PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN – PESI
Versión 3.0 – 2021-2022

Bogotá D.C., enero de 2022

Elaborado/Actualizado por:	Revisado por:	Aprobado por:
José Hernán Morales M. Consultor STS	Jesús Ríos – Contratista German Suárez – Experto G3-4	Martha Lucía Torres Giraldo Jefe Oficina de Tecnologías de la Información

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Según Gartner Group, los CISO[1] deben transformar sus empresas en organizaciones resilientes y preparadas frente a las siguientes siete tendencias emergentes de ciberseguridad y su impacto potencial[2]:

1. **Los líderes de SRM[3] están creando declaraciones pragmáticas de apetito por el riesgo vinculadas a los resultados comerciales para comprometer a sus partes interesadas de manera más efectiva**. Las consultas de los clientes de Gartner han demostrado que uno de los desafíos más serios para los líderes de SRM es la incapacidad de comunicarse efectivamente con los líderes empresariales. A pesar de que los CISO están más involucrados en reuniones estratégicas, los líderes empresariales a menudo no pueden evaluar si una tecnología o proyecto está creando demasiado riesgo y exposición o si la organización está perdiendo oportunidades por ser demasiado reacia al riesgo.

2. **Existe un renovado interés en implementar o madurar centros de operaciones de seguridad (SOC[4]) con un enfoque en la detección y respuesta de amenazas**. Dada la creciente complejidad y el impacto de los ataques de ciberseguridad, y la creciente complejidad de las herramientas de seguridad que generan alertas, las organizaciones buscan construir o revitalizar los SOC o tercerizar esta función. Para 2022, el 50% de todos los SOC se transformarán en SOC modernos con capacidades integradas de respuesta a incidentes, inteligencia de amenazas y búsqueda de amenazas, en comparación con menos del 10% en 2015. Las organizaciones ahora están invirtiendo en herramientas que son más sensibles y se están centrando en un equilibrio entre respuesta y detección versus prevención.

3. **Las organizaciones líderes están utilizando un marco de gobierno de seguridad de datos para priorizar las inversiones en seguridad de datos.** La seguridad de los datos no es simplemente un problema tecnológico. La seguridad efectiva de los datos puede requerir un marco de gobierno de seguridad de datos para proporcionar un modelo centrado en los datos que identifique y clasifique conjuntos de datos estructurados y no estructurados en todos los activos informáticos empresariales y defina políticas de seguridad de datos. Una vez que los SRM han abordado la estrategia comercial y la tolerancia al riesgo, el marco puede usarse como guía para priorizar las inversiones en tecnología

[1] CISO, Chief Information Security Officer
[2] GARTNER GROUP, Gartner top 7 security and risk trends for 2019
[3] SRM, Security and Risk Management
[4] SOC, Security Operation Center

4. **La autenticación "sin contraseña" está penetrando el mercado, impulsada por la demanda y la disponibilidad de datos biométricos y métodos sólidos de autenticación basados en hardware**. Eliminar las contraseñas ha sido un objetivo de larga data, pero solo ahora está comenzando a lograr una tracción real en el mercado. Las contraseñas son un imán para los atacantes y son susceptibles a una variedad de ataques como ingeniería social, phishing, relleno de credenciales y malware.

   Los estándares emergentes sin contraseña y la mayor disponibilidad de dispositivos que admiten métodos de autenticación sin contraseña están impulsando una mayor adopción. La biometría se ha vuelto cada vez más popular como método "sin contraseña" para una identificación más sólida, pero otras opciones incluyen tokens de hardware, teléfono como token, Identity Online rápido y análisis basados en comportamientos pasivos.

5. **Los proveedores de productos de seguridad están ofreciendo cada vez más servicios premium para ayudar a los clientes a obtener un valor más inmediato y para ayudar en el desarrollo de habilidades**. Se espera que el número de roles de seguridad cibernética no cubiertos en todo el mundo crezca de 1 millón en 2018 a 1.5 millones para fines de 2020. Las organizaciones están luchando para cumplir roles y pueden encontrar un desafío en retener a los empleados actuales. Al mismo tiempo, la proliferación y complejidad del software de seguridad está aumentando. Algunas tecnologías, especialmente aquellas que usan IA[5], requieren un monitoreo o investigación constante por parte de un experto en seguridad humana.

   Es posible que pronto no haya suficientes personas capacitadas para usar los productos. Como resultado, los proveedores ofrecen cada vez más servicios premium que combinan productos con implementación, configuración y servicios operativos continuos. Esto significa que los proveedores pueden ayudar a los clientes a obtener un valor más inmediato de las herramientas y las organizaciones pueden mejorar su gestión.

6. **Las organizaciones líderes están invirtiendo y madurando su competencia de seguridad en la nube a medida que se convierte en la plataforma informática principal**. A medida que las organizaciones se involucren cada vez más en plataformas basadas en la nube, los equipos de seguridad verán una variedad y complejidad cada vez mayores en lo que respecta a la seguridad en la nube.

[5] IA, Inteligencia Artificial

Las organizaciones líderes están estableciendo un equipo de centro de excelencia en la nube e invirtiendo en personas, procesos y herramientas para dominar este entorno que cambia rápidamente. Las herramientas como los Agentes de Seguridad de Acceso a la Nube (CASB), la Gestión de la Postura de Seguridad en la Nube (CSPM) y las Plataformas de Protección de la Carga de Trabajo en la Nube (CWPP) ofrecen capacidades de seguridad en la nube superpuestas para abordar los riesgos, pero las organizaciones también deben invertir en personas y procesos, como adoptar un estilo de trabajo SecDevOps[6]

7. **El enfoque estratégico de CARTA para la seguridad está comenzando a aparecer en los mercados de seguridad más tradicionales.** La Confianza y Evaluación Continua de Riesgo Adaptativo (CARTA) es un enfoque estratégico de la seguridad que reconoce que no existe una protección perfecta y que la seguridad debe ser adaptativa, en todas partes, todo el tiempo.

   La seguridad tradicional de la red LAN y la seguridad del correo electrónico son dos mercados que están comenzando a adoptar una mentalidad CARTA al enfocarse en las capacidades de detección y respuesta dentro del perímetro.

La transición de un modelo de seguridad tradicional a un modelo de seguridad adaptativa no es rápida puesto que es necesario contar con personal más capacitado y adecuadas herramientas de gestión para adoptar un esquema de seguridad centrada en las personas y basada en la confianza que son las exigencias del nuevo mundo digital.

Mientras las organizaciones dan el giro hacia un modelo de seguridad adaptativa se debe continuar con el fortalecimiento de la protección de los activos de información y trabajar en tres términos comunes que se utilizan de manera indistinta: Ciberseguridad, Seguridad informática y seguridad de la información; sin embargo, cada uno tiene sus alcances bien delimitados:

ISACA[7] define ciberseguridad como:

> *"Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".*

En ese orden de ideas, la ciberseguridad tiene como objetivo la protección de la información digital que vive en los sistemas interconectados, muy relacionado con el de seguridad informática que involucra los métodos, procesos o técnicas para el tratamiento

[6] SecDevOps, Nuevo paradigma para el diseño y desarrollo de código seguro
[7] ISACA, www.isaca.org

automático de la información en formato digital y extendiéndose a la protección de las redes e infraestructura tecnológica.

El propósito de la seguridad en todos sus ámbitos de aplicación es la reducción de riesgos hasta un nivel aceptable para los interesados en mitigar las amenazas latentes. Puesto que la información se puede encontrar de diferentes formas (digital, física o abstracta) y en diferentes estados (almacenada, procesada o transmitida), el ámbito de la **seguridad de la información** es brindar protección a la misma sin importar su forma o estado, por tanto, la seguridad informática y la ciberseguridad están contenidos dentro de la seguridad de la información.

El presente documento recoge los resultados de los diagnósticos de seguridad de la información realizados en 2019 y 2020 en la Agencia Nacional de Hidrocarburos – ANH y propone un plan de acción para el fortalecimiento y transformación de la función de seguridad de la información en la entidad.

2. DEFINICIONES Y TERMINOLOGÍA

- **Activo de Información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización[8].
- **Activos de información críticos:** Activos de información imprescindibles o de valor clave para la operación de la entidad. Cuando se trate de activos informáticos se entenderán como aquellos dispositivos tecnológicos que permiten la emisión, transmisión, procesamiento y recepción de información[9].
- **Acuerdo de confidencialidad:** Conocido también como acuerdo de no divulgación, es un documento formal entre al menos dos partes interesadas, para compartir información considerada como confidencial, pero restringida para el uso público con el fin de proteger secretos industriales[10]
- **Acuerdos de niveles de servicio (ANS o SLA Service Level Agreement por su sigla en inglés)**: Es un acuerdo entre un proveedor de servicios de tecnología de la información (TI) y un cliente. Un ANS describe el servicio de TI, documenta las metas de niveles de servicio y especifica las responsabilidades del proveedor de servicios de TI y del cliente. Un único ANS puede cubrir varios servicios de TI o múltiples clientes[11].
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización[12].

[8] ISO 27000:2018
[9] Ibidem
[10] Ley 256 de 1996, artículo 9, el cual define secretos empresariales y consecuencias de su divulgación no autorizada.
[11] ITIL
[12] Ibidem

- **Análisis de riesgo:** Proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo[13].
- **Bluetooth:** Estándar de transmisión de datos inalámbrico vía radiofrecuencia de corto alcance (unos 10 metros). Entre otras muchas aplicaciones, permite la comunicación entre videocámaras, celulares y computadoras que tengan este protocolo, para el intercambio de datos digitalizados (vídeo, audio, texto)[14]
- **Centro de Datos o Centro de Cómputo**: Espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización. Dichos recursos consisten esencialmente en áreas debidamente acondicionadas, computadoras y redes de comunicaciones[15].
- **Ciber:** Ciber o Cyber. Prefijo utilizado ampliamente en la comunidad Internet para denominar conceptos relacionados con las redes (cibercultura, ciberespacio, cibernauta, etc.). Su origen proviene del griego "cibernao" que significa "pilotar una nave"[16].
- **Cibernético:** Término acuñado por un grupo de científicos dirigidos por Norbert Wiener y popularizado por su libro "Cybernetics or Control and Communication in the Animal and the Machine" de 1948[17]. Ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas.
- **Cifrar**: Transcribir en guarismos (número arábigos), letras o símbolos, de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger[18].
- **Cloud Computing:** Concepto tecnológico que se basa en que las aplicaciones o software y los equipos o hardware con capacidad de proceso y almacenaje de datos están ubicados en un Centro de Datos que permite a los usuarios acceder a las aplicaciones y servicios disponibles a través de Internet o como se conoce coloquialmente, a través “la Nube” de Internet.[19]
- **Confidencialidad:** Propiedad de que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados[20].
- **Control de acceso:** El proceso de otorgar o denegar solicitudes específicas para: 1) obtener y usar información y servicios de procesamiento de información relacionados; y 2) ingresar a instalaciones físicas específicas (por ejemplo, edificios gubernamentales, establecimientos militares, centros de cómputo, otros)[21].
- **Correo electrónico (e-mail)**: El e-mail o email, del inglés electronic mail (correo electrónico), ha sido uno de los medios de comunicación de más rápido crecimiento en la historia de la humanidad. Por medio del protocolo de comunicación TCP/IP, permite el intercambio de mensajes entre las personas conectadas a la red de manera similar al correo tradicional[22].

[13] Ibidem
[14] NIST, Computer Security Resource Center - Glossary
[15] Ibidem
[16] Ibidem
[17] Ibidem
[18] Real Academia Española
[19] Guía 12 Seguridad en la Nube, MinTIC
[20] Ibidem
[21] NIST 800-12, An Introduction to Information Security
[22] www.internetglosario.com

- **Custodia:** Acción de guardar con cuidado y vigilancia una información o mensaje[23].
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[24].
- **Estimación de riesgos**: Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable[25].
- **Evaluación de riesgos**: Proceso global de identificación, análisis y estimación de riesgos en la operación de la entidad[26].
- **Incidente de seguridad**: Evento único o serie de eventos inesperados, no deseados, que poseen una probabilidad significativa de comprometer las operaciones de la entidad y amenazar la Seguridad de la Información[27].
- **Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen[28].
- **Información pública**: Es toda información que un sujeto obligado genere, obtenga, adquiera o controle en su calidad de tal[29].
- **Información pública clasificada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 de 2014[30].
- **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014[31].
- **Impacto**: Nivel de afectación de un servicio o negocio por una anomalía[32].
- **Infraestructura**: Conjunto de elementos, dotaciones o servicios necesarios para el buen funcionamiento de un país, de una ciudad o de una organización cualquiera[33]. Conjunto de activos o recursos técnicos, servicios o instalaciones que se consideran necesarios para el desarrollo normal de procesos o actividades.
- **Infraestructura Crítica Cibernética (ICC):** Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de

[23] Real Academia Española
[24] ISO 27000:2018
[25] Ibidem
[26] Ibidem
[27] Ibidem
[28] Ley 1712 de 2014
[29] Ibidem
[30] Ibidem
[31] Ibidem
[32] Ibidem
[33] Real Academia Española

Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales[34].

- **Integridad:** Propiedad de la información relativa a su exactitud y completitud[35].
- **IoT:** Del inglés Internet of Things - Internet de las Cosas. Comprende la tecnología en la que se interconectan dispositivos u objetos cotidianos, mediante internet[36].
- **MSPI:** Modelo de Seguridad y Privacidad de la Información. Ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información[37]
- **NFC (Near Field Communication)**: Tecnología de comunicación inalámbrica de corto alcance que facilita el intercambio de información entre dispositivos como smartphones y tablets[38].
- **No repudio:** El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido)[39].
- **Plan de continuidad del negocio (BCP):** Una colección documentada de procedimientos e información que se desarrolla, compila y mantiene preparada para su uso en un incidente para permitir que una organización continúe entregando sus productos y servicios críticos a un nivel predefinido aceptable[40]**.**
- **Plan de recuperación de desastres (DRP):** Un plan escrito para recuperar uno o más sistemas de información en una instalación alternativa en respuesta a una falla importante de hardware o software o la destrucción de instalaciones[41]
- **Política:** Documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información[42].
- **Privacidad:** Se entiende como el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar que genera la obligación de proteger dicha información en observancia del marco legal vigente[43].
- **Responsables por la seguridad de la información:** Son los funcionarios de carrera administrativa, en provisionalidad, contratistas, pasantes y/o judicantes, visitantes y terceros que tengan acceso o gestionen información de la ANH. En el presente documento se pueden encontrar, con el mismo significado, referencias a servidores públicos, contratistas, colaboradores y/o terceros.

[34] Fuente: Ministerio de Defensa.
[35] ISO 27000:2018
[36] www.internetglosario.com
[37] Mintic
[38] NIST, Computer Security Resource Center - Glossary
[39] Ibidem
[40] www.drii.org/glossary
[41] NIST 800-34
[42] MINTIC, Modelo de Seguridad y Privacidad de la Información, Guía 2 Elaboración de la Política General de Seguridad y Privacidad de la Información
[43] MINTIC, Modelo de Seguridad y Privacidad de la Información - MSPI

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias[44].
- **Rootkit:** Un conjunto de herramientas utilizadas por un atacante después de obtener acceso de nivel raíz a un host para ocultar las actividades del atacante en el host y permitir que el atacante mantenga el acceso de nivel raíz al host a través de medios encubiertos[45].
- **Sanitización:** Proceso para eliminar información de los medios de modo que la recuperación de información no sea posible. Incluye eliminar todas las etiquetas, marcas y registros de actividad[46].
- **Seguridad de la información:** La protección de la información y los sistemas de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados para proporcionar confidencialidad, integridad y disponibilidad[47].
- **Servicio Esencial:** El servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la educación, la seguridad, el bienestar social y económico de una comunidad, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas[48].
- **Sujetos obligados:** Cualquier persona física o jurídica colectiva que reciba y ejerza recursos públicos en el ámbito estatal o municipal; y, cualquier otra autoridad, entidad, órgano u organismo de los poderes estatal o municipal, que reciba recursos públicos[49].
- **Tecnología de la Información (TI):** Es el uso de la tecnología para el almacenamiento, la comunicación o el procesamiento de la información. Típicamente, la tecnología incluye computadores(as), telecomunicaciones, aplicaciones y otro software. La información puede incluir datos del negocio, voz, imágenes, vídeo, etc. A menudo, la tecnología de la información se utiliza para apoyar los procesos de negocio a través de servicios de TI[50].
- **Tecnología Operacional (T.O.):** Hardware y software que detecta o causa un cambio a través del monitoreo directo y / o control de dispositivos físicos, procesos y eventos en la empresa[51].
- **Vulnerabilidad.** Debilidad de un activo o control que puede ser explotada por una o más amenazas[52]
- **WiFi:** Abreviatura en inglés para "wireless fidelity". Un tipo de red inalámbrica (WLAN - wireless local area networks), que usa el protocolo inalámbrico de alcance limitado IEEE 802.11b, que transmite datos en banda ancha en el rango espectral de 2.4 GHz[53].

3. OBJETIVO

[44] ISO 27000:2018
[45] NIST, Computer Security Resource Center - Glossary
[46] Ibidem
[47] Ibidem
[48] Fuente: Ministerio de Defensa. Adaptación Ley 8/2011-Gobierno de España.
[49] Ley 1712 de 2014
[50] ITIL
[51] NIST, Computer Security Resource Center - Glossary
[52] ISO 27000
[53] NIST, Computer Security Resource Center - Glossary

Definir el plan estratégico de seguridad de la información (PESI) de la ANH, liderado por la Oficina de Tecnologías de la Información – OTI, que se recomienda desarrollar hasta la vigencia 2022, para la transformación y fortalecimiento de la seguridad de la información de la entidad alineada a las nuevas tendencias, que permitan la respuesta efectiva y oportuna ante los nuevos retos en esta materia.

4. OBJETIVOS ESPECIFICOS

- Presentar el estado actual de avance en la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información de la ANH y definir los pasos a seguir.

- Fortalecer la gobernabilidad de seguridad y privacidad de la información, mediante la estructuración de un modelo de trabajo claramente definido y articulado que permita la ejecución, revisión y mejora del Sistema de Gestión de Seguridad de la Información -SGSI

- Incrementar el nivel de capacidad del proceso de seguridad de la información mediante la optimización de la gestión de los riesgos de la información y la tecnología.

- Implementar los instrumentos requeridos en lineamientos y directrices gubernamentales, la estrategia de Gobierno Digital y la normatividad relacionada en seguridad de la información y protección de datos personales para mantener el nivel de cumplimiento.

- Definir los proyectos a realizar durante el siguiente bienio en seguridad y privacidad de la información.

5. ALCANCE

El PESI definido tiene como finalidad la protección de la información de todos los procesos incluidos en el mapa de procesos de la ANH[54] y para ello cubre tres frentes:

- Seguridad de la información (SI)
- Seguridad informática (ST)
- Ciberseguridad (CI)

Marco Normativo

Interno:

- ✓ Política General de Seguridad y Privacidad de la Información de la ANH.
- ✓ Manual de Políticas Específicas de Seguridad y Privacidad de la Información de la ANH
- ✓ Resolución 266 de 2018 – Adopción del Sistema de Gestión de Seguridad de la Información.
- ✓ Resolución 415 de 2016 – Comité de Seguridad de la Información.

[54] Agencia Nacional de Hidrocarburos – ANH, Mapa de procesos

Externo:

- ✓ Directrices y Guía PESI emitida por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC.
- ✓ Modelo de Seguridad y Privacidad de la información v3.0.2., Guía 5 Gestión clasificación de activos y Guía 21 Gestión de Incidentes
- ✓ Decreto 612 de 2018 – Integración Planes Institucionales, Función Pública
- ✓ Decreto 1008 de 2018 – Política de Gobierno Digital y Manual versión 7.
- ✓ Norma ISO 27001:2013.
- ✓ Resolución 1581 de 2012 y Decreto Reglamentario 1377 de 2013 – Protección de Datos Personales.
- ✓ Directrices emitidas por la Superintendencia de Industria y Comercio – SIC en materia de Datos Personales.
- ✓ Buenas prácticas y normatividad vigente sobre la materia.

6. SITUACIÓN ACTUAL

Conforme la traza de diagnósticos del estado de la implementación del Modelo de Seguridad y Privacidad de la Información en la ANH, se han venido planteando las acciones para reducir la brecha, estableciendo en el Plan de Seguridad y Privacidad de la Información aquellas acciones que por disponibilidad de tiempo o recursos no se lograron completar en vigencias anteriores así como las propuestas para continuar la implementación acorde con la realidad de la Entidad, teniendo como prioritarios los dominios con más oportunidad de mejora.

Así las cosas, en la vigencia 2020 debido a varios factores como la emergencia sanitaria y el escaso personal en la Oficina de Tecnologías de la Información, el porcentaje de avance del plan formulado fue del 74%, quedando actividades parcialmente realizadas o sin avances. En este sentido se identifica como reto o amenaza dicha emergencia sanitaria, ya que obligó a la realización de la totalidad de las acciones de manera virtual en pro de la salud y bienestar de los servidores y colaboradores de la ANH. Sin embargo para la vigencia 2021 el avance del plan fue del 86%.

Es importante destacar que según lo establecido en el Comité de Seguridad de la información en las sesiones de la vigencia 2020, para la vigencia 2021 se oficializaría la integración de este Comité al de Gestión Institucional y Desempeño, actividad pendiente para la vigencia 2022.

Para el éxito de las acciones propuestas se requiere la anuencia, concurso y colaboración de personal de otras áreas cuando sea convocado y de los colaboradores de seguridad de la información, que permita solventar tareas diarias, adicionales, emergentes y las propuestas en el presente plan, que garantice el cumplimiento de los lineamientos relacionados con Seguridad de la Información.

7. PLAN ESTRATEGICO DE SEGURIDAD DE LA INFORMACION - PESI

El plan estratégico de seguridad de la información (PESI) de la ANH se plantea de acuerdo con lo recomendado por COBIT[55], que se resume en que los objetivos de gobierno y gestión de la información y la tecnología se alineen con los objetivos empresariales. Para el caso puntual de seguridad de la información, el alineamiento propuesto por COBIT se observa en la siguiente tabla:

Objetivo de gobierno y gestión	Metas de Alineamiento	Objetivos Empresariales
DSS05 Gestionar los servicios de seguridad	AG02 Gestión del riesgo relacionado con información y tecnología AG07 Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad.	EG02 Gestión de riesgo del negocio EG06 Continuidad y disponibilidad del servicio del negocio
Practicas claves de gestión • Proteger contra el software malicioso • Gestionar la seguridad de la red y conectividad • Gestionar la seguridad de punto final • Gestionar la identidad del usuario y acceso lógico • Gestionar el acceso físico a los activos de información y tecnología • Gestionar los documentos sensitivos y dispositivos de salida • Gestionar las vulnerabilidades y monitorear la infraestructura para los eventos relacionados con la seguridad		

El Plan Estratégico de Seguridad de la Información (PESI) definido tiene las siguientes características:

- Se organiza como un programa compuesto por 13 proyectos.
- El portafolio de proyectos que lo conforman se estimó para un panorama a dos años. En 2022 el plan se debe revisar y formular uno nuevo acorde a los proyectos ya implementados y a las circunstancias existentes.
- Pretende disminuir las brechas identificadas en los informes de diagnóstico y análisis GAP de seguridad y privacidad de la información, y, encaminar la agencia hacia las nuevas tendencias de seguridad que exige el mundo digital.
- Requiere de la participación de la alta dirección, y de todos los colaboradores de la entidad.

A continuación, se presenta el programa organizado por proyectos, el valor de cada proyecto y el lapso de implementación por trimestres:

[55] COBIT 2019, Governance and Management Objectives

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - 2021-2022

PROYECTO No.	PROD/SERV	TITULO DEL PROYECTO	FRENTE	2021				2022			
				Trim.1	Trim.2	Trim.3	Trim.4	Trim.1	Trim.2	Trim.3	Trim.4
1	SERVICIO	P1. Fortalecimiento del Sistema de Seguridad de la Información y Ciberseguridad	SI			X	X	X	X	X	
2	PRODUCTO	P2. Fortalecimiento del sistema de seguridad adaptativa.	ST			X	X	X	X		
3	SERVICIO	P3. Fortalecimiento de la gestión del riesgo en materia de Seguridad y Privacidad de la Información en la entidad	SI			X	X	X	X		
4	PRODUCTO	P4. Implementación de herramientas de análisis de comportamiento en el uso de servicios y herramientas informáticas	ST				X	X	X	X	
5	PROD/SERV	P5. Aseguramiento de Servicios en la Nube	CI			X	X	X	X		
6	PRODUCTO	P6. Implementación de solución automatizada para la hardenización de infraestructura tecnológica.	ST					X	X	X	X
7	PROD/SERV	P7. Implementación de herramientas y procedimientos para desarrollo seguro	ST					X	X	X	X
8	PRODUCTO	P8. Implementación de una solución para aseguramiento y gestión de cuentas privilegiadas	ST						X	X	X
9	SERVICIO	P9. Implementación de mecanismos para protección de marca de la ANH	ST					x	x	x	x

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD - 2021-2022

PROYECTO No.	PROD/SERV	TITULO DEL PROYECTO	FRENTE	2021				2022			
				Trim.1	Trim.2	Trim.3	Trim.4	Trim.1	Trim.2	Trim.3	Trim.4
10	SERVICIO	P10. Fortalecimiento de gestión integral de activos tecnológicos en la CMDB	SI					X	X	X	X
11	PRODUCTO	P11. Implementación de solución de acceso a información sensible	ST						X	X	X
12	PRODUCTO	P12. Implementación de solución de seguridad inalámbrica	ST							X	X
13	SERVICIO	P13. Implementación del Sistema de Gestión de Resiliencia Organizacional	SI						X	X	X

NOTA: Convención de los Frentes
SI: Seguridad de la Información.
ST: Seguridad Informática.
CI: Ciberseguridad

A continuación, se presenta la ficha de cada proyecto: (El presupuesto incluye tanto servicios como las soluciones requeridas en cada caso que aplique)

PROYECTO	**P1. Fortalecimiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad**
JUSTIFICACION	El SGSI no ha tenido continuidad en su implementación, se identifica que las políticas no están aprobadas y deben ser actualizadas, el comité de seguridad de la información no se ha podido reunir en el último año, es necesario incluir el componente de ciberseguridad, así como ajustar los procedi-

PROYECTO	**P1. Fortalecimiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad**
	mientos asociados, no se cuenta actualmente con una declaración de aplicabilidad donde se refleje el nivel de madurez de los controles establecidos basado en Anexo ISO 27002.
OBJETIVO DEL PROYECTO	Tomar las acciones correspondientes con respecto a marcos individuales y hacer las inversiones de infraestructura, servicios profesionales y consultorías de mejores prácticas para cerrar la brecha de una manera progresiva en el marco de la seguridad de la información y ciberseguridad.
ALCANCE	1) Revisión, actualización, adaptación e implementación de las políticas y procedimientos de seguridad de la información, privacidad de la información y ciberseguridad, basado en los lineamientos de las buenas prácticas IS0 27001, ISO 27032. 2) Realizar campañas de sensibilización, concienciación y capacitación en seguridad, privacidad y ciberseguridad de la información, extendiéndola a proveedores críticos y contratistas. 3) Hacer revisión del sistema actual, realizar las consultorías de verificación según los procesos de información crítica para certificar el sistema de gestión de seguridad de la información enfocado en procesos misionales y de apoyo que manejen información sensible. 4) Establecer y gestionar la Declaración de aplicabilidad - SOA de SGSI. 5) Dar cumplimiento al marco normativo y regulatorio sobre lineamientos que genere MINTIC sobre el uso de Computación, integrando y actualizando el MSPI. 6) Actualizar el documento de gestión de riesgos de seguridad de la información para incluir la gestión de riesgos de ciberseguridad que se basa en el análisis de amenazas y vulnerabilidades. 7) Definir y conformar el equipo de respuesta a incidentes 8) Fortalecer el Uso y apropiación de las políticas y procedimientos de seguridad y privacidad de la información, Protección de datos. 9) Aseguramiento de la aplicación de las buenas prácticas de la ISO 27001 y el Anexo 27002, ISO 27032, ISO 27018, ISO 27017. 10) Robustecer las auditorias al Sistema de gestión de seguridad de la información y ciberseguridad, extendiéndola a los proveedores o terceros de servicios críticos. 11)Establecer la estructura y recursos necesarios para la gestión de la seguridad de la información, ciberseguridad, privacidad y protección de datos. 12) Diseñar y establecer los indicadores que permitan evaluar la eficacia y eficiencia de la gestión de ciberseguridad, seguridad de la información y protección de datos. 13) Establecer un procedimiento para la recolección de evidencia digital on premise y nube.

PROYECTO	**P1. Fortalecimiento del Sistema de Gestión de Seguridad de la Información y Ciberseguridad**
	14) Implementar los procesos relacionados con la gestión y el gobierno de los servicios TI para la gestión de los riesgos asociados con la aplicación de cambios en los negocios críticos o clientes que afecten a las aplicaciones (virtuales), las interfaces de los sistemas (APIs), las configuraciones y diseños, así como a la infraestructura de red y a los componentes del sistema, integrando a los proveedores de nube. 15) Integrar el procedimiento de gestión de cambios, basados en una validación de los resultados esperados en el entorno, que se establezca una preautorización de la dirección adecuada, y que se produzca la notificación, así como la autorización de los clientes, según el acuerdo de nivel de servicio (OLA). 16) Articular el plan de gestión de incidentes con el plan de recuperación de desastres - DRP en caso de que sea un incidente catastrófico. 17) El plan de gestión de seguridad de la información y el plan de tratamiento de riesgos pueden tener actividades comunes no necesariamente cruzadas, la gestión de riesgos debe dar la prioridad de implementación de esas actividades de control.
TIEMPO	18 meses.
PRESUPUESTO	980.000.000,00

PROYECTO	**P2. Fortalecimiento del sistema de seguridad adaptativa.**
JUSTIFICACION	Con el fin de aplicar acciones que apoyen la mitigación de riesgos de seguridad y ciberseguridad de la información, se requiere implementar un esquema de defensa en profundidad que cuente con análisis de comportamiento, inteligencia artificial, escaneo para aprendizaje (machine learning), que permitan reducir la vulnerabilidad a las amenazas que puedan presentarse en estaciones de trabajo.
OBJETIVO DEL PROYECTO	Automatizar y mejorar la postura de seguridad con herramientas y soluciones de protección de amenazas emergentes a nivel perimetral y a nivel de estaciones de trabajo.

ALCANCE	Algunas de las soluciones propuestas para este fortalecimiento son: 1) Orquestador de seguridad y Automatización de respuestas - SOAR 2) Solución de Control de Acceso a la Red (NAC) para aseguramiento de control a la red por parte de usuarios locales, externos, proveedores y dispositivos BYOD. 3) Solución Antivirus con funcionalidad EDR (Endpoint Defense and Response) 4) Sistema de autenticación de doble factor para usuarios y aplicaciones usando Single Sign On para aseguramiento de conexiones de usuarios remotos a servicios y aplicaciones de la entidad. Es el proceso en el cual se verifica la identidad de un cliente, entidad o usuario, en función de uno o varios factores de autenticación y consiste en verificar que el usuario es quien dice ser. Ejemplos de estos métodos son la autenticación de doble factor con token (de software o hardware) o pin a celular.
TIEMPO	12 meses
PRESUPUESTO	1.790.000.000,00

PROYECTO	**P3. Fortalecimiento de la gestión del riesgo en materia de Seguridad y Privacidad de la Información en la entidad**
JUSTIFICACION	Permitir la administración y seguimiento de la seguridad de la información y del marco de trabajo de ciberseguridad, mediante la administración de los activos de información y la gestión de los riesgos de ciberseguridad.
OBJETIVO DEL PROYECTO	Mantener un sistema de gestión, gobierno y cumplimiento de riesgos para lograr los objetivos estratégicos de la entidad.
ALCANCE	Las actividades o funcionalidades mínimas para desarrollar son: 1) Aumentar el nivel de madurez en cuanto a gobierno, riesgo y cumplimiento. 2) Capacitar, socializar, sensibilizar, desarrollar capacidades en gestión de riesgo corporativo. 3) Mantener actualizados y evaluados permanentemente los riesgos, mediante formalización planes de trabajo periódicos de gestión y seguimiento.
TIEMPO	12 meses
PRESUPUESTO	450.000.000,00

PROYECTO	**P4. Implementación de soluciones de análisis de comportamiento en el uso de servicios y herramientas informáticas**
JUSTIFICACION	Ante la constante situación de amenazas persistentes, la complejidad del malware y el tráfico malicioso se hace necesario implementar herramientas de análisis de comportamiento (machine learning) que le permitan a la entidad tomar acciones contra estos patrones anómalos no identificados.
OBJETIVO DEL PROYECTO	Bloquear comportamientos anómalos en la red y en los sistemas de la ANH
ALCANCE	Como mínimo se debe implementar las siguientes soluciones: 1) Establecer un Servicio o mecanismos de análisis de comportamiento de red (Network Behavior analytics), que permiten definir y monitorear líneas base de comportamiento de red, el monitoreo sobre anomalías, altos consumos, mayores aplicaciones usadas, e Indicador de compromiso (IoC) que conlleve hacia un fraude o malware avanzado. 2) Establecer un servicio o mecanismos de Análisis de comportamiento del usuario (User behavior analytics) que permita monitorear y detectar anomalías, las cuales pueden llevar a fraude, bien sea intencionales o por algún ente externo que esté usando una credencial de usuario de la entidad.
TIEMPO	12 meses
PRESUPUESTO	600.000.000,00

PROYECTO	**P5. Aseguramiento de Servicios en la Nube**
JUSTIFICACION	Protección de infraestructura y aplicaciones alojadas en servicios Cloud.
OBJETIVO DEL PROYECTO	Protección de usuarios finales y los servicios que son consumidos desde la nube de Microsoft de ataques cibernéticos
ALCANCE	Las soluciones propuestas a tener en cuenta son: 1) Firewall de Nueva Generación (NGFW Cloud) para aseguramiento perimetral de los servidores en la nube 2) Implementación de soluciones de seguridad de nube (CASB, CWPP, CSPM) 3) Implementar y monitorear una solución de WAF para las aplicaciones expuestas en el ciberespacio. 4) Implementar mecanismos de protección sobre correo electrónico corporativo - MS Office 365. 5) Fortalecer el aseguramiento en el uso y adaptación a entornos de computación en la nube con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

TIEMPO	12 meses
PRESUPUESTO	900.000.000,00

PROYECTO	**P6. Implementación de solución automatizada para la hardenización de infraestructura tecnológica.**
JUSTIFICACION	Se requiere asegurar la gestión de plantillas de seguridad en la plataforma tecnológica con el fin de conseguir configurar un sistema informático de manera segura y eliminar aplicaciones y servicios innecesarios.
OBJETIVO DEL PROYECTO	Asegurar la plataforma tecnológica con el fin de encontrar fallas en el sistema para priorizar los ajustes y parcheo de vulnerabilidades.
ALCANCE	El alcance mínimo se enmarca en: 1) Establecer estándares de seguridad (hardening). 2) Configuraciones recomendadas por el fabricante en la aplicación o dispositivo, con el objetivo de no dejar parámetros con valores que deja el fabricante por defecto. 3) Cada sistema operativo deberá ser fortalecido para proporcionar sólo los puertos necesarios, protocolos y servicios para satisfacer las necesidades del negocio y tener vigentes los controles técnicos de apoyo tales como: antivirus, integridad de los ficheros de monitorización y el inicio de sesión como parte de su línea base de operativa estándar o plantilla. 4) Realizar el endurecimiento de infraestructura a nivel de: servidores, bases de datos, aplicaciones, elementos activos de red. (ej. Tripwire).
TIEMPO	12 meses
PRESUPUESTO	435.000.000,00

PROYECTO	**P7. Implementación de herramientas y procedimientos para desarrollo seguro**
JUSTIFICACION	Fortalecer la seguridad en el ciclo de vida de sistemas de información.
OBJETIVO DEL PROYECTO	Asegurar los sistemas de información de la ANH publicados en la WEB (intranet e internet) utilizando metodologías de desarrollo seguro.
ALCANCE	Las actividades mínimas para desarrollar son: 1) Aseguramiento de pruebas no funcionales a través de (análisis de vulnerabilidades, análisis de stress o carga, EH, verificación de código seguro). Se plantea una solución similar a Fortify para análisis de código estático. 2) Establecer procedimientos y herramientas para la construcción, adquisición, mantenimiento y desarrollo seguro de aplicaciones, APPS, APIS y Sistemas de Información 3) Evaluar prácticas de ingeniería DevOps y DevSecOps para contemplar la

	tolerancia al riesgo y realizar el análisis de beneficio, se debe capacitar y exigir el uso de esta metodología
TIEMPO	12 meses
PRESUPUESTO	400.000.000,00

PROYECTO	**P8. Implementación de una solución para aseguramiento y gestión de cuentas privilegiadas**
JUSTIFICACION	No se tiene control sobre las acciones de cuentas privilegiadas, por lo cual no se puede realizar la trazabilidad o rastreo sobre los eventos reportados frente a un incidente de seguridad informática.
OBJETIVO DEL PROYECTO	Asegurar y monitorear las acciones de las cuentas privilegiadas en las plataformas tecnológicas críticas de la ANH
ALCANCE	Las actividades mínimas para desarrollar son: 1) Monitorear la gestión de usuarios privilegiados de las plataformas tecnológicas (Key Power Management) 2) Implementar el uso de las herramientas para gestionar usuarios privilegiados en nube o herramientas propias de los proveedores de nube, como la administración sobre Office 365.
TIEMPO	9 meses
PRESUPUESTO	350.000.000,00

PROYECTO	**P9. Implementación de mecanismos para protección de marca de la ANH**
JUSTIFICACION	Mitigar impactos reputacionales por información malintencionada publicada en redes sociales
OBJETIVO DEL PROYECTO	Proteger la reputación de la ANH en Redes Sociales
ALCANCE	Las actividades mínimas que debe contener: 1) Implementar como servicio la protección de marca que permita monitorear diferentes fuentes de información tales como sitios web, blogs y redes sociales. 2) Implementar herramientas especializadas en protección de marca (ej. Google alert, Radian6, sysomos) 3) Estructuración del rol de community manager para la gestión del buen nombre de la entidad en redes sociales.

TIEMPO	12 meses
PRESUPUESTO	200.000.000,00

PROYECTO	**P10. Fortalecimiento de gestión integral de activos tecnológicos en la CMDB**
JUSTIFICACION	No se tiene una apropiada gestión de los ítems de configuración o componentes tecnológicos de la entidad, ni clasificados los activos críticos mediante diagrama de relacionamiento a través de la CMDB, lo cual puede afectar los niveles de servicio esperados.
OBJETIVO DEL PROYECTO	Facilitar la gestión de los servicios TI a través de una base de datos donde se administre y gestione todos los elementos de la compañía (Configuration Ítems o CI) que son necesarios para la prestación de servicios.
ALCANCE	Las actividades mínimas para realizar son: 1) Identificar e inventariar los dispositivos físicos, sistemas, las plataformas de software y aplicaciones expuestas en el ciberespacio en la CMDB. 2) Gestionar el relacionamiento de componentes críticos tecnológicos 3) Categorizar dentro de la CMDB los activos con calificación alta criticidad desde los aspectos de confidencialidad, integridad y disponibilidad. 4) Revisar la Integración de los contratos con proveedores, vigencias de garantía, fechas de vencimiento de soportes de contratos, vigencias de suscripciones, entre otros 5) Fortalecer la gestión de activos de la ANH de tal manera que genere valor para los administradores de plataformas tecnológicas. 6) Establecer procedimiento para documentar el impacto del incidente y las acciones adoptadas con respecto a los componentes afectados. 7) Mantener actualizados en la CMDB los cambios según proceso de gestión de la configuración basado en ITIL.
TIEMPO	12 meses
PRESUPUESTO	350.000.000,00

PROYECTO	**P11. Implementación de solución de acceso a información sensible**
JUSTIFICACION	Con el fin de mitigar los riesgos asociados a fuga de información y afectaciones a la confidencialidad e integridad, se requiere proteger la información sensible en tránsito y reposo.
OBJETIVO DEL PROYECTO	Proteger la información en tránsito y en reposo

ALCANCE	Las actividades mínimas para realizar son: 1) Implementación solución de protección de datos sensibles de la ANH en tránsito y en reposo (ej. Vormetric) 2) Generación de tokenización virtual o físico 3) Proteger la información confidencial en las bases de datos no productivas a través del ofuscamiento 4) Identificar las tablas de las bases de Datos a cifrar 5) Identificar los usuarios que usan información sensible para brindarles tokens 6) identificación de repositorios que generan información sensible para cifrado local y en nube, o cifrado de discos determinados
TIEMPO	9 meses
PRESUPUESTO	300.000.000,00

PROYECTO	**P12. Implementación de solución de seguridad inalámbrica**
JUSTIFICACION	Proteger la información que viaja por las redes inalámbricas dado que la información confidencial de la Entidad puede ser interceptada a mitad de camino cuando transita entre el dispositivo de usuario y el router, sin que sea percibido.
OBJETIVO DEL PROYECTO	Asegurar la información que transita por las redes inalámbricas.
ALCANCE	Las funcionalidades mínimas para contemplar son: 1) Restricción de acceso de usuario a dispositivos de red inalámbricos no autorizados 2) Capacidad de detectar la presencia de dispositivos de red inalámbricos no autorizados (Rogue Access Point) para una desconexión oportuna de la red.
TIEMPO	6 meses
PRESUPUESTO	150.000.000,00

PROYECTO	**P13. Implementación del Sistema de Gestión de Resiliencia Organizacional**
JUSTIFICACION	La importancia de engranar los diferentes sistemas de gestión dentro de la entidad, con el fin de tener un enfoque que le permita tomar acciones estructuradas ante cualquier evento disruptivo que pueda afectar a la ANH y el desarrollo de capacidades y competencias para el Recurso Humano de la ANH en esta buena práctica.
OBJETIVO DEL PROYECTO	Mejorar la capacidad de recuperación ante incidentes disruptivos

ALCANCE	Las actividades mínimas para desarrollar son: 1) En el desarrollo del proyecto se debe integrar todos los lineamientos de la ISO 22316 2) Se debe establecer al marco de referencia con los recursos necesarios 3) Un plan de sensibilización asociado en toda la organización, con el objetivo que en todas las áreas se interiorice el marco de referencia definido. 4) Integrar y actualizar la metodología de riesgos de la ANH lo que contribuirá a la mitigación de riesgos que puedan afectar el cumplimiento de los objetivos estratégicos de la ANH, así como fortalecer la gestión del tratamiento de riesgos integral de todos los sistemas de gestión y el monitoreo permanente de los factores contribuyentes para mejorar su eficiencia. 5) Realizar pruebas y ejercicios de resiliencia organizacional integrando los diversos sistemas de gestión de la entidad, los planes de continuidad, contemplando el plan de comunicación de crisis y el plan de gestión de crisis. 6) Desarrollar un plan de comunicación a nivel interno y externo que involucre a toda la organización 7) Fortalecer esquemas de innovación y prospectiva todas las fases del programa de resiliencia organizacional
TIEMPO	9 meses
PRESUPUESTO	400.000.000,00

8. PROGRAMA DE INVERSION REQUERIDO

A continuación, se presenta el presupuesto de inversión estimado para la implementación del Plan Estratégico de Seguridad de la Información (PESI) definido[56].

PROYECTO No.	PROD/SERV	TITULO DEL PROYECTO	PRESUPUESTO - VALOR PROYECTO * (Incluye tanto servicios como soluciones tecnológicas)
1	**SERVICIO**	**P1. Fortalecimiento del Sistema de Seguridad de la Información y Ciberseguridad**	**$ 980.000.000,00**
2	**PRODUCTO**	**P2. Fortalecimiento del Sistema de Seguridad Adaptativa.**	**$ 1.790.000.000,00**

[56] Los valores para 2021 y 2022 se estimaron con base en un IPC estimado del 4% anual, se toman con referencia a listas de precios de fabricantes e información de proyectos similares en otras entidades.

3	**SERVICIO**	**P3. Fortalecimiento de la Gestión del Riesgo en Materia de Seguridad y Privacidad de la Información en la Entidad**	**$ 450.000.000,00**
4	**PRODUCTO**	**P4. Implementación de Soluciones de Análisis de Comportamiento en el uso de servicios y herramientas informáticas**	**$ 600.000.000,00**
5	**PROD/SERV**	**P5. Aseguramiento de Servicios en la Nube**	**$ 900.000.000,00**
6	**PRODUCTO**	**P6. Implementación de solución automatizada para la hardenización de infraestructura tecnológica.**	**$ 435.000.000,00**
7	**PROD/SERV**	**P7. Implementación de Herramientas y Procedimientos para desarrollo seguro**	**$ 400.000.000,00**
8	**PRODUCTO**	**P8. Implementación de una solución para Aseguramiento y Gestión de Cuentas privilegiadas**	**$ 350.000.000,00**
9	**SERVICIO**	**P9. Implementación de mecanismos para protección de marca de la ANH**	**$ 200.000.000,00**
10	**SERVICIO**	**P10. Fortalecimiento de gestión integral de activos tecnológicos en la CMDB**	**$ 350.000.000,00**
11	**PRODUCTO**	**P11. Implementación de solución de acceso a información sensible**	**$ 300.000.000,00**
12	**PRODUCTO**	**P12. Implementación de solución de seguridad inalámbrica**	**$ 150.000.000,00**
13	**SERVICIO**	**P13. Implementación del Sistema de Gestión de Resiliencia Organizacional**	**$ 400.000.000,00**
TOTAL PROYECTOS			**$ 7.305.000.000,00**

NOTA: Los presupuestos se toman con base en estudios de mercado y precios de lista de los fabricantes.

9. DOCUMENTOS DE REFERENCIA

9.1. INTERNOS.

- ✓ Política General de Seguridad y Privacidad de la Información de ANH.
- ✓ Resolución 266 de 2018 – Adopción del Sistema de Gestión de Seguridad de la Información.
- ✓ Resolución 415 de 2016 – Comité de Seguridad de la Información.
- ✓ Resolución 416 de 2017 – Responsabilidades de los administradores tecnológicos y administradores funcionales de las herramientas informáticas
- ✓ Resolución 429 de 2016 – Lineamientos para la implementación del teletrabajo en la ANH

9.2. EXTERNOS.

Lineamientos para la formulación del plan de seguridad de la información emitidas por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC[57].

10. SEGUIMIENTO Y MEDICIÓN

Se realizarán segum durante la vigencia para validar el cumplimiento en cada una de las actividades planteadas, con sus correspondientes productos o grado de avance, dejando las observaciones respectivas.

El presente Plan podrá ser actualizado o ajustado conforme cambios en las metas, la operación, nuevas directrices, normativas o lineamientos de Gobierno, condiciones emergentes o necesidades del servicio. En caso de imposibilidad del logro de las actividades total o parcialmente se dejará constancia en el seguimiento y ajuste realizado de las razones.

Para conocer el avance en a la ejecución del plan, se establece un indicador de gestión que mide la cantidad de acciones, procesos, procedimientos y operaciones realizadas durante el periodo a evaluar.

Nombre del Indicador	Descripción	Tipo	Unidad de Medida	Periodicidad	Responsable
Avance del plan	Avance realizado / Avance proyectado en el periodo	Gestión	Porcentaje	semestral	Profesionales de la OTI

11. BIBLIOGRAFÍA

- ✓ Manual de Gobierno Digital
- ✓ Plan de Seguridad y Privacidad de la Información de la ANH vigencia 2020
- ✓ Autodiagnóstico MSPI 2020
- ✓ Matriz Gobierno Digital 2020

12. REGISTROS

Para el presente plan no se utilizarán registros oficiales, sin embargo, se dejará plasmado el seguimiento en un documento tipo Excel con las observaciones para cada actividad.

[57] Mintic, Programa de Gobierno Digital, Lineamientos para la formulación del plan de seguridad de la información

13. CONTROL DE CAMBIOS.

FECHA	MOTIVO DEL CAMBIO	VERSIÓN
Noviembre de 2019	Creación del documento	1
Enero de 2021	Actualización del documento	2
Enero de 2022	Actualización del documento	3