INFORME EJECUTIVO

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

FECHA DE COMUNICACIÓN	17/10/2019
INICIO – TERMINACIÓN (fase de ejecución)	26/08/2019 hasta 30/08/2019

EQUIPO:

Rol	Nombre	Cargo/Contratista
Directora	Flor Alicia Rojas Aguilar	Jefe Oficina Control Interno (E)
Supervisora	Angela Patricia Panesso	Coordinadora Grupo de Procesos Misionales
Líder	Giovanni Esteban Martínez Bueno	Ingeniero de Sistemas – Contratista (Certificado 43082537/133653404)
Equipo Auditor	Giovanni Esteban Martínez Bueno	Ingeniero de Sistemas – Contratista (Certificado 43082537/133653404)

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 Guainía y Centro Zonal Inírida.

Objetivos específicos

Determinar si el Sistema de Gestión de Seguridad de la Información en la Regional Guainía y Centro Zonal Inírida.

- 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

- Esta implementado y mantenido eficazmente

- Identificar Oportunidades de Mejora.

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, Comunicación Estratégica, Gestión Financiera, Relación con el Ciudadano, Coordinación y Articulación del SNBF y Agentes, Inspección, Vigilancia y Control.

Periodo: 1 de enero de 2018 al 31 de julio de 2019.

Sede: Regional Guainía.
CZ Inírida

3. RELACIÓN DE HALLAZGOS

NUMERO DE CONFORMIDADES	NUMERO DE NO CONFORMIDADES
67	13

4. OTRAS SITUACIONES

BUENA PRÁCTICA	No RIESGOS	No OPORTUNIDADES	No RECOMENDACIONES DE MEJORA
0	0	0	1

5. CONCLUSIONES

Una vez culminado el proceso de auditoría interna al Sistema de Gestión de Seguridad de la Información del ICBF Regional Guainía y Centro Zonal Inírida se pudo determinar que este es conforme con los requisitos establecidos por la Entidad y frente a los requisitos de la Norma NTC-ISO-IEC 27001:2013; adicionalmente, se está implementando y manteniendo eficazmente dando cumplimiento a los controles definidos en el Anexo 3. Declaración de Aplicabilidad del Manual del Sistema Integrado de Gestión a Nivel Regional y de los Centros Zonales.

En el proceso de la auditoría, se evidenció:

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, 9.1 Seguimiento, medición, análisis y evaluación, 9.3 Revisión por la Dirección y 10. Mejora.

Cumplimiento de los objetivos de control: A.6.1.1 Roles y responsabilidades para la seguridad de la información, A.6.1.2 Separación de deberes, A.6.1.3 Contacto con las autoridades, A.6.1.5 Seguridad de la información en la gestión de proyectos, A.6.2.1 Política para dispositivos móviles, A.6.2.2 Teletrabajo, A.7.1.1 Selección, A.7.1.2 Términos y condiciones del empleo, A.7.2.1 Responsabilidades de la dirección, A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información, A.7.2.3 Proceso disciplinario, A.8.1.1 Inventario de activos, A.8.1.3 Uso aceptable de los activos, A.8.1.4 Devolución de activos, A.8.2.1 Clasificación de la información, A.8.2.2 Etiquetado de la información, A.8.2.3 Manejo de activos, A.8.3.1 Gestión de medios removibles, A.8.3.2 Disposición de los medios, A.8.3.3 Transferencia de medios físicos, A.9.1.1 Política de control de acceso, A.9.1.2 Acceso a redes y a servicios en red, A.9.2.1 Registro y cancelación del registro de usuarios, A.9.2.2 Suministro de acceso de usuarios, A.9.2.3 Gestión de derechos de acceso privilegiado, A.9.2.4 Gestión de información de autenticación secreta de usuarios, A.9.2.5 Revisión de los derechos de acceso de usuarios, A.9.2.6 Retiro o ajuste de los derechos de acceso, A.9.3.1 Uso de información de autenticación secreta, A.11.1.1 Perímetro de seguridad física, A.11.1.5 Trabajo en áreas seguras, A.11.1.6 Áreas de despacho y carga, A.11.2.2 Servicios de suministro, A.11.2.4 Mantenimiento de equipos, A.11.2.5 Retiro de activos, A.11.2.7 Disposición segura o reutilización de equipos, A.12.1.1 Procedimientos de

operación documentados, A.12.1.3 Gestión de capacidad, A.12.2.1 Controles contra códigos maliciosos, A.12.3.1 Respaldo de la información, A.12.6.2 Restricciones sobre la instalación de software, A.13.1.1 Controles de redes, A.13.1.3 Separación en las redes, A.13.2.1 Políticas y procedimientos de transferencia de información, A.13.2.4 Acuerdos de confidencialidad o de no divulgación, A.14.1.1 Análisis y especificación de requisitos de seguridad de la información, A.16.1.2 Reporte de eventos de seguridad de la información, A.16.1.3 Reporte de debilidades de seguridad de la información, A.17.1.1 Planificación de la continuidad de la seguridad de la información, A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información, A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales, A.18.1.2 Derechos de propiedad intelectual, A.18.1.3 Protección de registros, A.18.1.4 Privacidad y protección de información de datos personales, A.18.2.2 Cumplimiento con las políticas y normas de seguridad.

Cumplimiento parcial en el requisito: 7.5.3 Control de la Información Documentada, 8.1 Planificación y control operacional y en los controles: A.7.3.1 Terminación o cambio de responsabilidades de empleo, A.8.1.2 Propiedad de los activos, A.11.1.2 Controles de acceso físicos, A.11.1.3 Seguridad de oficinas, recintos e instalaciones, A.11.1.4 Protección contra amenazas externas y ambientales, A.11.2.1 Ubicación y protección de los equipos, A.11.2.3 Seguridad del cableado, A.11.2.4 Mantenimiento de equipos, A.11.2.8 Equipos de usuario desatendido, A.11.2.9 Política de escritorio limpio y pantalla limpia, A.17.1.2 Implementación de la continuidad de la seguridad de la información.

Recomendaciones para la mejora: en el requisito 8.1 Planificación y control operacional.

Eficacia:

Bajo los parámetros en que se desarrolló el ejercicio de auditoría interna se determina que en la Regional Guainía, el Sistema 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 de la Tecnología e Información gestionar con la Subdirección de Recursos Tecnológicos de la Sede de la Dirección General que se brinde orientación y

herramientas al ingeniero regional con el fin de mejorar la supervisión y/o control de la calidad de los servicios locales de TI.

Atentamente,

Yanira Villamil S.
Jefe de Oficina de Control Interno

Consolidó datos: Gina Yepes Skiner/OCI GYSK

Revisó: Giovanni Esteban Martínez/Líder de Auditoría OCI_____; Flor Alicia Rojas/ Coordinadora GPM OCI_____