



POLÍTICA
DE GESTIÓN
INTEGRAL
DE RIESGOS

CÓDIGO: POL-DEP-004
Documento vigente a partir del:
20/09/2023

VERSIÓN: 7

GESTIÓN INTEGRAL DE RIESGOS



POLÍTICA
DE GESTIÓN
INTEGRAL
DE RIESGOS

CÓDIGO: POL-DEP-004
Documento vigente a partir del:
20/09/2023

VERSIÓN: 7

Tabla de contenido

1. INTRODUCCIÓN	3
2. DECLARACIÓN DE VALOR	3
3. OBJETIVOS	4
4. ALCANCE	5
5. TÉRMINOS Y DEFINICIONES	6
6. PRINCIPIOS.....	9
7. INICIATIVAS	11
8. LINEAMIENTOS METODOLÓGICOS PARA LA ADMINISTRACIÓN DEL RIESGO Y RESPONSABLES.....	12
9. SEGUIMIENTO Y EVALUACIÓN DE LA POLÍTICA.	33
10. NATURALEZA DEL CAMBIO.....	34



POLÍTICA
DE GESTIÓN
INTEGRAL
DE RIESGOS

CÓDIGO: POL-DEP-004
Documento vigente a partir del:
20/09/2023

VERSIÓN: 7

1. INTRODUCCIÓN

El desarrollo de cualquier actividad está expuesto a situaciones que pueden impactar en forma negativa y afectar los objetivos propuestos. Como consecuencia de la diversidad de riesgos, se requiere un acercamiento más profundo, metodológico y sistemático a la administración de ellos.

Para la entidad los lineamientos normativos y metodológicos se realizan bajo lo establecido en el Modelo Integrado de Planeación y Gestión y en la Norma ISO 9001:2015.

Es importante aclarar que con la entrada en vigencia del modelo integrado de planeación y gestión (MIPG), que integra los sistemas de gestión de la calidad y de desarrollo administrativo; se crea un único sistema de gestión articulado con el sistema de control interno, el cual se actualiza y alinea con los estándares internacionales, como son el modelo COSO 2013, COSO ERM 2017 y el modelo de las tres líneas de defensa.

Es así que la definición de esta política ha sido articulada a las directrices que son emanadas producto de la implementación de lo anteriormente mencionado. Por ende, este documento recoge los mínimos institucionales establecidos para realizar la gestión integral de riesgos.

La gestión integral de riesgos es un proceso desarrollado por toda la organización para identificar y administrar los eventos potenciales que pueden afectar el logro de la estrategia, la ejecución de proyectos y los procesos en general. El ciclo de la gestión integral de riesgos comprende actividades de identificación, medición, control, monitoreo, comunicación y divulgación de los riesgos.

2. DECLARACIÓN DE VALOR



POLÍTICA
DE GESTIÓN
INTEGRAL
DE RIESGOS

CÓDIGO: POL-DEP-004
Documento vigente a partir del:
20/09/2023

VERSIÓN: 7

Como resultado de lo anterior, Artesanías de Colombia S.A. - BIC ha decidido implementar una política que permita reconocer de forma sistemática los eventos internos o externos a ella que pueden representar riesgos para el logro de los objetivos institucionales. Lo anterior requiere la implementación de herramientas para evaluarlos de manera consistente, determinar sus consecuencias y poder desarrollar acciones de mitigación que permitan mantenerlos en un nivel aceptable.

Esto por medio de la identificación, análisis, valoración e implementación de controles que permitan garantizar la eficiencia en el uso de los recursos físicos, financieros, tecnológicos y de talento humano en pro del beneficio de lo público.

Por esta razón el compromiso de la entidad en este sentido, se visibiliza a través de la declaración de valor que a continuación se presenta:

“Artesanías de Colombia está comprometida con la administración de los riesgos derivados del actuar de sus procesos, incluyendo aquellos hechos generadores de corrupción, mediante la identificación, análisis y valoración de ellos, con el propósito de definir las acciones necesarias tendientes a mitigar su materialización y el impacto que puedan tener sobre el cumplimiento de la misión de la entidad, los objetivos estratégicos, la ejecución de los planes, programas y proyectos y la óptima gestión pública”.

3. OBJETIVOS

Artesanías de Colombia S.A. - BIC ha establecido los siguientes objetivos

3.1. GENERAL:



Establecer los lineamientos metodológicos para identificar, clasificar, valorar, establecer controles, responsables y formular los planes de tratamiento de los riesgos de gestión y estratégicos, corrupción y seguridad digital de la entidad, en un nivel aceptable, asociados a todos los procesos, servicios y trámites, planes, programas, o proyectos, que puedan afectar el cumplimiento de los objetivos estratégicos y misionales de la entidad.

3.2. ESPECÍFICOS

- ✓ Realizar análisis periódicos del contexto organizacional, que permitan identificar oportunamente riesgos u oportunidades.
- ✓ Establecer controles e identificar oportunidades cuando se detecten desviaciones en los avances de la gestión, se identifiquen posibilidad de materialización de un riesgo o mejoras a los procesos
- ✓ Definir responsables que lideren y/o ejecuten las acciones de control orientadas a evitar la materialización de los riesgos identificados.
- ✓ Realizar seguimiento de manera periódica al avance y cumplimiento de los controles establecidos, que permitan identificar brechas y emprender acciones de manera oportuna.
- ✓ Definir las acciones a emprender en caso de materialización de los riesgos (acciones de contingencia).
- ✓ Mantener informadas a las partes involucradas sobre el estado y el perfil de riesgos de la entidad.

4. ALCANCE

Esta política, como elemento del Modelo Integrado de Planeación y Gestión, busca fomentarla cultura del autocontrol en los procesos definidos en el Modelo de Operación, por lo cual debe ser aplicada por todos los procesos, en



el marco de los diferentes proyectos, en la prestación de los servicios de la entidad y en las acciones ejecutadas por los colaboradores, durante del ejercicio de sus funciones y/o cumplimiento de sus obligaciones. Respecto a los riesgos de seguridad digital, estos se deben gestionar de acuerdo con el Plan de Seguridad y Privacidad de la Información.

5. TÉRMINOS Y DEFINICIONES

5.1. Activo de Seguridad de la Información: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital. (Guía para la administración del riesgo y el diseño de controles en entidades públicas- DAFP – Versión 5)

5.2. Administración o gestión del Riesgo: Es el proceso efectuado por las diferentes líneas de defensa, según su rol, para proporcionar un aseguramiento razonable con respecto al logro de los objetivos. Incluye el conjunto de elementos de control y sus interrelaciones, para que Artesanías de Colombia maneje los eventos, tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de sus objetivos institucionales. La gestión del riesgo contribuye a generar la cultura de autocontrol y autoevaluación al interior de la Entidad.

5.3. Análisis de Riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel del mismo

5.4. Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta



Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

5.5. Circunstancias Inmediatas: Se trata de aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituye la causa principal o básica- causa raíz- para que se presente el riesgo, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.

5.6. DAFP: Departamento Administrativo de la Función Pública.

5.7. Evaluación del Riesgo: Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

5.8. Evento: Presencia o cambio de un conjunto particular de circunstancias.

5.9. Fuente de Riesgos: Elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo.

5.10 Identificación del Riesgo: Proceso para encontrar, reconocer y describir el riesgo. Infraestructura crítica cibernética: Es aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado.

5.11. Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo

5.12. Mapa de calor de riesgo: matriz con dos ejes, donde el eje “y”



representa la probabilidad de frecuencia del riesgo y el eje “x” representa el impacto que puede tener el mismo, en el cual según la calificación del riesgo se puede evidenciar la ubicación del mismo y la zona de calor en la que se encuentra.

5.13. Monitoreo: Verificación, supervisión, observación crítica o determinación continua del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

5.14. Nivel o Zona del Riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo puede ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto

5.15. Nivel de aceptación del riesgo: Decisión informada de tomar un riesgo particular (NTC GTC137, numeral 3.7.1.6). Para riesgo de corrupción es inaceptable.

5.16. Plan para la Gestión del Riesgo: Conjunto de acciones para abordar riesgos que se encuentran dentro del marco de referencia para gestionarlos, en esta se definen componentes como los responsables, los recursos y plazos que se van a utilizar para mitigar, eliminar o asumir los riesgos.

5.17. Política de administración del riesgo: Declaración de la entidad e intenciones generales de la organización con respecto a la gestión integral del Riesgo.



POLÍTICA
DE GESTIÓN
INTEGRAL
DE RIESGOS

CÓDIGO: POL-DEP-004
Documento vigente a partir del:
20/09/2023

VERSIÓN: 7

5.18. Probabilidad: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

5.19. Revisión: Acción que se emprende para determinar la idoneidad, conveniencia y eficacia de la materia en cuestión para lograr los objetivos establecidos.

5.20. Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

5.21. Riesgo Fiscal: Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

5.22 Tipos de Riesgos

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

5.23. Tolerancia al riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad

6. PRINCIPIOS



POLÍTICA
DE GESTIÓN
INTEGRAL
DE RIESGOS

CÓDIGO: POL-DEP-004
Documento vigente a partir del:
20/09/2023

VERSIÓN: 7

Los riesgos de gestión, corrupción, seguridad digital y fiscal, surgen tanto de la amenaza de que algo no deseado ocurra, como de que algo bueno no ocurra.

El riesgo es un aspecto inesperado en la operación y debe ser adecuadamente administrado y gestionado, siendo por ello necesario analizar y considerar la existencia de condiciones, situaciones o eventos que pueden desencadenarse y resultar en consecuencias negativas para la entidad, sus clientes / beneficiarios/ funcionarios, contratistas, sus accionistas, la ciudadanía en general y demás partes interesadas.

Los principios mencionados aplican sobre todos los ámbitos del quehacer de la Empresa: operativo, financiero, de proyectos, medioambiental, recursos humanos, salud y seguridad de empleados y contratistas, legal y en temas relacionados con la comunidad, de reputación y sociales.

Por ende, la entidad cuenta con la presente política orientada a gestionar de manera integral los riesgos. Para estos efectos, se deben establecer los objetivos estratégicos, el análisis de alto nivel de los riesgos estratégicos que pueden afectarlos y la asignación de recursos para una adecuada ejecución de las acciones de mitigación según la naturaleza, complejidad y las actividades de la Empresa.

La línea estratégica tiene la responsabilidad de definir el marco general para la administración y el control del riesgo, así como desarrollar y aplicar las políticas y procedimientos necesarios para una adecuada gestión y el control de riesgos. Cada proceso debe aplicar medidas de control o de mitigación que permiten mantener la exposición a un nivel aceptable.

El desarrollo de la política abarcará como mínimo la definición del contexto



estratégico, entendido como el análisis de la situación, tanto interna como externa, que impacta a la organización. La identificación de los riesgos y su valoración, la definición y calificación de controles, el seguimiento permanente de estos y la autoevaluación una vez al año.

La aceptación del riesgo puede ocurrir sin tratamiento del riesgo. Los riesgos aceptados están sujetos a monitoreo. Se debe tener en cuenta que los riesgos de corrupción son inaceptables.

La metodología bajo la cual se desarrollará lo anteriormente expuesto, será la que defina el Departamento Administrativo de la Función Pública en su guía para administración del riesgo, que se encuentre vigente. La entidad adopta e implementa completamente la metodología allí definida, la cual determina los niveles de aceptación o tolerancia al riesgo y fija los niveles para calificar la probabilidad y el impacto en los procesos. La misma se implementará en la herramienta con la que cuenta la entidad para tal fin.

7. INICIATIVAS

Con el fin de que esta política se materialice de manera eficaz, se han definido cuatro grandes iniciativas:

7.1. La política será revisada anualmente y ajustada de ser necesario. La misma será aprobada en el Comité Institucional de Coordinación de Control Interno y socializada a todos los colaboradores de la entidad

7.2. La administración de los riesgos de corrupción, como componente del plan anticorrupción, deberá ser incluido en el plan de acción institucional.

7.3. La definición del mapa de riesgos, así como el seguimiento a las acciones de control, se realizará con el acompañamiento de la Oficina Asesora de Planeación e Información, siendo responsable directamente de esta tarea los



POLÍTICA
DE GESTIÓN
INTEGRAL
DE RIESGOS

CÓDIGO: POL-DEP-004
Documento vigente a partir del:
20/09/2023

VERSIÓN: 7

líderes y gestores de los diferentes procesos, quienes velarán por la participación activa de los

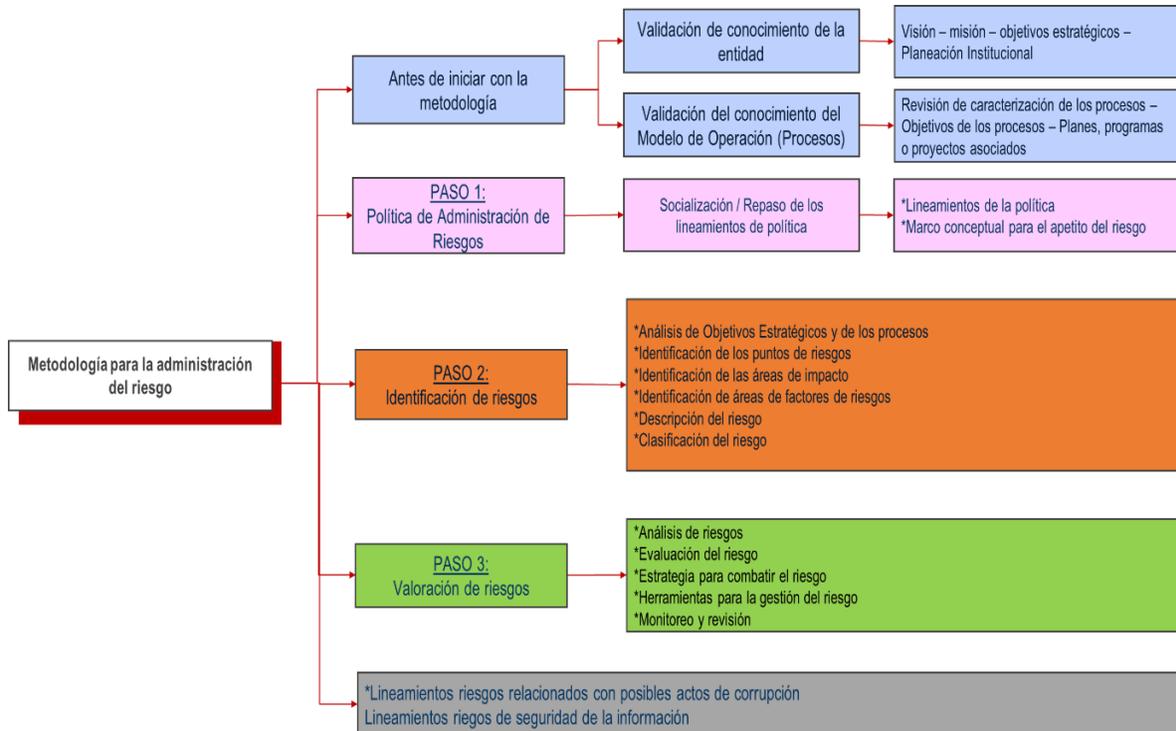
colaboradores que hacen parte de sus equipos. Las brechas que se identifiquen en los controles serán socializadas ante el comité Institucional de Gestión y Desempeño.

8. LINEAMIENTOS METODOLÓGICOS PARA LA ADMINISTRACIÓN DEL RIESGO Y RESPONSABLES

A continuación, se enumeran las acciones que permitirán realizar una adecuada gestión y administración del riesgo; teniendo en cuenta los lineamientos de la “Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas” (DAFP), y del MIPG. Esto último articulado con la política de Planeación Institucional, Política de Seguimiento y Evaluación del Desempeño Institucional y la Política de Control interno, en cumplimiento al decreto 1499 de 2017.

8.1. GESTIÓN DEL RIESGO:

De acuerdo a lo anterior, a continuación, se representa gráficamente el desarrollo de la metodología aplicada en la entidad. La misma ha sido tomada de la Guía mencionada anteriormente, pero con algunos ajustes alineados al lenguaje, dinámica y contexto organizacional.



A CONSIDERAR

Como se ha mencionado, todos los criterios a implementar serán conforme lo establezca la guía del DAFP; sin embargo, se han definido algunos criterios propios de la entidad, los cuales se relacionan a continuación, y deberán ser tenidos en cuenta paralelamente a la implementación de las directrices de la guía en mención.

✓ ANTES DE INICIAR

- Los líderes de proceso deberán definir el grupo de trabajo que se encargará de la identificación, monitoreo, reporte y socialización de los riesgos asociados a sus procesos. Los gestores velarán por la participación del equipo definido.
- La Oficina Asesora de Planeación e Información (OAPI), socializará los cambios que se den en el modelo de operación y en la política, con el fin de garantizar el conocimiento.



- En las mesas de trabajo que se establezcan, en caso de que los procesos así lo requieran, la OAPI socializará la política de Gestión Integral de Riesgos y la metodología a usar durante el ejercicio.

- La OAPI asesorará y acompañará, si el proceso lo requiere, las mesas de trabajo para la identificación del riesgo, realizando un acompañamiento y garantizando la implementación de la metodología establecida. Este acompañamiento irá, hasta el paso No. 3, con al menos uno de los riesgos completamente analizado. Al final, el ejercicio deberá ser concluido por cada proceso y enviado a la OAPI para su revisión y retroalimentación

✓ **PASO 2**

- Previo a la identificación de los riesgos, cada proceso realizará la autoevaluación de su mapa vigente. Autoevaluar es el ejercicio que corresponde a validar el nivel de cumplimiento de los controles establecidos para los riesgos que se encuentren vigentes, así como validar si los mismos se han materializado y que acciones se emprendieron de ser afirmativa la respuesta.

- La OAPI indagará sobre el cumplimiento del plan de contingencia (corrección) y de las acciones correctivas documentadas, en caso de haberse materializado alguno de los riesgos, conforme lo establece esta política. En caso de conocerse la materialización, solo hasta el momento de la autoevaluación, será documentada la acción correctiva correspondiente de manera inmediata, en caso de que el proceso no cuente con evidencias de las acciones de contingencia llevadas a cabo.

- Los riesgos que se encuentren en nivel de aceptación BAJO, que soporten documentación de sus controles en sus procedimientos y evidencien



implementación de sus controles existentes y no presenten materialización durante la vigencia, no requerirán nuevos planes de acción, pero serán monitoreados en la periodicidad definida

- El análisis de contexto será orientado por la OAPI, y la metodología definida para tal fin es la del DOFA. Producto de este ejercicio, la OAPI presentará DOFA institucional a la alta dirección, para su análisis e implementación de estrategias e iniciativas en el marco de la planeación estratégica, programas, planes o proyectos. Este DOFA será actualizado cada cuatro años, o antes, si la dinámica propia del entorno de la entidad, lo hace necesario.

- Para la identificación de riesgos y su redacción, la OAPI orientará sobre las técnicas que se encuentren vigentes, según lineamientos o directrices que se sugieran en la Guía del DAFP, anexos y/u otros documentos de estudio, todo encaminado a que la redacción de riesgos sea estandarizada a nivel institucional y busque por sí sola explicar el alcance del riesgo.

- Para la identificación de causas, se implementará la técnica de los 3 porqués, orientado a identificar la causa raíz.

✓ PASO 3

- Para el análisis preliminar (Riesgo Inherente), la OAPI asesorará sobre la implementación de la metodología acá definida. Así mismo capacitará sobre las técnicas para la calificación de la probabilidad y del impacto.

- Los niveles para calificar el impacto y la probabilidad, corresponden a los que establezca la guía para la administración del riesgo, emitida por el DAFP, y que se encuentre vigente.

- En cuanto análisis y evaluación de controles, la OAPI será quien socialice las técnicas de redacción y de valoración de los controles, que permitirán de manera efectiva evaluar su eficacia y por ende establecer el riesgo residual.



POLÍTICA
DE GESTIÓN
INTEGRAL
DE RIESGOS

CÓDIGO: POL-DEP-004
Documento vigente a partir del:
20/09/2023

VERSIÓN: 7

- Concluido el ejercicio por cada proceso, la OAPI consolidará el mapa institucional y lo cargará en la herramienta de monitoreo, revisión y seguimiento que tenga definida la entidad para tal fin.
- La OAPI presentará al Comité Institucional de gestión y desempeño, el mapa de riesgos consolidado, una vez se encuentre aprobado por los líderes de proceso, así como las acciones para abordar riesgos definidos.

Monitoreo:

- En concordancia con la cultura del autocontrol al interior de la entidad, los gestores de los procesos junto con su equipo realizarán seguimiento y evaluación permanente al Mapa de Riesgos de su respectivo proceso. Así mismo, cada responsable según el rol definido en esta política, realizará el monitoreo y revisión que corresponda.

Seguimiento:

- Según la periodicidad definida para cada acción encaminada a abordar riesgos, el gestor de proceso deberá verificar el seguimiento a las mismas junto con la evidencia, en el sistema definido para tal fin. Se deberá tener en cuenta la fecha Inicio y fecha fin establecida para su implementación.
- Los gestores de proceso y responsable de las acciones, deberán analizar los resultados del seguimiento y establecer acciones inmediatas ante cualquier desviación; la misma deberá ser comunicada al líder del proceso, según el nivel de aceptación del riesgo
- El responsable de la acción deberá documentar las acciones de corrección
- Cuando se modifique las acciones o ubicación del riesgo, se deberá revisar y actualizar el mapa de riesgos del proceso, para lo cual se deberá informar a la OAPI, quien validará los ajustes a realizar.



- El jefe de la Oficina de Control Interno, es el encargado de verificar y evaluar la elaboración, la visibilización, el seguimiento y el control del Mapa de Riesgos institucional, el cual deberá incluir los riesgos de corrupción. El seguimiento se realizatres (3) veces al año, así:

Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación del informe deberá surtirse dentro de los diez (10) primeros días del mes de mayo.

Segundo seguimiento: Con corte al 31 de agosto. La publicación del informe deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.

Tercer seguimiento: Con corte al 31 de diciembre. La publicación del informe deberá surtirse dentro de los diez (10) primeros días hábiles del mes de enero.

8.2. NIVELES DE ACEPTACIÓN DEL RIESGO (APETITO DEL RIESGO)

Acorde con los riesgos residuales aprobados por los líderes de cada proceso, se deberá definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados.

El nivel de aceptación adoptado en la entidad, dependerá del enfoque y de la zona de riesgo residual, es así que Artesanías de Colombia S.A. - BIC ha determinado que para los riesgos residuales de gestión y seguridad digital que se encuentren en zona de riesgo baja, está dispuesta a aceptar el riesgo y no se requiere la documentación de planes de acción, sin embargo, se deben monitorear conforme a la periodicidad establecida.

Para los riesgos de corrupción no hay aceptación del riesgo, siempre deben conducir a formular acciones de fortalecimiento

Para definir el tratamiento del riesgo, las acciones a seguir, según el nivel de



aceptación son:

✓ **ACEPTAR**

No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado). El riesgo se administra por medio de las actividades propias del proyecto o proceso asociado y se realiza en el reporte anual de su desempeño.

✓ **REDUCIR**

Se establecen acciones “para abordar riesgos” o acciones para fortalecer o mejorar los controles existentes, según su calificación, que permitan REDUCIR la probabilidad de ocurrencia o impacto del riesgo, o ambos. Se hace seguimiento SEMESTRAL y se registra sus avances en el Módulo de riesgos del sistema definido para tal fin.

✓ **EVITAR**

Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca y se establecen acciones “para abordar riesgos” que permitan MITIGAR la materialización del riesgo. Se monitorea TRIMESTRALMENTE y se registra sus avances en el Módulo de riesgos del sistema definido para tal fin.

✓ **COMPARTIR O TRANSFERIR**

Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Se establecen acciones “para abordar riesgos” o acciones para fortalecer o mejorar los controles existentes, según su calificación, las cuales pueden ser asumidas y compartidas con otros procesos.

Antes de su documentación, las mismas deberán ser aceptadas por el

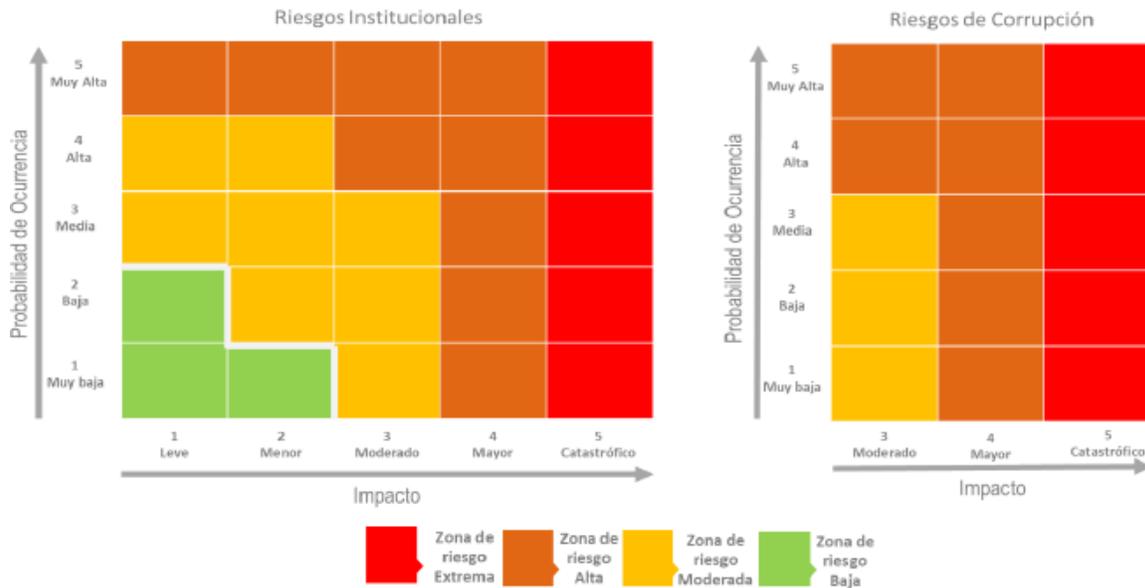
proceso que la recibirá. Se monitorea TRIMESTRALMENTE y se registra sus avances en el Módulo de riesgos del sistema definido para tal fin.

En la entidad la parametrización aprobada es como se muestra a continuación.

Se podrá optar por más de una:

TIPO DE RIESGO	ZONA DE RIESGO	NIVEL DE ACEPTACIÓN
GESTIÓN / SEGURIDAD DIGITAL / FISCAL (Institucionales)	Baja	<ul style="list-style-type: none"> • ACEPTAR
	Moderada	<ul style="list-style-type: none"> • REDUCIR
	Alta	<ul style="list-style-type: none"> • EVITAR • REDUCIR • COMPARTIR O TRANSFERIR
	Extrema	<ul style="list-style-type: none"> • EVITAR • COMPARTIR O TRANSFERIR
CORRUPCION	Baja	Ningún riesgo de corrupción podrá ser aceptado
	Moderada	<ul style="list-style-type: none"> • REDUCIR
	Alta	<ul style="list-style-type: none"> • EVITAR • REDUCIR • COMPARTIR O TRANSFERIR
	Extrema	<ul style="list-style-type: none"> • EVITAR • REDUCIR • COMPARTIR O TRANSFERIR

**Matriz de calificación del nivel de severidad del riesgo de gestión,
seguridad digital, riesgos de corrupción y fiscal**



Los niveles de aceptación definidos en la entidad se encuentran parametrizados en el módulo de riesgos del software que administra el sistema de gestión de calidad.

8.3. NIVEL DE CALIFICACIÓN DE PROBABILIDAD Y SEVERIDAD

8.3.1. Riesgos de gestión y seguridad digital

Teniendo en cuenta los lineamientos metodológicos de la guía para la Administración del riesgo y diseño de controles entidades públicas – DAFP, la entidad adopta la calificación de la frecuencia, con base en la exposición al riesgo asociado al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Los criterios para definir el nivel de probabilidad son:

Nivel	Probabilidad	Descripción
5	Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año
4	Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año
3	Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año
2	Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
1	Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año

En cuanto a la severidad o impacto se tendrá en cuenta para su análisis los siguientes criterios:

Nivel	Impacto	Afectación económica	Afectación reputacional
5	Catastrófico	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país
4	Mayor	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o
3	Moderado	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
2	Menor	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o
1	Leve	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización

8.3.1. Riesgos de corrupción

Para los riesgos de corrupción la probabilidad será validada por factibilidad o frecuencia, considerando los siguientes criterios:

Nivel	Descriptor	Factibilidad	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos una vez en el último año
3	Posible	El evento podrá ocurrir en algún momento	Al menos una vez en los últimos 2 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos una vez en los últimos 5 años
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años

Y el nivel de severidad, obedecerá al número de preguntas afirmativas en el siguiente cuestionario:

Nº	PREGUNTA: SI EL RIESGO DE CORRUPCION SE MATERIALIZA PODRÍA...
1	¿Afectar al grupo de funcionarios del proceso?
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?
3	¿Afectar el cumplimiento de la misión de la Entidad?
4	¿Afectar el cumplimiento de la misión del Sector Salud y Protección Social?
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?
6	¿Generar pérdida de recursos económicos?
7	¿Afectar la generación de los productos o la prestación de servicios?
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?
9	¿Generar pérdida de la información de la Entidad?
10	¿Generar intervención de los Organos de Control, de la Fiscalía, u otro ente?
11	¿Dar lugar a procesos sancionatorios?
12	¿Dar lugar a procesos disciplinarios?
13	¿Dar lugar a procesos fiscales?
14	¿Dar lugar a procesos penales?



POLÍTICA
DE GESTIÓN
INTEGRAL
DE RIESGOS

CÓDIGO: POL-DEP-004
Documento vigente a partir del:
20/09/2023

VERSIÓN: 7

15	¿Generar pérdida de credibilidad del sector?
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?
17	¿Afectar la imagen regional?
18	¿Afectar la imagen nacional?
19	¿Generar daño ambiental?

- Responder afirmativamente de UNA a CINCO preguntas= Impacto moderado (medianas consecuencias)
- Responder afirmativamente de SEIS a ONCE preguntas= Impacto mayor (altas consecuencias)
- Responder afirmativamente de DOCE a DIECINUEVE = Impacto catastrófico (Consecuencias catastróficas para la entidad)

8.3.2. Riesgo Fiscal

La gestión del riesgo fiscal debe vincularse al análisis general de los riesgos institucionales, a fin de contar con un esquema integral que facilite su seguimiento por parte de los líderes del proceso.

Para la identificación del riesgo es necesario establecer los puntos de riesgo fiscal y las circunstancias inmediatas.

Para redactar un riesgo fiscal se debe tener en cuenta:

- Iniciar con la oración: *Posibilidad de*
- Impacto: *Corresponde al qué*
- Circunstancia Inmediata: *Corresponde al cómo*
- Causa Raíz: *Corresponde al por qué*

La probabilidad es la posibilidad de ocurrencia del riesgo fiscal, se determina según el número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año:

Nivel	Impacto	Afectación reputacional
5	Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año
4	Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año
3	Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año
2	Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
1	Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año

Considerando la naturaleza y alcance del riesgo fiscal, este siempre tendrá un impacto económico, toda vez que el efecto dañoso ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública.

El impacto tiene diferentes niveles:

Nivel	Impacto	Afectación económica	Afectación reputacional
5	Catastrófico	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.
4	Mayor	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
3	Moderado	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
2	Menor	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o proveedores.
1	Leve	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos teniendo en cuenta las siguientes tipologías de controles:

- Control Preventivo: Busca establecer las condiciones que aseguren atacar la causa raíz y así evitar que el riesgo se concrete.
- Control Detectivo: Este control detectan el riesgo fiscal, pero generan reprocesos.
- Control Correctivo: Estos controles tienen costos implícitos.

8.4. LINEAMIENTOS EN CASO DE MATERIALIZACIÓN

TIPO DE RIESGO	RESPONSABLE	ACCION
CORRUPCION	Líder del proceso	<ul style="list-style-type: none"> • Informar al gestor del Proceso de Direccionamiento y Estratégico y Planeación (DEP) y a la OCI sobre el hecho encontrado. • Documentar la situación como una no conformidad “Riesgo Materializado” en el módulo de mejora del programa que administra el Sistema de Gestión de Calidad.



		<ul style="list-style-type: none">• Efectuar el análisis de causas y determinar acciones correctivas a las que haya lugar.• Actualizar el mapa de riesgos.
	Oficina Asesora de Planeación e información	<ul style="list-style-type: none">• Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente.• Informar al Líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar.• Informar a la segunda línea de defensa con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos.



GESTIÓN / ESTRATÉGICO	Líder del proceso	<ul style="list-style-type: none">• Proceder de manera inmediata a aplicar el plan de contingencia que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso). Este corresponderá a la sección de tratamiento, de la No Conformidad de Tipo “Riesgo materializado” que se encuentra en el aplicativo que administra el sistema de gestión de Calidad.• Realizar el análisis de causas y determinar acciones correctivas a implementar, documentar y replantear los riesgos del proceso.• Informar a la OCI, para validar que las acciones sean pertinentes para resolver el hecho• Informar al Proceso de Direccionamiento Estratégico sobre el hallazgo y las acciones tomadas.• Analizar y actualizar el mapa de riesgos, con la asesoría de OAPI.
	Oficina de Control Interno	<ul style="list-style-type: none">• Realizar seguimiento desde su rol.

8.5. ROLES / RESPONSABILIDADES:

LÍNEA DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
Estratégica	Alta Dirección – Comité Institucional de Coordinación de Control Interno	<ul style="list-style-type: none"> • Establecer y aprobar la Política de Gestión Integral de Riesgos, la que incluye la aprobación de los niveles de responsabilidad y autoridad con énfasis en la prevención del daño antijurídico. • Revisar la política de administración del riesgo por lo menos una vez al año para su actualización y validar su eficacia a la gestión del riesgo institucional. Se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta. Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo). Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles, y definir las estrategias, iniciativas o acciones a emprender de acuerdo al análisis realizado. • Realizar seguimiento y análisis periódico a los riesgos institucionales. Retroalimentar al Comité de Gestión y Desempeño Institucional sobre los ajustes



POLÍTICA
DE GESTIÓN
INTEGRAL
DE RIESGOS

CÓDIGO: POL-DEP-004
Documento vigente a partir del:
20/09/2023

VERSIÓN: 7

		<p>que se deban hacer frente a la gestión del riesgo y frente a las estrategias definidas a implementar de acuerdo al análisis del contexto interno y externo.</p> <ul style="list-style-type: none"> • Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del mismo.
<p>Primera línea</p>	<p>Gerentes Públicos- líderes de proceso Gestores de proceso (En general servidores públicos en todos los niveles de la organización)</p>	<ul style="list-style-type: none"> • Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera con énfasis en la prevención del daño antijurídico. • Aprobar y hacer seguimiento a los controles, propuesto por su equipo, para mitigar los riesgos identificados alineado con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • Desarrollar ejercicios de



POLÍTICA
DE GESTIÓN
INTEGRAL
DE RIESGOS

CÓDIGO: POL-DEP-004
Documento vigente a partir del:
20/09/2023

VERSIÓN: 7

		<p>autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.</p> <ul style="list-style-type: none"> • Informar a la OAPI (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo. • Reportar los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado.
Segunda Línea	<p>-Jefe Oficina Asesora de Planeación e Información</p> <p>-Comités de la Entidad (Gestión y Desempeño, contratación, de inventarios, de conciliación, grupo disciplinario, de convivencia)</p> <p>Personal</p>	<ul style="list-style-type: none"> • Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. • Consolidar el Mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos). • Acompañar, orientar y entrenar a los líderes y gestores de procesos en la identificación, análisis y valoración del riesgo. • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes, gestores de procesos y o responsables directos de las acciones para abordar riesgos.



	<p>(funcionarios) del área financiera Personal del área Tics Supervisores de contratos</p>	<ul style="list-style-type: none">• Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalúe y gestione los riesgos y controles para que se generen acciones.• Evaluar que los riesgos sean consistentes con la presente política de la entidad y que sean monitoreados por la primera línea de defensa.• Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.• Identificar cambios en el apetito del riesgo (niveles de aceptación) en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlo para aprobación del comité institucional de coordinación de control interno.• Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios.• Garantizar el cumplimiento de los planes de la entidad.
--	--	--



POLÍTICA
DE GESTIÓN
INTEGRAL
DE RIESGOS

CÓDIGO: POL-DEP-004
Documento vigente a partir del:
20/09/2023

VERSIÓN: 7

		<ul style="list-style-type: none">• Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información (TICS).• Definir el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control.• Generar recomendaciones de mejoras a la política de operación para la gestión integral del riesgo.
Tercera línea	Oficina de Control Interno	<ul style="list-style-type: none">• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.• Asesorar de forma coordinada con la Oficina Asesora de Planeación e Información, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles.• Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoría y reportar los resultados al CICCI.• Recomendar mejoras a la política de gestión integral del riesgo.



POLÍTICA
DE GESTIÓN
INTEGRAL
DE RIESGOS

CÓDIGO: POL-DEP-004
Documento vigente a partir del:
20/09/2023

VERSIÓN: 7

9. SEGUIMIENTO Y EVALUACIÓN DE LA POLÍTICA.

Como las demás políticas institucionales, esta será validada y actualizada, de ser requerido, de manera anual, teniendo en cuenta los lineamientos normativos, la dinámica propia de la organización y los resultados obtenidos en cada vigencia.

El cumplimiento de la política es garantizado desde la Oficina Asesora de Planeación e Información, validando la implementación de las acciones y estrategias. Así mismo la evaluación será realizada por la Oficina de Control interno.

Como parte del seguimiento se deberán diseñar mecanismos que permitan fortalecer la cultura de autocontrol, y así mejorar continuamente la gestión del riesgo.

10. NATURALEZA DEL CAMBIO

Versión	Fecha	Naturaleza del cambio
4	30/Sep./2019	Se cambió la versión por ajuste del nombre del proceso DEP
5	6/Nov/2020	Se ajustó el objetivo general, ampliando su definición, se incluyó un nuevo objetivo específico. Se amplió el alcance de la política, fueron ajustadas las estrategias alineadas a la dinámica actual de la entidad. Capítulo 8. Fue modificado completamente: Cambio su nombre con el fin de incluir toda la metodología adaptada al contexto organizacional. Así mismo fueron incluidos los niveles de aceptación de riesgo para ADC, se estableció la fuente para identificar los niveles para clasificar el impacto. Se estableció el tratamiento y accionar en caso de materialización de riesgos. Fueron ajustados los roles y responsabilidades, alineado al modelo de líneas de defensa.
6	23/sept/2022	Se revisó y actualizó: definiciones y el modelo de desarrollo de la metodología. Así mismo se ajustaron los lineamientos en cuanto a calificación de probabilidad e impacto, explicación y ajuste al nivel de aceptación, acorde a la nueva metodología de administración de riesgos – DAFP



POLÍTICA
DE GESTIÓN
INTEGRAL
DE RIESGOS

CÓDIGO: POL-DEP-004
Documento vigente a partir del:
20/09/2023

VERSIÓN: 7

7	14/sept/2023	<p>Se agregaron dos definiciones nuevas. Así mismo se incluyó el lineamiento en cuanto a la probabilidad e impacto y las tipologías de controles en todo lo referente a Riesgo Fiscal, de acuerdo al capítulo específico que presenta la Guía Administración de Riesgos – DAFFP.</p> <p>Se realizó cambio de uno de los responsables en lo referente al lineamiento, en caso de materialización del riesgo de corrupción.</p> <p>Se mejoró la redacción del responsable Oficina de Control Interno en el tipo de riesgo Gestión/ Estratégico.</p>
---	--------------	---

Elaboró	Revisó	Aprobó
<p>Nombre: Gimena Avila Pineda</p> <p>Cargo: Profesional OAPI</p> <p>Fecha: septiembre 18 de 2023</p>	<p>Nombre: Dora Alba Ortiz Gaviria</p> <p>Cargo: Jefe Oficina de Control interno</p> <p>fecha: septiembre 19 de 2023</p>	<p>Comité Institucional de Coordinación de Control Interno - CICCI</p> <p>Acta N° 84</p> <p>Fecha: septiembre 20 de 2023</p>