Agencia Nacional de Infraestructura

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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

Bogotá D.C. 2022

Control de Versiones

Fecha	Versión	Descripción
31/01/2020	1.0	Creación del Plan
26/04/2021	2.0	Revisión y Actualización capítulos 7 al 11 del Plan de seguridad y privacidad de la información. Estrategias, Proyectos, Metas, Acciones, Productos, Responsables. Ajuste de fechas.
31/01/2022	3.0	Actualización del Plan a la vigencia 2022.

Contenido

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

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: afectación de su imagen y reputación, costos económicos, sancionales legales, sino que pueden afectar la continuidad y supervivencia de su actividad. Lo anterior, sumado a un entorno laboral virtual en donde cada día se hace más complejo de administrar y asegurar los activos y la información, panorama que demanda entonces que cada vez más, acciones encaminadas a que la ciberseguridad forme parte de los objetivos y planes estratégicos de las organizaciones.

Lo anterior conlleva a que los responsables 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 de la entidad, independientemente si está es de carácter organizacional o personal, o si es de naturaleza 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 donde cobra valor el presente documento,

el cual se constituye como el plan que describirá las acciones relacionadas con la adecuada gestión de la Seguridad y Privacidad de la información en la ANI, así como con la estrategia de seguridad, 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 adoptar y aplicar el marco normativo de Seguridad y Privacidad de la Información que contempla 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 Digital[1], reglamentado a través del decreto 1078 de 2015, modificado por el Decreto 1008 de 2018. Este decreto 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, éstos últimos son: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los 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. Adicionalmente la resolución 500 del 10 de marzo del 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital, incorporó el modelo de seguridad y privacidad de la información – MSPI, a la política de Gobierno Digital (MinTIC, 2021).

La ANI como parte del proceso de implementación del modelo enunciado dispone de dos instrumentos: i) en donde se definen los lineamientos para la identificación y valoración de los activos de información y ii) en donde se definen 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[2][3] y la norma ISO 27001, los cuales proporcionan un marco metodológico basado en buenas prácticas para llevar a cabo la implementación del mencionado modelo de manera efectiva y adecuada.

[1] https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/
[2] https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf
[3] https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

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. ALCANCE

En la ANI el Modelo de Seguridad y Privacidad es de carácter transversal ya que tiene aplicabilidad a todos los procesos y aspectos administrativos de la organización y es de obligatorio 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, al efecto en los planes asociados, se contempla la protección de la información en cualquiera de sus medios y formas de presentación, esto es; tanto en medios digitales como no digitales.

3. ESTRATEGIA DE SEGURIDAD.

La estrategia de seguridad de la entidad en la presente vigencia 2022 se enfoca en fortalecer las medidas de control ya implementadas y continuar con la implementación de otros controles que hacen parte del modelo de seguridad y privacidad, manteniendo un enfoque preventivo que articula los aspectos de tipo técnico y administrativo, así como de talento humano, para garantizar el mejoramiento continuo del proceso de seguridad.

Los controles de seguridad se materializan por medio de documentos, procesos y actividades, éstas últimas que se desarrollan en forma permanente o esporádica, algunas de las cuales se relacionan a continuación:

- Políticas de Seguridad y Privacidad de la Información - GTEC-PT-001 versión 3.0 de mayo de 2020, documento que se constituye en la base de la pirámide del MSPI y que desarrolla aspectos importantes como: roles y responsabilidades; capítulos 5 y 6 y políticas y directrices de protección de datos personales; capítulo 8.
- Identificación y gestión de riesgos de seguridad de la Información. La entidad cuenta con una matriz que identifica y valora los riesgos de seguridad de la información, así como del plan de tratamiento de riesgos definido y actualizado en cada vigencia.
- Mantenimiento de una cultura y capacitación en seguridad y prevención de riesgos de la información.
- Realización de actividades de gestión y monitoreo de herramientas que protegen la infraestructura de TI.
- Incorporación de la seguridad en proyectos de implementación y adopción de tecnologías de la información y ciclo de vida del software.
- Aplicación del procedimiento de tratamiento incidentes seguridad de información (GTEC-I-004 v1).
- Disposición de proceso de autenticación y segregación de funciones y responsabilidades para el uso de servicios y sistemas de información.

- Aplicación de procesos de gestión y retención de información de respaldo mediante el instructivo copias de seguridad de TI (GTEC-I-005- V1).
- Gestión de la seguridad en terceros y partes interesadas
- Gestión de cambios en la TI mediante la aplicación del instructivo: Gestión de cambios de TI (GTEC-I-003 V1.0)

4. OBJETIVO ESTRATEGICO

El objetivo es minimizar la probabilidad de ocurrencia y el impacto de los riesgos que se puedan materializar, por medio del fortalecimiento de los controles contenidos en el Modelo de Seguridad y Privacidad de la Información en la Agencia Nacional de Infraestructura, en cumplimiento de las disposiciones vigentes.

Para el logro del objetivo antes mencionado, se contemplan los siguientes temas los cuales se detallan en proyectos a ejecutar en la vigencia, los cuales se detallan en la sección 7.

- Arquitectura de referencia de seguridad para la infraestructura tecnológica en la nube y en sitio.
- Seguridad de la información de los usuarios finales mediante la adopción y apropiación de herramientas y esquemas de seguridad.
- Revisar, generar y actualizar documentación de actividades de seguridad y disponibilidad de la infraestructura y adoptar las actividades incorporadas.
- Sensibilización apropiación y prevención de riesgos de seguridad de la información dirigido a usuarios finales y capacitación en técnicas de seguridad al personal del GIT de Tecnologías de la información y las Telecomunicaciones.
- Definir e implementar los esquemas de contingencia para los servicios de mayor criticidad.
- Ejecución del plan de tratamiento de riesgos, como se describe en el plan respectivo.

5. MARCO LEGAL.

- Resolución 500 de marzo 10 de 2021: Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital
- 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.

6. DOCUMENTOS RELACIONADOS CON ESTE PLAN

El plan de seguridad y privacidad se apalanca y tiene como base las políticas y procedimientos relacionados con la gestión de seguridad de la información, entre los cuales tenemos los siguientes:

- 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 enlace:
  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 Tratamiento de Riesgos de Seguridad y Privacidad de la Información - 2022

7. 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 a las necesidades propias de la entidad y en conjunto se reflejan y articulan en uno de los proyectos establecidos en el Plan Estratégico de Tecnologías de la Información – PETI (P.04 – Continuidad en la implementación del plan de seguridad y privacidad de la información).

Los proyectos que conforman este plan se relacionan a continuación:

- **PS-01:** Adoptar la arquitectura de referencia de seguridad en nube y en sitio. (Fase I)
- **PS-02:** Fortalecer la seguridad de los servicios para usuario final. (Fase I)
- **PS-03:** Generación de documentos con guías, políticas específicas y adopción de procesos de monitoreo de seguridad y disponibilidad.
- **PS-04:** Analizar, definir y documentar los esquemas de contingencia y recuperación.
- **PS-05**: Continuar la sensibilización y socialización en seguridad de la información.
- **PS-06**: Continuar el plan de tratamiento de riesgos en la vigencia 2022

La siguiente tabla detalla los proyectos asociados al plan con el objetivo asociado, los proyectos se detallan en las fichas de proyecto que se incluyen más adelante

Proyectos del Plan de Seguridad y Privacidad de la Información
2022

Proyecto	Descripción / Alcance.	Periodo ejecución
Adoptar la arquitectura de referencia de seguridad en nube y en sitio. **PS-01.**	• Servicios del aplicativo ANISCOPIO y Página WEB protegidos por las herramientas definidas en Fase I: Anti DDoS, Front Door y WAF. • Mejoramiento de la seguridad en sitio mediante el afinamiento del firewall y activación del módulo Intrusion Prevention System -IPS. • Gestionar las alertas excepcionales de seguridad de alta complejidad.	Enero – diciembre de 2022 Febrero – Marzo de 2022 Febrero-abril de 2022
Fortalecer la seguridad de los servicios para usuario final – **PS-02.**	• Despliegue o activación de los módulos de Microsoft 365, de la Fase I que se relacionan a continuación: Microsoft defender, AD en nube y cloud security. • Adoptar el uso de doble factor de autenticación para el personal que se vincula a la entidad.	Feb – Julio de 2022 Enero – Dic de 2022
Generación de documentos con guías, políticas específicas y adopción de procesos de monitoreo de seguridad y disponibilidad. **PS-03.**	• Desarrollo y formalización de protocolo de autorización y acceso al centro de cómputo y cuartos técnicos. • Desarrollo de guías para el monitoreo de: ○ Red ○ Seguridad (Firewall y Antivirus) ○ Disponibilidad de recursos físicos. • Revisión, ajuste y formalización del manual de políticas específicas de seguridad.	Ene – marzo de 2022 Marzo – abril de 2022 Abril - mayo de 2022
Analizar, definir y documentar los esquemas de contingencia y recuperación **– PS-4**	Documentar los esquemas de contingencia y recuperación para la plataforma ANIscopio y Página Web.	Febrero – mayo de 2022
Continuar la sensibilización y socialización en seguridad de la información **– PS-05.**	Continuar la sensibilización y socialización en seguridad de la información mediante campaña de sensibilización dirigida a todo el personal y capacitación técnica en seguridad al personal del GIT de Tecnologías de la Información y las Telecomunicaciones – PS-05	Abril -junio de 2022

Proyecto	Descripción / Alcance.	Periodo ejecución
Ejecutar el plan de tratamiento de riesgos de la vigencia 2022 – **PS-06**	Adelantar las actividades tendientes a mitigar los riesgos de seguridad de la información identificados en la entidad y que se detallan en el Plan incluyendo proyectos y macro actividades.	Febrero – Julio de 2022

7.1. FICHAS DE PROYECTO

Las siguientes fichas describen los proyectos que conforman el presente plan.

PS-01. Adoptar la arquitectura de referencia de seguridad en nube y en sitio.

Productos / entregables	• Servicios del aplicativo ANISCOPIO y Página WEB protegidos por las herramientas definidas en Fase I: Anti DDoS, Front Door y WAF y documento de arquitectura de seguridad en la nube; contiene diagrama de elementos de seguridad actuales, riesgos y elementos requeridos para fortalecer la seguridad de los servicios en la nube. • Afinamiento del firewall y módulo Intrusion Prevention System -IPS activo. Evidencia de ajustes en la configuración del firewall, así como de la activación del módulo IPS. • Realizados los ajustes de configuración y corrección de los componentes que generan las alertas de alta complejidad y alertas eliminadas del sistema.
Responsable y recursos involucrados.	Integrantes del equipo de infraestructura TI y seguridad de información del GIT de tecnologías de la información y las telecomunicaciones. -

PS-02: Fortalecer la seguridad de los servicios para usuario final.

Productos / entregables	• Despliegue o activación de: MS Defender for end point para los 505 dispositivos de usuario final que lo requieren, Cloud Security y Azure Active Directory para el 50% de los colaboradores de la ANI, equivalente a 350 usuarios finales (Fase I). • Doble factor de autenticación adoptado para todo nuevo colaborador de la entidad.
Responsable y recursos involucrados.	Integrantes del equipo de infraestructura TI y seguridad de información del GIT de tecnologías de la información y las telecomunicaciones. -

PS-03: Generación de documentos con guías, políticas específicas y adopción de procesos de monitoreo de seguridad y disponibilidad.

Productos / entregables	• Protocolo de autorización y acceso a centro de datos y cuartos técnicos formalizado y adoptado.
	• Actividades de monitoreo documentadas e implementadas, de los siguientes componentes:
	  ○ Red (networking y conectividad)
	  ○ Seguridad (firewall y antivirus)
	  ○ Recursos de servidores críticos (CPU, memoria y disco
	• Manual de políticas específicas formalizado.

Responsable y recursos involucrados.	Integrantes del equipo de infraestructura TI y seguridad de información del GIT de tecnologías de la información y las telecomunicaciones. -

PS-04: Analizar, definir y documentar los esquemas de contingencia y recuperación

Productos / entregables	Documento con el esquema de recuperación y contingencia de servicios de fase I: ANISCOPIO y Pagina web.
Responsable y recursos involucrados.	Integrantes del equipo de infraestructura TI y seguridad de información del GIT de tecnologías de la información y las telecomunicaciones. -

PS-05: Continuar la sensibilización y socialización en seguridad de la información

Productos / entregables	• Campaña de sensibilización realizada y dirigida a todos los colaboradores de la ANI, apoyada en videos, e-card y test de evaluación de asimilación y entendimiento. • Capacitación técnica en seguridad para el personal del GIT de Tecnologías de la Información y las Telecomunicaciones.
Responsable y recursos involucrados.	Integrantes del equipo de infraestructura TI y seguridad de información del GIT de tecnologías de la información y las telecomunicaciones. -

PS-06: Ejecutar el plan de Tratamiento de Riesgos de la vigencia 2022.

Productos / entregables	Los siguientes son los entregables que se generan desde el plan de tratamiento de riesgos: • Nueva versión del instructivo de Copias de Seguridad TI y ajustes aplicados en la operación. • Instructivo de recuperación de servicios ANISCOPIO y Página Web. • MS Defender for endpoint para los 505 dispositivos de usuario final que lo requieren. (Fase I).

	• Documentación y adopción del monitoreo proactivo de eventos que puedan afectar el rendimiento y desempeño de la plataforma, la Fase I la componen las siguientes plataformas: ○ Red (navegación y conectividad) ○ Seguridad (firewall y antivirus) ○ Recursos de servidores críticos (CPU, memoria y disco) • Campaña de sensibilización realizada y dirigida a todo el personal incorporando los siguientes elementos: Video, e-card y test de evaluación. • Jornada de capacitación técnica en seguridad para el personal del GIT de Tecnologías de la Información y las Telecomunicaciones. • Instructivo de gestión de activos en la entidad formalizado. • Actualización de parches así: Servidores: mensualmente, para PC: Mayo-Julio. • Ethical hacking con alcance a la página web y ANISCOPIO y gestión de las vulnerabilidades detectadas.
Responsable y recursos involucrados.	Integrantes del equipo de infraestructura TI y seguridad de información del GIT de tecnologías de la información y las telecomunicaciones. -

8. HOJA DE RUTA.

La siguiente tabla muestra la realización de actividades en el tiempo y acorde al alcance establecido.

Nombre del Proyecto	2022											
	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
PS-1 Adoptar la arquitectura de referencia de seguridad en nube y en sitio.												
Servicio del aplicativo ANISCOPIO y Página WEB protegidos por las herramientas definidas en Fase I: Anti DDoS, Front Door y WAF y documento de arquitectura de seguridad en la nube												
Afinamiento del firewall y activación del módulo Intrusion Prevention System -IPS.												
Ajustes de configuración y corrección de los componentes que generan alertas de alta complejidad y alertas eliminadas.												
PS-02 Fortalecer la seguridad de los servicios para usuario final.												
Despliegue o activación de módulos de seguridad habilitados – Fase I – Alcance: MS Defender for endpoint en 505 dispositivos que lo requieren, Cloud Security y Azure Active Directory para el 50% de los colaboradores (380 personas).												
Doble factor de autenticación adoptado para todo nuevo colaborador de la entidad.												
PS-03 Generación de documentos con guías, políticas específicas y adopción de procesos de monitoreo de seguridad y disponibilidad.												
Protocolo de autorización y acceso a datacenter y centros de cableado formalizado y adoptado.												
Actividades de monitoreo de red (networking y conectividad), seguridad (firewall y antivirus) y recursos de servidores críticos (CPU, memoria y disco) documentadas e implementadas.												

Nombre del Proyecto	2022											
	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
Manual de políticas específicas formalizado												
PS-04 Analizar, definir y documentar los esquemas de contingencia y recuperación.												
Documento de recuperación y contingencia de servicios de fase I: ANISCOPIO y Pagina web.												
PS-05 - Fortalecer el nivel de sensibilidad y conocimientos técnicos en seguridad.												
Jornada de sensibilización dirigida a todo el personal y capacitación técnica en seguridad para el personal del GIT de Tecnologías de la Información y las Telecomunicaciones.												
PS-06 Ejecutar el plan de tratamiento de riesgos de la vigencia 2022												

9. INDICADORES

El cumplimiento del presente plan se mide por indicadores de cumplimiento y eficacia como se muestra a continuación.

INDICADORES DE CUMPLIMIENTO

INDICADOR 01- ADOPTAR LA ARQUITECTURA DE REFERENCIA DE SEGURIDAD EN NUBE Y EN SITIO.		
OBJETIVO		
Medir el número de servicios de seguridad en la nube y en sitio implementadas y optimizadas		
TIPO DE INDICADOR:		
Indicador de Cumplimiento		
DESCRIPCION DE VARIABLES	**META**	**FRECUENCIA DE MEDICION**
Var01: Número de herramientas en nube y en sitio implementadas y optimizadas + alertas de alta complejidad solucionadas.	6	Trimestral
METAS		
CUMPLE: 6	CUMPLE PARCIALMENTE: 5 - 1	NO CUMPLE: 0
OBSERVACIONES		
Para la medición de este indicador se definen 4 servicios y 2 alertas, dentro del alcance: <u>Servicios</u>: • Front door • WAF • Anti DDoS		

• Firewall Alertas: 2 Alertas de alta complejidad solucionadas

INDICADOR 02- IMPLEMENTACION DE MÓDULOS DE SEGURIDAD, FORTALECIMIEENTO DEL PROCESO DE AUTENTICACIÓN.		
OBJETIVO		
Medir el número de servicios y características de seguridad habilitadas a usuarios finales con el alcance definido para la fase I.		
TIPO DE INDICADOR:		
Indicador de Cumplimiento		
DESCRIPCION DE VARIABLES	**META**	**FRECUENCIA DE MEDICION**
Var02 Número de módulos de seguridad en MS-365 activados (Microsoft defender, AD en nube, cloud security y doble factor de autenticación).	4	Trimestral
METAS		
CUMPLE: 4	CUMPLE PARCIALMENTE: 3-1	NO CUMPLE:0
OBSERVACIONES		
Para la medición de este indicador se definen 4 servicios dentro del alcance: Microsoft defender, AD en nube, cloud security y doble factor de autenticación		

INDICADOR 03- DOCUMENTACIÓN DE ESQUEMAS DE CONTROL Y OPERACIÓN DE SEGURIDAD Y DISPONIBILIDAD		
OBJETIVO		
Medir el número de documentos adoptados, en los cuales se basa la ejecución de actividades de control.		
TIPO DE INDICADOR:		
Indicador de Cumplimiento		
DESCRIPCION DE VARIABLES	**META**	**FRECUENCIA DE MEDICION**
Var03: Número de documentos formalizados.	5	Anual
METAS		
CUMPLE: 5	CUMPLE PARCIALMENTE 4 - 1	NO CUMPLE: 0

OBSERVACIONES		

Para la medición de este indicador se definen 5 documentos, que deben estar en su versión final y aprobados por el coordinador del GIT de tecnologías de la Información y las Telecomunicaciones, a saber:
• Protocolo de autorización y acceso a datacenter y cuartos técnicos
  • Red (navegación y conectividad)
  • Seguridad (firewall y antivirus)
  • Recursos de servidores críticos (CPU, memoria y disco)
• Manual de políticas específicas formalizado.		

INDICADOR 04- DOCUMENTACION DE ESQUEMAS DE CONTINGENCIA Y RECUPERACION			
OBJETIVO			
Medir el cumplimiento en la generación y formalización del documento de contingencia y recuperación para los servicios ANISCOPIO y Pagina web.			
TIPO DE INDICADOR:			
Indicador de Cumplimiento			
DESCRIPCION DE VARIABLES		**META**	**FRECUENCIA DE MEDICION**
Var04: Documento generado y adoptado		1	Trimestral
METAS			
CUMPLE	1	NO CUMPLE	0

INDICADOR 05- EJECUCIÓN DE ACTIVIDADES DE SENSIBILIZACION Y CAPACITACIÓN TECNICA EN SEGURIDAD		
OBJETIVO		
Medir la ejecución de la campaña y la actividad de capacitación en seguridad para el personal de ingeniería.		
TIPO DE INDICADOR:		
Indicador de Cumplimiento		
DESCRIPCION DE VARIABLES	**META**	**FRECUENCIA DE MEDICION**
	2	Trimestral

Var05: Ejecución de campaña y jornada de capacitación técnica en seguridad para personal del GIT.			
METAS			
CUMPLE	2	NO CUMPLE	0

INDICADOR DE EFICIENCIA

INDICADOR 05- GESTION DE INCIDENTES DE SEGURIDAD					
OBJETIVO					
Reflejar la gestión de los incidentes reportados sobre seguridad de la información					
TIPO DE INDICADOR:					
Indicador de Gestión.					
DESCRIPCION DE VARIABLES		**FORMULA**		**FRECUENCIA DE MEDICION**	
Var08: Número incidentes gestionados y cerrados Var09: Número total incidentes reportados		(Var08/Var09) *100		Trimestral	
METAS					
Mínima	75-80 %	Satisfactoria	80-90 %	Sobresaliente	100 %

Nota: Se aclara que La gestión de incidentes es medida y reportada como parte de la gestión de operación de servicios de T.I; por lo que este indicador está integrado en el tablero de control de indicadores de la gestión de T.I

10. SOCIALIZACION DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

El plan de Seguridad y Privacidad de la Información es aprobado con la firma y publicación del presente documento con fecha límite el 31 de enero de 2022.

Los mecanismos de socialización del presente plan hacia los interesados son los siguientes:

Tipo de audiencia	Medio de socialización	**Fecha planeada**	Instrumento
Directivos de la entidad	Comité MIPG	Primer semestre 2022	Presentación ejecutiva

Grupo Interno de Trabajo de Tecnologías de la Información y las Telecomunicaciones	Reunión de coordinación y seguimiento	04-02-2022	Documento
Colaboradores Internos	Correo electrónico	18-02-2022	Mensaje informativo / Piezas de comunicación
Colaboradores Externos y Partes Interesadas	Publicación en la página de la entidad	31-01-2022	Documento Plan de Seguridad y Privacidad de la Información.

11. APROBACION.

Nombre	Cargo	Firma
Elaboró	**Oscar Ramírez C** – Contratista GIT Tecnologías de la Información y las Telecomunicaciones.	
Revisó	**Erika Diaz Abella** Contratista GIT Tecnologías de la Información y las Telecomunicaciones.	
Aprobó	**Andrés Francisco Boada** Coordinador G.I.T. Tecnologías de la información y las Telecomunicaciones	
	Diego Alejandro Morales Silva Vicepresidente de Planeación Riesgo y Entorno	