



Agencia Nacional de
Infraestructura

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

G.I.T DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES

Historia de Revisión

Fecha	Versión	Descripción	Autor
31/01/2020	1.0	Creación del Plan	<p>Andrés Francisco Boada Icabuco Coordinador G.I.T. Tecnologías de la Información y las Telecomunicaciones</p> <p>Guillermo Cadena Ronderos Contratista G.I.T. Tecnologías de la Información y las Telecomunicaciones</p>
31/01/2021	2.0	<p>Revisión y Actualización capítulos 7 al 11 del Plan de seguridad y privacidad de la información. Estrategias, Proyectos, Metas, Acciones, Productos, Responsables.</p> <p>Ajuste de fechas.</p>	<p>Andrés Francisco Boada Icabuco Coordinador G.I.T. Tecnologías de la Información y las Telecomunicaciones</p> <p>Guillermo Cadena Ronderos Contratista G.I.T. Tecnologías de la Información y las Telecomunicaciones</p> <p>Erika Díaz Abella Contratista G.I.T. Tecnologías de la Información y las Telecomunicaciones</p>

Contenido

1.	INTRODUCCIÓN Y CONTEXTO	4
2.	OBJETIVOS.....	5
2.1	GENERAL	5
2.2	ESPECÍFICOS	6
3.	ALCANCE	6
4.	MARCO LEGAL.....	6
5.	DOCUMENTOS RELACIONADOS.....	6
6.	SITUACIÓN ACTUAL DE LA ENTIDAD	7
7.	ANÁLISIS DE BRECHAS.....	8
8.	PROYECTOS.	9
9.	HOJA DE RUTA.....	18
10.	INDICADORES.....	19
11.	SOCIALIZACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	21
12.	APROBACIÓN	21

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN Y CONTEXTO

Hoy en día, la información está definida como uno de los activos más valiosos y primordiales para cualquier tipo de organización, valor representado en la disponibilidad, integridad y confidencialidad de esta, lo que hace necesario que las organizaciones tengan una adecuada gestión de sus recursos y activos de información.

La defensa y protección de los activos de información es una tarea esencial para asegurar la continuidad y el desarrollo de los objetivos institucionales, así como para mantener el cumplimiento normativo y regulatorio aplicable a la entidad, además traslada confianza a las partes interesadas.

Cualquier tipo de organización independiente de su tamaño y naturaleza, debe ser consciente que la diversidad de amenazas existentes en la actualidad, atentan contra la seguridad y privacidad de la información y representan un riesgo que al materializarse no solo les puede acarrear costos económicos, sancionales legales, afectación de su imagen y reputación, sino que pueden afectar la continuidad y supervivencia del negocio. Lo anterior, sumando a un entorno tecnológico en donde cada día se hace más complejo de administrar y asegurar la información ello demanda entonces que cada vez más, las acciones encaminadas a la seguridad de la información formen parte de los objetivos y planes estratégicos de las organizaciones.

Por lo tanto, es indispensable que los responsables dentro de las organizaciones encargados de velar por la protección y seguridad de sus recursos, infraestructura e información, constantemente estén adoptando, implementando y mejorando medidas de seguridad orientadas a prevenir y/o detectar los riesgos que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de los activos de información a través de los cuales se gestiona la información del negocio, independientemente si está es de carácter organizacional o personal, o de tipo pública o privada.

Dicha gestión se debe realizar de manera preventiva, es decir, a través de actividades y definiciones previamente evaluadas de acuerdo con los riesgos identificados, clasificados y valorados, de tal forma que dé lugar al adecuado tratamiento de los mismos, y es justo ahí en donde cobra valor el presente documento, el cual se constituye como el plan que describirá las acciones relacionadas con la adecuada gestión para el aseguramiento de la Seguridad y privacidad de la información en la ANI, de acuerdo con su contexto de función, misión, visión y la normatividad que la rige.

La **AGENCIA NACIONAL DE INFRAESTRUCTURA** es consciente que la protección y aseguramiento de su información es fundamental para garantizar la debida gestión y contribuir de manera adecuada para que

el país pueda desarrollar la infraestructura de transporte a través de asociaciones público-privadas, generando competitividad, bienestar y confianza, razón por la cual debe establecer un marco normativo de Seguridad y Privacidad de la Información que contemple políticas, límites, responsabilidades y obligaciones frente a la seguridad y privacidad de la información de la entidad.

En atención a lo anterior, la entidad asumió el reto de implementar el MSPI – Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno Digital¹, a su vez reglamentado a través del Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital; de igual manera el Decreto 2106 de 2019, Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública, en el parágrafo del artículo 16 indica que (...)Las autoridades deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones

La ANI como parte del proceso de implementación del modelo enunciado dispondrá de dos instrumentos:

- i) en donde se definirá los lineamientos para la identificación y valoración de los activos de información y
- ii) en donde se definirá los lineamientos para la evaluación y tratamiento de los riesgos; siendo éstos el medio más eficaz de tratar, gestionar y minimizar los riesgos, considerando el impacto que éstos representan para la entidad y sus partes interesadas.

El presente documento contiene el plan para el establecimiento de las condiciones de seguridad informática y de la información de la ANI, el cual tomará como referencia el Modelo de Seguridad y Privacidad de la estrategia de Gobierno Digital y la norma ISO 27001², los cuales proporcionan un marco metodológico basado en buenas prácticas para llevar a cabo la implementación del mencionado modelo de manera efectiva y adecuada.

Así mismo, este documento tiene directa relación con la política de seguridad de información la cual corresponde a la declaración general que representa la posición de la Agencia Nacional de Infraestructura frente a la necesidad de protección de su información, al igual que de la preservación de aquellos activos de información que la soportan.

2. OBJETIVOS

2.1 GENERAL

Definir las actividades necesarias para la implementar el Modelo de Seguridad y Privacidad de la Información en la Agencia Nacional de Infraestructura en cada una de sus fases, en cumplimiento de

¹ <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>

² https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

las disposiciones legales vigentes y el aseguramiento de la información como el activo más importante de la entidad.

2.2 ESPECÍFICOS

- Realizar reconocimiento del contexto de la ANI con propósito de orientar la implementación del MSPI Modelo de Seguridad y Privacidad de la información
- Definir las etapas del plan para establecer la estrategia de seguridad de la información de la Agencia.
- Desarrollar las actividades definidas para el Modelo de Seguridad y Privacidad de la Información de la entidad de acuerdo con los requerimientos establecidos en la estrategia de Gobierno Digital.
- Definir e implementar políticas y directrices que guíen las prácticas de protección de la información en cuanto a su confidencialidad, integridad y disponibilidad.
- Gestionar los riesgos de seguridad de la Información a fin de reducir la probabilidad de ocurrencia.
- Identificar y gestionar las vulnerabilidades y amenazas presentadas sobre la plataforma tecnológica.
- Generar planes y acciones correctivas y preventivas adecuadas, aplicando las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y las de la propia organización.

3. ALCANCE

El Plan de Seguridad y Privacidad de la Información considera los controles de la norma NTC/ISO 27001:2013³, el análisis de riesgos realizado a los procesos de la ANI, y los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno Digital. Por tanto, El plan de seguridad y privacidad de la información y lineamientos asociados como directriz de la Presidencia de la ANI, será de aplicabilidad e implementación para todos los procesos y aspectos administrativos de la organización y, de cumplimiento por parte de todos aquellos servidores públicos y terceros que presten sus servicios o tengan algún tipo de relación con la información gestionada por la Entidad.

4. MARCO LEGAL.

- Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Norma NTC / ISO 27001:2013: Tecnología de la Información. Técnicas de seguridad de la información y Código de Práctica para controles de seguridad de la información
- Norma NTC/ISO 27002:2013: Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información
- Decreto 1008 de 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
- Norma NTC / ISO 31000:2009: Gestión de Riesgo, Principios y Directrices
- Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 4 del Departamento Administrativo de la Función Pública

5. DOCUMENTOS RELACIONADOS

³ <https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27001.pdf>

- Política General de Seguridad y Privacidad de la Información (GTEC-PT-001), la cual esta publicada en la página Web de la ANI y podrá ser consultada en el siguiente link:
https://www.ani.gov.co/sites/default/files/sig//gico-p-001_politica_de_seguridad_y_privacidad_de_informacion_v2.pdf
- Tratamiento de Vulnerabilidades Técnicas (GTEC-I-001)
- Gestión de incidentes y requerimientos TI V (GTEC-P-002)
- Plan de Seguridad y Privacidad de la Información
- Norma ISO 31000:2009

6. SITUACIÓN ACTUAL DE LA ENTIDAD

Medición seguridad de la información 2020:

Esta evaluación fue realizada en diciembre 2020, haciendo uso de la herramienta de autodiagnóstico generada por el Mintic durante el año 2020, de la cual se muestra a continuación lo arrojado como medición general, así como la medición y estado de los controles al cierre de la vigencia.

Contexto General:

- Evaluación y Diagnostico de la Seguridad de la Información: 90 %
- Implementación de la Seguridad de la Información: 60 %
- Seguimiento, Evaluación y mejora de la Seguridad de la Información: 30 %

De acuerdo con estas mediciones, la implementación de la seguridad de la información en la ANI está en un nivel Medio:

SEGURIDAD DE LA INFORMACIÓN



Nivel de avance en la implementación de la Política de Gobierno Digital		Escala de 0 - 100
	Bajo	Menor a 20
	Medio bajo	Igual o mayor a 20 y menor a 40
	Medio	Igual o mayor a 40 y menor a 60
	Medio alto	Igual o mayor a 60 y menor a 80
	Alto	Igual o mayor a 80 y menor o igual a 100

Medición y estado de los Controles:

No.	Evaluación de Efectividad de controles		
	DOMINIO	Calificación Actual 2020	Calificación Objetivo
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	76	100
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	66	100
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	53	100
A.8	GESTIÓN DE ACTIVOS	37	100

No.	Evaluación de Efectividad de controles		
	DOMINIO	Calificación Actual 2020	Calificación Objetivo
A.9	CONTROL DE ACCESO	63	100
A.10	CRIPTOGRAFÍA	60	100
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	62	100
A.12	SEGURIDAD DE LAS OPERACIONES	73	100
A.13	SEGURIDAD DE LAS COMUNICACIONES	60	100
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	72	100
A.15	RELACIONES CON LOS PROVEEDORES	77	100
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	65	100
A.17	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	31	100
A.18	CUMPLIMIENTO	52	100
PROMEDIO EVALUACIÓN DE CONTROLES		60	100

Como resultado de la misma medición, se indica la valoración de avance del ciclo PHVA para cada vigencia desde 2017 a 2020.

Año	AVANCE		
	COMPONENTE	% de Avance 2020	% Avance Esperado a cierre de cada vigencia
2017	Planificación	32%	40%
2018	Implementación	13%	20%
2019	Reevaluación y Redefinición		
2019	Diagnóstico y Planificación	70%	100%
2020	Implementación	60%	70%

7. ANÁLISIS DE BRECHAS



Las brechas más significativas encontradas fueron la Gestión de incidentes y la Gestión de Activos.

Respecto a la primera, se anota que se han gestionado y tratado los incidentes, sin embargo, es necesario realizar un afianzamiento en el procedimiento interno, así como reforzar y formalizar el relacionamiento externo con entidades de apoyo.

Sobre la gestión de activos, la ANI inicia un proceso de revisión y cambio en el procedimiento, en los instrumentos y las responsabilidades. La Coordinación de tecnología estará presentando el nuevo esquema en el primer semestre de 2021.

Las demás mediciones en general tienen su estado y nivel de maduración normal, se debe continuar con ese proceso evolutivo y de optimización.

Con la formulación de los proyectos que se realiza a continuación, la ANI pretende solventar y ajustar las falencias encontradas y ubicarse a través de una hoja de ruta, en una situación de cumplimiento e implementación adecuada de la seguridad de la información.

8. PROYECTOS.

El plan de seguridad y Privacidad de la información además de tener un origen normativo y de optimización de la seguridad y privacidad de la información en la ANI, responde también al desarrollo de uno de los proyectos establecidos en el Plan Estratégico de Tecnologías de la Información – PETI, el cual se describe a continuación:

Id del proyecto	P-04
Nombre del proyecto	Implementar el Modelo de Seguridad y Privacidad de la información
Objetivos del proyecto	<p>- Adopción del Modelo de Seguridad y Privacidad de la información por parte de las Entidades del Estado.</p> <p>- Contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.</p> <p>Para la vigencia 2021 se considera la ejecución de las siguientes actividades:</p> <ul style="list-style-type: none"> ○ Continuar la implementación del Plan de Seguridad y Privacidad de la información. ○ Continuar la implementación del plan de tratamiento de riesgos de seguridad digital.

	<p>Harán parte de los anteriores:</p> <ul style="list-style-type: none"> ▪ Realizar la matriz de valoración de riesgos de seguridad de la información del proceso GTEC. ▪ Elaborar el Manual Políticas Específicas de Seguridad y Privacidad de la Información
Capacidades de la entidad impactadas con el proyecto	<ul style="list-style-type: none"> ○ Recurso humano calificado para realizar la supervisión del proyecto ○ Recursos económicos disponibles para llevar a cabo el proyecto ○ Periodo de tiempo disponible para ejecutar el proyecto ○ Recurso humano para ejecución de actividades
Brechas que cierra	<ul style="list-style-type: none"> ○ Bloques de construcción de aplicación ○ Bloques de construcción que involucran infraestructura tecnológica de TI ○ Bloques de construcción que impactan contrataciones de servicios y operación ○ Bloques de construcción que involucra talento humano
Estimación de esfuerzo y tiempo	2019 - 2022
Estimación de costos	Desagregado por vigencia, en donde para el año 2021 se enuncia en el Plan Anual de Adquisiciones señalado en el documento PETI.

En coherencia con lo anterior y alineado con los objetivos del presente plan, se hace necesario adelantar los siguientes subproyectos a fin de cerrar las brechas identificados y aprovechar las oportunidades que brinda el MSPI.

8.1 Subproyectos Plan de Seguridad y Privacidad:

1. Planeación detallada de la Implementación
2. Formulación del Manual para el cumplimiento de la Política de seguridad y Privacidad de la información
3. Desarrollo e Implementación del Plan de tratamiento de los riesgos de seguridad de la información.
4. Renovación Plataforma de Seguridad Perimetral
5. Renovación de la Plataforma Antivirus
6. Renovación Direccionamiento IPV6
7. Sensibilización y Socialización - Cultura de la Seguridad de la Información.

Id del proyecto	SP-01:
Fase:	Planeación
Nombre del proyecto	Planeación detallada de la Implementación.
Objetivos del proyecto	<ul style="list-style-type: none"> - Realizar la verificación y actualización del diagnóstico de seguridad y privacidad de la información bajo criterios reconocidos tales como, el MSPI - Modelo de Seguridad y privacidad de la información de Gobierno Digital, al igual que bajo la ISO/IEC 27001:2013. - Obtener un informe con la identificación del estado de cumplimiento y conformidad de los aspectos de seguridad de la información de la ANI bajo el (los) modelos evaluados.
Capacidades de la entidad impactadas con el proyecto	<ul style="list-style-type: none"> - Recurso humano calificado para acompañar la supervisión del proyecto y la ejecución de actividades - Periodo de tiempo disponible para ejecutar el proyecto.
Actividades que involucran la realización del proyecto	<ul style="list-style-type: none"> - Definir y registrar las fases, actividades, recursos y tiempos necesarios para la planeación e implementación del modelo de seguridad y privacidad de la información. - Definir la estructura de roles y responsabilidades para la gestión de los propósitos del MSPI y de las fases definidas - Identificar los aspectos claves que definan y orienten las actividades para los propósitos de seguridad y privacidad de la información, entre ellos, la justificación, el alcance, la política y los objetivos del Modelo de Seguridad y Privacidad de la Información (MSPI). - Definir el mapa de ruta de las actividades orientadas a la planificación e implementación del modelo de seguridad y privacidad de la información acorde con el informe de diagnóstico.
Productos / entregables	Documento: Análisis y Contexto General de la Implementación del MSPI en la ANI.
Estimación de esfuerzo y tiempo	3 meses: Ene-Mar-2021 Proyectados en la Hoja de Ruta
Estimación de costos	No Presupuesto requerido
Responsable designado	Guillermo Cadena Ronderos – Contratista VPRE

Id del proyecto	SP-02
Fase:	Implementación
Nombre del proyecto	Formulación del Manual para el cumplimiento de la Política de seguridad y Privacidad de la información.
Objetivos del proyecto	Especificar los lineamientos definidos en la Política de Seguridad y privacidad de la información de la Agencia Nacional de Infraestructura, aplicables a los funcionarios, contratistas y demás partes interesadas.
Capacidades de la entidad impactadas con el proyecto	<ul style="list-style-type: none"> - Recurso humano calificado para acompañar la supervisión del proyecto y la ejecución de actividades - Periodo de tiempo disponible para ejecutar el proyecto.
Actividades que involucran la realización del proyecto	<ul style="list-style-type: none"> - Definir el modelo y esquema de gestión de políticas y directrices de seguridad de la información. - Desarrollar, complementar y ampliar los lineamientos establecidos en la Política de Seguridad y Privacidad e la Información. - Especificar los lineamientos concretos respecto de los documentos, formatos, instructivos, procedimientos y manuales que haya a lugar. - Gestionar la aprobación y socialización del documento en el marco del sistema integrado de gestión de la entidad.
Productos / entregables	Documento: Manual de políticas específicas de seguridad y privacidad de la información
Estimación de esfuerzo y tiempo	4 meses: Feb-May-2021 - Proyectados en la Hoja de Ruta
Estimación de costos	No Presupuesto requerido
Responsable designado	Guillermo Cadena Ronderos – Contratista VPRE

Id del proyecto	SP-03
Fase:	Implementación
Nombre del proyecto	Desarrollo e Implementación del Plan de tratamiento de Riesgos de seguridad de la información
Objetivos del proyecto	Identificar y valorar los riesgos Identificar Vulnerabilidades y Amenazas

	<p>Análisis de los Riesgos y gestionar los riesgos Calcular el nivel de riesgo asociado Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos</p>
Capacidades de la entidad impactadas con el proyecto	<ul style="list-style-type: none"> - Recurso humano calificado para acompañar la supervisión del proyecto y la ejecución de actividades - Periodo de tiempo disponible para ejecutar el proyecto.
Actividades que involucran la realización del proyecto	<ul style="list-style-type: none"> - Validación y actualización de los riesgos identificados de seguridad de la información - Actualización Inventario Tecnológico de la ANI. - Identificar las vulnerabilidades y amenazas a los que se encuentran expuestos los activos de información. - Determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo. - Realizar Seguimiento y actualización a la Matriz de Riesgos Proceso GTEC 2021 - Revisión y actualización de la Identificación de Impactos ante Interrupción de Servicios de Tecnológicos ANI definidos en la vigencia 2020. - Identificación y valoración de riesgos por activo de información - Socialización y formalización de la Matriz de Clasificación y Registro de Activos de Información. - Socialización y formalización del instructivo para Diligenciamiento y reporte de la Matriz de Activos de Información - Medición periódica de los resultados del plan de tratamiento de riesgos. -
Productos / entregables	<p>Documentos:</p> <ul style="list-style-type: none"> - Plan de Tratamiento de Riesgos actualizado. - Matriz de Riesgos de Seguridad y Privacidad de la Información - Matriz de Riesgos Proceso GTEC 2021 en la ANI. - Identificación de Impactos ante Interrupción de Servicios de Tecnológicos ANI actualizado. - Resultados de la medición de la implementación de plan de tratamiento de riesgos.
Estimación de esfuerzo y tiempo	17 meses: Feb 2021-Jun 2022 - Proyectados en la Hoja de Ruta
Estimación de costos	No Presupuesto requerido
Responsable designado	Guillermo Cadena Ronderos – Contratista VPRE

Id del proyecto	SP-04
Fase:	Implementación
Nombre del proyecto	Renovación Plataforma de Seguridad Perimetral
Objetivos del proyecto	Adquirir la renovación del licenciamiento y soporte de la plataforma de seguridad perimetral de la agencia nacional de infraestructura
Capacidades de la entidad impactadas con el proyecto	<ul style="list-style-type: none"> - Recurso humano calificado para realizar la supervisión del proyecto - Recursos económicos disponibles para llevar a cabo el proyecto - Periodo de tiempo disponible para ejecutar el proyecto - Recurso humano para ejecución de actividades
Actividades que involucran la realización del proyecto	<ul style="list-style-type: none"> - Gestionar la etapa precontractual del proceso lo cual implica las siguientes actividades: <ul style="list-style-type: none"> o Generar el estudio de mercado y definir el presupuesto de la contratación. o Generar el estudio previo que documenta, soporta y justifica la contratación o Definir el anexo técnico que contiene las especificaciones y condiciones técnicas para la contratación. o Generar la matriz de riesgo asociada al proceso, o Solicitar los registros y disposición presupuestales. o Solicitar inicio de proceso de contratación. - Gestionar y acompañar a la implementación del proceso para garantizar la actualización, puesta en marcha y realización de mantenimientos preventivos a los equipos que conforman la plataforma de seguridad perimetral con que cuenta la Entidad, esto es, Un (1) equipo FOTIGATE con serial FG6H0E5819900536, Un (1) equipo FORTIGATE con serial FG6H0E5819901021 y Un (1) equipo FORTIANALYZER con serial FL-2HFTB19000698, como lo especifica el ANEXO TÉCNICO. - Asegurar la correcta configuración y parametrización para lograr un adecuado desempeño sobre el blindaje, protección de la plataforma y la seguridad de la información. - Generación de estadísticas y revisión sobre eventos sospechosos de seguridad de la información que ocurran sobre la plataforma tecnológica -

Productos / entregables	Licenciamiento renovado y con nueva cobertura Informe de Mantenimientos realizados Nuevas versiones de configuraciones. Informe final de actividad adelantadas y cumplimiento de las obligaciones.
Estimación de esfuerzo y tiempo	6 meses: Jul-Dic 2021. Proyectados en la Hoja de Ruta
Estimación de costos	Presupuesto definido: \$ 70.000.000.00
Responsable designado	Guillermo Cadena Ronderos – Contratista VPRE Cesar Fabian Gonzalez – Contratista VPRE Javier Alonso Zuñiga - Experto G3/G5 VPRE

Id del proyecto	SP-05
Fase:	Implementación
Nombre del proyecto	Renovación de la Plataforma Antivirus
Objetivos del proyecto	Renovar el licenciamiento de software antivirus de la agencia nacional de infraestructura
Capacidades de la entidad impactadas con el proyecto	<ul style="list-style-type: none"> - Recurso humano calificado para realizar la supervisión del proyecto - Recursos económicos disponibles para llevar a cabo el proyecto - Periodo de tiempo disponible para ejecutar el proyecto - Recurso humano para ejecución de actividades
Actividades que involucran la realización del proyecto	<ul style="list-style-type: none"> - Gestionar la etapa precontractual del proceso lo cual implica las siguientes actividades: <ul style="list-style-type: none"> o Generar el estudio de mercado y definir el presupuesto de la contratación. o Generar el estudio previo que documenta, soporta y justifica la contratación o Definir el anexo técnico que contiene las especificaciones y condiciones técnicas para la contratación. o Generar la matriz de riesgo asociada al proceso, o Solicitar los registros y disposición presupuestales. o Solicitar inicio de proceso de contratación. - Gestionar y acompañar a la implementación del proceso para garantizar la correcta actualización, puesta en marcha del nuevo licenciamiento, configuración y

	<p>afinamiento de la plataforma. Actualización de la consola de administración.</p> <ul style="list-style-type: none"> - Asegurar la correcta configuración y parametrización para lograr un adecuado desempeño de las licencias y la plataforma. - Verificar la actualización automática de las políticas de prevención, las vacunas o patrones sin congestionar la red, ni afectar el rendimiento de las estaciones por el término de vigencia del licenciamiento. - Verificar la generación de reportes de los virus detectados y acciones realizadas por el término de vigencia del licenciamiento.
Productos / entregables	Licenciamiento actualizado con nueva vigencia y en operación. Informe final de actividad adelantadas y cumplimiento de las obligaciones.
Estimación de esfuerzo y tiempo	6 meses: Abr-Sept 2021. Proyectados en la Hoja de Ruta
Estimación de costos	Presupuesto definido: \$ 42.000.000.00
Responsable designado	Jhon Aguilar – Contratista VPRE Apoyo y Acompañamiento: Guillermo Cadena Ronderos – Contratista VPRE

Id del proyecto	SP-06
Fase:	Implementación
Nombre del proyecto	Renovación Direccionamiento IPV6
Objetivos del proyecto	Renovar el derecho a uso del pool de direcciones IPV6 con el que cuenta la Agencia Nacional de Infraestructura
Capacidades de la entidad impactadas con el proyecto	<ul style="list-style-type: none"> - Recurso humano calificado para realizar la supervisión del proyecto - Recursos económicos disponibles para llevar a cabo el proyecto - Periodo de tiempo disponible para ejecutar el proyecto - Recurso humano para ejecución de actividades
Actividades que involucran la realización del proyecto	<ul style="list-style-type: none"> - Gestionar la etapa precontractual del proceso lo cual implica las siguientes actividades: <ul style="list-style-type: none"> o Generar el estudio de mercado y definir el presupuesto de la contratación. o Generar el estudio previo que documenta, soporta y justifica la contratación

	<ul style="list-style-type: none"> ○ Definir el anexo técnico que contiene las especificaciones y condiciones técnicas para la contratación. ○ Generar la matriz de riesgo asociada al proceso, ○ Solicitar los registros y disposición presupuestales. ○ Solicitar inicio de proceso de contratación. <ul style="list-style-type: none"> - Validar la gestión de todos los tramites técnicos, administrativos y financieros que sean necesarios ante el organismo LACNIC - Latin América & Caribbean Network Information Centre (en español - Registro de Direcciones de Internet de América Latina y Caribe) para la renovación del prefijo de direcciones IPV6 que tiene asignado la Agencia Nacional de infraestructura - Verificar el cumplimiento de los requisitos y exigencias definidas por LACNIC para realizar todos los trámites de renovación. - Validar la entrega a la ANI la documentación técnica y administrativa que se derive del objeto contractual incluidos los comprobantes de pago efectuados a LACNIC
Productos / entregables	Derecho de uso actualizado con nueva vigencia y en operación. Informe final de actividad adelantadas y cumplimiento de las obligaciones.
Estimación de esfuerzo y tiempo	6 meses: Jul-Dic 2021. Proyectados en la Hoja de Ruta
Estimación de costos	Presupuesto definido: \$ 5.000.000.00
Responsable designado	Guillermo Cadena Ronderos – Contratista VPRE

Id del proyecto	SP-07
Fase:	Implementación.
Nombre del proyecto	Sensibilización y Socialización - Cultura de la Seguridad de la Información.
Objetivos del proyecto	Socialización de aspectos del MSPI y Toma de conciencia de seguridad de la información

Capacidades de la entidad impactadas con el proyecto	<ul style="list-style-type: none"> - Recurso humano calificado para acompañar la supervisión del proyecto y la ejecución de actividades - Periodo de tiempo disponible para ejecutar el proyecto.
Actividades que involucran la realización del proyecto	<ul style="list-style-type: none"> - Divulgar a toda la entidad la existencia del subsistema de gestión de seguridad de la información y sus componentes de apoyo - Socializar a todo el personal de la Entidad las políticas de seguridad de la información - Fomentar la cultura de la seguridad de la información como herramienta de protección de la información institucional - Generar y divulgar conocimiento a los colaboradores de la ANI respecto a la seguridad de la información. - Fortalecer las capacidades institucionales para prevenir y dar respuesta a eventos de seguridad - Explicar los mecanismos de control dispuestos por la entidad para evitar ataques informáticos - Generar Campañas y socialización con usuarios internos sobre buenas prácticas en Seguridad de la información - Explicar en manera sencilla en qué consisten diversos tipos de ataques informáticos y como controlarlos
Productos / entregables	<p>Documentos: Campañas de socialización Presentaciones sobre seguridad de la Información Encuestas</p>
Estimación de esfuerzo y tiempo	6 meses: Jul-Dic 2021. Proyectados en la Hoja de Ruta
Estimación de costos	No Presupuesto requerido
Responsable designado	Guillermo Cadena Ronderos – Contratista VPRE

9. HOJA DE RUTA.

Se indica que con el presente plan se está dando cumplimiento a las fases del MSPI y cada fase que lo compone relacionando los proyectos planteados

Nombre del Proyecto	2021												2022											
	ene	feb	mar	abr	mayo	jun	jul	ago	sep	oct	nov	dic	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
Planeación detallada de la Implementación																								
Formulación del Manual para el cumplimiento de la Política de seguridad y																								

Nombre del Proyecto	2021												2022											
	ene	feb	mar	abr	mayo	jun	jul	ago	sep	oct	nov	dic	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
Privacidad de la información																								
Desarrollo e Implementación del Plan de tratamiento de los riesgos																								
Renovación Plataforma de Seguridad Perimetral																								
Renovación de la Plataforma Antivirus																								
Renovación Direccionamiento IPV6																								
Sensibilización y Socialización – Cultura de Seguridad																								

10. INDICADORES

La medición del cumplimiento del presente plan hace parte del tablero de control definido para el Proceso de gestión Tecnología, como se describe a continuación

Indicador 2: Eficacia en el cumplimiento

Nivel	Indicador	Objetivo	Formula	Frecuencia de medición
1	Eficacia en el cumplimiento del PETI de la vigencia	Determinar el nivel de cumplimiento del Plan Estratégico de Tecnologías de la Información y las Comunicaciones de la vigencia	$\frac{\text{Número de actividades realizadas}}{\text{Número de actividades programadas}} * 100$	Semestral

Con el fin de hacer un seguimiento detallado al presente plan se han definido los siguientes indicadores de como herramientas de medición.

INDICADOR 01- MANEJO Y ATENCIÓN A INCIDENTES DE SEGURIDAD
OBJETIVO
Reflejar la gestión dada a los incidentes reportados sobre seguridad de la información
TIPO DE INDICADOR:
Indicador de Gestión.

DESCRIPCIÓN DE VARIABLES	FORMULA	FRECUENCIA DE MEDICIÓN			
Var04: ¿Número total de casos relacionados con la seguridad de la información atendidos y cerrados?	$(\text{Var04}/\text{Var05}) * 100$	Trimestral			
Var05: ¿Número total de casos reportados relacionados con la seguridad de la información?					
METAS					
Mínima	75-80 %	Satisfactoria	80-90 %	Sobresaliente	100 %

Nota: Se aclara que La gestión de incidentes es medida desde la vida de la implementación del Plan de seguridad y privacidad de la información objeto del presente documento y desde la gestión de operación de servicios de T.I.; por lo cual este indicador está integrado en el tablero de control de indicadores de la gestión de T.I.

INDICADOR 02- ADQUISICIONES PARA SEGURIDAD DE LA INFORMACIÓN			
OBJETIVO			
Validar si la entidad cumple con las adquisiciones previstas en el Plan de Seguridad y Privacidad de la Información.			
Las adquisiciones previstas y programadas son: Renovación de la Plataforma de Seguridad Perimetral, Renovación de la Plataforma de Antivirus y Renovación Dirección Direcciónamiento IPV6			
TIPO DE INDICADOR:			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES	FORMULA	FRECUENCIA DE MEDICIÓN	
Var01: Número de adquisiciones realizadas y completadas	$(\text{Var01}/\text{Var02}) * 100$	Anual	
Var02: Número de adquisiciones planeadas			
METAS			
CUMPLE	1	NO CUMPLE	0

INDICADOR 03- SENSIBILIZACIÓN Y SOCIALIZACIÓN		
OBJETIVO		
Validar si la entidad realiza socialización y divulgación a los usuarios de la política de seguridad de la información y los canales dispuestos para reporte un incidente de seguridad de la información.		
TIPO DE INDICADOR:		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	FORMULA	FRECUENCIA DE MEDICIÓN
Var01: Número de divulgaciones realizadas	$(\text{Var01}/\text{Var02}) * 100$	Semestral

Var02: Número divulgaciones planeadas			
METAS			
CUMPLE	1	NO CUMPLE	0

11. SOCIALIZACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El plan de Seguridad y Privacidad de la Información fue aprobado con la firma y publicación del presente documento el 31 de enero de 2021, con dicha aprobación se procede con su publicación en la página de la entidad sección: Transparencia / 6.3 Planes

Ahora bien, una vez aprobado, será socializado a los interesados de la siguiente manera:

Tipo de audiencia	Medio de socialización	Instrumento
Directivos de la entidad	Comité MIPG	Documento PETI / presentación
Colaboradores Internos	Correo electrónico	Mensaje informativo / Piezas de comunicación
Colaboradores Externos	Publicación en la página de la entidad	Documento Plan de Seguridad y Privacidad de la Información.

12. APROBACIÓN

Nombre	Cargo	Firma
Andrés Francisco Boada	Coordinador G.I.T. Tecnologías de la información y las Telecomunicaciones	
Diego Alejandro Morales Silva	Vicepresidente de Planeación Riesgo y Entorno	