ALCALDÍA MAYOR DE BOGOTÁ D.C.

DEPARTAMENTO ADMINISTRATIVO DE LA DEFENSORÍA DEL ESPACIO PÚBLICO

BOGOTÁ

Código SG/MIPG	127-PPPVM-02
Vigencia desde	24/08/2022
Versión	2

Política de Administración del Riesgo

Proceso

VERIFICACIÓN Y MEJORAMIENTO CONTINUO

Tabla de Contenido

1. Introducción

Para el Departamento Administrativo de la Defensoría del Espacio Público – DADEP- es un compromiso desde la gestión y el cumplimiento de resultados, lograr sus objetivos estratégicos, planes, proyectos y procesos institucionales a través de la realización de acciones soportadas en la prevención de los riesgos, implementando controles que promuevan la generación de comportamientos éticos que conlleven a la construcción de una cultura de buen gobierno, que impida la materialización de riesgos de gestión, corrupción y seguridad de la información.

Es así, como el DADEP, de acuerdo con la normatividad vigente y la metodología establecida por el Departamento Administrativo de la Función Pública, diseña la *política de gestión de riesgos* como mecanismo para fortalecer el control en los procesos que respondan, a los acontecimientos potenciales o aquellos en los que puedan desencadenar situaciones de riesgo de gestión, corrupción o seguridad de la información, en concordancia con las directrices en materia de gestión pública y el enfoque del Modelo Integrado de Planeación y Gestión- MIPG.

2. Términos y Definiciones

Accesibilidad: Acceso universal a la Web, independientemente del tipo de hardware, software, infraestructura de red, idioma, cultura, localización geográfica y capacidades de los usuarios (W3C World Wide Web Consortium). En el contexto colombiano, ha venido asumiéndose como las condiciones que se incorporan en sitios y herramientas web que favorecen el que usuarios en condiciones de deficiencia tecnológica, física o sensorial o en condiciones particulares de entornos difíciles o no apropiados, puedan hacer uso de estos recursos de la Web[1].

Aceptación de riesgo: Decisión generada por la entidad de aceptar las consecuencias y probabilidad de un riesgo en particular, sin adelantar acciones de reducción y control. La aceptación del riesgo también se deriva del nivel de riesgo o umbral en el cual el Departamento Administrativo de la Defensoría del Espacio Público acepta el riesgo.

Actitud (apetito) hacia el riesgo: Enfoque de la organización para evaluar y eventualmente buscar, retener, tomar o alejarse del riesgo.[2]

Activo: En el contexto de Seguridad de la Información 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.

[1] MinTic. Glosario: Página Web https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html. Actualizada el: 16 de octubre de 2018
[2] ICONTEC. NTC-ISO 31000: Norma técnica Gestión del riesgo Principios y Directrices. Numeral 2: Términos y definiciones Bogotá,2011 Página 5.

Activos de información: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización.

Administración de riesgos: Proceso efectuado por la Alta Dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación. (INTOSAI, 2000).

Amenaza informática: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.[3]

Amenaza: Causa Potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o una organización.[4]

Análisis cualitativo: Herramienta subjetiva que estandariza la evaluación de la probabilidad de ocurrencia y el impacto de los riesgos facilitando su evaluación y posibilidad de priorizarlos.

Análisis de riesgo: Uso sistemático de la información para identificar las fuentes y estimar el riesgo NTC-ISO /IEC 27001.

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.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

[3] Glosario del Mintic. Página Web https://www.mintic.gov.co/portal/604/w3-propertyvlue-1051.html.
[4] Guía para la administración de los riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas Agosto-2018 V2. Página 9.

Comunicación y Consulta: Procesos continuos y reiterativos que una organización lleva a cabo para suministrar, compartir u obtener información e involucrarse en un diálogo con las partes interesadas, con respecto a la gestión del riesgo[5].

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Consecuencia o impacto: Efectos generados por la ocurrencia de un riesgo que afecta los objetivos o un proceso de la entidad. Pueden ser entre otros, una pérdida, un daño, un perjuicio, un detrimento[6].
Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Medida que modifica al riesgo **(**Procesos, Política, dispositivos, prácticas u otras acciones**)**.[7]
Control: Medida que permite reducir o mitigar un riesgo.

Corrupción: Uso del poder para desviar la gestión de lo público hacia el beneficio privado.

Criterios para la evaluación de riesgos: Términos de referencia o parámetros con base en los cuales se evalúa la importancia de un riesgo. Los criterios para la evaluación del riesgo los establece la organización de acuerdo con sus necesidades y objetivos.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Evento: Presencia o cambio de un conjunto particular de circunstancias.[8] Dependiendo de las consecuencias o impactos que el evento pueda tener, se habla de que se materializa el riesgo para las situaciones en las cuales las consecuencias son negativas y se materializan las oportunidades cuando las consecuencias o impactos son positivos.
Factores de Riesgo: Son las fuentes generadoras de riesgos.

Identificación del riesgo. Proceso para encontrar, reconocer y describir el riesgo.[9]

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

Integridad: Propiedad de exactitud y completitud.

Mapa de riesgos: Es una herramienta, basada en los distintos sistemas de información, que pretende identificar las actividades o procesos sujetos a riesgo, cuantificar la probabilidad de estos eventos y medir el daño potencial asociado a su ocurrencia[10].

[5] ICONTEC. NTC31000:2011. Gestión del Riesgo. Términos y Definiciones. Numeral 2.12 Bogotá, 2011. Página 4.
[6] Función Pública. Manual Técnico del Modelo Estándar de Control Interno para el Estado Colombiano -MECI- 2014. Página 64.
[7] Guía para la administración de los riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas Agosto-2018 V2. Página 9.
[8] ICONTEC. NTC-ISO 31000: Norma técnica Gestión del riesgo Principios y Directrices. Numeral 2: Términos y definiciones Bogotá, 2011 Página 21.
[9] ICONTEC. NTC-ISO 31000: Norma técnica Gestión del riesgo Principios y Directrices. Numeral 2: Términos y definiciones Bogotá, 2011 Página 6.
[10] Atlantic Review of Economics – 2nd Volume – 2013. Resumen. Página 2

Nivel de 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 poder 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. Magnitud del riesgo, expresada en términos de la combinación de la probabilidad y las consecuencias o impacto que este tiene.

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Política para la gestión del riesgo: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.[11]

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.

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.

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de trámites y otros procedimientos administrativos OPAs: Son los riesgos de corrupción asociados a trámites y OPA que se opera en Bogotá, teniendo en cuenta el universo de trámites distritales. En el caso de las entidades que realizan la identificación, la mayoría de ellas la hace de manera general asociada a la prestación de todos los trámites y servicios de la entidad, y no particular, es decir, considerando las características de cada uno de estos, sus relaciones con los grupos de valor y las debilidades del proceso que generan riesgos.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

[11] Norma Técnica Colombiana. NTC-ISO 31000: Gestión del riesgo Principios y Directrices. Página 5.

Riesgo del Sistema de Administración de Riesgo de Lavado de Activos y de la Financiación del Terrorismo – SARLAFT: Es el Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo, está compuesto por dos componentes. El componente de prevención del riesgo y el componente de control. La **prevención de riesgos** como su nombre lo indica, trata de prevenir que las entidades vigiladas sean utilizadas para dar apariencia de legalidad a recursos provenientes de actividades delictivas o, para la canalización de recursos hacia la realización de actividades terroristas. **El componente de control** es utilizado para detectar las operaciones que se pretendan realizar o se hayan realizado; durante este proceso se aplican medidas tanto preventivas como correctivas, con el fin de establecer los procedimientos del SARLAFT.

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.

Tolerancia del 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.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

Tratamiento del riesgo: Proceso para modificar el riesgo. El tratamiento del riesgo puede implicar: Evitar el riesgo decidiendo no iniciar o continuar la actividad que lo originó, tomar o incrementar el riesgo con el fin de perseguir una oportunidad, retirar la fuente del riesgo, cambiar la probabilidad, cambiar las consecuencias, compartir el riesgo con una o varias de las partes (incluyendo los contratos y la financiación del riesgo) y retener el riesgo a través de la decisión informada. En ocasiones se hace referencia a los tratamientos del riesgo relacionados con consecuencias negativas como "mitigación del riesgo", "eliminación del riesgo", "prevención del riesgo" y "reducción del riesgo". El tratamiento del riesgo puede crear riesgos nuevos o modificar los existentes.[12]

Valoración del riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.[13]

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.[14]

[12] ICONTEC. NTC-ISO 31000: Norma técnica Gestión del riesgo Principios y Directrices. Numeral 2: Términos y definiciones Bogotá, 2011 Página 8.
[13]ICONTEC. NTC-ISO 31000: Norma técnica Gestión del riesgo Principios y Directrices. Numeral 2: Términos y definiciones Bogotá, 2011 Página 6.
[14] Guía para la administración del riesgo y el diseño de controles en entidades públicas Octubre-2020 V5. Página 12 y 13.

3. Política de Administración del Riesgo

El Departamento Administrativo de la Defensoría del Espacio Público se compromete a administrar adecuadamente los riesgos de gestión, de corrupción, de seguridad de la información, de lavado de activos y financiación del terrorismo, asociados a los objetivos estratégicos, planes, proyectos y procesos institucionales, tramites y otros procedimientos administrativos (OPAs), considerando la metodología propia para su gestión, determinando los controles preventivos y detectivos oportunamente para evitar la materialización y la acción correctiva inmediata ante los eventos presentados, buscando con esto aceptar, reducir y evitar el riesgo, ante su posible materialización y consecuencias a fin de mantener los niveles de riesgo aceptables.

4. Objetivos de la Política de Administración de Riesgos

4.1 Objetivo General de la Política de Administración de Riesgos del DADEP

Administrar los riesgos en el Departamento Administrativo de la Defensoría del Espacio Público - DADEP, los cuales harán énfasis en el fortalecimiento de los controles internos, con el fin de minimizar la probabilidad de materialización de cualquier tipo de riesgo que afecten el logro de las metas del Departamento.

4.2 Objetivo Específicos

- Generar una visión sistémica de la administración, control y evaluación de los riesgos de la Entidad.
- Proteger los recursos de la entidad, resguardándolos contra la materialización de los riesgos valorados como amenazas de corrupción.
- Introducir y fortalecer dentro de los procesos y procedimientos puntos de control, que permitan evitar, reducir o mitigar, las vulnerabilidades o potenciales amenazas que se puedan presentar.
- Mejorar el aprendizaje organizacional frente a la eficaz identificación y administración de los riesgos.

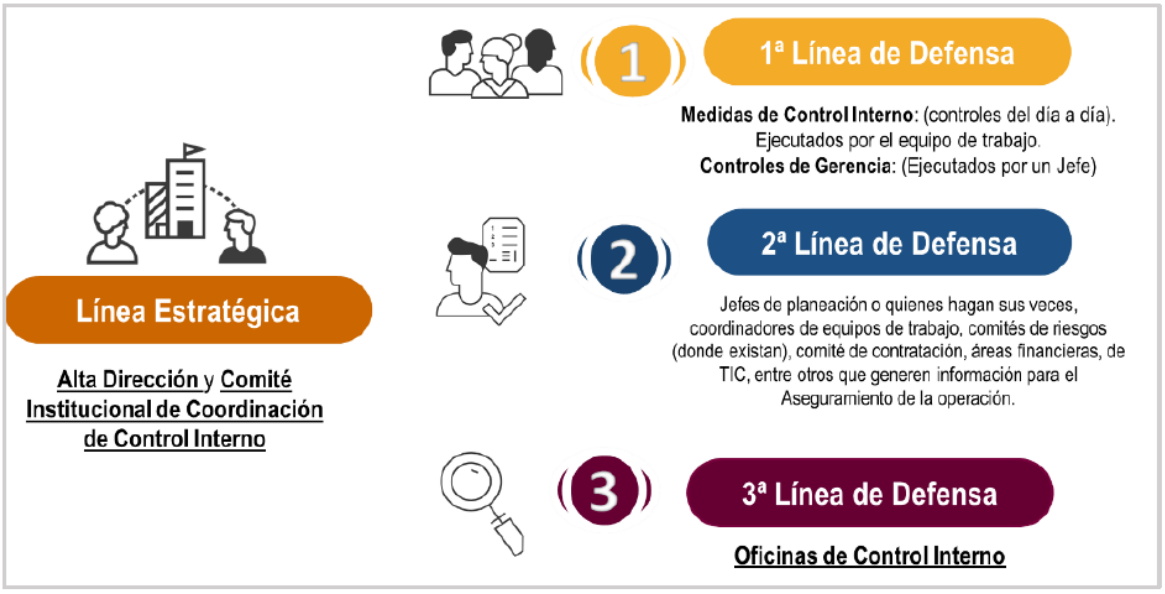
5. Alcance de la Política de Administración de Riesgos

La presente política aplica para todos y cada uno de los procesos institucionales, y los controles serán aplicados por todos los servidores públicos y contratistas del Departamento.

6. Roles y Responsabilidades en la Gestión del Riesgos

Con el fin de asegurar que las responsabilidades y autoridades para la gestión del riesgo se asignen y comuniquen a los roles pertinentes, el Departamento Administrativo de la Defensoría del Espacio Público determina las siguientes responsabilidades en relación con las líneas de defensa establecidas en el Modelo Integrado de Planeación y gestión MIPG:

Ilustración 1. Las Líneas de Defensa en el Modelo Estándar de Control Interno



Fuente: Manual Operativo del MIPG del DAFP 2019 V3.

Línea Estratégica	
Responsables	Equipo Directivo, Comité Institucional de Gestión y Desempeño; y el Comité Institucional de Coordinación de Control Interno.
Política, Identificación y Valoración del Riesgo	
Responsabilidades	• Definir y aprobar el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. • 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. • Definir y aprobar la política para la administración del riesgo. • Garantizar el cumplimiento de los planes de la entidad.
Actividades a Realizar	
– Establecer la política de gestión de riesgos de la entidad. – Definir los niveles de aceptación de riesgos. – Establecer la periodicidad del monitoreo y seguimiento. – Supervisar el cumplimiento de cada una de las etapas de la gestión de riesgos. – Revisar los cambios en el Direccionamiento Estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los existentes. – Revisar los planes de acción establecidos en los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar la posible repetición del evento.	
Comunicación y Consulta	
Corresponde al Comité Institucional de Coordinación de Control Interno establecer la Política de Gestión de Riesgos y asegurarse de su permeabilización en todos los niveles de la organización pública, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.	
Accionar Ante la Materialización del Riesgo de Corrupción	
Revisar los planes de acción establecidos en los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar la posible repetición del evento.	

Primera Línea de Defensa	
Responsables	Líderes de Proceso y Responsable de Proyecto
Política, Identificación y Valoración del Riesgo	
Responsabilidades	• Desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. • Orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro. • Informar a la Oficina Asesora de Planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo. • Asegurar que al interior de su grupo de trabajo se reconozca el concepto de "administración del riesgo", la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa.

Actividades a Realizar
– Delegar, por parte del líder del proceso, el (los) profesionales que se encargarán de la identificación, monitoreo, reporte y socialización del riesgo asociados. – Revisar los cambios en el Direccionamiento estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los existentes. – Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. – Revisar el adecuado diseño y ejecución de los controles establecidos para la mitigación de riesgos. – Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar los posibles riesgos que se están materializando. – Revisar y reportar a planeación, lo eventos de riesgos que se han materializado en la entidad. – Revisar los planes de acción establecidos en los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar la posible repetición del evento. – Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa en relación con la gestión de riesgos. – Reportar los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos.
Comunicación y Consulta
– Asegurarse de implementar la metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades. – Divulgar y sensibilizar al interior de sus dependencias el mapa de riesgos junto con el plan de manejo y políticas de operación que se derivan.
Accionar Ante la Materialización del Riesgo de Corrupción
– Informar al Proceso de Direccionamiento Estratégico sobre el hecho encontrado. – 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. – Proceder de manera inmediata a aplicar el plan de contingencia (si lo hay) que permita la continuidad del servicio o el restablecimiento de este (si es el caso), documental en el Plan de mejoramiento. – Iniciar el análisis de causas y determinar acciones preventivas y de mejora, documentar en el Plan de Mejoramiento Institucional y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos. – Analizar y actualizar los riesgos del proceso.

Segunda Línea de Defensa	
Responsables	Jefe de la Oficina Asesora de planeación, supervisores e interventores de contratos o proyectos.
Política, Identificación y Valoración del Riesgo	
Responsabilidades	• Asegurar que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende. • Monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.
Actividades a Realizar	

– Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos. – Revisar la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar. – Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de estos. – Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad. – Realizar seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos. – Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos. – Realizar el monitoreo a los riesgos en la periodicidad establecida.
Comunicación Y Consulta
– Difundir y asesorar a la primera línea de defensa en la metodología, así como de los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación. – Impulsar a nivel institucional una cultura de gestión del riesgo, a través de capacitaciones, mesas de trabajo y asesorías, con el fin de mejorar el conocimiento y apropiación del enfoque basado en riesgos. – Consolidar el Mapa de Riesgos de la entidad. – Divulgar del Mapa de Riesgos de Corrupción a partes interesadas y comunidad en general a través de su publicación en la página web de la Entidad.
Accionar Ante la Materialización del Riesgo de Corrupción
– Asesorar a la primera línea de defensa en el análisis de causas y la determinar acciones preventivas y de mejora, documentar en el Plan de Mejoramiento Institucional. – Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos. – Actualizar el mapa de riesgos, con la información reportada por la primera línea de defensa.

Tercera Línea de Defensa	
Responsables	Oficina de Control Interno
Política, Identificación Y Valoración Del Riesgo	
Responsabilidades	• Proporcionar información sobre la efectividad de la entidad en la gestión, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa • Proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del S.C.I. • Proporcionar aseguramiento objetivo en los temas identificadas no cubiertas por la segunda línea de defensa.

	• Recomendar mejoras a la política de operación para la administración del riesgo

Actividades a Realizar

- Asesorar a la primera línea de defensa de forma coordinada con la Oficina Asesora de Planeación, en la metodología e identificación de los riesgos y diseño de controles.
- Revisar los cambios en el "Direccionamiento Estratégico" o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.
- Revisión de la adecuada definición de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
- Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción.
- Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos.
- Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.
- Para mitigar los riesgos de los procesos estos se deben encontrar documentados y actualizados en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, se lleven llevar a cabo de manera oportuna, estableciendo la causa raíz del problema y buscando evitarse en lo posible, la repetición de hallazgos y la materialización de los riesgos.

Comunicación y Consulta

- Impulsar a nivel institucional una cultura de gestión del riesgo, a través de capacitaciones, mesas de trabajo y asesorías, con el fin de mejorar el conocimiento y apropiación del enfoque basado en riesgos.
- Informar sobre la efectividad de la entidad en la gestión a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.

Accionar Ante la Materialización del Riesgo de Corrupción

- Informar al líder del proceso sobre el hecho.
- 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.
- Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho.
- Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

7. Alineación de la Política con la Plataforma Estratégica de la Entidad

El Departamento Administrativo de la Defensoría del Espacio Público - DADEP fue creado mediante el Acuerdo del Distrito Capital 018 del 31 de julio de 1999, y tiene como principal función definida en el artículo 3 "Son funciones de la Defensoría del Espacio Público, sin perjuicio de las atribuciones de otras autoridades, la defensa, inspección, vigilancia, regulación y control del espacio público del Distrito Capital; la administración de los bienes inmuebles, y la conformación del inventario general del patrimonio inmobiliario Distrital".

Dentro de su misionalidad, el DADEP ha construido una plataforma estratégica, la cual hace parte integral en la definición de los lineamientos de administración de riesgos descritos en esta política.

7.1 Misión:

Contribuir al mejoramiento de la calidad de vida en Bogotá, por medio de una eficaz defensa del espacio público, de una óptima administración del patrimonio inmobiliario de la ciudad y de la construcción de una nueva cultura del espacio público, que garantice su uso y disfrute colectivo y estimule la participación comunitaria.

7.2 Visión:

En 2024 el Departamento Administrativo de la Defensoría del Espacio Público será una entidad reconocida a nivel distrital y nacional como líder en la protección integral del espacio público y del patrimonio inmobiliario distrital, la gestión del conocimiento urbanístico de los bienes de uso público y fiscales del nivel central de Bogotá, y por promover la participación ciudadana, la corresponsabilidad y la coordinación interinstitucional.

7.3 Objetivos Estratégicos:

- Contribuir al incremento del uso, goce y disfrute del patrimonio inmobiliario distrital y el espacio público, con acceso universal a la ciudadanía.
- Aumentar la oferta cuantitativa, cualitativa y la equidad territorial del patrimonio inmobiliario distrital y el espacio público.
- Mejorar la coordinación interinstitucional con todas las entidades que tienen competencia en materia de espacio público, así como la comunicación con los grupos de interés y de valor.
- Fortalecer la capacidad institucional en el marco del Modelo Integrado de Planeación y Gestión, bajo los enfoques de una gestión orientada a resultados, la eficiencia en el

manejo de recursos, la transparencia, el gobierno abierto y la participación de los grupos de interés.

7.4 Mapa de Procesos:

Por lo tanto, dentro de los aspectos que el DADEP tiene en cuenta para la identificación de los riesgos esta:

Ilustración 2. Conocimiento y análisis de la entidad

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP 2020 V5.

8. Metodología y Normatividad Aplicable

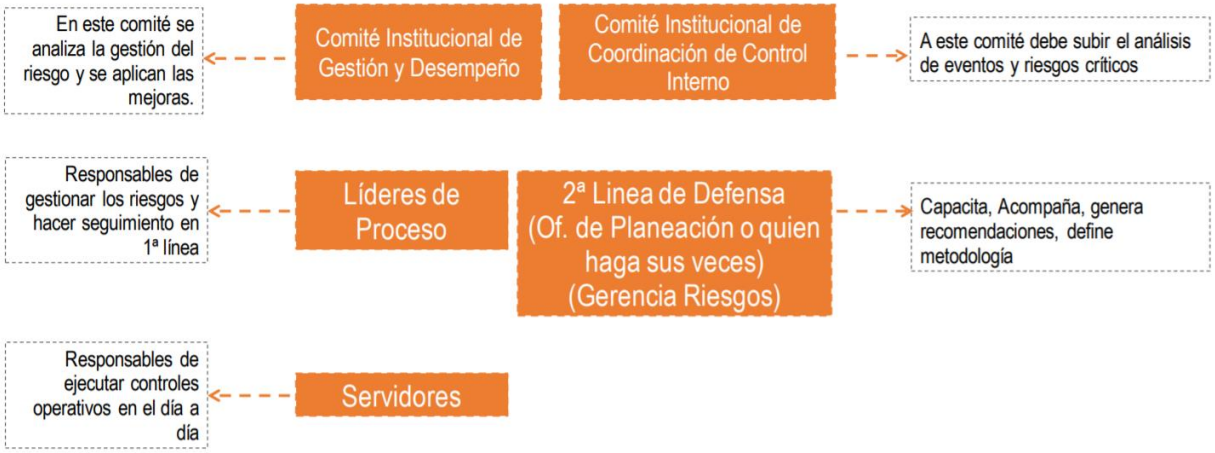
El Departamento Administrativo de la Defensoría del Espacio Público, aplicará la metodología establecida por el Departamento Administrativo de la Función Pública, descrita en la Guía para la administración de los riesgos de Gestión, Corrupción y Seguridad de la Información y el Diseño de Controles en Entidades Públicas.

Así mismo, se aplicarán los lineamientos del Modelo Integrado de Planeación y Gestión MIPG- Según lo contemplado en la normatividad vigente, principalmente el Decreto 1499 de 2017, la Guía para Elaborar el Mapa de Aseguramiento en las Entidades del Distrito de la Secretaria

General y el Decreto Distrital 807 de 2019 "Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital y se dictan otras disposiciones"

El modelo integrado de planeación y gestión (MIPG) define para su para su operación articulada la creación en todas las entidades del Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:

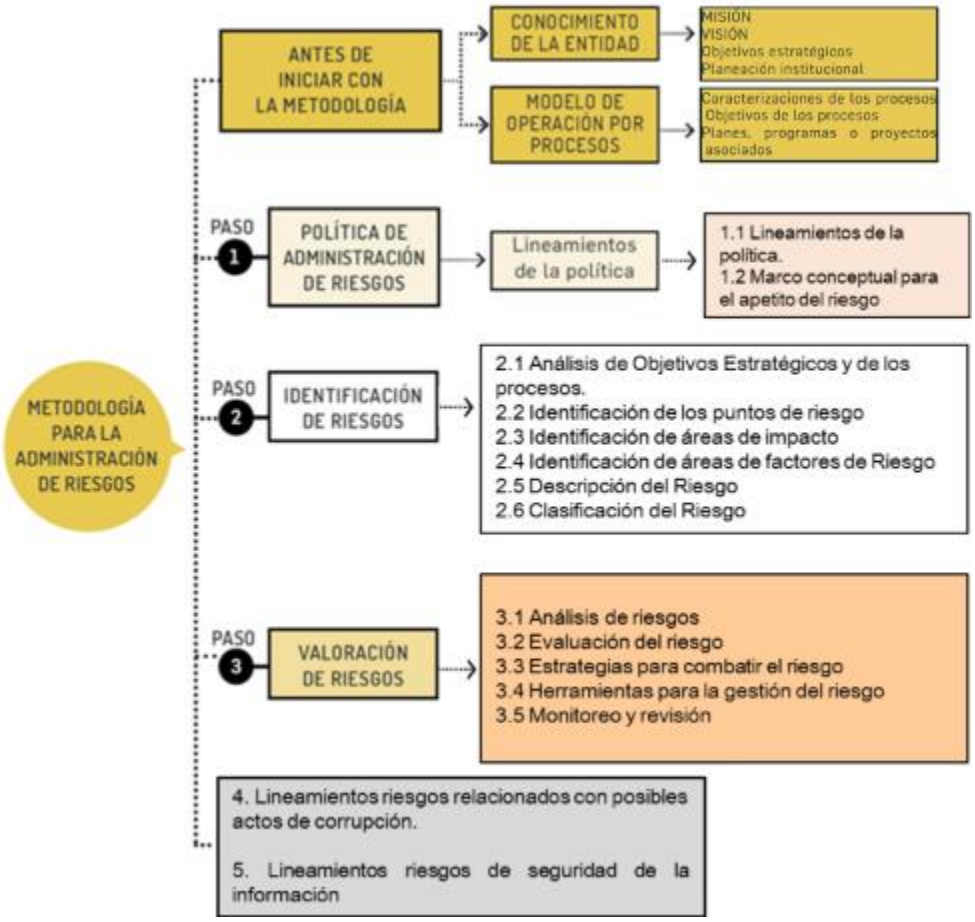
Ilustración 3.Operatividad Institucionalidad para la Administración del Riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP 2020 V5.

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada, como se muestra a continuación:

Ilustración 4, Metodología para la administración del riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP.

9. Establecimiento del contexto de la entidad

Una vez determinados estos lineamientos básicos, es preciso analizar el contexto general de la entidad para establecer su complejidad, procesos y planeación institucional, entre otros aspectos, esto permite conocer y entender la entidad y su entorno, lo que determinará el análisis de riesgos y la aplicación de la metodología en general.

Para la identificación de los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos; por lo tanto, los factores internos y externos para la administración del Riesgo en el DADEP son los siguientes:

9.1 Factores del Contexto Externo que pueden afectar el funcionamiento del Departamento Administrativo de la Defensoría del Espacio Público.

Políticos: Cambios de gobierno, legislación, políticas públicas y regulación (Cambios en la administración central y territorial que genera cambios en los planes de desarrollo).

Económicos y financieros: disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia. Restricciones de orden económico que pueden afectar el funcionamiento de la entidad o la ejecución de los proyectos, Cambios en la asignación presupuestal de la entidad o para el proyecto por cambio de prioridades de la administración.

Sociales y culturales: Demografía, responsabilidad social y orden público. Mayor demanda de espacio público por Incremento de migración de población hacia Bogotá y desplazamiento de esta a la periferia de la ciudad y sus municipios circunvecinos, Requerimientos de las partes interesadas externas (Vecinos, comerciantes, alcalde, concejales).

Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.

Ambientales: Emisiones y residuos, energía, catástrofes naturales y desarrollo sostenible. Cambio de las políticas que propendan por disminuir la afectación ambiental a través de procesos de mitigación de impacto ambiental, Manejo de residuos y Contribución al desarrollo sostenible

Legales y Reglamentarios: Normatividad externa (leyes, decretos, ordenanzas y acuerdos). Nuevas disposiciones legales que afecten a la Entidad (laborales, contratación, manejo de espacio público, sectoriales).

9.2 Factores del Contexto Interno que pueden afectar el funcionamiento del Departamento Administrativo de la Defensoría del Espacio Público.

Financieros: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.

Personal: Competencia del personal, disponibilidad, seguridad y salud ocupacional.

Procesos: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.

Tecnología: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.

Estratégicos: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo

Comunicación Interna: Canales utilizados y su efectividad, flujo de la información adecuado.

9.3 Factores del Contexto del Proceso que pueden afectar el funcionamiento del Departamento Administrativo de la Defensoría del Espacio Público.

Diseño del proceso: claridad en la descripción del alcance y objetivo del proceso.

Interacciones con otros procesos: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.

Transversalidad: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.

Procedimientos asociados: pertinencia en los procedimientos que desarrollan los procesos.

Responsables del proceso: grado de autoridad y responsabilidad de los funcionarios frente al proceso.

Comunicación entre los procesos: efectividad en los flujos de información determinados en la interacción de los procesos.

Activos de Seguridad de la Información del proceso: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano. Ver conceptos básicos relacionados con el riesgo páginas 8 y 9.

10. Niveles de Valoración del Riesgo para calificar la probabilidad y el impacto

Con el fin de poder determinar la posibilidad de ocurrencia de un riesgo, se adoptan los siguientes criterios para clasificar la probabilidad de riesgo en el DADEP.

Ilustración 5. Criterios para definir el nivel de probabilidad de los riesgos de gestión y de seguridad de la información

DESCRIPTOR	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

Ejemplo:
- La actividad se real iza 120 veces al año, la probabilidad de ocurrencia del riesgo es media.

Ilustración 6. Criterios para definir el nivel de impacto de los riesgos de gestión y de seguridad de la información

DESCRIPTOR	Afectación Económica (o presupuestal)	Pérdida Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de alguna área de la organización
Menor-40%	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 de proveedores
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	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
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país

Ejemplo:
- La afectación económica se calcula en 500 SMLMV, el impacto del riesgo es mayor.

Sin embargo, también se podrá tener en cuenta la siguiente tabla de valoración de impacto para los Riesgos de Seguridad de la Información.

Ilustración 7. Valoración de impacto de Riesgos Seguridad de la Información

Nivel	Valor del Impacto	Impacto (Consecuencias) Cuantitativo	Impacto (Consecuencias) Cualitativo
CATASTRÓFICO	5	Afectación en un valor ≥ 50% de la población. Afectación en un valor ≥ 50% del presupuesto anual de la entidad Afectación muy grave del medio ambiente que requiere ≥ 3 años de recuperación.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. Interrupción de las operaciones de la Entidad por más de cinco 5 días
MAYOR	4	Afectación en un valor ≥ 20% e inferior al 50% de la población. Afectación en un valor ≥ 20% e inferior al 50% del presupuesto de la entidad. Afectación importante del medio ambiente que requiere de 1 a 3 años de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. Interrupción de las operaciones de la Entidad entre 2 y 4 días
MODERADO	3	Afectación en un valor ≥ 10% y menor al 20% de la población. Afectación en un valor ≥ 10% y menor al 20% del presupuesto de seguridad de la información en la entidad. Afectación leve del medio ambiente requiere de 3,1 a 1 año de recuperación.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros. Interrupción de las operaciones de la Entidad por un (1) día.
MENOR	2	Afectación en un valor ≥ 1% y menor al 10%de la población. Afectación en un valor ≥ 1% y menor al 10%del presupuesto de seguridad de la información en la entidad. Afectación leve del medio ambiente requiere de 1 a 3 meses de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad Interrupción de las operaciones de la Entidad hasta por 8 horas (1 jornada laboral)
INSIGNIFICANTE	1	Afectación en un valor menor al 1% de la población. Afectación en un valor menor al 1% del presupuesto de seguridad de la información en la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad No hay interrupción de las operaciones de la entidad

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP

Estas calificaciones serán plasmadas para todos los riesgos en las herramientas denominadas mapas de calor, donde se graficarán las probabilidades de ocurrencia de los riesgos analizados, tanto para los riesgos inherentes, como los riesgos residuales después de la implementación de controles.

Ilustración 8. Mapa de Calor

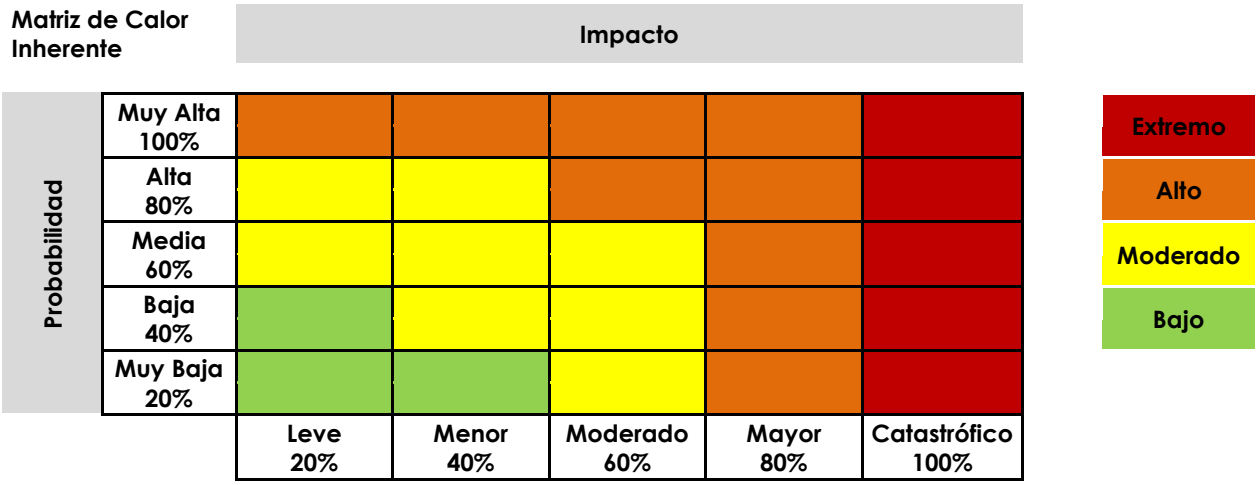


Ilustración 9. Valoración de probabilidad de riesgos de Corrupción

PROBABILIDAD			
NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	Posible	El evento podría ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 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.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP.

Ilustración 10. Medición de impacto de riesgos de Corrupción

IMPACTO CORRUPCIÓN			
NOMBRE DEL RIESGO DE CORRUPCION			
Posibilidad de alterar o manipular información			
No.	SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la Entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?		
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?		

IMPACTO CORRUPCIÓN			
NOMBRE DEL RIESGO DE CORRUPCION			
Posibilidad de alterar o manipular información			
No.	SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SI	NO
9	¿Generar pérdida de información de la Entidad?		
10	¿Generar intervención de los órganos 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?		
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?		
TOTAL RESPUESTAS AFIRMATIVAS		0	

Responder afirmativamente de 1 a 5 pregunta(s) genera un impacto **Moderado** - 3.
Responder afirmativamente de 6 a 11 preguntas genera un impacto **Mayor** - 4.
Responder afirmativamente de 12 a 19 preguntas genera un impacto **Catastrófico**- 5.
MODERADO Genera medianas consecuencias sobre la entidad
MAYOR Genera altas consecuencias sobre la entidad.
CATASTRÓFICO Genera consecuencias desastrosas para la entidad
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP

Estas calificaciones serán plasmadas en las herramientas denominadas mapas de calor para corrupción, donde se graficarán las probabilidades de ocurrencia de los riesgos analizados, tanto para los riesgos inherentes, como los riesgos residuales después de la implementación de controles.

Ilustración 11. Mapa de Calor para Riesgos de Corrupción

PROBABILIDAD	IMPACTO				
	Insignificante(1)	Menor(2)	Moderado(3)	Mayor(4)	Catastrófico(5)
Casi Seguro (5)	Calificación 5 Zona de riesgo alta	Calificación 10 Zona de riesgo alta	Calificación 15 Zona de riesgo extrema	Calificación 20 Zona de riesgo extrema	Calificación 25 Zona de riesgo extrema
Probable (4)	Calificación 4 Zona de riesgo moderada	Calificación 8 Zona de riesgo alta	Calificación 12 Zona de riesgo alta	Calificación 16 Zona de riesgo extrema	Calificación 20 Zona de riesgo extrema
Posible (3)	Calificación 3 Zona de riesgo baja	Calificación 6 Zona de riesgo moderada	Calificación 9 Zona de riesgo alta	Calificación 12 Zona de riesgo extrema	Calificación 15 Zona de riesgo extrema
Improbable (2)	Calificación 2 Zona de riesgo baja	Calificación 4 Zona de riesgo baja	Calificación 6 Zona de riesgo moderada	Calificación 8 Zona de riesgo alta	Calificación 10 Zona de riesgo extrema
Rara vez (1)	Calificación1 Zona de riesgo baja	Calificación 2 Zona de riesgo baja	Calificación 3 Zona de riesgo moderada	Calificación 4 Zona de riesgo alta	Calificación 5 Zona de riesgo alta

Nivel de Severidad	Bajo	Moderado	Alto	Extremo

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP

11.Lineamientos para Riesgos de Seguridad de la Información

Se debe tener en cuenta que la política de seguridad de la información se vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

Los riesgos de seguridad de la información se basan en la afectación de tres pilares en un activo o tipos de activos de información dentro del proceso: "Integridad, confidencialidad o disponibilidad". Se identificarán riesgos de seguridad de la información a los activos o tipos de activos de información que se encuentren clasificados como críticos en el proceso, de acuerdo con la documentación de activos de información de la Entidad.

Existen tres tipos de riesgos asociados a seguridad de la información, entre los que se incluyen: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos de información.

Las amenazas y vulnerabilidades comunes a todas las entidades del sector público pueden ser consultadas en el documento "Anexo 4 Modelo Nacional de Gestión de riesgos de Seguridad de la Información en Entidades Públicas del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC).

11.1 Identificación de los activos de seguridad de la información

Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

Ilustración 12. Identificación activos de información.

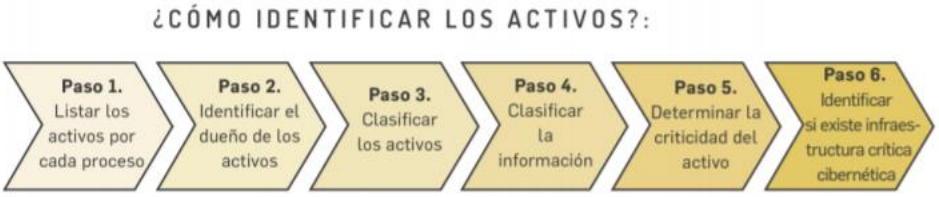
¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización	Permite determinar **qué es lo más importante que cada entidad y sus procesos poseen** (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).

¿Qué son los activos?	¿Por qué identificar los activos?
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber **qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano**, aumentando así su confianza en el uso del entorno digital.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. 2020

Para la identificación de los activos de información debe cumplirse con los siguientes pasos:

Ilustración 13. Pasos identificación activos de información



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. 2020

Para realizar la identificación de activos deberá remitirse a la sección 3.1.6 del anexo 4 "Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas" que hace parte de la Guía para la Administración de Riesgos y Controles, Versión 5 del año 2020.

Ejemplo identificación activos del proceso:

Ilustración 14. Ejemplo identificación de activos de información

Proceso	Activo	Descripción	Dueño del activo	Tipo del activo	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe de oficina financiera	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión financiera	Aplicativo de nómina	Servidor web que contiene el *front office* de la entidad	Jefe de oficina financiera	Software	N/A	N/A	BAJA	MEDIA	BAJA	MEDIA
Gestión financiera	Cuentas de cobro	Formatos de cobro diligenciados	Jefe de oficina financiera	Información	Información pública	No contiene datos personales	BAJA	BAJA	BAJA	BAJA

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. 2020

11.2 Identificación de los activos de seguridad de la información

Se podrán identificar tres (3) tipos de riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas que hace parte de la guía para la administración de riesgos y controles Versión 5 del año 2020.

Para la construcción de los riesgos de seguridad de la información, es necesario contar con la siguiente información:

Ilustración 15. Información requerida para la construcción de los riesgos de seguridad de la información

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/ VULNERA-BILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políti-cas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.	Modificación no autorizada	Seguridad digital	Falta de políticas de seguridad digital	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo(legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.
					Ausencia de políticas de control de acceso	
					Contraseñas sin protección	
					Autenticación débil	

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. 2020

11.3 Infraestructura Crítica Cibernética

Los riesgos de seguridad de la información deben tener en cuenta los criterios de criticidad en las variables definidas en la Guía para la Identificación de Infraestructura Crítica Cibernética - ICC- de Colombia, para la valoración del impacto de afectación de los servicios esenciales de acuerdo con su nivel de criticidad:

- El impacto social: Valorado en función de la afectación de la población (incluyendo pérdida de vidas humanas), el sufrimiento físico y la alteración de la vida cotidiana (se estima como el 0,5% de la población total colombiana).
- El impacto económico: Valorado en función de la magnitud de las pérdidas económicas en relación con el Producto Interno Bruto de Colombia – PIB – (Se estima como el PIB diario o el 0,123% del PIB anual).

- **Impacto medioambiental**: Valorado en función de los años que tarda la recuperación del medio ambiente (se estima como 3 años).

Un ejemplo de este es:

Impacto social 0,5 % Población Nacional	Impacto económico PIB de un día o 0.123% del PIB Anual	Impacto medioambiental
250.000 personas	464.619.736,13	3 años

Fuente: información tomada de la Guía para la Identificación de Infraestructura Crítica Cibernética -ICC- de Colombia

Para la valoración del riesgo es importante tener en cuenta:

Ilustración 16. Variables a tener en cuenta para la valoración de los riesgos de seguridad de la información

Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.
La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.
La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.
La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. 2020

11.4 Controles asociados a la seguridad de la información

La entidad podrá mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", y deben tenerse en cuenta para el análisis de riesgos. Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración:

Ilustración 17. características de diseño y ejecución de los riesgos de seguridad de la información

Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la perdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del *software* y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5. 2020

12. Niveles de aceptación al riesgo

La gestión del riesgo en la Defensoría del Espacio Publicó se seguirá gestionando, mediante la aplicación de la línea estratégica y las tres líneas de defensa establecidas en el Modelo Integrado de Planeación y Gestión MIPG, durante las etapas de desarrollo de la gestión institucional y se establecen los niveles de aceptación del riesgo así:

12.1 Riesgos a Controlar – Administrar

Se establece que la totalidad de riesgos identificados en el mapa de riesgos institucional y por procesos estarán sujetos al seguimiento, monitoreo, control y ajuste mediante la aplicación de la metodología establecida por el Departamento Administrativo de la Función Pública teniendo en cuenta los siguientes lineamientos:

12.2 Para los riesgos de Gestión y Seguridad de la Información se establece el siguiente nivel de aceptación:

Zona de riesgo **BAJO**: Se asumirá el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado.

Zona de riesgo **MODERADO**: Se establecen acciones de control preventivas que permitan reducir la probabilidad de ocurrencia del riesgo.

Zona de riesgo **ALTO**: Se establecen acciones de control preventivas que permitan mitigar la materialización del riesgo.

Zona de riesgo **EXTREMO**: se establecen acciones de Control Preventivas y correctivas que permitan mitigar la materialización del riesgo.

Los riesgos identificados se deben incluir en el mapa de riesgos Institucional y se les realizará monitoreo cada cuatro (4) meses.

10.2.1. Riesgos a priorizar

Los riesgos ubicados en la zona de riesgo extrema y alta serán atendidos a través de acciones concretas. En todo caso, se tendrá como referencia el análisis costo/beneficio para el manejo o la administración del riesgo.

12.3 Para los Riesgos de Corrupción se establece el siguiente nivel de aceptación.

Zona de riesgo **BAJA**: **Ningún riesgo de corrupción podrá ser aceptado**.

Zona de riesgo **MODERADA**: Se establecen acciones de control preventivas que permitan reducir la probabilidad de ocurrencia del riesgo.

Zona de riesgo **ALTA y EXTREMA** Se adoptan medidas para:

- Reducir (Mitigar), la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.

- Reducir (Transferir o compartir), una parte del riesgo para reducir la probabilidad o el impacto de este.
- Evitar, Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.

Periodicidad cuatrimestral de seguimiento para evitar su materialización por parte de los procesos a cargo de estos.

De igual manera el Departamento Administrativo de la Defensoría del Espacio Público-DADEP establece las acciones a seguir por el líder de proceso ante la materialización del riesgo de corrupción, así:

- Informar al Proceso de Direccionamiento Estratégico sobre el hecho encontrado.
- Realizar la denuncia ante la instancia de control correspondiente (cuando se requiera),
- Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento,
- Actualizar el mapa de riesgos.
- Ante la materialización del riesgo de gestión en zona alta, extrema y moderada se procede de manera inmediata a aplicar el plan de contingencia que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso) y documentarlo en el Plan de mejoramiento.

12.4 Plan de Manejo de Riesgos

Los planes de manejo son el conjunto de actividades (acciones) encaminadas a realizar el tratamiento del riesgo, en ellos se identifica los responsables, las fechas de cumplimiento y los indicadores para medir la eficacia de las acciones implementadas.

Adicionalmente, si al valorar los riesgos estos resultan en zona de riesgo “Extrema”, se puede formular opcionalmente un Plan de Contingencia cuyo contenido proyecta aquellas acciones inmediatas a ejecutar en caso de la materialización del riesgo. Esto evita que se presente inconvenientes en el cumplimiento de los objetivos de la Entidad.

Los responsables de las tareas deberán realizar sus reportes cada cuatro meses respecto al avance de estas, de manera tal que la Oficina de Control Interno pueda realizar seguimiento a la efectividad de las medidas para mitigar el riesgo.

13. Escenarios de pérdida de continuidad

Los escenarios de riesgo corresponden a descripciones de situaciones que agrupan la ocurrencia de uno o más riesgos que generan la pérdida de continuidad en las actividades institucionales. La entidad adopta el siguiente conjunto de escenarios de riesgo estandarizados para el diseño de la estrategia de continuidad de negocio:

Escenario	Descripción
Emergencia Social	Imposibilidad de uso de las instalaciones debido a revueltas sociales, asonadas o pérdida del orden público que hace imposible la prestación del servicio o generación del producto.
Desastre Natural y Colapso de Infraestructura Física	Imposibilidad de acceso o abandono súbito de las instalaciones debido a un caso fortuito, fenómeno natural o fuerza mayor.
Desastre Tecnológico	Pérdida total de la capacidad tecnológica o delos procesos institucionales para prestar los servicios o generar los productos.
Crisis Financiera	Inexistencia de los bienes y servicios necesarios para el normal funcionamiento de la entidad que impacta la disponibilidad de recursos financieros, humanos, físicos y tecnológicos
Endemia y Pandemia	Crisis sanitaria que impide el funcionamiento de los procesos institucionales, incluye pandemias y epidemias declaradas por los organismos de salud del Estado.

Cuando se presentan eventos que materializan uno o más de los escenarios de continuidad del negocio la Entidad evaluará las características de la emergencia para autorizar la activación del plan de continuidad, designar recursos y autorizar cualquier comunicación oficial hacia todos los grupos de valor, una vez declarada oficialmente la emergencia, se aplican las acciones de respuesta definidas en el plan de continuidad de negocio para dar respuesta a la misma.

14. Etapas y Herramientas para la Gestión del Riesgo

La gestión de riesgos comprende las actividades de análisis del contexto interno y externo, identificación y análisis del riesgo, valoración, evaluación, definición de controles para el tratamiento y seguimiento. Las diferentes etapas con sus entradas, instrumentos y resultados se describen en la Guía para la administración del riesgo y el diseño de controles en entidades Públicas del DAFP y como complemento en el DADEP se cuenta con el 127-PROVM-01 - Procedimiento administración de los riesgos y 127-FORVM-13 Formato MAPA DE RIESGOS INSTITUCIONALES para el desarrollo de la metodología.

No obstante, como anexo a la gestión del riesgo es necesario referenciar o tener en cuenta con documentos técnicos que orientan esta gestión como el Manual Operativo del MIPG.

15. Control y Monitoreo (Periodo de revisión riesgos institucionales)

El control y monitoreo de riesgos en el DADEP se realizará:

- En primera instancia por el responsable o líder del proceso y
- En instancias posteriores por las auditorías internas programadas por la Oficina de Control Interno.

La finalidad principal de éstas es verificar las disposiciones de monitoreo y sugerir los correctivos u oportunidades de mejora para los ajustes necesarios a los riesgos identificados.

El monitoreo a los riesgos deberá realizarse cuatrimestral, con corte a 30 de abril, 31 de agosto y el 31 de diciembre, durante los 10 primeros días hábiles contados a partir de dichas fechas de corte.

El monitoreo debe incluir la actualización de los riesgos si se presentan cambios en el proceso que generen nuevos riesgos o se requieran modificar los factores determinantes que modifiquen la valoración de los riesgos identificados.

16. Comunicación y Consulta

La administración del riesgo debe ser un tema conocido por todos los funcionarios públicos y contratistas del Departamento Administrativo de la Defensoría del Espacio Público, para lo cual se utilizarán los medios de comunicación virtuales y presenciales. Los mapas de riesgos de la entidad se publicarán conforme indique la normatividad vigente, en el visor del Sistema de Gestión de la Entidad sgc.dadep.gov.co y en la página Web de la entidad www.dadep.gov.co.

Elaboró: Luis Fernando Arango Vargas. Profesional Oficina Asesora de Planeación y Alexander Oliveros Paredes, Contratista.

Revisó: Diana María Camargo Pulido, Jefe Oficina Asesora de Planeación.
Aprobó: Comité Institucional de Coordinación de Control Interno. 24/08/2022
Código de archivo: 140-155-5

CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE MODIFICACIÓN
1	29/01/2021	Actualización de acuerdo con la guía de riesgos del Departamento Administrativo de la Función Pública – versión 5 de diciembre 2020; esta política se encontraba en el proceso de Direccionamiento Estratégico por lo que cuenta con dos versiones anteriores en este proceso.
2	14/07/2021	Actualización de acuerdo con la guía de riesgos del Departamento Administrativo de la Función Pública – versión 5 de diciembre 2020, en aspectos como de Seguridad de la Información; esta política se encontraba en el proceso de Direccionamiento Estratégico por lo que cuenta con dos versiones anteriores en este proceso.
3	23/08/2022	Actualización de la política ampliando los conceptos de acuerdo con la guía de riesgos del Departamento Administrativo de la Función Pública – versión 5 de diciembre 2020, en aspectos de los Riesgos SARLAFT, Servicios y OPAs, y Seguridad de la Información.