

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



| 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 | | |
| Si la certificación cubre más de un sitio permanente donde se realicen actividades del sistema de gestión, indicar 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: Avenida Santander Carrera 23 No. 39 – 60 | Manizales, Caldas, Colombia | Todas las actividades del alcance |
| Regional Caquetá: | Florencia, Caquetá, Colombia | Todas las actividades del alcance |

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



| | | |
|---|--|-----------------------------------|
| Transversal 6; Avenida Circunvalar Barrio San Judas | | |
| 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 Santander: Calle 5 AN Avenida 13 E Barrio San Eduardo | Cúcuta - Norte de Santander Colombia | Todas las actividades del alcance |
| Regional Putumayo: Calle 14 No. 9 - 100 Barrio San Francisco | Mocoa – Putumayo Colombia | Todas las actividades del alcance |
| Regional Quindío: Carrera 23 Calles 3ra | Armenia, Quindío, Colombia | Todas las actividades del alcance |

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



| | | |
|---|---|-----------------------------------|
| y 4ta Barrio Sesenta Casas | | |
| 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

VERSION EN INGLÉS

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. CATEGORÍA DE ISO/TS 22003: NA

1.7. REQUISITOS DE SISTEMA DE GESTIÓN: ISO/IEC 27001:2013

AUDITORÍA CON EL APOYO DE MEDIOS TECNOLÓGICOS PARCIALMENTE REMOTA

1.8. REPRESENTANTE DE LA ORGANIZACIÓN

Nombre: Amanda Castellanos Mendoza

Cargo: Directora de Planeación y Control

Correo electrónico: amanda.castellanos@icbf.gov.co

**PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN**



| | | |
|---|--------------------------------------|--------------------|
| 1.9. TIPO DE AUDITORÍA: | | |
| <input type="checkbox"/> Inicial o de Otorgamiento <input checked="" type="checkbox"/> Seguimiento <input type="checkbox"/> Renovación <input type="checkbox"/> Ampliación <input type="checkbox"/> Reducción <input type="checkbox"/> Reactivación <input type="checkbox"/> Extraordinaria <input type="checkbox"/> Actualización <input type="checkbox"/> Migración (aplica para ISO 45001) | | |
| Aplica toma de muestra por multisitio: Si <input checked="" type="checkbox"/> No <input type="checkbox"/> | | |
| Auditoría combinada: Si <input type="checkbox"/> No <input checked="" type="checkbox"/> | | |
| Auditoría integrada: Si <input type="checkbox"/> No <input checked="" type="checkbox"/> | | |
| 1.10. Tiempo de auditoría | | |
| | FECHA | Días de auditoría) |
| Etapa 1 (Si aplica) | | |
| Preparación de la auditoría en sitio y elaboración del plan | 2021-05-21 | 1.0 |
| Auditoría remota | 2021- 06- 08 hasta 2021-06- 16 | 12.5 |
| Auditoría en sitio | NA | NA |
| Elaboración de informe | 2021-07-09 | 1.0 |
| 1.11. EQUIPO AUDITOR | | |
| Auditor líder | Libardo Chávez Pérez LCP | |
| Auditor | Diego Camilo Rodríguez DCR | |
| Experto Técnico | No aplica | |
| 1.12. DATOS DEL CERTIFICADO DE SISTEMA DE GESTIÓN | | |
| Código asignado por ICONTEC | 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 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 |
|-------------------------------------|

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



- 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 y en qué fechas:

| Sitios Permanentes | Fecha de auditoría |
|--------------------|--------------------|
| Dirección General | 01,05-08-2022 |
| Metrópolis piso 3 | 01,02-08-2022 |
| Bogotá | 03-08-2022 |
| Nariño | 03-08-2022 |
| Caquetá | 04-08-2022 |
| Quindío | 04-08-2022 |
| Boyacá | 04-08-2022 |
| | |

- 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

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



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

3.11. ¿Es una auditoría de ampliación o reducción?

Si 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?:

Si No NA

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 No NA

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

En caso afirmativo, cuáles:

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

En caso afirmativo descríbalas,

3.16. Para sistemas de gestión de calidad; ¿Se subcontratan con proveedores el suministro de productos y servicios que hacen parte del alcance del certificado?

Si No

¿En caso afirmativo, se encontraron controlados los proveedores de estos productos y servicios?

Si No

En el caso en el cual la organización subcontrata el suministro de 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 | CONWARE |

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



| | |
|-------------------------------|----------------|
| Datacenter | IFX |
| Línea 145 Atendida por un BPO | IQ Outsourcing |

- 3.17. ¿Se presentaron, durante la auditoría, cambios que hayan impedido cumplir con el plan de auditoría inicialmente acordado con la Organización?
Si No 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
- 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 NA
- 3.20. ¿Aplica restauración para este servicio?
Si No 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. | <p>A.11.2.2 Servicios de suministro No hay protección adecuada frente a interrupciones de suministro eléctrico.</p> <p>En la Regional Norte de Santander: No se encuentra en el momento de la auditoría protección de la planta eléctrica ni de la UPS ya que ésta última está averiada. No se encontraron los registros de mantenimiento para la UPS</p> <p>En la Regional Caldas: La planta eléctrica se encontró desconectada y rodeado de vehículos a menos de un metro de distancia. No se encontraron los registros de mantenimiento para la UPS</p> | <p>Se evidencia la documentación del contrato y la Captura de pantalla de su publicación en SECOP II. Acta de adjudicación para el mantenimiento preventivo y correctivo de las ups a nivel nacional, adicionalmente se evidencian en actas de seguimiento el control a la ejecución pertinente a dicho contrato que garantiza el funcionamiento adecuado de los equipos relacionados.</p> <p>Se evidencia en obra civil yd e infraestructura la instalación adecuada de las plantas eléctricas faltantes.</p> | SI |
| 2 | <p>A.12.4.4. Sincronización de relojes</p> <p>Descripción: No hay Sincronización de relojes entre las diferentes fuentes. Evidencia: En la regional Norte de Santander: En el momento de la auditoría se evidencia un desfase de tres minutos con</p> | <p>Se evidencio la implementación del diligenciamiento permanente y disciplinado del reporte y minutas por parte de los vigilantes del monitoreo de los NVR con la hora</p> | Si |

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



| | | | |
|---|---|---|----|
| | las diferentes cámaras del circuito cerrado de TV, (en todas las cámaras arroja una lectura de 08:30 a.m., mientras que la hora legal colombiana es 08:33 a.m.) | legal colombiana, garantizando el control y sincronización efectivo. | |
| 3 | <p>A.12.5.1 Instalación de software en sistemas operativos</p> <p>Descripción: No se evidenció restricción en la instalación/desinstalación de software en sistemas operativos</p> <p>En la regional Meta: Al inspeccionar los privilegios de instalación de software desde computadores asignados a funcionarios diferentes al personal de soporte técnico, se encontró que es posible instalar el software WINZIP en el computador de escritorio asignado a Martha Eugenia Solano Coordinadora del Grupo Administrativo.</p> <p>Se encontró desinstalado el antivirus SOPHOS en el computador de escritorio asignado a Luz Ángela Cruz Enlace Adolescencia y Juventud.</p> | <p>Se evidencio los diferentes comunicados de sensibilización, adicional las actas de asistencias a la charlas y listados de acceso a las grabaciones, videos y otros medios utilizados en la concientización de los usuarios. Durante el muestreo realizado el 100% de las maquinas revisadas cumplen con la política establecida.</p> <p>Procedimiento actualizado P2.GTI "Procedimiento de Gestión de Solicitudes de Tecnología"</p> | 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.

- ✓ El análisis del contexto evidencia un ejercicio juicioso, serio y detallado que le permite al ICBF tomar decisiones y definir estrategias asertivas, las cuales facilitan el logro de sus objetivos.
- ✓ La coherencia entre lo estratégico y operativo garantiza la apropiación de las estrategias y su materialización a través de los planes de acción.
- ✓ El modelo de monitoreo y evaluación de la gestión institucional permite determinar el grado de efectividad y de manera oportuna tomar los correctivos pertinentes. (semaforización- comité de desempeño)
- ✓ Se evidencia un SGSI sólido debidamente divulgado y lo más importante apropiado por cada una de las regionales, el cual brinda elementos de seguridad y continuidad en la prestación del servicio del instituto.

PLAN DE AUDITORÍA EN SITIO

SISTEMA DE GESTIÓN



- ✓ En la totalidad de las regionales auditadas (Sede nacional, Metrópolis, Bogotá, Nariño, Caquetá, Quindío, Boyacá) es de destacar diferentes aspectos como:
- ✓ La disposición de todo el personal es la mejor.
- ✓ El nivel de conocimiento que se tiene por parte de todo el equipo sobre SGSI es excelente.
- ✓ El nivel cumplimiento de los diferentes controles evaluados.
- ✓ El orden y aseo en cada una de las instalaciones .
- ✓ La correcta señalización de las diferentes áreas seguras.
- ✓ El mantenimiento de los facilites que protegen y previene incidentes en las áreas seguras.
- ✓ La organización del cableado estructurado en los centros de datos.
- ✓ La creatividad en la divulgación, genera un mayor grado de apropiación del SGSI.
- ✓ El compromiso con el SGSI evidenciado en la preparación del material tanto institucional como específico del SGSI para cada entrevista.

- ✓ Las cámaras de seguridad con tecnología IP utilizadas para el monitoreo de las instalaciones, presentan gran calidad de imagen y permiten escalabilidad en caso de requerirse.

- ✓ Diversas campañas de capacitación y toma de conciencia en temas de seguridad de la información (ABC SEGURIDAD DE LA INFORMACIÓN, CHARLAS DELITOS INFORMÁTICOS, PRUEBAS DE INGENIERÍA SOCIAL (PHISHING), CARTELERA SGSI, YAMMER, MIERCOLES DE SEGURIDAD, VID) entre otras, ya que fortalecen la gestión de conocimiento en la materia y genera recordación y cultura.

- ✓ Implementación suite visión empresarial para el manejo de activos facilitará su organización y gestión.

- ✓ El nivel de detalle de los informes de restauración de información genera una trazabilidad completa de dicha actividad generando confianza y disponibilidad de la información.

- ✓ El seguimiento detallado a la gestión de vulnerabilidades, reduce la posibilidad de materialización de riesgos que puedan afectar los activos de información, garantizando la confiabilidad, disponibilidad e integridad de la información.

- ✓ Las campañas de Ingeniería social son de resaltar por el grado de recordación y repercusión que este ejercicio generó, y el momento en el cual se realizó (previo a las elecciones), el cual fue muy oportuno logrando resultados a nivel de cultura y sensibilidad con respecto a seguridad de la información.

- ✓ Los resultados de cada uno de los indicadores revisados evidencian un desempeño destacable, lo cual habla muy bien del instituto y del impacto positivo que este genera en la población objetivo y en general en la sociedad colombiana.

- ✓ La tendencia hacia la mejora que muestran los resultados de los indicadores del proceso **RELACION CON EL CIUDADANO, pasando de 88.1% a un 97.9%**, habla muy bien de la gestión realizada por este.

- ✓ La iniciativa de particularizar el BIA por regional, partiendo de un modelo institucional hace que este sea mucho más real y en consecuencia las acciones derivadas de este, serán mucho más efectivas, garantizando la continuidad del negocio.

PLAN DE AUDITORÍA EN SITIO

SISTEMA DE GESTIÓN



- ✓ Las buenas prácticas de desarrollo seguro evidenciadas, garantizan la minimización de los riesgos derivados de esta actividad.
- ✓ La documentación y su nivel de detalle, garantizan la generación e conocimiento al servicio del instituto.
- ✓ Los controles efectivos que tienen definidos y que son llevados a cabo con rigor garantizan la seguridad de la información durante todo el ciclo de desarrollo.
- ✓ La planificación detallada de los cambios hace que el despliegue y liberación de los mismos sean efectivos, garantizando tanto la seguridad como la disponibilidad de los sistemas afectados por estos.
- ✓ La manera disciplinada y detallada con que se controla el desarrollo contratado con terceros, hace que el cumplimiento de lo establecido en las fichas técnicas sea una práctica normalizada.
- ✓ Los múltiples controles de acceso al centro de datos principal ubicado en IFX y el centro alternativo ubicado en la sede nacional, reducen posibilidad de accesos no autorizados.

4.2 Oportunidades de mejora

- ✓ A pesar de los muy buenos resultados de la gestión realizada por el instituto, esta no se evidencia en la percepción de la comunidad en general, sería conveniente revisar la estrategia de divulgación de estos resultados y de la gestión que realiza el ICBF.
- ✓ En la revisión de las bases de datos del proceso RELACIÓN CON EL CIUDADANO es conveniente revisar si es necesario hacer uso de la función hash o algoritmo hash, en el evento que estas grabaciones se requieran como evidencia digital.
- ✓ La calificación de los activos es conveniente revisarla y aprovechar la coyuntura de la entrada en servicio de la nueva plataforma SUIT VISION EMPRESARIAL, de manera que se aproveche como un espacio de refuerzo para la apropiación de la metodología. (No olvidar que el activo se califica independientemente de los controles establecidos).
- ✓ Es conveniente revisar la condensación tanto de riesgos como de activos de información ya que en la búsqueda de la practicidad se pueden perder de la visual activos que deben manejarse de manera particular debido a su criticidad.
- ✓ Los controles existentes es conveniente describirlos en la matriz de riesgo según corresponda ya que pueden afectar de manera conveniente la calificación del riesgo.
- ✓ Cando se hable de activos físicos y electrónicos en la misma fila de la matriz del riesgos, es importante describir los controles correspondiente para cada tipo, de manera que se mantenga la coherencia y así garantizar la seguridad del mismo.
- ✓ Con el fin de fortalecer el monitoreo y seguimiento de procesos a través de indicadores de valor, se recomienda consultar la norma ISO/IEC 27004.
- ✓ Realizar revisiones periódicas a las cámaras de seguridad de los centros de cableado, con el fin de validar su correcto funcionamiento.
- ✓ Digitalizar historias laborales con el fin de mejorar la oportunidad en la búsqueda de esta información.

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



- ✓ Implementar un termohigrómetro en el archivo de gestión de historias laborales con el fin de reducir la posibilidad de materialización de riesgos que afecten esta información tan importante.
- ✓ Dar mayor claridad a la finalidad que se documenta en la autorización de tratamiento de datos personales para funcionarios, esto con el fin de ajustarse más a lo solicitado en la ley de protección de datos personales.
- ✓ Con el fin de reducir la posibilidad de divulgaciones no autorizadas de información, incluir un tiempo de vigencia de los acuerdos de confidencialidad posterior a la finalización del vínculo laboral.
- ✓ Con el fin de fortalecer la efectividad de los controles, se puede trabajar en un modelo de auditoría basada en riesgos que califique el diseño, efectividad y tenga en cuenta pruebas a los controles. Como material de apoyo se pueden consultar metodologías de calificación de diseño y efectividad de controles en la gestión de riesgos.

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 |
|--|-----------------|------------------|
| No Aplica | | |

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

2020-2021: 17 incidentes de seguridad de bajo impacto.
Se sigue una metodología para gestionar los incidentes que inicia con el reporta del incidente, luego se registra y categoriza, se escala, se gestiona y finalmente se genera un informe. Durante la vigencia 2020 y 2021 se presentaron 17 incidentes de seguridad de la información, todos de bajo impacto y los cuales fueron solucionados particularmente con formación y toma de conciencia, actualización de procedimientos documentados de TI, todo siguiendo la metodología documentada.

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

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

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



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 GESTIÓN)
Si 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.

| 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 | | |
| 2ª de seguimiento del ciclo | | |
| Auditorias especiales (Extraordinaria, reactivación, ampliación) | | |

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

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 desde el mes de marzo de 2021. 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 mes de marzo de 2021. 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 No

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?
Si No NA .

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



- 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
- 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 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 REVISADAS

¿Se presentaron no conformidades mayores? SI NO

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

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

En caso afirmativo diligencie el siguiente cuadro:

Fecha de la verificación complementaria: No Aplica

| 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 | | |

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



| | | | | |
|---|-------|------|----|----|
| Se recomienda mantener el alcance del certificado o del Sistema de Gestión | | | | |
| Se recomienda renovar el certificado del Sistema de Gestión | X | | | |
| 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 migrar 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: Libardo Chávez Pérez (LCP) | Fecha | 2022 | 08 | 15 |

| 9. ANEXOS QUE FORMAN PARTE DEL PRESENTE INFORME | | |
|--|--|----|
| Anexo 1 | 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 2 | Información específica de esquemas de certificación de sistema de gestión | X |
| Anexo 3 | Correcciones, análisis de causa y acciones correctivas Aceptación de la organización firmada. Información de la confirmación del cumplimiento de las condiciones para realizar auditoria con el apoyo de medios tecnológicos | X |
| Anexo 4 | Información específica por condición de emergencia | X |
| Anexo 5 | Declaración de aplicación (solo para ISO 28001) | NA |

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



ANEXO 1
PLAN DE AUDITORÍA

| | | | |
|---|---|--|--|
| EMPRESA: | INSTITUTO COLOMBIANO DE BIENESTAR FAMILIAR | | |
| Dirección del sitio: | Avenida carrera 68 No. 64 C 75, Bogotá D.C., Colombia | | |
| Representante de la organización: | Amanda Castellanos Mendoza | | |
| Cargo: | Directora de Planeación y Control de gestión | Correo electrónico | amanda.castellanos@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: | | | |
| Criterios de Auditoría | ISO – IEC 27001:2013+ la documentación del Sistema de Gestión | | |
| Tipo de auditoría: | | | |
| <input type="checkbox"/> Inicial u otorgamiento <input checked="" type="checkbox"/> Seguimiento <input type="checkbox"/> Renovación <input type="checkbox"/> Ampliación <input type="checkbox"/> Reducción <input type="checkbox"/> Reactivación. <input type="checkbox"/> Extraordinaria. <input type="checkbox"/> Actualización / Migración | | | |
| Modalidad: | | | |
| <input type="checkbox"/> Auditoría en sitio <input checked="" type="checkbox"/> Auditoría parcialmente remota <input type="checkbox"/> Auditoría totalmente remota | | | |
| Aplica toma de muestra por multisitio: | | <input checked="" type="checkbox"/> Si | <input type="checkbox"/> No |
| Existen actividades/procesos que requieran ser auditadas en turno nocturno: | | <input type="checkbox"/> Si | <input checked="" type="checkbox"/> No |

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



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 PARA LA CERTIFICACION DE SISTEMAS DE GESTIÓN.

| | | | |
|------------------|------------------------------|--------------------|-------------------------|
| Auditor Líder: | Libardo Chávez Pérez. (LCP) | Correo electrónico | lchavez@icontec.net |
| Auditor | Diego Camilo Rodríguez (DCR) | | dcrodriguez@icontec.net |
| Experto técnico: | NA | | |

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



| | |
|-----------------------------------|----|
| Observador – Profesional de apoyo | NA |
|-----------------------------------|----|

| 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 | | | | | |
| 01/08/2022 Dirección General-Metrópolis /Sede Nacional | 08:00 | 08:30 | Reunión de apertura | DCR/LCP | <p>Álvaro Andrés Rueda Zapata <Alvaro.Rueda@icbf.gov.co>;</p> <p>Astrid Vanessa Castro Cortes <Astrid.CastroC@icbf.gov.co>;</p> <p>Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co</p> |
| | 08:30 | 11:00 | <p>Direccionamiento Estratégico</p> <p>4. Contexto de la Organización</p> <p>5. Liderazgo</p> <p>6.2 Objetivos de seguridad de la información.</p> <p>9.1 Seguimiento y medición</p> <p>9.3 Revisión por la dirección</p> <p>10.1 No conformidades y acciones correctivas</p> <p>10.2 Mejora continua</p> | LCP | <p>Álvaro Andrés Rueda Zapata Alvaro.Rueda@icbf.gov.co;</p> <p>Astrid Vanessa Castro Cortes Astrid.CastroC@icbf.gov.co>;</p> <p>Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co</p> <p>Leonardo Ordonez Carrascal Leonardo.Ordonez@icbf.gov.co</p> |

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



| Fecha/ Sitio (si hay más de uno) | Hora de inicio de la activi dad de auditor ía | Hora de finalizaci ón de la activida d de auditorí a | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|--|--|--|-------------------|---|
| | 8:30 | 11:00 | <p>A.11 Seguridad física y del entorno</p> <p>Verificación del centro de monitoreo.</p> <p>Verificación Datacenter principal</p> <p>Revisión de los diseños de seguridad</p> | DCR | <p>Álvaro Andrés Rueda Zapata Alvaro.Rueda@icbf.gov.co</p> <p>Luz Helena Mejia Zuluaga Luz.Mejia@icbf.gov.co</p> <p>Paolo Armando Tenjo Carrillo <Paolo.Tenjo@icbf.gov.co></p> <p>Astrid Vanessa Castro Cortes <Astrid.CastroC@icbf.gov.co></p> <p>Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co</p> <p>Alix Lorena Moreno Cordoba Alix.MorenoC@icbf.gov.co</p> |
| | 11:00 | 12:30 | <p>Relación con el Ciudadano</p> <p>27001: A.6.2.2, 8.1, A.8.2.3, A.8.3.1 A.9, A.12.1</p> | LCP | <p>Patricia Ochoa Restrepo Patricia.Ochoa@icbf.gov.co</p> <p>Oscar Javier Bernal Parra Oscar.Bernal@icbf.gov.co</p> <p>Astrid Vanessa Castro Cortes <Astrid.CastroC@icbf.gov.co>;</p> |

**PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN**



| Fecha/ Sitio (si hay más de uno) | Hora de inicio de la activi dad de auditor ía | Hora de finalizaci ón de la activida d de auditorí a | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|--|--|--|-------------------|---|
| | 11:00 | 12:30 | Gestión Talento Humano 5.3 Roles, responsabilidades y autoridades 7.2 Competencia 7.3, 7.4 y A.7 Seguridad de los recursos humanos | DCR | John Fernando Guzman Uparela John.Guzman@icbf.gov.co Neyffe Patricia Gamboa Ovalle Neyffe.Gamboa@icbf.gov.co Teresa Quilindo Sarasti Teresa.Quilindo@icbf.gov.co Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co |
| | 13:00 | 14:30 | Receso | | |
| | 14:30 | 17:00 | Adquisición de Bienes y Servicios 8.1 Planificación y control operacional 9.1 Seguimiento análisis y evaluación A.15 Relación con los proveedores | DCR | Gustavo Mauricio Martinez Perdomo Gustavo.Martinez@icbf.gov.co Gonzalo Eduardo Carreno Padilla Gonzalo.Carreno@icbf.gov.co Helen Ortiz Carvajal Helen.Ortiz@icbf.gov.co |

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



| Fecha/ Sitio (si hay más de uno) | Hora de inicio de la activi dad de auditor ía | Hora de finalizaci ón de la activida d de auditorí a | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|--|--|---|-------------------|---|
| | | | | | <p>Ana Milena Bustos Sanchez Ana.Bustos@icbf.gov.co</p> <p>Nelcy Stefany Parra Mora Stefany.Parra@icbf.gov.co;</p> <p>Johanna Fernanda Villareal Guzman Johanna.Villareal@icbf.gov.co</p> <p>Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co</p> |
| | 14:30 | 17:00 | <p>Servicios Administrativos</p> <p>8.1 Planificación y control operacional</p> <p>9.1 Seguimiento análisis y evaluación</p> <p>A.15 Relación con los proveedores</p> | LCP | <p>Luz Helena Mejía Zuluaga Luz.Mejia@icbf.gov.co</p> <p>Milton Yesid Rey Cubillos Milton.Rey@icbf.gov.co</p> <p>Paolo Armando Tenjo Carrillo Paolo.Tenjo@icbf.gov.co</p> <p>Leonardo Ordonez Carrascal Leonardo.Ordonez@icbf.gov.co</p> |

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



| Fecha/ Sitio (si hay más de uno) | Hora de inicio de la activi dad de auditor ía | Hora de finalizaci ón de la activida d de auditorí a | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|--|--|---|-------------------|---|
| | | | | | <p>Ana Maria Rengifo Ovalle Ana.Rengifo@icbf.gov.co</p> <p>Ana Lissette Agudelo Ballesteros Ana.Agudelo@icbf.gov.co</p> <p>Astrid Vanessa Castro Cortes Astrid.CastroC@icbf.gov.co</p> |
| | 17:00 | 17:30 | Balance diario | DCR LCP | <p>Álvaro Andrés Rueda Zapata Alvaro.Rueda@icbf.gov.co</p> <p>Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co</p> <p>Astrid Vanessa Castro Cortes Astrid.CastroC@icbf.gov.co</p> |
| DIA 2 | | | | | |
| 02/08/2022 Dirección General/ Metrópolis | 08:30 | 12:30 | Gestión de la tecnología y de la información Diseño y Desarrollo de las aplicaciones (Diseño y desarrollo | LCP | <p>Álvaro Andrés Rueda Zapata <Alvaro.Rueda@icbf.gov.co>;</p> <p>Astrid Vanessa Castro Cortes <Astrid.CastroC@icbf.gov.co>;</p> |

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



| Fecha/ Sitio (si hay más de uno) | Hora de inicio de la activi dad de auditor ía | Hora de finalizaci ón de la activida d de auditorí a | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|--|--|--|-------------------|--|
| | | | Seguridad de servicios de las aplicaciones en redes públicas (Criptografía) A.10, A.14 | | Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co Alix Lorena Moreno Cordoba Alix.MorenoC@icbf.gov.co |
| | 08:30 | 12:30 | A.8 Gestión de Activos, inventario y devoluciones. Clasificación de la información A.12 Seguridad de las Operaciones | DCR | Álvaro Andrés Rueda Zapata < Alvaro.Rueda@icbf.gov.co >; Astrid Vannessa Castro Cortes < Astrid.CastroC@icbf.gov.co >; Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co Jairo Correa Mojica Jairo.Correa@icbf.gov.co |
| | 12:30 | 14:00 | Receso | | |
| | 14:00 | 16:30 | A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio. | LCP | Álvaro Andrés Rueda Zapata Alvaro.Rueda@icbf.gov.co ; Astrid Vannessa Castro Cortes Astrid.CastroC@icbf.gov.co ; Jairo Correa Mojica Jairo.Correa@icbf.gov.co |

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



| Fecha/ Sitio (si hay más de uno) | Hora de inicio de la activi dad de auditor ía | Hora de finalizaci ón de la activida d de auditorí a | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|--|--|--|-------------------|--|
| | 14:00 | 15:30 | A.12.6 Gestión de vulnerabilidades técnicas | DCR | <p>Álvaro Andrés Rueda Zapata Alvaro.Rueda@icbf.gov.co;</p> <p>Astrid Vannessa Castro Cortes Astrid.CastroC@icbf.gov.co;</p> <p>Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co</p> |
| | 15:30 | 17:30 | A.16 Análisis de incidentes de seguridad | DCR | <p>Álvaro Andrés Rueda Zapata Alvaro.Rueda@icbf.gov.co;</p> <p>Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co</p> <p>Astrid Vannessa Castro Cortes Astrid.CastroC@icbf.gov.co;</p> |
| | 17:00 | 17:30 | Balance Diario | LCP | <p>Álvaro Andrés Rueda Zapata Alvaro.Rueda@icbf.gov.co;</p> <p>Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co</p> |

**PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN**



| Fecha/ Sitio (si hay más de uno) | Hora de inicio de la activi dad de auditor ía | Hora de finalizaci ón de la activida d de auditorí a | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|--|--|---|-------------------|---|
| | | | | | Astrid Vanessa Castro Cortes Astrid.CastroC@icbf.gov.co; |
| Dia 3 | | | | | |
| 03/08/2022 Regional Bogotá | 07:45 | 08:00 | Prueba de conexión remota | LCP | Dolly Cuero Angulo Dolly.Cuero@icbf.gov.co ; Cristian Orlando Quiroz Pineros CRISTIAN.QUIROZ@icbf.gov.co Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co Astrid Vanessa Castro Cortes Astrid.CastroC@icbf.gov.co |
| | 08:00 | 08:30 | Recorrido por la sede A.11 Seguridad física y del entorno | LCP | Diana Patricia Arboleda Ramírez Diana.Arboleda@icbf.gov.co Dolly Cuero Angulo Dolly.Cuero@icbf.gov.co Karen Mainory Martinez Roa Karen.MartinezR@icbf.gov.co |

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



| Fecha/ Sitio (si hay más de uno) | Hora de inicio de la activi dad de auditor ía | Hora de finalizaci ón de la activida d de auditorí a | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|--|--|--|-------------------|---|
| | | | | | <p>Cristian Orlando Quiroz Pineros CRISTIAN.QUIROZ@icbf.gov.co</p> <p>Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co</p> <p>Astrid Vannessa Castro Cortes Astrid.CastroC@icbf.gov.co</p> |
| | 8:30 | 12:30 | <p>Promoción y prevención – Primera Infancia (Regional)</p> <p>A.6.2.2 Teletrabajo</p> <p>A. 8.1 Responsabilidad por los activos</p> <p>A.8.2.3 Uso aceptables de los activos</p> <p>A.8.3.1 Gestión de medios removibles</p> <p>A.9 Control de acceso</p> <p>A.12.2 Controles contra códigos maliciosos</p> | LCP | <p>Diana Patricia Arboleda Ramirez Diana.Arboleda@icbf.gov.co</p> <p>Dolly Cuero Angulo Dolly.Cuero@icbf.gov.co</p> <p>Karen Mainory Martinez Roa Karen.MartinezR@icbf.gov.co</p> <p>Cristian Orlando Quiroz Pineros CRISTIAN.QUIROZ@icbf.gov.co</p> <p>Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co</p> |

**PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN**



| Fecha/ Sitio (si hay más de uno) | Hora de inicio de la activi dad de auditor ía | Hora de finalizaci ón de la activida d de auditorí a | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|--|--|--|-------------------|--|
| | | | | | Astrid Vannessa Castro Cortes Astrid.CastroC@icbf.gov.co |
| Receso | | | | | |
| 03/08/2022 Regional Nariño | 13:45 | 14:00 | Prueba de conexión remota | LCP | Maria Mercedes Arellano Ortiz Maria.Arellano@icbf.gov.co Jorge Luis Villegas Maguiña Jorge.Villegas@icbf.gov.co Alix Lorena Moreno Córdoba Alix.MorenoC@icbf.gov.co Astrid Vannessa Castro Cortes Astrid.CastroC@icbf.gov.co |
| | 14.00 | 17:00 | Protección (Adopciones) (MT) 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 | LCP | Maria Mercedes Arellano Ortiz Maria.Arellano@icbf.gov.co Jorge Luis Villegas Maguiña Jorge.Villegas@icbf.gov.co Alix Lorena Moreno Córdoba Alix.MorenoC@icbf.gov.co Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co |

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



| Fecha/ Sitio (si hay más de uno) | Hora de inicio de la activi dad de auditor ía | Hora de finalizaci ón de la activida d de auditorí a | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|--|--|-------------------------------------|-------------------|---|
| | | | | | Astrid Vanessa Castro Cortes Astrid.CastroC@icbf.gov.co |
| | 17:00 | 17:30 | Balance diario | LCP | Álvaro Andrés Rueda Zapata <Alvaro.Rueda@icbf.gov.co>; Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co Astrid Vanessa Castro Cortes Astrid.CastroC@icbf.gov.co |
| Dia 4 | | | | | |
| 04/08/2022 Regional Caquetá | 07:45 | 08:00 | Prueba de conexión remota | LCP | Bertulio Cabrera Plazas Bertulio.Cabrera@icbf.gov.co Yurany Ospina Pisso <Yurany.Ospina@icbf.gov.co>; Teresa Quilindo Sarasti Teresa.Quilindo@icbf.gov.co Astrid Vanessa Castro Cortes Astrid.CastroC@icbf.gov.co |

**PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN**



| Fecha/ Sitio (si hay más de uno) | Hora de inicio de la activi dad de auditor ía | Hora de finalizaci ón de la activida d de auditorí a | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|--|--|---|-------------------|--|
| | 08:00 | 12:30 | Promoción y prevención – Primera Infancia (Regional) (MT) 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 | LCP | Bertulio Cabrera Plazas Bertulio.Cabrera@icbf.gov.co Yurany Ospina Pisso <Yurany.Ospina@icbf.gov.co>; Teresa Quilindo Sarasti Teresa.Quilindo@icbf.gov.co Astrid Vannessa Castro Cortes Astrid.CastroC@icbf.gov.co |
| | | | Receso | | |
| 04/08/2022 Regional Quindío | 13:45 | 14:00 | Prueba de conexión remota | LCP | Adriana Echeverri Gonzalez Adriana.EcheverriG@icbf.gov.co Osney Castano Medina Osney.Castano@icbf.gov.co Jairo Correa Mojica Jairo.Correa@icbf.gov.co Astrid Vannessa Castro Cortes Astrid.CastroC@icbf.gov.co |

**PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN**



| Fecha/ Sitio (si hay más de uno) | Hora de inicio de la activi dad de auditor ía | Hora de finalizaci ón de la activida d de auditorí a | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|--|--|--|-------------------|---|
| | 14:00 | 17:00 | Protección (Adopciones) (MT) 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 | LCP | Adriana Echeverri Gonzalez Adriana.EcheverriG@icbf.gov.co Osney Castano Medina Osney.Castano@icbf.gov.co Jairo Correa Mojica Jairo.Correa@icbf.gov.co |
| | 17:00 | 17:30 | Balance diario | LCP | Álvaro Andrés Rueda Zapata <Alvaro.Rueda@icbf.gov.co>; Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co Astrid Vannessa Castro Cortes Astrid.CastroC@icbf.gov.co |
| Quinto Dia | | | | | |
| 05/08/2022 Regional Boyacá | 7:45 | 8:00 | Prueba de conexión remota | LCP | |

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



| Fecha/ Sitio (si hay más de uno) | Hora de inicio de la activi dad de auditor ía | Hora de finalizaci ón de la activida d de auditorí a | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|--|--|---|-------------------|--|
| | | | | | <p>Adriana del Pilar Camacho Leon Adriana.Camacho@icbf.gov.co</p> <p>Luis Eduardo Herrera Ospina Luis.Herrera@icbf.gov.co</p> <p>Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co</p> <p>Astrid Vanessa Castro Cortes Astrid.CastroC@icbf.gov.co</p> |
| | 08:00 | 11:30 | <p>Promoción y Prevención (Primera Infancia) (MT)</p> <p>A.6.2.2 Teletrabajo</p> <p>A.8.1 Responsabilidad por los activos</p> <p>A.8.2.3 Uso aceptables de los activos</p> <p>A.8.3.1 Gestión de medios removibles</p> <p>A.9 Control de acceso</p> <p>A.12.2 Controles contra códigos maliciosos</p> | LCP | <p>Adriana del Pilar Camacho Leon Adriana.Camacho@icbf.gov.co</p> <p>Luis Eduardo Herrera Ospina Luis.Herrera@icbf.gov.co</p> <p>Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co</p> <p>Astrid Vanessa Castro Cortes Astrid.CastroC@icbf.gov.co</p> |
| | 08:30 | 11:30 | Preparación Informe | DCR | Astrid Vanessa Castro Cortes Astrid.CastroC@icbf.gov.co |

**PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN**



| Fecha/ Sitio (si hay más de uno) | Hora de inicio de la activi dad de auditor ía | Hora de finalizaci ón de la activida d de auditorí a | PROCESO / REQUISITOS POR AUDITAR | EQUIPO AUDITOR | CARGO Y NOMBRE (Todas las personas que serán entrevistadas en la auditoría) |
|---|--|--|--|-------------------|---|
| | 11:30 | 12:30 | Reunión auditores revisión informe parcial | DCR/LCP | |
| | | | Receso | | |
| 05/08/2022 Dirección General | 14:00 | 16:30 | (MT) Verificación del uso del logo en los diferentes medios de publicidad usados por la Entidad. Elaboración de Informe preliminar | LCP | Álvaro Andrés Rueda Zapata <Alvaro.Rueda@icbf.gov.co>; Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co Astrid Vanessa Castro Cortes Astrid.CastroC@icbf.gov.co |
| | 16:30 | 17:00 | Reunión representante de la dirección | LCP | Álvaro Andrés Rueda Zapata <Alvaro.Rueda@icbf.gov.co>; Guillermo Enrique Gaines Ospina Guillermo.Gaines@icbf.gov.co Astrid Vanessa Castro Cortes Astrid.CastroC@icbf.gov.co |
| | 16:00 | 17:00 | Reunión de cierre | LCP | Todos los auditados |

Observaciones:

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



Durante toda la auditoría se verificarán los requisitos como: Política; Acciones para abordar riesgos y oportunidades; Comunicación; Información documentada; Seguimiento, medición, análisis y evaluación; Competencia; Toma de conciencia; No conformidad y acción correctiva.

Los requisitos comunes que serán auditados en todos los procesos.

6.1 Acciones para abordar riesgos y oportunidades

7.4 Comunicación

7.5 Información documentada

9.1 Seguimiento, medición, análisis y evaluación

10. Mejora

A.9.3 Responsabilidades de los usuarios

“Por razones de seguridad y atendiendo la emergencia sanitaria, se realizará la auditoría por medio de la herramienta seleccionada (por ejemplo, MS, Teams), conservando la seguridad y confidencialidad de la información y la información compartida será utilizada con el único propósito de realizar la auditoría Parcialmente Remota.

Se requiere que las personas que recibirán la auditoría por medio remoto puedan acceder a la plataforma TEAMS.

Se requiere la coordinación de la logística para el desplazamiento a sedes y/o proyectos.

Se sugiere que la auditoría este acompañada por una persona de la organización o guía, con el fin de:

- Establecer contactos y asistir con la ejecución del cronograma de entrevistas.
- Orientar al equipo auditor frente a las reglas relacionadas a la protección personal y de seguridad establecidas por la organización.
- Testificar la auditoría en nombre de la organización y proveer información aclaratoria cuando así sea solicitado por el equipo auditor.
- Identificar y transmitir la información generada a la organización.

Esta auditoría no es objeto de testificación por un Organismo de Acreditación.

La función del equipo evaluador consiste en observar y evaluar la competencia del equipo auditor y la aplicación de los procedimientos de ICONTEC para dar cumplimiento a los requisitos de acreditación con la norma ISO/IEC 17021-1.

Diariamente previo al inicio de la auditoría, se realizará verificación de conexión medios tecnológicos.

La auditoría por medios remotos se realizará utilizando la plataforma TEAMS.

PLAN DE AUDITORÍA EN SITIO
SISTEMA DE GESTIÓN



Solo Aplica para auditorías en sitio. 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: | 2022-07-15 |
|---|------------|

ANEXO 2

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

Marque con una X si el sistema de gestión auditado.

X ISO/IEC 27001

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 X No
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 Código: A3.MS.DE 28/06/2022 – V. 11 | Modificación de la justificación de los controles a partir de la revisión y actualización de los riesgos. |

- ¿Los procedimientos adoptados por el cliente brindan confianza en el SGSI?
Si x No
- Describa brevemente los documentos revisados como evidencia de las muestras tomadas para la evaluación del SGSI

Se revisaron los documentos como: Políticas de seguridad de la información, Registro de incidentes o eventos de seguridad, Registro de perfiles a colaboradores, Revisión de cuentas desactivadas de

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

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 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, Planes de auditoría interna 2021 y 2022, Informes de auditoría interna 2021 y 2022 Procedimientos Auditoría Internas SIGE, Formato gestión integral de cambios (ISOLUCION a SVE - SIGE), Consolidación riesgos de seguridad de la información 2022.

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).

La metodología de gestión de riesgos está completamente alineada con la ISO 31000 evidenciando una aplicabilidad total de las diferentes fases (identificación, valoración, tratamiento, seguimiento) y destacable por la participación de los dueños de los procesos la identificación, registro, de los riesgos inherentes, la identificación de los controles y/o implementación de los controles para los riesgos residuales

Mediante la implementación de planes de tratamiento definidos de manera coherente, incluyendo responsables y recursos asociados y tiempos de ejecución, lo que facilita su seguimiento y evaluación. La siguiente grafica muestra la gestión consolidada a nivel nacional.

Consolidados Riesgos de Seguridad de la Información



| No. | PROCESO | TOTAL | No. | PROCESO | TOTAL | No. | REGIONAL | TOTAL | No. | REGIONAL | TOTAL | No. | REGIONAL | TOTAL |
|-----|--|-------|-----|--------------------------------------|-------|-----|-----------|-------|-----|--------------------|-------|--------------|------------|-------|
| 1 | Adquisición de Bienes y Servicios | 8 | 9 | Gestión del Talento Humano | 4 | 1 | AMAZONAS | 28 | 14 | CUNDINAMARCA | 20 | 27 | SANTANDER | 17 |
| 2 | Comunicación Estratégica | 2 | 10 | Inspección, Vigilancia y Control | 1 | 2 | ANTIOQUIA | 26 | 15 | GUAINÍA | 7 | 28 | SUCRE | 15 |
| 3 | Coordinación y Articulación del SNBF y Agentes | 0 | 11 | Mejora e Innovación | 1 | 3 | ARAUCA | 35 | 16 | LA GUAJIRA | 13 | 29 | TOLIMA | 26 |
| 4 | Direccionamiento Estratégico | 2 | 12 | Monitoreo y Seguimiento a la Gestión | 2 | 4 | ATLÁNTICO | 38 | 17 | GUAVIARE | 16 | 30 | VALLE | 12 |
| 5 | Evaluación Independiente | 2 | 13 | Promoción y Prevención | 3 | 5 | BOGOTÁ | 18 | 18 | HUILA | 22 | 31 | VAUPÉS | 9 |
| 6 | Gestión de la Tecnología e Información | 17 | 14 | Protección | 7 | 6 | BOLÍVAR | 28 | 19 | MAGDALENA | 26 | 32 | VICHADA | 10 |
| 7 | Gestión Financiera | 2 | 15 | Relación con el Ciudadano | 2 | 7 | BOYACÁ | 18 | 20 | META | 29 | | | |
| 8 | Gestión Jurídica | 12 | 16 | Servicios Administrativos | 2 | 8 | CALDAS | 18 | 21 | NARIÑO | 35 | | | |
| | TOTAL | | | 86 | | 9 | CAQUETÁ | 34 | 22 | NORTE DE SANTANDER | 7 | | | |
| | | | | | | 10 | CASANARE | 11 | 23 | PUTUMAYO | 29 | TOTAL | 658 | |
| | | | | | | 11 | CAUCA | 9 | 24 | QUINDÍO | 20 | | | |
| | | | | | | 12 | CÉSAR | 5 | 25 | RISARALDA | 41 | | | |
| | | | | | | 13 | CHOCÓ | 23 | 26 | SAN ANDRÉS | 13 | | | |

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

Porcentaje de riesgos de seguridad de la información gestionados: para el tercer cuatrimestre la valoración del indicador se ubica en Adecuado, con un 94,39% (455 cumplidas de 482) de la ejecución de las actividades de los planes de tratamiento que fueron planeadas para este periodo.

ANEXO 3 - CORRECCIONES, CAUSAS Y ACCIONES CORRECTIVAS.

- Se recibió la propuesta de correcciones, análisis de causas y acciones correctivas para la solución de no conformidades el 2021-06-29 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 2021-06-29

| | | |
|---|------------------------------------|-----------------------------|
| SOLICITUD DE ACCIÓN CORRECTIVA | | No. 1 de 2 |
| <input type="checkbox"/> No - Conformidad Mayor <input checked="" type="checkbox"/> No - Conformidad Menor | Norma(s): ISO/IEC 27001:2013 | Requisito(s): 10.1 b) c) |
| Descripción de la no conformidad: | | |
| 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. | | |
| Corrección | Evidencia de Implementación | Fecha |
| Realizar análisis de los datos del primer semestre 2022 de los RFC de emergencia para identificar las causas de la desviación del indicador y definir las actividades de tratamiento. | Acta de reunión | 30/09/2022 |
| - | - | - |

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

INFORME DE AUDITORÍA DE SISTEMAS DE GESTIÓN



| | | |
|---|---|--------------|
| - | - | - |
| Descripción de la (s) causas (s) | | |
| <ol style="list-style-type: none"> 1. Las métricas de medición interna de operación solo se están revisando en las reuniones de seguimiento con los proveedores de servicio y especialistas. 2. La periodicidad de los comités operacionales de gestión de cambios no se ajusta a lo requerido por la operación. 3. Desconocimiento del procedimiento de gestión del cambio de tecnología por algunos de los involucrados. | | |
| Acción correctiva | Evidencia de Implementación | Fecha |
| 1. Ajustar el procedimiento y/o Formato de control de cambios para incluir las Subcategorías de los RFC de emergencias, responsabilidades relacionadas con el PIR y periodicidad de los comités. | Documentos publicados en el portal ICBF con los ajustes requeridos. | 31/10/2022 |
| 2. Dar a conocer a los colaboradores que participan del proceso, la actualización del procedimiento de cambios (DIT y áreas funcionales). | Listados de asistencia o Registro de Asistencia Teams, Captura de Pantalla, Presentación Utilizada o Grabación. | 30/11/2022 |
| 3. Dar a conocer a los Directivos los puntos relevantes de la actualización del procedimiento de cambios. | Listado de Asistencia o Registro de Asistencia Teams y Captura de Pantalla. | 30/11/2022 |
| 4. Incorporar en la agenda de Reunión de Seguimiento DIT, los resultados de las métricas Internas para tomar decisiones en caso de desviaciones. | Acta de reunión o presentación en la cual se evidencie la inclusión de la revisión de las métricas. | 30/10/2022 |

| | |
|--|----------------------|
| SOLICITUD DE ACCIÓN CORRECTIVA | No. 2 de 2 |
| <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 40%;"> <input type="checkbox"/> No - Conformidad Mayor <input checked="" type="checkbox"/> No - Conformidad Menor </div> <div style="width: 30%; text-align: center;"> Norma(s): ISO/IEC 27001:2013 </div> <div style="width: 25%; border: 1px solid black; padding: 5px;"> Requisito(s): 17.1.3 </div> </div> | |

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

INFORME DE AUDITORÍA DE SISTEMAS DE GESTIÓN



| | | |
|---|---|--------------|
| Descripción de la no conformidad: | | |
| 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". | | |
| Corrección | Evidencia de Implementación | Fecha |
| No aplica corrección | No aplica | No aplica |
| - | - | - |
| - | - | - |
| Descripción de la (s) causas (s) | | |
| <ol style="list-style-type: none"> 1. Falta de relación entre los formatos, procedimientos y planes asociados a la Continuidad de la Operación para dar mayor claridad de los pasos a seguir en las pruebas de los escenarios. 2. En el procedimiento P18.DE "PROCEDIMIENTO PLAN DE CONTINUIDAD DE LA OPERACIÓN", no se precisa cuando procede el diligenciamiento del formato F6.PL9.GTI "FORMATO REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN". 3. En el formato F3.P18.DE "INFORME FINAL PLAN DE CONTINUIDAD" no tiene relacionada la verificación de los requisitos de seguridad de la información. | | |
| Acción correctiva | Evidencia de Implementación | Fecha |
| 1. Verificar los formatos, procedimientos y planes asociados a la Continuidad de la Operación. | Acta de reunión con el resultado de la verificación de los formatos, procedimientos y planes. | 30/11/2022 |
| 2. Gestionar los cambios documentación de continuidad de la operación que se requiera conforme a los resultados de la verificación (formatos, procedimientos y planes) ante la SMO. | Correos electrónicos remitidos a la SMO para la modificación o actualización de los documentos. | 30/11/2022 |
| 3. Socializar los cambios de los formatos a los colaboradores que participan o intervienen en la continuidad de la operación. | Listado de asistencias, capturas de pantalla y/o presentación | 30/05/2023 |

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

INFORME DE AUDITORÍA DE SISTEMAS DE GESTIÓN




| | | |
|---|--|------------|
| 4. Realizar prueba de continuidad de la operación en donde se evidencie el cumplimiento de los cambios realizados a los documentos. | Formatos diligenciados conforme a lo definido en el procedimiento P18.DE "PROCEDIMIENTO PLAN DE CONTINUIDAD DE LA OPERACIÓN" | 30/05/2023 |
|---|--|------------|

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](https://www.icontec.org/%e2%80%8bdocumentos-servicios-icontec/) en la ruta <https://www.icontec.org/%e2%80%8bdocumentos-servicios-icontec/> en el link Evaluación de la conformidad.

Ruta: www.icontec.org Nuestra compañía – Documentos servicios – Evaluación de la conformidad.

| | |
|--|--|
| RESULTADOS DE AUDITORÍA: | |
| Número de no conformidades por esquema detectadas en esta auditoría: (0) Mayores (2) menores | |
| Número de no conformidades pendientes que no se cerraron en esta auditoría: (0) menores () N.A. | |
| Plazo para la entrega de propuesta de corrección y acción correctiva (de acuerdo con lo establecido en el R-PS-007) hasta: <u>2022-08-20</u> | |
| Fecha tentativa de verificación complementaria, cuando aplique <u>N.A.</u> | |
| 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 el número de la no conformidad _____ y el requisito al que fue reportada _____. En este caso la organización deberá solicitar una reposición dirigida al Gerente de Certificación. | |
| Nombre del Representante de la Organización: Álvaro Andres Rueda Zapata | Firma:  |

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

INFORME DE AUDITORÍA DE SISTEMAS DE GESTIÓN



| CONFIRMACIÓN DEL CUMPLIMIENTO DE LAS CONDICIONES PARA REALIZAR AUDITORIA CON EL APOYO DE MEDIOS TECNOLÓGICOS | | |
|---|--|---|
| 1 | Medio(s) tecnológico(s) empleado(s): | XT EAMS o OTRA Cuál? _____ |
| 2 | ¿Cuáles actividades de la auditoria o procesos del SG fueron realizados en forma remota? | |
| 3 | ¿El tamaño del muestreo fue suficiente y la organización estaba preparada para suministrar las evidencias solicitadas por este medio? En los casos en los que se haya dado la unión de dos eventos de auditoria, la muestra de los requisitos y procesos a auditar asociados con el control operacional fue suficiente? | X SI o NO |
| 4 | ¿Cuáles herramientas fueron empleadas para la verificación de los procesos de realización o prestación del servicio de manera remota? | No aplica puesto que por el mismo medio se pudo verificar la aplicación del proceso |
| 5 | ¿El tiempo fue suficiente para abarcar todo lo planificado? | X SI o NO |
| 6 | ¿La conexión por medio de la herramienta tecnológica permitió dar inicio y desarrollar la auditoria de acuerdo con los tiempos previstos en el plan de auditoria? | XSI o NO |
| 7. | ¿Se concluye que se cumplieron los objetivos de la auditoria? | X SI o NO |

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

INFORME DE AUDITORÍA DE SISTEMAS DE GESTIÓN



ANEXO 4 - INFORMACIÓN ESPECÍFICA POR CONDICIÓN DE EMERGENCIA

Tipo de emergencia: COVID-19

| VERIFICACIÓN DE RIESGOS Y REQUISITOS MÍNIMOS PARA EL DESARROLLO DE LA AUDITORIA CON EL APOYO DE MEDIOS TECNOLOGICOS | | SI | NO |
|--|--|-----------|-----------|
| 1 | ¿Se cuenta con los requisitos mínimos de conexión y herramienta tecnológica para el desarrollo de la auditoría con el apoyo de medios tecnológicos? | X | |
| 2 | ¿La calidad de la comunicación con el apoyo de medios tecnológicos permite una comunicación eficaz y continua? | X | |
| 3 | ¿El uso de medios tecnológicos permite el mantenimiento de la confidencialidad y seguridad de la información? Nota: confirmar con la empresa si está de acuerdo en compartir información a través de la herramienta tecnológica. | X | |
| 4 | ¿Se cuenta con los requisitos mínimos de información (acceso a la información de los procesos en medio digital o electrónico o escaneado en el momento que el auditor lo solicite durante el ejercicio en vivo)? | X | |
| 5 | ¿Las actividades Core del negocio incluidas en el alcance de la certificación, pueden ser verificadas por medio remoto? | X | |
| 6 | ¿La organización está en funcionamiento, es decir que las actividades CORE del negocio, a incluir en el alcance de la certificación se están desarrollando conforme los requisitos establecidos en la norma de referencia del sistema de gestión a auditar? Nota. En el caso que la respuesta sea NO porque no está realizando ninguna de las actividades CORE del negocio, informar al Coordinador de programación y al Ejecutivo de Cuenta, que se debe reprogramar la auditoría. | X | |
| 7 | ¿La auditoría con el apoyo de medios tecnológicos a las actividades Core del negocio incluidas en el alcance de la certificación puede afectar la calidad o seguridad del producto o servicio? Nota: confirmar con la empresa si se puede hacer uso de herramientas tecnológicas durante la auditoría a las actividades de prestación del servicio, ej: usar cámaras en un banco o durante la atención en salud, etc. | | X |
| 8 | ¿Si las actividades del Core del negocio son prestadas fuera de las instalaciones de la organización, ¿estas pueden ser verificadas por medios remotos? | X | |
| 9 | ¿El personal de la organización cuenta con la disposición y competencia para el atender la auditoría con el apoyo de medios tecnológicos? Nota: se espera que la empresa confirme que las personas que van a recibir la auditoría están capacitadas en el uso de la herramienta. | X | |
| 10 | ¿Se detectaron otros riesgos de alto impacto que no permiten el desarrollo de la auditoría? Por favor relacione los otros riesgos identificados: Con respecto al desempeño del Sistema de Gestión Integrado del Banco de la República, es importante mencionar que se evidencian bases estructurales 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. | | X |
| 11 | De encontrar situaciones que generen riesgos en relación con las preguntas 1 a 10, ¿consideran que éstos pueden ser mitigados o eliminados para la realización de la auditoría etapa 2 con la utilización de herramientas tecnológicas? | x | |

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

INFORME DE AUDITORÍA DE SISTEMAS DE GESTIÓN



| | | | | | | | | | |
|---------------------|--|-------------------|----|---------------------|--|---------------------|--|--|--|
| | <p>Explique su respuesta, incluyendo los métodos que se utilizarán para mitigar los riesgos</p> <ul style="list-style-type: none"> • No asegurar las condiciones de infraestructura para la prestación del servicio: este se mitiga destinando 0,5 días para la visita. • No contar con la información necesaria para verificar los requisitos de los procesos: se enviará una propuesta de planificación con el fin de acordarla con la organización teniendo en cuenta la disponibilidad de la información y validan la necesidad de verificar procesos en sitio. • Por la situación actual de la emergencia sanitaria se realizará verificación de la modalidad de enseñanza con medios remotos según lo definido por la Entidad. <p>Nota. Recuerde que se generan riesgos si la respuesta a las preguntas 1 a 5, 6, 8 y 9 es NO, y las correspondientes a las preguntas 7 y 10 es SI.</p> | | | | | | | | |
| 12 | <p>En los casos en que se haya autorizado por parte de la UT realizar cambio de modalidad de parcialmente remoto a totalmente remoto con la participación de un profesional de apoyo, ¿se comunicó a la organización el rol del profesional de apoyo?</p> <p>o SI o NO</p> <p>¿Se cuenta con el consentimiento de la organización, incluyendo el compromiso con el suministro de los medios tecnológicos requeridos para asegurar la conectividad?</p> <p>o SI o NO</p> | | NA | | | | | | |
| 13 | <p>De acuerdo con el análisis de riesgos realizado y teniendo en cuenta los objetivos de la auditoría se concluye que se puede realizar la auditoría (Marcar con una X en frente de la metodología seleccionada):</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 80%;">Totalmente remota</td> <td style="width: 20%; text-align: center;">X</td> </tr> <tr> <td>Parcialmente remota</td> <td></td> </tr> <tr> <td>Totalmente en sitio</td> <td></td> </tr> </table> | Totalmente remota | X | Parcialmente remota | | Totalmente en sitio | | | |
| Totalmente remota | X | | | | | | | | |
| Parcialmente remota | | | | | | | | | |
| Totalmente en sitio | | | | | | | | | |

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización

ANEXO 5

Declaración de aplicación (solo para ISO 28001)

No aplica

Este informe es propiedad de ICONTEC y se comunicará después de la auditoría únicamente a la Organización y no será divulgado a terceros sin autorización de la Organización