PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

2020-2021

CENTRAL DE INVERSIONES S.A.

BOGOTA, ENERO 2020

VERSIÓN 01

Contenido

1. Presentación 3
2. Objetivo 3
3. Alcance 3
4. Principios del PESI 4
5. Marco Normativo 4
6. Situación Actual 6
6.1 Contexto de la Organización 6
6.2 Contexto Interno 6
6.3 Contexto Externo 9
6.4 Liderazgo y Compromiso 11
6.5 Planificación 12
6.6 Apoyo 14
6.7 Operación 14
6.8 Evaluación de Desempeño 14
6.9 Mejoramiento 17
7. Iniciativas 18
8. Presupuesto 21
8.1 Presupuesto de Inversión 21
8.2 Presupuesto de Operación 21
9. Recursos 22

1. Presentación

Central de Inversiones S.A., en adelante CISA, en el desarrollo de sus actividades ha identificado que uno de los activos mas 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 2021, 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

Central de Inversiones 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 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.

6. Situación Actual

6.1 Contexto de la Organización

Central de Inversiones S.A. – CISA es el único colector público del Estado Colombiano. Una entidad vinculada al Ministerio de Hacienda y Crédito Público que tiene por objetivo comprar, comercializar y administrar todo tipo de inmuebles y cartera, propiedad de las entidades públicas de cualquier orden o rama; así como, de los organismos autónomos e independientes previstos en la Constitución Política y en la Ley, sociedades con aportes estatales de régimen especial y patrimonios autónomos titulares de activos provenientes de las entidades anteriormente mencionadas.

6.2 Contexto Interno

- **Factor Humano**

  Los colaboradores, personal de servicio tercerizado, estudiantes en práctica, clientes, proveedores y contratista hacen parte de los activos de información de la entidad. Cada uno de estos recursos se encuentran en interacción con cada uno de los procesos de la entidad realizando diferentes actividades como; gestionando, procesando, almacenando, distribuyendo, intercambiando y/o consultando información que puede estar clasificada como; confidencial, uso interno o pública. Por lo dicho anteriormente el factor humano es un factor importante para el cumplimiento de los lineamientos y políticas de seguridad de la información. Como el factor humano representa un riesgo en CISA se ha dispuesto un plan de comunicaciones y de capacitación donde se sensibiliza, capacita y concientiza al factor humano.

- **Infraestructura Física**

  La oficina principal de CISA está ubicada en Bogotá y en su primer piso cuenta con la sucursal Bogotá. Este edificio es propio y está ubicado en la calle 63 numero 11-09 cuenta con tres pisos. Donde se tienen controles de seguridad como:

- ✓ Para acceder al edificio, se exige portar el carné en un lugar visible tanto para los colaboradores como para los visitantes.
- ✓ Control de acceso físico para cada unas de las personas que acceden al edificio.
- ✓ Circuito cerrado de televisión para monitoreo y seguridad en el edificio.
- ✓ Identificación de Áreas Seguras.
- ✓ Señalización de la ruta de Evacuación.
- ✓ Señalización de áreas
- ✓ Para ingresar al centro de cableado de cada piso centro de cómputo, se realiza únicamente personal autorizado con el uso de llaves y con acceso biométrico. (Para el caso del centro de cómputo se cuenta con una planilla de acceso para los visitantes).

Además, CISA tiene 3 sucursales ubicadas en las siguientes ciudades; Cali, Medellín y Barranquilla. Con respecto a los controles están implementados de la siguiente manera:

- ✓ Para acceder al edificio, se exige portar el carné en un lugar visible tanto para los colaboradores como para los visitantes.
- ✓ Control de acceso físico es realizado por el Front de la sucursal a través del software de gestión documental.
- ✓ Circuito cerrado de televisión para monitoreo y seguridad de los locales.
- ✓ Señalización de la ruta de Evacuación.

- **Infraestructura Tecnológica**

CISA, cuenta con un centro de cómputo ubicado en el tercer piso de la oficina de la ciudad de Bogotá y el cual es el principal centro de procesamiento de la compañía y centraliza servicios como; telefonía, impresión, bases de datos, sitios web entre otros. Es necesario que dicho lugar conserve un nivel de seguridad física y ambiental adecuado. Por ello el centro de cómputo posee un control de acceso, de manera que se evite el acceso a personal no autorizado a los equipos y a la información almacenada en éste.

La estratégica de recuperación ante desastres -DRP. Con base en la capacidad de recuperación tecnológica, con el fin de atender un evento

que conlleve a la indisponibilidad de los servicios de información claves presentes en el centro de computo principal y que son la herramienta principal para habilitar las operaciones de los procesos críticos de CISA frente a un evento de interrupción.

Analizando los dominios de infraestructura tecnológica (Seguridad, Almacenamiento, Servidores, Comunicaciones, Directorio Activo), la Alta Dirección determinó como estrategia de recuperación ante desastres el servicio (DRaaS):

Plan de Recuperación ante Desastres como Servicio (DRaaS- Disaster Recovery as a Services).

Se basa en la replicación, mediante el alojamiento de los datos, se almacenan, administran y procesan en una red de servidores virtualizados alojados de forma remota (físicos o virtuales), los cuales pertenecen a un tercero que los administra de acuerdo con las necesidades de CISA. Se accede utilizando internet para la recuperación de la tecnología de información en caso de presentarse un evento de interrupción.

- **Gestión por proceso**

Teniendo en cuenta que la competitividad de CISA va mucho más allá de la calidad y de la productividad para transcender hacia el desarrollo y protección del personal, su infraestructura y activos operacionales sin afectar el ambiente, asegurar la información y tratamiento de los riesgos que pueden tener. La entidad viene trabajando, desde hace tiempo atrás, en la implementación de los requerimientos normativos a partir del direccionamiento y compromiso empresarial, la administración documental, los registros, las auditorías internas, las acciones correctivas y preventivas, el entrenamiento del personal, el involucramiento de los diferentes grupos objetivo y las mediciones, entre otros.

El sistema de seguridad de la información inicia la implementación a partir del año 2013 en el proceso de infraestructura tecnológica y a la fecha se extendiendo a nueve procesos adicionales como lo son; Gestión de Activos, Comunicaciones y Relacionamiento, Soluciones para el Estado, Servicio Integral al Ciudadano, Gestion Jurídica del

Negocio, Saneamiento, Administrativa y Suministros, Direccionamiento Estratégico y Gestión del Talento Humano.

Para el año 2021 se encuentra proyectado la implementación para los cuatro procesos restantes del mapa de procesos de la entidad. Logrando así que cada uno de los procesos estén alineado y enmarcado en el sistema de seguridad de la información facilitando, diseñando, estableciendo e implementando la seguridad para la información de la entidad.

6.3 Contexto Externo

- **Factor Tecnológico**

CISA, como entidad mixta vinculada al Ministerio de Hacienda y crédito publico debe promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor publico en entorno de confianza digital a través de la política de gobierno digital.

MINTIC a través de la dirección de gobierno digital Formula las políticas, programas y planes de adopción y apropiación de Tecnologías de la Información en las entidades del Estado, en orden a garantizar la efectividad de la gestión y la interoperabilidad entre los diferentes sistemas, incorporando la debida gestión de riesgos asociada a la información, bajo las pautas de las entidades dedicadas a la seguridad digital en el país.

- **Factor Normativo y Legislativo**

CISA, dispone de un procedimiento para la identificación y actualización de los requisitos legales aplicables y otros requisitos del Sistema de Gestión de Seguridad de la Información -SGSI basado en las normas internacionales y normativas legales vigentes. Las normas, leyes, decretos y resoluciones, etc. Las cuales se han tenido en cuenta para la implementación del SGSI las cuales se encuentran identificadas, documentadas y en los casos que se requiera con su respectivo plan de acción en la matriz de requisitos legales de Seguridad de la Información. Dentro de los requisitos legales más

relevantes para seguridad de la información se encuentran; el modelo de seguridad y privacidad de la información (MSPI), la ley Orgánica de Protección de Datos 1581 de 2012 (LOPD), la ley de transparencia y de acceso a la información 1712 de 2014, Decreto 1499 de 2017, Modelo de Integración de Planeación y Gestión -MIPG. Donde CISA, para dar cumplimiento a cada uno de estos requisitos a definido los respectivos planes de acción. Dependiendo de la complejidad de los diferentes planes, sus actividades pueden ser extensas y depender de recursos por esta razón se encuentra definido realizar la revisión de los requisitos legales por lo menos una vez al año.

- **Factor Económico**

  CISA, cuenta con recursos propios para la ejecución del presupuesto. En caso de que la economía del país se ve afectada por cualquier variable, algunas líneas de negocio de CISA se afectarían porque no se podría desarrollar las metas como se encuentran establecidas. Para mitigar este riesgo CISA cuenta con un plan de continuidad del negocio para el desarrollo de sus actividades.

- **Factor Político**

  A nivel político CISA, fue establecida a través de la ley 795 de 2003 en el artículo 91, el decreto 033 de 2015 y el articulo 2 de los estatutos sociales. Por lo anteriormente se encuentra como amenaza las siguientes actividades:

  - ✓ En caso de que se modifique la ley cambiando el rol que tiene actualmente CISA.
  - ✓ Si se declara amnistía para toda la cartera pública del estado.
  - ✓ En el momento que se determine fusionar entre CISA y cualquier otra entidad.

- **Entes de Control**

  CISA, esta continuamente expuesta a revisiones y seguimientos por parte de los entes de control; la entidad se apoya en el SGSI como un mecanismo de control que le permite mantener la confidencialidad, integridad y la disponibilidad de los activos de información para responder oportuna y eficazmente las solicitudes de los entes de control.

  Las entidades que revisan a CISA, son:

  - ✓ Procuraduría General de la Nación
  - ✓ Contaduría General de la Nación
  - ✓ Contraloría General de la República
  - ✓ Archivo General de la Nación
  - ✓ Oficina de Auditoría Interna

6.4 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 lideres 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 quien tiene responsabilidad y autoridad para:

- Asegurar que el sistema integrado de gestión se establece, implementa y mantiene de acuerdo a los requisitos de las normas que se encuentran definidas para CISA.
- Informar a la alta dirección sobre el desempeño del sistema integrado de gestión 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.

A través del articulo 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.

6.5 Planificación

La planeación estratégica de seguridad de la información se encuentra enmarcada dentro del mapa de ruta para los años 2020 al 2021 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 dependiendo de lo que disponga la Entidad para aprobar.

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

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.

6.6 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 octubre del año respectivo, se realiza la revisión por parte de la Alta Dirección y el Representante de la Dirección del SIG 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.

6.7 Operación

La seguridad de la información opera desde la Jefatura de Procesos en el marco de referencia de la norma NTC 27001:2013.

6.8 Evaluación de Desempeño

Actualmente el sistema de seguridad de la información cuenta con tres indicadores en el proceso de mejora se ajustan los indicadores existentes y se definen uno nuevos para apoyar el plan estratégico de seguridad de la información.

En CISA, se establece el procedimiento que permite realizar seguimiento y medición del desempeño del Sistema Integrado de Gestión.

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 lideres de los procesos realicen una revisión integral de los indicadores, con el fin de asegurar la pertinencia de los mismos; 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

En CISA, se cuenta con una Política y Procedimiento para Planear y Ejecutar Auditorías Internas al Sistema Integrado de Gestión. A continuación, se listan las generalidades al respecto:

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

  a) La información suficiente y apropiada para planificar las auditorias
  b) La cooperación adecuada de los auditados
  c) El tiempo y los recursos adecuados

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

- Debe realizarse mínimo una auditoria interna al año para el Sistema Integrado de Gestión.

- Las auditorias deben cumplir con la metodología planteada en la Política y Procedimiento para Planear y Ejecutar Auditorías Internas al Sistema Integrado de Gestión.

- 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 auditoria interna deben llevarse a cabo la metodología establecida.

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

Para llevar a cabo la planificación del programa de auditoria interna, es necesario que los responsables de la planificación del programa de auditorias tengan en cuenta los siguientes parámetros:

- Determinar los objetivos del programa de auditoria para dirigir la planificación y realización de las auditorias.

- Determinar la amplitud del programa de auditora, es decir, definir:

  - ✓ Objetivo de la auditoria
  - ✓ Alcance
  - ✓ Frecuencia de las auditorias que se realicen

  Es pertinente considerar como entrada de información para determinar la amplitud del programa:

  - ✓ Conclusiones y resultados de auditorías previas

- ✓ Resultado de la revisión de programas de auditorías previas
- ✓ Cambios significativos en la organización o en sus operaciones
- ✓ Revisión por la Dirección previas
- ✓ Los resultados de la valoración de riesgos de las actividades de los procesos

- Determinar los recursos necesarios para el programa de auditoria, tales como:

  - ✓ Recursos financieros para desarrollar, implementar, dirigir y mejorar actividades de auditoria.
  - ✓ Procesos para alcanzar y mantener la competencia de los auditores y para mejorar su desempeño
  - ✓ Amplitud del programa de auditoria
  - ✓ Tiempo de viaje, alojamiento y otras necesidades de la auditoria

6.9 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.

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 practicas
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. Iniciativas

Desde Seguridad de la Información se define el plan de proyecto del año 2020 al 2021 alineado a las perspectivas del plan estratégico de la Entidad.

PERSPECTIVA	OBJETIVO DE SEG. INF.	DIMENSION MIPG	PROYECTO
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
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
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
Excelencia Operativa	Disminuir el nivel de riesgo asociado a los activos de información.	- Direccionamiento	Ampliación del alcance de SGSI

		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.	
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)
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
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	Análisis de vulnerabilidades en código fuente

		eficacia de los procesos frente a las necesidades de los grupos de valor.	
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
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

8. Presupuesto

8.1 Presupuesto de Inversión

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

- Plan de Sensibilización en Seguridad de la Información
- Fortalecimiento de Competencias específicas en Seguridad de la Información
- Centro de monitoreo de Ciberseguridad 7x24 - SOC (Security Operation Center)
- Gestión de Accesos Privilegiados
- Análisis de vulnerabilidades en código fuente
- Fortalecimiento de capacidades en gestión de incidentes
- Revisión independiente de la gestión de la seguridad de la información

8.2 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

9. Recursos

El Sistema de Seguridad de la Información cuenta actualmente con una asignación presupuestal a través de rubro asignado a la Dirección de Tecnología. 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
Ordenes de Servicios Vigentes	Actualmente se cuenta con Orden de Servicio vigentes para: 1. Análisis de Vulnerabilidades 2. Mantenimiento Herramienta de Gestión del Sistema de Seguridad de la Información Es importante indicar que para los proyectos planteados para el año 2020 se tiene presupuesto asignado tanto para ordenes de servicio como contratos.