INFORME	PERIODO EVALUADO	FECHA
INFORME DE SEGURIDAD DE LA INFORMACIÓN	AÑO 2021	28/09/2021

NORMATIVIDAD APLICABLE

- Ley 1273 de 2009. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
- Ley 1341 de 2009. " Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC y se dictan otras disposiciones"
- Ley 1437 de 2011. “Procedimiento Administrativo y aplicación de criterios de seguridad”
- Ley 1581 de 2012. “Por la cual se dictan disposiciones generales para la Protección de Datos Personales”
- Decreto 2364 de 2012. “Firma electrónica”.
- Decreto 2609 de 2012. “Expediente electrónico”.
- Decreto 2693 de 2012. “Gobierno electrónico”.
- Decreto 1510 de 2013. “Contratación pública electrónica”.
- Decreto 1008 del 2018 "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital".
- Decreto 338 de 2018.” Por el cual se expide el Decreto Único del “Sistema Integral de Gestión y Control (SIGC) del Nivel Central de la Administración Departamental”, y se dictan otras disposiciones”.
- Política Pública: CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa, CONPES 3854 de 2016 Política Nacional de Seguridad digital.
- ISO 27001:2013

ANÁLISIS Y RESULTADOS DE LA EVALUACIÓN Y SEGUIMIENTO

La Oficina de Control Interno en cumplimiento de la ley 87 de 1993 y el Plan Anual de auditoría vigencia 2021, aprobado en Comité Institucional de Coordinación de Control Interno el 10 de mayo 2021 y su modificación el 14 de julio de 2021, la Oficina de Control Interno realizó la solicitud de la información objeto de Evaluación con mercurio número CI-2021338744 y reiteración con mercurio numero CI-2021340209, a la cual la Secretaría de las Tecnologías de la Información y las Comunicaciones da respuesta y envía evidencias el día 22 de septiembre de 2021 con el numero de mercurio CI-2021341195.

I. Verificación en el Marco de la Política de Gobierno Digital (Decreto 1078 de 2015, Decreto 1008 de 2018, Decreto 338 de 2018) y Controles de Seguridad de la Norma ISO 27001:2013

Teniendo en cuenta los lineamientos impartidos por el Ministerio de Tecnologías de la Información y las Comunicaciones mediante el Modelo de Seguridad y Privacidad de la información en el marco de la Política de Gobierno Digital establecida en el Decreto 1078 de

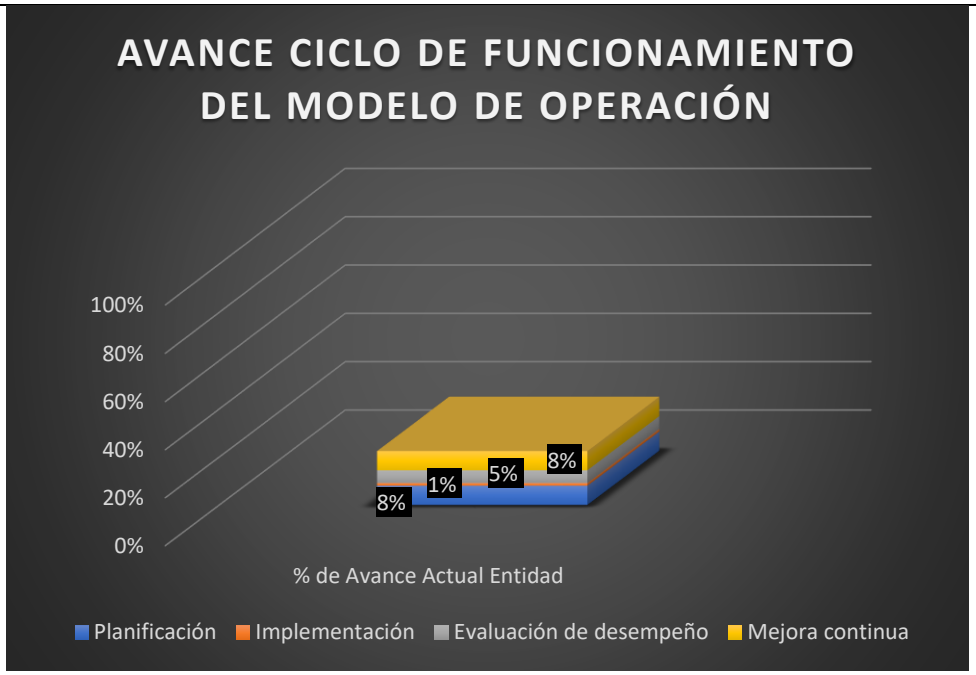
2015, Modificada por Decreto 1008 de 2018, en el cual se establecen los componentes, habilitadores transversales, responsables de su implementación y principios de la estrategia de Gobierno Digital, el Decreto 338 del 25 de octubre 2018 y los Controles de Seguridad de la Norma ISO 27001:2013, los cuales garantizan la confidencialidad, integridad y disponibilidad en la entidad.

Para revisar el nivel de madurez modelo seguridad y privacidad de la información se utilizó la herramienta autodiagnóstico[1] denominada "*instrumento de identificación de la línea base de seguridad*" emitido por MINTIC, el cual tiene como base los controles de las 14 secciones de norma ISO 27001:2013, evidenciando los siguientes resultados a nivel de dominio:

No.	Evaluación de Efectividad de controles	
	DOMINIO	**Calificación Actual**
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	10
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	24
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	67
A.8	GESTIÓN DE ACTIVOS	33
A.9	CONTROL DE ACCESO	39
A.10	CRIPTOGRAFÍA	20
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	10
A.12	SEGURIDAD DE LAS OPERACIONES	29
A.13	SEGURIDAD DE LAS COMUNICACIONES	33
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0
A.15	RELACIONES CON LOS PROVEEDORES	0
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	20
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20
A.18	CUMPLIMIENTO	10
PROMEDIO EVALUACIÓN DE CONTROLES		**23**

En cuanto al avance ciclo de funcionamiento del modelo de operación (PHVA) se observa un 22%.

1 INF_SGSI_YAHA_002_Instrumento_Evaluacion_MSPI



Con relación al nivel de implementación la Secretaría Tecnologías de la Información y las Comunicaciones en el oficio CI-2021341195[2] indica que actualmente se encuentran en el proceso de actualización del Modelo de Seguridad y Privacidad de la Información por lo que el nivel de madurez es bajo, ya que no alcanza nivel inicial.

II. Verificación de Cumplimiento Guía para la Gestión de Riesgos de Activos de Información "A-GT-GUI-017":

Adicionalmente se realizó la verificación del cumplimiento de la Guía para la Gestión de Riesgos de Activos de Información "A-GT-GUI-017", establecida por el proceso de Gestión Tecnológica y la Política Administración de Riesgos de la Gobernación de Cundinamarca, evidenciando lo siguiente:

La guía para la gestión de riesgos de activos de información se encuentra desactualizada, ya que las directrices que se toman como referencia son de versiones anteriores a las que están vigentes. La Secretaría indica que se encuentra en actualización teniendo en cuenta la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP versión 5 (Vigente), y el ANEXO 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas.

Dentro de los roles y responsabilidades establecidos en la guia A-GT-GUI-017 se evidencia que:

A. Documentos en construcción y en actualización: según oficio CI-2021341195:

- Política para gestión de riesgos de Seguridad de la Información

2 INF_SGSI_YAHA_001_RESPUESTA_SEC_TIC

- Reportes del monitoreo de riesgos, planes de tratamiento a través de las autoevaluaciones del proceso y seguimientos al plan de riesgos
- Planes de acción para mitigar y/o eliminar riesgos: Con relación a los planes de mitigación la Secretaría indica que actualmente se encuentran en la etapa de Análisis de Riesgo y en la creación del Proceso de Seguridad de la Información junto con la DDO.
- Política de cambio de contraseñas de los sistemas de información: Se observan las recomendaciones para el cambio de contraseñas en el oficio CI-2021341195, pero no se evidencia la Política de Cambio de Contraseñas en Isolución ni información relacionada a pesar de que a nivel de directorio activo tienen reglas hacia los usuarios.

B. Documentos en Isolución:

- Metodología para gestión de riesgos de Seguridad de la Información: se evidencia que existe el procedimiento de "*gestión de activos de información TIC*", el cual tiene como objetivo clasificar y gestionar los activos de información de TIC, lo que genera un inventario y clasificación de activos como resultado, como tal no es una metodología para la gestión de riesgos.

- Roles y responsabilidades: se evidencia que esta Compuesto por los líderes de los Procesos Estratégicos, Misionales, Apoyo y Evaluación, apoyados por el Secretario de las TIC, el Director de Gobierno digital, el Director de Sistemas de Información y Aplicaciones, el Director de Infraestructura Tecnológica y el Director de Desarrollo Organizacional , así como los líderes de aquellos procesos que se encuentren en el alcance del S.G.S.I y que cuenten con activos dentro del Data center de la Gobernación.

- Matriz inventario y clasificación de activos de información: Se evidencia el formato establecido con Código: A-GT-FR-062, en el cual se realiza la identificación, valoración, clasificación y etiquetado de la información a través de la identificación del activo de información, ubicación del activo de información, responsables asociados al activo de información, valoración del activo de información y la clasificación y etiquetado de activos

- Matriz valoración de riesgos de activos de información: Se evidencia el formato establecido con Código: A-GT-FR-063, en el cual establecen las fases de identificación del riego, análisis del riesgo, evaluación del riesgo y el plan de tratamiento

- Reportes de los eventos generadores de riesgos de Seguridad de la Información: en el oficio CI-2021341195 mencionan que existen 8 clases de incidentes con sus características y tratamientos, pero no se evidenciaron los reportes de la vigencia 2021.

- Soportes de la divulgación de las matrices consolidadas de riesgos a los propietarios: La Secretaría indica que se está realizando la actualización de la información de los activos y sus Propietarios, Dueños del Riesgo, Administrador Técnico del Activo, Administrador funcional y sus respectivos Backups, la concertación del Proceso de Seguridad de la información con la Dirección de Desarrollo Organizacional, adicionalmente se observa el formato con Código: A-GT-FR-071 "*acta plan de tratamiento riesgos activos de información TIC*".

- Actas de Comité de Seguridad de la Información del año 2021: Se evidencia que para la vigencia 2021 se ha realizado un comité.

- Política de respaldos: Se observa el procedimiento de respaldo de información de servidores TIC, con el objetivo de garantizar la disponibilidad inmediata, segura y confiable de los datos almacenados en los servidores corporativos existentes en el Data Center, mediante un proceso de Backup y generación de copias de respaldo que garanticen la integridad y disponibilidad de los datos en cualquier momento.

De lo anterior se puede concluir que, a pesar de tener procedimientos, formatos, guias y manuales establecidos, la entidad denota debilidades en la gestión de riesgos de seguridad de la información.

III. Verificación en relación con el Modelo Integrado de Planeación MIPG y MECI:

En relación con el Modelo Integrado de Planeación y Gestión – MIPG, el presente informe se relaciona con la 1ª. Dimensión "*Talento Humano***"** y la 2ª. Dimensión "*Direccionamiento Estratégico y Planeación***",** ya que la gestión es basada en procesos soportada en identificación de riesgos y definición de controles que asegure el cumplimiento de gestión institucional.

Frente a los componentes del Sistema de Control Interno, y sus criterios diferenciales se relaciona lo siguiente:

Línea de defensa	Componente asociado	Criterio diferencial o atributo de calidad	Resultado
Primera Segunda	Actividades de Control	Monitoreo a los riesgos acorde con la política de administración de riesgo establecida para la entidad.	No Cumple
Primera Segunda	Actividades de Control	El diseño de otros sistemas de gestión (bajo normas o estándares internacionales como la ISO), se integran de forma adecuada a la estructura de control de la entidad	Cumple Parcialmente

En cuanto a los criterios diferenciales del Sistema de Control Interno, se evidencia la baja respuesta desde la primera y segunda línea de defensa para el desarrollo y mantenimiento de controles de TI de tal forma que se mitiguen los riesgos, suceso que también se soporta en el resultado de la evaluación de la ejecución de los controles y su ejecución.

HALLAZGOS

Los hallazgos para el presente informe se anexan en el Formato EV-SEG-FR-056 - TABLA DE NO CUMPLIMIENTOS Y OBSERVACIONES.

CONCLUSIONES

El nivel de madurez del Modelo de Seguridad y Privacidad de la Información es bajo, teniendo en cuenta que el sistema de gestión de la información se creo hace varios años.

Es importante que se adelante la oficialización, aprobación y publicación de la información, que se genera y actualiza ya que un gran porcentaje de las evidencias aun están en borrador.

Elaborar una estrategia de implementación del SGSI articulado al MSPI a corto, mediano y largo plazo.

Es transcendental crear estrategias para la revisión de esta documentación y poder agilizar el trámite ante el sistema de calidad de la entidad acorde a la implementación ISO 27001:2013.

Realizar una revisión completa de los riesgos de seguridad de la información a fin de obtener unidad de criterio en la definición de controles y planes de tratamiento y facilitar el análisis y gestión frente a la posible materialización de los mismos.

Es importante que las capacitaciones o socializaciones con los funcionarios y contratistas sea también del SGSI (Procedimientos, Políticas, Formatos, etc.) ya que no todos han sido socializados y es importante que todos conozcámonos sobre el sistema.

Fortalecer las actividades tendientes a la adecuada gestión de riesgos a nivel de seguridad de la información y establecer controles efectivos.

Consolidar el plan de tratamiento de riesgos y el de vulnerabilidades, ya que se evidencia debilidad en evaluación y análisis de estos planes.

Se sugiere que por parte de la segunda línea de defensa se tenga mas participación en el proceso.

Elaboró

Nombre: Yuly Andrea Huertas Alonso
Cargo: Contratista

Aprobó

Nombre: Yoana Marcela Aguirre Torres
Cargo: Jefe de Oficina de Control Interno

Revisó

Nombre: Ludy Rocio Vargas Vargas
Cargo: Contratista