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

Sistema Integrado de Planeación y Gestión de la UNGRD certificado en:

Informe de Auditoria a la Estrategia de Gobierno en Línea (Seguridad y Privacidad de la Información)

Oficina de Control Interno

29 de Diciembre 2017

TABLA DE CONTENIDO

I. OBJETIVO

Verificar el cumplimiento de los requisitos aplicables al proceso de Gestión de Sistemas de Información y al subproceso de Gestión de Infraestructura Tecnológica, frente a la norma NTC-ISO 27001:2013 y a las disposiciones de la Estrategia de Gobierno en Línea, en su componente de Seguridad y Privacidad de la Información para evaluar su nivel de madurez.

II. ALCANCE

La auditoría corroborará las actividades adelantadas por el proceso de Gestión de Sistemas de Información y el subproceso de Gestión de Infraestructura Tecnológica, desde el 01 enero de 2017 al 31 octubre de 2017, relacionadas con el componente de seguridad y privacidad de la información definido en la Estrategia de Gobierno en Línea.

III. METODOLOGÍA

La presente auditoria fue de tipo documental en donde se verificó la información documentada exigida por la Norma NTC-ISO-IEC 27001: 2013 en el procesos de Gestión de Sistemas de Información y en el subproceso de Gestión de Infraestructura Tecnológica, así como los indicadores y controles establecidos, y la manera en que son gestionados los riesgos asociados al proceso.

IV. MARCO LEGAL O CRITERIOS

Los criterios para realizar la auditoría al Sistema de Gestión de Seguridad de la Información son:

- Decreto 1078 de 2015
- Decreto 2573 de 2014
- Norma NTC-ISO- IEC 27001:2013
- Marco de Referencia de Arquitectura TI
- Modelo de Seguridad y Privacidad de la Información.
- Manual Gobierno en Línea
- Acto Administrativo de creación del “Comité de Gobierno en Línea y Racionalización de Trámites”.
- Ley 1712 de 2014
- Decreto 103 de 2015
- Resolución de 3563 de 2015
- Plan de Estratégico Institucional 2014-2018
- Plan de Acción 2017
- Plan Anual de Adquisiciones 2017

V. RESULTADOS DE AUDITORIA

A. NO CONFORMIDADES

Al Sistema de Gestión de Seguridad de la Información:

1. Al hacer la revisión de los roles y responsabilidades del Sistema de Gestión de Seguridad de la Información y basados en las entrevistas realizadas a los funcionarios del proceso y subproceso auditados, no se evidencia el rol de Responsable de Seguridad de la Información u Oficinal de Seguridad de la Información, de acuerdo a lo establecido en el numeral 6.3.1 de la Guía No. 4 de Seguridad y Privacidad de la Información, y al literal A. del numeral 5.3 de la norma.

B. OBSERVACIONES

Al proceso de Gestión de Sistemas de Información:

1. Se verificaron las actividades establecidas en el Plan de Tratamiento de Riesgos de Aplicaciones que se encuentra documentado en la Matriz de riesgos de Aplicaciones. Sin embargo, se evidencia que las actividades de "*Definición e implementación del plan de mitigación de vulnerabilidades*", "*Retest de la prueba de hacking ético*" y "*Definir los aplicativos que se encuentran sub - utilizados*" no se han desarrollado de acuerdo a las fechas programadas en el Plan, por lo que se puede presentar un incumplimiento al requisito 8.3 de la norma NTC-ISO-IEC 27001:2017.
2. Teniendo en cuenta el incidente del 12 de septiembre de 2017, en donde se borró la carpeta del 6simulacronacional, y considerando que el proceso identificó en su matriz de riesgos para el SGSI el riesgo de "*Modificación no autorizada de información o configuración*" el cual se materializó en este incidente, se hace necesario que el proceso levante una acción correctiva puesto que si no se realiza se puede presentar un incumplimiento al numeral 10.1 y u incumplimiento al procedimiento de "*Acciones Correctivas, Preventivas Y De Mejora, PR-1300-SIPG-05*".

Al proceso de Gestión de Infraestructura Tecnológica:

3. Se verificaron las actividades establecidas en el Plan de Tratamiento de Riesgos de Aplicaciones que se encuentra documentado en la Matriz de riesgos de Aplicaciones. Sin embargo, se evidencia que las actividades de capacitación ante el "Robo de documentos o información en impresoras, escáneres y plotters" y la "Subutilización de un aplicativo o componente de Software" no se han desarrollado de acuerdo a las fechas programadas en el Plan, por lo que se puede presentar un incumplimiento al requisito 8.3 de la norma NTC-ISO-IEC 27001:2017.

Al Sistema de Gestión de Seguridad de la Información:

4. Al verificar los actividades desarrolladas por parte del Comité Institucional SIPLAG frente al Sistema de Gestión de Seguridad de la Información, se pudo evidenciar que dentro de las reuniones ordinarias no se han tratado temas relacionados con el mismo, por lo que se podría presentar un posible incumplimiento a lo establecido en el Art. 3 de la resolución 1568 de 2016 respecto a las actividades que este Comité debe adelantar con relación al SGSI y un incumplimiento al artículo 2.2.9.1.2.4 del decreto 1078 de 2015, el cual se refiere a la responsabilidad de implementar la Estrategia de Gobierno en Línea.

5. Se verificó la matriz de indicadores del proceso frente al Manual del Sistema de Gestión de Seguridad de la Información en el proceso de Gestión de Sistemas de Información, se pudo evidenciar que no se tienen implementados los indicadores descritos en este manual, por lo que no se ha realizado alguna medición del cumplimiento de los objetivos del Sistema y la efectividad de los controles establecidos, lo cual puede generar un incumplimiento frente al numeral 9.1 de la Norma NTC-ISO-IEC 27001:2017.

VI. RIESGOS IDENTIFICADOS

Al proceso de Gestión de Sistemas de Información:

1. La falta de personal para el proceso de gestión de Sistemas de Información puede generar retrasos e incumplimientos en el desarrollo de las actividades estratégicas, tácticas y operativas que este deberá desarrollar en el marco de la implementación, mantenimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información; en la implementación de la Estrategia de Gobierno Digital; en la implementación de nuevos módulo del Sistema Nacional de Información para la Gestión del Riesgo de Desastres (Proyecto de Inversión); el apoyo a la implementación del nuevo Modelo Integrado de Planeación y Gestión, y liderar la definición, implementación y mantenimiento de la arquitectura empresarial de la entidad, que son actividades que tienen un valor estratégico importante para la gestión de la UNGRD.

Al Sistema de Gestión de Seguridad de la Información:

2. De acuerdo a los roles y responsabilidades establecidos el numeral 5.3 de la Norma NTC-ISO-IEC 27001: 2013, el Sistema de Gestión de Seguridad de la Información debe contar con un Responsable de Seguridad de la Información y cuyas funciones no están siendo asumidas por ninguno de los profesionales que desarrollan labores en el proceso de Gestión de Sistemas de Información o en el subproceso de Gestión de Sistemas de Información.
3. La reducción en el presupuesto asignado a la Entidad hace que se prioricen los gastos de funcionamiento frente a los gastos de inversión, situación que puede dificultar la financiación proyectos de tecnologías de la información encaminados a la adquisición de equipos de cómputo, software y de servicios especializados.

VII. RECOMENDACIONES

Al Proceso de Gestión de Sistemas de Información:

1. Aunque la matriz de riesgos del Sistema de Gestión de Seguridad de la Información es una fortaleza para el sistema, se recomienda evaluar la viabilidad y pertinencia de añadir al Plan de Tratamiento de Riesgos un espacio en donde se registren los avances en el cumplimiento de las actividades programadas dentro de este Plan.
2. Al hacer la verificación del procedimiento de identificación, clasificación y etiquetado de información se encontró una oportunidad de mejora frente al documento, encaminado a que se documenten los controles que se tienen para las actividades desarrolladas en este procedimiento.

3. Se recomienda actualizar el protocolo de la Página Web, toda vez que se requiere ajustar dicho protocolo con los profesionales que intervienen en las actividades de gestión y soporte del sitio web y la plataforma Sharepoint.

Al Proceso de Gestión de Infraestructura Tecnológica:

4. Hacer una revisión a los procedimientos del subproceso, toda vez que se encontró que algunos no cuentan con controles que permitan validar la correcta ejecución de los mismos, en otros no se cuenta con registros que permitan evidenciar la realización ciertas actividades en el marco de una auditoría externa y por último, para analizar la pertinencia de si es necesario que el Comité Institucional SIPLAG autorice y valide ciertas actividades que se desarrollan dentro de los procedimientos de forma rutinaria, ya que este requerimiento puede ocasionar que ciertas actividades se demoren más de lo esperado.

Al Sistema de Gestión de Seguridad de la Información:

1. Considerar la posibilidad de revisar la matriz de partes interesadas, toda vez que la última actualización fue realizada en 2014 y no se observa en estas entidades como Ministerio de Tecnologías de la Información y la Comunicaciones parte interesada en la implementación de la Estrategia de Gobierno en Línea y en los avances del Modelo Integrado de Planeación y Gestión.
2. Definir la pertinencia de implementar gradualmente los indicadores del Manual del Sistema de Gestión de Seguridad de la Información en los procesos en donde se generan los datos y que servirán de insumo para realizar los reportes, el análisis de los indicadores y para la revisión por la Dirección.
3. Elevar al Comité Institucional del SIPLAG para que en esta instancia se tome la decisión de que proceso será el responsable de liderar el proceso de implementación del Sistema de Gestión de Seguridad de la Información en el resto de los procesos de la Unidad, adelantar las inspecciones, el monitoreo y mantenimiento del sistema teniendo en cuenta la definición de roles y responsabilidades es un requisito de la norma NTC-ISO-IEC 27001:2013.
4. Teniendo en cuenta que el Sistema Integrado de Planeación y Gestión cuenta con un manual de Gestión Ambiental y Salud en el Trabajo - SST para contratista, en donde establece requisitos y responsabilidades frente a estos dos sistemas de gestión, el cumplimiento de sus políticas y el compromiso frente al cumplimiento de los objetivos, se recomienda incluir dentro de este documento los deberes que tienen los contratistas y proveedores de la Unidad frente al Sistema de Gestión de Seguridad de la Información.
5. Se recomienda definir un mecanismo, ya sea a través de un informe de seguimiento al Plan de Tratamiento o dentro de la matriz de riesgos, en donde se destine una columna de seguimiento y monitoreo por parte del dueño del proceso, o por parte del oficial de seguridad de la información o por parte de la Oficina de Control Interno, con el objetivo de hacer seguimiento a este Plan y que queden registros de los mismos, pensando en que esto debe hacer parte de los insumos para la revisión por la dirección.
6. Considerando el nivel de madurez del Sistema de Gestión de Seguridad de la Información de la UNGRD y teniendo en cuenta que la presente auditoria tuvo un enfoque documental, para el próximo ciclo de auditoría se recomienda que incluir actividades que permitan verificar a través de pruebas técnicas la efectividad de los controles establecidos y la revisión de las vulnerabilidades identificadas dentro de los mapas de riesgos del sistema, tanto en el proceso de Gestión de Sistemas de Información y el subproceso de Gestión de Infraestructura Tecnológica.

VIII. CONCLUSIONES

El Sistema de Gestión de Seguridad de la Información de la UNGRD se encuentra documentado de acuerdo a los requisitos establecidos en la Norma NTC-ISO-IEC 27001:2013 y que son aplicables al proceso de Gestión de Sistemas de Información y al subproceso de Gestión de Infraestructura Tecnológica. Sin embargo, el SGSI se encuentra aún en proceso de implementación de algunos componentes acuerdo a los soportes que fueron allegados por parte del subproceso, a la verificación realizada durante la presenta auditoría y teniendo en cuenta el alcance del sistema.

También 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.

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.

IX. Anexos

1. Resultados de auditoria proceso Gestión de Sistemas de Información
2. Resultados de auditoria subproceso Gestión de Infraestructura Tecnológica

ORIGINAL FIRMADO

JEFE OFICINA DE CONTROL INTERNO UNGRD

Fecha elaboración: 29/12/17
Elaboró: Jairo R. Tapias.
Revisó: Germán Moreno.
Aprobó: Germán Moreno.