 39 – 60		
Regional Caquetá: Transversal 6; Avenida Circunvalar Barrio San Judas	Florencia, Caquetá, Colombia	Todas las actividades del alcance
Regional Casanare: Diagonal 9 No. 8 – 85 Barrio Luz María Jiménez	Yopal, Casanare, Colombia	Todas las actividades del alcance
Regional Cauca: Carrera 26 Calle 6 Frente al Cementerio Central Popayán	Popayán, Cauca, Colombia	Todas las actividades del alcance
Regional Cesar: Calle 16 A No. 11-15 Barrio Loperena	Valledupar - Cesar Colombia	Todas las actividades del alcance
Regional Córdoba: Carrera 9 No. 10-26	Montería, Córdoba, Colombia	Todas las actividades del alcance
Regional Cundinamarca: Calle 47 No. 91 – 68 Barrio La Castellana	Bogotá, D.C. - Cundinamarca Colombia	Todas las actividades del alcance
Regional Guaviare: Avenida los Colonizadores No. 23 – 106 Barrio La Esperanza	San José del Guaviare Guaviare – Colombia	Todas las actividades del alcance
Regional Huila: Avenida Circunvalar; Calle 21 No. 1 E 40, Barrio San Vicente de Paul	Neiva – Huila Colombia	Todas las actividades del alcance
Regional Magdalena: Avenida del Ferrocarril Carrera 12 No. 25-55	Santa Marta, Magdalena,Colombia	Todas las actividades del alcance
Regional Meta: Carrera 22 No. 10 – 73 / 89 Sur Piso 3 Barrio Doña Luz	Villavicencio – Meta Colombia	Todas las actividades del alcance
Regional Nariño: Carrera 3 A con calle 23 Esquina Barrio el Mercedario	Pasto, Nariño, Colombia	Todas las actividades del alcance
Regional Norte de	Cúcuta - Norte de Santander	Todas las actividades del alcance

Santander: Calle 5 AN Avenida 13 E Barrio San Eduardo	Colombia	
Regional Putumayo: Calle 14 No. 9 - 100 Barrio San Francisco	Mocoa – Putumayo Colombia	Todas las actividades del alcance
Regional Quindío: Carrera 23 Calles 3ra y 4ta Barrio Sesenta Casas	Armenia, Quindío, Colombia	Todas las actividades del alcance
Centro Zonal Armenia Sur. Carrera 23 Calles 3 y 4 Barrio Sesenta Casas, Armenia - Quindío	Armenia, Quindío, Colombia	Todas las actividades del alcance
Regional Risaralda Calle 35 No. 8 B - 11	Pereira,Risaralda, Colombia	Todas las actividades del alcance
Regional San Andrés: Calle 6 No. 1 - 82; Avenida Francisco Newball Barrio Los Almendros	San Andrés y Providencia - San Andrés Colombia	Todas las actividades del alcance
Regional Santander: Calle 1 N No. 16 D 86, Barrio La Juventud	Bucaramanga, Santander, Colombia	Todas las actividades del alcance
Regional Sucre: Transversal 27 C No. 27 A – 21 Urbanización Boston	Sincelejo, Sucre, Colombia	Todas las actividades del alcance
Regional Tolima: Avenida Carrera 5 No. 43-23 Frente Piscinas Olímpicas Barrio Restrepo	Ibagué – Tolima Colombia	Todas las actividades del alcance
Regional Valle: Avenida 2 Norte No. 33 - 45	Cali, Valle, Colombia	Todas las actividades del alcance

1.4. ALCANCE DE LA CERTIFICACIÓN:

Gestión y control de la seguridad de la información en las actividades asociadas a los procesos involucrados en la prestación del Servicio Público del Instituto Colombiano de Bienestar Familiar para el desarrollo y la protección integral de la primera infancia, la adolescencia, la juventud y el bienestar de las familias y comunidades colombianas asociadas a los programas del ICBF, así como propender por las actividades de tecnología de la información y telecomunicaciones (TIC). Declaración de Aplicabilidad A3.MS.DE 28/06/2022 – V11

Management and control of information security in the activities associated with the processes involved in the provision of the Public Service of the Colombian Institute of Family Welfare for the development and comprehensive protection of early childhood, adolescence, youth, and the well-being of Colombian families and communities associated with ICBF programs, as well as promoting information technology and telecommunications (ICT). Statement Applicability A3.MS.DE 28/06/2022 – V11.

1.5. CÓDIGO IAF: 36, 38	
1.6. REQUISITOS DE SISTEMA DE GESTIÓN: ISO/IEC 27001:2013	
1.7. REPRESENTANTE DE LA ORGANIZACIÓN	
Nombre:	Milton Fabian Forero Melo
Cargo:	Directora de Planeación y Control
Correo electrónico	Milton.forero@icbf.gov.co

1.8. TIPO DE AUDITORÍA:

□ **Inicial o de Otorgamiento**
X Seguimiento
□ **Renovación**
□ **Renovación (con restauración)**
□ **Renovación (anticipada)**
□ **Ampliación**
□ **Reducción**
□ **Auditoria especial (reactivación/extraordinaria)**
□ **Actualización**

Es organización multisitio: Si X No □

Auditoría combinada: Si X No □ ISO 9001:2015; ISO 14001:2015; ISO 45001:2018

Auditoría integrada: Si □ No X

1.9. Tiempo de auditoría	FECHA	Días de auditoría)
Etapa 1 (Si aplica)	NA	NA
Preparación de la auditoría y elaboración del plan	2023-06-26	1.0
Auditoria remota	NA	NA
Auditoría en sitio	2023-07-10 al 2023-07-14	7.5

1.10. EQUIPO AUDITOR	
Auditor Coordinador	NA
Auditor líder	Jairo Yobany Vargas Gordillo
Auditor	Jhoan David Coral Mejía
Experto Técnico	NA
Observador	NA

1.11. DATOS DEL CERTIFICADO DE SISTEMA DE GESTIÓN	
Fecha de aprobación inicial	SI-CER444445
Fecha de aprobación inicial	2016-01-15
Fecha de próximo vencimiento:	2024-08-16

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 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? (Se aplica solo para auditorías iniciales o de otorgamiento):
Si □ No □ NA X

3.8. Si se aplicó toma de muestra de múltiples sitios, indicar cuáles sitios permanentes se auditaron, en qué fechas:

Sitios Permanentes	Fecha de auditoría
Dirección General	2023-07-10, 11, 14
Metrópolis piso 3	2023-07-10, 11, 14
Regional Antioquia	2023-07-12

Regional Casanare	2023-07-11
Regional Risaralda:	2023-07-12
Regional Cundinamarca:	2023-07-13

3.9. ¿En el caso del Sistema de Gestión auditado están justificados los requisitos no aplicables acordes con lo requerido por el respectivo referencial?
Si □ No □ NA X Se encuentran declarados como aplicables todos los controles de la norma.

3.10. ¿Se auditaron actividades en sitios temporales o fuera del sitio de acuerdo al listado de contratos o proyectos entregado por la Organización?:
Si □ No □ NA X

3.11. ¿Es una auditoría de ampliación o reducción?
Si □ No X□

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?: Si X No □ NA □

No se encuentra de manera explícita en el alcance, sin embargo, se utiliza el desarrollo de software como apoyo a los aplicativos que se utilizan para el cumplimiento de la función misional. En el desarrollo de la auditoria se verificaron los desarrollos para los sistemas: CUENTAME y SIM. Se evidencia que la organización ha implementado los requisitos A.14 de la ISO/IEC 27001.

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 X No □

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 □ No X
En caso afirmativo, cuáles:

¿Debido a los cambios que ha reportado la Organización, se requiere aumentar el tiempo de auditoría de seguimiento?
Si □ No X

3.15. ¿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?
Si □ No □ NA X
En caso afirmativo descríbalas,

3.16. ¿Se tienen actividades, productos y servicios declarados en el alcance del certificado que han sido tercerizados con proveedores o contratistas?
Si X No □

¿En caso afirmativo, se encontraron controlados los proveedores o contratistas de estas actividades, productos y servicios?
Si X No □

En el caso en el cual la organización subcontrate el suministro de actividades, productos y servicios que hacen parte del alcance certificado, relaciónelos en la siguiente tabla:

Servicios y productos incluidos en el alcance que son proporcionados al cliente por un tercero en nombre de la organización auditada:	Proveedor:
Mesa Servicios	SELCOMP
Datacenter	IFX
Línea 145 Atendida por un BPO	IQ Outsourcing
Servicios de NOC (Network Operations Center o Centro de Operaciones de Red) y SOC (Security Operations Center o Centro de Operaciones de Seguridad).	SONDA

3.17. ¿Se presentaron, durante la auditoría, cambios que hayan impedido cumplir con el plan de auditoría inicialmente acordado con la Organización?
Si □ No X En caso afirmativo, cuáles:

3.18. ¿Existen aspectos o resultados significativos de esta auditoría, que incidan en el programa de auditoría del ciclo de certificación?

Si □ No X

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

3.20. ¿Aplica reactivación para este servicio?
Si □ No X NA □

3.21. 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.

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? Si/No
1	Numeral 10.1 b) c)	Se evidencia ajuste en los procedimiento y/o Formato de	Si

	No se evidencia análisis de causas y acciones correctivas para mitigar el incumplimiento del indicador "Cambios Emergencia vs Cambios Normales", durante el primer semestre 2022. Evidencia: Registros de seguimiento a indicadores y acciones correctivas 2022.	control de cambios en donde se incluyeron las Subcategorías de los RFC de emergencias, responsabilidades relacionadas con el PIR y periodicidad de los comités. Así mismo se evidenció la divulgación del procedimiento de cambios (DIT y áreas funcionales) y sensibilización en análisis de causas.		
2	Control A.17.1.3 No se está realizando la verificación, revisión y evaluación de la continuidad de la seguridad de la información. Evidencia: Registros de las pruebas de continuidad realizadas 24 de junio de 2022, Código: F3.P18.DE "INFORME FINAL PLAN DE CONTINUIDAD".	Se evidencia que la organización realiza pruebas de continuidad de la operación, en donde se incluye la verificación de la eficacia de las pruebas de los planes de continuidad.	Si	

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.

- Se destaca la Planeación Estratégica de Tecnología de la Información – PETI, porque identificaron las necesidades de la Institución, analizaron alternativas y definieron requisitos técnicos para lograr elaborar un Plan de IT coherente con la Entidad.
- El enfoque de las iniciativas que surgen a partir de la planeación estratégica, los informes de seguimiento al cumplimiento de la estrategia, el seguimiento a los planes de acción, los múltiples comités y el estatus de las operaciones.
- Los aplicativos SIM (Sistema de información misional) y Cuéntame, permiten llevar trazabilidad de las actividades del instituto, garantizando la seguridad de los datos y la toma decisiones.
- La disciplina en el cumplimiento gestión de capacidad, garantizan la disponibilidad de la infraestructura tecnológica.
- Se destacan las proyecciones de expansión de buenas prácticas en seguridad y políticas de seguridad de la información a nivel nacional.
- La herramienta Help people porque permiten solidez para atender los casos de soporte y para resolverlos manteniendo una interacción continua con el cliente interno y externo.
- Se destaca el monitoreo de las plataformas tecnológicas, las copias de respaldo y el seguimiento a las tareas pendientes/consignadas en los informes de gestión de la plataforma.
- En la gestión de privilegios de acceso de los usuarios se destaca el retiro de los derechos de acceso.

- La robustez de la infraestructura tecnológica (Datacenter TIER 3), proporciona condiciones importantes de estabilidad, seguridad y respaldo de los principales servicios del Instituto.
- La gestión de privilegios de acceso a: correos personales, instalación de software, redes sociales, doble factor de autenticación para office 365, entre otros, han permitido disminuir la pérdida de confidencialidad de la información.
- La gestión de los proyectos de desarrollo de software, el equipo de trabajo logrado, la metodología de diseño/desarrollo tradicional + ágil y las revisiones realizadas en los escenarios de pruebas funcionales de software y análisis de riesgos, son la clave fundamental para cumplir con los compromisos establecidos en los cronogramas de proyecto.
- El trabajo en equipo de la Secretaria General y la Dirección de Información y Tecnología en la implementación de la metodología de continuidad de negocio.
- La implementación del SIEM (Security Information and Event Management) y la metodología de gestión de incidentes.
- Se destacan los frecuentes ejercicios de ingeniería social, mediante phishing sumillado, realizadas por el Instituto, porque son una estrategia importante para evaluar la confianza de los colaboradores y el nivel de apropiación de las políticas de seguridad de la información. Se destaca porque ha contribuido con el fortalecimiento de la seguridad de la organización y la reducción del riesgo de exposición a las amenazas cibernéticas.
- El repositorio documental del sistema de gestión, porque aporta trazabilidad en la consulta de la información y a la salvaguarda bajo políticas de seguridad de la información.
- El Sistema de Gestión Integrado auditado tiene bases consistentes, que han sido cimentadas gracias a la solides de los procesos, lo cual les ha permitido alcanzar una adecuada dinámica alrededor de la prestación de los servicios, con calidad y seguridad de la información.
- Se destaca la estructura interna de la Institución para abordar los cambios y la capacidad de evaluación del cumplimiento de las políticas de seguridad de la información, procedimientos y el mejoramiento de los servicios, demuestran madurez organizacional, que basa su éxito en análisis estratégico que ayuda en la consecución de objetivos.
- La coordinación de cursos de inducción, capacitación y sensibilización en seguridad de la información, demuestran el compromiso con el mejoramiento de la competencia, el bienestar y la salud de los colaboradores.
- Los análisis de riesgos a partir de la unificación en el aplicativo Suite Vision Empresarial.
- El hecho de que las actividades de adquisiciones de bienes y servicios se base en gestión de riesgos es un aspecto destacable dado que proporciona una estructura sólida y proactiva para identificar, evaluar y mitigar los riesgos relacionados con la seguridad de la información.
- En las sedes regionales:
    - Alto nivel de conocimiento en seguridad de la información de los diferentes funcionarios de las regionales. Esto fortalece la seguridad, promueve una cultura de seguridad y contribuye al cumplimiento normativo, generando confianza en todas las interacciones con la organización.
    - El Instituto interiorizó la importancia de mantener la privacidad, confidencialidad y disponibilidad de la información de los niños, niñas y adolescentes del país, esto es relevante porque demuestra que se cumplen los objetivos misionales, pero con niveles razonables de seguridad de la información.
    - Las actividades de las sedes regionales que se apoyan en herramientas tecnológicas como One drive, Orfeo, SIM, Microsoft Teams, les ha permitido optimizar las labores de los

funcionarios y alcanzar los objetivos establecidos. Estas herramientas mejoran la eficiencia, la precisión y la seguridad en el desempeño de las tareas diarias. Al estar respaldados por herramientas tecnológicas adecuadas, los funcionarios pueden aumentar su productividad y contribuir al éxito general de la organización.

- ⊕ Se destaca el orden y aseo de cada una de las instalaciones (infraestructura física), Centros de cableado, áreas comunes y zonas de plantas eléctricas.
- ⊕ Es destacable la organización y el cumplimiento de los mantenimientos de los elementos ubicados en el centro de cableado de las sedes regionales, aspecto relevante porque permite mantener la eficiencia de las comunicaciones, reduce los tiempos de inactividad y brinda una base sólida para el crecimiento y la evolución tecnológica de la organización.
- ⊕ Contar con un responsable exclusivo de seguridad de la información es un factor clave para una gestión sólida y especializada en esta área.
- ⊕ Es un aspecto relevante la constate exploración de la solución de problemas prácticos con ayuda de la tecnología, incentivando a los funcionarios para que desde sus procesos den a conocer, las ideas y/o propuestas de innovación.
- ⊕ El trabajo de los Epicos en su rol de promotores de las buenas prácticas en el Sistema de Gestión.

4.2 Oportunidades de mejora

- Fortalecer la revisión por la dirección garantizando presentación del estado de las acciones con relación a las revisiones previas por la dirección, retro alimentación de las partes interesadas y conclusiones en términos de conveniencia, adecuación y eficacia del Sistema de Gestión de la Seguridad de la Información para que con esta información se tomen decisiones pertinentes y asertivas que garanticen los beneficios para todos los grupos de interés.
- Mejorar las distintas herramientas utilizadas y escenarios en los que se verifica la postura de seguridad de la información.
- Mejorar los indicadores de los procesos: Caso Indicadores del proceso de desarrollo de software. Ejemplo: Calidad del software, esfuerzo, desviación estándar, entre otros.
- En el proceso gestión de copias de respaldo mejorar el programa de pruebas de restauración, de manera que les permita ampliar la ejecución de las pruebas de restauración.
- A partir del monitoreo de la capacidad de las plataformas tecnológicas, adquirir herramientas que les permita realizar las proyecciones de los requisitos de capacidad futura. Mejorar ayudas gráficas.
- Al realizar las pruebas de los planes de continuidad de negocio, mejorar el registro de todas las actividades realizadas para lograr el retorno a la normalidad de la operación, a la sede principal (Consultar a manera de orientación la norma ISO/IEC 22313 Gestión de la Continuidad de Negocio. Guía de implementación).
- Mejorar el BIA (Análisis de Impacto en el Negocio). A mondo de consulta revisar la norma ISO/IEC 22317. Sistema de Gestión de Continuidad de Negocio. Directrices para el Análisis de Impacto en el Negocio.
- Mejorar la coherencia entre los escenarios de falla y las pruebas de restauración.
- Finalizar las pruebas de los planes de continuidad de negocio adicionando el retorno a la normalidad.

- Es necesario reevaluar el sistema de contingencia contra interrupciones de energía de la sede Metrópolis para evitar que la infraestructura crítica como switches e internet queden inoperantes y se garantice la continuidad del servicio.
- Apoyar las actividades del equipo de seguridad de manera que se logre mayor enfoque en labores de: asesoría en temas de seguridad de la seguridad de la información, análisis de vulnerabilidad técnica, computación forense y monitoreo de la postura de seguridad de la información.
- Aumentar la frecuencia y cobertura de realización de análisis de vulnerabilidad técnica y los retest en los servidores de la Institución. Hacer un análisis de tendencias de las vulnerabilidades más repetitivas, a fin de atacar la causa raíz de manera transversal.
- Es importante aumentar la cobertura y frecuencia de ejecución de auditorías internas en las sedes regionales, para llevar un mayor control y seguimiento a la eficacia de los controles implementados por el Instituto.
- La revisión y ajustes de procesos de auditorías internas tomando como referencia la guía ISO 19011 ayudará a fortalecer el SIGE.
- En el informe de auditoría interna: incluir fortalezas. Oportunidades de Mejora con énfasis en el para qué se debe atender la oportunidad de mejora.
- Mejorar la oportunidad en la entrega de los informes de auditoría. Así mismo auditar anualmente al menos una vez a la Dirección de Tecnología de la Información.
- Mejorar la profundidad y exigencia en la auditoría de controles, a modo de consulta revisar la norma: ISO 27008 Information technology - Security techniques Guidelines for auditors on information security controls.
- Para los indicadores que demuestran tendencia al cumplimiento reevaluar las metas a fin de obtener metas más retadoras.
- Continuar con los ejercicios de ingeniería social, de tal forma que se pueda analizar si hay debilidades de conocimiento y/ó confianza por parte de los colaboradores en distintos entornos.
- Aunque se realiza adecuado análisis de indicadores en el proceso “Relación con el Ciudadano”, es pertinente documentar en la matriz las acciones a tomar derivadas de estos análisis para brindar mayor visibilidad de la reacción oportuna ante estas métricas.
- Ampliar el alcance de las certificación del Sistema de gestión de la Seguridad de la Información del ICBF a centros zonales.
- Es pertinente incluir nuevos escenarios de riesgos para continuidad de negocio para tener un panorama global de los eventos que pueden desencadenar en impacto negativo para la regional. Por ejemplo, el escenario en que fallen las acometidas de internet.
- Revisar los tiempos y fechas límite para lograr realizar la transición a la nueva versión ISO/IEC 27001:2022. Al respecto conviene consultar el pan de transición de ICONTEC definido en la página web: https://www.icontec.org/wp-content/uploads/2023/03/PLAN-TRANSICION-ISOIEC-27001-2013-A-VERSION-2022.pdf
- Continuar mejorando la metodología de análisis de riesgos mediante la consulta de los siguientes estándares: ISO 31000, ISO 27005 y NIST SP 800-30. Así mismo mejorar la redacción en la descripción de los riesgos, evitando caer en la globalidad y/o la recopilación de más de un pilar de la seguridad en el mismo riesgo.
- En las sedes regionales:
    - Mejorar los soportes utilizados como evidencia del encendido quincenal de la planta eléctrica.

- ⊕ Es pertinente incluir nuevos escenarios de riesgos para continuidad de negocio para tener un panorama global de los eventos que pueden desencadenar en impacto negativo para la regional.
- ⊕ Es fundamental implementar mayores medidas de seguridad y rigurosidad en la disposición de información confidencial en medios físicos y en las áreas consideradas seguras. A pesar de contar con controles de monitoreo y videovigilancia en la regional, es crucial asegurar que la información documental en formato papel se custodie de manera adecuada en los espacios destinados específicamente para este propósito.

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

5.1. Análisis de la eficacia del sistema de gestión certificado

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
NA		

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

Se han registrado en el año 2023: 24 incidentes de seguridad de la información de bajo impacto. Todos los incidentes reportados han sido solucionados mediante la aplicación del procedimiento Gestión de Incidentes de Seguridad de la Información. Se tienen disposiciones para la recolección de evidencias, análisis de causas, corrección y acción correctiva a partir de los incidentes presentados.

5.1.3. 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.

5.1.4. ¿Existen quejas de usuarios de la certificación recibidas por ICONTEC durante el último periodo evaluado? (Aplica a partir del primer seguimiento)?
Si □ No X

5.1.5. ¿Se evidencia la capacidad del sistema de gestión para cumplir los requisitos aplicables y lograr los resultados esperados?:
Si X No □

Nota. Para auditorías de renovación se deben tener en cuenta quejas de terceros recibidos durante el ciclo de la certificación, los resultados de las auditorías de seguimiento del ciclo y los resultados de la presente auditoría.

5.1.6. ¿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 X No □.

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

El ciclo de certificación inicia con una auditoría de otorgamiento o renovación, a partir de esta indicar contra cuáles requisitos se han reportado no conformidades.

En el caso de renovación se deben incluir las no conformidades reportadas durante el ciclo del certificado que esta culminado (seguimiento 1, seguimiento 2 y renovación)

Auditoria	Número de no conformidades	Requisitos
Otorgamiento / **Renovación**	3	A.11.2.2, A.11.2.4.4., A.12.5.1
1ª de seguimiento del ciclo	2	10.1 b) c), 17.1.3
2ª de seguimiento del ciclo	6	A.9.1.2, A.9.2.4, A.11.1.2, A.11.1.4, A.12.4.4, A.13.1.3
Auditorias especiales (Extraordinaria, reactivación, ampliación)	NA	
	NA	
¿Se evidencia recurrencia de no conformidades detectadas en las auditorías de ICONTEC en el último ciclo de certificación? Si □ No □ NA X		

5.3 Análisis del proceso de auditoría interna

El equipo auditor fue conformado auditores competentes según los requisitos establecidos por la organización. Se cuenta con procedimiento de auditoría en donde se establecen todos los requisitos. La auditoría se orienta de acuerdo con directrices de ISO 19011. El ciclo de auditorías se realizó en el mes de marzo de 2023. El alcance y duración de la auditoría interna se considera apropiada a la naturaleza y necesidades de los sistemas de gestión, se encontró programa de auditoría, plan de auditoría, informe de auditoría y acciones correctivas.

5.4 Análisis de la revisión del sistema por la dirección

Se realizó un análisis de los requisitos establecidos en el numeral 9.3 y de los resultados de los procesos y de los compromisos establecidos por la dirección. La revisión por la dirección se realizó en el 06 de marzo de 2023. Se identificaron tópicos para el mejoramiento de los procesos y se precisaron buenas prácticas para apoyar y cimentar el crecimiento en los procesos.

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…)?

Si X No □ Página web

6.2. ¿La publicidad realizada por la Organización está de acuerdo con lo establecido en el R-PS-007 REGLAMENTO DE LA CERTIFICACIÓN ICONTEC DE SISTEMAS DE GESTIÓN y el Manual de aplicación E-GM-001 USO DE LA MARCA DE CONFORMIDAD DE LA CERTIFICACIÓN ICONTEC PARA SISTEMAS DE GESTIÓN?
Si X No □ 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?
Si □ No □ NA X

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.?
Si X No □.

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 REVISADA

¿Se presentaron no conformidades mayores? SI □ NO X

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

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

En caso afirmativo diligencie el siguiente cuadro:

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? Si/No
No conformidades mayores identificadas en esta auditoría			
	No Aplica		
No conformidades pendientes de la auditoría anterior que no se solucionaron			
	No Aplica		
No conformidades detectadas en esta auditoría que fueron cerradas			
	No Aplica		

8. RECOMENDACIÓN DEL EQUIPO AUDITOR DE ACUERDO CON EL R-PS-007				
			SI	**NO**
Se recomienda otorgar la Certificación del Sistema de Gestión				
Se recomienda mantener el alcance del certificado del Sistema de Gestión			X	
Se recomienda renovar el certificado del Sistema de Gestión				
Se recomienda renovar anticipadamente el certificado del Sistema de Gestión				
Se recomienda ampliar el alcance del certificado del Sistema de Gestión				
Se recomienda reducir el alcance del certificado				
Se recomienda reactivar el certificado				
Se recomienda actualizar el certificado del Sistema de Gestión				
Se recomienda restaurar el certificado, una vez finalice el proceso de renovación				
Se recomienda suspender el certificado				
Se recomienda cancelar el certificado				
Nombre del auditor líder: Jairo Yobany Vargas Gordillo	Fecha	2023	07	28

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	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 5	F-PS-946 ANEXO 5 ANÁLISIS DE RIESGOS DE AUDITORÍAS DE SISTEMAS DE GESTIÓN	NA
Anexo 6	Confirmación de cumplimiento de los objetivos de la auditoria con el uso de las TIC	NA
Anexo 7	Declaración de aplicación (solo para ISO 28001)	NA
Anexo 8	Verificación de riesgos y requisitos para realizar auditorías con la participación de Expertos Técnicos	NA

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 2023-07-27 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 2023-07-27.

SOLICITUD DE ACCIÓN CORRECTIVA		**No.** 1 de 6
☐ No - Conformidad Mayor ☒ No - Conformidad Menor	Norma(s): ISO/IEC 27001:2013	Requisito(s): A.9.1.2 Acceso a redes y a servicios en red

Descripción de la no conformidad:

No se evidenció restricción de acceso a sitios web libres no seguros (Caso acceso a iLovepdf.com)).

Evidencia:

Al inspeccionar el acceso a internet desde los computadores asignados a: Carolina Romero – Enlace de seguimiento a los servicios de primera infancia y María Juliana González – Enlace de asistencia técnica primera infancia, se encontró libre acceso al sitio web iLovepdf.com.

Corrección	**Evidencia de Implementación**	**Fecha**
Realizar configuración para inhabilitar el acceso a la página https://www.ilovepdf.com/	Informe ejecutivo con las actividades y pruebas realizadas.	30/12/2023

Descripción de la (s) causas (s) porques? Espina de pescado

- El ICBF mediante memorando 20201230000120903 del 25/08/2020 y Resolución 5360 de 30/06/2023, solicita que la información de los documentos requeridos por tipo de contrato o modalidad de atención sea entregada en un solo documento PDF, lo cual ocasiona que los colaboradores accedan a ILOVE PDF para unificar los documentos.

- Falta de recursos para adquirir el licenciamiento requerido que permita cubrir las necesidades de la entidad en lo relacionado con la Suite de Adobe que tiene la funcionalidad de unificar PDF.
- La Entidad no cuenta con la cantidad de licencias suficientes de la Suite Adobe que permiten unificar PDF, para otorgar a todos los colaboradores.

Acciones correctivas	**Evidencia de Implementación**	**Fecha**

1. Verificar alternativas de software (licenciados u open source) que nos permita cubrir la necesidad que tiene la entidad de unificar PDF.	Acta de reunión con los resultados de la verificación de las alternativas de software (licenciados u open source).	30/10/2023
2. Realizar análisis de vulnerabilidades a los software seleccionados y socializarlas al nivel Directivo para la toma de decisiones conforme a las necesidades y capacidades que tiene el ICBF.	Acta de reunión donde se evidencie la decisión tomada y las actividades a ejecutar para el despliegue del software. - En caso de que sea la decisión la utilización de Open Source se debe identificar el riesgo asociado a su uso. - En caso de que sea software licenciado se debe solicitar la inclusión en el plan de compras para la vigencia 2024.	30/11/2023
3. Realizar capacitación del uso del software seleccionado a los colaboradores del ICBF y al personal de la mesa de servicios.	listados de asistencia de Microsoft Teams, correos electrónicos y presentación en Power Point.	30/12/2023
4. Realizar despliegue del software a los equipos de cómputo de la entidad.	Informe ejecutivo con las actividades y pruebas realizadas.	30/12/2023
5. Realizar la inclusión en el inventario del software seleccionado.	Listados de asistencia de Microsoft Teams, correos electrónicos y presentación en Power Point.	30/12/2023
6. Hacer seguimiento al cumplimiento de estas acciones en la reunión con el oficial de Seguridad de la Información.	Actas de reunión	30/12/2023

SOLICITUD DE ACCIÓN CORRECTIVA		No. 2 de 6
[ ] No - Conformidad Mayor [x] No - Conformidad Menor	Norma(s): ISO/IEC 27001:2013	Requisito(s): A.9.2.4 Gestión de información de autenticación secreta de usuarios

Descripción de la no conformidad:

No se está ejecutando el control de autenticación secreta de usuarios, en el navegador Microsoft Edge.

Evidencia:

En el equipo de cómputo identificado como 11SJQ perteneciente al área administrativa de la Regional Risaralda, se logró evidenciar que se guardan de manera permanente credenciales de acceso a portales web en el navegador Microsoft Edge, lo cual contraviene la política de asignación de información de autenticación secreta

Corrección	Evidencia de Implementación	Fecha
1. Eliminar del navegador Microsoft Edge del equipo de cómputo 11SJQ las credenciales de acceso guardas en el mismo.	Informe ejecutivo que relacione las actividades de eliminación y verificación de que el usuario ya no tiene en los navegadores credenciales de acceso almacenadas.	30/08/2023

Descripción de la (s) causas (s) porques? Espina de pescado

- No se cuenta con una política de dominio que impida el almacenamiento de credenciales de acceso en los navegadores por parte de los usuarios, atendiendo que la entidad no tiene un software para el almacenamiento de contraseñas.
- Falta de apropiación de los usuarios en el manejo de la información de sus credenciales de acceso y los riesgos que se derivan de su mal uso.
- Los navegadores tienen la opción para activar el almacenamiento de credenciales de acceso a los sitios que navegan.

Acciones correctivas	Evidencia de Implementación	Fecha
1. Realizar mesas técnicas con el fin de definir una estrategia mediante Directorio activo que impida el almacenamiento de credenciales de acceso en los navegadores por parte de los usuarios.	Acta de reunión con los resultados de la validación de la estrategia.	29/09/2023
2. Implementar la estrategia que impida el almacenamiento de credenciales de acceso en los navegadores.	Informe ejecutivo con las actividades y pruebas realizadas.	31/10/2023
3. Planear y ejecutar una estrategia que permita fortalecer la apropiación de los colaboradores en el manejo de sus credenciales de acceso.	Soportes actividades que se generen en el marco del plan de cambio y cultura.	30/11/2023
4. Incluir y verificar mediante el POSIGE del SGSI, que no se almacenen las credenciales de acceso en los	Soportes remitidos en cumplimiento de la actividad	30/05/2024

navegadores por parte de los usuarios en los equipos de cómputo institucionales.	del POSIGE definida para el 2024.	
5. Hacer seguimiento al cumplimiento de estas acciones en la reunión con el Oficial de Seguridad de la Información.	Actas de reunión	30/05/2024

SOLICITUD DE ACCIÓN CORRECTIVA	No. 3 de 6

☐ No - Conformidad Mayor ☒ No - Conformidad Menor	Norma(s): ISO/IEC 27001:2013	Requisito(s): **A.11.1.2 Controles de acceso físicos**

Descripción de la no conformidad:

No se está realizando estricto control de acceso físico a las áreas consideradas seguras.

Evidencia:

Se logró ingresar a la oficina de archivo documental ubicada en el primer piso de la Regional Casanare, sin control de acceso físico, ni evidencia de acceso, teniendo en cuenta que se encuentra demarcada como área segura por el tipo de información que se custodia.

Corrección	Evidencia de Implementación	Fecha
Trasladar el archivo físico ubicado en la oficina 48 a las instalaciones del archivo de gestión del grupo de asistencia técnica de la Regional Casanare.	Informe ejecutivo con las actividades realizadas.	**30/08/2023**

Descripción de la (s) causas (s) porques? Espina de pescado

- Falta de implementación y seguimiento de controles para la custodia y protección de la información física de las áreas seguras.
- Falta de conciencia de los colaboradores en la custodia y ubicación de los activos de información.
- Acumulación de activos de información en áreas seguras por alta rotación de expedientes y no verificar cuales de estos deben trasladarse a las instalaciones del archivo de gestión.

Acciones correctivas	Evidencia de Implementación	Fecha
1. Realizar diagnóstico de los controles de seguridad física de las áreas seguras identificadas en la Regional Casanare, que se encuentran registradas en el formato F2.G10.GTI "Formato de identificación de áreas seguras a nivel nacional", con el fin de validar las mejoras en la implementación de estos.	Informe ejecutivo con los resultados del diagnóstico de áreas seguras.	30/09/2023
2. Actualizar el formato F2.G10.GTI "Formato de identificación de áreas seguras a nivel nacional" como resultado del ejercicio de diagnóstico realizado por la regional.	Formato actualizado F2.G10.GTI "Formato de identificación de áreas seguras a nivel nacional".	10/11/2023
3. Identificar los activos de información de baja rotación para el traslado a las instalaciones del archivo de gestión del Grupo de Asistencia Técnica y Grupo Jurídico de la Regional Casanare y definir el protocolo para su gestión.	Actas de reunión.	30/12/2023
4. Aplicar el protocolo definido para la gestión de los activos y verificar que se efectúen los traslados a las instalaciones del archivo de gestión del Grupo de Asistencia Técnica y Grupo Jurídico de la Regional Casanare.	Actas de reunión.	29/03/2024
5. Implementar las mejoras identificadas en el diagnóstico realizado a los controles de las áreas seguras según corresponda, aplicando los controles de seguridad física	Informe ejecutivo con las mejoras implementadas.	30/04/2024

definidas en la Política de Seguridad y Privacidad de la información.		
6. Sensibilizar a los colaboradores sobre la custodia de los activos de información conforme a lo establecido en la Política de Seguridad y Privacidad de la Información y aplicar Instrumentos de medición que permita determinar el nivel de apropiación.	Listados de asistencia, presentación, instrumentos de medición e informe de medición.	29/03/2024
7. Hacer seguimiento al cumplimiento de estas acciones en la reunión con el oficial de Seguridad de la Información.	Actas de reunión	15/04/2023

SOLICITUD DE ACCIÓN CORRECTIVA	No. 4 de 6

☐ No - Conformidad Mayor	Norma(s): ISO/IEC 27001:2013	Requisito(s):
x No - Conformidad Menor		A.11.1.4 Protección contra amenazas externas y ambientales

Descripción de la no conformidad:

No se evidencia que se diseña y aplica protección física contra amenazas externas, ataques maliciosos o accidentes en el cuarto de la planta eléctrica (ubicada en el sótano del edificio) y la zona de UPS Grupo Jurídico, (ubicado en el piso 3), de la Regional Cundinamarca.

Evidencia:

En el cuarto de la planta eléctrica de 150 KVA se encontraron cajas de cartón en el piso y en el Grupo Jurídico, ubicado en el piso 3, de la Regional Cundinamarca, se encontraron cajas con documentos cerca de las UPS.

Corrección	Evidencia de Implementación	Fecha
Retirar el material inflamable que se ubica cerca de la Planta Eléctrica y la UPS del tercer piso (Grupo Jurídico).	Acta de reunión donde se relacionan las actividades del retiro del material inflamable cerca de la UPS y Planta Eléctrica.	30/08/2023

Descripción de la (s) causas (s) porques? Espina de pescado

- Desconocimiento por parte de los colaboradores sobre los riesgos asociados a la ubicación de material inflamable (Cajas de Cartón y archivo de gestión) cerca de las UPS y Planta Eléctrica.
- El personal operario que realizó el mantenimiento a la Planta eléctrica, por descuido no retiró del cuarto donde se ubica esta infraestructura el material inflamable que utilizó para sus actividades.
- Falta de verificación por parte de la Regional de las zonas donde se ubican las UPS y planta eléctrica para validar que no tengan cerca materiales inflamables

Acciones correctivas	Evidencia de Implementación	Fecha
1. Sensibilizar a los colaboradores de la Regional sobre el riesgo que representa la ubicación de elementos inflamables cerca de las UPS y planta eléctrica, recomendando la aplicación de buenas prácticas asociadas a los Ejes de Seguridad de la Información, Ambiental y Seguridad y Salud en el Trabajo, aplicando Instrumentos de medición que permitan determinar el nivel de apropiación.	Encuesta de medición de la sensibilización, piezas gráficas, listados de asistencia y presentación.	30/10/2023
2. Socializar a los operarios que realizan mantenimiento a la Planta Eléctrica sobre el riesgo que representa la ubicación de elementos inflamables cerca de plantas eléctricas.	Listados de asistencia y presentación.	30/10/2023
3. Realizar inspección quincenal a las instalaciones de la Sede Regional con el fin de evidenciar la aplicación	Informe ejecutivo.	30/11/2023

de buenas prácticas asociadas a los Ejes de Seguridad de la Información, Ambiental y Seguridad y Salud en el Trabajo.		
4. Hacer seguimiento al cumplimiento de estas acciones en la reunión con el oficial de Seguridad de la Información.	Actas de reunión	15/12/2023

SOLICITUD DE ACCIÓN CORRECTIVA	No. 5 de 6

☐ No - Conformidad Mayor ☒ No - Conformidad Menor	Norma(s): ISO/IEC 27001:2013	Requisito(s): A.12.4.4 Sincronización de relojes

Descripción de la no conformidad:

No se evidencia que los relojes de todos los sistemas de procesamiento de información, pertinentes dentro de la Entidad o ámbito de seguridad se encuentran sincronizados con una única fuente de referencia de tiempo.

Evidencia:

No se encuentran sincronizados los relojes de los siguientes dispositivos con la hora legal colombiana en:
Sede principal:

- UPS de 200 Kva de centro de cómputo, 37 minutos de diferencia.
- Aire acondicionado marca CANTAL ubicado en el centro de cómputo, 4 horas de diferencia.
- CCTV interno de centro de cómputo, 1 minuto de diferencia.

Regional Antioquia:

- UPS marca PowerSun ubicada en cuarto de UPS, 3 minutos de diferencia.
- Sistema de alarmas ubicado en la bodega, 8 minutos de diferencia.

Corrección	Evidencia de Implementación	Fecha
1. Sincronizar la hora de la UPS de 200 Kva, el aire acondicionado marca CANTAL y el CCTV interno de centro de cómputo con la hora legal.	Informe ejecutivo que relacione las actividades de sincronización de los relojes de la UPS de 200 Kva, el aire acondicionado marca CANTAL y el CCTV interno de centro de cómputo con la hora legal.	30/08/2023
2. Sincronizar la hora de la UPS marca PowerSun del cuarto de cableado y el Sistema de alarmas ubicado en la bodega con la hora legal de Colombia.	Informe ejecutivo que relacione las actividades de sincronización de los relojes de la UPS marca PowerSun del cuarto de cableado y el Sistema de alarmas ubicado en la bodega con la hora legal de Colombia.	30/08/2023

Descripción de la (s) causas (s) porques? Espina de pescado

- Falta de monitoreo de la sincronización de relojes de los dispositivos por parte de los ingenieros regionales, proveedores de tecnología y el operador de servicios de vigilancia.
- No existe una conexión directa al servidor NTP de los dispositivos.
- No está incluida como actividad del POSIGE del Sistema de Gestión de Seguridad de la Información, el seguimiento y monitoreo a la sincronización de los relojes de los dispositivos de procesamiento de información.

Acciones correctivas	Evidencia de Implementación	Fecha

1. Diseñar un Formato que permita registrar el monitoreo, seguimiento y control de la hora de las UPS, alarmas, equipos de cómputo, CCTV y aires acondicionados.	Formato de Registro de monitoreo y seguimiento publicado en el portal web.	30/11/2023
2. Verificar que dispositivos pueden sincronizarse de forma automática con la hora legal de Colombia, y para estos realizar las configuraciones pertinentes en el caso que aplique.	Informe ejecutivo con la verificación y actividades realizadas de sincronización.	30/10/2023
3. Incluir en el Plan Operativo del SGSI la revisión de la sincronización de relojes de UPS, telefonía IP, equipos de cómputo, aires acondicionados y sistemas de alarmas.	Plan operativo del SGSI aprobado y remitido a los Ingenieros Regionales.	29/03/2024
4. Aplicar el formato de Registro de monitoreo, seguimiento y control de la hora, para verificar su sincronización en las UPS, alarmas, equipos de cómputo, CCTV y aires acondicionados. En caso de que los ingenieros Regionales no puedan realizar la configuración manual de la hora, deberán realizar el escalamiento del requerimiento a la mesa informática de soluciones.	Formato de registro de monitoreo, seguimiento y control de la hora y en caso de ser necesario los Ticket a MIS.	31/05/2024
5. Definir un cronograma de monitoreo de la sincronización de los dispositivos ubicados en los centros de cómputo y la UPS que son administrados por el proveedor de servicios tecnológicos.	Acta de reunión en la cual se establezca el cronograma.	30/11/2023
6. Verificar el cumplimiento de cronograma de monitoreo de la sincronización de los dispositivos UPS por parte del proveedor de servicios tecnológicos, realizando los ajustes que correspondan a los dispositivos que no estén sincronizados con la hora legal de Colombia.	Formatos de Registro de monitoreo, seguimiento y control de la hora.	31/05/2024
7. Hacer seguimiento al cumplimiento de estas acciones en la reunión con el oficial de Seguridad de la Información.	Actas de seguimiento	31/05/2024

SOLICITUD DE ACCIÓN CORRECTIVA	No. 6 de 6

☐ No - Conformidad Mayor ☒ No - Conformidad Menor	Norma(s): ISO/IEC 27001:2013	Requisito(s): A.13.1.3 Separación en las redes

Descripción de la no conformidad:

No se evidencia que los grupos de servicios de información, redes de usuarios visitantes y sistemas de información se separan en redes seguras en las Regionales: Risaralda y Casanare.

Evidencia:

- Se logra establecer vinculo vía wifi mediante ping desde el SSID visitantes, a equipos de cómputo de la red LAN de la Regional Risaralda, lo cual representa un riesgo latente de ataques como escaneo de puertos o fuga de información.

- Equipo de cómputo identificado como 5411ZC9 de G58 de la Regional Casanare permite conexión vía wifi a modem 4g, lo cual contraviene el control de navegación establecido por el Instituto.

Corrección	Evidencia de Implementación	Fecha
No aplica	**No aplica**	**No aplica**

Descripción de la (s) causas (s) porques? Espina de pescado

- No están restringidas las conexiones inalámbricas a redes externas del ICBF en algunos equipos institucionales, porque no se cuenta con un control para esto y no están definidas claramente las políticas de uso de los dispositivos MIFI.
- Los switches de acceso y controladoras de acceso point no permiten aislar las VLANs debido a su obsolescencia.
- Se cuenta con switches y acces point de diferentes características técnicas, lo que obliga a desagregar su control.

Acciones correctivas	Evidencia de Implementación	Fecha
1. Realizar mesas técnicas con el fin de definir una estrategia de segmentación de todos los dispositivos de acces point, desde el Firewall principal del ICBF.	Acta de reunión con los resultados de la verificación de la validación de estrategia.	15/11/2023
2. Realizar sesiones técnicas con el fin de validar la implementación de un portal cautivo centralizado.	Acta de reunión con los resultados de las sesiones técnicas.	15/11/2023
3. Gestionar la inclusión de un NAC en la Ficha de Condiciones de Técnicas para el servicio de seguridad perimetral del ICBF.	Correos electrónicos que demuestren la gestión y/o la Ficha de Condiciones Técnicas que relacione este tema.	30/09/2023
4. Implementar la estrategia de segmentación definida conforme a las mesas técnicas adelantadas.	Informe ejecutivo con las actividades y pruebas realizadas.	30/03/2024
5. Revisar y actualizar las políticas de uso de los dispositivos MIFI en la documentación del Sistema de Gestión de Seguridad de la Información.	Documentos controlados del Sistema de Gestión de Seguridad de la Información que describen	30/11/2023

	las políticas del uso de dispositivos MIFI (Guía de Navegación, Política de Seguridad y Privacidad de la Información).	
6. Definir un único formato para la entrega de los dispositivos MIFI a nivel nacional, que relacione las políticas de uso las cuales deben cumplir los colaboradores.	Formato de entrega de los dispositivos MIFI.	30/11/2023
7. Realizar mesas técnicas para validar si es posible restringir y controlar mediante el antivirus la conexión de dispositivos MIFI.	Acta de reunión con los resultados de las mesas técnicas.	15/12/2023
8. Incluir y verificar mediante el POSIGE del SGSI el cumplimiento de las políticas de uso de dispositivos MIFI y la implementación de la estrategia de segmentación.	Soportes remitidos en cumplimiento de la actividad del POSIGE definida para el 2024.	30/05/2024
9. Hacer seguimiento al cumplimiento de estas acciones en la reunión con el oficial de Seguridad de la Información.	Actas de seguimiento	31/05/2024

ANEXO 2

INFORMACIÓN ESPECÍFICA DE ESQUEMAS DE CERTIFICACIÓN DE SISTEMA DE GESTIÓN

Sistema de gestión de seguridad de la información ISO/IEC 27001
Sistema de gestión de privacidad de la información ISO/IEC 27701

Marque con una X si el sistema de gestión auditado.

ISO/IEC 27001 X
ISO/IEC 27001 + ISO/IEC 27701 □

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:
a) 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;
b) Las comunicaciones de las partes externas como es requerido por la norma ISO/IEC 27001 e ISO/IEC 27701;
c) Los cambios en la documentación del SGSI/SGPI;
d) Las zonas sujetas a cambio;
e) los requisitos de la norma ISO/IEC 27001 e ISO/IEC 27701 cuando sea aplicable.

Actividades desarrolladas

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

- ¿Se modificó la declaración de aplicabilidad?
  Si □ No X
  Si aplica, mencionar el cambio y la versión (Asegúrese de colocar la declaración de aplicabilidad vigente en el alcance de la certificación) en la siguiente tabla:

VERSIÓN VIGENTE:	JUSTIFICACIÓN DEL CAMBIO
Declaración de Aplicabilidad A3.MS.DE 28/06/2022 – V11	No Aplica

- ¿Los procedimientos adoptados por el cliente brindan confianza en el SGSI/ SGPI?
  Si X No □
  Si la respuesta es NO, se debe justificar porque no brindan confianza

- Describa brevemente los documentos revisados como evidencia de las muestras tomadas para la evaluación del SGSI/ SGPI (Ver PE-PS-079 PROCEDIMIENTO ESPECIFICO PARA CERTIFICACION ISO/IEC 27001 y el PE-PS-133 PROCEDIMIENTO ESPECIFICO PARA LA GESTION DE LA PRIVACIDAD DE LA INFORMACION ISO/IEC 27701).

  Se revisaron los documentos concernientes a: Políticas de seguridad de la información, Registro de incidentes o eventos de seguridad, 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, Capacitación de seguridad de la información, Declaración de aplicabilidad, Formato identificación de perfiles a colaboradores, Gestión de vulnerabilidades, Identificación y análisis de riesgos, Identificación, clasificación y valoración de activos de información, Incidentes de seguridad, Inventario de activos de información, Manual identificación, clasificación y valoración de activos de información, Manual 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, Registro de incidentes o eventos de seguridad, Registro de revisiones de perfiles a colaboradores, Registro de vulnerabilidades, Revisión de cuentas desactivadas de usuarios retirados, Revisión física de equipos de cómputo y Roles de seguridad de la información.

Análisis de la eficacia del sistema de gestión certificado

- Describa brevemente el análisis de riesgos, de la revisión de los planes de tratamiento y del riesgo residual (Ver PE-PS-079 y PE-PS-133).

  - En el año 2023 en total se registraron 82 riesgos de seguridad de la información. Se evidenciaron los correspondientes planes de tratamiento del riesgo. Los dueños del riesgo identifican los riesgos y registran la aprobación de los riesgos inherentes y el riesgo residual de manera estandarizada.
  - La herramienta utilizada es: Suite Visión Empresarial.
  - La metodología de análisis de riesgos se destaca por su alcance, cobertura y por la constante participación de todos los líderes de los procesos. Los dueños del riesgo identifican los riesgos y registran la aprobación de los riesgos inherentes y el riesgo residual de manera estandarizada.
  - En el riesgo residual, la gestión de los 406 planes de tratamiento del riesgo se realiza a través de planes de acciones claramente definidos, con responsables y recursos asociados.

ANEXO 3

PLAN DE AUDITORÍA

EMPRESA:	**INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR**		
Dirección del sitio:	Avenida Carrera 68 No 64C – 75 Bogotá D.C, Colombia		
Representante de la organización:	MILTON FABIAN FORERO MELO		
Cargo:	Director	Correo electrónico	Milton.forero@icbf.gov.co
Alcance de la certificación: Gestión y control de la seguridad de la información en las actividades asociadas a los procesos involucrados en la prestación del Servicio Público del Instituto Colombiano de Bienestar Familiar para el desarrollo y la protección integral de la primera infancia, la adolescencia, la juventud y el bienestar de las familias y comunidades colombianas asociadas a los programas del ICBF, así como propender por las actividades de tecnología de la información y telecomunicaciones (TIC). Declaración de Aplicabilidad A3.MS. 28/06/2022 –V.11			
Alcance de la auditoría: Gestión y control de la seguridad de la información en las actividades asociadas a los procesos involucrados en la prestación del Servicio Público del Instituto Colombiano de Bienestar Familiar para el desarrollo y la protección integral de la primera infancia, la adolescencia, la juventud y el bienestar de las familias y comunidades colombianas asociadas a los programas del ICBF, así como propender por las actividades de tecnología de la información y telecomunicaciones (TIC). Declaración de Aplicabilidad A3.MS. 28/06/2022 –V.11			
Criterios de Auditoría	**ISO/IEC 27001:2013** + la documentación del Sistema de Gestión.		
Tipo de auditoría: □ Inicial u otorgamiento **X Seguimiento** □ Renovación □ **Ampliación** □ Reducción □ Auditorias especiales (Reactivación/extraordinaria) □ Extraordinaria □ Actualización / Migración □ Renovación (con restauración) □ Renovación (anticipada)			
Modalidad: **X Auditoría en sitio** □ Auditoria parcialmente remota □ Auditoría totalmente remota			
Aplica toma de muestra por multisitio:	**X Si** **No** □		
Sitio(s) a ser muestreado(s) en la presente auditoria:	Actividades del sistema de gestión/alcance a auditar en cada sitio durante la presente auditoría:		
Dirección General: Avenida Carrera 68 No 64C – 75 Bogotá D.C, Colombia	Todas las actividades del alcance		

Metrópolis: Av. 68 # 75 a – 50 piso 3 Sede Metrópolis, Bogotá D.C., Cundinamarca,Colombia	Gestión de la Tecnologías deinformación y comunicaciones
Regional Antioquia: Calle 45 No. 79 - 141 Medellín, Antioquia, Colombia	Todas las actividades del alcance
Regional Casanare: Diagonal 9 No. 8 – 85 Barrio Luz María Jiménez, Yopal, Casanare, Colombia	Todas las actividades del alcance
Regional Risaralda: Calle 35 No. 8 B – 11, Pereira, Risaralda, Colombia	Todas las actividades del alcance
Regional Cundinamarca: Calle 47 No. 91 – 68 Barrio La Castellana, Bogotá, D.C. – Cundinamarca, Colombia	Todas las actividades del alcance
Existen actividades/procesos que requieran ser auditadas en turno nocturno:	□ Si **X 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 se encuentran indicadas en el R-PS-007 REGLAMENTO DE LA CERTIFICACIÓN ICONTEC DE SISTEMAS DE GESTIÓN.

Auditor Líder:	Yobany Vargas G.- YVG	Correo electrónico	jvargas@icontec.net +57 3114467103
Auditor:	Jhoan David Coral Mejía - JDC	Correo electrónico	jcoral@icontec.org 3158332424
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)
DIA 1					
2023/07/10 Dirección General: Avenida Carrera 68 No 64C – 75 Bogotá	08:00	08:30	Reunión de apertura	YVG/JDC	**Director de Información y Tecnología** Jose Ebert Bonilla Olaya **Coordinador Equipo Seguridad de la Información (Contratista)** Astrid Vannessa Castro Cortes **Equipo SGSI (Contratista)** Teresa Quilindo Sarasti **Promotor EPICO de la DIT (Contratista)** Luis Felipe Garcia Forero
	08:30	10:30	Direccionamiento Estratégico y Revisión por la Dirección 4. Contexto de la Organización 5. Liderazgo 6.2 Objetivos de seguridad de la información. 9.1 Seguimiento y medición 9.3 Revisión por la dirección 10.1 No conformidades y acciones correctivas 10.2 Mejora continua	YVG	**Director de Información y Tecnología** Jose Ebert Bonilla Olaya **Contratistas SMO** Maria Fernanda Heron (SMO) Giovanna Bazanni (SMO) Diana Victoria López (SMO) Mariluz Quintero (SMO) **Coordinador Equipo Seguridad de la Información (Contratista)** Astrid Vannessa Castro Cortes **Promotor EPICO de la DIT (Contratista)** Luis Felipe Garcia Forero
	10:30	12:30	Gestión Humana	YVG	**Director de Gestión Humana** Daniel Antonio Estrada Montes

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)
			5.3 Roles, responsabilidades y autoridades 7.1 Recursos, 7.2 Competencia, 7.3 Toma de Conciencia, 7.4 Comunicación, y A.7 Seguridad de los recursos humanos		**Promotora EPICO Dirección Gestión Humana (Contratista)** Neyffe Patricia Gamboa Ovalle **Equipo SGSI (Contratista)** Teresa Quilindo Sarasti
	08:30	11:00	Seguridad Física A.11 Seguridad física y del entorno. Verificación del centro de monitoreo. Verificación Datacenter Principal. Revisión de los diseños de seguridad.	JDC	**Contratista Subdirección de Recursos Tecnológicos** Lizeth Tatiana Ardila Otero **Equipo SGSI (Contratista)** Teresa Quilindo Sarasti
Metrópolis	11:00	12:30	Relación con el Ciudadano A.6.2.2 Teletrabajo, 8.1 Planificación y control operacional, A.8.2.3 Manejo de activos, A.8.3.1 Gestión de medios removibles A.9 Control de Acceso, A.12.1 Procedimientos operacionales y responsabilidades.	JDC	**Directora de Servicios y Atención** Ingrid Johanna Cubides Puentes Ingrid.Cubides@icbf.gov.co **Coordinadora Grupo de Canales** Lina Margarita Perez Arango Lina.Perez@icbf.gov.co **Profesional Especializado Grupo Gestión de Calidad para el Servicio y la Atención** Edna Nino Vargas Edna.Nino@icbf.gov.co **G-58 (Contratista)** Christian Felipe Gelvez Torres Christian.Gelvez@icbf.gov.co

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)
					Promotor EPICO (Contratista) Oscar Javier Bernal Parra Oscar.Bernal@icbf.gov.co **Ingeniero Leonardo Castillo Leon (Contratista)** Leonardo.Castillo@icbf.gov.co
	12:30	13:30	Receso	YVG	
Metrópolis	13:30	15:00	Evaluación Independiente 6.1 Acciones para abordar riesgos y oportunidades 7.5 Información documentada 8.2 Valoración de riesgos de la seguridad de la información 8.3 Tratamiento de riesgos de la seguridad de la información 9.2 Auditoría Interna	YVG	**Jefe Oficina de Control Interno** Yanira Villamil Suzunaga **Promotor EPICO de Control Interno (Contratista)** Andres Fernando Muñoz Salazar **Coordinador Equipo Seguridad de la Información (Contratista)** Astrid Vannessa Castro Cortes

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)
Metrópolis	15:00	16:30	Mejoramiento Requisitos ISO 27001 9.1 Seguimiento, medición, análisis y evaluación, 10. Mejora *Cierre de no conformidades menores de la auditoria anterior*	YVG	**Coordinador Equipo Seguridad de la Información (Contratista)** Astrid Vannessa Castro Cortes **Promotor EPICO de la DIT (Contratista)** Luis Felipe Garcia Forero
	14:30	16:30	Adquisición de Bienes y Servicios 8.1 Planificación y control operacional 9.1 Seguimiento análisis y evaluación A.15 Relación con los proveedores.	JDC	**Director de Abastecimiento** Luis Fernando Duque Venegas **Contratista Promotor EPICO (Dirección de Abastecimiento)** Ana Milena Bustos Sánchez **Director de Contratación** Kerly Jazmin Agamez Berrio **Contratista Promotor EPICO (Dirección de Contratación)** Nelcy Stefany Parra Mora **Equipo SGSI (Contratista)** Teresa Quilindo Sarasti
	16:30	17:00	Balance diario	YVG/JDC	**Director de Información y Tecnología** Jose Ebert Bonilla Olaya **Coordinador Equipo Seguridad de la Información (Contratista)** Astrid Vannessa Castro Cortes **Equipo SGSI (Contratista)** Teresa Quilindo Sarasti
DIA 2					

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)
2023/07/11 Dirección General/ Metrópolis	08:30	12:30	Gestión de la tecnología y de la información A.5 Políticas de la seguridad de la información (Planeación estratégica de Tecnología) A.6 Organización de la seguridad de la información. A.8 Gestión de Activos, inventario y devoluciones. Clasificación de la información. A.9 Control de Acceso. A.10 Criptografía. A.11.2 Seguridad de los equipos A.12 Seguridad de las operaciones. A.13 Seguridad de las comunicaciones.	YVG	**Subdirectora de Recursos Tecnológicos** Rubby Ligia Clavijo Torres **Coordinador Equipo Seguridad de la Información (Contratista)** Astrid Vannessa Castro Cortes **Equipo SGSI (Contratista)** Teresa Quilindo Sarasti **Especialistas de la Subdirección de Recursos Tecnológicos**
	12:30	13:30	Receso		
Metrópolis	13:30	16:30	Gestión de la tecnología y de la información A.12.6 Gestión de vulnerabilidades técnicas. A.16 Análisis de incidentes de seguridad A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio. A.18 Cumplimiento	YVG	**Subdirectora de Recursos Tecnológicos** Rubby Ligia Clavijo Torres **Ingeniero SRT (Contratista)** Fabio Alexander Triana Caro **Secretaría General (Contratista)** Claudia Milena Garces **Coordinador Equipo Seguridad de la Información (Contratista)** Astrid Vannessa Castro Cortes

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)
					Equipo SGSI (Contratista) Teresa Quilindo Sarasti
	16:30	17:00	Balance Diario	YVG	**Director de Información y Tecnología** Jose Ebert Bonilla Olaya **Coordinador Equipo Seguridad de la Información (Contratista)** Astrid Vannessa Castro Cortes **Equipo SGSI (Contratista)** Teresa Quilindo Sarasti
2023/07/11 Regional Casanare	08:00	08:30	Reunión Introductoria	JDC	**Director Regional** Josue David Parales Giron **Coordinador Asistencia Técnica** Sandra Milena González **Coordinadora Administrativa** Margareth Ortiz Rubio **Coordinador Financiero** William Irenarco Benavides Martinez **Ingeniero Regional SGSI (Contratista)** Eymar Silva Meza **Ingeniero regional (Contratista)** Willmar Arbey Suarez Rodriguez

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)
					Referente calidad (Contratista) Diana Marcela Lopez Arias
	08:30	09:00	Recorrido por la sede A.11 Seguridad física y del entorno	JDC	**Director Regional** Josue David Parales Giron **Ingeniero Regional SGSI (Contratista)** Eymar Silva Meza **Ingeniero regional (Contratista)** Willmar Arbey Suarez Rodriguez **Contratista Grupo Administrativo** Camilo Andrés Luna
	09:00	12:00	Revisión tecnología utilizada en la prestación del servicio. A.9 Control de acceso A.11 Seguridad física y del entorno A.12 Seguridad de las Operaciones A.13 Seguridad de las comunicaciones A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio.	JDC	**Director Regional** Josue David Parales Giron **Ingeniero Regional SGSI (Contratista)** Eymar Silva Meza **Ingeniero regional (Contratista)** Willmar Arbey Suarez Rodriguez
	12:00	13:30	Receso	JDC	
	13:30	16:00	Protección (Adopciones) A.6.2.2 Teletrabajo A. 8.1 Responsabilidad por los activos A.8.2.3 Uso aceptables de los activos	JDC	**Director Regional** Josue David Parales Giron **Coordinadora Asistencia Técnica** Sandra Milena Gonzalez Cárdenas

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)
			A.8.3.1 Gestión de medios removibles A.9 Control de acceso A.12.2 Controles contra códigos maliciosos		**Defensora de Familia Secretaria Comité de Adopciones** Herli Lucero Rivera Gomez **Trabajadora Social Adopciones** Mayerlid Tatiana Bustos Origua **Ingeniero Regional SGSI (Contratista)** Eymar Silva Meza
	16:00	17:00	Reunión de cierre diario	JDC	**Director Regional** Josue David Parales Giron **Coordinador Asistencia Técnica** Sandra Milena González **Coordinadora Administrativa** Margareth Ortiz Rubio **Coordinador Financiero** William Irenarco Benavides Martinez **Ingeniero Regional SGSI (Contratista)** Eymar Silva Meza **Ingeniero Regional (Contratista)** Willmar Arbey Suarez Rodriguez
DIA 3					

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)
2023/07/12 Regional Risaralda	08:00	08:30	Reunión Introductoria	JDC	**Directora Regional** Claudia Patricia Serna Gallego **Coordinadora Grupo de Planeación y Sistemas** Olga Inés Botero Duque **Coordinador Grupo Administrativo** Juan Antonio Carvajal Echavarria. **Coordinadora Grupo Jurídico** Ledia del Pilar Giraldo Ossa **Coordinadora Grupo de Asistencia Técnica** Maria Nydia Henao Castaño **Ingeniera Regional Referente SGSI (Contratista)** Dolly Cuero Angulo **Ingeniero Regional Enlace DIT (Contratista)** Gustavo Alegría Pino
	08:30	09:00	Recorrido por la sede A.11 Seguridad física y del entorno	JDC	**Coordinadora Grupo de Planeación y Sistemas** Olga Inés Botero Duque **Ingeniera Regional Referente SGSI (Contratista)** Dolly Cuero Angulo **Ingeniero Regional Enlace DIT (Contratista)** Gustavo Alegría Pino

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)
	09:00	10:30	Revisión tecnología utilizada en la prestación del servicio. A.9 Control de acceso A.11 Seguridad física y del entorno A.12 Seguridad de las Operaciones A.13 Seguridad de las comunicaciones A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio.	JDC	**Coordinadora Grupo de Planeación y Sistemas** Olga Inés Botero Duque **Ingeniera Regional Referente SGSI (Contratista)** Dolly Cuero Angulo **Ingeniero Regional Enlace DIT (Contratista)** Gustavo Alegría Pino
	10:30	11:00	Protección (Adopciones) A.6.2.2 Teletrabajo A. 8.1 Responsabilidad por los activos A.8.2.3 Uso aceptables de los activos A.8.3.1 Gestión de medios removibles A.9 Control de acceso A.12.2 Controles contra códigos maliciosos	JDC	**Coordinadora Grupo de Asistencia Técnica** Maria Nydia Henao Castaño **Coordinadora Grupo de Planeación y Sistemas** Olga Inés Botero Duque **Ingeniera Regional Referente SGSI (Contratista)** Dolly Cuero Angulo **Ingeniero Regional Enlace (Contratista)** Gustavo Alegría Pino
	11:00	12:30	Reunión de cierre diario	JDC	**Directora Regional** Claudia Patricia Serna Gallego **Coordinadora Grupo de Planeación y Sistemas** Olga Inés Botero Duque **Coordinador Grupo Administrativo**

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)
					Juan Antonio Carvajal Echavarria **Coordinadora Grupo Jurídico** Ledia del Pilar Giraldo Ossa **Coordinadora Grupo de Asistencia Técnica** Maria Nydia Henao Castaño **Ingeniera Regional Referente SGSI (Contratista)** Dolly Cuero Angulo **Ingeniero Regional Enlace DIT (Contratista)** Gustavo Alegría Pino
2023/07/12 Regional Antioquia	08:00	08:30	Reunión Introductoria	YVG	**Directora Regional** Martha Yolanda Ciro Flores **Coordinadora de Planeación y Sistemas** Loren Andrea Grisales Mejía **Coordinadora Administrativa** Olga Elpidia Zapata Correa **Coordinadora Financiera** Ana Milena Cuartas Tobón **Coordinadora de Ciclos de Vida y Nutrición** Sandra Patricia Guerrero Montoya **Coordinadora de Gestión y Talento Humano** Evelyn e Jesús Toro Ayus

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)
					Coordinadora de Protección Brenda Estella Cardona Vargas **Coordinador Jurídico** Orlando Guzmán Benitez, **Asesora Jurídica** Laura Inés Gómez, **Ingeniera de Sistema (Contratista)** Yaritza Shirley Montoya Bolívar **Ingenieros (Contratistas)** Sandor Andrés Osorio Cano José Gregorio Herrera Calle
	08:30	09:00	Recorrido por la sede A.11 Seguridad física y del entorno	YVG	**Directora Regional** Martha Yolanda Ciro Flores **Coordinadora de Planeación y Sistemas** Loren Andrea Grisales Mejía **Ingeniera de Sistema (Contratista)** Yaritza Shirley Montoya Bolívar **Ingenieros (Contratistas)** Sandor Andrés Osorio Cano José Gregorio Herrera Calle
	09:00	12:30	Revisión tecnología utilizada en la prestación del servicio. A.9 Control de acceso A.11 Seguridad física y del entorno A.12 Seguridad de las Operaciones	YVG	**Coordinadora de Planeación y Sistemas** Loren Andrea Grisales Mejía **Ingeniera de Sistema (Contratista)** Yaritza Shirley Montoya Bolívar

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)
			A.13 Seguridad de las comunicaciones A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio.		**Ingenieros (Contratistas)** Sandor Andrés Osorio Cano José Gregorio Herrera Calle
	12:30	13:30	Receso	YVG	
	13:30	16:00	Promoción y prevención – Primera Infancia (Regional) A.6.2.2 Teletrabajo A. 8.1 Responsabilidad por los activos A.8.2.3 Uso aceptables de los activos A.8.3.1 Gestión de medios removibles A.9 Control de acceso A.12.2 Controles contra códigos maliciosos	YVG	**Coordinadora de Ciclos de Vida y Protección** Sandra Patricia Guerrero Montoya **Coordinadora de Planeación y Sistemas** Loren Andrea Grisales Mejía **Ingeniera de Sistema (Contratista)** Yaritza Shirley Montoya Bolívar **Ingenieros (Contratistas)** Sandor Andrés Osorio Cano José Gregorio Herrera Calle
	16:00	17:00	Reunión de cierre diario	YVG	**Directora Regional** Martha Yolanda Ciro Flores, **Coordinadora de Planeación y Sistemas** Loren Andrea Grisales Mejía **Coordinadora Administrativa** Olga Elpidia Zapata Correa, **Coordinadora Financiera** Ana Milena Cuartas Tobón **Coordinadora de Ciclos de Vida y Nutrición**

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)
					Sandra Patricia Guerrero Montoya **Coordinadora de Gestión y Talento Humano** Evelyn e Jesús Toro Ayus, **Coordinadora de Protección** Brenda Estella Cardona Vargas **Coordinador Jurídico** Orlando Guzmán Benitez **Asesora Jurídica** Laura Inés Gómez **Ingeniera de Sistema (Contratista)** Yaritza Shirley Montoya Bolívar **Ingenieros (Contratistas)** Sandor Andrés Osorio Cano José Gregorio Herrera Calle
DIA 4					
2023/07/13 Regional Cundinamarca	08:00	08:30	Reunión Introductoria	YVG	**Director Regional** Francisco Javier Beltrán **Coordinador Grupo Planeación y Sistemas** Luis Enrique Leguizamón- **Ingenieros Regionales** Orlando Reyes (Profesional Especializado) Hermes Gómez (Contratista) Carlos Mauricio Pinto Martinez

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)
					(Contratista)
	08:30	09:00	Recorrido por la sede A.11 Seguridad física y del entorno	YVG	**Ingenieros Regionales** Orlando Reyes (Profesional Especializado) Hermes Gómez (Contratista) Carlos Mauricio Pinto Martinez (Contratista)
	09:00	12:30	Revisión tecnología utilizada en la prestación del servicio. A.9 Control de acceso A.11 Seguridad física y del entorno A.12 Seguridad de las Operaciones A.13 Seguridad de las comunicaciones A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio.	YVG	**Coordinador Grupo Planeación y Sistemas** Luis Enrique Leguizamón **Ingenieros Regionales** Orlando Reyes (Profesional Especializado) Hermes Gómez (Contratista) Carlos Mauricio Pinto Martinez (Contratista)
	12:30	13:30	Receso	YVG	
	13:30	16:00	Promoción y prevención – Primera Infancia (Regional) A.6.2.2 Teletrabajo A. 8.1 Responsabilidad por los activos A.8.2.3 Uso aceptables de los activos A.8.3.1 Gestión de medios removibles A.9 Control de acceso A.12.2 Controles contra códigos maliciosos	YVG	**Coordinador Grupo Asistencia Técnica** Ana Liliana Camacho **Coordinador Administrativo** Eliana Katherine Garzón Garzón **Coordinador Grupo Financiero** Elba Matilde Ojeda Pedraza. **Coordinador Grupo Jurídico** Mauris Yolanda Orozco Hincapie

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)
					Coordinador Grupo Planeación y Sistemas Luis Enrique Leguizamón- **Ingenieros Regionales** Orlando Reyes (Profesional Especializado) Hermes Gómez (Contratista) Carlos Mauricio Pinto Martinez (Contratista)
	16:00	17:00	Reunión de cierre diario	YVG	**Director Regional** Francisco Javier Beltrán **Coordinador Grupo Planeación y Sistemas** Luis Enrique Leguizamón **Profesional Especializado** Orlando Reyes **Ingenieros Regionales** Orlando Reyes (Profesional Especializado) Hermes Gómez (Contratista) Carlos Mauricio Pinto Martinez (Contratista) **Coordinador Grupo Asistencia Técnica** Ana Liliana Camacho **Coordinador Administrativo** Eliana Katherine Garzón Garzón **Coordinador Grupo Financiero** Elba Matilde Ojeda Pedraza

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)
					Coordinador Grupo Jurídico Mauris Yolanda Orozco Hincapie
DIA 5					
2023/07/14 Metrópolis	08:30	12:30	Gestión de la tecnología y de la información Diseño y Desarrollo de las aplicaciones (Diseño y desarrollo Seguridad de servicios de las aplicaciones en redes públicas Criptografía) A.10, A.14	YVG	**Director de Información y Tecnología** José Ebert Bonilla Olaya **Subdirectora de Sistemas Integrados de Información** Olga Patricia Ríos Ríos **Contratistas Subdirección de Sistemas Integrados de Información** Lina Janneth Bohorquez Paez Oveymar Enrique Rodriguez Jimenez **Equipo SGSI (Contratista)** Teresa Quilindo Sarasti **Coordinador Equipo Seguridad de la Información (Contratista)** Astrid Vannessa Castro Cortes
	12:30	13:30	Receso		
Dirección General	13:30	16:00	Verificación del uso del logo en los diferentes medios de publicidad usados por la Entidad. Elaboración de Informe preliminar	YVG	**Equipo SGSI (Contratista)** Teresa Quilindo Sarasti **Coordinador Equipo Seguridad de la Información (Contratista)** Astrid Vannessa Castro Cortes
Dirección General	16:00	17:00	Reunión de cierre	YVG	**Director de Información y Tecnología**

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)
					Jose Ebert Bonilla Olaya **Coordinador Equipo Seguridad de la Información (Contratista)** Astrid Vannessa Castro Cortes **Equipo SGSI (Contratista)** Teresa Quilindo Sarasti **Promotor EPICO de la DIT (Contratista)** Luis Felipe Garcia Forero

Observaciones:

Los requisitos comunes que serán auditados en todos los procesos para ISO 9001 son:

6.1 Acciones para abordar riesgos y oportunidades
6.3 Planificación de cambios
7.1.6 Conocimientos de la organización
7.5 Información documentada
9.1.3 Análisis y Evaluación
10 Mejora

Los requisitos comunes que serán auditados en todos los procesos para ISO/IEC 27001 son:

7.5 Información documentada
9. Evaluación del desempeño
A.9.3 Responsabilidades de los usuarios

Temas relacionados con la Política de seguridad y los controles relacionados con la documentación se puede revisar en cualquier proceso
Se solicita tener disponible tener una memoria USB disponible para hacer comprobación de políticas de removibles.
En cualquier equipo se puede revisar los controles de navegación en internet.

Esta auditoría no es testificada por un Organismo de Acreditación.

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:	2023-06-26

ANEXO 4

ACEPTACIÓN DE LOS RESULTADOS DE LA AUDITORIA FIRMADA POR LA ORGANIZACIÓN:	
Número de no conformidades ISO/IEC 27001 detectadas en esta auditoría: (0) Mayores (6) menores Número de no conformidades pendientes que no se cerraron en esta auditoría: (0) 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: 2023-07-28 Fecha tentativa de verificación complementaria, cuando aplique N.A.	
ACEPTACIÓN DE LA ORGANIZACIÓN:	
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:	
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: José Ebert Bonilla Olaya	Firma: 

ANEXO 5

No Aplica

ANEXO 6

No Aplica

ANEXO 7

No Aplica

ANEXO 8

No Aplica