Fecha: 30 de marzo de 2023	**Ciudad:** Bucaramanga
Equipo auditor: CLAUDIA ORELLANA HERNÁNDEZ; Jefe Oficina Control Interno de 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 2023

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- Versión 5 de diciembre 2020, generada por el DAFP, capítulo 5 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.
- Evaluar si los controles definidos en la matriz de riesgos de seguridad de la información son eficaces y eficientes.

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 28 de febrero de 2023.

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 establecido en el artículo 133 de la

- Manual Operativo Modelo Integrado de Planeación y Gestión-MIPG, Versión 4, marzo 2021, del Consejo para la Gestión y Desempeño Institucional.
- Guía para la administración del riesgo y el diseño de controles en las entidades públicas, de la Función Pública, versión 5 diciembre 2020.

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, analizando las causas, revisando los riesgos y la efectividad de los controles incorporados en la matriz de la presente vigencia.

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 en el periodo comprendido entre el 1 de enero al 28 de febrero de 2023 y muestra el avance de la Alcaldía de Bucaramanga en tema de la gestión de riesgos de seguridad de la información.

RESULTADOS DEL SEGUIMIENTO

La Oficina de Control Interno de Gestión durante el mes de marzo, realizó seguimiento al cumplimiento de las acciones planteadas en el mapa de Riesgo de Seguridad de la Información correspondiente a la vigencia 2023, con corte a 28 de febrero de 2023, con los siguientes resultados:

ACTIVO DE INFORMACIÓN	CANT RIESGOS	CANT ACCIONES	0% - 50%	51% - 99%	100%	Avance
Sistemas de Información y Aplicativos Software	1	3	3	0	0	0%
Dispositivos de Sistemas de Información - Hardware	3	3	3	0	0	25%
TOTAL	**4**	**6**	**6**	**0**	**0**	**12,5%**

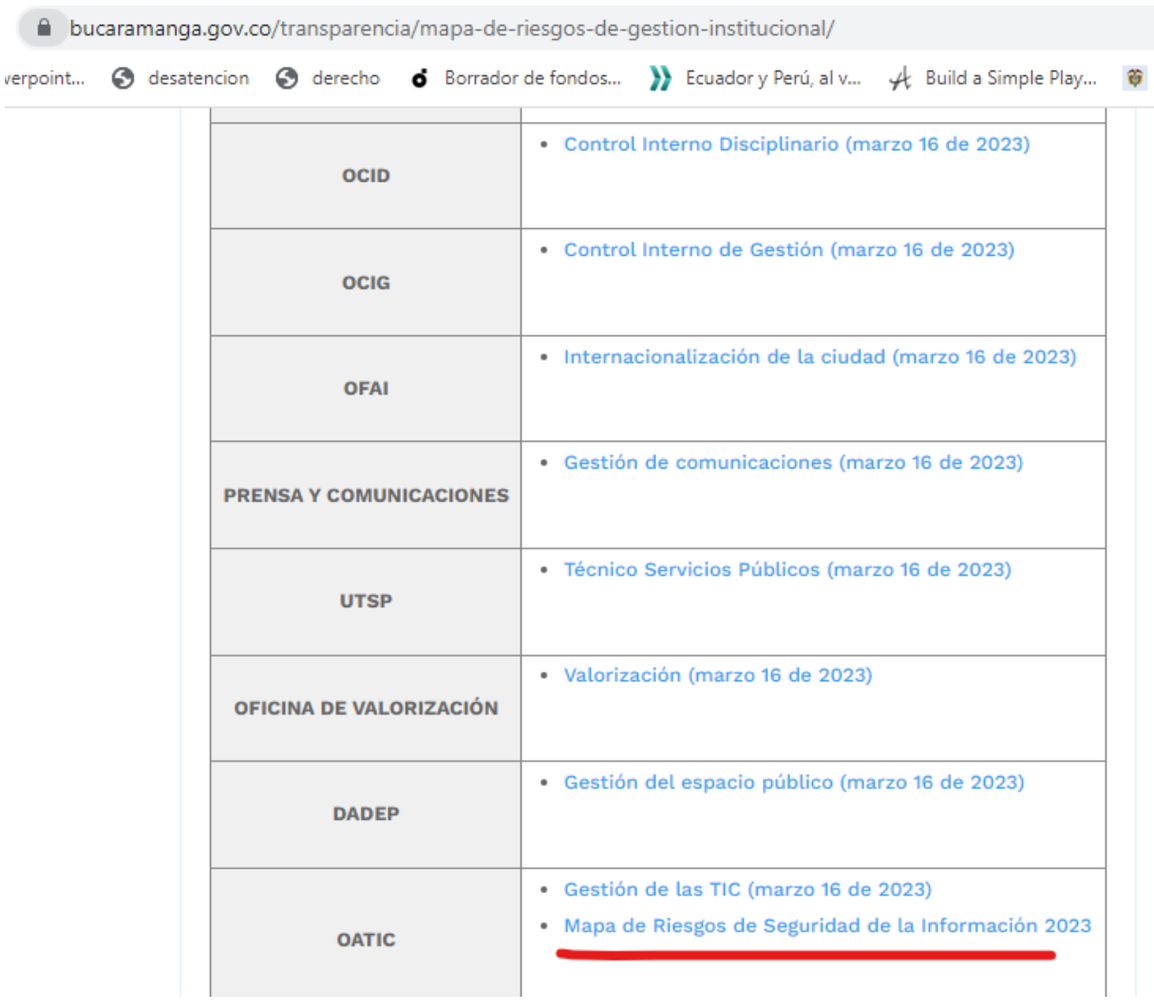
En el cuadro anterior se reflejan 6 acciones preventivas proyectadas en el Mapa de Riesgos de Seguridad de la Información, las cuales presentan cumplimiento del 12,5%.

La Oficina TIC elaboró la primera versión del mapa de riesgos de seguridad digital y fue presentada en los Comités de Gestión y Desempeño y Coordinación de Control Interno el 25 de noviembre y 21 de diciembre del 2023 respectivamente. Dicho mapa está en proceso de mejora continua en el que se puede incluir activos de seguridad digital como son la red de datos y servicios de base tecnológica.

Los controles establecidos a los activos incluidos presentan debilidades en su diseño, por cuanto no se puede determinar fácilmente quién es el responsable, la periodicidad y el objetivo del control. Para mejorar el diseño es necesario atender los lineamientos de la Guía de Administración del Riesgo del DAFP para una adecuada redacción del control se propone que en su estructura se identifique claramente el cargo del servidor o colaborador que ejecuta el control, en caso de que sean controles automáticos se debe identificar el sistema que realiza la actividad, se determine la acción que deben realizar como parte del control y se describan los detalles que permitan identificar claramente el objeto del control.

No se evidencia la elaboración del análisis de contexto interno y externo de acuerdo con los lineamientos para la gestión de riesgos de seguridad de la información que da el DAFP.

Se evidenció la publicación de la matriz de riesgos de seguridad de la información en la sección de Transparencia de la página web de la Administración Central, tal cómo se señala en la imagen:



6. RECOMENDACIONES

- 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 los mismos.

- Complementar el Mapa de Riesgos de Seguridad de la Información con los activos de seguridad digital críticos no incluidos, lo anterior teniendo en cuenta que el mapa no incluye activos tales como la red de datos, los servicios de base TIC y las redes sociales.

- Fortalecer los controles en cuanto a su diseño y aplicación de acuerdo con los lineamientos de la Guía de Administración del Riesgo del DAFP. Adicionalmente, considerar la implementación de otros controles adicionales, como monitoreo y registro de acceso a los sistemas y activos de información, encriptación de la información

sensible, entre otros, para reducir el riesgo de pérdida de confidencialidad.

- Realizar una evaluación más completa del riesgo “Pérdida de Integridad de los datos almacenados y gestionados en las bases de datos de los sistemas de información de la entidad utilizados en los diferentes procesos” y de las medidas de control propuestas para determinar si son adecuadas y efectivas para mitigar el riesgo. También se sugiere monitorear de manera regular la implementación de las medidas de control y su efectividad en la mitigación del riesgo.

- Realizar un seguimiento riguroso a la ejecución del mantenimiento preventivo anual, de los equipos Core de la infraestructura tecnológica de la entidad, y a la elaboración del informe de resultados. Es importante asegurarse de que el mantenimiento se realice de manera adecuada y que se documenten todos los hallazgos y acciones tomadas. Así mismo evaluar si la periodicidad del mantenimiento preventivo es suficiente para garantizar la disponibilidad de los sistemas de información y considerar la implementación de otros controles adicionales, como redundancia en los sistemas, respaldo de datos, planes de contingencia, entre otros, para reducir el riesgo de pérdida de disponibilidad.

- 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.

- Los planes de tratamiento de riesgos y los indicadores para medir la eficacia o la efectividad se deberán generar como lo indica el Esquema 9. Consolidación de los Planes de Tratamiento de Riesgos, de la “Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas” emitida por el DAFP.

- Evaluar periódicamente los riesgos residuales para determinar la efectividad de los planes de tratamiento y de los controles propuestos, según lo establecido en la Política de Administración de Riesgos de la Administración Central. También se deben tener en cuenta los incidentes de seguridad de la información y las métricas o indicadores definidos para hacer seguimiento a las medidas de seguridad implementadas. Esto permite la toma de decisiones en el proceso de revisión de riesgo por parte de la alta dirección y el comité de coordinación de control interno, así como de las demás partes interesadas.

- Contar con el registro de los incidentes de seguridad de la información que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar. El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.

- Adelantar la planificación y organización de la sensibilización en temas relacionados con la calidad de los datos y su importancia, de manera que se garantice su cumplimiento en

la fecha establecida y se cuente con tiempo suficiente para monitorear su efectividad y hacer ajustes si es necesario.

- Publicar en la sección de Transparencia de página web de la Administración Central el mapa de riesgos de seguridad de la información en un enlace diferente al de Mapa de Riesgos por Procesos, pero dentro de la sección de Planeación, para facilitar la búsqueda por parte de los ciudadanos.

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 a 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**
Cargo: Jefe Oficina Control Interno de Gestión	Cargo: CPS Profesional