

INFORME EJECUTIVO

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

FECHA DE COMUNICACIÓN	18/11/2019
INICIO – TERMINACIÓN	07/10/2019 hasta 11/10/2019

EQUIPO:

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

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 Chocó y Sede Centro Zonal Quibdó.

Objetivos específicos

Determinar si el Sistema de Gestión de Seguridad de la Información en la Regional Chocó y Sede Centro Zonal Quibdó:

- 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 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.

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

Sede: Regional Chocó
CZ Quibdó

3. RELACIÓN DE HALLAZGOS

NUMERO DE CONFORMIDADES	NUMERO DE NO CONFORMIDADES
73	14

4. OTRAS SITUACIONES

BUENA PRÁCTICA	No RIESGOS	No OPORTUNIDADES	No RECOMENDACIONES DE MEJORA
1	0	0	2

5. CONCLUSIONES

De acuerdo con los objetivos, el alcance, los procesos, la muestra y los puntos considerados para la auditoría interna al Sistema Integrado de Gestión 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 Chocó y Centro Zonal Quibdó se refleja en 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, 7.2.2 Toma de Conciencia, 7.4 Comunicación, 9. Evaluación del Desempeño y 10. Mejora.

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 Información Documentada y 8. Operación 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, A.13 Seguridad de las Comunicaciones y A.18. Cumplimiento.

Recomendaciones para la mejora en los controles: A.12.2.1 Controles contra código malicioso y A.18.1.4 Privacidad y protección de información de datos personales.

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 determina que en la Regional Chocó, 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 información, verificar y actualizar el antivirus en los equipos que se requiera.

Desde el Proceso de Servicios Administrativos instalar el aviso de protección de datos personales (en acrílico) ya que se observó a la entrada de la Regional una fotocopia publicada en la cartelera.

Atentamente,



Yanira Villamil S.
Jefe de Oficina de Control Interno

Consolidó datos: Gina Yepes Skinner/OCI GYSK

Revisó: Maria Lucerito Achury Carrion/OCI _____; Flor Alicia Rojas/ Coordinadora GPM OCI Flor

PUBLICA