



SUPERINTENDENCIA DE LA ECONOMIA SOLIDARIA

RESOLUCION 2022120001645 DE

5 de abril de 2022

Por la cual se adopta el Sistema de Gestión de Seguridad de la Información y Seguridad Digital–SGSI- de la Superintendencia de la Economía Solidaria

EL SUPERINTENDENTE DE LA ECONOMÍA SOLIDARIA

En ejercicio de las facultades legales y en especial las conferidas en el numeral 3° del artículo 5° del Decreto 186 del 26 de enero de 2004,

CONSIDERANDO:

Que la Constitución Política de Colombia, en su artículo 15, consagra que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar la Información que se haya recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas

Que la Ley Estatutaria 1581 de 2012, “*por la cual se dictan disposiciones generales para la protección de datos personales*”, tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15, 17 y 20 de la Constitución Política.

Que la 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*”, tiene como objeto principal regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información

Que el Decreto 1078 de 2015, modificado por el Decreto 1008 de 2018 “*Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones*”, en el artículo 2.2.9.1.1.3., incluye la seguridad de la información entre los principios de la Política de Gobierno Digital; de igual manera, en el artículo 2.2.9.1.2.1. se establece que la Política de Gobierno Digital se desarrollará a través de componentes y habilitadores transversales¹, y respecto de estos últimos indica que son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Que el numeral 8 del artículo 2 de la Ley 1341 de 2009 establece que el Gobierno Nacional fijará los mecanismos y condiciones para garantizar la masificación del Gobierno en Línea, con el fin de lograr la prestación de servicios eficientes a los ciudadanos, así mismo, la citada Ley determinó que es función del Estado intervenir en el sector de las TIC, con el fin de promover condiciones de seguridad del servicio al usuario final, incentivar acciones preventivas y de seguridad informática y de redes

Continuación de la Resolución Por la cual se adopta el Sistema de Gestión de Seguridad de la Información y Seguridad Digital– SGSI- de la Superintendencia de la Economía Solidaria

para el desarrollo de dicho sector; así como reglamentar las condiciones en que se garantizará el acceso a la información en línea, de manera abierta, ininterrumpida y actualizada

Que el Gobierno Nacional expidió el Decreto 1008 de 2018 *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y subrogó el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"*.

Que el capítulo I, sección 2, artículo 2.2.9.1.1.3., del decreto 1008 incluye la seguridad de la información entre los principios de la Política de Gobierno Digital, igualmente el artículo 2.2.9.1.2.1. define la seguridad de la información como habilitador transversal de la Política de Gobierno Digital que junto a los demás habilitadores permiten el desarrollo de los componentes y logros incluidos en dicha política.

Que el CONPES 3854 de 2016 establece Política Nacional de Seguridad Digital.

Que alineados con la política de Gobierno Digital y teniendo en cuenta la norma NTC-ISO/IEC 27001, que da lineamientos de cómo gestionar la seguridad de la información en una organización, se determina que la implementación del Sistema de Gestión de Seguridad de la Información – SGSI- se realice en el marco de dicha norma, sobre el cual se desarrolla la política de seguridad y privacidad de la información.

Que a través de la resolución 2020121009145 del 30 de septiembre de 2020 la Superintendencia de la economía solidaria adoptó el Plan Estratégico de Tecnologías de Información – PETI 2019 – 2022 y el Plan de Seguridad y Privacidad de la Información 2019.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones expidió la Resolución 500 de 2021, *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital."*

Que el artículo 3 de la resolución anteriormente citada establece que *"Los sujetos obligados deben adoptar medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Las entidades deben contar con políticas, procesos, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI. En ese sentido, deben adoptar los lineamientos del MSPI, guía de riesgos y gestión de incidentes de seguridad digital."*

Para todos los procesos, trámites, sistemas de información, infraestructura tecnológica e infraestructura crítica de los sujetos obligados, se deben adoptar medidas de seguridad eficientes alienadas al MSPI, para prestar servicios de confianza, generando protección de la información de los ciudadanos, gestionando los riesgos y los incidentes de seguridad digital."

Que el artículo 4 de la Resolución 500 de 2021 señala que *"Los sujetos obligados deben aplicar los modelos, guías, y demás documentos técnicos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones a través del habilitador de seguridad y privacidad de la información en el marco de la Política de Gobierno Digital y propenderán por la incorporación de estándares internacionales y sus respectivas actualizaciones o modificaciones, al igual que otros marcos de trabajo que defina mejores prácticas en la materia."*

Que el artículo 5 ibidem, indica que *"Los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de*

Continuación de la Resolución Por la cual se adopta el Sistema de Gestión de Seguridad de la Información y Seguridad Digital- SGSI- de la Superintendencia de la Economía Solidaria

2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue.

Que dado lo anterior, se hace necesario adoptar mediante acto administrativo el Sistema de Gestión de Seguridad de la Información -SGSI- y Seguridad Digital de la Superintendencia de la Economía Solidaria.

Que en mérito de lo anterior.

RESUELVE:

ARTÍCULO 1°.-ADOPCIÓN. La presente resolución tiene por objeto la adopción del Sistema de Gestión de Seguridad de la Información y Seguridad Digital - SGSI de la Superintendencia de la Economía Solidaria.

ARTÍCULO 2. OBJETIVO. Esta resolución tiene por objetivo establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI y la NTC 27001. Así mismo, establece las directrices y estándares para la estrategia de seguridad digital.

ARTÍCULO 3. LINEAMIENTOS GENERALES. Se deben adoptar los lineamientos del MSPI, guía de riesgos y Gestión y Clasificación de Incidentes de Seguridad de la Información del MINTIC. Para los procesos de Gestión de Servicios de TI (GSTI) y Gestión de Tecnologías de la Información (GETI), se deben adoptar medidas de seguridad eficientes alienadas al MSPI, para prestar servicios de confianza, generando protección de la información de los ciudadanos, gestionando los riesgos y los incidentes de seguridad digital.

ARTÍCULO 4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL. El Plan de Seguridad y Privacidad de la Información contempla la protección de la información digital, medios impresos y físicos digitales y no digitales.

La estrategia de seguridad digital se debe definir en la implementación del MSPI, así como de la Política para la Administración de Riesgos de la Superintendencia de la economía solidaria y del procedimiento de gestión de incidentes de seguridad digital.

ARTÍCULO 5. LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y LA GESTIÓN DE RIESGOS DE LA SUPERINTENDENCIA DE LA ECONOMÍA SOLIDARIA. Se debe implementar controles para mitigar los riesgos que afecten la seguridad digital y física teniendo en cuenta los resultados del análisis y evaluación de los riesgos.

ARTÍCULO 6. CONTROLES E INTEROPERABILIDAD. Se deben implementar controles y procesos que habiliten la integración al servicio ciudadano digital de interoperabilidad de forma segura y cumpliendo de los lineamientos dados sobre el particular en el marco de la política de gobierno digital.

ARTÍCULO 7. GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL. Se debe establecer un procedimiento de gestión de incidentes de seguridad digital, para realizar el tratamiento, investigación y gestión de los incidentes de seguridad digital que se presente en relación con los activos de información de los procesos de Gestión de Servicios de TI (GSTI) y Gestión de Tecnologías de la Información (GETI).

ARTÍCULO 8. PRIVACIDAD DE LA INFORMACIÓN. Se debe definir una estrategia que permita brindar servicios, controles y condiciones de protección de la privacidad de la información de la Superintendencia de la Economía Solidaria y los ciudadanos acordes con lo exigido en la Ley 1581 de 2012 y los decretos reglamentarios.

Continuación de la Resolución Por la cual se adopta el Sistema de Gestión de Seguridad de la Información y Seguridad Digital– SGSI- de la Superintendencia de la Economía Solidaria

ARTÍCULO 9. MECANISMOS DE AUTENTICACIÓN. Se deben emplear mecanismos para la autenticación y segregación de las funciones y responsabilidades de los usuarios con privilegios de administrador o que brindan soporte remoto.

ARTÍCULO 10. RETENCIÓN Y DESTRUCCIÓN FINAL DE INFORMACIÓN. Se deben establecer procesos y procedimientos para la retención y destrucción final de la información digital, para ello se debe seguir las normas de gestión documental digital dispuestas por el Archivo General de la Nación.

ARTÍCULO 11. SEGURIDAD DIGITAL DESDE EL PROCESO DE DESARROLLO DE SOFTWARE. Se debe integrar la seguridad digital, dentro del ciclo de vida del desarrollo del software para todos los sistemas de información, aplicaciones web y móviles, así como cualquier otro sistema que almacene, transmita o presente información, desde las etapas iniciales como el diseño y el levantamiento de requerimientos, hasta las pruebas de seguridad.

ARTÍCULO 12. TERCEROS, COLABORADORES Y SEGURIDAD DIGITAL. Deben incluir en su estrategia de seguridad digital y su plan de Seguridad y privacidad de la información, las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas y controles para la gestión de los riesgos de seguridad y privacidad de la información por parte de terceros y colaboradores.

ARTÍCULO 13. CONTROL DE LAS ACTIVIDADES INCLUIDAS EN LA ESTRATEGIA DE SEGURIDAD DIGITAL Y GESTIÓN DE RIESGOS. Se debe establecer los mecanismos de control al interior de la Superintendencia de la Economía Solidaria que permita verificar el cumplimiento de las disposiciones establecidas en la política de seguridad de la información, realizando auditorías de seguridad de la información al menos una vez al año, que contemplen aspectos técnicos de la seguridad digital como análisis de vulnerabilidades a sistemas de información.

ARTÍCULO 14. RESPONSABLE. Será responsable del sistema de gestión de seguridad de la información el Oficial de seguridad de la información, que en caso de no contar con esta figura la responsabilidad será asumida por el Jefe de la Oficina Asesora de Planeación y Sistemas.

ARTÍCULO 15. APROBACIÓN. De conformidad con el Comité Institucional de Gestión y Desempeño llevado a cabo el día 30 de noviembre del 2021, soportado en el acta número 21, se aprobó la adopción del Sistema de Gestión de Seguridad de la Información y Seguridad Digital– SGSI y sus políticas complementarias que a continuación se relacionan:

1. PO-GETI-001 Política de Backup y Restauración V.0.
2. PO-GETI-002 Política de control de acceso V.0.
3. PO-GETI-003 Política de seguridad y privacidad de la información V.0.
4. PO-GETI-004 Políticas de adquisición, desarrollo y mantenimiento de sistemas de información
5. PO-GETI-005 Políticas de criptografía V.0.
6. PO-GETI-006 Política de gestión de activos de información
7. PO-GETI-007 Políticas de gestión de incidentes de seguridad de la información V.0.
8. PO-GETI-008 Políticas de la organización de la seguridad de la información
9. PO-GETI-009 Políticas de relación con los proveedores
10. PO-GETI-010 Políticas de seguridad de las comunicaciones
11. PO-GETI-011 Políticas de seguridad de las operaciones
12. PO-GETI-012 Políticas de seguridad de los recursos humanos
13. PO-GETI-013 Políticas de seguridad física y el entorno

Continuación de la Resolución Por la cual se adopta el Sistema de Gestión de Seguridad de la Información y Seguridad Digital– SGSI- de la Superintendencia de la Economía Solidaria

ARTÍCULO 16. VIGENCIA Y DEROGATORIA. La presente resolución rige a partir de la fecha de su publicación y deroga las disposiciones que sean contrarias.

COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C., a los
5 de abril de 2022

VIVIAN CAROLINA BARLIZA ILLIDGE
Superintendente

Proyectó: Luis Edwin Osorio
Proyectó: Erika Jazmín Ladino
Revisó: Javier Enrique Ariza Rodríguez
Revisó: Robin Andrey Suarez Toscano
Revisó: Rodolfo Yanguas Rengifo
Revisó: Yina Paola Gutiérrez Castellanos
Revisó: María Mónica Pérez López