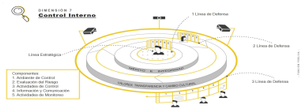
Nombre de la Entidad:	**DEPARTAMENTO ADMINISTRATIVO DE LA DEFENSORÍA DEL ESPACIO PÚBLICO - DADEP**
Periodo Evaluado:	**PRIMER SEMESTRE 2026**



Estado del sistema de Control Interno de la entidad	**89,94%**

Conclusión general sobre la evaluación del Sistema de Control Interno

¿Están todos los componentes operando juntos y de manera integrada? (Si / en proceso / No) (Justifique su respuesta):	En proceso	Los lineamientos verificados en la presente evaluación, permiten medir el grado de cumplimiento con relación a la estructura de control establecida en el Sistema de Control Interno del DADEP. Se evidencia el mantenimiento en la definición e implementación de los instrumentos mínimos para la ejecución del ciclo PHVA de la gestión pública, el modelo de operación por procesos, así como la existencia de los instrumentos mínimos para el ejercicio de la actividad de auditoría interna. De igual manera, se evidencia la operación del Comité de Coordinación de Control Interno de la Entidad, la Política de Administración del Riesgo, el Esquema de las Tres Líneas y el mapa de aseguramiento. No obstante es necesario fortalecer y continuar con la aplicación permanentemente de los principios de autocontrol, autorregulación y autogestión con el fin de mantener una gestion adecuada de los riesgos y el compromiso de la Alta Dirección para la toma de decisiones.
¿Es efectivo el sistema de control interno para los objetivos evaluados? (SI/No) (Justifique su respuesta):	Si	El estado de avance de la implementación del Sistema de Control Interno en el DADEP para el Primer semestre de 2026, a partir de cada uno de los cinco (5) componentes de su estructura definida en la séptima dimensión del MIPG, (Ambiente de Control, Evaluación del Riesgo, Actividades de Control, Información y Comunicación, y Actividades de Monitoreo), se observa que dicho sistema es efectivo en un 89,94%, cuyo resultado se resumen en: Ambiente de control, cuyo nivel de implementación es del 96%, correspondiente a los veinticuatro (24) lineamientos evaluados, de ellos veintidós (22) se califican en la categoría mantenimiento del control, dos (2) en deficiencia de control. Este componente frente al periodo anterior aumento en (2) puntos porcentuales. •Evaluación de riesgos, cuyo nivel de implementación es del 76%, correspondiente a diecisiete (17) lineamientos evaluados, de ellos, doce (12) se califican en la categoría mantenimiento del control y cinco (5) se encuentran con deficiencia de control. De esta manera, respecto al periodo anterior se disminuye dos (2) puntos porcentuales. •Actividades de control, con un nivel de cumplimiento del 92%, correspondiente a doce (12) lineamientos evaluados, de los cuales diez (10) se califican en la categoría mantenimiento del control, y dos (2) de ellos, se encuentran en deficiencia de control. De esta manera se observa un aumento de cuatro (4) puntos porcentuales frente al periodo anterior •Información y comunicación con un nivel de cumplimiento del 93%, respecto a catorce (14) lineamientos evaluados, de ellos, doce (12) se califican en la categoría mantenimiento del control y dos (2) en deficiencia de control. En este caso se mantiene sin variación del resultado frente al periodo anterior. •Actividades de Monitoreo con un nivel de cumplimiento del 93%, correspondiente a catorce (14) lineamientos evaluados, de ellos, doce (12) se califican en la categoría mantenimiento del control y dos (2) en deficiencia de control. Este componente frente al periodo anterior se disminuyó en dos (2) puntos porcentuales. Por lo anterior, se concluye que el sistema de Control Interno de la Defensoría del Espacio Público es efectivo y se ajusta a los planes y programas definidos por la Entidad, contribuyendo al logro de los objetivos institucionales y en aras de continuar con el fortalecimiento del mismo.
La entidad cuenta dentro de su Sistema de Control Interno, con una institucionalidad (Líneas de defensa) que le permita la toma de decisiones frente al control (Si/No) (Justifique su respuesta):	Si	El Departamento Administrativo de la Defensoría del Espacio Público, cuenta con la Política de Administración del Riesgo actualizada, la cual contempla el esquema de las líneas de defensa con los roles por cada línea. Los líderes de política tienen designadas responsabilidades en la implementación del MIPG, que le permite a la entidad la toma de decisiones frente al control, conforme a la séptima dimensión de MIPG.

Componente	¿El componente está presente y funcionando?	Nivel de Cumplimiento componente	Estado actual: Explicacion de las Debilidades y/o Fortalezas	Nivel de Cumplimiento componente presentado en el informe anterior	Estado del componente presentado en el informe anterior	Avance final del componente
Ambiente de control	Si	96%	Conclusiones de la evaluación: La evaluación del componente Ambiente de Control alcanzó un resultado del 94%, lo que permite concluir que la Entidad cuenta con un ambiente de control adecuado y efectivo, que proporciona una base razonable para el funcionamiento del Sistema de Control Interno. Sin perjuicio de lo anterior, las oportunidades de mejora identificadas deberán ser atendidas con el fin de fortalecer la operatividad de las líneas de defensa, la gestión del riesgo, la cultura de control y la mejora continua, en concordancia con los principios del MECI y el Modelo Integrado de Planeación y Gestión (MIPG). Fortalezas: La Entidad dispone de condiciones adecuadas para promover una cultura de control, integridad, ética y responsabilidad, así como para soportar el funcionamiento del Sistema de Control Interno. Se observa el compromiso de la Alta Dirección con el fortalecimiento de la gestión institucional, la definición de responsabilidades y el desarrollo de mecanismos de supervisión que contribuyen al logro de los objetivos institucionales. Deficiencias: Producto del seguimiento se evidenció oportunidades de mejora relacionadas con el fortalecimiento del marco metodológico para la administración del riesgo y la gestión de la información estratégica. En particular, se identificó la necesidad de actualizar el procedimiento Administración de Riesgos (código 127-PRCVM-07) y la Política de Administración de Riesgos, incorporando actividades, políticas de operación y lineamientos que definan los tiempos y mecanismos de reporte ante la materialización de riesgos, con el fin de garantizar una gestión más oportuna y efectiva. Asimismo, aunque la Entidad realiza seguimiento al Plan Estratégico y al Plan de Acción mediante el Comité Institucional de Gestión y Desempeño, es necesario que la Alta Dirección revise los resultados del plan estratégico y su alineación a los objetivos de la Entidad. Recomendaciones: -Actualizar la Política de Administración del Riesgo, acorde con la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, así como el procedimiento Administración de Riesgos (código 127-PRCVM-07), con la definición clara de las actividades a realizar cuando se materialice un riesgo. -Fortalecer los mecanismos de seguimiento y revisión por parte de la Alta Dirección al Plan Estratégico Institucional y al Plan de Acción, mediante la socialización periódica e integral de sus avances, el análisis de los indicadores de gestión y la consideración de las alertas preventivas emitidas por la Oficina de Control Interno, con el propósito de facilitar la toma de decisiones y asegurar el cumplimiento de los objetivos estratégicos.	94%	Conclusiones de la evaluación: En el marco de la implementación del Modelo Integrado de Planeación y Gestión (MIPG) y en articulación con el Sistema de Control Interno, conforme a los lineamientos del Modelo Estándar de Control Interno (MECI), y teniendo en cuenta los resultados obtenidos en el segundo semestre de 2025, los cuales reflejan un nivel de cumplimiento del 94%, se puede concluir que el componente de Ambiente de Control se encuentra formalizado, implementado y en funcionamiento dentro de la entidad; sin embargo se evidencian aspectos de oportunidad de mejora. Las prácticas de cultura organizacional se encuentran orientadas hacia el autocontrol, la integridad y la mejora continua, contribuyendo de manera significativa al mantenimiento y fortalecimiento del Sistema de Control Interno. En el mismo sentido, se evidencia que la entidad ha formulado el Plan de Integridad como un componente fundamental del Programa de Transparencia y Ética Pública (PTEP). Respecto a las evaluaciones de las actividades relacionadas con el Ingreso del personal, la entidad cuenta con el plan estratégico del talento humano, el cual fue objeto de seguimiento del líder del proceso; a su vez, la Oficina de Control Interno efectuó auditoría a la planta de personal de la entidad, identificando hallazgos asociados al proceso de vinculación y a las actuaciones administrativas correspondientes. El Departamento de la Defensoría del Espacio Público ha formalizado las instancias requeridas para la implementación y el mantenimiento del Sistema de Control Interno, a través del funcionamiento del Comité Institucional de Gestión y Desempeño y del Comité Institucional de Coordinación de Control Interno. Durante el primer semestre, dichas instancias sesionaron conforme a lo establecido en las Resoluciones 363 de 2024 y 161 de 2024, aprobando los planes de acción en cumplimiento del Decreto 612 de 2018, así como el Plan Anual de Auditoría, respectivamente. En relación con la Política de Administración del Riesgo, esta se encuentra implementada y aplicada de manera transversal en todos los niveles de la entidad. La misma incorpora el esquema de las tres líneas de defensa; sin embargo, el procedimiento "Administración de Riesgos" (código 127-PRCVM-07), no describe actividades frente a la materialización de riesgos y su reporte oportuno. Recomendaciones: Se recomienda continuar con el fortalecimiento de la Política de Talento Humano, en coherencia con las rutas definidas en el Modelo Integrado de Planeación y Gestión (MIPG), específicamente las rutas de la felicidad, el crecimiento, el servicio, la calidad y el análisis de datos, con el fin de consolidar una gestión integral del talento humano. Se sugiere fortalecer el proceso de ingreso de personal, garantizando el estricto cumplimiento de la normatividad vigente aplicable y atendiendo de manera oportuna las observaciones formuladas por la Oficina de Control Interno (OCI) en el informe de auditoría a la planta de personal. Se recomienda revisar y actualizar la Política de Administración del Riesgo y el procedimiento "Administración de Riesgos" (Código 127-PRCVM-07), incorporando de manera expresa las actividades, responsables y mecanismos de seguimiento frente a la materialización de los riesgos identificados.	2%

Evaluación de riesgos	**Si**	**76%**	Conclusiones de la evaluación: Con un nivel de implementación del 76%, el componente Evaluación del Riesgo presenta un grado de madurez aceptable, al evidenciar la existencia de mecanismos para gestionar los riesgos institucionales y apoyar la toma de decisiones. Sin embargo, persisten oportunidades de fortalecimiento en la administración del riesgo y en la evaluación de la efectividad de los controles, cuya atención permitirá mejorar la capacidad de la Entidad para prevenir la materialización de riesgos y asegurar el cumplimiento de sus objetivos estratégicos. Fortalezas: La entidad cuenta con el lineamiento institucional para la gestión del riesgo, formalizado a través de la Política de Administración del Riesgo. Dicha política establece los criterios para el tratamiento, seguimiento y control de los riesgos que puedan afectar el cumplimiento de los objetivos institucionales. En concordancia con este marco, se evidencia que la entidad realiza el monitoreo de la gestión de riesgos con una periodicidad cuatrimestral, responsabilidad atribuida a la segunda línea de defensa. Por su parte, la tercera línea de defensa llevó a cabo la evaluación independiente, en la cual se identificaron riesgos materializados, los cuales fueron reportados de manera oportuna conforme a los procedimientos establecidos. Deficiencias: La evaluación del componente evidenció oportunidades de mejora en la gestión integral del riesgo, relacionadas con el fortalecimiento del marco metodológico, la operación de las líneas de defensa y el seguimiento a los riesgos materializados. Se identificó la necesidad de actualizar la Política de Administración del Riesgo y el procedimiento Administración de Riesgos (código 127-PRCVM-07), incorporando lineamientos claros para la actuación frente a la materialización de riesgos, incluyendo actividades, responsabilidades, tiempos de respuesta y mecanismos de reporte y seguimiento. Asimismo, se evidenciaron debilidades en el tratamiento de los riesgos materializados, debido a la ausencia de planes de tratamiento, acciones implementadas y mecanismos que garanticen su trazabilidad, particularmente en los riesgos asociados al proceso de Seguridad y Privacidad de la Información (sin tratamiento desde el 2025). De igual forma, se observaron oportunidades de fortalecimiento en el ejercicio de monitoreo por parte de la segunda línea de defensa y en la supervisión del Comité Institucional de Gestión y Desempeño, al no evidenciarse la revisión de las acciones adoptadas frente a la materialización de riesgos. Estas situaciones limitan la efectividad de la gestión del riesgo y reducen la capacidad institucional para prevenir, controlar y mitigar los potenciales eventos que afectan el logro de los objetivos. Recomendaciones: -Revisar los mapas de riesgos de Seguridad y Privacidad de la Información correspondientes a las vigencias 2025 y 2026, con el fin de identificar los riesgos materializados y definir, documentar e implementar los respectivos planes de tratamiento, incorporando acciones, responsables, plazos y mecanismos de seguimiento que garanticen la trazabilidad de su gestión y eviten la recurrencia de eventos similares. -Fortalecer el liderazgo y la supervisión de la Alta Dirección en la gestión integral del riesgo, promoviendo la revisión periódica de los riesgos institucionales, el seguimiento al cumplimiento de los planes de tratamiento, la evaluación de la efectividad de las acciones implementadas y la identificación oportuna de potenciales eventos que puedan afectar el logro de los objetivos estratégicos y la toma de decisiones. -Establecer en la Política de Administración del Riesgo, los niveles de responsabilidad acorde con el esquema de línea de defensa, definiendo funciones claras y acciones a cargo de cada línea con especial énfasis en la línea estratégica, a fin de fortalecer la gobernanza, la supervisión y la toma de decisiones frente a los riesgos.	**78%**	Conclusiones de la evaluación: La entidad cuenta con el lineamiento institucional para la gestión del riesgo, formalizado a través de la Política de Administración del Riesgo. Dicha política establece los criterios para el tratamiento, seguimiento y control de los riesgos que puedan afectar el cumplimiento de los objetivos institucionales. En concordancia con este marco, se evidencia que la entidad realiza el monitoreo de la gestión de riesgos con una periodicidad cuatrimestral, responsabilidad atribuida a la segunda línea de defensa. Por su parte, la tercera línea de defensa llevó a cabo la evaluación independiente, en la cual se identificaron riesgos materializados, los cuales fueron reportados de manera oportuna conforme a los procedimientos establecidos. En relación con las actividades definidas en la Política de Administración del Riesgo asignadas a la Alta Dirección, se evidencian debilidades en los procesos de monitoreo y evaluación de las fallas asociadas a los riesgos institucionales. En particular, se identifican deficiencias en la gestión de los riesgos de Seguridad y Privacidad de la Información, los cuales fueron modificados durante la vigencia 2025 sin considerar los antecedentes de materialización de dichos riesgos, lo que limita la efectividad de los controles y la toma de decisiones informadas. Ahora bien, al comparar el componente de evaluación de riesgos entre el primer y segundo semestre de la vigencia 2025, se evidencia una disminución en su desempeño, al pasar de un 79 % en el primer semestre a un 78 % en el segundo semestre. Esta variación refleja debilidades en los procesos de identificación, evaluación y gestión de eventos potenciales, tanto internos como externos, que podrían afectar el cumplimiento de los objetivos institucionales. Recomendaciones: Fortalecer las actividades a cargo de la Alta Dirección con el acompañamiento de la Oficina Asesora de Planeación, para gestionar de manera correcta los riesgos materializados y su tratamiento en la entidad. Se recomienda revisar y actualizar el mapa de riesgos de Seguridad y Privacidad de la Información, considerando de manera expresa los riesgos que se hayan materializado, y establecer los correspondientes planes de tratamiento, de conformidad con la metodología institucional. Así mismo, se sugiere documentar y sustentar técnicamente las justificaciones que respalden la eliminación de riesgos de esta naturaleza del mapa de riesgos de la entidad. Frente a las funciones de la línea estratégica (Alta Dirección), realizar la evaluación periódica de los riesgos de gestión en el marco del Comité Institucional de Coordinación de Control Interno y del Comité Institucional de Gestión y Desempeño, definiendo acciones concretas orientadas al fortalecimiento de su administración. En este sentido, se sugiere a la Oficina Asesora de Planeación presentar de manera sistemática el estado de la gestión de riesgos, así como proponer las mejoras que resulten pertinentes. Se recomienda realizar capacitaciones y mesas de trabajo articuladas entre la Oficina Asesora de Planeación (OAP) y las diferentes dependencias, con el fin de fortalecer la adecuada identificación, evaluación, tratamiento y seguimiento de los riesgos institucionales, en concordancia con la metodología de gestión del riesgo adoptada por la entidad.	**-2%**
Actividades de control	**Si**	**92%**	Con un resultado del 92%, el componente Actividades de Control presenta un buen nivel de implementación y madurez en el DADEP, evidenciando que la Entidad dispone de controles adecuados para apoyar la gestión de los riesgos y el logro de los objetivos institucionales. Sin perjuicio de lo anterior, se presentan oportunidades de mejora identificadas por la OCI que permitirán fortalecer la actualización, ejecución y evaluación de la efectividad de los controles, incrementando la capacidad institucional para responder a los cambios del entorno, optimizar los procesos y garantizar un Sistema de Control Interno cada vez más efectivo. Fortalezas: La Entidad evidencia un adecuado diseño e implementación de las actividades de control, respaldadas por documentación actualizada y formalizada, con la asignación de funciones y responsabilidades acorde al esquema de líneas de defensa. Asimismo, se observa un proceso permanente de actualización de los instrumentos del Sistema Integrado de Gestión (Visor MIPG), lo que contribuye a fortalecer la gestión del riesgo, la eficacia de los controles y el cumplimiento de los objetivos institucionales. Deficiencias: Si bien la Entidad cuenta con un modelo operativo por procesos, responsabilidades definidas y controles formalmente establecidos para la gestión institucional y la seguridad de la información, se evidenciaron oportunidades de mejora en la efectividad de las actividades de control. En particular, persisten debilidades en la segregación de funciones derivadas de la limitada planta de personal y en la operación de los controles asociados a la gestión de riesgos de Seguridad y Privacidad de la Información, al no evidenciarse la definición, implementación y seguimiento de acciones de tratamiento frente a los riesgos materializados (2025). Estas situaciones limitan la trazabilidad y la eficacia de los controles implementados en concordancia con los lineamientos del MECI y la Política de Administración del Riesgo. Recomendaciones: -Fortalecer los mecanismos de evaluación del diseño y la operación de los controles incorporados en los mapas de riesgos, con el fin de verificar periódicamente su efectividad para mitigar los riesgos identificados y asegurar el cumplimiento de los objetivos institucionales. -Asegurar la alineación de los controles con los procesos, procedimientos y actividades críticas de la Entidad, con el fin de garantizar que su diseño responda a los riesgos asociados y a la realidad operativa e institucional de cada proceso. -Implementar revisiones periódicas de la adecuación, pertinencia y eficacia de los controles, en coordinación con los líderes de proceso y las áreas responsables, considerando los cambios normativos, organizacionales, tecnológicos, operativos y las evaluaciones independientes que puedan afectar su funcionamiento. -Fortalecer la cultura de autocontrol y autogestión en la primera línea de defensa, promoviendo la ejecución consistente de los controles, el monitoreo permanente de los riesgos y el reporte oportuno de las desviaciones o eventos que puedan afectar el cumplimiento de los objetivos institucionales.	**88%**	Conclusiones de la evaluación: Como resultado de la evaluación, se observa un aumento en el nivel de desempeño del componente de actividades de control, pasando de un 85% en el primer semestre a un 88% en el segundo semestre de 2025. Esto obedece a las actividades de control y segregación de funciones, acorde con el esquema de líneas de defensa. No obstante, se presentan deficiencias actividades de control relevantes sobre las infraestructuras tecnológicas, especialmente de los procesos de seguridad de la información y los riesgos identificados acorde con las realidades de la entidad. En el marco del esquema de líneas de defensa, se evidenció que la Oficina Asesora de Planeación (OAP), en su calidad de segunda línea de defensa, realiza el monitoreo de los riesgos institucionales y de corrupción con periodicidad cuatrimestral. Estos últimos fueron actualizados durante el primer semestre de 2025 mediante mesas de trabajo desarrolladas con las diferentes áreas de la entidad. Adicionalmente, la tercera línea de defensa, representada por la Oficina de Control Interno (OCI), incorpora un componente de evaluación de riesgos en las evaluaciones independientes efectuadas durante el segundo semestre de 2025. Recomendaciones: •Mantener las matrices de riesgos (gestión, corrupción, seguridad de la información y fiscales) actualizadas, teniendo en cuenta la materialización de riesgos para cada uno de los procesos de acuerdo con los cambios del entorno, haciendo énfasis en la identificación y diseño de los riesgos, así como el establecimiento de controles efectivos y el cumplimiento de los mismos. •Continuar con los monitoreos de las matrices de riesgos de los procesos, cumpliendo con la política de administración del riesgo aprobada. Los resultados de la gestión y administración de estos riesgos deberán ser informados a la dirección para mejorar el proceso de toma de decisiones. La entidad en cabeza de la Oficina de Tecnologías de la información deberá: "Mantener y asegurar con acciones tangibles y medibles los controles de la infraestructura tecnológica, la seguridad de la información, desarrollo y mantenimiento de las tecnologías de la entidad". •Realizar las gestiones para la designación del Oficial de Protección de Datos Personales y el simulacro de pérdida de datos. •Mantener actualizado las matrices de roles de usuarios de los diferentes sistemas de información de la entidad y asegurar la segregación de funciones y el mantenimiento del control interno en los encargos generados en los diferentes sistemas.	**4%**
Información y comunicación	**Si**	**93%**	Conclusión: Durante el primer semestre de 2026, el componente de Información y Comunicación mantuvo un desempeño estable frente al segundo semestre de 2025, con avances en la actualización del Mapa de Riesgos de Seguridad de la Información, la implementación del Plan Estratégico de Comunicaciones 2026 y el fortalecimiento de los controles relacionados con la confidencialidad, integridad y disponibilidad de la información. Así mismo, continuó el uso de los sistemas misionales SIDEP, SIGDEP y del Sistema Gerencial, junto con los mecanismos de comunicación interna y externa, el seguimiento a métricas de redes sociales y la evaluación de la percepción de usuarios. Sin embargo, se mantienen observaciones identificadas en el periodo anterior relacionadas con la actualización y publicación del Inventario de Activos de Información y de la caracterización de ciudadanos, usuarios y grupos de valor. Adicionalmente, se evidenció la necesidad de actualizar algunos documentos del proceso de Atención a la Ciudadanía y de formalizar las acciones de mejora derivadas de las encuestas de satisfacción, definiendo responsables, plazos e indicadores que permitan verificar su implementación y efectividad. Fortalezas -Actualización del Mapa de Riesgos de Seguridad de la Información y fortalecimiento de los controles asociados. -Implementación del PEC 2026 con indicadores para medir la efectividad de la comunicación interna y externa. -Continuidad de los sistemas de información misionales, los canales institucionales y los mecanismos de evaluación de la percepción de usuarios. Deficiencias -Persistencia en la falta de actualización y publicación del Inventario de Activos de Información y de la caracterización de usuarios y grupos de valor. -Documentos del proceso de Atención a la Ciudadanía pendientes de actualización y publicación. Recomendaciones -Culminar y publicar las versiones actualizadas del Inventario de Activos de Información y de la caracterización de usuarios y grupos de valor. -Actualizar los documentos pendientes del proceso de Atención a la Ciudadanía. -Formalizar las acciones de mejora derivadas de las encuestas de satisfaccion usuarios como proceso de autoevaluacion, estableciendo responsables, plazos, indicadores y mecanismos de seguimiento.	**93%**	Conclusión: Durante el segundo semestre de 2025, el componente de Información y Comunicación del DADEP evidenció un nivel de madurez y estabilidad acorde con los principios del Modelo Estándar de Control Interno (MECI) y el esquema de Líneas de Defensa, donde se ha mantenido su indicador en un 93% reafirmando la consistencia frente a los resultados del primer semestre y fortaleciendo progresivamente la gestión de la información y la comunicación institucional. Fortalezas: - Consolidación y fortalecimiento de los sistemas de información misionales y de apoyo (SIDEP 2.0, Sistema Gerencial, CAPID, SICAPITAL, ORFEO y sitio web institucional), mejorando la disponibilidad, confiabilidad y trazabilidad de la información. - Gestión estructurada del inventario de activos de información, con actualización de atributos de seguridad, confidencialidad, integridad y disponibilidad. - Integración de fuentes de información internas y externas a través del SIGDEP, el Observatorio del Espacio Público y la Batería de Indicadores, garantizando interoperabilidad y acceso oportuno a información clave. - Implementación sostenida de controles de seguridad de la información mediante el MSPI y la gestión de riesgos asociados. - Continuidad de los mecanismos de comunicación interna y externa a través del Plan Estratégico de Comunicaciones, procedimientos definidos y canales institucionales, incluyendo Bogotá Te Escucha. Deficiencias: - Actualización insuficiente del mapa de riesgos de seguridad de la información frente a riesgos materializados y sus tratamientos. - Falta de armonización documental en la caracterización de usuarios y grupos de valor, al mantenerse como soporte una versión con fecha anterior. Recomendaciones - Actualizar oportunamente el mapa de riesgos de seguridad de la información y fortalecer su seguimiento. - Armonizar y publicar la caracterización actualizada de usuarios y grupos de valor en los repositorios institucionales. - Mejorar la oportunidad en la publicación y uso de los resultados de percepción para la toma de decisiones. - Mantener la evaluación periódica de la efectividad de los canales de comunicación, incorporando métricas de impacto.	**0%**
Monitoreo	**Si**	**93%**	Conclusión: Para el primer semestre de 2026, el componente de Actividades de Monitoreo obtuvo un resultado del 93%, presentando una disminución de tres puntos porcentuales frente al 96% alcanzado en el segundo semestre de 2025. Durante el periodo se mantuvieron las actividades de seguimiento por parte de la Alta Dirección, la ejecución del Plan Anual de Auditoría con enfoque basado en riesgos, el monitoreo de la segunda línea de defensa y la evaluación de los planes de mejoramiento internos y externos. No obstante, la disminución estuvo asociada principalmente a debilidades en la generación y seguimiento de acciones derivadas de autoevaluaciones de la primera línea de defensa, la evaluación de los servicios tercerizados según su nivel de riesgo y el uso de la información del sistema PQRSD para definir acciones internas de mejora. Fortalezas: -Se mantuvo el seguimiento al Plan Anual de Auditoría y la evaluación periódica del Sistema de Control Interno por parte de la Alta Dirección. -La Oficina de Control Interno ejecutó las evaluaciones independientes con enfoque basado en riesgos y realizó seguimiento a los planes de mejoramiento internos y externos mediante el aplicativo ECM. -Se mantuvo el monitoreo permanente de indicadores, planes institucionales y mapas de riesgos por parte de la segunda línea de defensa. - Consideración de evaluaciones externas y análisis de su impacto en el Sistema de Control Interno. - Reporte oportuno de deficiencias de control interno a los niveles directivos y líderes de proceso. Deficiencias: -No se evidenciaron acciones de mejoramiento derivadas específicamente de ejercicios de autoevaluación realizados por la primera línea de defensa. -La evaluación de los servicios tercerizados no incorporó la clasificación del nivel de riesgo, los controles aplicados ni los resultados del seguimiento según su criticidad. -El análisis de la información del Sistema PQRSD continuó siendo principalmente estadístico. Recomendaciones -Fortalecer la implementación de autoevaluaciones por parte de la primera línea de defensa y asegurar que generen acciones de mejoramiento debidamente documentadas y monitoreadas. -Incorporar criterios de clasificación del riesgo, controles y resultados del seguimiento en la evaluación de los servicios tercerizados. -Fortalecer el análisis de la información proveniente del Sistema PQRSD, definiendo acciones de mejora internas, responsables, plazos y mecanismos de seguimiento que permitan utilizar este insumo como herramienta para el fortalecimiento del Sistema de Control Interno.	**96%**	Conclusión: Para el segundo semestre de 2025, se evidenció que la entidad modifico su calificacion pasando de un 98% a un 96% de cumplimiento en su componente de Actividades de Monitoreo. En general, se evidenció un funcionamiento adecuado de los mecanismos de seguimiento y evaluación, así como una participación activa de la Alta Dirección y de las instancias de control en el análisis de resultados y la toma de decisiones. En este periodo, el Comité Institucional de Coordinación de Control Interno aprobó y realizó seguimiento al Plan Anual de Auditoría 2025 (versión 3), mientras que la Oficina de Control Interno desarrolló evaluaciones independientes con enfoque basado en riesgos y presentó oportunamente sus resultados. A su vez, la segunda línea de defensa adelantó actividades de monitoreo continuo sobre indicadores, planes y riesgos, apoyándose en el uso del aplicativo ECM para el seguimiento de acciones de mejora y la trazabilidad de las evidencias. Fortalezas: -Seguimiento efectivo al Plan Anual de Auditoría y a su ejecución por parte del CICCI. - Evaluación periódica de los resultados del Sistema de Control Interno por la Alta Dirección. - Ejecución de evaluaciones independientes con enfoque basado en riesgos y socialización de resultados. - Aplicación del esquema de Líneas de Defensa, con monitoreo continuo y seguimiento sistemático a los planes de mejoramiento mediante el aplicativo ECM. - Consideración de evaluaciones externas y análisis de su impacto en el Sistema de Control Interno. - Reporte oportuno de deficiencias de control interno a los niveles directivos y líderes de proceso. Deficiencias: - No se evidenció la formulación de acciones de mejora derivadas de autoevaluaciones realizadas por la primera línea de defensa. - Demoras en la gestion de las acciones del plan de mejoramiento, generando alertas por cargue de evidencias incompletas o inconsistentes en el sistema ECM. Recomendaciones - Fortalecer la cultura de autoevaluación en la primera línea de defensa y su articulación con los planes de mejoramiento. - Mejorar la oportunidad en la validación y publicación de los informes derivados del Sistema PQRD. - Revisar si es necesario actualizar la Política de Administración del Riesgo. - Verificar si es necesario modificar la metodología para la elaboracion de matrices de riesgo. - Mantener y optimizar el uso del aplicativo ECM como herramienta de seguimiento y control. - Reforzar la articulación entre dependencias responsables del cumplimiento de planes de mejora, mediante reuniones de seguimiento.	**-3%**