**Fecha de Emisión del Informe:** 08-08-2023

| | |
|---|---|
| **Sistema auditado:** | Sistema de Gestión de Seguridad de la Información (NTC ISO/IEC 27001:2022) |
| **Proceso (s) auditado (s):** | Gestión de TICS, Inteligencia para la Movilidad, Gestión de Trámites y Servicios a la Ciudadanía, Gestión de Tránsito y Control de Tránsito y Transporte, Control Disciplinario, Gestión de Talento Humano, Direccionamiento Estratégico, Gestión Administrativa. |
| **Dependencia (s) auditada (s):** | Oficina de Tecnologías de la Información y las Comunicaciones, Dirección de Atención al Ciudadano, Dirección de Inteligencia para la Movilidad, Dirección de Talento Humano. |
| **Nombre y cargo del responsables del proceso / dependencia auditada:** | Leydy Yohana Pineda Afanador-Jefe de Oficina de Tecnologías de la Información y las Comunicaciones. |
| **Equipo auditor:** | Robert Veloza Gonzalez<br>Marisol Veloza Rios |
| **Fechas de Ejecución de la Auditoria:** | Fecha de Apertura: 27-07-2023 Fecha de Cierre: 10-08-2023 |

| | |
|---|---|
| **Objetivo de la auditoría** | • Verificar que el Sistema de gestión de seguridad de la información -SGSI- se ha implementado y se mantiene de manera eficaz, eficiente y efectiva para satisfacer los requisitos conforme a la NTC ISO/IEC 27001:2022.<br>• Determinar la conformidad del sistema de gestión con los requisitos del estándar de sistema de gestión.<br>• Evaluar la capacidad del sistema de gestión para asegurar el cumplimiento de los requisitos legales y reglamentarios aplicables al alcance del sistema de gestión y a la norma de requisitos de gestión.<br>• Determinar la eficacia de la implementación del sistema de gestión de seguridad de la información.<br>• Identificar oportunidades de mejora en el sistema de gestión. |
| **Alcance de la Auditoría:** | La auditoría se aplica a la seguridad sobre la información que sea creada, procesada, transmitida o resguardada dentro de su sede principal por las partes interesadas y que a su vez hagan parte de los procesos misionales de la Entidad, como lo son:<br>• Planeación de transporte e infraestructura<br>• Gestión social<br>• Gestión de trámites y servicios para la ciudadanía<br>• Gestión contravencional y transporte publico<br>• Gestión de tránsito y control de tránsito y transporte<br>• Ingeniería de tránsito.<br>Y aquellos procesos de apoyo cuyo objetivo contemple la implementación de controles de seguridad de la información de manera transversal para la Secretaría Distrital de Movilidad |

| | |
|---|---|
| **Criterios de la Auditoría:** | NTC ISO/IEC 27001:2022 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos<br>Procedimientos propios de la entidad y demás normatividad aplicable al alcance y/o sistema de gestión de seguridad de la información |
| **Declaración del Auditor o Equipo Auditor.** | En el desarrollo de la presente auditoría, el auditor o equipo de auditoría no fue sujeto de presiones indebidas, no presentó ningún tipo de impedimento que afectara su objetividad, actuó con el debido cuidado profesional y bajo los principios éticos y reglas de conducta del estatuto de auditoría. |

**RESUMEN EJECUTIVO**

| Tipo de Hallazgo | Cantidad |
|---|---|
| No conformidad | 3 |
| Oportunidad de mejora | 0 |
| Total | 3 |

## DESARROLLO DE LA AUDITORÍA

La auditoría de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001:2022 es un proceso fundamental para evaluar la eficacia de los controles de seguridad implementados. La combinación de entrevistas y muestreo estratégico permitió obtener una comprensión completa del sistema y garantiza una evaluación precisa de su cumplimiento con los requisitos normativos. A continuación, se presenta la metodología aplicada que integró entrevistas y muestreo para llevar a cabo la auditoría de manera efectiva:

- **Planificación de la Auditoría:** a. Definir los objetivos de la auditoría y el alcance del SGSI a ser evaluado. b. Identificar las áreas clave de enfoque, como la gestión de riesgos, la seguridad en las comunicaciones y la seguridad física. c. Seleccionar a los participantes clave para las entrevistas, incluidos los responsables de la implementación del SGSI.
- **Entrevistas:** a. Realizar entrevistas individuales con los representantes de la alta dirección, el equipo de seguridad de la información y otros empleados clave. b. Obtener información sobre la estructura del SGSI, las políticas, los procedimientos y los controles implementados. c. Discutir la comprensión de los roles y responsabilidades, la conciencia de los riesgos de seguridad y la capacitación del personal.
- **Muestreo Estratégico:** a. Identificar una muestra representativa de procesos, sistemas y activos de información para ser evaluados. b. Seleccionar documentos, registros y evidencias relevantes para la muestra, como políticas, registros de incidentes, resultados de evaluaciones de riesgos y planes de tratamiento de riesgos.
- **Evaluación y Análisis:** a. Examinar la documentación y la evidencia recopilada para verificar la implementación y la eficacia de los controles de seguridad. b. Comparar los hallazgos con los requisitos de la norma ISO 27001:2022 y evaluar cualquier brecha o incumplimiento identificado. c. Identificar áreas de mejora y oportunidades de fortalecimiento en la gestión de seguridad de la información.
- **Informe de Auditoría:** a. Elaborar un informe detallado que resuma los hallazgos, incluidas las fortalezas, debilidades y recomendaciones de mejora. b. Proporcionar una evaluación global de la conformidad del SGSI con la norma ISO 27001:2022 y destacar áreas de éxito y áreas que requieren atención.

## RESULTADOS

### No conformidad No. 001

En la sección de Roles, Responsabilidades y Autoridades de la entidad (5.3.a) no se ha designado una persona específica para el rol de Seguridad de la Información. Se espera que la entidad identifique y designe a un individuo claramente responsable del rol de Seguridad de la Información. Este rol debe incluir la supervisión y el control de las políticas y procedimientos de seguridad, así como la gestión de riesgos y la respuesta a incidentes de seguridad. La falta de designación de un Rol de Seguridad de la Información se debe a la falta de asignación de una persona para el rol, dicha ausencia puede resultar en un enfoque menos coordinado y coherente para la gestión de la seguridad de la información.

### No conformidad No. 002

Se ha identificado que en el proceso de Preparación de las TIC para la continuidad de negocio (5.30), no se han identificado ni ejecutado pruebas de continuidad de negocio de manera adecuada. En concordancia con las buenas prácticas de gestión de continuidad de negocio, se espera que la entidad identifique los sistemas críticos de TIC y realice pruebas periódicas de continuidad de negocio para asegurarse de que estos sistemas puedan recuperarse eficazmente en caso de interrupciones. La falta de identificación y ejecución de pruebas de continuidad de negocio puede atribuirse a una inmadurez en la ejecución del sistema de continuidad de negocio el cual se encuentra en formación, sin embargo por la omisión de pruebas de continuidad de negocio puede tener consecuencias significativas en caso de interrupciones reales. Si no se han probado los sistemas críticos de TIC, la entidad podría enfrentar dificultades para recuperarse rápidamente, lo que podría resultar en tiempo de inactividad prolongado, pérdida de datos y daños a la reputación.

### No conformidad No. 003

Se ha identificado que en el proceso de Prevención de Fugas de Datos (8.12) no se ha aplicado un control efectivo para mitigar la fuga de datos en la entidad. De acuerdo con las mejores prácticas de seguridad de la información, se espera que la entidad implemente controles técnicos y procedimientos para prevenir y mitigar la fuga de datos, garantizando la confidencialidad y la integridad de la información sensible. La falta de aplicación de un control adecuado puede deberse a diversas razones, entre ellos carencia de recursos asignados para la implementación del control o la no identificación completa de posibles puntos de fuga. La ausencia de un control efectivo para mitigar la fuga de datos puede tener consecuencias graves para la entidad, esto podría resultar en la divulgación no autorizada de información confidencial o sensible, lo que podría comprometer la privacidad de los clientes, dañar la reputación de la entidad y provocar sanciones legales.

## IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

Con gran satisfacción, se completó una revisión exhaustiva de las matrices de riesgos de seguridad de la información presentadas. Estas matrices demuestran un enfoque aplicado para identificar y evaluar los posibles riesgos que podrían afectar la integridad, confidencialidad y disponibilidad de los activos de información crítica. Se aprecia especialmente la inclusión de una amplia gama de amenazas potenciales, así como la asignación cuidadosa de niveles de impacto y probabilidad. Además, el uso de una escala de calificación claramente definida y criterios de evaluación coherentes mejora la claridad y objetividad en la valoración de riesgos. Se ha evidenciado un esfuerzo por considerar tanto las amenazas internas como externas, lo cual contribuye a una comprensión holística de la seguridad de la información en la organización. En resumen, esta matriz de riesgos refleja un enfoque riguroso y bien estructurado para la gestión de la seguridad de la información, sentando una sólida base para la toma de decisiones informadas en materia de mitigación y prevención de riesgos.

## FORTALEZAS

Durante la auditoría del Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001:2022, se han identificado varias fortalezas en las áreas de seguridad en las comunicaciones y seguridad física. Estas fortalezas demuestran un compromiso sólido y efectivo de la entidad para proteger sus activos de información y garantizar la confidencialidad, integridad y disponibilidad de los mismos:

1. Políticas y Procedimientos de Comunicaciones Seguras: La entidad ha establecido políticas y procedimientos claros para el uso seguro de las comunicaciones electrónicas. Estos documentos establecen directrices específicas para la transmisión segura de datos, el cifrado de información confidencial y la autenticación de usuarios, lo que refleja una sólida cultura de seguridad cibernética.
2. Seguridad de Redes y Firewalls: Se ha implementado una infraestructura de seguridad de red sólida, con la utilización de firewalls y tecnologías de detección de intrusiones. Estas medidas ayudan a proteger los sistemas y datos contra amenazas externas y aseguran que solo el tráfico autorizado pueda acceder a los recursos de la red.
3. Capacitación y Concientización de los Empleados: La entidad ha invertido en la formación y concientización de los empleados en materia de seguridad de la información y buenas prácticas de comunicaciones seguras. Esto contribuye a crear una fuerza laboral informada y consciente de los riesgos, reduciendo la posibilidad de errores humanos y amenazas internas.
4. Monitoreo y Detección de Incidentes: Se ha implementado un sistema de monitoreo y detección de incidentes en las comunicaciones y redes. Esto permite una respuesta temprana ante posibles amenazas y asegura una acción rápida y eficiente en caso de actividades sospechosas.
5. Control de Acceso Físico: La entidad ha establecido un sólido control de acceso físico a sus instalaciones, restringiendo la entrada solo a personal autorizado. Esto ayuda a prevenir el acceso no autorizado a áreas sensibles y salvaguarda los activos físicos y de información.
6. Vigilancia y Seguridad Física: Se ha implementado un sistema de vigilancia y seguridad física en las instalaciones. La presencia de cámaras de seguridad, sistemas de alarma y controles de acceso contribuye a disuadir amenazas y proporciona una capa adicional de protección.

**7.** Respaldo y Recuperación de Datos: La entidad cuenta con procedimientos de respaldo y recuperación de datos sólidos para garantizar la disponibilidad y recuperación de la información en caso de eventos inesperados. Esto asegura la continuidad de operaciones y la integridad de la información.

## CONCLUSIONES

En el proceso de auditoría del Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO 27001:2022, se han identificado avances notables y áreas de fortaleza en la entidad que merecen reconocimiento. Es importante destacar la sólida gestión de redes y comunicaciones, así como el enfoque eficaz en la seguridad física, que evidencian un compromiso significativo con la protección integral de los activos de información.

Es recomendable ampliar y fortalecer los esfuerzos en el mejoramiento de madurez del plan de continuidad de negocio para abordar una variedad más amplia de escenarios de interrupción. Esta mejora contribuirá a una respuesta más eficiente y eficaz ante situaciones de crisis, minimizando el impacto en las operaciones.

Además, se sugiere la migración documental a la versión 2022 de la norma ISO 27001, lo que permitirá mantener la alineación con las últimas mejores prácticas y requisitos actualizados. Esta actualización asegurará que el sistema de gestión de seguridad de la información siga siendo relevante y robusto en el entorno en constante evolución de la ciberseguridad.

En general, la entidad ha demostrado un fuerte compromiso con la protección de la información y la seguridad. Las áreas de excelencia, como la gestión de redes y comunicaciones y la seguridad física, son testimonio de la dedicación y el trabajo arduo del equipo. Con la continua implementación de mejoras en la continuidad de negocio y la migración documental, la entidad estará en una posición aún más sólida para enfrentar los desafíos de seguridad de la información y mantener la confianza de sus partes interesadas.

Felicitamos a la entidad por sus logros hasta la fecha y esperamos ver su continuo progreso en el fortalecimiento de su Sistema de Gestión de Seguridad de la Información conforme a los estándares más altos de la norma ISO 27001:2022.

## RECOMENDACIONES

Basados en los resultados de la auditoría del Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO 27001:2022, se han identificado áreas clave que requieren atención y mejora. A continuación, se presentan recomendaciones específicas para fortalecer y optimizar el SGSI:

**1.** Madurez de la Continuidad de Negocio: Se recomienda aumentar la madurez del proceso de continuidad de negocio. Esto implica una evaluación exhaustiva de los riesgos y escenarios potenciales de interrupción, seguido de la implementación y prueba de planes de recuperación.

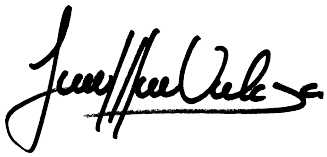
La planificación y simulación de diferentes situaciones de crisis permitirán una respuesta más efectiva y una reducción significativa de la posibilidad de tiempo de inactividad prolongado. Garantizar la disponibilidad continua de servicios críticos es esencial para mantener la confianza de los clientes y la resiliencia operativa.

**2.** Migración Documental a la Versión 2022: Es crucial considerar la migración documental a la versión más reciente de la norma ISO 27001 (2022). Esto asegurará que el sistema de gestión esté alineado con las últimas mejores prácticas y requisitos actualizados. La migración documental debe ser un proceso integral que incluya la revisión y actualización de políticas, procedimientos y otros documentos clave. Mantenerse actualizado con los cambios normativos garantizará que el SGSI siga siendo robusto y eficaz en la protección de la información sensible.

**3.** Mejora del Plan de Tratamiento de Riesgos: Se sugiere revisar y mejorar el plan de tratamiento de riesgos de seguridad de la información. Esto implica una evaluación más profunda y precisa de los riesgos identificados, seguida de la implementación de controles adecuados para mitigarlos.

**4.** Durante la auditoría, se ha observado que la aplicación disciplinaria por levantarse de la estación de trabajo sin bloquear la pantalla no se está llevando a cabo de manera consistente y efectiva en la entidad. En línea con las políticas de seguridad de la información y las mejores prácticas de privacidad, se espera que los empleados bloqueen la pantalla de su estación de trabajo al abandonarla para prevenir el acceso no autorizado a la información confidencial y los sistemas. La observación obedece dado que en la visita e inspección física realizada se evidenció la ausencia de un funcionario de la SDM de su estación de trabajo sin realizar el respectivo bloqueo. La falta de bloqueo de pantalla puede exponer información confidencial a miradas indiscretas, aumentando el riesgo de violaciones de privacidad y filtración de datos. Esto podría llevar a la pérdida de información sensible, violaciones de la confidencialidad y daño a la reputación de la entidad.

**ANEXOS: N/A**

| Nombre(s) y firma(s) auditor(es):<br>Marisol Veloza Rios | Nombre y Firma del Auditor líder<br>Robert Veloza Gonzalez |
|---|---|
|  |  |