Fecha: 14 de junio 2024	Ciudad: Bucaramanga
Líder Auditoría: Sandra Milena Mendoza Amado Profesional CPS	Proceso: Gestión de las TIC **Procedimiento(s):** • Procedimiento para implementar la administración de contenido de la estrategia de Gobierno en Línea. • Procedimiento para la Administración de contenidos del sitio Web Institucional de acuerdo con la implementación de la Estrategia de Gobierno en Línea. • Procedimiento para administración y soporte del centro de datos. • Procedimiento para atención a requerimientos sobre aplicaciones. • Procedimiento para Control y Monitoreo de la Central Telefónica y la Red Inalámbrica.
Equipo Auditor: María Angélica Morillo Galván - Profesional CPS	

Introducción:

La Oficina de Control Interno de Gestión, como líder estratégico de la Alcaldía de Bucaramanga, tiene como enfoque principal la prevención y evaluación de riesgos, siguiendo los lineamientos establecidos por el Decreto 648 de 2017. En este sentido, ha iniciado la Auditoría correspondiente al Modelo de Seguridad y Privacidad de la Información, en cumplimiento al Plan de Acción y Auditoría de la vigencia 2024 y al Procedimiento de Auditorías Internas P-CIG 1300-170-001.

El Proceso de Gestión de las TIC tiene por objetivo liderar la gestión de Tecnologías de la Información y Comunicaciones en la Administración Municipal. Esto se logra mediante la definición, implementación y mantenimiento de un modelo de arquitectura de TI que integra estrategias de gobierno electrónico y la normatividad vigente en el sector TIC, en beneficio de la gestión institucional y la ciudadanía.
En el ejercicio de la Auditoría Interna realizada, es importante destacar que una observación es el resultado de la comparación entre un criterio y la situación actual encontrada durante la auditoría del proceso. A continuación, se describirán los aspectos positivos y destacables del proceso auditado, así como las deficiencias, desviaciones, irregularidades o debilidades detectadas.

1. Objetivo General:

Evaluar la implementación del Modelo de Seguridad y Privacidad de la Información MSPI, de acuerdo con los lineamientos de la Estrategia de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones MinTic y la norma NTC ISO/ 27001:2013.

2. Objetivos Específicos:

- Verificar el avance en la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI
- Validar los controles establecidos por el proceso y presentar recomendaciones para implementar en la administración central del municipio de Bucaramanga de acuerdo a la evaluación del MSPI.
- Verificar el cumplimiento a las acciones formuladas en el plan de mejoramiento de los hallazgos de la vigencia 2023, respecto del MSPI.

3. Alcance:

En la auditoria se realizará la evaluación de la implementación del Modelo de Seguridad y Privacidad de la Información MSPI, de acuerdo a los lineamientos de la Estrategia de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones MinTic y la norma NTC ISO/ 27001:2013, vigencia 2023 y primer bimestre del 2024. No obstante, se podrán incorporar hechos adicionales que se evidencien en la auditoria y que estén por fuera del periodo definido en el alcance, hechos que quedarán habilitados para la evaluación que se adelante.

En los casos que sea necesario ampliar información, se tomaran muestras de soportes o transacciones de años anteriores o meses posteriores.

5. Resumen de Hallazgos

No.	Hallazgo	Responsable(s)
01	Bajo nivel de implementación del MSPI (Reiterativo)	OATIC
02	Debilidades en la gestión de incidentes de seguridad de la información (Reiterativo)	OATIC
03	Incumplimiento al Plan de Mejoramiento de Auditoría Interna vigencia 2023 (Reiterativo).	OATIC
04	Debilidades en la formulación del Plan de Seguridad y Privacidad de la Información y diligenciamiento de la matriz de diagnóstico del MSPI	OATIC
05	Ausencia de actualización y publicación del Mapa de Riesgos de Seguridad de la Información para la Vigencia 2024 en la página web institucional	OATIC
06	Inadecuado monitoreo del estado actual de la implementación de la seguridad y privacidad de la información	OATIC
07	Deficiencia en la medición de cumplimiento de los Objetivos de Seguridad de la Información (Reiterativo vigencia 2022)	OATIC
08	Deficiencia en la implementación de la estrategia de continuidad de negocio (Reiterativo)	OATIC

6. Recomendaciones

Actualizar el documento de autodiagnóstico propuesto por el Min TIC para incluir campos específicos de evidencia, brecha y recomendación para cada ítem evaluado, antes y después de la implementación del Plan Estratégico. Esta acción permitirá una identificación precisa del estado de cumplimiento de cada criterio, facilitando la identificación de áreas de mejora y proporcionando una guía clara para la implementación de medidas correctivas necesarias en el marco del MSPI.

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 reuniones de seguimiento periódicas para revisar el progreso de cada acción de mejoramiento, identificar y resolver de manera proactiva cualquier obstáculo, y tomar medidas correctivas inmediatas para asegurar el cumplimiento de los plazos y objetivos establecidos.

Establecer un proceso formal de revisión y corrección de documentos antes de su publicación para evitar errores y asegurar la integridad de la información.

Mantener la integridad intelectual de la información generada en la Alcaldía de Bucaramanga es esencial para garantizar la credibilidad, transparencia, legitimidad y cumplimiento normativo, así como para prevenir la desinformación y proteger la reputación y el liderazgo de la institución.

Establecer procesos de monitoreo para evaluar la efectividad de la gestión de riesgos y la implementación de los planes de acción, asegurando la objetividad y la mejora continua. Esto permitirá garantizar una adecuada mitigación de los riesgos y una respuesta oportuna en caso de que se materialicen. Además, se sugiere realizar una revisión periódica de los controles de seguridad implementados, documentar los resultados y establecer acciones de mejora a partir de los resultados, para asegurar su efectividad y eficacia. Esto ayudará a mantener un nivel adecuado de seguridad de la información y a identificar posibles áreas de mejora.

Elaborar fichas detalladas para cada indicador del MSPI, incluyendo frecuencia de evaluación, responsable, gráficos, y la información requerida en el formato F-MC-1000-238,37-045 TABLERO DE INDICADORES, para ser incluidos en el SIGC de la Alcaldía de Bucaramanga y evaluarlos regularmente. Esto permitirá un monitoreo continuo de la mitigación de riesgos, la identificación temprana de problemas, el cumplimiento de la normatividad vigente y promoverá la toma de decisiones informadas, fomentando así el mejoramiento continuo de la seguridad de la información.

Implementar el Plan de Recuperación Ante Desastres PL-TIC-1400-170-001 en el que se detallen los recursos mínimos requeridos en la estrategia de recuperación, esto garantizará que haya una guía clara para el proceso de recuperación y se disponga de los recursos necesarios en caso de un evento de desastre. Además, se sugiere que se incluyan indicadores que permitan estimar los tiempos de respuesta tanto en las pruebas como en los eventos reales. Estos indicadores serán útiles para evaluar la efectividad del plan de recuperación y permitirán medir y mejorar la capacidad de respuesta ante situaciones de crisis.

Implementar un proceso de registro de los mantenimientos realizados en los equipos, asegurando que se documenten las fechas, tareas, resultados y acciones de seguimiento. Además, realizar inspecciones regulares para garantizar el correcto funcionamiento de los equipos. Esto contribuirá a asegurar la disponibilidad e integridad continuas de los equipos y respaldará la gestión eficaz del mantenimiento.

Realizar la planificación de los mantenimientos al inicio del año, considerando la cantidad de equipos en la entidad, y ejecutarlos de acuerdo con el cronograma establecido a lo largo de la vigencia. Esto permitirá una gestión más eficiente y efectiva de los mantenimientos, asegurando la disponibilidad y el buen funcionamiento de los equipos de manera continua.

Implementar un enfoque sistemático y documentado para realizar pruebas de funcionalidad de la seguridad, así como establecer una periodicidad para las pruebas de detección de incidentes. Además, es fundamental documentar los resultados de estas pruebas y tomar las acciones correctivas necesarias en caso de identificar vulnerabilidades o debilidades en el entorno de desarrollo.

Articular con la Secretaría Administrativa (área de Talento Humano y Calidad) para revisar los Controles del Anexo A del estándar ISO/IEC 27001:2013 y dominios aplicables a esta área con el fin de garantizar el cumplimiento y mejorar continuamente los criterios implementados.

Gestionar la participación del equipo de la OATIC en otros grupos de interés profesionales como foros y asociaciones especializadas en seguridad, que permita el fortalecimiento de los controles en la seguridad de la información en la Alcaldía de Bucaramanga y adoptar mejores prácticas de otras experiencias.