Fecha: 17 de marzo de 2025	**Ciudad:** Bucaramanga
Equipo auditor: SANDRA MILENA MENDOZA AMADO; Contratista Profesional OCIG	Proceso: Todos Procedimiento: Programa:
Clase de Informe: Seguimiento: X Evaluación:	**Tema:** Seguimiento Mapa de Riesgos de Seguridad de la Información vigencia 2024

1. OBJETIVO GENERAL

Evaluar la correcta identificación, análisis, efectividad de los controles y cumplimiento de las acciones de mitigación en la gestión de Riesgos de seguridad de la información de la Administración Central, con el fin de fortalecer las buenas prácticas de seguridad de la información como son: confidencialidad, integridad y disponibilidad y autenticidad de la información.

2. OBJETIVOS ESPECIFICOS

- Verificar la aplicación de los lineamientos del MIPG, componente administración del riesgo y, Guía para la administración del riesgo y el diseño de controles en entidades públicas, generada por el DAFP, capítulo Lineamientos riesgos de seguridad de la información
- Establecer el nivel de cumplimiento de las acciones propuestas en los mapas de riesgo de seguridad de la información de la Administración Central.
- Identificar las acciones de mejora necesarias para dar cumplimiento a todas las acciones propuestas y a los estándares exigidos.

3. ALCANCE

Verificar el cumplimiento de las acciones establecidas por la Administración Central para la definición y tratamiento de los riesgos de seguridad de la información con corte a 31 de diciembre de 2024.

4. MARCO NORMATIVO

- Constitución Política de Colombia de 1991: Art. 209, Art. 269.
- Ley 87 de 1993: Por la cual se establecen normas para el ejercicio del Control Interno en las entidades y organismos del Estado y se dictan otras disposiciones.
- Ley 1712 de 2014: La cual tiene por objeto regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.
- Decreto 103 de 2015: Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones, Titulo VI seguimiento a la gestión de la información.
- Decreto 648 de 2017: Art. 17 “Roles Oficinas de Control Interno o quien haga sus veces” artículo 2.2.21.5.3 del Decreto 1083 de 2015, el cual quedará así: “De las Oficinas de Control Interno. Las Unidades u Oficinas de Control Interno o quien haga sus veces desarrollarán su labor a través de los siguientes roles: liderazgo estratégico; enfoque hacia la prevención, evaluación de la gestión del riesgo, evaluación y seguimiento, relación con entes externos de control”
- Decreto 1499 de 2017: Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión
- Manual Operativo Modelo Integrado de Planeación y Gestión-MIPG

- Guía para la administración del riesgo y el diseño de controles en las entidades públicas, de la Función Pública.

5. DESARROLLO

Dando cumplimiento a las funciones propias de la Oficina de Control Interno y al Plan de acción y auditorías se efectúo seguimiento al mapa de riesgos de seguridad de la información, y la incorporación de las recomendaciones dadas en el seguimiento realizado en el 2024.

En este sentido, la Oficina de Control Interno ejerce su rol de seguimiento permanente a las actividades implementadas por los diferentes responsables de la entidad, encaminadas al fortalecimiento, desarrollo e implementación de una Política de Administración del Riesgo, colaborando así en la consolidación de un entorno organizacional orientado hacia la prevención.

Este seguimiento se realiza con corte a 30 de junio de 2024 y muestra el avance de la Alcaldía de Bucaramanga en tema de la gestión de riesgos de seguridad de la información y la implementación de las recomendaciones dadas en el último seguimiento.

RESULTADOS DEL SEGUIMIENTO

La Oficina de Control Interno de Gestión realizó seguimiento al cumplimiento de las acciones planteadas en el mapa de Riesgo de Seguridad de la Información correspondiente a la vigencia 2024, con corte a 31 de diciembre de 2024, con los siguientes resultados:

ACTIVO DE INFORMACIÓN	CANT RIESGOS	CANT ACCIONES	0% - 50%	51% - 99%	100%	Avance
Sistemas de Información y Aplicativos Software y Bases de Datos	1	1	0	0	1	100%
Sistemas de Información y Aplicativos Software	2	3	1	0	2	83,3%
Sistemas de información, equipos de infraestructura y bases de datos	1	1	1	0	0	33%
Servidores, sistemas de almacenamiento, bases de datos, sistemas de información	1	1	1	0	0	0%
Equipo de seguridad perimetral (Firewall) Consola de antivirus Software de monitoreo de red PRTG Consola de office 365	1	1	1	0	0	50%
Sistemas de información Plataformas de administración	1	1	1	0	0	25%
TOTAL	**7**	**8**	**5**	**0**	**3**	**49%**

En el cuadro anterior se reflejan 8 acciones preventivas proyectadas en el Mapa de Riesgos de Seguridad de la Información las cuales presentan cumplimiento del 49% a corte de 31 de diciembre de 2024.

6. RECOMENDACIONES

- Se reitera realizar el análisis de contexto interno y externo de acuerdo con lo establecido en el “ANEXO 4 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS” y dejar evidencia documental del mismo. Lo anterior permitirá asegurar el alcance de los activos de seguridad digital y establecer el tratamiento de estos.
- Se reitera el fortalecimiento de los controles tanto en su diseño como en su aplicación, alineándolos con los lineamientos establecidos en la Guía de Administración del Riesgo del Departamento Administrativo de la Función Pública (DAFP). Asimismo, sugerimos considerar la implementación de medidas adicionales, entre las cuales se incluye:
    - Involucrar activamente a los propietarios de cada activo de información en la formulación y aplicación de controles específicos, fortaleciendo así la participación directa de los responsables de cada recurso.
    - Incorporar controles que proporcionen alertas ante posibles amenazas o comportamientos atípicos en el acceso a la información, mejorando la capacidad de detección temprana de potenciales riesgos.
    - Establecer revisiones internas periódicas para evaluar la eficacia de los controles implementados, asegurando un monitoreo constante y la adaptación proactiva a las dinámicas cambiantes de riesgos y amenazas.

- Identificar los activos de software que requieren autenticación digital en el inventario de activos de información. Si solo el titular de la información puede realizar los trámites y/o servicios digitales, se debe establecer un control de autenticación digital. Para determinar el nivel adecuado de control, se debe realizar un análisis de pérdida de confidencialidad, integridad y disponibilidad, considerando la vulnerabilidad de la ausencia de mecanismos de identificación y autenticación, y la amenaza de falsificación de derechos sobre estos activos de software. Posteriormente, analizar la probabilidad e impacto de la materialización de estos riesgos y establecer el grado de confianza de autenticación digital adecuado. Una vez identificado el nivel de confianza adecuado, se deben seguir los lineamientos de la guía para la vinculación y uso de los servicios ciudadanos digitales.
- Priorizar la corrección de las vulnerabilidades identificadas en los sitios web durante las pruebas de seguridad.
- Proporcionar capacitación continua al equipo de desarrollo de software sobre buenas prácticas de seguridad de la información y actualizaciones de OWASP Projects.
- Socializar los avances en la implementación de las medidas correctivas y los resultados de las pruebas de seguridad a todas las partes interesadas
- Formalizar el Procedimiento de Gestión de Incidentes de Seguridad Digital y la Guía para la Gestión de Eventos y/o Incidentes de Seguridad para asegurar una respuesta efectiva ante eventos de seguridad digital. Estos documentos deben definir claramente los pasos a seguir en caso de incidentes, desde la identificación hasta la recuperación, para garantizar una gestión adecuada de los mismos.
- Gestionar y elaborar un informe periódico para analizar los incidentes de seguridad de la información, incluyendo un plan de acción para mitigar las vulnerabilidades identificadas. Este informe debe detallar la ejecución y seguimiento del plan, así como las lecciones aprendidas para mejorar la respuesta futura a incidentes.
- Establecer un mecanismo para el seguimiento y evaluación continuos de la eficacia de los procedimientos de gestión de incidentes. Esto permitirá realizar ajustes y mejoras según sea necesario para mantener la seguridad de la información de la organización.
- Implementar seguimiento de las actividades de mantenimiento, documentando los resultados y verificando que todos los sistemas críticos hayan sido cubiertos. Esto debe incluir la generación de informes post-mantenimiento que permitan evaluar la efectividad de los procesos realizados y garantizar la continuidad de los servicios.
- Actualizar el Plan de Recuperación de desastres vigente en la nube que incluya los escenarios de prueba, los sistemas críticos considerados, los procedimientos de

restauración y los indicadores de éxito.

- Ejecutar una prueba simulada de fallo total del centro de datos para validar la efectividad del DRP en un escenario de desastre real.
- Documentar los tiempos de restauración y compararlos con los objetivos establecidos en el plan.
- Incluir un análisis formal de debilidades detectadas y estrategias de optimización.
- Atender las recomendaciones tanto del MIN TIC como de la OCIG para avanzar en la implementación de un Centro de Analítica a fin de garantizar que la información esté siempre actualizada y que los usuarios puedan confiar en el portal para obtener datos recientes.

Las recomendaciones anteriormente mencionadas se realizan desde el rol de liderazgo estratégico con enfoque hacia la prevención y evaluación de la gestión del riesgo y no tiene otro fin que el de sugerir a la Administración Municipal, buenas prácticas y acciones de mejora que pueden ayudar a evidenciar de manera efectiva el cumplimiento de las metas de acuerdo con lo establecido en los indicadores, contribuyendo de esta manera a un proceso de mejora continua institucional.

7. FIRMAS

Firma	Firma
Nombre: **CLAUDIA ORELLANA HERNÁNDEZ**	Nombre: **SANDRA MILENA MENDOZA AMADO**
Cargo: Jefe Oficina Control Interno de Gestión	Cargo: CPS Profesional