INFORME EJECUTIVO

Auditoría Interna al Sistema de Gestión de Seguridad de la Información NTC- ISO/IEC 27001:2013

FECHA DE COMUNICACIÓN	20/04/2020
INICIO – TERMINACIÓN (Fase de Ejecución)	09/03/2020 - 13/03/2020

EQUIPO:

Rol	Nombre	Cargo/Contratista
Directora	Yanira Villamil S.	Jefe Oficina Control Interno
Supervisora	Flor Alicia Rojas Aguilar	Coordinadora Grupo de Procesos Misionales
Líder	Lucerito Achury Carrion	Ingeniera de Sistemas - Contratista
Equipo Auditor	Maria Lucerito Achury Carrión	Ingeniera de Sistemas (Certificado Inlac No. 15-10-4590) - Contratista

1. OBJETIVOS:

Objetivo general

Evaluar el Sistema de Gestión de Seguridad de la Información NTC-ISO-IEC 27001 Versión 2013 en el Instituto Colombiano de Bienestar Familiar - Regional Bogotá y Sede Centro Especializado Puente Aranda.

Objetivos específicos

- Determinar si el Sistema de Gestión de Seguridad de la Información en la Regional Bogotá y Sede Centro Especializado (CESPA) Puente Aranda:
    - Es conforme con los requisitos de la organización para su sistema de gestión de la seguridad de la información y con los requisitos de la Norma Técnica NTC ISO IEC 27001:2013.
    - Está implementado y mantenido eficazmente.

- Identificar Oportunidades de Mejora.
- Realizar seguimiento a los hallazgos de auditorías internas anteriores al Sistema de Gestión de la Seguridad de la Información.

2. ALCANCE:

Procesos: Direccionamiento Estratégico, Monitoreo y Seguimiento a la Gestión, Mejora e Innovación, Gestión de la Tecnología e Información, Gestión del Talento Humano, Adquisición de Bienes y Servicios, Gestión Jurídica, Servicios Administrativos, Promoción y Prevención, Protección, Comunicación Estratégica, Gestión Financiera, Relación con el Ciudadano, Coordinación y Articulación del SNBF y Agentes, Inspección, Vigilancia y Control, aplicables a la Regional y Centro Especializado (CESPA) Puente Aranda.

Periodo: 01 de enero de 2019 al 29 de febrero de 2020.

Sede: Regional Bogotá.
Centro Zonal Especializado Puente Aranda.

3. RELACIÓN DE HALLAZGOS

NUMERO DE CONFORMIDADES	NUMERO DE NO CONFORMIDADES
72	17

4. OTRAS SITUACIONES

No BUENAS PRÁCTICAS	No RIESGOS	No OPORTUNIDADES	No RECOMENDACIONES DE MEJORA
0	0	0	4

5. CONCLUSIONES

De acuerdo con los objetivos, el alcance, los procesos, la muestra y los puntos considerados para la auditoría interna al Sistema de Gestión de Seguridad de la Información se concluye por parte de la Oficina de Control Interno que el Sistema de Gestión de Seguridad de la Información del ICBF bajo la norma NTC ISO IEC 27001:2013, numerales auditados en la Regional Bogotá y Centro Especializado Puente Aranda, refleja los siguientes resultados:

- **Numerales Conformes:**

4.1. Conocimiento de la Organización y de su Contexto, 4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas, 4.4 Sistema de Gestión de Seguridad de la Información, 5.1 Liderazgo y Compromiso, 5.3 Roles, Responsabilidades y Autoridades en la Organización, 6. Planificación, 7.1 Recursos, 7.2 Competencia, 7.3. Toma de Conciencia, 7.4 Comunicación, 7.5.1 Generalidades, 7.5.2 Creación y Actualización, 9.1 Seguimiento medición y análisis y 9.3 Revisión por la Dirección.

- **Cumplimiento de los objetivos de control:**

A.6 Organización de la Seguridad de la Información, A.12 Seguridad en las Operaciones, A.16 Gestión de Incidentes de Seguridad de la Información y A.17 Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio.

- **Cumplimiento parcial en los requisitos:**

7.5.3 Información Documentada, 8. Operación y 10. Mejora y en los controles: A.7 Seguridad de los Recursos Humanos, A.8 Gestión de Activos, A.9 Control de Acceso, A.11 Seguridad Física y del Ambiente y A.13 Seguridad de las Comunicaciones y A.18 Cumplimiento.

- **Numerales y Controles con No Conformidades:**

7.5.3 Control de la Información Documentada, 8.1 Planificación y Control Operacional y 10.1 No Conformidades y Acciones Correctivas y en los controles: A.7.3.1 Terminación o cambio de responsabilidades de empleo, A.8.1.4 Devolución de activos, A.8.2.2. Etiquetado de la información, A.8.3.2 Disposición de los medios, A.9.2.1 Registro y cancelación del registro de usuarios, A.11.1.4 Protección contra amenazas externas y ambientales, A.11.2.2 Servicios de

Suministro, A.11.2.3 Seguridad del Cableado, A.11.2.5 Retiro de Activos, A.11.2.7 Disposición Segura o Reutilización de equipos, A11.2.9 Política de Escritorio Limpio y Pantalla Limpia y A13.2.4 Acuerdos de confidencialidad y de no divulgación y A18.1.4 Privacidad y protección de información de datos personales.

- **Recomendaciones para la mejora en los controles**:

7.3.1 Terminación o cambio de responsabilidades de empleo, A.11.1.4 Protección contra amenazas externas y ambientales y A.11.2.1 Ubicación y protección de los equipos

Nota. El objetivo de control A.14 Adquisición, desarrollo y mantenimiento de sistemas no aplicó para la Regional en esta auditoría, teniendo en cuenta que no se evidenciaron solicitudes de adquisición, desarrollo y mantenimiento de sistemas de información en la Regional.

Eficacia

Bajo los parámetros en que se desarrolló el ejercicio de auditoría interna se pudo determinar que en la Dirección Regional Bogotá y Centro Especializado Puente Aranda el Sistema Integrado de Gestión del ICBF (eje de Seguridad de la Información) se implementa y se mantiene; sin embargo, se requiere dar tratamiento a las No Conformidades detectadas con el fin de que la Entidad mejore continuamente la Eficacia del mismo.

6. RECOMENDACIONES

Desde el proceso de Gestión del Talento Humano fortalecer la gestión documental con el fin de ubicar fácilmente la documentación que soporta los cambios en los términos y condiciones del empleo de los funcionarios de la Regional Bogotá.

Desde el proceso de Gestión de Contratación fortalecer la gestión documental con el fin de disponer la documentación cuando se terminan los contratos por prestación de servicios profesionales de la Regional Bogotá.

Desde el Proceso de Servicios Administrativos reforzar la ventana del archivo del Centro Especializado Puente Aranda que comunica con el CESPA con el fin de evitar el ingreso de elementos en caso de presentarse disturbios en el mismo.

Desde el Proceso de Gestión de la Tecnología evitar que los equipos de cómputo se ubiquen e instalen directamente en el piso para protegerlos de golpes o que les caiga líquidos cuando los colaboradores de servicios generales realizan labores de aseo.

Atentamente,

Yanira Villamil S.
Jefe de Oficina de Control Interno

Consolidó datos: Gina Yepes Skiner/OCI GYSK

Revisó: Lucerito Achury Carrion/Líder de Auditoría OCI ; Flor Alicia Rojas/ Coordinadora GPM OCI