PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2020-2022

CENTRAL DE INVERSIONES S.A.

BOGOTA, ENERO 2022
VERSIÓN 03

Contenido

1. Presentación

Central de Inversiones S.A., en adelante CISA, en el desarrollo de sus actividades ha identificado que uno de los activos más importantes para la entidad es la información que se encuentra almacenada de forma física o electrónica; en los sistemas de información, servidores, computador, folios entre otros.

El plan estratégico de seguridad de la información determina los objetivos a cumplir para salvaguardar la información en sus pilares de confidencialidad, integridad y disponibilidad. A través de las diferentes iniciativas y proyectos estratégicos.

2. Objetivo

Definir la estrategia de seguridad de la información en adelante PESI liderada por la alta dirección apoyando el cumplimiento del plan estratégico de la entidad para la vigencia 2020 hasta 2022, respondiendo a la necesidad de preservar la confidencialidad, integridad y disponibilidad de los activos de información. Y, además disminuyendo el nivel de riesgos asociado a los activos de información.

3. Alcance

Conservando el análisis del contexto externo, interno y las partes interesadas de CISA se define el alcance del plan estratégico de seguridad de la información (PESI). En términos de las características de la entidad, su ubicación, sus activos de información. Adopta, establece, implementa, opera, verifica y mejora el sistema de seguridad de la información (SGSI) para los 14 procesos de la entidad (Estratégicos, Misionales, Apoyo y Control).

4. Principios del PESI

CISA a través del plan estratégico de seguridad de la información debe:

- Facilitar la integración de la seguridad de la información entre las unidades de negocio y con los clientes del portafolio ofrecido por CISA.
- Fortalecer las competencias de seguridad de la información.
- Proponer soluciones que aseguren la información estén a la vanguardia de la tecnología, se han flexibles, adaptables y escalables para las necesidades que tenga la entidad.

5. Marco Normativo

- 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.
- Decreto 090 de 2018, el cual establece plazo para que se inscriban las bases de datos que contengan datos personales.
- Decreto 1499 de 2017, Modelo de Integración de Planeación y Gestión -MIPG. En cada una de las entidades se integrará un comité institucional de gestión y desempeño encargado de orientar la implementación y operación del modelo integrado de planeación y gestión MIPG, el cual sustituirá los demás comités que tengan relación con el modelo y que no sean obligatorios por mandato legal.
- Resolución 01126 de 2021 por la cual se modifica la Resolución 2710 octubre 2017, adopción IPv6. Por lo cual se establece lineamientos para la adopción del protocolo IPv6
- Documento Conpes 3854 de 2016. POLÍTICA NACIONAL DE SEGURIDAD DIGITAL.
- Decreto 1083 de 2015. Por el cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, el cual

incluye el Decreto 2573 de 2014 que establece los lineamientos generales de la Estrategia de Gobierno en Línea (Hoy Gobierno Digital).

- Decreto 1078 de 2015. Por el cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, el cual incluye el Decreto 2573 de 2014, el cual establece los lineamientos generales de la Estrategia de Gobierno en Línea (Hoy Gobierno Digital).

- Ley 1712 de 2014. Por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Decreto 103 de 2015. Que reglamenta parcialmente la ley de transparencia.

- Decreto 886 de 2014 (Registro Nacional de Base de Datos). El responsable del Tratamiento debe inscribir en el Registro Nacional de Bases de Datos, de manera independiente, cada una de las bases de datos que contengan datos personales sujetos a Tratamiento.

- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

- Ley 1273 de 2009, la protección de la información y de los datos. Atendiendo los atentados contra la confidencialidad, la integridad y disponibilidad de los datos y de los sistemas informáticos.

- Ley 603 de 2000 y Ley 23 de 1982, el estado del cumplimiento de las normas sobre propiedad intelectual y derechos de autor por parte de la sociedad.

- Ley 527 de 1999, se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

- Decreto 1360 de 1989, la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.

- Directiva Presidencial 03, Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

- Anexo 1, Modelo de Seguridad y Privacidad de la Información, el cual establece los lineamientos generales de la Estrategia de Seguridad Digital.

- Ley 2121 de 2021, por medio del cual se crea el régimen de trabajo remoto y se establecen normas para promoverlo, regularlo y se dictan otras disposiciones.

- Resolución 05 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.

6. Situación Actual

6.1 Contexto de la Organización

Son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de la Entidad. Definir el contexto institucional contribuye al autoconocimiento de la Entidad frente a la exposición al riesgo, ya que permite identificar las situaciones generadoras de riesgos.

El establecimiento del contexto permite a CISA articular los objetivos frente a las características del entorno interno y externo en el cual opera.

El contexto de CISA se determinó por medio de la metodología DOFA, la cual permite identificar los aspectos clave a considerar para definir el alcancé de los objetivos y potencializar las fortalezas y oportunidades, así como también minimizar el riesgo asociado a las debilidades y amenazas; para lo cual se evaluó con el líder de cada proceso las fortalezas y debilidades en relación con las oportunidades y amenazas que ellos identifican en la operación

Algunos de los componentes evaluados fueron:

Tipo de contexto	Definición	Ejemplos
Establecimiento del contexto del proceso	Se determinan las características o aspectos esenciales del proceso y sus interrelaciones.	Objetivo, alcance, interrelaciones existentes, procedimientos y responsables del proceso.
Establecimiento del contexto interno	Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad.	Estructura organizacional, funciones y responsabilidades, políticas, objetivos y estrategias, recursos y conocimiento y cultura organizacional.
Establecimiento del contexto externo	Se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos.	Político, económico y financiero, social y cultural, tecnológico, ambiental y legal.

El contexto institucional de CISA se revisará teniendo en cuenta los cambios administrativos que puedan afectar la operación, está se realizará por lo menos cada dos años mediante un ejercicio ejecutado por los líderes de proceso quienes garantizaran la participación de sus equipos de trabajo junto con el apoyo y direccionamiento de la Gerencia de Planeación Estratégica.

6.2 Establecimiento del contexto a nivel de procesos

Se define que todos los procesos deberán estar debidamente documentados y actualizados; así las cosas, los siguientes son elementos mínimos que se deberán considerar y documentar en el establecimiento del contexto en cada uno de los procesos del mapa de procesos de CISA:

Factores de Riesgo del Proceso	Descripción
Diseño del proceso	Claridad en la descripción del alcance (misión y visión). Objetivos estratégicos vinculados al proceso. Objetivo del procesos y características claves. Actividades clave utilizadas por el proceso para el cumplimiento del objetivo. Sistemas de información utilizados en la operación.
Interacciones con otros procesos	Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes. Proveedores o terceros que soportan el proceso. Cantidad de ciudadanos afectados por el proceso.
Procedimientos asociados	Pertinencia en los procedimientos que desarrollan los procesos. Caracterización del proceso.
Responsable del proceso	Grado de autoridad y responsabilidad de los funcionarios frente al proceso. Estructura organizacional que soporta el proceso.
Comunicación entre los procesos	Efectividad en los flujos de información determinados en la interacción de los procesos, así como la toma de decisiones.

6.3 Establecimiento del contexto interno

El contexto interno es el ambiente interno en el cual CISA busca alcanzar sus objetivos. Es importante que la administración del riesgo este alineada con la cultura, los procesos, la estructura y la estrategia de la organización. Para este análisis se tuvieron en cuenta los factores internos como las debilidades y fortalezas más relevantes (número de veces mencionada por el área), el resultado es el siguiente:

A continuación, se presentan los factores de riesgo internos definidos actualmente en la Entidad:

Factores de Riesgo	Clasificación del riesgo DAFP	Clasificación del riesgo CISA	Situaciones
Talento Humano: Se analiza posible dolo e intención frente a la corrupción.	**Fraude interno:** Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abusos de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros	**Comportamiento humano**	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por hurto de activos, compromiso y comportamiento no ético (principios y valores) de los empleados, fraude interno, corrupción y/o soborno.

Factores de Riesgo	Clasificación del riesgo DAFP	Clasificación del riesgo CISA	Situaciones
	Relaciones laborales: Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación	**Ambiente laboral**	Existe cierto riesgo de que la entidad sufra pérdidas causadas por ambiente laboral desfavorable.
	Usuarios, productos y prácticas: Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.	**Actividades Individuales**	Existe cierto riesgo de que la entidad sufra pérdidas causadas por negligencia, error humano, personal no cuenta con las aptitudes y destrezas necesarias para afrontar la exigencia de los procesos, inadecuada contratación, estabilidad laboral y disponibilidad de personal.

Factores de Riesgo	Clasificación del riesgo DAFP	Clasificación del riesgo CISA	Situaciones
Tecnología: Eventos relacionados con la infraestructura tecnológica de la entidad.	**Fallas tecnológicas:** Errores en hardware, software, telecomunicaciones y/o interrupción de servicios básicos.	**Aspectos tecnológicos**	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por uso inadecuado de los sistemas de información, comunicación y/o tecnologías inherentes en los procesos, hechos que atenten contra la confidencialidad, integridad, operación, disponibilidad, vigencia, pertinencia, estado de los sistemas de información, daño a equipos, caída de los aplicativos o redes, errores en los programas, fallas en la parametrización, bases de datos reducidas, falta de automatización de procesos y/o automatizar nuevas líneas de negocio.

Factores de Riesgo	Clasificación del riesgo DAFP	Clasificación del riesgo CISA	Situaciones
Procesos: Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	**Ejecución y administración de procesos:** Pérdidas derivadas de errores en la ejecución y administración de procesos.	**Procesos internos**	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por diseño inadecuado de los procesos internos o que hayan fijadas unas políticas inadecuadas que mermen el desarrollo de las operaciones e impidan ofrecer un producto o servicio de calidad, políticas rígidas, falta de sinergia entre los procesos, procesos desagregados, falta de entendimiento de los objetivos estratégicos o del proceso, falta de capacitación, sistemas de información y/o falta de mejora continua.
		Actividades y Controles gerenciales	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por los mecanismos de seguimiento y medición institucionales, errores en la grabación de los negocios o autorizaciones, falta de información para la toma de decisiones, gestión deficiente de proveedores y contingencias legales.

Factores de Riesgo	Clasificación del riesgo DAFP	Clasificación del riesgo CISA	Situaciones
		Aspectos técnicos	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por fallas en la capacidad operativa en la respuesta del desarrollo de sus funciones y/o obligaciones (inoportunidad en la entrega de productos/servicios), insuficiencia de inventario de inmuebles, falta de información en el mercado de inmuebles, modelos de valoración no ajustado a las necesidades actuales, estructura de costos alta, procesos de contratación mixta, falta de planificación a corto plazo, nuevas líneas de negocio y variedad de activos por vender.

Como base en esta información se definen y priorizan las oportunidades de mejora, fortalezas de la entidad frente a su contexto interno; y a su vez, se enfocan los esfuerzos en las debilidades con acciones que permitan la mitigación a la exposición de potenciales riesgos.

6.4 Establecimiento del contexto externo

El contexto externo es el ambiente externo en el cual CISA busca alcanzar sus objetivos. Entenderlo es importante para garantizar que los objetivos y las precauciones de las partes interesadas externas se tomen en consideración en el momento de tomar decisiones.

Para el análisis de contexto externo, se tuvieron en cuenta los factores externos como las oportunidades y amenazas más relevantes (número de veces mencionada por el área), el resultado es el siguiente:

Factores de Riesgo	Clasificación del riesgo CISA	Situaciones
Infraestructura: Eventos relacionados con la infraestructura física de la entidad.	**Eventos Externos**	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por emisiones, residuos generados y dispuestos de forma errónea, cortes de energía, catástrofes naturales, incendios, fallas en el desarrollo sostenible del ambiente, fallas en los servicios públicos o pandemias.
Eventos externos: Situaciones externas que afectan la entidad.	**Fraude externo**	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por actos delictivos, ataques cibernéticos, robos, atentados o vandalismo.
	Circunstancias políticas	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por cambios de gobierno, legislación, planes, políticas públicas, decisiones gubernamentales, nuevas líneas de negocio, participación directa con el gobierno o cobro de comisiones fijas para la venta de inmuebles.
	Económicas (por la falta de recursos)	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por capacidad financiera de la entidad o administración de los recursos disponibles.

Factores de Riesgo	Clasificación del riesgo CISA	Situaciones
	Relaciones comerciales y legales	Existe cierto riesgo de que la Entidad sufra pérdidas causadas por bajo reconocimiento o posicionamiento en el mercado, uso inadecuado de redes sociales, estrategias de marketing ineficientes, clientes con posibles dependencias, relacionamientos inadecuados con clientes externos y contrataciones ineficientes.
	Entorno digital	Clientes, proveedores de servicios y empresas que sean competencia directa y/o se relacionen con la misión de la entidad. Normativas o aspectos jurídicos que apliquen directa o indirectamente a la entidad. Dependencias económicas y financieras por parte de otras empresas. Entorno Cultural Cualquier otro factor externo de tipo internacional, nacional (gobierno), regional o local. Cantidad de ciudadanos a los cuales la entidad pública brinda servicios a través del entorno digital como trámites a través de páginas web. Aspectos externos que pueden verse afectados con los riesgos de seguridad digital, tales como el ambiente social, económico y ambiental que tengan alguna relación con las operaciones asociadas a la entidad.

6.5 Liderazgo y Compromiso

La presidencia en CISA se caracteriza por un estilo dirección enfocado en el trabajo en equipo, la constante comunicación con la vicepresidencia y líderes de cada proceso, la generación de comités de trabajo y un enfoque hacia la atención y calidad en el servicio al cliente, tal como se define en los valores de CISA.

La alta dirección ha designado al vicepresidente Financiero y Administrativo como el representante para el sistema integrado de gestión, SIG (El Sistema de Gestión de Seguridad de la Información hace parte del SIG) quien tiene responsabilidad y autoridad para:

- Asegurar que el sistema integrado de gestión, SIG (El Sistema de Gestión de Seguridad de la Información hace parte del SIG) se establece, implementa y mantiene de acuerdo con los requisitos de las normas que se encuentran definidas para CISA.

- Informar a la alta dirección sobre el desempeño del sistema integrado de gestión, SIG (El Sistema de Gestión de Seguridad de la Información hace parte del SIG) y de cualquier necesidad de mejora.

- Asegurarse de que se promueve la toma de conciencia de los requisitos del cliente en todos los niveles de la entidad.

- Determinar disposiciones, políticas y prácticas adecuadas que cumplan con los requerimientos de las normas técnicas que componen el SIG, para cumplir las necesidades de CISA.

- Identificar y dirigir programas para mejorar el sistema integrado de gestión, SIG (El Sistema de Gestión de Seguridad de la Información hace parte del SIG).

A través del artículo 133 de la ley 1753 de 2015 se creó el sistema de gestión el cual integra los sistemas los sistemas de desarrollo administrativo y gestión de calidad y deberá articularse con el sistema de control interno, para lo cual el modelo integrado de planeación y gestión – MIPG surge como el

mecanismo que facilita dicha integración y articulación, de tal manera que permite el fortalecimiento de los mecanismo, métodos y procedimiento de gestión y control al interior de los organismos y entidades del estado.

Las funciones del comité son:

- Aprobar y hacer seguimiento, por lo menos una vez al trimestre, a las acciones y estrategias adoptadas para la operación del Modelo Integrado de Planeación y Gestión -MIPG.

- Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del Modelo Integrado de Planeación y Gestión -MIPG.

- Proponer al Comité Sectorial de Gestión y el Desempeño Institucional, iniciativas que contribuyan al mejoramiento en la implementación y operación del Modelo Integrado de Planeación y Gestión -MIPG.

- Adelantar y promover acciones permanentes de autodiagnóstico para facilitar la valoración interna de la gestión.

- Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.

- Reglamentar la operación para el Comité Institucional de Gestión y Desarrollo y el Equipo Operativo.

- Las demás que tengan relación directa con la implementación, desarrollo y evaluación del Modelo.

6.6 Planificación

La planeación estratégica de seguridad de la información se encuentra enmarcada dentro del mapa de ruta para los años 2020 al 2022 con nueve planes que se encuentran dimensionados dentro de las perspectivas del plan estratégico de la entidad.

La aprobación de la planeación estratégica de seguridad de la información fue el día 19 de diciembre de 2019 donde sesionó el comité institucional de gestión y desempeño -CIGD, como se puede evidenciar en el acta 11 donde se aprueban las actividades para los planes presentados.

En el plan estratégico de seguridad de la información se encuentra incluido en la herramienta de seguridad de la información (NovaSec) donde el oficial de seguridad de la información realiza seguimiento a las actividades y de forma trimestral a través del aplicativo de seguimiento a la estrategia (ASE) lo realiza el Comité Institucional de Gestión y Desempeño.

A continuación, se listan cada uno de los proyectos definidos en el mapa de ruta, los cuales cuentan con la aprobación de recursos asignados:

1. Plan de Sensibilización en Seguridad de la Información.

2. Fortalecimiento de Competencias específicas en Seguridad de la Información.
3. Fortalecer la definición, establecimiento e implementación de la normatividad para la gestión de la seguridad de la información.
4. Ampliación del alcance de SGSI.
5. Centro de monitoreo de Ciberseguridad 7x24 - SOC (Security Operation Center).
6. Gestión de Accesos Privilegiados.
7. Análisis de vulnerabilidades en código fuente.
8. Fortalecimiento de capacidades en gestión de incidentes.
9. Revisión independiente de la gestión de la seguridad de la información.

Para el recurso humano se asigno por parte de la entidad un practicante de sistemas asignado por el Sena. Además, en la ultima auditoria interna realizada por el proceso de Auditoria se determino como oportunidad de mejora evaluar la posibilidad
Como proceso de mejora se revisaron los indicadores existentes del sistema de seguridad de la información y se plantean indicadores nuevos para que apoyen y gestionen los proyectos definidos dentro del plan estratégico de seguridad de la información.

6.7 Apoyo

Con el fin de asegurar la adecuación, convivencia, eficacia y alineación continua con el direccionamiento estratégico de CISA, al menos una vez al año entre los meses de septiembre y noviembre del año respectivo, se realiza la revisión por la Dirección del SGSI (Sistema de Gestión de Seguridad de la Información) en el Comité Institucional de Gestión y Desempeño.

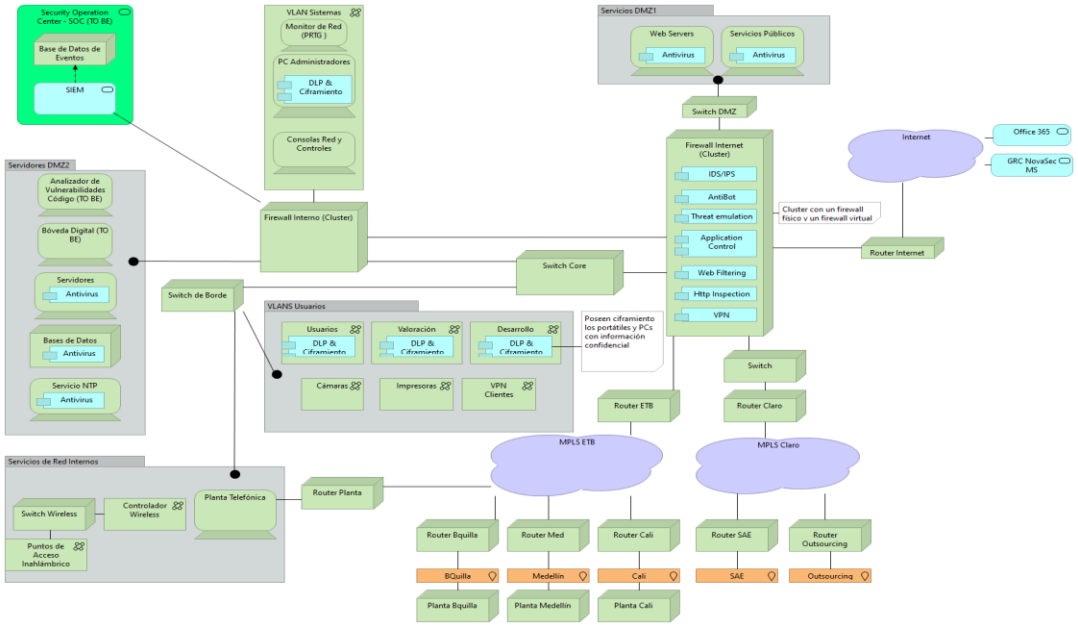
Es necesario que, en el ejercicio de la revisión, se incluya como mínimo la siguiente información:

- Retroalimentación sobre el desempeño de la seguridad de la información, incluidas las tendencias relativas a: No conformidades, acciones correctivas, seguimientos, resultados de las mediciones, resultados de las auditorias y cumplimiento de los objetivos.
- Retroalimentación de las partes interesadas
- Los resultados de la valoración del riesgo, estado del plan de tratamientos de riesgos y oportunidades de mejora.
- El estado de las acciones con la relación a las revisiones previas por la dirección.
- Los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de seguridad de la información.

6.8 Operación

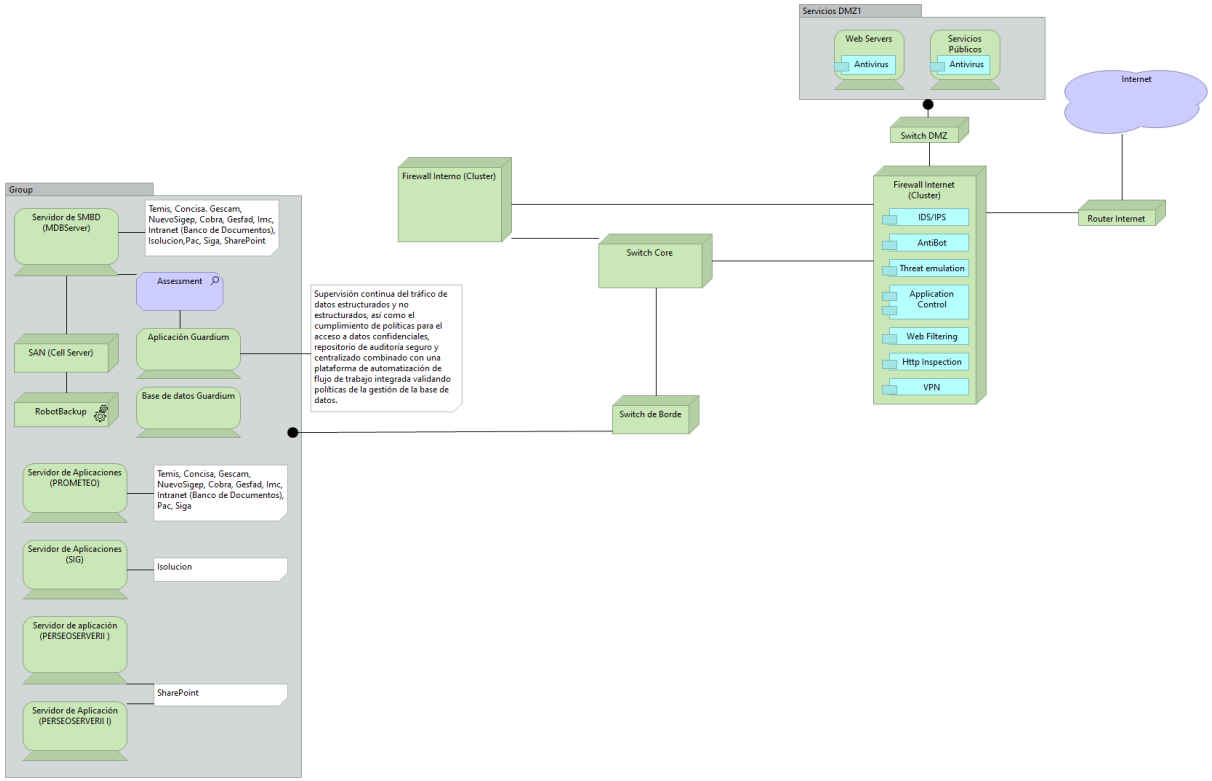
CONTROLES DE SEGURIDAD DIGITAL

Dentro de la arquitectura de seguridad de la información podemos encontrar la capa de control de seguridad donde se han establecidos diferentes controles tanto físicos como lógicos que se pueden observar en el siguiente mapa:



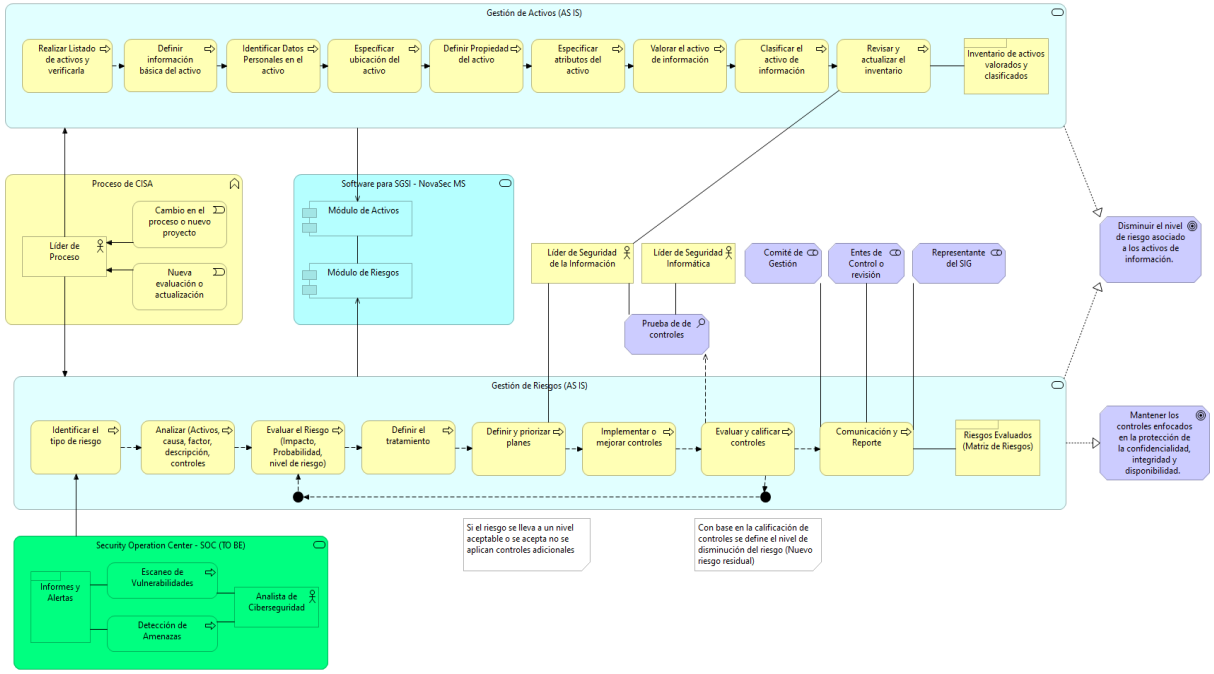
DATOS E INFORMACIÓN

Dentro de la arquitectura de seguridad de la información podemos encontrar la capa de datos e información donde se han establecidos diferentes controles tanto físicos como lógicos que se pueden observar en el siguiente mapa:



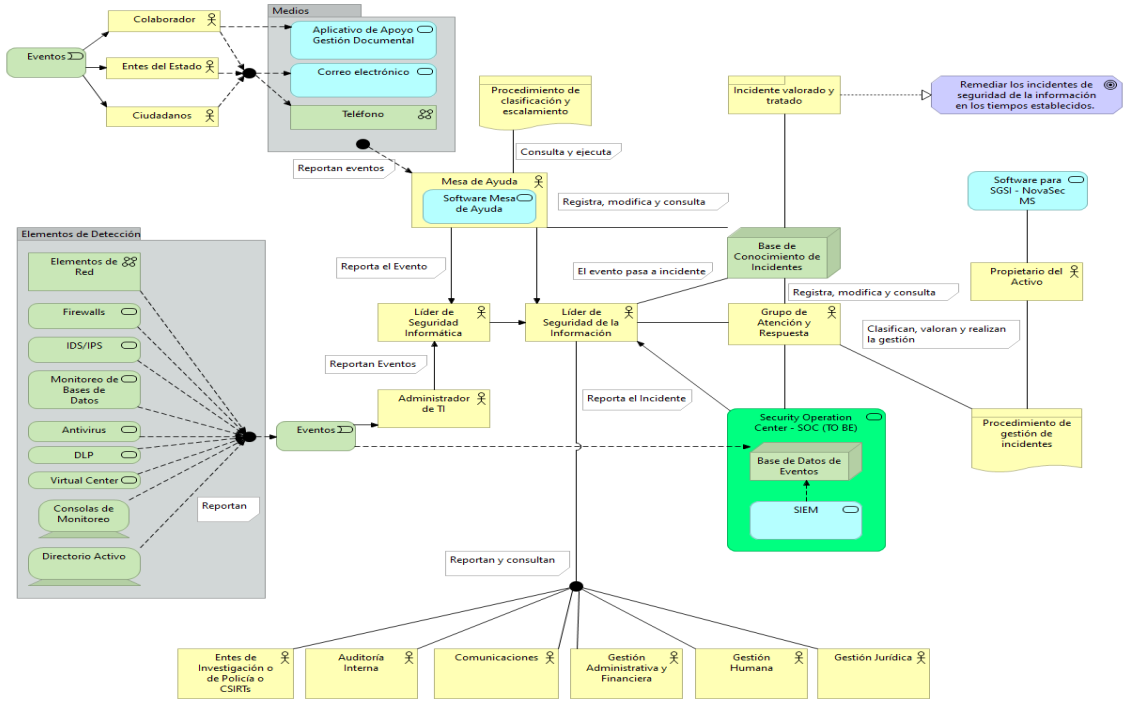
GESTIÓN DE ACTIVOS Y RIESGOS

Dentro de la arquitectura de seguridad de la información podemos encontrar la capa de gestión de activos y riesgos donde se han establecidos diferentes controles tanto físicos como lógicos que se pueden observar en el siguiente mapa:



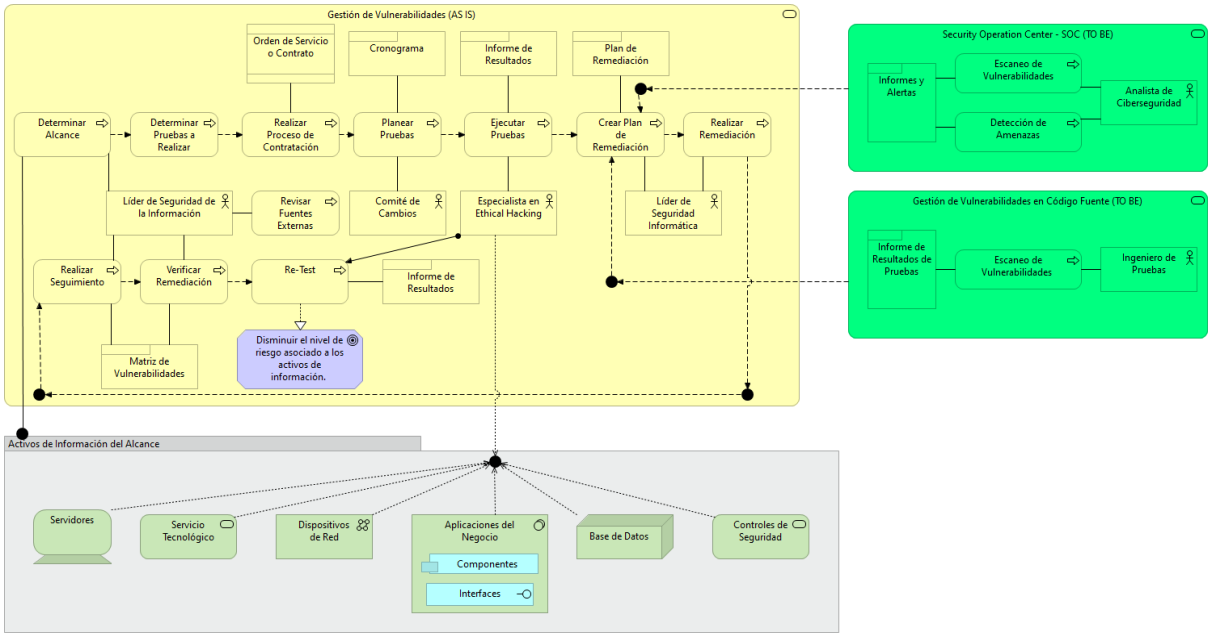
GESTIÓN DE INCIDENTES

Dentro de la arquitectura de seguridad de la información podemos encontrar la capa de gestión de incidentes donde se han establecidos diferentes controles tanto físicos como lógicos que se pueden observar en el siguiente mapa:



GESTIÓN DE VULNERABILIDADES

Dentro de la arquitectura de seguridad de la información podemos encontrar la capa de gestión de vulnerabilidades donde se han establecidos diferentes controles tanto físicos como lógicos que se pueden observar en el siguiente mapa:



6.9 Evaluación de Desempeño

Actualmente el sistema de seguridad de la información cuenta con cuatro indicadores en el proceso de mejora se ajustan los indicadores existentes y se definen uno nuevo para alinear de manera directa el cumplimiento de los objetivos del plan estratégico de seguridad de la información con el plan estratégico de la entidad.

En CISA, se establece el procedimiento que permite realizar seguimiento y medición del desempeño del Sistema Integrado de Gestión, SIG (El Sistema de Gestión de Seguridad de la Información hace parte del SIG).

Los procesos deben contar como mínimo con un indicador de eficacia y eficiencia. Estos indicadores deben ser definidos por cada líder de proceso.

Los indicadores definidos deben permitir la recolección de los datos de manera sencilla y oportuna, con el fin de que la medición se presente en la frecuencia establecida y poder realizar el análisis de los datos obtenidos con base en las tendencias en el logro de los objetivos y metas propuestas.

Cuando no se alcancen los resultados planificados, deben llevarse a cabo correcciones y acciones correctivas, según sea conveniente, para asegurar la conformidad del proceso.

Se recomienda que al menos una vez al año los líderes de los procesos realicen una revisión integral de los indicadores, con el fin de asegurar la pertinencia de estos; es decir, asegurar que las mediciones tengan coherencia con políticas y objetivos determinados al interior de CISA.

Se debe definir una meta la cual facilita el análisis y la toma de decisión sobre la necesidad de implementación de acciones para abordar riesgos, acciones correctivas y/o de mejora. La determinación de la meta se puede lograr por alguno de los siguientes métodos:

- Con base a los requisitos de las partes interesadas.
- Con base en el desempeño histórico (tendencias).
- Con base en la Experiencia del Negocio y Deseo de Logro.

La revisión independiente del SGSI y de los controles se hacen a través de auditorías internas realizada por la jefatura de procesos y la parte técnica es apoyada por empresas especializadas contratadas por seguridad de la información.

En CISA, se cuenta con una Política y Procedimiento para Planear y Ejecutar Auditorías Internas al Sistema Integrado de Gestión, SIG (El Sistema de Gestión de Seguridad de la Información hace parte del SIG).

A continuación, se listan las generalidades al respecto:

- La viabilidad de las auditorias debe determinarse teniendo en consideración factores de disponibilidad de:

  - ✓ La información suficiente y apropiada para planificar las auditorias
  - ✓ La cooperación adecuada de los auditados
  - ✓ El tiempo y los recursos adecuados

- Deben obtener evidencia valida y suficiente por medio de análisis, inspección, observación, interrogación, confirmación y otros procedimientos de auditoría, con el propósito de allegar bases razonables a la auditoria.

- Debe realizarse mínimo una auditoría interna al año para el Sistema Integrado de Gestión, SIG (El Sistema de Gestión de Seguridad de la Información hace parte del SIG).

- Las auditorias deben cumplir con la metodología planteada en la Política y Procedimiento para Planear y Ejecutar Auditorías Internas al Sistema Integrado de Gestión, SIG (El Sistema de Gestión de Seguridad de la Información hace parte del SIG).

- Todo hallazgo de auditoria se trata como una No Conformidad real y toda observación se trata como una oportunidad de mejora, cuya implementación se llevará a cabo dependiendo del criterio del auditado y el auditor interno asignado.

- Para cerrar todas las acciones correctivas y/o de mejora detectadas en una auditoría interna deben llevarse a cabo la metodología establecida.

- Los auditores internos, no deben auditar su propio trabajo o proceso.

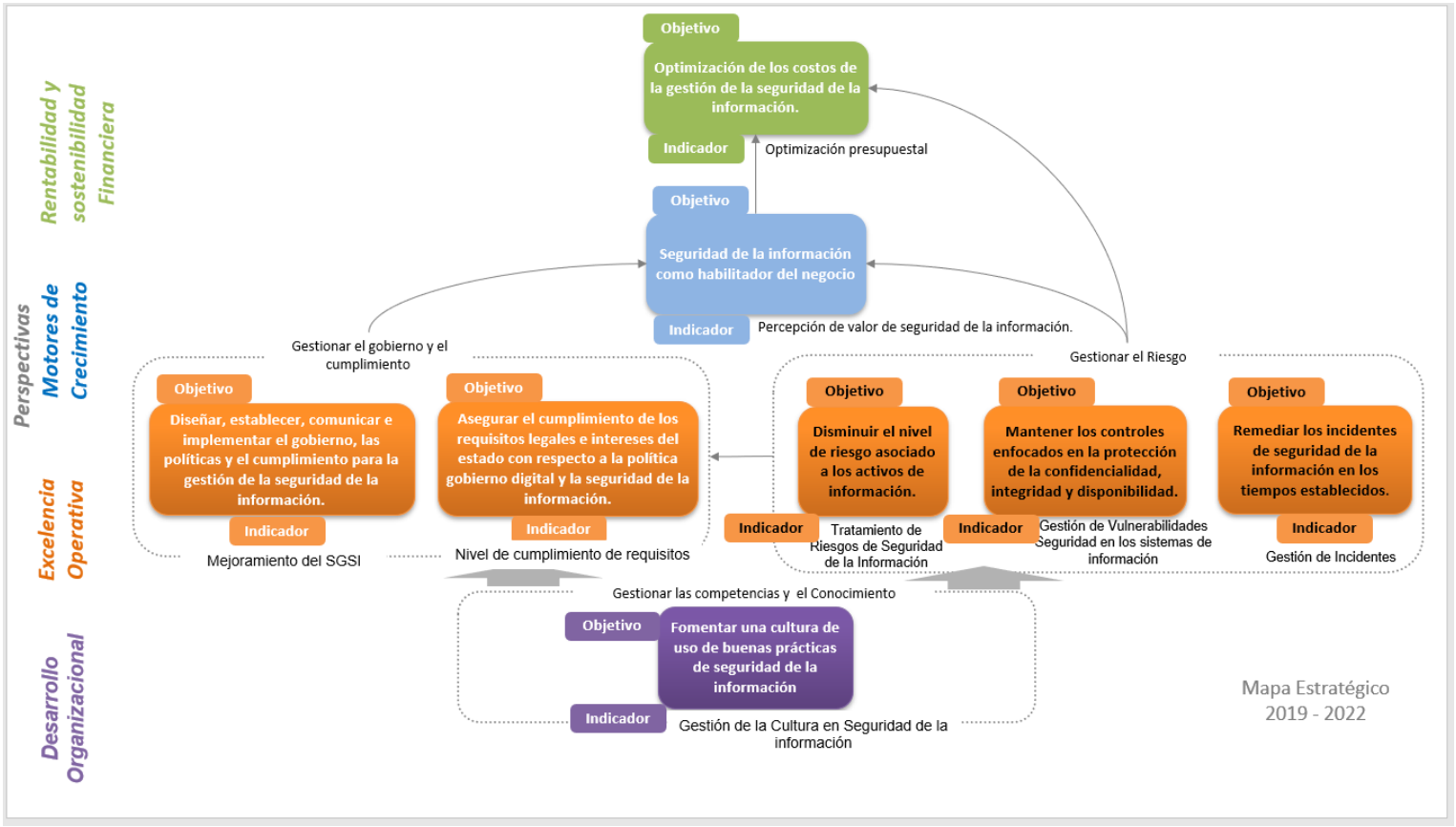
6.10 Mejoramiento

Actualmente CISA, cuenta con un procedimiento para la gestión de la mejora donde se establece una metodología para determinar y seleccionar las oportunidades de mejora e implementar cualquier acción necesaria para cumplir los requisitos previstos en el Sistema Integrado de Gestión, SIG (El Sistema de Gestión de Seguridad de la Información hace parte del SIG).

Las fuentes potenciales de oportunidades de mejora para el sistema de seguridad de la información son:

1. Revisión de Controles, políticas o procedimientos del sistema de seguridad de la información.
2. Incidentes de Seguridad de la Información.
3. El grado de satisfacción de las partes interesadas.
4. Experiencias obtenidas de las No Conformidades y de las acciones correctivas relacionadas.
5. Estudios comparativos externos de las mejoras prácticas.
6. Nueva legislación o los cambios propuestos a la legislación vigente para el SGSI.
7. Resultados de las auditorías internas.
8. Evaluación y análisis de los resultados de seguimiento y medición
9. Opiniones de las partes interesadas.
10. Resultados de la Revisión por la Dirección.

7. Cuadro de Mando Integral



8. Iniciativas

Desde Seguridad de la Información se define el portafolio de proyecto del año 2020 al 2022 alineado a las perspectivas del plan estratégico de la Entidad.

PERSPECTIVA	OBJETIVO DE SEG. INF.	DIMENSION MIPG	PROYECTO	DESCRIPCIÓN
Desarrollo Organizacional	Fomentar una cultura de uso de buenas prácticas de seguridad de la información en los procesos de Central de Inversiones S.A.	-Talento Humano TH fortalecido en sus conocimientos y competencias, de acuerdo con las necesidades institucionales	Plan de Sensibilización en Seguridad de la Información	Definir e implementar un plan de sensibilización y de gestión de la cultura de seguridad de la información para disminuir la probabilidad de ocurrencias de incidentes y evitar impactos reputacionales, financieros y otros relacionados con los riesgos de seguridad de la información para seguir fortaleciendo el reconocimiento de la entidad y la confianza por parte de los grupos de interés.

PERSPECTIVA	OBJETIVO DE SEG. INF.	DIMENSION MIPG	PROYECTO	DESCRIPCIÓN
Desarrollo Organizacional	Fomentar una cultura de uso de buenas prácticas de seguridad de la información en los procesos de Central de Inversiones S.A.	-Talento Humano TH fortalecido en sus conocimientos y competencias, de acuerdo con las necesidades institucionales	Fortalecimiento de Competencias específicas en Seguridad de la Información	Llevar a cabo entrenamientos especializados para asegurar que el personal cuente con las competencias requeridas para soportar las actividades más críticas de la gestión de la seguridad de la información y asegurar los productos y servicios de la entidad.
Excelencia Operativa	Diseñar, establecer, comunicar e implementar el gobierno, las políticas y el cumplimiento para la gestión de la seguridad de la información.	- Direccionamiento estratégico y planeación Planes de acción o planes operativos orientados a resultados y a satisfacer las necesidades de sus grupos de valor, con los recursos necesarios que aseguren su cumplimiento	Fortalecer la definición, establecimiento e implementación de la normatividad para la gestión de la seguridad de la información	Definir, establecer, comunicar e implementar mejoras a la normatividad de gestión de seguridad de la información en cuanto: Plan estratégico de seguridad de la información PESI, nueva circular normativa para seguridad de la información, actualización de la normatividad para que refleje la organización de la seguridad de la información y las actividades del proceso de seguridad de la información.

PERSPECTIVA	OBJETIVO DE SEG. INF.	DIMENSION MIPG	PROYECTO	DESCRIPCIÓN
Excelencia Operativa	Disminuir el nivel de riesgo asociado a los activos de información.	- Direccionamiento estratégico y planeación Gestión basada en procesos soportada en identificación de riesgos y definición de controles que asegure el cumplimiento de gestión institucional. -Información y Comunicación. Información considerada como un activo de la entidad para la generación de conocimiento.	Ampliación del alcance de SGSI	Asegurar que todos los procesos de la entidad hacen parte del alcance del SGSI llevando a cabo las actividades a su cargo relacionadas con gestión de activos, riesgos y controles de seguridad de la información.

PERSPECTIVA	OBJETIVO DE SEG. INF.	DIMENSION MIPG	PROYECTO	DESCRIPCIÓN
Excelencia Operativa	Disminuir el nivel de riesgo asociado a los activos de información.	- Control Interno *Análisis del entorno institucional que permite la identificación de los riesgos y sus posibles causas *Actividades de Monitoreo	Centro de monitoreo de Ciberseguridad 7x24 - SOC (Security Operation Center)	Servicio de monitoreo y detección de eventos y amenazas avanzadas de ciberseguridad y gestión de capacidad en modalidad 7x24 sobre los activos de información más críticos de TI que soportan los negocios de CISA, para poder identificar de manera temprana los posibles riesgos de seguridad de la información, tecnología, continuidad y ciberseguridad que podrían afectar el negocio. Este centro de operaciones de ciberseguridad debe poseer como mínimo las siguientes capacidades: Servicio 7×24 de: - Monitoreo de la gestión de la configuración. - Monitoreo de la gestión de cambios. - Centralización y monitoreo de eventos de red y ciberseguridad. - La gestión de fallas. - Medición del desempeño y capacidad. - Centralización de eventos de ciberseguridad. - Correlación de eventos de ciberseguridad. - Detección y análisis de amenazas. - Gestión de vulnerabilidades. - Capacidades de SIEM.

PERSPECTIVA	OBJETIVO DE SEG. INF.	DIMENSION MIPG	PROYECTO	DESCRIPCIÓN
Excelencia Operativa	Mantener los controles enfocados en la protección de la confidencialidad, integridad y disponibilidad.	- Control Interno *Auditoría interna que asegura la calidad de su proceso auditor	Gestión de Accesos Privilegiados	Adquisición e implementación de una solución de bóveda digital para poder monitorear y gestionar el uso de cuentas privilegiadas sobre activos críticos y prevenir riesgos asociados con ataques externos, abusos y fraude.
Excelencia Operativa	Mantener los controles enfocados en la protección de la confidencialidad, integridad y disponibilidad.	- Control Interno Auditoría interna que asegura la calidad de su proceso auditor - Evaluación de Resultados Evaluaciones del desempeño y la eficacia de los procesos frente a las necesidades de los grupos de valor.	Análisis de vulnerabilidades en código fuente	Adquisición e implementación de una solución o servicio para la evaluación permanente de buenas prácticas de seguridad en el desarrollo y mantenimiento de sistemas de información, para la identificación de vulnerabilidades en el código fuente del software que produce CISA.

PERSPECTIVA	OBJETIVO DE SEG. INF.	DIMENSION MIPG	PROYECTO	DESCRIPCIÓN
Excelencia Operativa	Disminuir el nivel de riesgo asociado a los activos de información.	-Talento Humano TH fortalecido en sus conocimientos y competencias, de acuerdo con las necesidades institucionales - Evaluación de Resultados Evaluaciones que permiten a la entidad saber si logró sus objetivos y metas en los tiempos previstos, con las condiciones de cantidad y calidad esperadas y con el uso óptimo de recursos	Fortalecimiento de capacidades en gestión de incidentes	Realización de pruebas al procedimiento de gestión de incidentes de seguridad de la información de la entidad para verificar su eficacia operativa y definir e implementar las oportunidades de mejora identificadas.
Excelencia Operativa	Disminuir el nivel de riesgo asociado a los activos de información.	- Control Interno Auditoría interna que asegura la calidad de su proceso auditor - Evaluación de Resultados Evaluaciones del desempeño y la eficacia de los procesos frente a las necesidades de los grupos de valor.	Revisión independiente de la gestión de la seguridad de la información	Realizar las revisiones pertinentes al SGSI para asegurar su desempeño y mejora continua a nivel de las actividades de gestión y el adecuado desempeño de sus controles más críticos.

9. Presupuesto

9.1 Presupuesto de Inversión

A continuación, se listan los proyectos de inversión para el sistema de seguridad de la información que requieren de asignación de presupuesto para el año en curso.

- Fortalecimiento de Competencias específicas en Seguridad de la Información.
- Análisis de vulnerabilidades en código fuente

El valor estimado de la inversión es de $215,626,500,00 para el año 2022.

Nota: Para el proyecto Centro de monitoreo de Ciberseguridad 7x24 - SOC (Security Operation Center). Se explorar para el año 2022 con las herramientas entregadas por MINTIC.

9.2 Presupuesto de Operación

A continuación, se listan los proyectos de Operación para el sistema de seguridad de la información:

- Mantenimiento Herramienta de Monitoreo de Base de Datos
- Mantenimiento Herramienta de Gestión del Sistema de Seguridad de la Información (Software GRC).
- Revisión independiente de la gestión de la seguridad de la información.
- Plan de Sensibilización en Seguridad de la Información.
- Horas de Consultoría.
- Mantenimiento Herramienta de Gestión de Accesos Privilegiados.

El valor de la operación son 233,885,224,00 para el año 2022.

10. Recursos

El Sistema de Seguridad de la Información cuenta actualmente con una asignación presupuestal a través de rubro asignado a la Jefatura de Procesos y Productividad. Lo cual permite tener contrataciones u ordenes de servicios para desarrollar los proyectos de competencia del sistema de seguridad de la información:

TIPO DE RECURSO	ESPECIFICACIONES
Humano	Ingeniero de Seguridad Informática
	Aprendiz de Seguridad de la información
	Oficial de Seguridad de la Información
	Horas de Consultoría
Ordenes de Servicios Vigentes	Actualmente se cuenta con Orden de Servicio vigentes para: 1. Mantenimiento Herramienta de Monitoreo de Base de Datos. 2. Mantenimiento Herramienta de Gestión del Sistema de Seguridad de la Información (Software GRC). 3. Plan de Sensibilización en Seguridad de la Información. 4. Mantenimiento Herramienta de Gestión de Accesos Privilegiados. Es importante indicar que para el proyecto de análisis de código fuente se tiene asignado presupuesto para el año 2022 y se espera ejecutar después de ley de garantías. Actualmente se realizó revisión de las herramientas lideres en el cuadrante de gartner cada una con su prueba de concepto y análisis económico de las necesidades que tiene CISA.
Comunicaciones Corporativas	La Gerencia de Mercado y Comunicaciones es la encargada de realizar las diferentes comunicaciones

	internas y externas definidas en el plan de comunicaciones. Además, se cuenta con la herramienta MocEducate donde para 70 usuarios críticos se les entrega newsletter (boletines de seguridad) y videos. Para validar la cultura de los funcionarios se realizan pruebas de seguridad de forma aleatoria.
Plan de Capacitación	La gerencia de recursos es la encargada de realizar las diferentes capacitaciones establecidas en el PIC (Plan Institucional de Capacitaciones).

Aprobado por:	Elaborado por:	Fecha de Aprobación:
Jaime Andres Monroy Jefe de Procesos y Productividad	Diana Rocio Lancheros Gonzalez Oficial de Seguridad de la Información	28/01/2022