INFORME DE AUDITORIA

NOMBRE DEL PROCESO, ÁREA O TEMA A AUDITAR: Auditoría Integral de Gestión al Proceso de Infraestructura Tecnológica Componente Seguridad de la Información y Ciberseguridad.

INFORME PRELIMINAR: 24/04/2021 **INFORME DEFINITIVO**: 10/05/2021

1. INTRODUCCIÓN

El Gobierno de Seguridad de la Información garantiza la confidencialidad, integridad y disponibilidad de la información, evitando acciones no autorizadas con ella, en particular, su uso, divulgación, distorsión, alteración, investigación y destrucción. Las disposiciones de seguridad de la información son las mismas para todas las formas de almacenamiento de información: física, digital o cualquier otra. La información solicitada y aportada por el Oficial de la Información de Central de Inversiones S.A., así como la recolectada a través de las entrevistas y mesas de trabajo fue la base sobre la cual se desarrolló la Auditoría al Componente de Seguridad de la Información, por esta razón se deja explicito que la información base de la evaluación al componente cuenta con las características de integridad requeridas para sustentar los hallazgos, las observaciones y las recomendaciones generadas en el presente informe.

2. OBJETIVO DE LA AUDITORÍA AL COMPONENTE DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

El objetivo general de la auditoría es evaluar la gestión del componente de Seguridad de la Información y Ciberseguridad en cuanto a preservar la confidencialidad, integridad, disponibilidad de los datos en los activos de información de Central de Inversiones S.A. CISA.

Los objetivos específicos definidos para la evaluación de este componente son los siguientes:

a. Identificación de la normatividad interna y externa que deberá cumplir de conformidad con los organismos de control.
b. Evaluación del Modelo de gobierno de Ciberseguridad.
c. Análisis de los riesgos, amenazas y vulnerabilidades a los cuales está expuesta la entidad, y la identificación de controles existentes.
d. Identificación de herramientas utilizadas por la entidad para la gestión de la Ciberseguridad y sugerencia de nuevas herramientas.
e. Revisión y evaluación de la valoración del riesgo y tratamiento de riesgos.
f. Evaluación de la gestión de seguridad realizada por la entidad.
g. Evaluación de la metodología de riesgos de seguridad de la información y su aplicación.
h. Verificación del estado actual del plan de tratamiento de riesgos.
i. Evaluación de los roles y responsabilidades de seguridad de la información.
j. Evaluación de políticas y procedimientos existentes sobre seguridad de la información (Incluyendo ciberseguridad).
k. Verificación de la vigencia y consistencia del inventario de activos de información.
l. Evaluación de la responsabilidad de los propietarios de los activos de información.
m. Evaluación de los requerimientos de seguridad para proveedores.
n. Evaluación del proceso de gestión de incidentes de seguridad de la información.
o. Evaluación de controles para protección de la integridad y confidencialidad de los sistemas de información.
p. Evaluación del cumplimiento del marco legal, regulatorio y contractual de seguridad de la información. (Acuerdos de confidencialidad, protección y datos personales, derechos de autor, entre otros).
q. Evaluación de la seguridad de la plataforma tecnológica y sistemas de información.
r. Revisión y evaluación de la configuración de seguridad de las instancias de la base de datos “Local”, que contiene la información de las aplicaciones Core contra las buenas prácticas de seguridad Microsoft.
s. Revisión del estándar de seguridad para la configuración de las bases de datos, de conformidad a los mejores estándares.
t. Revisión y verificación de perfiles-usuarios en las aplicaciones que se tienen acceso a atributos (crear, modificar, actualizar y borrar).
u. Identificación de las debilidades y oportunidades de mejora relacionados con la Ciberseguridad.
v. Verificación de la preparación de la entidad, para afrontar y enfrentan ataques cibernéticos a través de una estrategia adecuada de Ciberseguridad.

w. Establecimiento de un plan de acción para minimizar la brecha entre el nivel de madurez que tiene CISA y el nivel deseado en la gestión de Seguridad de la Información que incluye la Ciberseguridad.

3. ALCANCE

Se realizó Auditoría Interna de Gestión al componente de Seguridad de la Información, evaluando la aplicabilidad de los procesos y procedimientos establecidos en los manuales y las circulares internas, políticas y normatividad legal vigente, donde se evaluó el periodo comprendido entre el 1 de enero de 2020 al 31 de diciembre de 2020.

Esta auditoría se llevó acabo en cumplimiento a las normas y técnicas de auditoría generalmente aceptadas, con fundamento en normas internacionales de auditoría basadas en riesgos, la guía de auditoria para entidades públicas versión 3, Estatuto de Auditoria Interna, séptima dimensión y tercera línea de defensa del Modelo Integrado de Planeación y Gestión – MIPG, la auditoría se realizó del 23 de febrero al 5 de abril de 2021.

4. DESARROLLO DE LA AUDITORÍA

La auditoría se desarrolló basada en el cumplimiento de las fases y actividades desarrolladas principalmente en el Modelo de Seguridad y Privacidad de la Información establecido por MINTIC y dado que CISA es una entidad de naturaleza pública, está en la obligación de acoger su Sistema de Gestión de Seguridad de la Información de acuerdo a los lineamientos establecidos en el Decreto 1078 de 2015 de MINTIC, las buenas prácticas ISO 27001:2013 y la NIST 800-53 Marco de Referencia de Ciberseguridad.

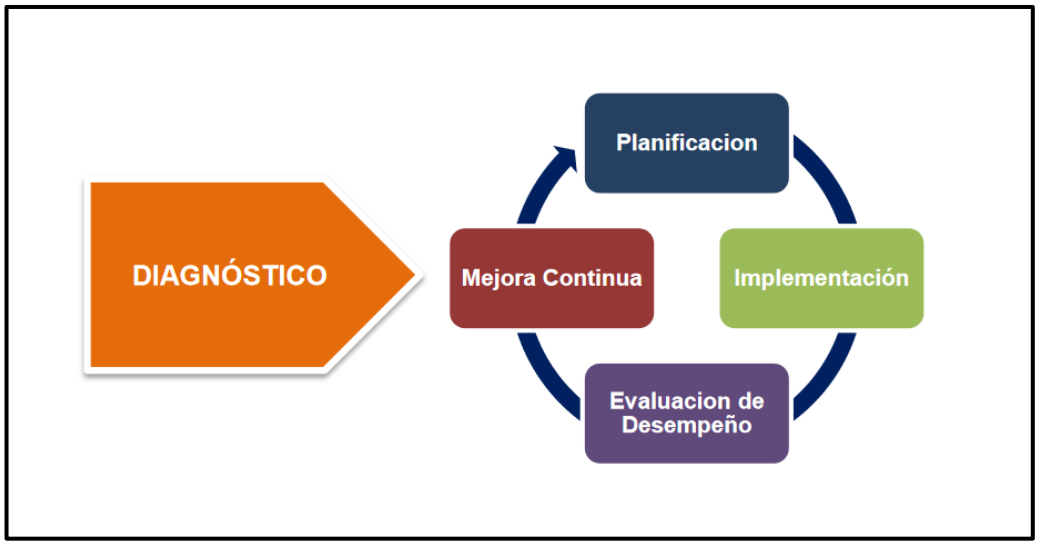


Figura 1. Ciclo del Modelo de Seguridad y Privacidad de la Información

Dentro del alcance de la auditoría se establecieron actividades a evaluar que hacen parte del Modelo de Seguridad y Privacidad de la Información en sus distintas fases. Presentamos los resultados producto del análisis de las evidencias suministradas por el Oficial de Seguridad de la Información.

4.1. EVALUACIÓN DE AUDITORÍAS ANTERIORES

4.1.1. Auditorías Anteriores: Revisadas las acciones previstas en el Plan de Mejoramiento suscrito producto de la Auditoria realizada en el año 2017 se observaron 2 hallazgos asociados al componente de Seguridad de la Información cuyo detalle se encuentran en el hallazgo 6.4 Diagnóstico sobre la implementación ISO27001. A continuación, se muestra la gestión realizada por el Oficial de Seguridad de la Información sobre estos hallazgos.

HALLAZGO	DESCRIPCION DE HALLAZGO	ACCION DE MEJORA	ACTIVIDADES / DESCRIPCIÓN	ACTIVIDADES / UNIDAD DE MEDIDA
6.4 Diagnóstico sobre la implementación ISO27001	No se cuenta con indicadores que permitan medir el cumplimiento de las prácticas de seguridad CISA por terceros	Crear indicadores de control de aplicación y cumplimiento de buenas prácticas de seguridad por parte de terceros	Crear set de indicadores como son: i. Tratamiento de eventos relacionados en el marco de Seguridad y Privacidad de la Información, ii. Cumplimiento de políticas de SI en la Entidad.	Indicadores creados, aprobados y medidos
6.4 Diagnóstico sobre la implementación ISO27001	No se cuenta con indicadores que permitan medir el cumplimiento de las prácticas de seguridad CISA por terceros	Trasladar la responsabilidad del Comité de Seguridad de la información al Comité Institucional de Desarrollo Administrativo - PDA	Formalizar la inclusión del Comité de SI en el alcance del Comité PDA	Comité instaurado y con trazabilidad dentro del PDA

OBSERVACIÓN 6.4 Diagnóstico sobre la implementación ISO27001: Se implementaron cláusulas de auditabilidad en temas de seguridad de la información para proveedores críticos de la entidad y en el Comité Institucional de Gestión y Desempeño se incluyeron funciones de monitoreo y seguimiento al Modelo de Seguridad y Privacidad de la Información.

En la ruta \\serverfile\Presidencia\AUDITORIA_INTERNA\2017\AuditoriadeTecnologia, provista por CISA para verificación de evidencias, se observan los soportes de plan de mejoramiento hacia Auditoría Interna.

Se concluye que las evidencias suministradas pueden cerrar las oportunidades de mejora señaladas en el informe.

4.1.2. Plan de Mejoramiento CGR – TI: Revisado el Plan de Mejoramiento suscrito entre la Contraloría General de la Republica y CISA, no se identificaron acciones relacionadas con el componente de Seguridad de la Información.

4.2. EVALUACIÓN DE RIESGOS

4.2.1. Metodología de Riesgos: Central de Inversiones S.A tiene definido en la Circular Normativa N° 107 "*Política de Administración de Riesgos en Central de Inversiones S.A*" Versión 22 del 18 de diciembre de 2020, los lineamientos relacionados con la gestión de los riesgos que se aplican en los procesos de la organización, dentro de los cuales se encuentra los del proceso de Seguridad de la Información de la entidad. La metodología está alineada con los aspectos definidos en la guía de riesgos de la Función Pública y el estándar internacional ISO 31000 sobre Administración de Riesgos.

4.2.2. Valoración y Tratamiento de los Riesgos: La información de riesgos aportada por el proceso auditado, refleja que el Oficial de Seguridad de Información viene aplicando la metodología definida en la Circular Normativa N°107 "*Política de Administración de Riesgos en Central de Inversiones S.A*" Versión 22 del 18 de diciembre de 2020, y que se ha realizado el monitoreo periódico correspondiente. En el mapa relacionado se evidencian 51 riesgos enfocados a la seguridad de la información, sin embargo, en el análisis realizado a estos riesgos se identifican que algunos de ellos no tienen asociadas causas que puedan afectar la integridad, disponibilidad y confidencialidad de la información y también se confunden causas con riesgos.

4.2.3. Identificación y Calificación de los Controles

En la matriz de riesgos de seguridad de la información suministrada por la Oficial de Seguridad de la Información se evidencia que algunos controles implementados para mitigar los riesgos se enfocan a mitigar la probabilidad de ocurrencia más no al impacto. Existen seis (6) riesgos con calificación pura extrema y alta que siguen manteniendo la misma calificación en el riesgo residual, dejando a la entidad en un perfil de riesgo alto.

Es importante señalar que los riesgos de seguridad de la información siempre serán adversos, es decir, que siempre que se presenten podrán afectar cualquiera de los

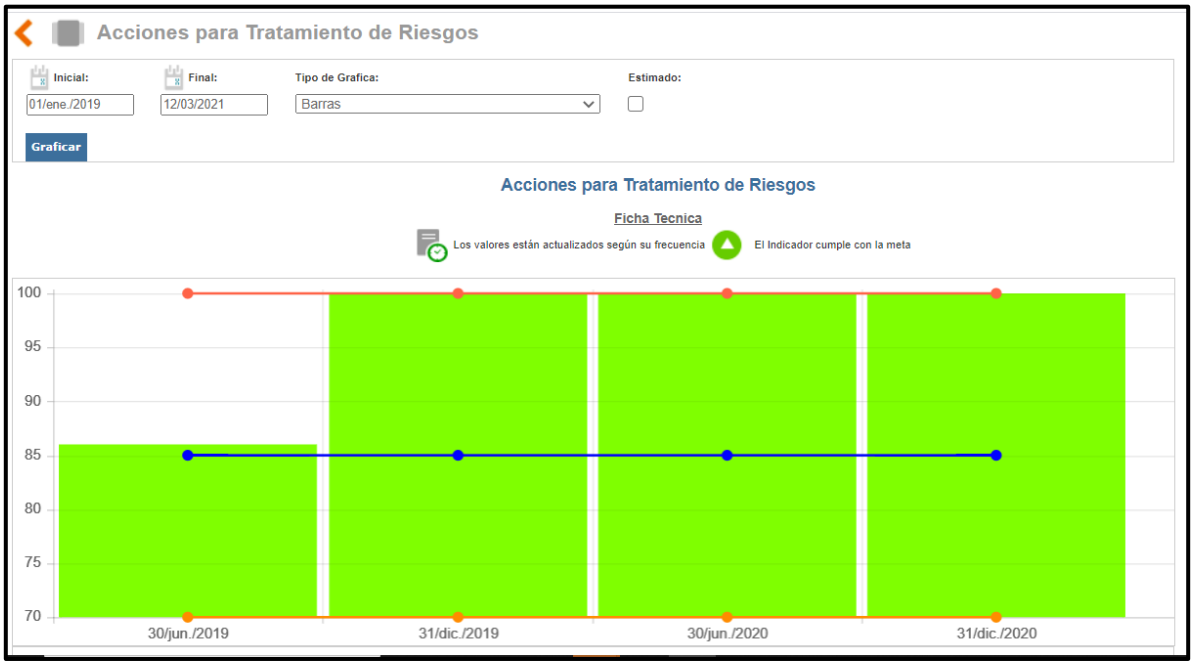
principios de seguridad de la información, por lo tanto, la aplicación de controles debería estar enfocado a mitigar probabilidad de ocurrencia e impacto.

Se debe tener en cuenta que Central de Inversiones S.A. CISA es una entidad que entre sus servicios se encuentra la de diseñar y desarrollar software para terceros, además con este software también se soportan los procesos misionales, en este sentido se recomienda que el perfil de riesgo de seguridad de la información esté por lo menos en un nivel moderado.

4.3. EVALUACIÓN DE INDICADORES

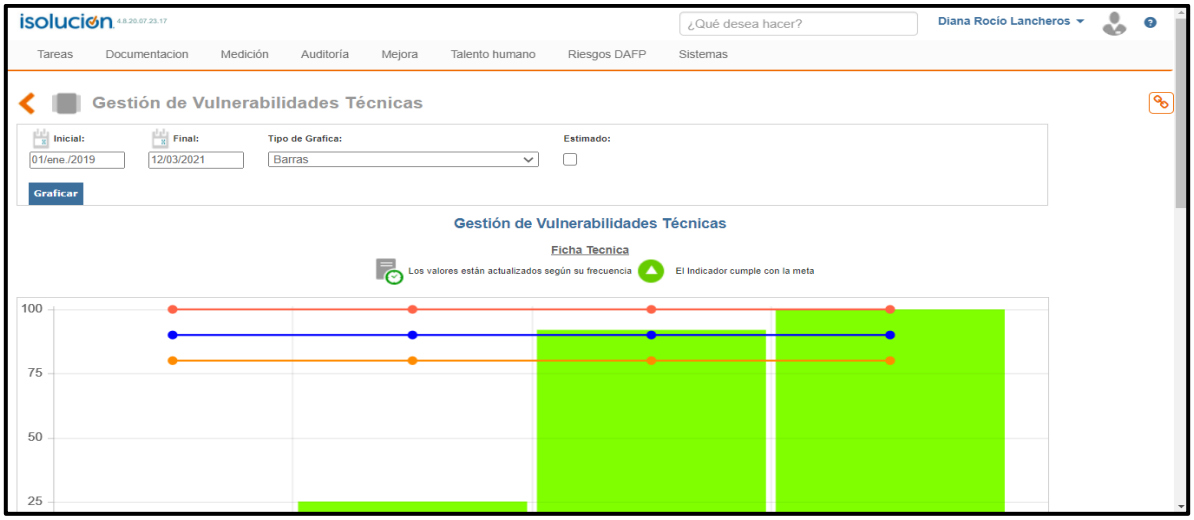
Se revisaron los indicadores del Proceso de Seguridad de la Información registrados y monitoreados, a través del sistema ISOLUCION. Este proceso tiene definido tres (3) indicadores y cuyo análisis se presenta a continuación:

4.3.1. Acciones para el Tratamiento de Riesgos: El objetivo de este indicador es medir el cumplimento de los planes de tratamiento definidos para los riesgos encontrados en la valoración de los activos de información de SGSI. Dentro de los 2 seguimientos de cumplimiento de este indicador realizados en el año 2020 se observa el 100% de cumplimiento:



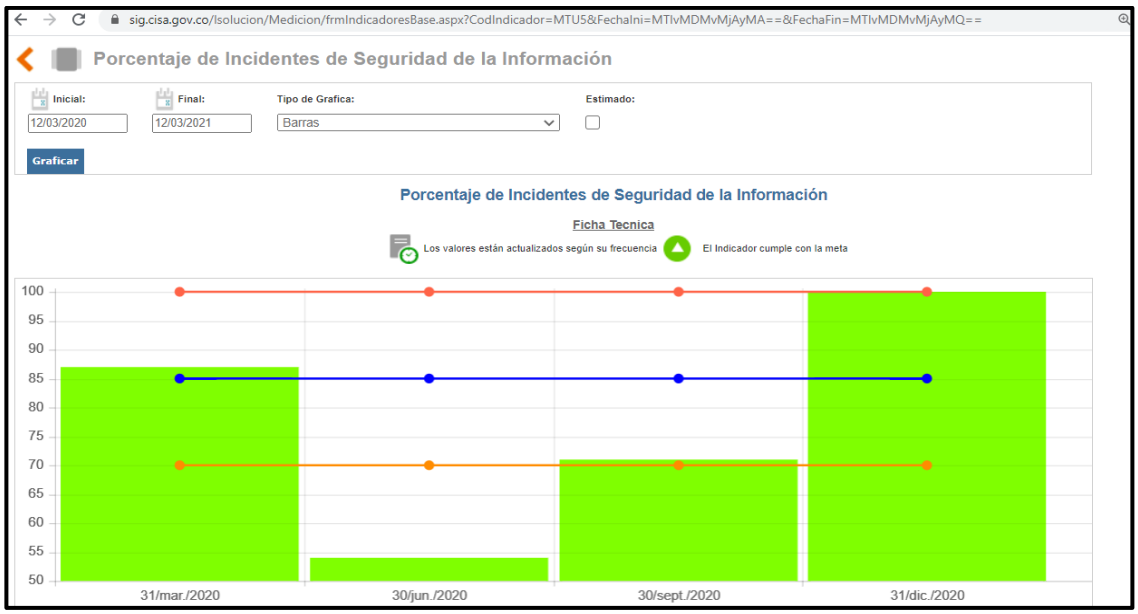
Fuente: 1-Información del Oficial de Seguridad de la Información con corte a marzo 2021

4.3.2. Gestión de vulnerabilidades técnicas: El objetivo de este indicador es realizar la medición de las vulnerabilidades técnicas críticas que sean tratadas en los tiempos definidos para su mitigación después de su identificación. Dentro de los 2 seguimientos de cumplimiento de este indicador realizados en el año 2020 se observa el 100% de cumplimiento:



Fuente: 2-Información del Oficial de Seguridad de la Información con corte a marzo 2021

4.3.3. Porcentaje de incidentes de seguridad de la información: El objetivo de este indicador es medir los incidentes de seguridad de la información atendidos.



Fuente: 3-Información del Oficial de Seguridad de la Información con corte a marzo 2021

Los indicadores acá mencionados y evaluados están acorde con el nivel de madurez del cumplimiento del Modelo de Seguridad y Privacidad de la Información que tiene CISA y cumplen con lo establecido por MINTIC.

4.4. GESTIÓN DE VULNERABILIDADES TÉCNICAS

A finales del 2020 CISA contrató los servicios del proveedor NEWNET para realizar un análisis de vulnerabilidades técnicas a 10 activos considerados críticos para la entidad. A continuación, mostramos un resumen de los resultados de la evaluación realizada:

ACTIVO	DIRECCIÓN IP	CRÍTICAS	ALTAS	MEDIAS
vpn.cisa.gov.co	201.217.201.197	0	0	3
www.cisa.gov.co	201.217.201.202	0	1	3
junta.cisa.gov.co	201.217.201.203	0	0	1
prometeo.cisa.gov.co	201.217.201.210	0	0	2
ase.cisa.gov.co	201.217.201.215	0	2	2
monitoreo.cisa.gov.co	201.217.201.216	0	0	4
informes.cisa.gov.co	201.217.201.220	0	0	3
TemisAAA.cisa.gov.co	201.217.201.223	0	0	3
MDBSERVER	172.30.1.106	1	1	4
PROMETEO	172.30.1.139	0	0	2

Fuente 4. Tomado del Informe de vulnerabilidades de NewNet – Febrero 2021 suministrado por la Oficial de Seguridad

Se solicitó el plan de remediación de las vulnerabilidades críticas y altas, donde se evidencia que no se tienen actividades claras y definidas para mitigar la vulnerabilidad crítica encontrada en el servidor MDBSERVER, así mismo se evidencia que no se tienen establecidas actividades para mitigar las vulnerabilidades críticas y altas encontradas en el servidor ASE.CISA.GOV.CO.

No obstante, consideramos que el plan de mitigación para la vulnerabilidad crítica del servidor MDSERVER es procedente y debe quedar como las acciones posteriores a la evaluación por parte de la Auditoría, es decir, que las observaciones

realizadas por la Oficial de Seguridad de la Información en la mesa de trabajo del día 5 de mayo de 2021 y la documentación soporte y comentarios escritos vía correo electrónico del día 6 de mayo de 2021 deben ser consideradas como plan de mejoramiento, por lo tanto el hallazgo 5.1 del informe preliminar de este documento se mantiene.

Es importante mencionar que la vulnerabilidad critica encontrada en el servidor MDBSERVER podría afectar la integridad y disponibilidad de las bases de datos instaladas en este servidor, por lo que se hace imprescindible la ejecución inmediata del plan de mitigación elaborado por la Dirección de Tecnología.

4.5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CISA cuenta con la Circular Normativa 093 Política y Procedimiento de Gestión Tecnológica – Versión 62 del 30 de diciembre de 2020*en* la cual se establecen directrices de seguridad informática y operación de tecnología, pero no establece ningún lineamiento sobre seguridad de la información.

En el año 2020 se presentó a la Alta Dirección un documento que consolida la política general y las políticas específicas de seguridad de la información (Políticas y Procedimientos del SGSI v1). Dentro del análisis realizado a la política general de seguridad de la información se evidencia que esta política no cuenta con los siguientes elementos:

- Compromiso de la Alta Dirección para asegurar los activos de información.
- La entidad requiere recurso humano, económico y tecnológico para que pueda gestionar los riesgos de seguridad de la información a los que está expuesta la entidad.
- El compromiso del cumplimiento legal y de buenas prácticas.
- Esta política debe estar aprobada y oficializada en el SIG.

La Oficial de Seguridad de la Información informó al equipo auditor que este documento había sido presentado en el Comité Institucional de Gestión y Desempeño del mes de diciembre de 2020, pero no se evidenció el acta de aprobación y su correspondiente formalización en la intranet de CISA.

4.6. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

En el año 2020 se presentó a la Alta Dirección un documento que consolida la política general y las políticas específicas de seguridad de la información (Políticas y Procedimientos del SGSI v1). Dentro del análisis realizado al documento se evidencia que CISA adopta las siguientes políticas de seguridad:

- Dispositivos móviles.
- Trabajo en casa.
- Política de mensajes y correos electrónicos.
- Manejo de medios.
- Medios de almacenamiento externo.
- Reutilización o eliminación de equipos de cómputo.
- Control de acceso.
- Usuarios y contraseñas.
- Desbloqueo de cuentas de usuario.
- Eliminación de usuarios.
- Superusuario.
- Usuarios de red.
- Gestión de derechos de acceso privilegiado.
- Monitoreo.
- Gestión de activos de información
- Seguridad física y del entorno.
- Gestión de capacidad y disponibilidad.
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Política de generación y restauración de backup.
- Sincronización de relojes.
- Gestión de vulnerabilidades técnicas.
- Política de desarrollo seguro.
- Política para el uso de recursos de internet

No obstante, no se encuentran políticas enfocadas a:

- Gestión de incidentes de seguridad de la información.
- Gestión de seguridad con los proveedores.
- Roles y responsabilidades.
- Seguridad de la información en la continuidad de negocio.
- Cumplimiento.

La Oficial de Seguridad de la Información informó al equipo auditor que este documento había sido presentado en el Comité Institucional de Gestión y Desempeño del mes de diciembre de 2020, pero no se evidenció el acta de aprobación y su correspondiente formalización en la intranet de CISA.

4.7. PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

CISA cuenta con los siguientes procedimientos que soportan el cumplimiento de algunas políticas de seguridad de la información establecidas por la entidad las cuales se muestran a continuación:

Anexo No 01	Procedimiento para gestionar las vulnerabilidades de la plataforma tecnológica
Anexo No 02	Instructivo de Identificación, Clasificación y Plan de tratamiento de Activos de Información
Anexo No 03	Instructivo para la copia de Información en medios extraíbles
Anexo No 04	Procedimiento para el borrado seguro de dispositivos móviles, discos y volúmenes lógicos
Anexo No 05	Instructivo Gestión de Cambios
Anexo No 06	Instructivo para la generación y restauración de backup
Anexo No 07	Instructivo para la atención de incidentes y requerimientos de seguridad de la información
Anexo No 08	Procedimiento para el registro de software desarrollado en CISA
Anexo No 09	Matriz de requisitos legales de Seguridad de la Información
Anexo No 10	Formato de Cadena de Custodia
Anexo No 11	Planilla de Control Ingreso al Centro de Computo

Sin embargo, no se evidencian procedimientos que soporten el cumplimiento de las siguientes políticas de seguridad de la información: criptografía, seguridad de las comunicaciones y relaciones con proveedores tal como lo establece la Guía No 3

Numeral 6 Procedimientos de Seguridad de la Información establecidos por el Modelo de Seguridad y Privacidad de la Información de MINTIC.

4.8. ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

CISA cuenta con un Oficial de Seguridad de la Información quién tiene la responsabilidad de planear, coordinar y administrar las actividades que soportan el Sistema de Gestión de Seguridad de la Información como lo son, entre otras:

- Gestión de Activos de Información
- Gestión de Riesgos de Seguridad de la Información
- Gestión de Incidentes de Seguridad de la Información
- Plan de Cultura y Sensibilización de Seguridad de la Información
- Elaboración, formalización y seguimiento al cumplimiento de las Políticas de Seguridad de la Información
- Participación en las actividades de Desarrollo de Software y Control de cambios

Por otra parte, el Comité Institucional de Gestión y Desempeño tiene establecidas funciones con el fin de asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información en la entidad.

El equipo auditor observó que el área de Seguridad de la Información tiene fortalezas enfocadas al Gobierno de Seguridad de la Información (elaboración y formalización de políticas, lineamientos y procedimientos de seguridad), no obstante, también se observa que se tienen falencias en la operación y seguimiento del Modelo de Seguridad y Privacidad dado que no se cuenta con el personal suficiente para atender los requerimientos, seguimiento y cumplimiento del gobierno de seguridad.

4.9. GESTIÓN DE ACTIVOS DE INFORMACIÓN

CISA cuenta con los siguientes documentos e instrumentos para realizar la gestión de activos de información:

- Circular Normativa 093 – Anexo 09 "Instructivo de Identificación, Clasificación y Plan de tratamiento de Activos de Información."
- Aplicativo Novasec – Módulo Activos de Información.

- Matriz de registro de activos de información publicada en la página web de CISA.

En los instrumentos anteriormente señalados se encuentran controles de seguridad de la información tales como:

- Propietario de los activos.
- Uso apropiado de los activos.
- Devolución de los activos.
- Clasificación de la Información.
- Manejo de los activos.
- Etiquetado de los activos.

No se evidencia el rotulado de la información de acuerdo con la clasificación establecida por la entidad (información pública, información pública clasificada e información pública reservada).

4.10. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

CISA cuenta con los siguientes elementos para realizar la gestión de incidentes de seguridad de la información en la entidad:

- Instructivo para la atención de incidentes y requerimientos de seguridad de la información.

- Herramienta tecnológica ZEUS cuya función es ingresar y categorizar los incidentes de seguridad de la información para que éstos sean gestionados por el Oficial de Seguridad de la Información.

4.11. EVALUACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Durante el desarrollo de la auditoría se evidenció el cumplimiento de los siguientes controles de seguridad de la información:

- Cancelación o ajuste a los derechos de usuarios.
- Sistema de Gestión de Contraseñas.
- Seguridad del Cableado.

- Mantenimiento a los Equipos.
- Política de Escritorio y Pantalla Limpia.
- Protección Contra Código Malicioso.
- Seguridad de los servicios de red.
- Sincronización de relojes.
- Perímetro de seguridad física.
- Controles de acceso físico.
- Protección contra amenazas externas y ambientales.
- Trabajo en áreas seguras.
- Revisión y verificación de perfiles-usuarios en las aplicaciones.
- Seguridad en bases de datos.
- Hardening de servidores.

Producto de la revisión de la auditoría se observaron las siguientes situaciones:

a. No se realiza una revisión periódica de las políticas de seguridad de las bases de datos por parte del Oficial de Seguridad de la Información. La última revisión de estas políticas fue realizada en el año 2019.

b. No se cuenta con controles ambientales en las instalaciones físicas de CISA. Existe una oportunidad de mejora (número 1199) la cual se encuentra en desarrollo y cuyo objetivo es implementar controles de seguridad ambiental en el Centro de Cómputo.

c. No se cuenta con evidencia que soporte la revisión de los roles y perfiles de las aplicaciones por parte de los líderes de los procesos misionales. El administrador ICM remite mensualmente el listado de usuarios, roles y perfiles de las aplicaciones misionales a los líderes de los procesos, pero en algunos casos no se evidencian las actividades de revisión por parte de dichos líderes.

5. HALLAZGOS

Para efectos de mitigar adecuadamente los riesgos a los cuales podría estar expuesta el área de seguridad de la información, la auditoría ha evidenciado las siguientes oportunidades que mejorarán el ambiente de control tecnológico en el componente de Seguridad de la Información. A continuación, se exponen las

oportunidades de mejora sugeridas, para las cuales se espera su revisión y definición de los planes de acción correspondientes:

5.1. Gestión de Vulnerabilidades Técnicas

No se han establecido actividades claras y definidas para mitigar las vulnerabilidades críticas y altas encontradas en el servidor ASE.CISA.GOV.CO producto de la evaluación realizada por el proveedor NEWNET con informe entregado en febrero de 2021, lo cual incumple la política 5.13.3 Remediación de Vulnerabilidades de la Circular Normativa N°093 Política y Procedimiento de Gestión Tecnológica – Versión 62 del 30 de diciembre de 2020.

5.2. Evaluación de controles de seguridad de la información

a. No se realiza una revisión periódica de las políticas de seguridad de las bases de datos por parte del Oficial de Seguridad de la Información. La última revisión de estas políticas fue realizada en el año 2019.

b. No se cuenta con controles ambientales en las instalaciones físicas de CISA. Existe una oportunidad de mejora (número 1199) la cual se encuentra en desarrollo la cual busca implementar controles de seguridad ambiental en el Centro de Cómputo.

5.3. Evaluación de Riesgos

Se evidenció que existen riesgos puros con calificación extrema y alta que tienen el mismo nivel de calificación de riesgo residual luego de la evaluación de controles, situación que se presenta dado que algunos controles implementados para mitigar los riesgos se enfocan a mitigar la probabilidad de ocurrencia más no al impacto.

6. OBSERVACIONES

6.1. Gestión de Incidentes de Seguridad de la Información

Se observó que no se tiene documentado un manual de incidentes de seguridad de la información en donde se muestre de manera detallada las categorías y subcategorías de incidentes que determine la entidad, así como las actividades que se deben realizar en cada una de las fases sugeridas para la gestión de incidentes

de seguridad (preparación, detección, contención, erradicación, recuperación, seguimiento).

6.2. Roles y Responsabilidades

Se observaron falencias en la operación y seguimiento del Modelo de Seguridad y Privacidad dado que no se cuenta con el personal suficiente para atender los requerimientos, seguimiento y cumplimiento del gobierno de seguridad.

6.3. Procedimientos de seguridad de la información

No se evidencian procedimientos que soporten el cumplimiento de las siguientes políticas de seguridad de la información: criptografía, seguridad de las comunicaciones y relaciones con proveedores tal como lo establece la Guía No 3 Numeral 6 Procedimientos de Seguridad de la Información establecidos por el Modelo de Seguridad y Privacidad de la Información de MINTIC.

6.4. Política General de Seguridad de la Información

La política general de seguridad de la información no cuenta con los siguientes elementos y que deberían estar incluidos de acuerdo con lo establecido en las buenas prácticas ISO 27001:2013 Numeral 4.2.1 que cita:

- Compromiso de la Alta Dirección para asegurar los activos de información.
- La entidad requiere recurso humano, económico y tecnológico para que pueda gestionar los riesgos de seguridad de la información a los que está expuesta la entidad.
- El compromiso del cumplimiento legal y de buenas prácticas.
- Esta política debe estar aprobada y oficializada en el SIG.

6.5. Evaluación de controles de seguridad de la información

No se cuenta con evidencia que soporte la revisión de los roles y perfiles de las aplicaciones por parte de los líderes de los procesos misionales. El administrador ICM remite mensualmente el listado de usuarios, roles y perfiles de las aplicaciones misionales a los líderes de los procesos, pero en algunos casos no se evidencian las actividades de revisión por parte de dichos líderes.

7. RECOMENDACIONES

7.1. Gestión de Vulnerabilidades Técnicas

Se recomienda que los planes de acción sean diseñados e implementados de manera inmediata dado que las vulnerabilidades críticas y altas halladas podrían afectar la disponibilidad de la información de la base de datos del servidor MDBSERVER y ASE.CISA.GOV.CO.

Lo anterior con el fin de dar cumplimiento a lo estipulado en la Circular Normativa 93 de diciembre de 2020 que establece en el numeral 5.13.1 Identificación de Vulnerabilidades Técnicas, que el Oficial de Seguridad de la Información debe planificar las actividades de identificación para prevenir efectos adversos en la ejecución de descubrimientos automáticos y aplicar medidas, tales como horarios no productivos, backups, protocolos de comunicación y monitoreo de servicios entre otros.

7.2. Evaluación de controles de seguridad de la información

a. Se recomienda realizar monitoreo al cumplimiento de las políticas para el desarrollo de seguridad a las bases de datos con el fin de detectar de manera oportuna errores o problemas que se puedan presentar en la configuración de las bases de datos y que podrían afectar la integridad, confidencialidad y disponibilidad de la información contenida en las mismas. Lo anterior en concordancia con lo estipulado en la Circular Normativa 93 de diciembre de 2020 señalado en el capítulo 5.9.6 Políticas para el desarrollo de bases de datos.

b. Se recomienda retomar las actividades para implementar controles ambientales en las instalaciones de CISA con el fin de atender la oportunidad de mejora número 1199 y reducir el impacto que podría tener la entidad en caso de que se presentarán riesgos de naturaleza ambiental que podría afectar la disponibilidad, confidencialidad e integridad de la información.

c. Se recomienda que los líderes de proceso documenten la evidencia sobre la revisión del informe mensual que genera el administrador ICM y éste sea reportado al Oficial de Seguridad de la Información, en concordancia con el numeral 5.1.3.4 Actualización de las cuentas de acceso a los componentes tecnológicos y/o sistemas de información que establece que los líderes de proceso

son los responsables de la creación, eliminación o modificación de perfiles de acceso.

7.3. Evaluación de Riesgos

Se recomienda establecer controles de seguridad de la información que permitan disminuir el impacto sobre los riesgos que podrían afectar la confidencialidad, disponibilidad e integridad de la información, principalmente en los riesgos puros cuya calificación es alta y extrema.

Lo anterior dará cumplimiento a los lineamientos establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas de la Función Pública Numeral 5.4 Controles Asociados a la Seguridad de la Información.

7.4. Política General de Seguridad de la Información

Se recomienda incluir los siguientes elementos en la política general de seguridad de la información con el fin de dar cumplimiento a lo establecido en la norma ISO 27001:2013 Numeral 4.1.2 que establece:

- Compromiso de la Alta Dirección para asegurar los activos de información.
- La entidad requiere recurso humano, económico y tecnológico para que pueda gestionar los riesgos de seguridad de la información a los que está expuesta la entidad.
- El compromiso del cumplimiento legal y de buenas prácticas.
- Esta política debe estar aprobada y oficializada en el SIG.

7.5. Gestión de Incidentes de Seguridad de la Información

Se recomienda elaborar un manual o guía de gestión de incidentes de seguridad de la información que contenga las categorías y subcategorías de incidentes que determine la entidad, así como las actividades que se deben realizar en cada una de las fases sugeridas para la gestión de incidentes de seguridad (preparación, detección, contención, erradicación, recuperación, seguimiento). Este documento ayudará a minimizar los impactos adversos de los incidentes en CISA y sus operaciones mediante las salvaguardas adecuadas como parte de la respuesta a los incidentes que se puedan presentar.

7.6. Roles y Responsabilidades

Se recomienda a la Alta Dirección tomar la opción de ampliar la planta de personal del área de Seguridad de la Información dado que se evidencian falencias en la operación y seguimiento del Modelo de Seguridad y Privacidad dado que no se cuenta con el personal suficiente para atender los requerimientos, seguimiento y cumplimiento del gobierno de seguridad. Lo anterior fortalecerá la implementación y monitoreo del Modelo de Seguridad y Privacidad de la Información establecido en CISA.

Entre las estrategias que pueden contribuir a las funciones del área de Seguridad de la Información respecto al monitoreo en línea de la infraestructura tecnología con herramientas especializadas, identificación y atención de incidentes de seguridad y ciberseguridad es el apoyo de un Centro de Operaciones de Seguridad (SOC), para lo cual sugerimos analizar la viabilidad de la contratación de este tipo de servicio.

7.7. Procedimientos de seguridad de la información

Se recomienda elaborar, formalizar y hacer seguimiento a los procedimientos que soporten el cumplimiento de las siguientes políticas de seguridad de la información: criptografía, seguridad de las comunicaciones y relaciones con proveedores tal como lo establece la Guía No 3 Numeral 6 Procedimientos de Seguridad de la Información establecidos por el Modelo de Seguridad y Privacidad de la Información de MINTIC.

8. CONCLUSIONES

En el resultado general de la evaluación al componente de Seguridad de la Información se evidenció lo siguiente:

El área de Seguridad de la Información, de Central de Inversiones S.A., refleja en la información aportada, el adecuado desarrollo y trabajo realizado evidenciado en varios elementos como son la política general de seguridad de la información, políticas específicas de seguridad informática, gestión de activos de información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, plan operacional del Modelo de Seguridad y Privacidad de la Información e indicadores de gestión de seguridad de la información.

Así mismo, se identificaron diferentes herramientas tecnológicas que le han permitido al área de seguridad de la información cumplir con los objetivos de asegurar y mantener la confidencialidad, integridad y disponibilidad de la información. Aun así, se identificaron oportunidades de mejora relacionada con la elaboración, formalización, actualización de la documentación de algunos procedimientos y lineamientos de seguridad de la información, revisión de la efectividad de controles de seguridad de la información, fortalecimiento de las etapas de la gestión de incidentes de seguridad de la información, planes de mitigación de vulnerabilidades técnicas, implementación de controles para mitigar el impacto de los riesgos con calificación extrema y alta e identificación de infraestructuras críticas y gestión de riesgos de ciberseguridad de acuerdo con lo establecido en el CONPES 3701 Lineamientos de Ciberseguridad en el Estado Colombiano.

9. MESA DE TRABAJO

En atención al “Procedimiento para Auditorías Internas de Gestión”, una vez remitido el informe preliminar por el Auditor Interno, se realizó mesa de trabajo el día 5 de mayo de 2021, entre el Director de T.I, Equipo Auditor Bellicorp SAS y el Equipo de Auditoría Interna, con el fin de consolidar el informe definitivo, los ajustes y observaciones allí presentados quedan soportados en el acta de mesa de trabajo que hace parte de los papeles de trabajo de la auditoría interna y estarán disponibles para su consulta en caso de ser requeridos.

Aprobado por:	Elaborado por:	Fecha aprobación
Elkin Orlando Ángel Muñoz Auditor Interno	**Bellicorp SAS** **Auditor Externo** **Equipo Auditor**	(10/05/2021)