UNGRD
Unidad Nacional para la Gestión del Riesgo de Desastres
Sistema Nacional de Gestión del Riesgo de Desastres

Informe Auditoria Interna

Sistema de Gestión en Seguridad de la Información
ISO/IEC 27001:2013

22/08/2023

OFICINA DE CONTROL INTERNO

FR-1400-OCI-31 VERSIÓN 06

GOBIERNO DE COLOMBIA

Tabla de contenido

1. INTRODUCCIÓN

La Norma Técnica Colombiana NTC-ISO-27001:2013 ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de la seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización. Se espera que todos estos factores de influencia cambien con el tiempo.

El sistema de gestión de la seguridad de la información preserva la confidencialidad, la integridad y la disponibilidad de la información, mediante la aplicación de un proceso de gestión del riesgo, y brinda confianza a las partes interesadas acerca de que los riesgos son gestionados adecuadamente.

Es importante que el sistema de gestión de la seguridad de la información sea parte de los procesos y de la estructura de gestión total de la información de la organización y que esté integrado con ellos, y que la seguridad de la información se considere en el diseño de procesos, sistemas de información y controles. Se espera que la implementación de un sistema de gestión de seguridad de la información se difunda de acuerdo con las necesidades de la organización.

Por tal motivo y en consonancia con lo dispuesto en el numeral 9.2 Auditoría Interna. *"La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información a) es conforme con: 1) los propios requisitos de la organización para su sistema de gestión de la seguridad de la información; y 2) los requisitos de esta Norma; y b) si está implementado y es mantenido eficazmente*", la oficina de control interno de la UNGRD programó la auditoría al Sistema de Seguridad de la Información de la entidad con los siguientes objetivos.

2. OBJETIVOS

2.1 OBJETIVO 1

Verificar el cumplimiento de las disposiciones planificadas en el Sistema de Gestión de Seguridad de la Información aplicables, evaluando los requisitos de la Norma ISO/IEC 27001:2013 y de los requisitos establecidos.

2.2 OBJETIVO 2

Comprobar que se han implementado y se mantienen de manera eficaz los controles, determinando cómo las directrices dadas por la norma ayudan a la Entidad a mantener todas sus operaciones seguras.

3. ALCANCE

Aplica a todos los procesos del Sistema de Gestión Integrado;

Procesos Estratégicos: Gestión Gerencial, Planeación Estratégica, Sistema Integrado de Planeación y Gestión; Gestión Jurídica, Gestión de Tecnología de la Información, Gestión Comunicaciones, servicio al ciudadano;

Procesos Misionales: Gestión de Conocimiento del Riesgo, Gestión de Reducción del Riesgo, Gestión de Manejo de Desastres;

Procesos de Apoyo: Gestión Financiera, Gestión para Cooperación Internacional, Gestión Contratación, Gestión de Control Disciplinario, Gestión de Talento Humano, Gestión Administrativa, Centro Logístico Nacional;

Procesos de Evaluación: Evaluación y seguimiento; así como todos los niveles y Gerencias de la Entidad.

4. METODOLOGÍA

La Auditoria Interna la Sistema de Gestión en Seguridad de la Información se desarrolla bajo una metodología presencial evaluando el cumplimiento de requisitos y la evidencia objetiva que se haya generado como resultado de la gestión del sistema implementado.

5. MARCO LEGAL

Documentos del Sistema de gestión bajo ISO/IEC 27001:2013.

Las obligatoriedades contraídas por requisitos legales se encuentran definidas como aplicables para cada uno de los procesos necesarios de la Entidad, descritos y analizados en el normograma aprobado para el Sistema de Gestión en Seguridad de la Información.

Requisitos Contractuales, Documentos necesarios aprobados por la Entidad.

6. VERIFICACIÓN DE ANTECEDENTES

Para el desarrollo del presente informe se toman como insumos base para la realización de la auditoría los resultados obtenidos en la última auditoria del Sistema de Gestión de Seguridad de la Información de la Unidad Nacional para la Gestión del Riesgo de Desastres – UNGRD y los documentos soporte de los procesos objeto de auditoría, relacionados con Seguridad de la Información.

7. DESARROLLO DEL INFORME

En atención a las actividades desarrolladas en los procesos objeto de la presente auditoria en Seguridad de la Información se obtuvieron los siguientes resultados:

7.1 FORTALEZAS:

1. El soporte brindado por Gestión de Tecnologías de la Información permite desarrollar actividades confiables y lo proyectan en gestión para llegar a ser un proceso independiente; las actividades generadas asociadas al control de riesgos ayudan a desarrollar actividades en Operación confiables y controladas.

2. Los resultados del sistema se evidencian en la planificación y acompañamiento de los Líderes de proceso, estos elementos fortalecen las operaciones y ayudan a garantizar eficacia en los controles en la Entidad.

3. La Dirección de la Entidad se encuentra comprometida en el avance y logro de los resultados previstos del Sistema de Gestión, hecho que fortalece y permite el logro de las actividades programadas, así como el aumento en la toma de Conciencia.

4. Los controles establecidos en el proceso de Gestión Administrativa aseguran mantener niveles de inventarios adecuados con proveedores confiables en la operación.

5. En el proceso de Gestión Conocimiento Riesgo al mantener trazabilidad en los Diseños generados permite mitigar riesgos en la obtención de productos finales, de acuerdo con los requisitos establecidos.

6. El soporte brindado por Gestión de Tecnología de la Información permite desarrollar actividades confiables en operaciones, gestión del riesgo y protección de activos.

7. Se evidencia una buena metodología para la evaluación de riesgos de la entidad y se evidencia seguimiento por parte del líder del proceso y de control interno dejando como soporte de: Evidencias, diseño de controles, efectividad de los controles, materialización del riesgo, recomendaciones, plan de tratamiento.

8. Se evidencia la asignación del rol de líderes SIPLAG y Ecosiplag, lo cual permite contar con una persona líder por dependencia con información directa del SIPLAG y a su vez bajar esta información a los diferentes niveles de la UNGRD.

9. Compromiso por parte del equipo de planeación para garantizar el mejoramiento continuo del Sistema integrado de gestión.

7.2 HALLAZGOS DE NO CONFORMIDAD:

No Conformidad No. 1:

La organización no garantiza la socialización de las responsabilidades del SGSI a sus funcionarios y contratistas, evidenciado en:

Gestión de tecnologías de la información: No se evidencia socialización de las responsabilidades en cuanto al SGSI, a su vez no se evidencia socialización del acuerdo de confidencialidad en términos de seguridad de la información de las funcionarias Ana María Castaño Álvarez - Cargo: secretaria general - Dependencia: secretaria general, Jhoanna Pino - Cargo: secretario ejecutivo, Dependencia: Oficina de control interno, y contratista Ingrid Vanesa Suarez - Profesional – Dependencia: Talento Humano.

Esta situación es un incumplimiento al numeral 5.3 Roles, responsabilidades y autoridad en la organización de la norma ISO 27001:2013, la cual dice: *"La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen."*

No Conformidad No. 2:

No se garantiza que se valide los controles determinados por la entidad con los correspondientes al anexo A, esto se evidencia en:

Gestión de tecnologías de la información: No se encuentra el comparativo de los controles determinados en la Entidad con los controles del Anexo A, ni la verificación de que no se han omitidos controles necesarios.

Esta situación es un incumplimiento al numeral 6.1.3 tratamiento de riesgos de la seguridad de la información literal c) de la norma ISO 27001:2013, la cual dice: "*La organización debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información para comparar los controles determinados en 6.1.3 b) con los del Anexo A, y verificar que no se han omitidos controles necesarios.*"

No Conformidad No. 3:

La organización no define la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles del Anexo A.

Gestión de tecnologías de la información: La Declaración de Aplicabilidad RG-1101-GTI-05_02 V2 270422 presenta inconsistencias en su contenido y en los controles implementados en el SG-SI. En los numerales A6.1.2, A6.1.3, A6.1.4, A6.1.5, A7.2.1, A8.1.1, A8.1.2, A8.1.3, A8.3.3, A9.1.2, A9.2.3, A9.4.5, A11.1.1, A11.1.2, A.11.1.3, A11.1.6, A12.2.1, A12.2.2, A12.2.3, A12.1.3, A12.2.1, A12.4.2, A12.4.3, A12.4.4, A12.6.1, A12.7.1, A13.1.2, A13.1.3, A14.1.2, A14.1.3, A14.2.1, A14.2.4, A14.2.5, A14.2.6, A14.2.9, A14.3.1, A17.1.3, A17.2.1, A18.1.3 y A18.2.3, se describen controles que no corresponden con los controles reales que se mantienen implementados en el Proceso de Gestión de Tecnologías de la Información.

Esta situación es un incumplimiento al numeral 6.1.3 tratamiento de riesgos de la seguridad de la información literal d) de la norma ISO 27001:2013, el cual dice que*: "la organización debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información para producir una declaración de aplicabilidad que contenga los controles necesarios (véanse el numeral 6.1.3 b) y c)) y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles del Anexo A"*

No Conformidad No. 4:

No se evidencia aprobación de los dueños de los riesgos, con relación al plan de tratamiento de riesgos de la seguridad de la información, y la aceptación de los riesgos residuales de la seguridad de la información

Gestión de tecnologías de la información: No se ha obtenido de parte de los responsables de los riesgos la aprobación del plan de tratamiento de riesgos de la

seguridad de la información, ni la aceptación de los riesgos residuales de la seguridad de la información.

Esta situación es un incumplimiento al numeral 6.1.3 tratamiento de riesgos de la seguridad de la información literal f) de la norma ISO 27001:2013, el cual dice que: *"La organización debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información para obtener de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos de la seguridad de la información, y la aceptación de los riesgos residuales de la seguridad de la información"*

No Conformidad No. 5:

No se garantiza que los registros y documentos se identifiquen y controlen de acuerdo con los requisitos establecidos en el Procedimiento de Control de Documentos PR–1300-SIPG-07_9 V9 230222, Procedimiento de Control de Registros PR-1300-SIPG-06_7 V7 010722 y Guía de parametrización de Documentos G-1300-SIPG-01 V5 270921, que aplican a la información Documentada del Sistema de Gestión en Seguridad de la Información de la entidad.

Gestión de tecnologías de la información: Metodología DOFA Registro: RG-1300-PE-09_01 V1 sin fecha de actualización; la Matriz de Riesgo de SI FR-1101-GTI-05 V3 301222 con aplicación en el Registro, sin fecha de actualización; la matriz de Riesgo no cumple con lo establecido en la Guía de Parametrización de Documentos G-1300-SIPG-01 V5 270921, el formato aprobado se encuentra con descripción FR-1101-GTI-05 V3 301222 y el formato en uso se encuentra con descripción FR-1101-GTI-05 V1 301222; la matriz de Riesgo no cuenta con un control establecido para registros; en el SIPLAG se mantiene referenciada la descripción RG-1101-GTI-04_4 V4 301222, en el registro en uso se referencia codificación del formato y nombre del archivo con codificación de registro y la Nueva Declaración de Aplicabilidad no cumple con lo establecido en la Guía de parametrización de Documentos G-1300-SIPG-01 V5 270921, donde se establece el uso de encabezados para todos los tipos de documentos del SIG.

Esta situación es un incumplimiento al numeral 7.5 Información documentada de la norma ISO 27001:2013. La Información Documentada del Sistema de Gestión en Seguridad de la Información se debe identificar y controlar de acuerdo con los requisitos establecidos en los Documentos de Control Documentos, Control de Registros y parametrización de Documentos del SG-SI, Procedimiento de Control de Documentos PR–1300-SIPG-07_9

V9 230222, Procedimiento de Control de Registros PR-1300-SIPG-06_7 V7 010722 y Guía de parametrización de Documentos G-1300-SIPG-01 V5 270921.

No Conformidad No. 6:

La entidad no garantiza la aplicabilidad del procedimiento de Gestión del Cambio implementada en SG-SI para las nuevas aplicaciones y actualización de la Declaración de Aplicabilidad.

Lo anterior incumpliendo el numeral 8.1 Planificación y control operacional de la norma ISO 27001:2013, la cual dice “la organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acciones para mitigar los efectos adversos, cuando sea necesario”.

8. CONTROLES ESTABLECIDOS

Los controles del Sistema de Gestión en Seguridad de la Información se encuentran establecidos en la Declaración de Aplicabilidad RG-1101-GTI-05_02 V2 270422, documento en modificación.

9. RIESGOS IDENTIFICADOS

Falta de control en los accesos restringidos de los usuarios internos de UNGRD a las redes sociales y páginas de ocio.

Perdida de la información por almacenamiento en los correos o escritorios de los equipos de cómputo.

10. CONCLUSIONES

- Con base al ejercicio de auditoría interna se generar 6 No Conformidades y 2 Observaciones.

- Se pudo verificar el cumplimiento de las disposiciones planificadas en el Sistema de Gestión de Seguridad de la Información aplicables, evaluando los requisitos de la Norma ISO/IEC 27001:2013 y de los requisitos establecidos.

- Se logró comprobar que se han implementado y se mantienen de manera eficaz los controles, determinando cómo las directrices dadas por la norma ayudan a la Entidad a mantener todas sus operaciones seguras.

11. OBSERVACIONES

Planeación estratégica:

1. Se evidencian dos archivos de presupuesto en el equipo del profesional William Wilches, con base a la política de seguridad de la información está prohibida esta práctica.

Control interno disciplinario:

2. Durante el proceso de auditoria se evidencia acceso a la página de YouTube por parte de la líder de Control Interno Disciplinario.

12. PAPELES DE TRABAJO

Plan de Auditoria FR-1400-OCI-07_2 V2
Lista de Chequeo FR-1400-OCI-29_1 V1
Informe de Auditoria Interna FR-1400-OCI-31_6 V6

13. PLAN DE MEJORAMIENTO

Conforme a lo establecido en el procedimiento PR-1400-OCI-11 Auditorías Internas de Gestión, se deben levantar acciones correctivas, preventivas y/o de mejora por parte del líder del proceso acorde con el procedimiento establecido en el proceso SIPLAG, dentro de los cinco (5) días hábiles siguientes a la recepción del informe, las cuales deben ser informadas por el Líder del proceso al Jefe de la Oficina de Control Interno para programar su verificación en el mes siguiente de su reporte.

Ahora bien, es importante anotar que, debido a las limitaciones de cualquier estructura de control interno, pueden ocurrir errores o irregularidades que no hayan sido detectadas bajo la ejecución de nuestros procedimientos de auditoría, evaluación o seguimiento, previamente planeados. La Unidad y las áreas que la componen, son responsables de establecer y mantener un adecuado sistema de control interno y de prevenir posibles irregularidades de acuerdo con lo establecido en el Modelo Integrado de Planeación y Gestión para las tres líneas de defensa

Así mismo, es responsabilidad del área la información suministrada, por cualquier medio, para la realización de esta actividad de manera oportuna, completa, integra y actualizada y la de informar en su momento las posibles situaciones relevantes y/o errores que pudieran haber afectado el resultado final de la actividad.

14. SALVAGUARDAS

Cabe resaltar que, debido a las limitaciones de cualquier estructura de control interno, pueden ocurrir errores o irregularidades que no hayan sido detectadas bajo la ejecución de nuestros procedimientos de auditoría, evaluación o seguimiento, previamente planeados.

La Unidad y las áreas que la componen, son responsables de establecer y mantener un adecuado sistema de control interno y de prevenir posibles irregularidades de acuerdo con lo establecido en el Modelo Integrado de Planeación y Gestión para las tres líneas de defensa.

Asimismo, es responsabilidad del área la información suministrada, por cualquier medio, para la realización de esta actividad de manera oportuna, completa, integra y actualizada y la de informar en su momento las posibles situaciones relevantes y/o errores que pudieran haber afectado el resultado final de la actividad.

Cordialmente,

ORIGINAL FIRMADO

Javier Herrera
Ingeniero Industrial
Auditor Líder ISO 9001:2015, ISO 45001:2018, ISO 14001:2015, ISO 27001

ORIGINAL FIRMADO

Alejandra Moreno Pico
Ingeniera Industrial
Auditor Líder ISO 9001:2015, ISO 45001:2018, ISO 14001:2015
Auditor Interno ISO 27001