



MINISTERIO DEL TRABAJO

RESOLUCIÓN NÚMERO 5699 DE 2016

(30 DIC 2016)

Por la cual se adopta la Política de Seguridad de la Información del Ministerio del Trabajo.

LA MINISTRA DEL TRABAJO

En uso de sus atribuciones constitucionales, legales y reglamentarias, y en particular, las conferidas por el Artículo 6º del decreto 4108 de 2011, y el numeral 10 del Artículo 28 de la resolución 3162 del 11 de agosto de 2016, y

CONSIDERANDO

Que el Ministerio del Trabajo reconoce que la información y su adecuado manejo es un activo esencial para su organización y funcionamiento;

Que el Ministerio del Trabajo tiene el deber legal de proteger su información de amenazas y de posibles riesgos que puedan afectar dicha información, los recursos para su procesamiento, manejo y transmisión;

Que el Ministerio del Trabajo debe establecer estrategias y controles adecuados, para garantizar la gestión segura y la protección de la información;

Que el Título 9 del decreto 1078 de 2015 o Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones - TIC, sobre Políticas y Lineamientos de Tecnologías de la Información; Capítulo 1, Estrategia de Gobierno en Línea; Sección 2, Artículo 2.2.9.1.2.1., y siguientes, definen los componentes, instrumentos y responsables de seguridad de la información, comprendiendo acciones transversales, tendientes a proteger la información y los sistemas de información e impedir el acceso, uso, divulgación, interrupción o destrucción no autorizados;

Que la Norma Técnica Colombiana NTC-ISO-IEC 27001:2013, ofrece un modelo para establecer, implementar, operar, revisar, hacer mantenimiento y mejorar los sistemas de gestión de seguridad de la información – SGSI;

Que el Ministerio del Trabajo mediante la Resolución 3162 del 11 de agosto de 2016, creó el Comité de Seguridad de la Información para asegurar el cumplimiento de la Política de Seguridad de la Información y los objetivos de la misma, acordes con la dirección estratégica de la entidad;

30 DIC 2016

Continuación de la Resolución "Por la cual se adopta la política de Seguridad de la información del Ministerio del Trabajo".

Que la Política de Seguridad de la Información fue discutida por el Comité de Seguridad de la Información, según acta del 6 de diciembre de 2016, contenida en el documento política de seguridad de la información del Ministerio del Trabajo.

En mérito de lo expuesto,

RESUELVE

ARTÍCULO PRIMERO. APROBAR Y ADOPTAR la Política de Seguridad de la información del Ministerio del Trabajo, cuyos enunciados, lineamientos y directrices generales, están referidos en el documento política de seguridad de la información del Ministerio del Trabajo.

ARTÍCULO SEGUNDO: ORDENAR al Comité de Seguridad de la Información, tomar las medidas pertinentes para asegurar la información del Ministerio del Trabajo, protegiendo su disponibilidad, integridad y confidencialidad, gestionando riesgos y amenazas contra los procesos informáticos y procurando su mejora continua;

ARTÍCULO TERCERO. VIGENCIA. La presente resolución rige a partir de la fecha de su publicación.

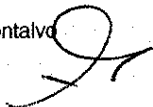
PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá D. C., a los

30 DIC 2016


CLARA EUGENIA LÓPEZ OBREGÓN
Ministra del Trabajo

Revisó: L. Fontalvo





 MINTRABAJO	DOCUMENTO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DEL TRABAJO	Código:
		Versión: 1.0
		Fecha: 01 de diciembre de 2016
		Página: 1 de 1

Tabla de Contenido

1. INTRODUCCIÓN	2
2. JUSTIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI.....	2
3. MARCO DE REFERENCIA NORMATIVA	3
4. OBJETIVO DEL SGSI	9
4.1. OBJETIVOS ESPECÍFICOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	9
5. ALCANCE DEL SGSI	9
6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	10

	DOCUMENTO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DEL TRABAJO	Código:
		Versión: 1.0
		Fecha: 01 de diciembre de 2016
		Página: 1 de 2

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 MECI y recomendaciones de nivel nacional a través del Ministerio de las TIC's y los documentos definidos por Gobierno en Línea (GEL).

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.


 MINTRABAJO	DOCUMENTO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DEL TRABAJO	Código:
		Versión: 1.0
		Fecha: 01 de diciembre de 2016
		Página: 1 de 3

Como parte del liderazgo y compromiso de la alta dirección del Ministerio del Trabajo, se crea el comité de 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 la misma, y que además sean compatibles con la dirección estratégica de la entidad. (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	<i>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.</i>
Ley 527 de 1999	Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos	<i>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".</i>
Ley 594 de 2000	Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones	Responsabilidad <i>"Los servidores públicos son responsables de la organización, conservación, uso y manejo de los documentos"</i> Administración y acceso. <i>"Es una obligación del Estado la administración de los archivos"</i>

	DOCUMENTO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DEL TRABAJO	Código:
		Versión: 1.0
		Fecha: 01 de diciembre de 2016
		Página: 1 de 6


Norma	Objeto	Referencia
	preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.	
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 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.
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 <i>“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 libertad y demás garantías consagradas en la Constitución ...”</i> .
Decreto 884 de	Por medio del cual se reglamenta	<i>El empleador debe informar al teletrabajador</i>

 MINTRABAJO	DOCUMENTO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DEL TRABAJO	Código:
		Versión: 1.0
		Fecha: 01 de diciembre de 2016
		Página: 1 de 7

Norma	Objeto	Referencia
2012	la Ley 1221 de 2008 y se dictan otras disposiciones.	<i>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.</i>
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, “ <i>las 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</i> ”.
Decreto Nacional 2573 de 2014	Estrategia de Gobierno en Línea de la República de Colombia	<i>Define los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad</i>
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 “ <i>Todas las personas tiene derecho a acceder a los documentos públicos salvo los casos que establezca la ley</i> ”.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones	“ <i>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</i>

 MINTRABAJO	DOCUMENTO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DEL TRABAJO	Código:
		Versión: 1.0
		Fecha: 01 de diciembre de 2016
		Página: 1 de 8

Norma	Objeto	Referencia
		<i>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."</i>
CONPES 3701	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.
CONPES 3854	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 país; y (ii) lucha contra el cibercrimen. Si bien esta política ha posicionado a Colombia como una 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

 MINTRABAJO	DOCUMENTO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DEL TRABAJO	Código:
		Versión: 1.0
		Fecha: 01 de diciembre de 2016
		Página: 1 de 9

Norma	Objeto	Referencia
		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.

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 de Gobierno en Línea (GEL) y el estándar internacional ISO 27001:2013.

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

- Garantizar la adecuada gestión del Sistema de Gestión de Seguridad de la Información.
- Brindar las herramientas necesarias para apoyar el incremento de la transparencia en la entidad.
- Definir los lineamientos necesarios para la implementación de la gestión de la seguridad y privacidad de la información en el Ministerio del Trabajo.
- Proteger la información, promoviendo siempre la aplicación de las mejores prácticas de seguridad de la información.
- Fortalecer el concepto de ciberseguridad en la entidad.
- Mantener el Sistema de Seguridad de la Información y los principios de seguridad y privacidad, alineados con el marco de referencia de arquitectura empresarial. Teniendo en cuenta el marco de referencia del Ministerio de Tecnologías de Información y las Comunicaciones (MINTIC) y el programa de Gobierno En Línea (GEL).

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

 MINTRABAJO	DOCUMENTO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DEL TRABAJO	Código:
		Versión: 1.0
		Fecha: 01 de diciembre de 2016
		Página: 1 de 10

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 cumplimiento 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

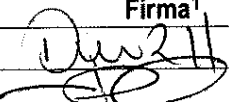

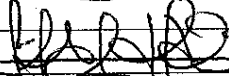
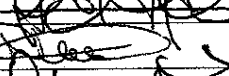

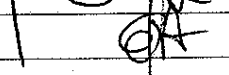
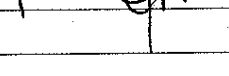
La Política de Seguridad de la información ha sido definida y aprobada por el comité de seguridad de la información y se establece en ella de forma clara, las líneas de actuación en Seguridad de la Información alineadas con los objetivos de la entidad.

A continuación se presenta la Política de Seguridad de la Información definida y aprobada por el Ministerio del Trabajo:

“De acuerdo con la misión de formular, adoptar y orientar la política pública en materia laboral, el Ministerio del Trabajo diseña y adopta las medidas necesarias para proteger la información que por su función custodia, administra y genera, de las amenazas que pueden llegar a afectar su disponibilidad, integridad y confidencialidad. Gestionando los riesgos de forma eficiente, efectiva y transparente en todos sus procesos y realizando una mejora continua en materia de seguridad de la información.”

	PROCESO ADMINISTRACIÓN DEL SIG FORMATO ACTA DE REUNIÓN	Código: ASIG-F-05
		Versión: 4.0
		Fecha: Abril 16 de 2015
		Página 1 de 2

1. DATOS GENERALES			
Acta de reunión No. 2-2016			
Fecha de reunión:	DICIEMBRE 06 DE 2016	Sitio de reunión:	SALA DE JUNTAS PISO 11
Hora:	8:45 AM	Convoca:	LIDER DE SEGURIDAD DELA INFORMACIÓN
Tema:	APROBACIÓN DE DOCUMENTOS DE POLÍTICAS DE SEGURIDAD		
Objetivo:	Aprobar política de seguridad y presupuesto de seguridad para 2017		


2. PARTICIPANTES			
Asistente	Cargo	Teléfono / extensión	Firma ¹
DIANA CASTIBLANCO	PROF.ESPEC.	6024	
JAVIER GÓMEZ	PROF.ESPEC.	1150	
SOFIA SALAMANCA	PROF.ESPEC.	1041	
IVÁN PARDO	JEFE TIC	1170	
NAYIBE GONZALEZ	CONTRATISTA SEG	1193	
ALVARO ESCOBAR	LIDER SEGURIDAD	1193	
EDGAR M. AYALA	PROF.ESPEC.	1170	

3. AGENDA DE REUNIÓN
1. Lectura y aprobación del acta anterior 2. Aprobación de políticas y documentos SGSI 3. Presentación presupuesto de seguridad de la Información para 2017 4. Proposiciones y varios.

4. REVISIÓN DE ACTIVIDADES PENDIENTES		
Actividad	Responsable	Fecha de Ejecución

5. DESARROLLO DE LA AGENDA
1. Se establece la agenda de la reunión. 2. Se lee, aprueba y firma el acta anterior. 3. Se define que la política general es el único documento que se debe firmar por la alta dirección. Se plantean dos posibilidades, a.) Creación de un acto administrativo, b.) Firma de la política por parte de la ministra. Se

¹ Si la reunión es VIRTUAL o NO PRESENCIAL, NO se requiere diligenciar el campo de firma.

	PROCESO ADMINISTRACIÓN DEL SIG FORMATO ACTA DE REUNIÓN	Código: ASIG-F-05
		Versión: 4.0
		Fecha: Abril 16 de 2015
		Página 2 de 2

eleva la consulta al área jurídica quienes manifiestan que el mejor mecanismo es realizar un acto administrativo a través de una resolución.

4. Se da lectura al documento de política SGSI.
5. El comité revisa y da el visto bueno a la política de seguridad de la información.
6. Se plantea nueva reunión para aprobación de las políticas particulares para la semana del 19 de diciembre.
7. El comité establece que se unifiquen las políticas particulares en un solo documento.
8. El líder de seguridad presenta presupuesto preliminar para 2017 el cual es aprobado por el comité y se anexa a la presente acta.
9. En el punto varios Diana Castiblanco pregunta sobre el resultado de la sensibilización, la respuesta es aun general porque a la fecha no se ha procedido a realizar la evaluación y la estadística final de participantes, sin embargo, se establece que el objetivo desensibilización inicial se ha cumplido a satisfacción.

6. ACTIVIDADES A REALIZAR

Actividad	Responsable	Fecha de Ejecución
Lectura y aprobación de documentos	Comité	16/12/2016
Proyectar el acto administrativo de aprobación de la política de seguridad.	Líder de seguridad y Jefe TIC	12/12/2016

Se cierra la sesión a las 9:55 am

**MINISTERIO DE TRABAJO
PRESUPUESTO PRELIMINAR SGSI 2017**

CONCEPTO	CANT	VL. UNITARIO	VL. TOTAL
PROFESIONALES EN SEGURIDAD (*)	11	\$ 12.000.000	\$ 132.000.000
SOFTWARE SGSI	1	\$ 120.000.000	\$ 120.000.000
CAMPAÑA SENSIBILIZACIÓN	1	\$ 50.000.000	\$ 50.000.000
PRUEBAS DE VULNERABILIDAD	20	\$ 2.000.000	\$ 40.000.000
CAPACITACIÓN AUDITOR INTERNO	5	\$ 6.000.000	\$ 30.000.000
PREAUDITORIA EXTERNA	1	\$ 40.000.000	\$ 40.000.000
TOTAL			\$ 412.000.000

(*) ACTIVIDADES A DESARROLLAR 2017

- LEVANTAMIENTO DE ACTIVOS PROCESOS ESTRATÉGICOS Y DE APOYO
- IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS PROCESOS ESTRATÉGICOS Y DE APOYO
- ESTABLECER PLAN DE TRATAMIENTO DE RIESGOS PROCESOS ESTRATÉGICOS Y DE APOYO
- ESTABLECIMIENTO DE PLANES PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD
- ESTABLECIMIENTO DE LOS PLANES DE CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN
- LIDERAR PROCESO DE SEGURIDAD DE LA INFORMACIÓN PARA EL SECTOR
- CULMINAR SENSIBILIZACIÓN A TODOS LOS FUNCIONARIOS
- CAPACITACIONES ESPECÍFICAS A LÍDERES DE PROCESOS
- SUPERVISAR PROCESOS DE AUDITORIA INTERNA Y EXTERNA
- DOCUMENTACIÓN SGSI EN HERRAMIENTA TECNOLÓGICA
- REVISIÓN DE PROCEDIMIENTOS TIC
- INCLUIR EN EL SGSI LAS TERRITORIALES

