PAPEL DE TRABAJO

Alcance de la Auditoría

La auditoría tendrá como alcance la evaluación de la **administración de la seguridad de los sistemas de información** de propiedad del Municipio, así como de las **plataformas tecnológicas utilizadas en modalidad de consulta y prestación de servicios**, cuya propiedad corresponda a entidades externas del orden **Municipal y Departamental**, y que sean empleadas por la administración municipal para el cumplimiento de sus funciones misionales.

En particular, la auditoría comprenderá:

- La verificación de la **existencia, implementación y aplicación de políticas, procedimientos y controles de seguridad de la información**, asociados al acceso, uso, administración y protección de los sistemas de información municipales y de las plataformas externas utilizadas.
- La evaluación de los **mecanismos de control de accesos**, perfiles de usuario, autenticación, autorización y trazabilidad, tanto en sistemas propios como en aquellos de terceros utilizados por el Municipio.
- La revisión de las **responsabilidades asignadas** para la administración de la seguridad de la información, incluyendo roles, segregación de funciones y supervisión.
- El análisis de los **acuerdos, convenios o instrumentos contractuales** que regulan el uso de plataformas externas, en lo relacionado con la seguridad de la información, confidencialidad, integridad, disponibilidad y protección de datos.
- La verificación del cumplimiento de la **normatividad vigente y lineamientos institucionales** aplicables en materia de seguridad de la información y gestión de tecnologías de la información.

Quedan excluidos del alcance los procesos de **desarrollo de software**, la **infraestructura tecnológica de terceros no administrada ni utilizada directamente por el Municipio**, y las evaluaciones técnicas profundas de vulnerabilidades, salvo aquellas que se evidencien a nivel de control administrativo y de gestión.

Alcance de la Auditoría – ISO/IEC 27001:2013

La auditoría tendrá como alcance la evaluación del **Sistema de Gestión de Seguridad de la Información (SGSI)**, en lo relacionado con la **administración de la seguridad de los sistemas de información** de propiedad del Municipio, así como de las **plataformas tecnológicas de entidades externas del orden Municipal y Departamental**, utilizadas por la administración municipal en modalidad de consulta y prestación de servicios.

La auditoría se desarrollará con base en los **requisitos establecidos en la Norma ISO/IEC 27001:2013**, verificando el grado de conformidad, implementación y eficacia de los controles aplicables, en especial los definidos en el **Anexo A**, respecto a:

- La definición y aplicación de **políticas de seguridad de la información** (A.5), relacionadas con el uso y administración de los sistemas de información municipales y de terceros.
- La **organización de la seguridad de la información** (A.6), incluyendo roles, responsabilidades y coordinación para la gestión de la seguridad en sistemas propios y plataformas externas.
- La gestión de **controles de acceso** (A.9), garantizando la adecuada autenticación, autorización, segregación de funciones y trazabilidad de los usuarios.
- La protección de los **activos de información** (A.8), considerando la clasificación, uso adecuado y responsabilidades sobre la información procesada o consultada en sistemas propios y de terceros.
- La gestión de **relaciones con proveedores y terceros** (A.15), evaluando los acuerdos, convenios o instrumentos contractuales que regulan el acceso, uso y protección de la información.
- La identificación y tratamiento de **riesgos de seguridad de la información** asociados al uso de sistemas propios y plataformas externas, conforme al enfoque de gestión del riesgo del SGSI (Cláusulas 6 y 8).
- El cumplimiento de **requisitos legales, normativos y contractuales** aplicables en materia de seguridad de la información (A.18).

La auditoría tendrá un enfoque **administrativo y de gestión**, orientado a la verificación de la conformidad del SGSI con la ISO/IEC 27001:2013, y no incluirá pruebas técnicas de penetración, análisis forense ni evaluaciones avanzadas de vulnerabilidades, salvo aquellas evidencias que se identifiquen a nivel de control y gestión.

MODELO DE PROCEDIMIENTO DE AUDITORÍA

ADMINISTRACIÓN Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Alcaldía de Pereira

---

1. OBJETIVO

Establecer el procedimiento para realizar auditorías a la administración y seguridad de los Sistemas de Información (SI) de propiedad del Municipio de Pereira y a las plataformas utilizadas en calidad de consulta y/o prestación de servicios, aun cuando sean propiedad de entidades externas del orden municipal o departamental, garantizando el cumplimiento normativo, la protección de la información y la adecuada gestión del riesgo.

---

2. ALCANCE

El presente procedimiento aplica a:

- Sistemas de información institucionales de la Alcaldía de Pereira.
- Infraestructura tecnológica asociada (servidores, redes, bases de datos, servicios en la nube).
- Plataformas externas utilizadas mediante convenios, contratos o interoperabilidad.
- Información pública, reservada, clasificada y datos personales administrados por la entidad.

---

3. MARCO NORMATIVO APLICABLE

- Constitución Política de Colombia.
- Ley 136 de 1994 y Ley 1551 de 2012 (Régimen Municipal).
- Ley 87 de 1993 (Control Interno).
- Ley 1581 de 2012 (Protección de Datos Personales).
- Ley 1712 de 2014 (Transparencia y Acceso a la Información Pública).
- Decreto 1078 de 2015 – Decreto Único del Sector TIC.
- Decreto 767 de 2022 – Política de Gobierno Digital.
- Resolución MinTIC 500 de 2021 – Modelo de Seguridad y Privacidad de la Información (MSPI).
- Modelo Integrado de Planeación y Gestión (MIPG).

- ISO/IEC 27001:2013 es la norma internacional que define cómo establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), basado en riesgos.

---

4. PRINCIPIOS DE LA AUDITORÍA

- Independencia y objetividad.

- Enfoque basado en riesgos.
- Confidencialidad de la información.
- Legalidad y debido proceso.
- Mejora continua.

---

5. ROLES Y RESPONSABILIDADES

5.1 Oficina de Control Interno

- Planear y ejecutar la auditoría.
- Elaborar informes de hallazgos y recomendaciones.
- Realizar seguimiento a los planes de mejoramiento.

5.2 Oficina TIC / Sistemas

- Facilitar el acceso a la información requerida.
- Atender requerimientos y observaciones de auditoría.
- Implementar acciones correctivas.

5.3 Dueños de Procesos

- Garantizar el uso adecuado de los sistemas.
- Cumplir las políticas de seguridad y protección de datos.

5.4 Proveedores o Entidades Externas

- Cumplir los acuerdos de seguridad de la información.
- Permitir auditorías conforme a lo pactado contractualmente.

---

6. METODOLOGÍA DE AUDITORÍA

6.1 Planeación

- Identificación de sistemas críticos.
- Análisis de riesgos de seguridad de la información.
- Definición del alcance, criterios y cronograma.
- Revisión de normativa, contratos y políticas internas.

6.2 Ejecución

- Evaluación del cumplimiento legal y normativo.

- Revisión de controles de seguridad (lógicos, físicos y administrativos).
- Verificación de gestión de accesos, respaldo, continuidad y trazabilidad.
- Revisión del tratamiento de datos personales.
- Evaluación de la interoperabilidad y uso de plataformas externas.

6.3 Análisis de Hallazgos

- Clasificación de hallazgos (crítico, alto, medio, bajo).
- Determinación de causas, efectos y riesgos.
- Identificación de responsables.

6.4 Informe de Auditoría

El informe deberá contener:

- Objetivo y alcance.
- Marco normativo aplicado.
- Hallazgos y evidencias.
- Conclusiones.
- Recomendaciones.

6.5 Plan de Mejoramiento y Seguimiento

- Definición de acciones correctivas.
- Asignación de responsables y plazos.
- Seguimiento periódico hasta el cierre de hallazgos.

---

7. CRITERIOS DE EVALUACIÓN

- Cumplimiento del MSPI.
- Gestión de riesgos de seguridad de la información.
- Confidencialidad, integridad y disponibilidad de la información.
- Cumplimiento de acuerdos de nivel de servicio (SLA).
- Protección de datos personales.

---

8. PRODUCTOS DE LA AUDITORÍA

- Programa de auditoría.
- Papeles de trabajo.
- Informe final de auditoría.
- Plan de mejoramiento.

- Reportes de seguimiento.

---

9. FRECUENCIA

Las auditorías de seguridad de la información deberán realizarse como mínimo una vez al año o cuando se presenten cambios significativos en los sistemas, incidentes de seguridad o requerimientos de los entes de control.

---

10. APROBACIÓN Y VIGENCIA

El presente procedimiento entra en vigencia a partir de su aprobación por la Alta Dirección de la Alcaldía de Pereira y deberá ser revisado y actualizado conforme a cambios normativos o tecnológicos.

Elaboró: Oficina de Control Interno
Entidad: Alcaldía de Pereira

ALIRIO SANCHEZ PEREZ

