SUPERINTENDENCIA DE LA ECONOMIA SOLIDARIA

INFORME PRELIMINAR RIESGOS TECNOLOGICOS

OFICINA DE CONTROL INTERNO

Abril de 2019

Carrera 7 No. 31-10 Piso 11. PBX (1) 7 560 557. Línea Gratuita 018000 180 430
www.supersolidaria.gov.co
NIT: 830.053.043 5 Bogotá D.C., Colombia

Tabla de contenido

1. GENERALIDADES DEL INFORME

1.1 INTRODUCCION.

De conformidad con lo establecido en el artículo 9° 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, y 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, dando cumplimiento a lo dispuesto en el Programa Anual de Auditoria para la vigencia del año 2019, en su componente de auditorías especiales, en su actividad No. 18 – Riesgos Tecnológicos, la Oficina de Control Interno presenta el informe Preliminar de Riesgos Tecnológicos.

1.2 OBJETIVO

Revisar la matriz de riesgos de Tecnología de la información y las comunicaciones TIC y sus planes de respuesta.

1.3 OBJETIVOS ESPECIFICOS

- Revisar cómo se Implementaron los controles a partir del riesgo.
- Evaluar el funcionamiento y la constitución de los planes de respuesta a cada riesgo documentados e implementados
- Revisar el planteamiento del riesgo, su calificación cuantitativa y cualitativa.
- Evaluar los riesgos seleccionados en la matriz

1.4 ALCANCE

Matriz de riesgos entregada por la oficina de planeación y sistemas, únicamente los riesgos tecnológicos

1.5 METODOLOGIA

1.5.1 Se solicitó a Planeación y Sistemas la matriz de riesgo TIC vigente con sus planes de respuesta

1.5.2 Como elementos de análisis de referencia se tomaron los siguientes:

- Guía para la administración del riesgo del Departamento Administrativo de la Función Pública, Bogotá, D.C., Colombia, octubre de 2018, ubicado en http://www.funcionpublica.gov.co/guias

- Informe de avances y proyección de la Oficina Asesora de Planeación y Sistemas 2015, el más reciente, ubicado en http://intranet.supersolidaria.gov.co/sites/default/files/publicacion%20con%20archivos/Informe%20de%20gestion%20OAPS%20%202015.pdf, revisado en lo referente al tema de riesgos TIC

- Gestión del riesgo principios y directrices NTC-ISO 31000 : 2009, ubicada en: https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf

- NORMA TECNICA COLOMBIANA NTC-ISO 52541 (Primera Actualización 2006-09-12) Gestión De Riesgo

- Norma Técnica Colombiana NTC-ISO 27001 Tecnología De La Información. Técnicas De Seguridad. Sistemas De Gestión De La Seguridad De La Información (Sgsi). Requisitos

1.5.3 Revisión de la matriz entregada, se revisa la matriz con el enfoque operacional en cuanto a los riesgos operacionales de la información de acuerdo con el enfoque de la ISO270001 de confidencialidad, disponibilidad e integridad características que determinan los riesgos de TIC.

1.5.4 Se consultó en Isolucion y en la intranet de la Superintendencia los documentos relacionados con el riesgo TIC, para tener un contexto general del manejo del riesgo en la Superintendencia.

2. RESULTADOS DEL INFORME

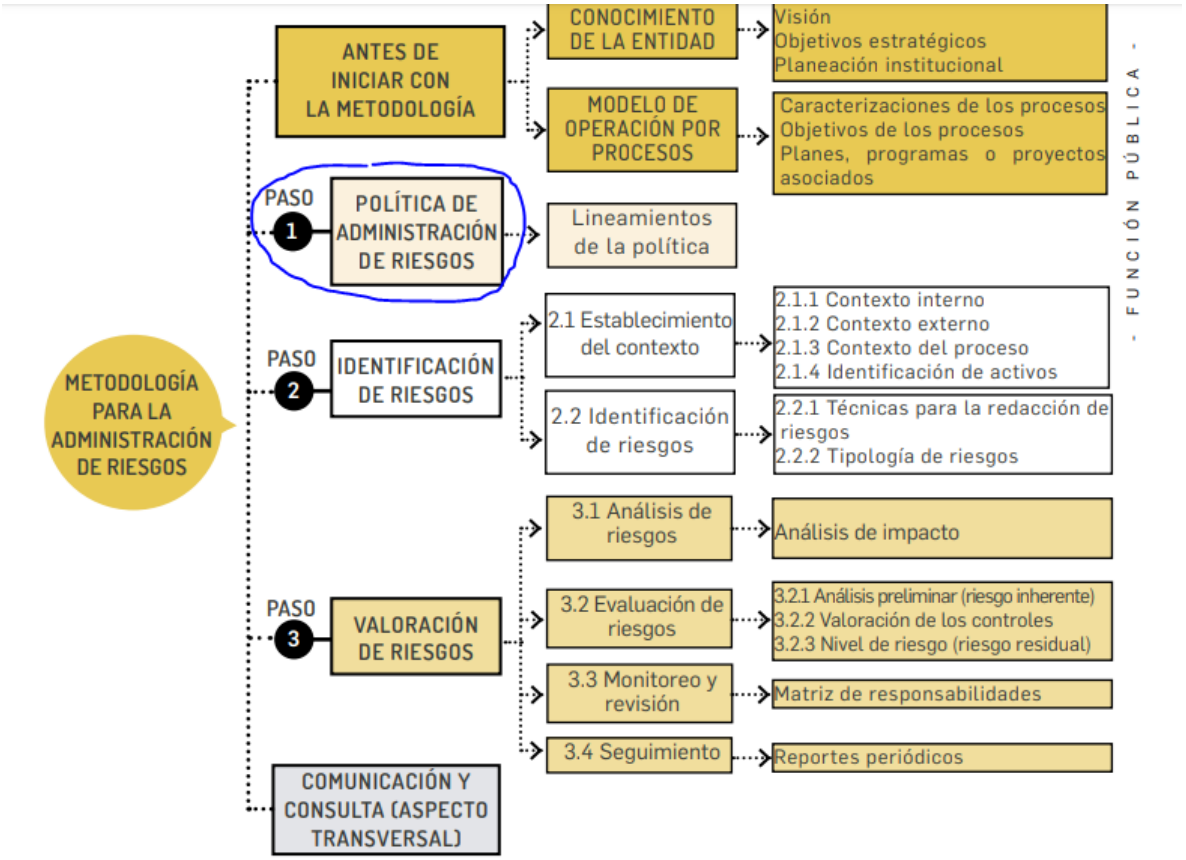
De la revisión y análisis de los archivos y aplicando la metodología indicada se encontraron los siguientes resultados:

2.1 La matriz de riesgo entregada es la general de la Superintendencia y de TIC solo contiene un riesgo que está asociado al proceso de Gestión de Infraestructura, el cual está denominado como "*Eliminación y/o modificación de los archivos y datos por parte de los usuarios.",* en el análisis realizado de este riesgo encontramos:

OBSERVACION	EXPLICACION
En la columna PELIGRO / VULNERABILIDAD / ASPECTO AMBIENTAL, cita dos aspecto no relacionados con el riesgo: 1. Falla tecnológica. 2. Falta de competencia por parte de los responsables de generar las copias de seguridad	El Nombre del riesgo no está asociado con la vulnerabilidad: "*Eliminación y/o modificación de los archivos y datos por parte de los usuarios.",* el riesgo indica que es por parte de los usuarios y la vulnerabilidad está planteada por falla tecnológica o falta de competencia por el operador.
En la columna TIPO DE RIESGO indica: "SEGURIDAD DE LA INFORMACION	El riesgo de acuerdo con la homologación del ISO27001 está relacionado con Confidencialidad, Integridad y disponibilidad.
En la columna "CAUSAS PROBABLES" del riesgo relacionan 8 así: 1. No realización periódica 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 cibernético 7. Falla de hardware. 8. Violación de las políticas de seguridad por parte de los usuarios.	El Nombre del riesgo: "*Eliminación y/o modificación de los archivos y datos por parte de los usuarios.",* es pertinente solo con las causas 2, 6 y 8.
En la columna "CONTROLES" subcolumna "FUENTE" indican las siguientes: 1. Mantenimiento preventivo trimestral a la infraestructura tecnológica. 2. Centro alterno de respaldo de información de servidores.	El Nombre del riesgo: "*Eliminación y/o modificación de los archivos y datos por parte de los usuarios.",* la fuente de los controles indicados no guardan correlación del control con el riesgo.
En la columna "CONTROLES" subcolumna "MEDIO / ADMINISTRATIVO" indican las siguientes: 1. Realización periódica de los back up	El Nombre del riesgo: "*Eliminación y/o modificación de los archivos y datos por parte de los usuarios.",* el control medio administrativo planteado es preventivo pero no eficaz, solo el nro. 2 está directamente relacionado con el

bases de datos e información de los servidores. 2. Firewall y estadísticas asociadas	control de contención del riesgo. .

2.2. No existe la POLÍTICA DE ADMINISTRACIÓN DE RIESGOS de la SuperIntendencia de Economía Solidaria, de acuerdo como lo solicita la Guía para la administración del riesgo del Departamento Administrativo de la Función Pública, Bogotá, D.C., Colombia, octubre de 2018, en la página 13, esquema 2.



2.3. La matriz de riesgo entregada solo contiene un riesgo, y los riesgos que debe contener son todos los relacionados con el manejo de la información en los aspectos de:

- Confidencialidad de la información
- Integridad de la información
- Disponibilidad de la información

2.4. En la resolución 2015121001175 del 2015 se aprueba el Plan Estratégico Institucional 2014 – 2018, en el cual de acuerdo con el documento Informe de avances y proyección de la Oficina Asesora de Planeación y Sistemas 2015, el más reciente, ubicado en http://intranet.supersolidaria.gov.co/sites/default/files/publicacion%20con%20archivos/Informe%20de%20gestion%20OAPS%20%202015.pdf , en la página 20, numeral o título 6. La OAPS frente al Plan Estratégico 2014 a 2018 y Plan Operativo Anual 2015, indican en la página 39 Anexo 3: Objetivo estratégico OAPS en Plan estratégico institucional 2014-2018 dentro del

objetivo estratégico: "*Implementar buenas prácticas de gestión, dirigidas al mejoramiento de la prestación de servicios a las organizaciones del sector de la economía solidaria bajo la supervisión de la Entidad, mediante el uso de TIC*", "*Consolidar el sistema de gestión integral de riesgos en la Entidad*", aspecto que a la fecha de acuerdo con la matriz recibida no se ha ejecutado.

3. OBSERVACIONES Y RECOMENDACIONES

3.1 Elaborar una matriz de riesgos completa, siguiendo la Guía para la administración del riesgo del Departamento Administrativo de la Función Pública, Bogotá, D.C., Colombia, octubre de 2018 y contemplando los riesgos operativos relacionados con los tres elementos básicos que indica la ISO27001:

- Confidencialidad de la información
- Integridad de la información
- Disponibilidad de la información

3.2 Definir la política de administración de riesgos para la Superintendencia, de acuerdo como lo indica la Guía para la administración del riesgo del Departamento Administrativo de la Función Pública, Bogotá, D.C., Colombia, octubre de 2018, en la página 13, esquema 2.

Las observaciones comunicadas se deberán incluir en el plan de mejoramiento a suscribir, contemplando acciones preventivas y/o correctivas para el caso mencionado de forma tal que se subsane la observaciones informadas, para la presentación del Plan de Mejoramiento se deberá utilizar el formato F-COIN-016 Seguimiento Cumplimiento Planes de mejoramiento (el cual se anexa al presente informe)

Cordialmente,

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

Elaboró: Rafael Luis Gabriel Vergara