TABLA DE CONTENIDO

1. INTRODUCCIÓN

Todas las entidades enfrentan riesgos procedentes de una amplia variedad de amenazas que pueden afectar de forma crítica la información y sus recursos de procesamiento y transmisión, y en pro de enfrentar estas circunstancias, las entidades deben establecer estrategias y controles adecuados, que garanticen una gestión segura de los procesos y permitan brindar mayor protección a la información, es por ello, que estas estrategias y lineamientos para la protección y control parten de marcos normativos establecidos, que deben ser desarrollados en las entidades públicas para realizar una gestión adecuada, como es el caso de la implementación de modelo integrado de planeación y gestión y recomendaciones de nivel nacional a través del Ministerio de las TIC's.

El Ministerio del trabajo ha reconocido la información como un activo vital en su organización, de esta forma, y con el fin de mitigar los riesgos y proteger la información, es necesario implementar un conjunto de controles y procedimientos para alcanzar un nivel apropiado de seguridad de la información, así como los mecanismos para administrar, mantener y mejorar los controles a lo largo del tiempo, por lo anterior se define un Sistema de Gestión de Seguridad de la Información (SGSI), el cual ayudará a identificar y reducir los riesgos vitales de seguridad de la información.

2. JUSTIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI

El Sistema de gestión de seguridad de la información (SGSI) hace parte del sistema integrado de gestión del Ministerio del Trabajo, este se basa en un enfoque de gestión de riesgos de seguridad de la información de los procesos. En el contexto de los riesgos globales de la Entidad, el SGSI tiene como objetivo establecer, implementar, operar, hacer seguimiento, mantener y mejorar la seguridad de la información.

La gestión de la seguridad de la información es una tarea continua que se realiza con el fin de preservar las propiedades de confidencialidad, integridad y disponibilidad en los activos de información que manejan los procesos del Ministerio del Trabajo, con base en su nivel de riesgo; en razón a ello, el SGSI permite a la entidad identificar, implementar, mantener y mejorar los controles que requiere para tratar los riesgos de seguridad de la información y llevarlos a niveles aceptables, de tal forma que estos controles sean suficientes para proporcionar un ambiente de control y seguridad adecuados.

Los lineamientos del Sistema de gestión de seguridad de la información son aplicables a cualquier proceso del Ministerio del Trabajo, sin importar su tamaño o función, dado que la implementación del sistema debe ser proporcional a la criticidad de los activos de información que maneja, y los riesgos identificados en los mismos.

El SGSI del Ministerio del Trabajo establece un sentido general de dirección, gestión y principios con relación a la seguridad de la información, orientados en su totalidad al cumplimiento de la política de seguridad de la información del Ministerio, teniendo en cuenta los requisitos normativos internos, los legales o reglamentarios, y las obligaciones contractuales.

Como parte del liderazgo y compromiso de la alta dirección del Ministerio del Trabajo, se crea el comité de gobierno digital y seguridad de la información mediante la resolución 3162 del 11 de agosto de 2016, para asegurar que se adopte la política general de seguridad de la información, las políticas técnicas y los procedimientos de esta, y que además sean compatibles con la dirección estratégica de la entidad. (Requisito de ISO 27001:2013 - 5.1 Liderazgo y Compromiso).

3. MARCO DE REFERENCIA NORMATIVA

A continuación se presenta el marco de referencia normativa bajo el cual se identifican los requerimientos legales que obligan al Ministerio del Trabajo diseñar, implementar, dar a conocer a todos los funcionarios, contratistas y terceros con los que se tiene relación y hacer seguimiento de los lineamientos planteados frente a la protección de la información, que se ha decidido implementar teniendo en cuenta los modelos y documentos guía del Ministerio de las Tecnologías de la información y las comunicaciones.

Norma	Objeto	Referencia
Ley 87 de 1993	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones	*Se entiende por control interno el sistema integrado por el esquema de organización y el conjunto de planes, métodos principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por cada entidad, con el fin de procurar que todas las actividades operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas y objetivos previstos.*
Ley 527 de 1999	Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos	El mensaje de datos es "*La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos, Internet, el correo electrónico, el telegrama, el télex o el telefax*".
Ley 594 de 2000	Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones	Responsabilidad "*Los servidores públicos son responsables de la organización, conservación, uso y manejo de los documentos*" Administración y acceso. "*Es una obligación del Estado la administración de los archivos públicos y un derecho de los ciudadanos el acceso a los mismos, salvo las excepciones que establezca la ley*;"
Ley 599 DE 2000	Por la cual se expide el Código Penal.	En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar

Norma	Objeto	Referencia
		la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa."
Ley 734 de 2002	Por la cual se expide el Código Disciplinario Único.	*Art 34. Deberes. Son deberes de todo servidor público "4. Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.* *5. Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos. "*
La Ley 850 de 2003	Por medio de la cual se reglamentan las veedurías ciudadanas.	Principio de Transparencia "*A fin de garantizar el ejercicio de los derechos, deberes, instrumentos y procedimientos consagrados en esta ley, la gestión del Estado y de las veedurías deberán asegurar el libre acceso de todas las personas a la información y documentación relativa a las actividades de interés colectivo de conformidad con lo dispuesto en esta ley y en las normas vigentes sobre la materia*".
Ley 962 de 2005	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.	Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.
Ley 1150 de 2007	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones	Específicamente, se establece la posibilidad de que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual prevé el

Norma	Objeto	Referencia
	generales sobre la contratación con Recursos Públicos.	desarrollo del Sistema Electrónico para la Contratación Pública, Secop.
Ley 1266 de 2008	Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.	Principio de seguridad. *La información que conforma los registros individuales constitutivos de los bancos de datos a que se refiere la ley, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado;*
Ley 1221 de 2008	Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones	Teletrabajo. *Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo*.
Ley 1273 de 2009	Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.	"*De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos"*
Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009	Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones.	Esta resolución modifica los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. Esta regulación establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet de implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT, cumpliendo los principios de confidencialidad de datos, integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así

Norma	Objeto	Referencia
		como medidas para autenticación, acceso y no repudio. Así mismo, establece obligaciones a cumplir por parte de los proveedores de redes y servicios de telecomunicaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información.
CONPES 3701 de 2011	Este documento busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.	Este documento define un plan de acción para la ejecución de la política en ciberseguridad y ciberdefensa, el cual estará a cargo de las entidades involucradas, fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra la defensa y seguridad nacional en el ámbito cibernético (ciberseguridad y ciberdefensa), creando un ambiente y unas condiciones para brindar protección en el ciberespacio. Para cumplir este objetivo general, se formularon tres objetivos específicos: (i) implementar instancias apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias cibernéticas para afrontar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional; (ii) brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberdefensa y ciberseguridad; y (iii) fortalecer la legislación en materia de ciberseguridad y ciberdefensa, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales en esta temática.
Ley 1581 de 2012	Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales	Se hace referencia, principalmente, al artículo 15 de la Constitución Nacional en el cual se establece que "*todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la*

Norma	Objeto	Referencia
		libertad y demás garantías consagradas en la Constitución…".
Decreto 884 de 2012	Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.	*El empleador debe informar al teletrabajador sobre las restricciones de uso de equipos y programas informáticos, la legislación vigente en materia de protección de datos personales, propiedad intelectual, seguridad de la información y en general las sanciones que puede acarrear por su incumplimiento.*
Decreto 886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, en lo relativo al Registro Nacional de bases de datos.	Serán objeto de inscripción en el Registro Nacional de Bases de Datos, "l*as bases de datos que contengan datos personales cuyo Tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él, en este último caso, siempre que al Responsable del Tratamiento o al Encargado del Tratamiento le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. Lo anterior sin perjuicio de las excepciones previstas en el artículo 2° de la Ley 1581 de 2012*".
Ley 1712 de 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública	Hace referencia, principalmente, al artículo 74 de la Constitución Nacional en el cual se establece que "*Todas las personas tiene derecho a acceder a los documentos públicos salvo los casos que establezca la ley*".
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones	"*La información pública que contiene datos semiprivados o privados, definidos en los literales g) y h) del artículo 3° de la Ley 1266 de 2008, o datos personales o sensibles, según lo previsto en los artículos 3° y 5° de la Ley 1581 de 2012 y en el numeral 3° del artículo 3° del Decreto 1377 de 2013, solo podrá divulgarse según las reglas establecidas en dichas normas."*
CONPES 3854 de 2016	Por el cual se crea y justifica la Política Nacional de Seguridad Digital.	*El enfoque de la política de ciberseguridad y ciberdefensa, hasta el momento, se ha concentrado en contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos de (i) defensa del*

Norma	Objeto	Referencia
		país; y (ii) lucha contra el cibercrímen. Si bien esta política ha posicionado a Colombia como uno de los líderes en la materia a nivel regional, ha dejado de lado la gestión del riesgo en el entorno digital. Enfoque esencial en un contexto en el que el incremento en el uso de las TIC para realizar actividades económicas y sociales ha traído consigo nuevas y más sofisticadas formas de afectar el desarrollo normal de estas en el entorno digital. Hecho que demanda una mayor planificación, prevención, y atención por parte de los países.
Decreto 1499 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.	*Establece dentro de las funciones que deben cumplir los Comités Sectoriales de Gestión y Desempeño (ARTÍCULO 2.2.22.3.6 inciso 5): " 5. Dirigir y articular a las entidades del sector administrativo en la operación de las políticas de gestión y desempeño y de las directrices impartidas por la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones en materia de Gobierno y Seguridad Digital."*
Decreto Nacional 1008 de 2018	Política de Gobierno Digital	*Establece lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.*

4. OBJETIVO DEL SGSI

El objetivo primordial del SGSI es el de implementar y mantener la seguridad de la información del Ministerio del Trabajo, involucrando sus procesos, los sistemas de información, la información generada y administrada que por sus funciones debe operar, las entidades, las personas interesadas en sus servicios y la transferencia de información. El SGSI, contiene las políticas, procedimientos, directrices, metodologías y controles necesarios para la gestión de seguridad de la Información, alineados con lo establecido por las directrices del Ministerio de telecomunicaciones - MINTIC y el estándar internacional ISO 27001:2013.

4.1. Objetivos específicos del Sistema de Gestión de Seguridad de la información

- Fortalecer la cultura de prevención de riesgos de seguridad de la información por medio de la sensibilización y el entrenamiento constante de los funcionarios del Ministerio.

- Gestionar oportunamente los riesgos de seguridad de la información a través del establecimiento e implementación de planes de tratamiento y el mejoramiento continuo de los controles de seguridad.

- Garantizar la disponibilidad requerida por el Ministerio, de los sistemas informáticos vitales para el desarrollo de los procesos misionales de la entidad.

- Minimizar los riesgos sobre los sistemas informáticos, identificando y gestionando oportunamente las vulnerabilidades técnicas a nivel de sistemas operativos, aplicaciones de software y bases de datos utilizadas por los procesos internos y los servicios prestados por el Ministerio.

- Gestionar diligentemente los eventos e incidentes de seguridad y ciberseguridad, fortaleciendo la capacidad de Ministerio para hacer frente a las amenazas y ataques informáticos incluyendo los generados desde el ciberespacio.

- Fortalecer el mejoramiento continuo del sistema a través de la planeación y ejecución de los programas de auditoría y la aplicación oportuna de las acciones correctivas y de mejora requeridas por el Sistemas de Gestión de Seguridad de la información (SGSI).

5. ALCANCE DEL SGSI

Es importante aclarar que la adopción de políticas, normas y procedimientos debe obedecer a decisiones estratégicas adoptadas por el Ministerio del Trabajo y estas deben analizarse, diseñarse e implementarse para satisfacer los requerimientos, las necesidades, los objetivos, los requisitos de seguridad, los procesos implementados, el tamaño y estructura de la misma. Por lo anterior es importante que el Sistema de Gestión de Seguridad de la Información, sea conocido y difundido a todos los funcionarios, contratistas y terceros o partes interesadas que posean cualquier vínculo contractual con la entidad, y su cumplimento es una obligación de todos los funcionarios de la entidad independientemente de sus cargos, jerarquías, niveles de responsabilidad, o tipos de vinculación con el Ministerio.

El Sistema de Gestión de Seguridad de la Información cubre la totalidad de las dependencias del Ministerio del Trabajo de acuerdo con el organigrama institucional y abarca la totalidad de sus procesos.

6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la información ha sido definida y aprobada por el comité de seguridad de la información y se establece en ella de forma clara, las líneas de actuación en Seguridad de la Información alineadas con los objetivos de la entidad.

A continuación, se presenta la Política de Seguridad de la Información definida y aprobada por el Ministerio

"De acuerdo con la misión de formular, adoptar y orientar la política pública en materia laboral, el Ministerio del Trabajo diseña, implementa y supervisa las medidas necesarias para proteger la información que por su función custodia, administra y genera, de los riesgos a los que está expuesta dicha información y que pueden llegar a afectar su disponibilidad, integridad y confidencialidad. Estos riesgos son gestionados de forma eficiente, efectiva y transparente en todos sus procesos, fomentando la mejora continua en materia de seguridad de la información."