PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

MINAMBIENTE

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

somos MADS
Ministerio de Ambiente y Desarrollo Sostenible

PROCESO:

Gestión Estratégica de Tecnologías de la Información.

- TIC

VERSIÓN: 3

30/06/2018

Oficina de Tecnologías de la Información y la Comunicación - TIC

Contenido

PRESENTACION

El Ministerio de Ambiente y Desarrollo Sostenible tiene como política general de su Sistema de Gestión de Seguridad de la Información –SGSI-:

> " *En cumplimiento de su objeto misional, la normativa vigente y con criterios técnicos, el Ministerio de Ambiente y Desarrollo Sostenible, como rector del Sistema Nacional Ambiental, se compromete a garantizar la satisfacción de las partes interesadas, hacer un uso eficiente de sus recursos y preservar la confidencialidad, integridad y disponibilidad de la información, bajo un enfoque de prevención de riesgos, mejora continua y autocontrol en los procesos y en la prestación de los servicios, con el apoyo de un equipo humano competente y comprometido*."

De igual manera, tiene como objetivos específicos para el cumplimiento de la Política y del objetivo estratégico del SGSI:

1. *Sensibilizar al personal del Ministerio de Ambiente y Desarrollo Sostenible en seguridad de la información.*

2. *Gestionar los incidentes de seguridad de la información que atenten contra la confidencialidad, integridad y disponibilidad de los activos de información del Ministerio de Ambiente y Desarrollo Sostenible.*

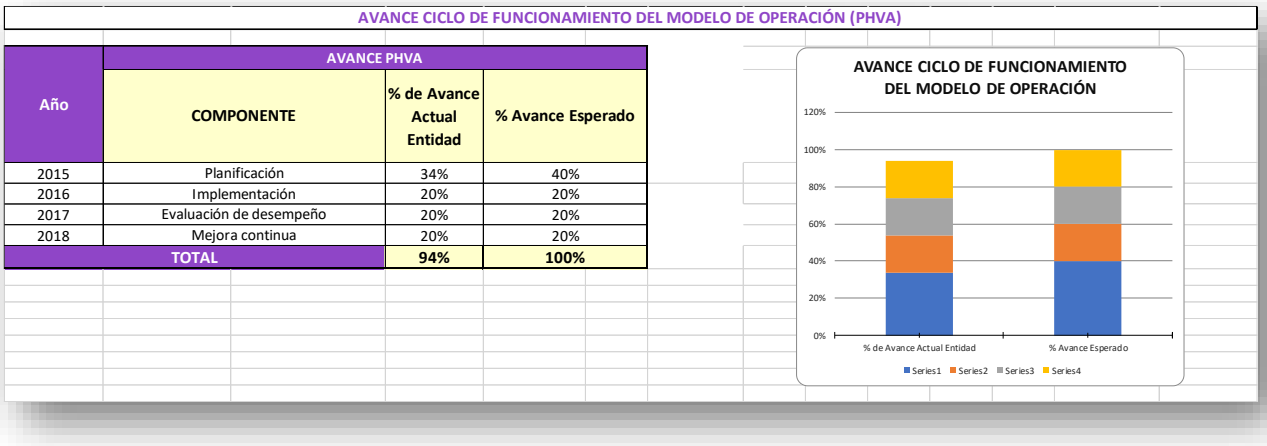
En ese orden de ideas, el presente documento recoge las actividades formuladas para la vigencia 2018 con el fin de alcanzar estos objetivos y mantener la mejora continua de su SGSI. Para ello se incluyó un capítulo de diagnóstico, que evidencia la situación de partida con corte a diciembre de 2017 y otro con las acciones formuladas para la vigencia 2018 y con el presupuesto asignado, para finalizar con un capitulo asociado al seguimiento del plan.

1. DIAGNÓSTICO

1.1 Modelo de Seguridad y Privacidad de la Información –MSPI-

De acuerdo con el instrumento de seguimiento del MSPI del Ministerio de las TIC, con corte a diciembre de 2017, el Ministerio tenía un avance del 94% en el ciclo de funcionamiento del modelo de operaciones (PHVA) y un 86% de evaluación de efectividad de sus controles.

Figura 1: Informe MSPI ciclo PHVA 2017

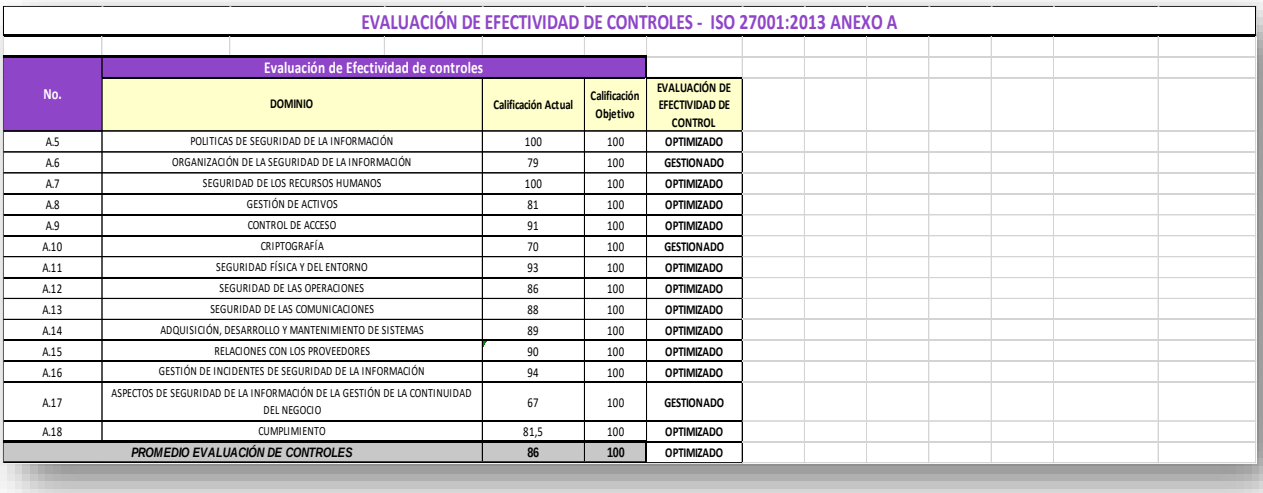


AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2015	Planificación	34%	40%
2016	Implementación	20%	20%
2017	Evaluación de desempeño	20%	20%
2018	Mejora continua	20%	20%
TOTAL		94%	100%

Fuente: Matriz de seguimiento MSPI – MinTIC

Figura 2: Informe MSPI Controles 2017



EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	79	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	81	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	91	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	70	100	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	93	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	86	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	88	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	89	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	90	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	94	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	67	100	GESTIONADO
A.18	CUMPLIMIENTO	81,5	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		86	100	OPTIMIZADO

Fuente: Matriz de seguimiento MSPI - MinTIC

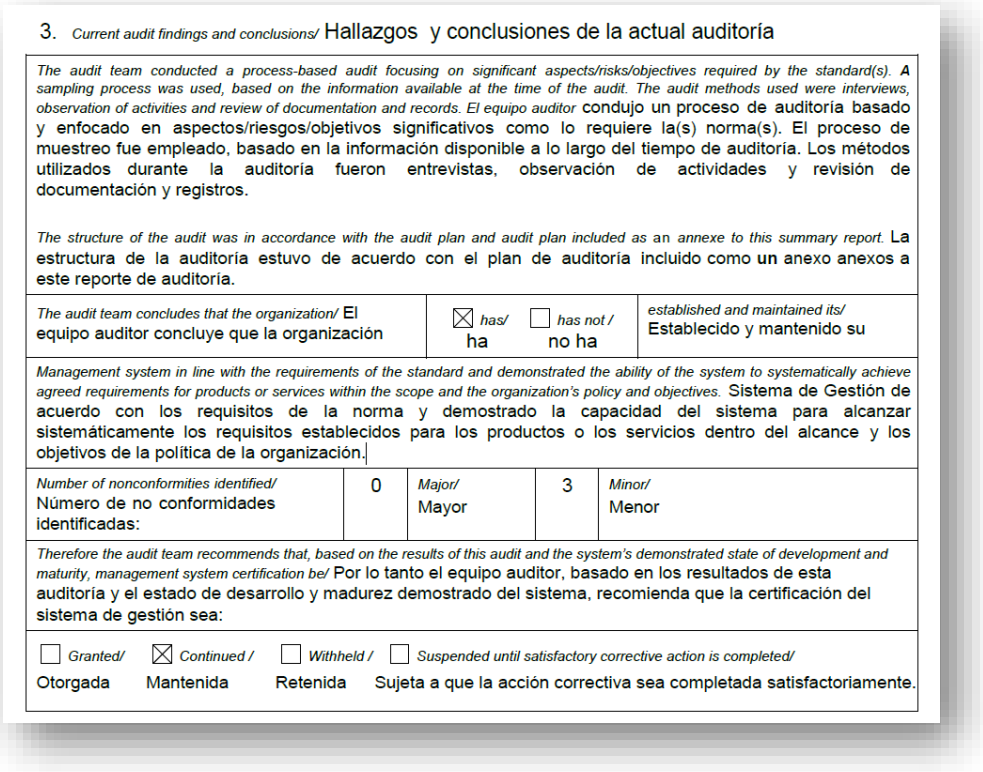
1.2 Modelo Integrado de Planeación y Gestión II –MIPG- y Formulario Único Reporte de Avances de la Gestión -FURAG-

El nuevo Modelo de planeación y Gestión adoptado mediante Decreto 1499 de 2017, establece en su Manual Operativo como tercera Dimensión: "Gestión con Valores para el Resultado" la Política Gobierno Digital: TIC para la gestión, en la cual se incluye el ámbito de "Seguridad de la información" señala que "las entidades deben seguir cada uno de los componentes del Marco de Seguridad y Privacidad de la Información, así como las …actividades para su correcta gestión". De igual manera, esta dimensión establece una "Política de Seguridad Digital" soportada en el Documento CONPES 3854 de 2016, que incorpora la Política Nacional de Seguridad Digital coordinada desde la Presidencia de la República y el Ministerio de las TIC, para orientar y dar los lineamientos respectivos a las entidades.

1.3 Auditoría de seguimiento al SGSI 2017

La Auditoría de Seguimiento realizada entre el 16 y el 18 de enero de 2017, concluyó que:

> "*la organización ha establecido y mantenido su Sistema de Gestión de acuerdo con los requisitos de la norma y demostrado la capacidad del sistema para alcanzar sistemáticamente los requisitos establecidos para los productos o los servicios dentro del alcance y los objetivos de la política de la organización*."



3. *Current audit findings and conclusions/* Hallazgos y conclusiones de la actual auditoría

The audit team conducted a process-based audit focusing on significant aspects/risks/objectives required by the standard(s). A sampling process was used, based on the information available at the time of the audit. The audit methods used were interviews, observation of activities and review of documentation and records. El equipo auditor condujo un proceso de auditoría basado y enfocado en aspectos/riesgos/objetivos significativos como lo requiere la(s) norma(s). El proceso de muestreo fue empleado, basado en la información disponible a lo largo del tiempo de auditoría. Los métodos utilizados durante la auditoría fueron entrevistas, observación de actividades y revisión de documentación y registros.

The structure of the audit was in accordance with the audit plan and audit plan included as an annexe to this summary report. La estructura de la auditoría estuvo de acuerdo con el plan de auditoría incluido como un anexo anexos a este reporte de auditoría.

The audit team concludes that the organization/ El equipo auditor concluye que la organización	☒ *has/* ha ☐ *has not /* no ha	*established and maintained its/* Establecido y mantenido su

Management system in line with the requirements of the standard and demonstrated the ability of the system to systematically achieve agreed requirements for products or services within the scope and the organization's policy and objectives. Sistema de Gestión de acuerdo con los requisitos de la norma y demostrado la capacidad del sistema para alcanzar sistemáticamente los requisitos establecidos para los productos o los servicios dentro del alcance y los objetivos de la política de la organización.

Number of nonconformities identified/ Número de no conformidades identificadas:	0	*Major/* Mayor	3	*Minor/* Menor

Therefore the audit team recommends that, based on the results of this audit and the system's demonstrated state of development and maturity, management system certification be/ Por lo tanto el equipo auditor, basado en los resultados de esta auditoría y el estado de desarrollo y madurez demostrado del sistema, recomienda que la certificación del sistema de gestión sea:

☐ *Granted/* Otorgada	☒ *Continued /* Mantenida	☐ *Withheld /* Retenida	☐ *Suspended until satisfactory corrective action is completed/* Sujeta a que la acción correctiva sea completada satisfactoriamente.

Fuente: Informe de auditoría de seguimiento SGS - 2017

De igual manera el Ministerio logró reducir el número de no conformidades al pasar de cuatro (4) reportadas en la auditoría 2016, a tres (3) no conformidades menores en 2017.

Por todo lo anterior, el equipo auditor, basado en los resultados de esta auditoría y el estado de desarrollo y madurez demostrado del sistema, recomendó que la certificación del sistema de gestión sea mantenida, sujeta a que la acción correctiva sea completada satisfactoriamente.

A continuación, se detallan las tres no conformidades menores y sus respectivas acciones de mejora:

Tabla 1: No conformidades menores auditoria se seguimiento

No conformidad	Acción correctiva
1. *No se evidenció tratamiento adecuado a la observación de auditoria externa de segundo seguimiento que indicaba "Área Gestión de servicios de información y soporte TIC: Aumentar la seguridad en la puerta de salida de emergencia piso -1 (Apertura solo desde*	Se realizó la gestión necesaria para el ajuste del brazo instalado en la puerta del Área Gestión de servicios de información y soporte TIC.

No conformidad	Acción correctiva
oficina, brazo de cierre mecánico)", se observó que solo se instaló un brazo el cual no realiza su cierre eficaz, la puerta siempre permanece abierta y se puede abrir desde el exterior de la oficina. incumpliendo control seguridad información A11.1.3 Seguridad de oficinas, salones e instalaciones. Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones.	
2. *Debilidad en la continuidad del negocio, no se evidencia tiempos de recuperación conforme, evidenciado para el servidores web, directorio activo, DB, correo (tiempo global); no se ha determinado la estratégica de recuperación para cada servidor (aplicaciones) y en revisión de acción correctiva auditoria interna No. 7 establece temas de "actualizar el plan de continuidad, planeación de pruebas, gestión de riesgos" sin detalle de los ítems para lograr el objetivo de asegurar la continuidad del negocio, incumpliendo A17.1.2 Implementación de la continuidad de la seguridad de la información. La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.*	Se adelantó una contratación de un profesional especializado para la implementación de las buenas prácticas de la norma ISO 22301 en el Ministerio. Contrato No. 476 de 2017.
3. *Debilidad en el control de registros, no se evidenció memorando de "requerimiento de especio físico para almacenamiento de archivos en recurso hídrico; no se dispone de registro diligenciado F-E-SIG-04 y no se evidenció control adecuado de almacenamiento de archivos en gestión (almacenamiento – espacio) incumpliendo 7.5.3 La información documentada se debe controlar para asegurar que: a. Esté disponible y adecuado para su uso, cuando y donde se requiere. Para controlar la información se debe tratar su almacenamiento y preservación.*	1. La solicitud se generó nuevamente en el nuevo sistema para que quede la trazabilidad de la misma. 2. La solicitud se realizó al grupo de servicios administrativos, quien es el responsable de la administración del espacio físico de la entidad. 3. El formato F-E-SIG-04 se encuentra en blanco por que únicamente define los parámetros para el Listado Maestro de Documentos que se exporta desde la herramienta MadsiGestion

Fuente: Informe de auditoría de seguimiento SGS - 2017

A continuación, se detallan las observaciones generales y oportunidades para mejora (16), identificadas en la cita auditoria y las acciones de mejora adoptadas por el Ministerio:

Tabla 2: Observaciones generales y oportunidades para mejora.

Observaciones generales y oportunidades para mejora	Acción de mejora
1. *Soporte técnico TIC: En la casilla gestión de cambios de los documentos, detallar el motivo o ítems del cambio en el documento.*	MADSSIG realiza mejora en la casilla cuando se realizan cambios sobre los documentos. La solicitud de cambios se realiza por medio del sistema web.
2. *Incorporar en la gestión de cambios de los documentos que sea de forma automática (Vigencia, aprobación, versión).*	
3. *Riesgos: en la metodología de riesgos cuando el riesgo este en el criterio "Medio - Bajo", no es obligatorio determinar plan de tratamiento de riesgos; si la organización determinó realizar plan de tratamiento debería incluir actividades diferentes a las implementadas actualmente.*	Se revisó y ajustó la matriz de riesgos.
4. *Riesgos: En la metodología de riesgos incluir el detalle sobre las actividades a ejecutar en el plan de tratamiento de riesgos. En los planes de tratamiento ampliar el detalle de las actividades y recursos requeridos para asegurar el objetivo propuesto. Ejemplo DMZ plan "adquisición infraestructura necesaria Dic 2018".*	Se realizó la creación de un plan de tratamiento solo para seguridad de la información independiente que compile lo incluido institucionalmente.
5. *Soporte técnico TIC: Fortalecer y determinar una periodicidad de la proyección de capacidad de servidores.*	Se realizó revisión y actualización de la documentación relacionada.
6. *Soporte técnico TIC: Fortalecer las actividades del proceso con la implementación de buenas prácticas de sistemas de gestión de servicios TI (ISO 20000).*	Se adelantó una contratación de un profesional especializado para la implementación de la norma ISO 20000-1 en el Ministerio, avanzando en un 77% en su implementación a diciembre de 2017. Contrato.
7. *Soporte técnico TIC: Incorporar un seguimiento bimensual de usuarios vigentes en Aranda.*	Se plantea una revisión periódica de los usuarios para realizar depuración.
8. *Almacén: Reducir el tiempo de asignación de activos cuando hay cambio de cargo.*	Se realizó una revisión completa por parte de la coordinadora actual para mejorar los tiempos.
9. *Adm. Talento Humano En los cursos de formación incluir en los requisitos de contratación, que la entidad que dicte la formación genere un soporte consolidado de los participantes.*	Se incluye en los requisitos de contratación, que la entidad que dicte la formación genere un soporte consolidado de los participantes. Cuando sea legalmente posible

Observaciones generales y oportunidades para mejora	Acción de mejora
10. *Adm. Talento Humano En la carta "Entrenamiento en el puesto de trabajo" incluir una nota que se tenga en cuenta lo establecido en el Manual de funciones sección "conocimientos básicos esenciales" para tener en cuenta en el plan de capacitación.*	En la carta "Entrenamiento en el puesto de trabajo" se incluye una nota para tener en cuenta lo establecido en el Manual de funciones sección "conocimientos básicos esenciales" para tener en cuenta en el plan de capacitación.
11. *Instrumentación ambiental - Negocios verdes: Aumentar los controles de ubicación de la información (se observa desorden de cajas).*	Se realizó orden de las cajas y depuración del archivo.
12. *Gestión documental: Agilizar el etiquetado de ubicación "Módulos – estantes" con el fin de facilitar su ubicación y control.*	Se asigna personal contratistas para tal tarea.
13. *Gestión documental: Generar contingencia de llaves de acceso a las áreas de depósito 1 – 2 y 3.*	Se realizó la generación de copias de llaves como contingencia.
14. *Gestión documental: Agilizar la implementación de tablas de retención - valoración documental.*	Se estableció el contacto con el archivo general de la nación
15. *Gestión documental: Fortalecer los controles de seguridad entorno (temperatura – humedad) en especial rollos microfilmación.*	Se fortaleció controles ambientales, salvaguardar rollos de microfilmación.
16. *Contratación: En los casos en donde se determine no habilitación por temas técnicos incorporar un control de seguridad de información, en donde se de claridad de la fecha de entrega del soporte faltante, tipo de registro y responsable de validar los soportes.*	Observación no aceptada. En casos esporádicos se generan gran cantidad de carpetas de un contrato.

Fuente: Informe de auditoría de seguimiento SGS - 2017

1.4 Plan de tratamiento de riesgos de seguridad y privacidad de información 2017

Dado que en el Ministerio existe un sistema integrado de gestión y el sistema de gestión de seguridad de la información (SGSI) es un sub-sistema de este, el Plan de tratamiento de riesgos de seguridad y privacidad de información se encuentra incorporado en el Plan tratamiento de riesgos del sistema integrado.

A continuación, se relaciona el plan de manejo de los riesgos de seguridad y privacidad de información identificados a diciembre de 2017 de los procesos de Gestión de información y comunicaciones (para la vigencia 2018 cambia a Gestión Estratégica de Tecnologías de la Información.) y el de Gestión de Servicios de Información y Soporte Tecnológico.

Tabla 3: Plan de manejo del riesgo proceso de Gestión de información y comunicaciones (2017)

OPCIONES DE MANEJO	PLAN DE MANEJO DEL RIESGO			
	ACCIONES A TOMAR	RESPONSABLE	CRONOGRAMA	INDICADOR PARA EVALUAR ACCIONES IMPLEMENTADAS
Evitar el Riesgo	1 .Actualizar y/o modificar Procedimientos. (Incluir herramienta)	Jefe Oficina TIC	31/05/2017	Procedimiento publicado
Reducir el Riesgo	1. Generar el Instrumento PETIC	Jefe Oficina TIC	30/06/2017	Documento elaborado
	2. Implementación del Instrumento PETIC en todas sus fases	Jefe Oficina TIC	31/12/2019	Implementación al 100%
Reducir el Riesgo	1. Generar herramientas de seguimiento y control al cumplimiento de política de seguridad en la información	Jefe Oficina	31/12/2017	Herramienta de seguimiento y control implementada

Fuente: Oficina TIC

Tabla 4: Plan de manejo del riesgo proceso de Gestión de Servicios de Información y Soporte Tecnológico (2017)

OPCIONES DE MANEJO	PLAN DE MANEJO DEL RIESGO			
	ACCIONES A TOMAR	RESPONSABLE	CRONOGRAMA	INDICADOR PARA EVALUAR ACCIONES IMPLEMENTADAS
Mitigar Riesgo	Adquisición de herramienta tipo SIEM para la prevención de incidentes informáticos sobre la infraestructura de la entidad	Coordinación grupo de sistemas	Diciembre de 2017	Herramienta adquirida e implementada
Compartir Riesgo	Implementación y mejora de acuerdos y planes de continuidad. Solicitud de presupuesto para implementación. Acompañamiento especializado para mantenimiento y mejora.	Coordinación grupo de sistemas - Oficina TIC	Diciembre de 2018	planeación e Informe de pruebas realizadas
Mitigar Riesgo	Planeación y adquisición de infraestrucutra necesaria y cambios en la topología de red necesaria	Coordinación grupo de sistemas	Diciembre de 2018	Presupuesto para adquisición de infraestructura
Mitigar Riesgo	Implementación y difusión herramienta Kaspersky, Eliminación Veracrypt, monitoreada por siem.	Coordinación grupo de sistemas	Diciembre de 2017	Herramienta adquirida e implementada
Mitigar Riesgo	Mejorar Moniterio, DLP, implementación herramientas	Coordinación grupo de sistemas	Diciembre de 2018	Presupuesto aprobado para adquirir herramientas

Fuente: Grupo de Sistemas

2. ACTIVIDADES 2018

Las actividades del plan se enfocan en atender los objetivos del SGSI indicados en la introducción a partir del diagnóstico que se ilustró en el capítulo 1, como se detalla a continuación.

2.1 Objetivo: Sensibilizar al personal del Ministerio en seguridad de la información

A continuación, se incluye el cronograma de actividades asociadas a este objetivo y que son lideradas por la Oficina de las TIC y la Oficina Asesora del Planeación del Ministerio.

Tabla 5: Cronograma de trabajo Oficina TIC – Oficina Asesora de Planeación.

Name	Begin date	End date
Enero	01/01/18	31/01/18
•Cronograma de actividades para la ejecución del contrato.	01/01/18	31/01/18
Febrero	01/02/18	28/02/18
•Documento de coordinación del lanzamiento del curso de Seguridad de la Información ISO 27001, generado por la Oficina TIC.	01/02/18	28/02/18
•Reporte de publicación de los documentos del proceso de gestión estratégica en el aplicativo MADSIG	01/02/18	28/02/18
•Planificación estrategia de sensibilización de seguridad de la información	01/02/18	28/02/18
Marzo	01/03/18	30/03/18
•Documento que contenga el seguimiento al desarrollo del curso de Seguridad de la Información ISO 27001, generado por la Oficina TIC.	01/03/18	30/03/18
•Implementación de la estrategia de sensibilización de seguridad de la información	01/03/18	30/03/18
Abril	02/04/18	30/04/18
•Documento de cierre del curso de Seguridad de la Información ISO 27001, generado por la Oficina TIC.	02/04/18	30/04/18
Mayo	01/05/18	31/05/18
•Soportes de las actividades encaminadas a la preparación auditoria interna al sistema de Seguridad de la información	01/05/18	31/05/18
Junio	01/06/18	29/06/18
•Informe de las actividades desarrolladas durante la atención de la auditoria interna al sistema de Seguridad de la información	01/06/18	29/06/18

Tabla 5: Cronograma de trabajo Oficina TIC – Oficina Asesora de Planeación. (Continuación)

Name	Begin date	End date
•Reporte de los documentos actualizados del SIG como estrategia de actualización de los activos de información.	01/06/18	29/06/18
Julio	02/07/18	31/07/18
•Informe de las actividades desarrolladas para la formulación y seguimiento de los planes de mejoramiento en atención a los resultados de la auditoría interna del Sistema de seguridad de la Información	02/07/18	31/07/18
Agosto	01/08/18	31/08/18
•Soportes de las actividades encaminadas a la preparación auditoria externa o autoevaluación al sistema de Seguridad de la información	01/08/18	31/08/18
Septiembre	03/09/18	28/09/18
•Informe de las actividades desarrolladas durante la atención de la auditoria externa o autoevaluación al sistema de Seguridad de la información	03/09/18	28/09/18
Octubre	01/10/18	31/10/18
•Informe de las actividades desarrolladas para la formulación y seguimiento de los planes de mejoramiento en atención a los resultados de la auditoría externa o autoevaluación del Sistema de seguridad de la Información	01/10/18	31/10/18
Noviembre	01/11/18	30/11/18
•activos de información actualizados	01/11/18	30/11/18
•Bases de datos personales actualizadas	01/11/18	30/11/18
Diciembre	03/12/18	31/12/18
•Mapa de riesgos institucional en su componente de seguridad de la información revisado y actualizado	03/12/18	31/12/18

Plan de Sensibilización para la Seguridad de la Información:

Como se puede apreciar en la Tabla 5, desde el mes de febrero se lanzará el curso virtual de seguridad de la información, el cual es el eje central de la estrategia de sensibilización de seguridad de la información.

Una vez termine el curso, se adelantarán las gestiones para que sea incorporado como parte de los cursos de inducción y re-inducción del Ministerio, lo cual hará permanente esta sensibilización.

2.2 Objetivo: Gestionar los incidentes de seguridad de la información

A continuación, se incluye el cronograma de actividades asociadas a este objetivo y que son lideradas por el Grupo de sistemas del Ministerio, el cual depende la Subdirección Administrativa y Financiera de la Secretaría General.

Tabla 6: Cronograma de trabajo Grupo de sistemas

PLAN DE TRABAJO SGSI GRUPO DE SISTEMAS 2018													
Id	Actividades	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
1	Atención a los incidentes de seguridad de la información que se presenten y reporten en la entidad por medio de la mesa de ayuda o por correo electrónico												
2	Acompañamiento en charlas de sensibilización y/o trasferencia de conocimiento respecto al SGSI al interior de la entidad para los colaboradores del Ministerio, siempre que sea requerido por el supervisor del contrato.												
3	Proponer nuevas actividades a desarrollar para la mejora del Sistema de Gestión de Seguridad de la Información (SGSI) desde el grupo de sistemas												
4	Actividades de acompañamiento para la gestión del plan de continuidad de negocio dentro de la entidad, incluyendo el análisis de impacto al negocio (BIA), pruebas tecnológicas.												
5	Acompañamiento técnico a la implementación y puesta en funcionamiento de los procesos y actividades que permitan garantizar la mejora continua del Sistema de Gestión de Seguridad de la Información.												
6	Análisis de pruebas de vulnerabilidades a la infraestructura cuando sean requeridas por la entidad.												
7	Realizar acompañamiento para dar cumplimiento a los objetivos internos relacionados con la seguridad informática, en concordancia con las políticas y procedimientos establecidos en el Ministerio.												
8	Realizar acompañamiento, así como participar en el establecimiento de mejoras para la actualización de los procedimientos, procesos, planes y demás que correspondan de conformidad al Sistema de seguridad de la información correspondiente al grupo de sistemas.												
9	Seguimiento a los controles de seguridad implementados para evaluar su eficacia.												
10	Realizar las actividades correspondientes a la actualización sobre los inventarios de los activos de la información del grupo de sistemas, de conformidad con los lineamientos internos y externos												
11	Actualización continua de la gestión de riesgos en seguridad de la información del grupo de sistemas, así como al plan de tratamiento de riesgos												
12	Apoyar al grupo de sistemas en todas las actividades y procesos de auditorias internas y externas que relacionen aspectos del Sistema de gestión de Seguridad de la Información (SGSI) que sean llevadas a cabo a la entidad.												
13	Realizar los planes de mejoramiento respecto a los resultados de las auditorias de la obligación anterior, garantizando la ejecución de las acciones correctivas y preventivas a que hubiere lugar de acuerdo al SGSI, mediante su respectivo seguimiento.												
14	Revisión y apoyo en la actualización de documentación del SGSI en lo que respecto al grupo de sistemas												

Fuente: Grupo de sistemas

2.3 Acciones correctivas auditoría 2017 a atender en la vigencia 2018

- Se relacionan las acciones pendientes de la Tabla 1, que no se pudieron atender en la vigencia 2017.

2.4 Acciones de mejora auditoría 2017 a atender en la vigencia 2018

- Se relacionan las acciones pendientes de la Tabla 2, que no se pudieron atender en la vigencia 2017.

2.5 Plan de tratamiento de riesgos de seguridad y privacidad de información 2018

Se anexa el Plan de manejo del riesgo del proceso de Gestión Estratégica de Tecnologías de la Información (2018) y el del Proceso de Gestión de Servicios de Información y Soporte Tecnológico (2018).

Tabla 7: Plan de manejo del riesgo proceso de Gestión Estratégica de Tecnologías de la Información (2018)

OPCIONES DE MANEJO	PLAN DE MANEJO DEL RIESGO			
	ACCIONES A TOMAR	RESPONSABLE	CRONOGRAMA	INDICADOR PARA LA EVALUACIÓN DE ACCIONES IMPLEMENTADAS
Asumir el Riesgo	Solicitar la designación de enlaces por dependencia, para garantizar el cumplimiento de cada subcriterio Realizar seguimiento semestral al cumplimiento de los subcriterios a través de los enlaces Socializar ante el Comité Institucional de Gestión y desempeño, y el comité de Gerencia el nuevo procedimiento de la Estrategia de TI (GEL-Digital)	Jefe TIC Todos las dependencias	15 de abril de 2018 31 de diciembre de 2018 Primer comité Institucional de Gestión y desempeño 2018 y comité de Gerencia según programación	Memorandos solicitando la designación de enlaces Formato Diagóstico de Gobierno en línea F-E-GET-03 actualizado semestralmente Actas de reunión tanto de Comité Institucional como de Gerencia con evidencia de la socialización
Asumir el riesgo	Elaboración del instrumento para el seguimiento a la implementación del PETI Realizar la revisión del PETI institucional anualmente, con cada proceso a través de los enlaces de la oficina TIC	Jefe TIC	31 de diciembre de 2018	Instrumento de seguimiento adoptado PETI revisado
Reducir el riesgo	Documentar el procedimiento para la actualización del protocolo de gestión de información sectorial y los lineamientos de política de TI	Jefe TIC	31 de diciembre de 2018	Procedimiento adoptado

Fuente: Oficina TIC

Tabla 8: Plan de manejo del riesgo proceso de Gestión de Servicios de Información y Soporte Tecnológico (2018).

OPCIONES DE MANEJO	PLAN DE MANEJO DEL RIESGO			
	ACCIONES A TOMAR	RESPONSABLE	CRONOGRAMA	INDICADOR PARA EVALUAR ACCIONES IMPLEMENTADAS
Mitigar Riesgo	Definir nuevo esquema de copias de seguridad a nivel de sistemas de información y servidores.	Coordinación grupo de sistemas	Agosto de 2018	Documentación actualizada
Compartir Riesgo	Implementación y mejora de acuerdos y planes de recuperación. Solicitud de presupuesto para implementación. Acompañamiento especializado para mantenimiento, pruebas y mejora.	Coordinación grupo de sistemas - Oficina TIC	Diciembre de 2018	Planeación y ejecución de pruebas - Informe de resultados
Mitigar Riesgo	Planeación y adquisición de infraestructura necesaria y cambios en la topología de red necesaria.	Coordinación grupo de sistemas	Diciembre de 2018	Presupuesto para adquisición de infraestructura
Mitigar Riesgo	Implementación de herramientas para el control de información de dispositivos móviles (Tipo Celular).	Coordinación grupo de sistemas	Diciembre de 2018	Presupuesto para adquisición de herramientas

Fuente: Grupo de sistemas.

2.6 Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia

Como una de las metas del Plan de seguridad y privacidad del Ministerio, dado su carácter de cabeza de Sector, se planteó como meta construir con apoyo del Comando Conjunto Cibernético y las Entidades del Sector, el Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia del Sector Ambiente y RRNN PSPICCN V 1.0 Año 2018.

Su construcción se realizará a través de mesas de trabajo mensuales, siguiendo el cronograma definido por el Comando Conjunto Cibernético.

2.7 Otras actividades

- Bases de datos personales identificadas en MINAMBIENTE consolidadas (Es atendida a través de la actividad indicada en la Tabla 5 en el mes de noviembre)
- Ampliación del alcance de implementación de la norma ISO/IEC 27001. (Actividad de gestión, será tratada en el Comité Institucional de planeación y desempeño.)
- Articulación con el MIPG y el MSPI. (Actividad de gestión, será tratada en el Comité Institucional de planeación y desempeño.)

2.8 Presupuesto

Los recursos para el desarrollo de las actividades de este plan corresponden a $122.556.196 y soportan la Actividad desagregada 7.4 del Plan de acción de la Oficina TIC: *"Implementar el componente "Seguridad y privacidad de la información" para garantizar la seguridad de la información*, vale recordar que durante la vigencia 2017, la Oficina de TIC logró unificar en la ficha del proyecto a su cargo (que sustenta su plan de acción) las actividades de TI que antes estaban en la ficha de la Secretaría General, por ello esta actividad del plan se reporta con insumos de la gestión tanto de la Oficina TIC, como de la gestión del grupo de sistemas.

3. SEGUIMIENTO

3.1 Plan de acción

El seguimiento a las actividades se realiza en dos momentos:

- Mensualmente a través de la supervisión de los contratos que soportan los cronogramas de las actividades señaladas en la Tablas 5 y 6. Tarea que es realizada por el Jefe de la Oficina TIC y la Coordinadora del Grupos de sistemas, respectivamente.

- Reporte para seguimiento a la Oficina Asesora de Planeación del avance de la actividad del Plan de acción a cargo de la Oficina TIC: Actividad desagregada 7.4 del Plan de acción de la Oficina TIC: "Implementar el componente "Seguridad y privacidad de la información" para garantizar la seguridad de la información.

3.2 Informe trimestral seguridad de la información

De acuerdo con el ANEXO 1 ROLES Y RESPONSABILIDADES del Manual del SGSI el Responsable(s) asignado para Seguridad de la Información/ Oficial de Seguridad de la información debe informar trimestralmente del estado de la seguridad de la información al grupo operativo de Seguridad de Información de MINAMBIENTE.

Para ello se utilizará el instrumento de seguimiento del MSPI del Ministerio de las TIC, presentado en el diagnóstico de este plan.

GLOSARIO

Instrumento de Evaluación MSPI[1]: Es una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente "Seguridad y Privacidad de la Información". Fue creada por el Ministerio de Tecnologías de la Información y las Comunicaciones con uso libre sin fines lucrativos, por esta razón se prohíbe la comercialización y explotación de la misma.

[1] Tomado de: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

BIBLIOGRAFIA

COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LA COMUNICACIÓN. Manual para la implementación de la Estrategia de Gobierno en Línea de la República de Colombia. Versión 2015. Lineamientos para el avance de la estrategia de Gobierno electrónico de Colombia.

COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LA COMUNICACIÓN. Modelo de Seguridad y Privacidad de la Información –MSPI-.
Disponible en: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html.

Decreto 3570 de 2011: Por el cual se modifican los objetivos y la estructura del Ministerio de Ambiente y Desarrollo Sostenible.

Decreto 2573 de 2014: Reglamenta parcialmente la Ley 1341 (Compilado en el Decreto 1078 de 2015).

Decreto 1499 de 2017: Modelo Integrado de planeación y gestión.

Conpes 3072 de 2000. Política Agenda de Conectividad.

Conpes 3701 de 2011. Lineamientos de política para la Ciberseguridad y Ciberdefensa.

Conpes 3854 de 2016. Política Nacional de Seguridad Digital.

Documento Conpes 3650 de 2010: Implementación y sostenibilidad de la estrategia gobierno en línea GEL
Ley 1341 de 2009: Establece los mecanismos para la masificación del Gobierno en Línea.

Ley 1437 de 2011 Establece que el Gobierno Colombiano fijara los estándares y protocolos que deberán cumplir las autoridades nacionales para incorporar de forma gradual la aplicación de los medios electrónicos en los procedimientos administrativos.

Ley 1450 de 2011 Plan Nacional de Desarrollo en sus artículos 227, 230 y 232. Estrategia de Gobierno Electrónico del Estado Colombiano.

Ley 1474 de 2011: Normas orientadas al fortalecimiento de mecanismos de prevención, investigación y sanción de actos de corrupción y efectividad en el control de la gestión pública.

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública.

Ministerio de Ambiente y Desarrollo Sostenible. Manual del SGSI.

VERSIÓN	FECHA	RELACIÓN DE LAS SECCIONES O PÁGINAS MODIFICADAS	NATURALEZA DEL CAMBIO
1	30/01/2018	No aplica a la versión inicial	No aplica a la versión inicial
2	30/04/2018	Ajuste Plan de tratamiento de riesgos de seguridad y privacidad de información 2018	Actualización a nuevo plan.
3	30/06/2018	Se realiza actualización del plan de manejo de riesgos a nivel de infraestructura	Actualización a nuevo plan.

ELABORÓ	REVISÓ:	APROBÓ
NOMBRE: Gilber Corrales Rubiano	NOMBRE: Jose Rene Alvarado	NOMBRE: Gilber Corrales Rubiano
CARGO: Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones (TIC)	CARGO: Facilitador MADSIG- Oficina TIC	CARGO: Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones (TIC)
FIRMA:	FIRMA:	FIRMA: