

Nombre de la Entidad:	Contraloría General de Medellín	
Periodo Evaluado:	30/06/2021 - 31/12/2021	

Estado del sistema de Control Interno de la entidad	90%
---	-----

Componente	¿El componente está presente y funcionando?	Nivel de Cumplimiento Componente	Estado actual: Explicación 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
Entorno de control	Si	92%	Fortalezas (Aspectos que se encuentran presentes y funcionando correctamente, por lo tanto se requiere acciones o actividades dirigidas a su mantenimiento dentro del marco de las líneas de defensa): • Aplicación del Código de Integridad - Mecanismos para el manejo de conflictos de interés - Evaluación de las acciones transversales de integridad, mediante el monitoreo permanente de los riesgos de corrupción - Análisis sobre viabilidad para el establecimiento de una línea de denuncia interna • Creación o actualización del Comité Institucional de Coordinación de Control Interno - Definición y documentación del Esquema de Líneas de Defensa • Definición de líneas de reporte en temas clave para la toma de decisiones, atendiendo el Esquema de Líneas de Defensa - Definición y evaluación de la Política de Administración del Riesgo - Definición de los niveles de aceptación del riesgo, teniendo en cuenta cada uno de los objetivos establecidos • Evaluación de la planeación estratégica, considerando áreas frente a posibles incumplimientos, necesidades de recursos y cambios en el entorno • Evaluación de la planeación estratégica, considerando áreas frente a posibles incumplimientos, necesidades de recursos y cambios en el entorno • Políticas claras y comunicadas relacionadas con la responsabilidad de cada servidor sobre el desarrollo y mantenimiento del control interno (la línea de defensa) • Aparte de la información suministrada por la 22 y 3a línea de defensa se toma decisiones para garantizar el cumplimiento de las metas y objetivos • Seguimiento al Plan Anual de Auditoría de la OCI - Evaluación frente a los productos y servicios en los cuales participan los controladores de apoyo - Análisis de información asociada con la generación de reportes financieros por parte de la Alta Dirección - Evaluación del impacto de los informes presentados por la OCI en relación con la mejora institucional Oportunidad de mejora (Aspectos que se encuentran presentes y funcionando, pero requieren acciones dirigidas a fortalecer o mejorar su diseño y/o ejecución): • Mecanismos frente a la detección y prevención del uso inadecuado de información privilegiada u otras situaciones que puedan implicar riesgos para la entidad - Evaluación del impacto del Sistema de Control Interno - Acordar con la estructura del Esquema de Líneas de Defensa definición estándares de reporte, periodicidad y responsables frente a diferentes temas críticos de la entidad - Evaluación de la estructura de control a partir de los cambios en procesos, procedimientos, u otras herramientas	82%	Fortalezas (Aspectos que se encuentran presentes y funcionando correctamente, por lo tanto se requiere acciones o actividades dirigidas a su mantenimiento dentro del marco de las líneas de defensa): • Mecanismos para el manejo de conflictos de interés - Evaluación de las acciones transversales de integridad, mediante el monitoreo permanente de los riesgos de corrupción - Análisis sobre viabilidad para el establecimiento de una línea de denuncia interna - Definición y documentación del Esquema de Líneas de Defensa - Definición y evaluación de la Política de Administración del Riesgo - Definición de los niveles de aceptación del riesgo, teniendo en cuenta cada uno de los objetivos establecidos • Evaluación de la planeación estratégica, considerando áreas frente a posibles incumplimientos, necesidades de recursos y cambios en el entorno • Evaluación de la planeación estratégica, considerando áreas frente a posibles incumplimientos, necesidades de recursos y cambios en el entorno • Políticas claras y comunicadas relacionadas con la responsabilidad de cada servidor sobre el desarrollo y mantenimiento del control interno (la línea de defensa) • Aparte de la información suministrada por la 22 y 3a línea de defensa se toma decisiones para garantizar el cumplimiento de las metas y objetivos • Seguimiento al Plan Anual de Auditoría de la OCI - Evaluación frente a los productos y servicios en los cuales participan los controladores de apoyo Oportunidad de mejora (Aspectos que se encuentran presentes y funcionando, pero requieren mejoras frente a su diseño, ya que opera de manera efectiva): • Definición de líneas de reporte en temas clave para la toma de decisiones, atendiendo el Esquema de Líneas de Defensa Oportunidad de mejora (Aspectos que se encuentran presentes y funcionando, pero requieren acciones dirigidas a fortalecer o mejorar su diseño y/o ejecución): • Aplicación del Código de Integridad - Mecanismos frente a la detección y prevención del uso inadecuado de información privilegiada u otras situaciones que puedan implicar riesgos para la entidad - Creación o actualización del Comité Institucional de Coordinación de Control Interno - Evaluación del impacto del Plan Institucional de Capacitación - Acordar con la estructura del Esquema de Líneas de Defensa definición estándares de reporte, periodicidad y responsables frente a diferentes temas críticos de la entidad - Análisis de información asociada con la generación de reportes financieros en OCI - Evaluación de la estructura de control a partir de los cambios en procesos, procedimientos, u otras herramientas - Evaluación del impacto de los informes presentados por la OCI en relación con la mejora institucional	10%
Evaluación de riesgos	Si	91%	Fortalezas (Aspectos que se encuentran presentes y funcionando correctamente, por lo tanto se requiere acciones o actividades dirigidas a su mantenimiento dentro del marco de las líneas de defensa): • Mecanismos para vincular o relacionar el plan estratégico con los objetivos estratégicos y estos a su vez con los objetivos operativos • Los objetivos de los procesos, programas o proyectos (según aplique) que están definidos, son específicos, medibles, alcanzables, relevantes, delimitados en el tiempo • Evaluación periódica de los objetivos establecidos para asegurar que estos continúan siendo consistentes y apropiados para la Entidad • A partir de la política de Administración del Riesgo, su alcance define lineamientos para toda la entidad • Consolidación de información clave por parte de la Oficina de Planeación, frente a la gestión del riesgo y riesgos de materiales por parte de la Alta Dirección, definición y seguimiento de la planeación estratégica y la política de Administración del Riesgo • Acordar con el análisis del entorno interno y externo, definición de los procesos, programas o proyectos (según aplique), susceptibles de posibles actos de corrupción • Monitoreo a los riesgos de corrupción con la periodicidad establecida en la Política de Administración del Riesgo • Para el desarrollo de las actividades de control, se realiza división de las funciones y segregación en diferentes personas para reducir el riesgo de acciones fraudulentas • Monitoreo a los riesgos aceptados revalidando que sus condiciones no hayan cambiado y definir su pertinencia para sostenidos o ajustarlos • Monitoreo de los factores internos y externos fuente para la definición de acciones • Evaluación en las fallas en los controles (diseño y ejecución) para definir cursos de acción apropiados para su mejora, por parte de la alta dirección Oportunidad de mejora (Aspectos que se encuentran presentes y funcionando, pero requieren acciones dirigidas a fortalecer o mejorar su diseño y/o ejecución): • Análisis de los riesgos asociados a actividades tercerizadas, basados en los informes de la segunda y tercera línea de defensa • Evaluación en las fallas en los controles (diseño y ejecución) para definir cursos de acción apropiados para su mejora • Análisis del impacto sobre el control interno por cambios en los diferentes niveles organizacionales	81%	Fortalezas (Aspectos que se encuentran presentes y funcionando correctamente, por lo tanto se requiere acciones o actividades dirigidas a su mantenimiento dentro del marco de las líneas de defensa): • Mecanismos para vincular o relacionar el plan estratégico con los objetivos estratégicos y estos a su vez con los objetivos operativos • Los objetivos de los procesos, programas o proyectos (según aplique) que están definidos, son específicos, medibles, alcanzables, relevantes, delimitados en el tiempo • Evaluación periódica de los objetivos establecidos para asegurar que estos continúan siendo consistentes y apropiados para la Entidad • A partir de la política de Administración del Riesgo, su alcance define lineamientos para toda la entidad • Consolidación de información clave por parte de la Oficina de Planeación, frente a la gestión del riesgo y riesgos de materiales por parte de la Alta Dirección, definición y seguimiento de la planeación estratégica y la política de Administración del Riesgo • Acordar con el análisis del entorno interno y externo, definición de los procesos, programas o proyectos (según aplique), susceptibles de posibles actos de corrupción • Monitoreo a los riesgos de corrupción con la periodicidad establecida en la Política de Administración del Riesgo • Para el desarrollo de las actividades de control, se realiza división de las funciones y segregación en diferentes personas para reducir el riesgo de acciones fraudulentas • Monitoreo a los riesgos aceptados revalidando que sus condiciones no hayan cambiado y definir su pertinencia para sostenidos o ajustarlos • Monitoreo de los factores internos y externos fuente para la definición de acciones • Evaluación en las fallas en los controles (diseño y ejecución) para definir cursos de acción apropiados para su mejora, por parte de la alta dirección Oportunidad de mejora (Aspectos que se encuentran presentes y funcionando, pero requieren acciones dirigidas a fortalecer o mejorar su diseño y/o ejecución): • Revisión de riesgos materiales, definición y seguimiento de acciones a seguir y la revisión y actualización de mapa de riesgos correspondiente • Análisis de los riesgos asociados a actividades tercerizadas, basados en los informes de la segunda y tercera línea de defensa • Análisis del impacto sobre el control interno por cambios en los diferentes niveles organizacionales • Evaluación en las fallas en los controles (diseño y ejecución) para definir cursos de acción apropiados para su mejora, basados en los informes de la segunda y tercera línea de defensa	10%
Actividades de control	Si	86%	Fortalezas (Aspectos que se encuentran presentes y funcionando correctamente, por lo tanto se requiere acciones o actividades dirigidas a su mantenimiento dentro del marco de las líneas de defensa): • La división de las funciones y segregación en diferentes personas para reducir el riesgo de error o de incumplimiento de alto impacto en la operación • La identificación y documentación de las situaciones específicas en donde no es posible segregarse adecuadamente las funciones, con el fin de definir actividades de control alternativas para cubrir los riesgos identificados • El diseño de otros sistemas de gestión (bajo normas o estándares internacionales como la ISO), se integran de forma adecuada a la estructura de control de la entidad • Establecimiento de actividades de control relevantes sobre las infraestructuras tecnológicas, los procesos de gestión de la seguridad y sobre los procesos de adaptación, desarrollo y mantenimiento de tecnologías • Selección y desarrollo de actividades de control internas sobre las actividades realizadas por el proveedor de servicios de tecnología • Se cuenta con matrices de roles y usuarios siguiendo los principios de segregación de funciones • La evaluación del diseño de controles frente a la gestión del riesgo • La verificación de que los responsables están ejecutando los controles tal como han sido diseñados • Monitoreo a los riesgos acorde con la política de administración de riesgo establecida para la entidad Oportunidad de mejora (Aspectos que se encuentran presentes y funcionando, pero requieren acciones dirigidas a fortalecer o mejorar su diseño y/o ejecución): • La generación de información de la 3a línea de defensa, como evaluador independiente en relación con los controles implementados por el proveedor de servicios, para asegurar que los riesgos relacionados se mitigan • La evaluación de la actualización de procesos, procedimientos, políticas de operación, instructivos, manuales u otras herramientas para garantizar la aplicación adecuada de las principales actividades de control • La evaluación de la adecuación de los controles a las especificidades de cada proceso, considerando cambios en regulaciones, estructuras internas u otros aspectos que determinen cambios en su diseño	79%	Fortalezas (Aspectos que se encuentran presentes y funcionando correctamente, por lo tanto se requiere acciones o actividades dirigidas a su mantenimiento dentro del marco de las líneas de defensa): • La división de las funciones y segregación en diferentes personas para reducir el riesgo de error o de incumplimiento de alto impacto en la operación • El diseño de otros sistemas de gestión (bajo normas o estándares internacionales como la ISO), se integran de forma adecuada a la estructura de control de la entidad • Establecimiento de actividades de control relevantes sobre las infraestructuras tecnológicas, los procesos de gestión de la seguridad y sobre los procesos de adaptación, desarrollo y mantenimiento de tecnologías • Selección y desarrollo de actividades de control internas sobre las actividades realizadas por el proveedor de servicios de tecnología • Se cuenta con matrices de roles y usuarios siguiendo los principios de segregación de funciones • La evaluación del diseño de controles frente a la gestión del riesgo • La verificación de que los responsables están ejecutando los controles tal como han sido diseñados • Monitoreo a los riesgos acorde con la política de administración de riesgo establecida para la entidad Oportunidad de mejora (Aspectos que se encuentran presentes y funcionando, pero requieren acciones dirigidas a fortalecer o mejorar su diseño y/o ejecución): • La identificación y documentación de las situaciones específicas en donde no es posible segregarse adecuadamente las funciones, con el fin de definir actividades de control alternativas para cubrir los riesgos identificados • La generación de información de la 3a línea de defensa, como evaluador independiente en relación con los controles implementados por el proveedor de servicios, para asegurar que los riesgos relacionados se mitigan • La evaluación de la actualización de procesos, procedimientos, políticas de operación, instructivos, manuales u otras herramientas para garantizar la aplicación adecuada de las principales actividades de control • La verificación de que los responsables están ejecutando los controles tal como han sido diseñados • La evaluación de la adecuación de los controles a las especificidades de cada proceso, considerando cambios en regulaciones, estructuras internas u otros aspectos que determinen cambios en su diseño	9%
Información y comunicación	Si	86%	Fortalezas (Aspectos que se encuentran presentes y funcionando correctamente, por lo tanto se requiere acciones o actividades dirigidas a su mantenimiento dentro del marco de las líneas de defensa): • El diseño de sistemas de información para capturar y procesar datos y transformarlos en información para alcanzar los requerimientos de información definidos • Inventario de información relevante (interna y externa) y mecanismo que permita su actualización • Determinación de fuentes de datos (internas y externas) para la captura y procesamiento posterior de información clave para la consecución de metas y objetivos • Existencia de mecanismos que permitan dar a conocer los objetivos y metas estratégicas, de manera tal que todo el personal entienda su papel en su consecución (Considera los canales generadores y de flujo de información) • Políticas de operación relacionadas con la administración de la información (niveles de autoridad y responsabilidad) • Políticas y procedimientos para facilitar una comunicación interna efectiva • Desarrollo e implementación de canales que facilitan la comunicación externa, la cual incluye políticas y procedimientos • Existencia de canales externos definidos de comunicación, asociados con el tipo de información a divulgar, y estos son reconocidos a todo nivel de la organización • Procesos o procedimientos para el manejo de la información externa (qué se recibe, quién la clasifica, quién la responde y la respuesta responde (qué se la canaliza y la respuesta) • Análisis periódico de los resultados frente a la evaluación de percepción por parte de los usuarios o grupos de valor para la incorporación de las mejoras correspondientes Oportunidad de mejora (Aspectos que se encuentran presentes y funcionando, pero requieren acciones dirigidas a fortalecer o mejorar su diseño y/o ejecución): • Desarrollo e implementación de canales de control sobre la integridad, confidencialidad y disponibilidad de los datos e información definidos como relevantes • Definición e implementación de canales de información internos para la denuncia anónima o confidencial de posibles situaciones irregulares y mecanismos específicos para su manejo • Definición e implementación de procedimientos encaminados a evaluar la efectividad de los canales de comunicación con partes externas, así como sus contenidos, de tal forma que se puedan mejorar • Análisis periódico de la caracterización de usuarios o grupos de valor, a fin de actualizarla cuando sea pertinente	79%	Fortalezas (Aspectos que se encuentran presentes y funcionando correctamente, por lo tanto se requiere acciones o actividades dirigidas a su mantenimiento dentro del marco de las líneas de defensa): • El diseño de sistemas de información para capturar y procesar datos y transformarlos en información para alcanzar los requerimientos de información definidos • Existencia de mecanismos que permitan dar a conocer los objetivos y metas estratégicas, de manera tal que todo el personal entienda su papel en su consecución (Considera los canales más apropiados y evalúa su efectividad) • Políticas de operación relacionadas con la administración de la información (niveles de autoridad y responsabilidad) • Políticas y procedimientos para facilitar una comunicación interna efectiva • Existencia de canales externos definidos de comunicación, asociados con el tipo de información a divulgar, y estos son reconocidos a todo nivel de la organización • Procesos o procedimientos para el manejo de la información externa (qué se recibe, quién la clasifica, quién la canaliza), y a la respuesta requerida (qué se la canaliza y la respuesta) • Análisis periódico de los resultados frente a la evaluación de percepción por parte de los usuarios o grupos de valor para la incorporación de las mejoras correspondientes Oportunidad de mejora (Aspectos que se encuentran presentes y funcionando, pero requieren acciones dirigidas a fortalecer o mejorar su diseño y/o ejecución): • Inventario de información relevante (interna y externa) y mecanismo que permita su actualización • Determinación de fuentes de datos (internas y externas), para la captura y procesamiento posterior de información clave para la consecución de metas y objetivos • Desarrollo e implementación de canales de control sobre la integridad, confidencialidad y disponibilidad de los datos e información definidos como relevantes • Definición e implementación de canales de información internos para la denuncia anónima o confidencial de posibles situaciones irregulares y mecanismos específicos para su manejo • Definición e implementación de procedimientos encaminados a evaluar la efectividad de los canales de comunicación con partes externas, así como sus contenidos, de tal forma que se puedan mejorar • Análisis periódico de la caracterización de usuarios o grupos de valor, a fin de actualizarla cuando sea pertinente	11%
Monitoreo	Si	93%	Fortalezas (Aspectos que se encuentran presentes y funcionando correctamente, por lo tanto se requiere acciones o actividades dirigidas a su mantenimiento dentro del marco de las líneas de defensa): • Aprobación y seguimiento en el COCI del Plan Anual de Auditoría presentado por parte del Jefe de Control Interno • Realización de evaluaciones independientes periódicas (con una frecuencia definida por base en el análisis de riesgo), que le permite evaluar el diseño y operación de los controles establecidos y definir su efectividad para enfocar la materialización de riesgos • Implementación de procedimientos de monitoreo continuo como parte de las actividades de la 3a línea de defensa, a fin de contar con información clave para la toma de decisiones • Mirada independiente de las operaciones a partir de la evaluación externa de organismos de control y vigilancia, así como la consolidación y conclusión sobre el impacto en el Sistema de Control Interno, a fin de determinar las rutas de acción • Políticas donde se establece a quién reportar las deficiencias de control interno como resultado del monitoreo continuo • Seguimiento a las acciones correctivas relacionadas con las deficiencias comunicadas sobre el Sistema de Control Interno y si se han cumplido en el tiempo establecido • Evaluación de los procesos y/o servicios tercerizados, acorde con su nivel de riesgo • Verificación del manejo y cumplimiento de las acciones incluidas en los planes de mejoramiento producto de las autoevaluaciones (2° Línea) • Evaluación de la efectividad de las acciones incluidas en los Planes de mejoramiento producto de las auditorías internas y de entes externos • Reporte de las deficiencias de control interno a los responsables de nivel jerárquico superior, para tomar las acciones correspondientes Oportunidad de mejora (Aspectos que se encuentran presentes y funcionando, pero requieren acciones dirigidas a fortalecer o mejorar su diseño y/o ejecución): • Evaluación de los resultados de las evaluaciones (continuas e independientes) para concluir acerca de la efectividad del Sistema de Control Interno • Evaluación del efecto de las evaluaciones independientes en el Sistema de Control Interno de la entidad y su impacto en el logro de los objetivos, a fin de determinar cursos de acción para su mejora	79%	Fortalezas (Aspectos que se encuentran presentes y funcionando correctamente, por lo tanto se requiere acciones o actividades dirigidas a su mantenimiento dentro del marco de las líneas de defensa): • Aprobación y seguimiento en el COCI del Plan Anual de Auditoría presentado por parte del Jefe de Control Interno • Realización de evaluaciones independientes periódicas (con una frecuencia definida por base en el análisis de riesgo), que le permite evaluar el diseño y operación de los controles establecidos y definir su efectividad para enfocar la materialización de riesgos • Mirada independiente de las operaciones a partir de la evaluación externa de organismos de control y vigilancia, así como la consolidación y conclusión sobre el impacto en el Sistema de Control Interno, a fin de determinar los cursos de acción • Políticas donde se establece a quién reportar las deficiencias de control interno como resultado del monitoreo continuo • Seguimiento a las acciones correctivas relacionadas con las deficiencias comunicadas sobre el Sistema de Control Interno y si se han cumplido en el tiempo establecido • Evaluación de la información suministrada por los usuarios (Sistema PORD), así como de otras partes interesadas para la mejora del Sistema de Control Interno de la Entidad • Evaluación de la efectividad de las acciones incluidas en los Planes de mejoramiento producto de las auditorías internas y de entes externos Oportunidad de mejora (Aspectos que se encuentran presentes y funcionando, pero requieren acciones dirigidas a fortalecer o mejorar su diseño y/o ejecución): • Evaluación de los resultados de las evaluaciones (continuas e independientes) para concluir acerca de la efectividad del Sistema de Control Interno • Evaluación de los procesos y/o servicios tercerizados, acorde con su nivel de riesgos • Implementación de procedimientos de monitoreo continuo como parte de las actividades de la 3a línea de defensa, a fin de contar con información clave para la toma de decisiones • Evaluación del efecto de las evaluaciones independientes en el Sistema de Control Interno de la entidad y su impacto en el logro de los objetivos, a fin de determinar cursos de acción para su mejora • Reporte de las deficiencias de control interno a los responsables de nivel jerárquico superior, para tomar las acciones correspondientes • Verificación del manejo y cumplimiento de las acciones incluidas en los planes de mejoramiento producto de las autoevaluaciones (2° Línea)	14%

