SUPERINTENDENCIA DE LA ECONOMIA SOLIDARIA

RIESGOS TECNOLOGICOS

OFICINA DE CONTROL INTERNO

Bogotá, D.C, mayo de 2020

TÍTULO DE LA AUDITORÍA: Evaluar los riesgos Tecnológicos y sus controles	**RESPONSABLE:** Oficina Asesora de Planeación y Sistemas
LUGAR Y FECHA DE REALIZACIÓN DE LA AUDITORÍA: Bogotá, 13 al 24 de abril de 2020	**PERIODO A AUDITAR:** 01 de enero al 31 de diciembre de 2019 y lo corrido de 2020
EQUIPO AUDITOR: Alexandra Triviño Martínez - Contratista	

INTRODUCCIÓN

De conformidad con lo establecido en el artículo 9º de la Ley 87 de 1993 le corresponde a la Oficina de Control Interno asesorar a la Dirección en la continuidad del proceso administrativo, la reevaluación de los planes establecidos y en la introducción de los correctivos necesarios para el cumplimiento de las metas u objetivos previstos; en desarrollo de tales funciones, el artículo 17 del Decreto 648 de 2017 identifica la evaluación y seguimiento como uno de los principales tópicos que enmarcan el rol de las Oficinas de Control Interno.

De igual forma, teniendo en cuenta que el artículo 6º del Decreto 648 de 2017, establece que le corresponde a la Oficina de Control Interno en cada entidad *"Medir y evaluar la eficiencia, eficacia y economía de los demás controles adoptados por la entidad, así como asesorar y apoyar a los directivos en el desarrollo y mejoramiento del Sistema Institucional de Control Interno a través del cumplimiento de los roles establecidos"*, mediante la formulación de recomendaciones y observaciones para lograr el cumplimiento de las funciones y objetivos misionales, y dando cumplimiento a lo dispuesto en el Programa Anual de Auditorias para la vigencia 2020 en su componente Informes especiales, en su actividad No. 23 – Riesgos Tecnológicos, la Oficina de Control Interno, se permite presentar el Informe de Auditoría.

I. OBJETIVO GENERAL

Evaluar los riesgos de Tecnología de la Información y la Comunicación y sus controles identificados en la Matriz de riesgos institucional.

II. NORMATIVIDAD

Constitución Política de Colombia de 1991, Artículo 209: La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones.

Constitución Política de Colombia de 1991, Artículo 269: En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas.

Ley 87 de 1993, por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado.

Decreto 1078 de mayo 26 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1083 de mayo 26 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública. Título 22, Parte 2 Del Libro 2 “Sistema de gestión”.

Decreto 1499 de septiembre 11 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión (Título 22, Parte 2 del Libro 2).

Guía para la administración del riesgo y el diseño de controles en entidades públicas V- 4 de la función pública.

Marcos de referencia de normas internacionales como ITIL, COBIT, ISO2700

III. ALCANCE

Evaluar los riesgos tecnológicos y sus controles identificados en la Matriz de riesgos institucional sobre el proceso de gestión de infraestructura.

IV. DECLARACIÓN

Esta auditoría fue realizada con base en el análisis de diferentes muestras aleatorias seleccionadas y se fundamenta en el siguiente soporte documental: procesos y procedimientos del Sistema de Gestión de la entidad, página web, intranet, normas internas y externas.

Una consecuencia de esto es la presencia del riesgo de muestreo, es decir, el riesgo de que la conclusión basada en la muestra analizada no coincida con la conclusión a que se habría llegado en caso de haber examinado todos los elementos que componen la población.

En aplicación del artículo 2.2.21.4.8 del Decreto 648 de 2017, la Oficina de Control Interno incorpora los siguientes instrumentos para la actividad de auditoría interna:

a) Código de Ética del Auditor Interno que tendrá como bases fundamentales, la integridad, objetividad, confidencialidad, conflictos de interés y competencia de éste.

b) Estatuto de auditoría, en el cual se establezcan y comuniquen las directrices fundamentales que definirán el marco dentro del cual se desarrollarán las actividades de la Unidad u Oficina de Control Interno, según los lineamientos de las normas internacionales de auditoría.

Compromiso del auditado

Carta de representación en la que se establezca la veracidad, calidad y oportunidad de la entrega de la información presentada a la Oficina de Control Interno.

V. METODOLOGÍA

Para el desarrollo de la verificación y el seguimiento se estableció un esquema metodológico, con los siguientes pasos:

a) Entendimiento del proceso: Se identificó la normatividad externa, se verifico en el Sistema de Sistema de Gestión de Calidad “Isolucion”, la documentación, relacionados con los riesgos institucionales y los riesgos asociados al proceso de Gestión de infraestructura.

b) Diseño del plan de auditoria: Se estableció el plan de trabajo para el desarrollo de la auditoria para lograr el cumplimiento de los objetivos propuestos.

c) Obtención y análisis de la información: Se realizó la solicitud de la información relacionada con los riesgos tecnológicos a la Oficina Asesora de Planeación y Sistemas, revisión y evaluación de la información remitida.

d) Ejecución de pruebas: Desarrollo de pruebas de verificación diseñadas.

e) Definición de observaciones y recomendaciones: Producto de la evaluación realizada.

f) Seguimiento a las observaciones presentadas en el informe de la vigencia anterior 2019, lo anterior, teniendo en cuenta que no se suscribió y presento un plan de mejoramiento por parte de la Oficina Asesora de Planeación y Sistemas, responsable de la ejecución de las acciones.

VI. DESARROLLO DEL EJERCICIO DE AUDITORIA.

1. Riesgos Tecnológicos

El Riesgo Tecnológico es la pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia en el hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de distribución de Información.

También se puede decir que es la contingencia de que la interrupción, alteración, o falla de la infraestructura de TIC´s (tecnológica de la información y de las

comunicaciones), sistemas de información, bases de datos y procesos de TI, provoque pérdidas financieras en una entidad.

2. Información Analizada

La Oficina de Control Interno analizó la información entregada por la Oficina Asesora de Planeación y Sistemas relacionada con:

- Plan de Arquitectura Empresarial 2019.
- Planes de Seguridad y Privacidad de la Información
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
- Metodología gestión de riesgos – SGSI

La información publicada en la página web de la entidad correspondiente a:

- Matriz institucional de riesgos

3. Resultados de la Evaluación

A continuación, se presentan los resultados del seguimiento efectuado por la Oficina de Control Interno a los riesgos tecnológicos.

3.1 Metodología de evaluación de los riesgos

La entidad ha establecido acciones a través de la Oficina Asesora de Planeación y Sistemas para actualizar la metodología de evaluación de los riesgos institucionales alineada a las directrices del Departamento Administrativo de la Función Pública – DAFP, teniendo en cuenta la Guía de Administración de Riesgos del DAFP que incluye la temática de riesgos de seguridad digital y los mecanismos para la adecuada identificación y calificación de los riesgos, documento que se encuentra como propuesta para ser aprobado .

La metodología propone unificar la descripción y elaboración para todos los tipos de riesgos que se manejan en la entidad como:

Riesgos de Seguridad de la Información : Disponibilidad; Integridad y Confidencialidad

Tipo de Riesgo	Descripción
Riesgos Operativos	Derivados del funcionamiento de los sistemas de gestión institucional, la definición y ejecución de los procesos, la operación de los sistemas de información y herramientas de apoyo a la gestión, de la estructura de la entidad y de los mecanismos de comunicación y articulación entre dependencias.
Riesgos de Tecnología	Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
Riesgo Ambiental	Son los riesgos que están relacionados con la responsabilidad y compromiso de la entidad hacia el cuidado del ambiente
Riesgo de Seguridad y Salud en el Trabajo	Son los riesgos que están relacionados con el compromiso de la entidad de preservar la salud y seguridad de los funcionarios y servidores
Riesgo de Seguridad de la Información	Son los riesgos asociados con la afectación a la confidencialidad, la integridad y la disponibilidad de información.

Fuente Metodología de evaluación de riesgos

La auditoría **recomienda** a la Oficina Asesora de Planeación y Sistemas adelantar las gestiones que consideren necesarias para para revisar, ajustar y aprobar (institucionalmente) la metodología para la evaluación de los riesgos en la entidad.

3.2 Plan de tratamiento de riesgos de seguridad y privacidad de la información

La entidad a través de la Oficina Asesora de Planeación y Sistemas Diseño y elaboro el Plan de Tratamiento de riesgos de seguridad y privacidad de la información, con el fin de contar con una herramienta que proporcione los lineamientos requeridos para desarrollar y fortalecer una adecuada gestión de los riesgos de seguridad de la información, documento que se encuentra en revisión.

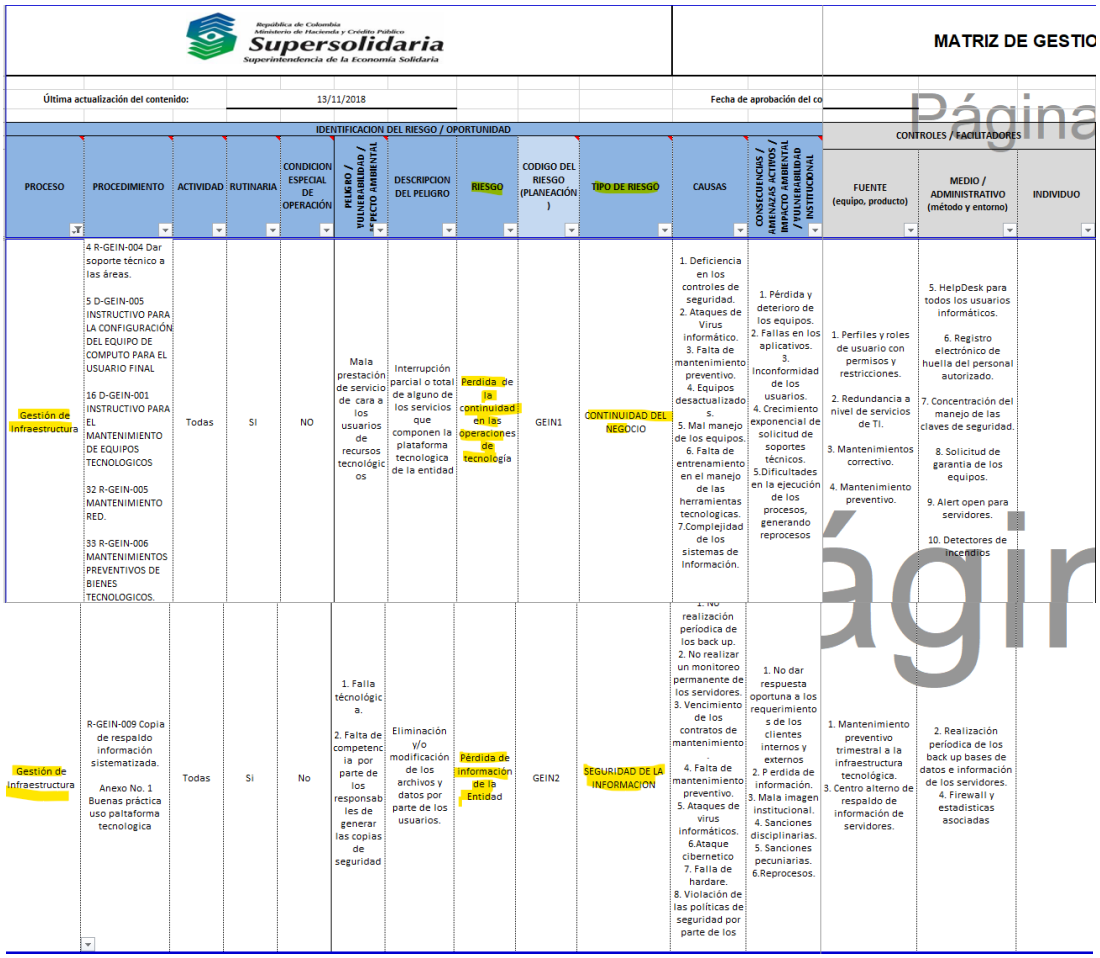
La auditoría **recomienda** a la Oficina Asesora de Planeación y Sistemas adelantar las gestiones que consideren necesarias para para ajustar y aprobar (institucionalmente) el plan de tratamiento de riesgos de seguridad y privacidad de la información.

3.3 Riesgos Proceso de Infraestructura

Observación No.1 Falta de riesgos de TIC´s

Descripción o situación encontrada:

Como resultado de la revisión efectuada a al mapa de riesgos institucional de la entidad para el proceso de Gestión de Infraestructura, se identificaron dos (2) riesgos asociados, como se observa en la siguiente figura:



MATRIZ DE GESTIO

Última actualización del contenido: 13/11/2018

Fecha de aprobación del co

Página

IDENTIFICACION DEL RIESGO / OPORTUNIDAD

CONTROLES / FACILITADORES

PROCESO	PROCEDIMIENTO	ACTIVIDAD	RUTINARIA	CONDICION ESPECIAL DE OPERACIÓN	PELIGRO / VULNERABILIDAD / ASPECTO AMBIENTAL	DESCRIPCION DEL PELIGRO	RIESGO	CODIGO DEL RIESGO (PLANEACIÓN)	TIPO DE RIESGO	CAUSAS	CONSECUENCIAS / AMENAZAS ACTIVOS / IMPACTO AMBIENTAL / VULNERABILIDAD INSTITUCIONAL	FUENTE (equipo, producto)	MEDIO / ADMINISTRATIVO (método y entorno)	INDIVIDUO
Gestión de Infraestructura	4 R-GEIN-004 Dar soporte técnico a las áreas. 5 D-GEIN-005 INSTRUCTIVO PARA LA CONFIGURACIÓN DEL EQUIPO DE COMPUTO PARA EL USUARIO FINAL 16 D-GEIN-001 INSTRUCTIVO PARA EL MANTENIMIENTO DE EQUIPOS TECNOLOGICOS 32 R-GEIN-005 MANTENIMIENTO RED. 33 R-GEIN-006 MANTENIMIENTOS PREVENTIVOS DE BIENES TECNOLOGICOS.	Todas	SI	NO	Mala prestación de servicio de cara a los usuarios de recursos tecnológicos	Interrupción parcial o total de alguno de los servicios que componen la plataforma tecnologica de la entidad	Perdida de la continuidad en las operaciones de tecnología	GEIN1	CONTINUIDAD DEL NEGOCIO	1. Deficiencia en los controles de seguridad. 2. Ataques de Virus informático. 3. Falta de mantenimiento preventivo. 4. Equipos desactualizados. 5. Mal manejo de los equipos. 6. Falta de entrenamiento en el manejo de las herramientas tecnologicas. 7.Complejidad de los sistemas de información.	1. Pérdida y deterioro de los equipos. 2. Fallas en los aplicativos. 3. Inconformidad de los usuarios. 4. Crecimiento exponencial de solicitud de soportes técnicos. 5.Dificultades en la ejecución de los procesos, generando reprocesos	1. Perfiles y roles de usuario con permisos y restricciones. 2. Redundancia a nivel de servicios de TI. 3. Mantenimientos correctivo. 4. Mantenimiento preventivo.	5. HelpDesk para todos los usuarios informáticos. 6. Registro electrónico de huella del personal autorizado. 7. Concentración del manejo de las claves de seguridad. 8. Solicitud de garantia de los equipos. 9. Alert open para servidores. 10. Detectores de incendios	
Gestión de Infraestructura	R-GEIN-009 Copia de respaldo información sistematizada. Anexo No. 1 Buenas práctica uso paltaforma tecnologica	Todas	SI	No	1. Falla técnológica. 2. Falta de competencia por parte de los responsables de generar las copias de seguridad	Eliminación y/o modificación de los archivos y datos por parte de los usuarios.	Pérdida de información de la Entidad	GEIN2	SEGURIDAD DE LA INFORMACION	1. No realización periodica de los back up. 2. No realizar un monitoreo permanente de los servidores. 3. Vencimiento de los contratos de mantenimiento. 4. Falta de mantenimiento preventivo. 5. Ataques de virus informáticos. 6.Ataque cibernetico 7. Falla de hardare. 8. Violación de las políticas de seguridad por parte de los	1. No dar respuesta oportuna a los requerimientos de los clientes internos y externos 2. P erdida de información. 3. Mala imagen institucional. 4. Sanciones disciplinarias. 5. Sanciones pecuniarias. 6.Reprocesos.	1. Mantenimiento preventivo trimestral a la infraestructura tecnológica. 3. Centro alterno de respaldo de información de servidores.	2. Realización periodica de los back up bases de datos e información de los servidores. 4. Firewall y estadisticas asociadas	

Mapa de riesgos institucional

Se realizó una revisión al mapa de riesgos y controles, observando lo siguiente:

- La última actualización al mapa de riesgos fue realizada el 13 de noviembre de 2018.
- En el mapa se incluyen únicamente dos riesgos relacionados con Perdida de la continuidad en las operaciones de tecnología y Pérdida de información de la Entidad.

  Dicho mapa NO considera aspectos tan importantes como:

- ✓ Fallas en el equipo de telecomunicaciones
- ✓ Fallas en los servicios de Internet y/o correo electrónico
- ✓ Fallas en los recursos de red existentes, etc.
- ✓ Incumplimiento en los servicios esperados
- ✓ Estrategia de los servicios de TI
- ✓ Gestión de proyectos de TI
- ✓ Ejecución y administración de procesos

Posibles causas identificadas por la Oficina de Control Interno:

Riesgos tecnológicos no identificados que pueden afectar la continuidad de la operación de la entidad.

Descripción del riesgo:

Pérdidas económicas y reputación

Recomendaciones

Definir los riesgos tecnológicos de acuerdo a los siguientes ámbitos de operación: proyectos, infraestructura de TIC´s, sistemas de información, servicios de TI, gestión de seguridad informática para los cuales, se debe desarrollar un ciclo de evaluación de cada uno de ellos, teniendo como resultado, un análisis de impacto, una priorización y a partir de esto definir los objetivos generales y específicos para establecer controles de mitigación.

Tener en cuenta los marcos de referencia de normas internacionales como ITIL, COBIT, ISO 27001, entre otras y las mejores prácticas fundamentan las políticas y procedimientos para la administración de riesgos de TIC y Gestión y administración de mitigación de los riesgos en los proyectos de TIC´s.

OBSERVACIÓN OFICINA ASESORA DE PLANEACIÓN Y SISTEMAS

Teniendo en cuenta que el objetivo general de la auditoría era: "*Evaluar los riesgos de Tecnología de la Información y la Comunicación y sus controles identificados en la Matriz de riesgos institucional"*, es importante mencionar que los riesgos registrados en la matriz de riesgos institucional, corresponden al proceso de Gestión de Infraestructura, mas no propiamente a los riesgos de tecnología de la información y la comunicación; por lo tanto, estos riesgos se identificaron dentro de la caracterización existente del proceso bajo la metodología actual, donde la misma no da directrices para la identificación de riesgos de tecnología de la información y la comunicación. Razón por la cual, la Oficina Asesora de Planeación y Sistemas adelanta la adopción de lineamientos dados por el DAFP a través del anexo 4 de la guía para la administración del riesgo y diseño de controles en entidades públicas versión 4, donde se dieron instrucciones para gestionar los riesgos de gestión, corrupción y seguridad digital; una vez adoptados y aprobados estos lineamientos, se procederá a realizar la gestión de riesgos de tecnología de la información y la comunicación.

Para la revisión se debe tener en cuenta lo documentado en el proceso de gestión de infraestructura y los riesgos propiamente del proceso.

Por lo anterior, no se acepta la observación.

RESPUESTA OFICINA DE CONTROL INTERNO:

De acuerdo con la respuesta y argumentos presentados por la Oficina Asesora de Planeación y Sistemas, la Oficina de Control Interno, aclara que si bien la OAPS se encuentra en un proceso de actualización del sistema de administración de riesgos alineado a las directrices del DAFP el Proceso de Gestión de Infraestructura, por lo anterior y con el fin de fortalecer el sistema de administración de riesgos, es importante que durante la actualización del mapa de riesgos institucional, se tengan en cuenta las observaciones y recomendaciones presentadas en este informe en cuanto a la identificación de riesgos que afecten la gestión, la seguridad de la información y prestación de servicios de las TIC´s, por lo anterior, se ratifica la observación modifica la redacción de la misma frente a los términos inicialmente señalados en el informe de seguimiento, la cual quedará así: "***Faltan riesgos por definir asociados a las TIC´s en la Matriz de riesgos institucional*".**

3.4 Seguimiento a las observaciones presentadas en el informe anterior

Observación No. 2 Falta de una Política de Administración de riesgos

Descripción o situación encontrada:

No existen las Políticas de Administración de Riesgos que identifique las opciones para tratar y manejar los riesgos basadas en la valoración de los mismos, para tomar decisiones adecuadas y fijar los lineamientos, que van a transmitir la posición de la dirección y establecen las guías de acción necesarias a todos los servidores de la entidad.

Posibles causas identificadas por la Oficina de Control Interno:

Falta de control y seguimiento a los riesgos potenciales, que puedan afectar los objetivos y resultados institucionales.

Descripción del riesgo:

Incumplimiento en el logro de los objetivos institucionales

Recomendaciones

1. La auditoría reitera la importancia de adoptar la política de administración de riesgos en la Superintendencia que defina claramente el procedimiento a seguir en caso de materialización de un riesgo, dentro del cual se incluya como mínimo políticas para:

   - Riesgos de Tecnología de Información
   - Sistema integrado de Gestión de riesgos en la seguridad de la información

   Atendiendo los lineamientos establecidos en la Guía para la administración del riesgo del Departamento Administrativo de la Función Pública.

OBSERVACIÓN OFICINA ASESORA DE PLANEACIÓN Y SISTEMAS

Es importante tener en cuenta que la entidad cuenta con la Política de Gestión Integral de Riesgos y Oportunidades aprobada mediante resolución 2017100007035 del 29 de diciembre de 2017; sin embargo, la Oficina Asesora de Planeación y Sistemas, dentro de su plan de trabajo tiene contemplada la actualización y ajustes a la misma de acuerdo con los lineamientos dados por el DAFP a través de la guía para la administración del riesgo y diseño de controles en entidades públicas, documento que se tiene programado culminar en el mes de mayo de 2020 con el fin de ser presentado para revisión y aprobación ante el Comité Institucional de Coordinación de Control Interno.

RESPUESTA OFICINA DE CONTROL INTERNO:

Una vez revisados los argumentos presentados por la Oficina Asesora de Planeación y Sistemas, se evidencia que esta dependencia, se encuentra en el proceso de actualización de la Política de Administración de riesgos, la Oficina de Control Interno, ***ratifica la observación***, por cuanto al cierre de la auditoria evidencio que la entidad no tiene a la fecha una política formalizada de administración de riesgos con los lineamientos establecidos en la Guía de Administración de Riesgo del Departamento Administrativo de la Función pública, emitida en octubre de 2018, en donde incluyo la temática de riesgos de seguridad digital. Así mismo procederá a modificar la redacción de la observación, en el sentido de dar un mayor entendimiento a la misma, por lo cual quedará así: "***Falta de una Política de Administración de riesgos actualizada, atendiendo los lineamientos establecidos en la Guía para la administración del riesgo del DAFP, emitida en octubre de 2018***".

VII. OPORTUNIDADES DE MEJORA

La Oficina de Control Interno en cumplimiento de sus funciones de revisión y verificación, realizó la respectiva revisión de la información recibida, evidenciando que la Superintendencia de la Economía Solidaria tiene establecidos procedimientos y actividades formales y no formales para la administración del mapa de riesgos de tecnología.

Sin embargo, nos permitimos dejar a consideración de la entidad las siguientes oportunidades de mejora que le permitan fortalecer la definición de los riesgos de TIC´s en la entidad.

1. Avanzar y formalizar institucionalmente la metodología de evaluación de los riesgos y plan de tratamiento de riesgos de seguridad y privacidad de la información.

2. Actualizar el mapa de riesgos de tecnológicos teniendo en cuenta las recomendaciones presentadas.

3. Definir la política de riesgos.

VIII. CONCLUSIONES

Una vez realizada la evaluación a la matriz de riegos institucional relaciona con el proceso de infraestructura, la Oficina de Control Interno encuentra no se tiene una matriz de riesgos tecnológicos actualizada.

No se tiene definida una política de administración del riesgo.

Finalmente, y de considerarlo pertinente, se solicita dar respuesta por este mismo medio y sobre este mismo expediente, sobre las observaciones incluidas en el presente informe de auditoría, respecto de situaciones o soportes que de manera objetiva puedan modificar algunas de las evidencias presentadas; dicha replica deberá ser presentada a más tardar, dentro de los dos (2) días hábiles siguientes a partir de la fecha de remisión.

Una vez concluido este término, el presente informe será remitido al Superintendente de la Economía Solidaria, de conformidad con lo establecido en el parágrafo primero del artículo 2.2.21.4 del Decreto 1083 de 2015, junto con el formato “F-COIN-016 Seguimiento Cumplimiento Planes de mejoramiento”, para que se realice la suscripción del Plan de Mejoramiento correspondiente por parte del líder del proceso dentro de los cinco (5) días hábiles siguientes a partir de la fecha de remisión.

IX. RESUMEN DE OBSERVACIONES

No	OBSERVACIONES	REPETITIVO
1	Faltan riesgos por definir asociados a las TIC´s en la Matriz de riesgos institucional	NO
2	Falta de una Política de Administración de riesgos actualizada, atendiendo los lineamientos establecidos en la Guía para la administración del riesgo del DAFP, emitida en octubre de 2018	NO

Cordialmente,

(Original firmado)
MABEL ASTRID NEIRA YEPES
Jefe Oficina de Control Interno

Elaboró: Alexandra Triviño Martínez