Supersolidaria
Superintendencia de la Economía Solidaria

El emprendimiento es de todos
Minhacienda

SUPERINTENDENCIA DE LA ECONOMIA SOLIDARIA

INFORME DE AUDITORÍA A LAS POLÍTICAS DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

OFICINA DE CONTROL INTERNO

Bogotá, D.C, mayo de 2020

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

TÍTULO DE LA AUDITORÍA: Auditoria a las Políticas de seguridad de la información.	**RESPONSABLE:** Oficina Asesora de Planeación y Sistemas
LUGAR Y FECHA DE REALIZACIÓN DE LA AUDITORÍA: Bogotá, 04 al 15 de mayo 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 auditorias Informes especiales, en su actividad No. 21 – Políticas de seguridad de la información (Criterios de Evaluación COBIT, ITIL, ISO), la Oficina de Control Interno, se permite presentar el Informe de Auditoría.

I. OBJETIVO GENERAL

Evaluar las Políticas de Políticas de seguridad de la información.

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.

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones

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 415 de 2016: Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.

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, establecido en el artículo 133 de la Ley 1753 de 2015.

MinTIC. Modelo de seguridad y privacidad de la información, lineamientos y guías establecidos para la implementación del SGSI.

Norma técnica colombiana NTC ISO/IEC 27001:2013, marcos de referencia de normas internacionales como COBIT, ISO2700.

III. ALCANCE

Verificar las Políticas de Políticas de seguridad de la información durante la vigencia 2019 y lo corrido del año 2020.

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*" y en la página web de la entidad, la documentación, relacionados con las Políticas de seguridad de la información.

b) Diseño del plan de auditoria: Se estableció la programación del plan de trabajo para el desarrollo de la auditoria para lograr el cumplimiento del objetivo propuesto.

c) Obtención y análisis de la información: Se realizó la solicitud de la información relacionada con las Políticas de Seguridad de la Información a la Oficina Asesora de Planeación y Sistemas, revisión y evaluación de la información remitida.

d) Ejecución de pruebas: Se realizó la verificación sobre la información. Desarrollo de pruebas de verificación diseñadas.

e) Definición de observaciones y recomendaciones: Producto de la evaluación realizada a la información entregada, socializándolas con el líder del proceso.

VI. DESARROLLO DEL EJERCICIO DE AUDITORIA.

1. Auditoria a las Políticas de seguridad de la información

Las políticas de seguridad se desarrollan con el fin de preservar la información y los sistemas de una Empresa, y garantizando la integridad, confidencialidad y disponibilidad de la información. Las políticas de seguridad deben ser conocidos por todo el personal de una organización.

Las Políticas de Seguridad de la Información son elementos fundamentales dentro del SGSI puesto que contienen directrices que enmarcan la actuación de todos los servidores públicos y el cumplimiento de los requisitos legales relacionados con las mismas.

La adopción de las Políticas de Seguridad de la Información es una decisión estratégica que tiene como propósito la protección de los activos estratégicos de una entidad que dependen o usan las tecnologías de la información y las comunicaciones, así como el fortalecimiento de la cultura de la Seguridad de la Información, en los servidores públicos.

1. Información Analizada

La Oficina de Control Interno reviso y analizó la información sobre las Políticas de Políticas de Seguridad de la Información entregada por la Oficina Asesora de Planeación y Sistemas, mediante memorando No. 20201200006033 con fecha del 28 de abril de 2020, la dispuesta en el drive “Control Interno - Sistemas” compartido (https://drive.google.com/drive/folders/0AAPCseHTvPEBUk9PVA), la publicada en el sistema Isolución en el proceso de Gestión de Infraestructura y la publicada en la página web de la entidad en planes y programas, correspondiente a los documentos:

- Plan de seguridad y privacidad de la información
- Alcance, política y objetivos del sistema de gestión de seguridad de la información
- Compromiso y política de seguridad de acceso a la infraestructura tecnológica

2. Resultados de la Evaluación

A continuación, se presenta el desarrollo de cada una de las evaluaciones realizadas y las observaciones resultantes de las actividades efectuadas por la Oficina de Control Interno a las Políticas de seguridad de la información.

Las observaciones producto de la evaluación realizada, se dieron a conocer a la Oficina Asesora de Planeación y Sistemas por medio de correo electrónico de fecha 13 de mayo de 2020, recibiendo comentarios el día 14 de mayo de 2020 y aclaradas en reunión virtual del día 18 de mayo de 2020.

I. Políticas de Seguridad de la Información

Observación - Falta de adopción de las políticas de seguridad de la información

Descripción o situación encontrada:

Los lineamientos de la Política de Gobierno Digital así como norma técnica colombiana NTC ISO/IEC 27001:2013 y las mejores prácticas ISO-IEC 27002:2013, buscan que las Entidades consideren un esquema de gobierno de TI que establezca la implementación de políticas de seguridad de la información con el fin de favorecer, la adecuada gestión y control de la infraestructura de Tecnología de Información y Comunicaciones "TICs" y la seguridad de la información de la entidad.

1. La Oficina Asesora de Planeación elaboro durante el año 2019, el documento "*Plan de Seguridad y Privacidad de la Información*", el cual define el plan de acción para la implementación del Sistema de Seguridad de la Información alineado con los demás sistemas institucionales y que está en proceso de revisión. El documento describe las directrices requeridas para definición e implementación de las Políticas para la Seguridad de la Información, como se observa en la siguiente imagen:

10. ANALISIS OBJETIVOS DE CONTROL

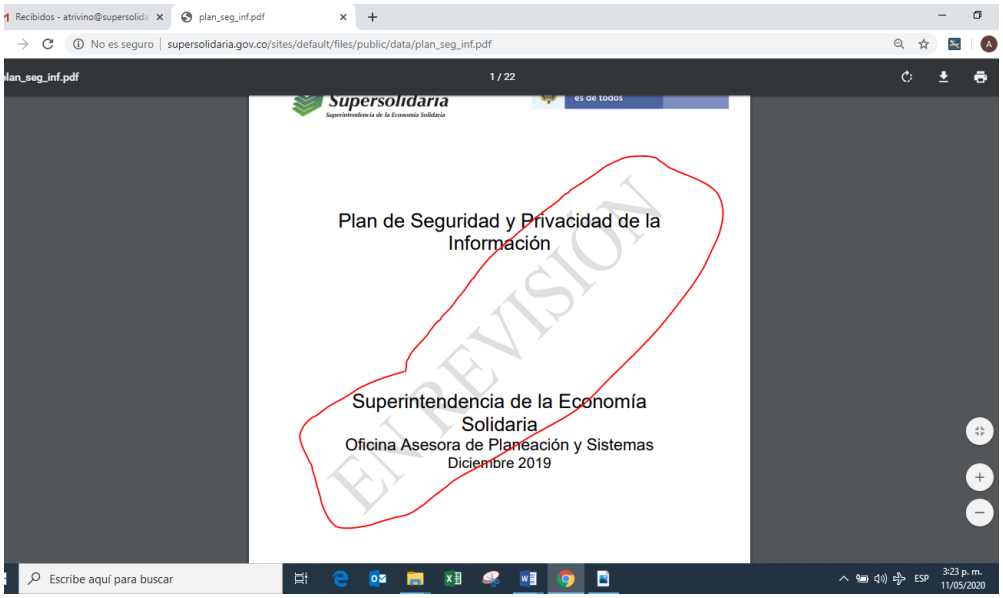
ISO 27002	Objetivo de Control	Control
A.5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.

Fuente: Plan de Seguridad y Privacidad de la Información publicado en la página Web.

La presentación para su aprobación está programada para la sesión tres (3) del Comité Institucional de Gestión y Desarrollo que se realizara en el mes de septiembre de 2020, donde se presentarán los documentos trabajados por la Oficina Asesora de Planeación y Sistemas sobre el tema "Gestión del conocimiento Seguridad de la Información", de acuerdo al cronograma de sesiones establecido, tal como se observa en la siguiente imagen:

Fuente: Cronograma presentaciones al Comité de Gestión y Desempeño 2020

La auditoría observó que en la página web de la Superintendencia, se encuentra publicado el "Plan de Seguridad y Privacidad de la Información de fecha diciembre 2019", con la nota informativa "*EN REVISION*", al respecto la Oficina Asesora de Planeación y Sistemas informo que el documento publicado corresponde al documento formulado y que esta para ser presentado al Comité Institucional de Gestión y Desarrollo, tal como se observa en la siguiente imagen:



2. El documento "*DEFINICIÓN DEL ALCANCE, POLÍTICA Y OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN*" de octubre de 2019, fue elaborado por la Oficina Asesora de Planeación para definir el alcance,

política y objetivos del sistema de gestión de seguridad de la información a implementar por la entidad.

3. El documento “COMPROMISO Y POLÍTICA DE SEGURIDAD DE ACCESO A LA INFRAESTRUCTURA TECNOLOGICA”, que se encuentra publicado en el Sistema de Gestión de Calidad define la política de seguridad y acceso a la infraestructura tecnológica por parte de los usuarios de la entidad.

Una vez analizados los documentos anteriores, la auditoría evidencia:

1. El documento “Plan de Seguridad y Privacidad de la Información”, se encuentra en proceso de revisión por parte de la Oficina Asesora de Planeación.

2. La Superintendencia **no** posee el Plan de Seguridad y Privacidad de la Información aprobado y formalizado a nivel institucional con los lineamientos establecidos por la Política de Gobierno Digital, no se tienen definidas las políticas para la seguridad de la información, aprobadas por la dirección, publicadas y comunicada a los empleados y partes externas pertinentes.

Posibles causas identificadas por la Oficina de Control Interno:

1. Demora en la revisión del Plan de Seguridad y Privacidad de la Información.
2. No se tiene el del Plan de Seguridad y Privacidad de la Información aprobado para iniciar con la implementación de las Políticas de Seguridad de la Información.

Descripción del riesgo:

1. Pérdida de confidencialidad, integridad, disponibilidad de la información.

Recomendaciones:

1. Realizar las gestiones que sean necesarias para revisar y ajustar el documento Plan de Seguridad y Privacidad de la Información.
2. Presentar el Plan de Seguridad y Privacidad de la Información ante el Comité Institucional de Gestión y desempeño en la fecha establecida y a la alta Dirección, para su aprobación y publicación en la página web.
3. Una vez aprobado el Plan de Seguridad y Privacidad de la Información, definir una metodología que incluya un plan de trabajo y un cronograma, que permitan realizar el seguimiento a las actividades ejecutadas para la definición e

implementación de las Políticas de Seguridad de la Información de acuerdo a los lineamientos de la política de Gobierno Digital .

COMENTARIO OFICINA ASESORA DE PLANEACIÓN Y SISTEMAS

Se sugiere enmarcar la observación como falta de adopción de la política de seguridad de la información definida y aprobada.

RESPUESTA OFICINA DE CONTROL INTERNO:

De acuerdo con el comentario presentado por la Oficina Asesora de Planeación y Sistemas, la Oficina de Control Interno, aclara que la auditoria se realizó a las de Políticas de Seguridad de la Información, por lo anterior, la observación se mantiene en los términos señalados en el informe.

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 no tiene el Plan de Seguridad y Privacidad de la Información aprobado y definidas las políticas para la seguridad de la información, por lo anterior recomienda:

1. Realizar la presentación del *Plan de Seguridad y Privacidad de la Información* al Comité Institucional de Gestión y Desempeño, para su aprobación y formalización.

2. Definir una metodología que incluya un plan de trabajo y un cronograma, para la definición e implementación de las Políticas de Seguridad de la Información de acuerdo a los lineamientos de la política de Gobierno Digital.

3. Realizar seguimiento periódico a las Políticas de Seguridad de la Información para mantenerlas actualizadas de acuerdo a los lineamientos normativos y procesos de la Entidad.

VIII. CONCLUSIONES

La Oficina Asesora de Planeación y Sistemas durante la vigencia 2019 elaboro el Plan de Seguridad y Privacidad de la Información, teniendo en cuenta los lineamientos establecidos por Gobierno Digital y la metodología de MinTIC, documento que se encuentra en revisión para su presentación, aprobación y formalización ya que este es

el insumo para la adopción de las Políticas de Seguridad de la Información en la Entidad.

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 cinco (5) 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	Falta de adopción de las políticas de seguridad de la información	NO

Cordialmente,

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

Elaboró: Alexandra Triviño Martínez