Plan de Seguridad y Privacidad de la Información

Versión 1 enero 2020

Contenido

1. INTRODUCCIÓN

El Plan de Seguridad Digital y Privacidad de la Información, establece un análisis de brecha con el fin de determinar el nivel de madurez del Sistema de Gestión de Seguridad de la Información norma NTC ISO/IEC 27001:2013 de la Agencia Nacional de Minería, (en adelante ANM).

Se toma como base la documentación desarrollada por la Oficina de Tecnología e Información que se tiene actualmente, el conocimiento de las personas frente al Sistema de Gestión de Seguridad de la Información y un análisis de todos los dominios de la norma NTC ISO/IEC 27001:2013 establecidos en la Declaración de Aplicabilidad para su implementación de los controles en la ANM.

Es así como, el Plan de Seguridad y Privacidad de la Información y Ciberseguridad está alineado al cumplimiento de la normativa de Gobierno Digital y Seguridad Digital, y se enfoca en acciones para la protección de los activos críticos de información, contrarrestando las amenazas y riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

2. OBJETIVO

Identificar y ejecutar actividades orientadas a fortalecer el aseguramiento de los servicios de TI y la información que genera u obtiene la Agencia Nacional de Minería - ANM, para preservar la confidencialidad, integridad y disponibilidad de la información relacionada con los titulares de derechos o realicen actividades de minería el marco de la Ley 1581 de 2012.

2.1. Objetivos Específicos

a. Fortalecer el aseguramiento de los servicios de TI y la información suministrada o relacionada con titulares de derechos mineros, mediante la medición de la Implementación del Modelo de Seguridad y Privacidad de la Información.

b. Fomentar en los procesos de la Entidad, la gestión de riesgos de seguridad de la información, con base en los activos críticos previamente identificados y las acciones para mitigar el riesgo.

c. Ejecutar actividades en el marco de una metodología de gestión de la seguridad, para establecer un modelo de madurez aplicable y repetible.

d. Definir y socializar políticas, lineamientos, buenas prácticas y recomendaciones para establecer cultura en Seguridad de la Información en la Entidad para lograr el uso y apropiación de las buenas practicas.

3. ALCANCE

La Agencia Nacional de Minería, genera, obtiene, almacena, intercambia, divulga y actualiza información clasificada, reservada y pública, relacionada con los titulares de derechos mineros, sus funcionarios, contratistas y/o terceros contratados por proveedores.

Esta información se considera un activo de valor para la Entidad ya que registra y soporta sus actuaciones en un contexto histórico, frente a las partes interesadas como lo son:

- Titulares de Derechos Mineros.
- Entidades Nacionales
- Entidades Territoriales
- Sociedad y Comunidad Internacional
- Cliente Interno - Unidad

4. DEFINICIONES

Activo de Información: Cualquier elemento que soporta uno o más procesos del negocio, con información definible e identificable, almacenada en cualquier medio y que tiene valor para la ANM, por lo tanto, debe protegerse.

Amenaza: Circunstancia potencial, evento o persona que puede manifestarse en un lugar y momento específico de forma voluntaria o involuntaria y que tiene el potencial de causar daño a un sistema de información de la organización.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo para poder estimar o determinar su nivel. Este análisis provee las bases para la evaluación del riesgo y las decisiones requeridas para implementar su tratamiento.

Ciberespacio: Entorno donde las entidades que están conectadas a la red informática mundial de internet, interactúan.

Confidencialidad: Característica de los activos de información que determina que éstos sólo sean revelados a individuos, procesos, áreas o entidades autorizadas.

Control de Seguridad: Procedimiento, práctica o actividad estructurada, definida para mantener los riesgos de seguridad y privacidad de la información, por debajo de los niveles aceptables.

Disponibilidad: Característica de los activos de información que determina que éstos accesibles y utilizables, cuándo y cómo se requieran, para solicitud de una persona o ente autorizado.

Integridad: Característica de los activos de información que determina que éstos se salvaguarden con exactitud y en completo estado.

Norma NTC-ISO/IEC 27001:2013: Es la versión del año 2013 de la norma ISO 27001 que "proporciona los requisitos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información".

Norma NTC-ISO/IEC 27002:2013: Es la versión del año 2013 de la norma ISO 27002 que "está diseñada para que las organizaciones la usen como un marco de referencia para seleccionar controles dentro del proceso de implementación de un sistema de gestión de la seguridad de la información".

Riesgo: Probabilidad existente que una amenaza pueda explotar una vulnerabilidad y causar un daño a los servicios informáticos de una organización, incluyendo la información existente en estos servicios.

Seguridad de la Información: Gestión de las medidas y controles diseñados para el tratamiento de los riesgos generados por la afectación de la confidencialidad, integridad y/o disponibilidad de los activos de información de una organización de acuerdo con la política de gestión de riesgos aprobada por la Dirección General. Estas medidas y controles incluyen: políticas, procedimientos, guías de implementación, estándares, soluciones de software y hardware, controles electrónicos, capacitación y concienciación.

5. JUSTIFICACIÓN

Adicionalmente el Estado Colombiano cuenta con Normativa vigente que obliga el adecuado tratamiento de la información manejada por la Entidad en términos de confidencialidad, integridad y disponibilidad. Entre otras se citan:

a. **Ley 1437 de 2011, Capítulo IV,** *"utilización de medios electrónicos en el procedimiento administrativo".*
"Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos."

b. **Ley 1581 de 2012**, *Principio de seguridad:*
"La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."

c. **Ley 1581 de 2012, Artículo 17, ítem d**: "*Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento*"

d. **Ley 1712 de 2014**, "*principio de transparencia*":
"*Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia, de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley.*"

e. **Ley 1712 de 2014, artículo 7**: "*Disponibilidad de la información*"
"*En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones.*

Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten."

f. **Ley 1712 de 2014** -Título III "*Excepciones acceso a la información*"
"*Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito.*"

g. **Decreto 2573 de 2014:** *"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea…" donde se encuentra como componente el modelo de Seguridad y Privacidad de la Información.*

h. **Decreto 1413 de 2017**, artículo 2.2.17.6.6, "*Seguridad de la información.*"
"*Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información.*"

i. **Decreto 1413 de 2007**, artículo 2.2.17.6.1, "*Responsable y encargado del tratamiento"*:

"Los operadores de servicios ciudadanos digitales serán responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente y encargados del tratamiento respecto de los datos que otras entidades le proporcionen."

j. **Artículo 2.2.17.6.3**, "*Responsabilidad demostrada*".
"*Los operadores de servicios ciudadanos digitales deberán adoptar medidas apropiadas, efectivas y verificables que le permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, deben crear e implementar un Programa Integral de Gestión de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales.*"

k. **Decreto 1413 de 2007**, artículo 2.2.17.6.5, "*Privacidad por diseño y por defecto*":
"Los operadores de servicios ciudadanos digitales deberán atender las buenas prácticas y principios desarrollados en el ámbito internacional en relación con la protección y tratamiento de datos personales que son adicionales a la Accountability, y que se refieren al Privacy by design (PbD) y Privacy Impact Assessment (PIA), cuyo objetivo se dirige a que la protección de la privacidad y de los datos no puede ser asegurada únicamente a través del cumplimiento de la normativa, sino que debe ser un 'modo de operar de las organizaciones, y aplicarlo a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y a las empresas en relación con la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador".

l. **Decreto 1413 de 2017, artículo 2.2.17.5.10**, *"Derechos de los usuarios de los servicios ciudadanos digitales":*
"Registrarse de manera gratuita eligiendo al operador de servicios ciudadanos digitales de su preferencia entre aquellos que estén vinculados por el articulador.

1. Aceptar, actualizar y revocarlas autorizaciones para recibir información, comunicaciones y notificaciones electrónicas desde las entidades públicas a su elección a través de los servicios ciudadanos digitales.

2. Hacer uso responsable de los servicios ciudadanos digitales a los cuáles se registre.

3. Interponer peticiones, quejas, reclamos y solicitudes de información en relación con la prestación a los servicios ciudadanos digitales.

4. Elegir y cambiar libremente el operador de servicios ciudadanos digitales

5. Solicitar en cualquier momento, y a través de cualquiera de los medios de atención al usuario, su retiro de la plataforma de servicios en· cuyo caso podrá descargar su información a un medio de almacenamiento propio.

m. **Decreto 1413 de 2017, artículo 2.2.17.2.1.1** *"Descripción de los servicios ciudadanos digitales, 1.5 servicio de interoperabilidad:*
Cualquier desarrollo en el marco de los servicios ciudadanos digitales especiales deberá hacer uso de o estar soportado en los servicios ciudadanos digitales básicos cuando lo requieran."

n. **Decreto 612 de 2018, artículo 1.** *"Integración de planes institucionales y estratégico. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web."*

o. **Conpes 3854 de 2016,** *objetivo general "Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país".*

Por lo anterior, la ANM debe emprender acciones orientadas a la protección de la información que gestiona, realizando la identificación y tratamiento de riesgos de la información y ciberseguridad de los activos críticos que la soportan, de manera que se establecen y realiza el seguimiento a dichas acciones en el marco del plan de acción y del Sistema Integrado de Gestión.

6. ANTECEDENTES

6.1. Políticas de Seguridad de Información

Por medio de la resolución 421 del 5 de Julio de 2019, firmada por la Presidencia de la ANM, se adoptan las políticas de Seguridad de la Información y Ciberseguridad de cumplimiento por parte de directivos, funcionarios, usuarios y terceros que accedan a la información de la ANM, usen equipos informáticos y de comunicaciones, interactúen con herramientas tecnológicas y/o servicios informáticos y/o ingresen de manera física o lógica a las instalaciones de la ANM. Se puede consultar a través:

http://10.0.100.100/intranet/sites/default/files/documentos/SGSI/ManualdePoliticasdeSeguridaddelaInformacion.pdf

6.2. Levantamiento de Inventarios de Activos de Información

En el año 2016, en el marco del Sistema Integrado de Gestión y el Subsistema de Gestión de Seguridad de la Información, varios procesos de la Entidad realizaron el levantamiento de los activos de información con base en la guía de registro de activos de información. Este insumo permitió en el mes de enero de 2018, dar cumplimiento a lo establecido en la Ley 1712 de 2014, respecto a la generación y publicación de los siguientes productos:

- Registro de activos
- Índice de información clasificada o reservada
- Esquema de publicación

Esta actividad permitió la identificación, clasificación y valoración de criticidad de activos tipo información, software y hardware en los procesos, bajo una metodología documentada y aprobada por la Entidad que permitirá su actualización periódica, la cual es desarrollada por el equipo de seguridad de la información y se apoya la gestión para su aprobación por parte del proceso de gestión documental.

http://10.0.100.100/intranet/sites/default/files/documentos/SGSI/Registro%20de%20Activos/35-SGD-ANM-Guia-RegistroActivosInform.Escaneado.pdf

6.3. Elaboración de Matriz de Riesgos

En el año 2016, teniendo en cuenta las actividades ejecutadas en periodos anteriores, la Oficina de Tecnologías e Información generó la matriz de riesgos de seguridad de la información, conforme a la Metodología de Administración Gestión de Riesgos de la Entidad. El procedimiento se detalla en el siguiente enlace:

http://10.0.100.100/intranet/sites/default/files/documentos/SGSI/InstructivoparaIdentificaci%C3%B3nyValoraciondeRiesgos.pdf

6.4. Plan de Tratamiento de Riesgos

En el marco de la metodología de riesgos establecida por la Oficina Asesora de Planeación de la ANM, en el año 2016 se construyeron los planes de tratamiento para riesgos, dentro del marco legal, sin embargo, es una actividad compleja e integral, que requiere la participación de todos los funcionarios de la ANM, para la aplicación de estos controles.

Dado lo anterior, se hace necesaria la documentación específica que requiere cada una de las etapas para el tratamiento de riesgos, en este caso se retomará la metodología usada actualmente con algunas modificaciones para llevar acabo su implementación.

6.5. Plan de Capacitación y Concienciación

La Oficina de Tecnologías de la Información en el año 2016, estableció y ejecutó un plan de sensibilización de dicha vigencia.

Sin embargo, el plan de capacitación y concienciación con respecto a la Seguridad y Privacidad de la Información y Ciberseguridad, es una de las carencias con respecto al estado actual del SGSI en la ANM.

Dentro de Este contexto se contemplará el desarrollo de un plan de capacitación y concienciación que busque disminuir la brecha actual en los funcionarios de la ANM, frente a las responsabilidades con la Seguridad de la Información tanto digital como física, en donde se plantearán temas diferentes con propuestas en:

- ✓ Conceptos fundamentales en Seguridad y Privacidad de la Información y Ciberseguridad
- ✓ Capacitaciones a los Funcionarios y contratistas
- ✓ Difundir las Políticas del SGSI y el Manual de Seguridad de la Información
- ✓ Conceptos en el marco Legal y Regulatorio para la gestión del SGSI
- ✓ Conceptos de Gobierno de Protección de Datos Personales
- ✓ Amenazas Cibernéticas (Phishing, Malware, Ramsonware, etc.)

6.6. Gestión de Incidentes de Seguridad de la Información

En la ANM se encuentra afianzado el manejo de gestión de incidentes desde la Oficina de Tecnología e Información de forma general.

Es así que se fortalecerá la Gestión de Incidentes de Seguridad y Privacidad de la Información y Ciberseguridad, con el fin de ser más predictivos frente a las amenazas del ciberespacio.

6.7. Registro de Activos de Información

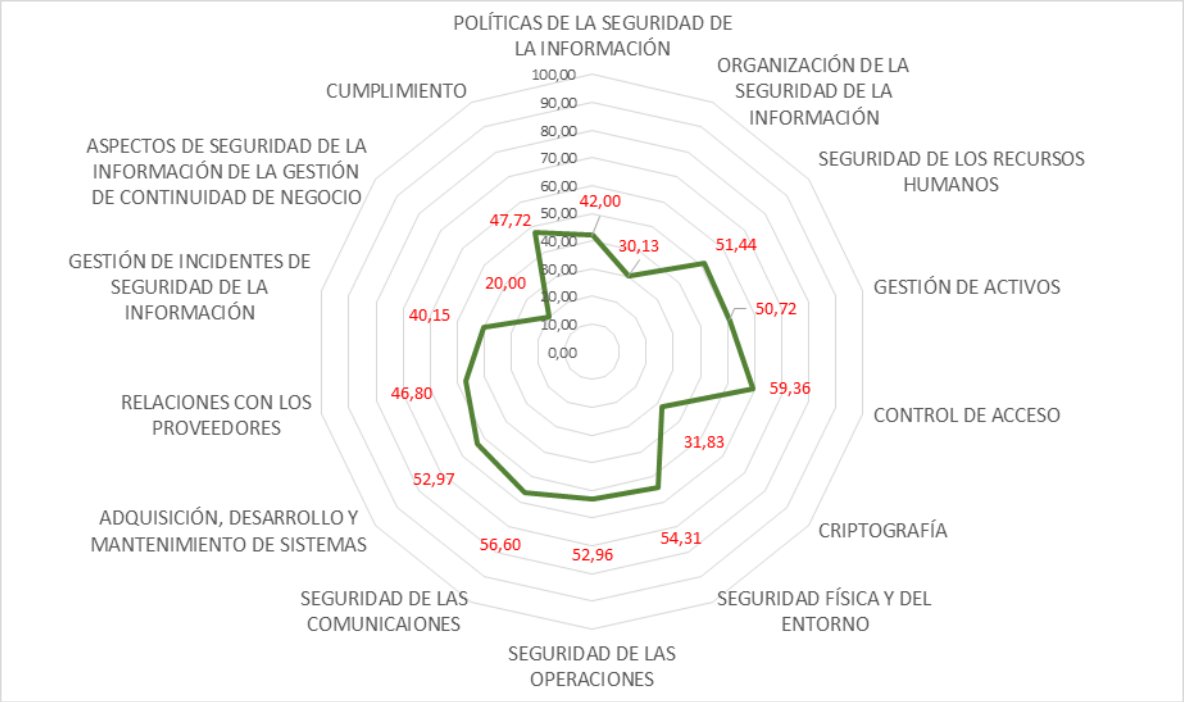
La Gestión de Activos de Información, ha tenido un trabajo muy importante, sin embargo, al revisar la matriz de los activos de información con el grupo de Servicios Administrativos, se observa que no están contemplados los activos intangibles como el software, por lo que son parte importante identificarlos dentro de la matriz definida para este dominio.

Igualmente, es parte fundamental la identificación de los activos críticos de la ANM para su respectivo tratamiento y protección frente a las amenazas del ciberespacio.

6.8. Modelo de Seguridad y Privacidad de la Información

La Oficina de Tecnología de la Información en el año 2019, obtuvo medición de la evaluación de la implementación del Modelo de Seguridad y Privacidad de la Información del MinTIC - MSPI, como se aprecia a continuación:

BRECHA ANEXO A ISO 27001:2013



En el mes de diciembre de 2019 se obtuvo un promedio total de 45.5% en la evaluación de los controles, lo cual permitió evidenciar que la gestión de la OTI en seguridad de la información está en un término aceptable.

El dominio que presenta menos avance es el de aspectos de seguridad de la información de la gestión de la continuidad. Sobre este dominio se esperan importantes avances durante el año 2020.

7. PROGRAMA DE IMPLEMENTACIÓN DEL SGSI Y CIBERSEGURIDAD

AGENCIA NACIONAL DE MINERÍA	PLAN DE TRABAJO ANUAL	CRONOGRAMA 2020
	COD - SGSI - CS - SGCN / VERSIÓN: 01	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMAIÓN - CIBERSEGURIDAD Y CONTINUIDAD DE NEGOCIO

AÑO		2020																							
PERIODO		I						II						III						IV					
ACTIVIDAD		ENE		FEB		MAR		ABR		MAY		JUN		JUL		AGO		SEP		OCT		NOV		DIC	
		P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E
No	1. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD																								
1.1	Elaborar Políticas de Seguridad de la Información y Ciberseguridad	1		1																					
1.2	Elaborar Políticas de Continuidad de Negocio			1		1																			
1.3	Identificación de Riesgos de Seguridad de la Información y Ciberseguridad			1		1		1		1															
1.4	Identificación de Riesgos de Continuidad de Negocio			1		1		1		1															
1.5	Planificación Documental SGSI-CS			1		1		1		1															
1.6	Planificación Documental SGCN					1		1		1															
1.7	Requisitos Legales (Matriz de Requisitos Legales)			1		1																			
1.8	Comité SGSI-CS-SGCN	1		1		1		1		1		1		1		1		1		1		1		1	
	2. POLÍTICAS																								
2.1	Metodología de Gestión y Tratmiento de Riesgos de Seguridsad	1	1	1	A																				
2.2	Política Uso Aceptable de Activos	1	1	1	p																				
2.3	Política de Escritorio y Pantalla Limpia	1	1	1	r																				
2.4	Política Transferencia de Información	1	1	1	o																				
2.5	Política para Dispositivos Móviles y Teletrabajo	1	1	1	b																				
2.6	Política de Uso e Instalación de Software	1	1	1	a																				
2.7	Política de Controles Criptográficos	1	1	1	c																				
2.8	Política de Seguridad de las Comunicaciones	1	1	1	i																				
2.9	Política de Privacidad y Protección de Datos Personales	1	1	1	o																				
2.10	Políticas de Proveedores y Contratistas	1	1	1	n																				
2.11	Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información	1	1	1																					
	3. PROCEDIMIENTOS																								
3.1	Procedimiento de Control de Acceso	1																							
3.2	Procedimiento de Clasificación de Información	1	1																						
3.3	Procedimiento Seguridad Física y del Entorno	1																							
3.4	Procedimiento de Copias de Respaldo			1																					
3.5	Procedimiento de Transferencia de Información	1	1	1																					
3.6	Procedimiento de Protección Contra Códigos Maliciosos	1		1																					
3.7	Procedimiento de Gestión de Vulnerabilidades Técnicas	1	1																						

4. IMPLEMENTACIONES EN PROCESOS Y SUBPROCESOS																											
4.1	Ejercicios de Clasificación de Información			1		1		1		1		1		1		1		1		1		1		1		1	
4.2	Ejercicios de Identificación de Riesgos			1		1		1		1		1		1		1		1		1		1		1		1	
4.3	Ejercicios de Estrategias de Continuidad							1		1																	
4.4	Ejercicios Análisis de Impacto al Negocio			1		1		1						1		1		1		1		1		1			
4.5	Ejercicios de Planes de Contingencia y Continuidad					1														1							
4.6	Ejercicios de Implementación de Planes de Tratamiento					1		1		1		1		1		1		1		1		1		1		1	
5. INDICADORES - AUDITORÍA INTERNA - REVISIÓN POR LA ALTA DIRECCIÓN																											
5.1	Indicador de Sensibilización			1				1				1				1				1				1			
5.2	Indicador de Gestión de Riesgos			1				1				1				1				1				1			
5.3	Indicador de Gestión de Vulnerabilidades			1				1				1				1				1				1			
5.4	Indicador de Gestión de Proveedores			1				1				1				1				1				1			
5.5	Indicador de Gestión de Incidentes			1				1				1				1				1				1			
6. PROCESOS (Nivel de Madurez)																											
6.1	Proceso Gestión de la Configuración					1	R	N	M																		
6.2	Proceso Gestión de Cambios			1			e	i	a																		
6.3	Proceso Gestión de la Disponibilidad					1	v	v	d																		
6.4	Proceso Gestión de la Capacidad					1	i	e	u																		
6.5	Proceso Gestión de Incidentes			1			s	l	r																		
6.6	Proceso Gestión de Vulnerabilidades			1			i		e																		
6.7	Proceso Gestión de Proveedores					1	ó		z																		
6.8	Proceso Gestión Acuerdos de Niveles de Servicio - SGSI-CS					1	n																				
6.9	Proceso Mesa de Ayuda SGSI-CS					1																					
No. ACTIVIDADES PROGRAMADAS / CUMPLIDAS		19	14	32	0	18	0	15	0	9	0	9	0	5	0	10	0	5	0	11	0	5	0	10	0		
PORCENTAJE DE CUMPLIMIENTO		74%		0%		0%		0%		0%		0%		0%		0%		0%		0%		0%		0%			

7.1. Alineación del Plan con Gobierno Digital

En el marco del contexto del plan de Seguridad y Privacidad de la Información y Ciberseguridad, se establecen las iniciativas encaminadas a responder bajo los lineamientos del marco de Gobierno Digital.

8. CONCLUSIONES

a) Es necesario dar continuidad al trabajo que se viene realizando frente a la Seguridad y Privacidad de la información y Ciberseguridad de la ANM, alcanzado hitos importantes para fortalecer la protección de la información frente a las amenazas del ciberespacio.

b) La parte de mayor prioridad es la de involucrar a los dueños de los procesos, quienes deben tomar conciencia en cuanto a la debida diligencia frente a la gestión de riesgos y de los controles requeridos para proteger su información.

c) La capacitación y concienciación de los funcionarios y dueños de los procesos es uno de los frentes que se debe trabajar con prioridad. Sin la motivación y participación activa de todos los involucrados, no se logrará los objetivos en la implementación del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

d) Se debe dejar en contexto que la Seguridad y Privacidad de la información y la Ciberseguridad, es responsabilidad de toda la Entidad.

e) La metodología de Gestión de Riesgos de Seguridad y Privacidad de la Información y Ciberseguridad, se ajustará tomando como referencia el procedimiento de gestión de riesgos que se tiene actualmente publicado en Planeación.

f) Se debe fortalecer la gestión de Incidentes de Seguridad de la Información, en donde se cree un equipo de Respuesta a Incidentes de Seguridad en la ANM, y participe cada especialista de TI involucrado.

g) El Plan de Continuidad del Negocio, debe estar basado en las consideraciones dispuestas desde un análisis de impacto al negocio y de riesgos de disrupción, con el fin de facilitar las estrategias de contención y recuperación para mejorar la resiliencia cibernética de la ANM.

Anexo 1 Control de Cambios

Versión	Fecha del cambio	Descripción de la modificación
1	30 de enero de 2020	Creación.