GUÍA DE ADMINISTRACIÓN DEL RIESGO Y OPORTUNIDADES

ANH-GES-GU-03

VERSIÓN 5

Contenido

INTRODUCCIÓN

Esta propuesta metodológica constituye un soporte para el fortalecimiento de la política de la Administración del Riesgo y Oportunidades, la implementación del Modelo Estándar de Control Interno-MECI, el Modelo Integral de Planeación y Gestión MIPG, el cual contribuye al fortalecimiento e interiorización de la cultura de Autocontrol y Autoevaluación.

Para el desarrollo de esta política la ANH enmarca en su gestión el proceso de planeación, los procesos institucionales y los controles para garantizar el logro de los objetivos estratégicos y de los procesos.

Esta guía facilita el camino para que la administración del riesgo y oportunidades para que sea incorporada en la práctica diaria como una política de gestión y de control por parte de la alta presidencia y cuente con la participación y respaldo de todos los funcionarios de la ANH, tarea que se facilitará con la implementación de la metodología aquí presentada y con la herramienta informática **SIGECO,** la cual contiene un módulo especial para la administración del riesgo y Oportunidades, lo cual permite establecer mecanismos para identificar, analizar, valorar y administrar los riesgos a los que constantemente están expuestos y a través de ello fortalecer el Sistema de Control Interno para lograr un alto grado de eficacia y eficiencia institucional.

La Administración de Riesgos y Oportunidades que viene adelantando la ANH, es un proceso continuo basado en el conocimiento, evaluación y manejo de los riesgos y oportunidades, el cual es liderado por la Vicepresidencia Administrativa y Financiera.

El objetivo de la administración de riesgos es reducir la posibilidad de ocurrencia o mitigar el impacto de aquellas situaciones (internas o externas) que pueden afectar el logro de los objetivos institucionales o la calidad de los productos o servicios ofrecidos por la Entidad.

Este proceso es desarrollado por el equipo de trabajo que involucra cada proceso (autoridad, líder, facilitador y responsables de la ejecución de actividades del proceso) con la asesoría del equipo de administración de riesgos del equipo de Planeación.

1. OBJETIVOS DE LA GESTIÓN DEL RIESGO Y OPORTUNIDADES

- Aumentar la probabilidad de alcanzar los objetivos estratégicos y de los procesos.
- Involucrar y comprometer a todos los servidores de la entidad en la búsqueda de las acciones encaminadas a prevenir y administrar los riesgos y oportunidades.
- Proteger los recursos del estado.
- Establecer una base confiable para la toma de decisiones y la planificación.
- Asignar y usar eficazmente los recursos para el tratamiento del riesgo y oportunidades.
- Mejorar la eficacia, eficiencia y efectividad operativa.
- Mejorar el aprendizaje y flexibilidad.

2. MARCO NORMATIVO.

El Riesgo y su administración están fundamentados en el siguiente marco normativo:

NORMA	ALCANCE
Ley 87 de 1993	Por la cual se establecen normas para el ejercicio del Control Interno en las entidades y organismos del estado. (Modificada parcialmente por la Ley 1474 de 2011) Artículo 2. OBJETIVOS DEL CONTROL INTERNO: literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.
Ley 489 de 1998	Estatuto Básico de Organización y Funcionamiento de la Administración pública Capítulo VI. Sistema Nacional de Control Interno
Decreto 2145 de 1999	Por el cual se dictan normas sobre el Sistema Nacional de Control Interno de las Entidades y Organismos de la Administración Pública del Orden Nacional y territorial y se dictan otras disposiciones. (Modificado parcialmente por el Decreto 2593 del 2000). (y por el Art. 8º. de la ley 1474 de 2011).
Directiva Presidencial 09 de 1999	Lineamientos para la implementación de la política de lucha contra la corrupción
Decreto 2593 del 2000	Por el cual se modifica parcialmente el Decreto 2145 de noviembre 4 de 1999.

NORMA	ALCANCE
Decreto 1537 de 2001	Por el cual se reglamenta parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado. Parágrafo del Artículo 4º señala los objetivos del sistema de control interno (…) define y aplica medidas para prevenir los riesgos, detectar y corregir las desviaciones…y en su Artículo 3º establece el rol que deben desempeñar las oficinas de control interno (…) que se enmarca en cinco tópicos (…) valoración de riesgos. Así mismo establece en su Artículo 4º la Administración de riesgos, como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas (…).
Decreto 1599 de 2005	Por el cual se adopta el Modelo Estándar de Control Interno para el Estado Colombiano y se presenta el anexo técnico del MECI 1000:2005. Numeral 1.3 Componentes de administración del riesgo.
Decreto 4485 de 2009	Por el cual se adopta la actualización de la NTCGP a su versión 2009. Numeral 4.1 Requisitos Generales literal g) “establecer controles sobre los riesgos identificados y valorados que puedan afectar la satisfacción del cliente y el logro de los objetivos de la entidad” cuando un riesgo se materializa es necesario tomar acciones correctivas para evitar o disminuir la probabilidad de que vuelva a suceder”. Este decreto aclara la importancia de la Administración del riesgo en el Sistema de Gestión de la Calidad en las entidades.
Ley 1273 de 2009	Crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan Integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
Ley 1474 de 2011	**Estatuto Anticorrupción.** Artículo 73. “Plan Anticorrupción y de Atención al Ciudadano” que deben elaborar anualmente todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias antitrámites y los mecanismos para mejorar la atención al ciudadano.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Decreto 1074 de 2015, sus modificaciones y vigencias	Por el cual se expide el Decreto Único reglamentario del Sector Comercio, Industria y Turismo, en lo relacionado con las disposiciones generales para la protección de datos personales.
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Publico, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 del a Ley 1753 de 2015.

NORMA	ALCANCE
NTC – ISO 31000 de 2018	Norma técnica colombiana, gestión del riesgo - principios y directrices
Decreto 1078 de 2015, sus modificaciones y vigencias	Decreto Único Reglamentario del sector TIC. En particular las normas atinentes a la Estrategia de Gobierno Digital y el habilitador Seguridad y Privacidad de la Información que se encuentren vigentes.
Decreto 338 de 2022	Se adiciona el Decreto Único Reglamentario del sector TIC número 1078 de 2015 para establecer los lineamientos y gobernanza de la Seguridad Digital
Decreto 415 de 2016	Se adiciona el decreto único reglamentario del sector de la función pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones; Arts. 2.2.35.5; 2.2.35.6
Resolución 500 de 2021 - MINTIC	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"
Guías e instrumentos del Modelo de Seguridad y Privacidad de la Información	Modelo de Gestión de Riesgos de Seguridad Digital, sus anexos y demás marcos de referencia gubernamentales vigentes.

3. MARCO CONCEPTUAL

Todas las organizaciones están permanentemente expuestas a diferentes riesgos o eventos que pueden afectar el cumplimiento de los objetivos estratégicos y metas institucionales.

Las entidades requieren constante actualización y apertura al cambio, empleando herramientas que les permita ser más eficientes, razón por la cual es necesario formalizar herramientas o metodologías que busquen minimizar la probabilidad de ocurrencia de riesgos en el cumplimiento de los objetivos asignados; e incluso se pueda garantizar la misma presencia y aporte institucional. Por ello es importante resaltar la trascendencia del concepto de riesgo en las organizaciones estatales, ya que éste, con la debida administración, se minimiza, reduce o elimina su impacto negativo en el logro de la misión encomendada, así como se aumenta la protección y la privacidad de la información.

Es crítico establecer la metodología que se aplicará en el proceso, en el caso de la ANH se cuenta con una metodología que supera las exigencias mínimas dadas por el Departamento Administrativo de la Función Pública.

3.1. DEFINICIONES

- **Acciones:** es la aplicación concreta de las opciones del manejo del riesgo que entrarán a prevenir o a reducir el riesgo y harán parte del plan de manejo del riesgo.
- **Activo (de Información):** se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. La información se puede almacenar en muchas formas, incluyendo: forma digital, forma material, así como información en forma de conocimiento de los empleados. Cualquiera que sea la forma que adopte la información o el medio por el que se transmita, siempre necesita la protección adecuada[1].
- **Amenaza:** Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización[2].
- **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[3].
- **Causas:** se asocia a los factores que originan que ocurran determinadas situaciones. Dichos factores pueden clasificarse en externos e internos los cuales pueden generar un impacto positivo o negativo dentro de la organización.
- **Control:** se refiere a toda medida tomada para mitigar o gestionar el riesgo, y para que la probabilidad de que el negocio / proceso logre sus metas y objetivos sea mayor. Son incorporados en los procesos para garantizar que se cumplan los requerimientos del flujo de trabajo y los objetivos generales del negocio y de los procesos.
- **Consecuencias:** 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[4]. Una consecuencia puede ser segura o incierta y, en el contexto de la seguridad de la información, suele ser negativa. Las consecuencias pueden expresarse cualitativa o cuantitativamente. Las consecuencias iniciales pueden incrementarse a través de los efectos secundarios[5].
- **Control existente**: especificar cuál es el control que la entidad tiene implementado para combatir, minimizar o prevenir el riesgo.
- **Descripción:** se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.
- **Efectos:** constituyen las consecuencias de la ocurrencia del riesgo sobre los objetivos de la entidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como: daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.
- **Evento:** presencia o cambio de un conjunto particular de circunstancias.

[1] Guía ISO 73: 2009, ISO 27000:2018
[2] ISO 27000:2018
[3] Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5-2020 - Función Pública
[4] Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5-2020 - Función Pública
[5] ISO 27000:2018

- **Evento (de Seguridad):** Una ocurrencia identificada en el estado de un sistema, servicio o red, indicando una posible violación de la seguridad de la información, política o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad[6]. Un evento de seguridad no necesariamente es un incidente de seguridad[7].
- **Factor de riesgo:** se entiende por factores de riesgo, las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo operativo.
- **Gestión del Riesgo:** actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Gestión de riesgos de seguridad digital:** Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego[8]
- **Factor de riesgo:** se entiende por factores de riesgo, las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo operativo.
- **Gestión de riesgos de seguridad digital:** Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades, ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego[9]
- **Identificación del riesgo:** procesos para encontrar, reconocer y describir el riesgo.
- **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Incidente**: Evento que no es parte de la operación y funcionamiento estándar de un servicio y que puede provocar una interrupción o reducción en la calidad de este[10]
- **Incidente de seguridad de la información**: Evento único o serie de eventos inesperados, no deseados, que poseen una probabilidad significativa de comprometer las operaciones de la Entidad y amenazar la Seguridad de la Información[11]
- **Infraestructura Crítica Cibernética (ICC):** Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales[12]. Complementariamente, la **Infraestructura crítica cibernética nacional** 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. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar

[6] Norma ISO 27035
[7] ISO/IEC 27000:2018
[8] Modelo Nacional de Gestión de Riesgos de Seguridad Digital
[9] CONPES 3854
[10] ISO 27000:2018
[11] ISO 27000:2018
[12] Ministerio de Defensa

económico de los ciudadanos o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública[13].

- **Inventario de activos**: Sigla en inglés: Assets inventory. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del Sistema de Gestión de Seguridad de la Información - SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos[14].
- **Mapa de riesgos:** cuadro resumen mediante el cual se presentan los distintos aspectos tenidos en cuenta en el análisis, valoración y manejo de los riesgos de la Agencia.
- **Marco de referencia para la gestión del riesgo:** conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **Nivel de riesgo:** el resultado de la aplicación de la escala escogida para determinar el nivel de riesgo de acuerdo a la posibilidad de ocurrencia, teniendo en cuenta los controles existentes.
- **Política para la Gestión del riesgo:** declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.
- **Probabilidad:** oportunidad o posibilidad de que algo suceda.
- **Privacidad:** Se entiende como el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar que genera la obligación de proteger dicha información en observancia del marco legal vigente[15]
- **Riesgo:** representa la posibilidad de ocurrencia de un evento que pueda entorpecer el normal desarrollo de las funciones de la entidad y afectar el logro de sus objetivos.
- **Riesgos Estratégicos:** son riesgos causados por eventos o situaciones en su mayoría externas a la ANH que tienen un impacto significativo sobre las decisiones estratégicas y actividades.
- **Riesgos de Procesos:** los riesgos de procesos son inherentes en las actividades permanentes que se desarrollan en los procesos de la ANH.
- **Riesgos de Proyectos**: son riesgos asociados con proyectos que son de una naturaleza específica, corto o largo plazo y son frecuentemente asociados con adquisiciones, integración de proyectos, cambios en la estructura, ampliación de las operaciones y, en general manejo de cambios importantes.
- **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[16].
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital

- **Seguridad Digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales
- **SGSI:** Sigla para Sistema de Gestión de Seguridad de la Información

[13] CONPES 3854
[14] ISO 27000:2018
[15] MINTIC, Modelo de Seguridad y Privacidad de la Información - MSPI
[16] Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5-2020 - Función Pública

- **Valoración del riesgo:** proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

Como complemento a las definiciones, se sugiere consultar el Glosario del Sistema de Gestión de Seguridad de la Información - SGSI publicado en el Sistema de Gestión de Calidad de la Entidad.

4. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Teniendo en cuenta que la administración de riesgos es estratégica para el logro de los objetivos institucionales a continuación se enuncian las principales guías o marcos de acción que permitirán tomar decisiones relativas a la respuesta de la Agencia frente al riesgo. Para ello se han agrupado en los siguientes ejes temáticos:

4.1. OBJETIVO

Fortalecer la administración de los riesgos de corrupción, gestión, seguridad de la información y seguridad digital, orientando la toma de decisiones y el tratamiento de los riesgos, de acuerdo con las metodologías vigentes establecidas y teniendo en cuenta los atributos de disponibilidad, integridad y confidencialidad de la información para su correcta identificación, análisis, valoración, registro, monitoreo y evaluación.

4.2. ALCANCE DE LA POLÍTICA

La administración de riesgos en la Agencia Nacional de Hidrocarburos tendrá un carácter prioritario y estratégico, iniciando con la definición del contexto estratégico de los riesgos a los que está expuesta la entidad dando cubrimiento a los procesos estratégicos, misionales, de apoyo y evaluación, aplicando los criterios diferenciales para los riesgos de seguridad de la información y de seguridad digital[17] y, concluye con el plan de acción mediante el cual se realizará el tratamiento, monitoreo y revisión de los riesgos identificados.

4.3. ROLES Y RESPONSABILIDADES

De acuerdo con los Lineamientos establecidos en el Modelo Integrado de Planeación y Gestión - MIPG, para la administración de riesgos se adopta lo establecido en el esquema de líneas de defensa para identificar la responsabilidad de la gestión y control que está distribuida de la siguiente manera:

[17] El alcance de la administración del riesgo de seguridad digital debe ser extensible y aplicable a los procesos de la entidad pública que indiquen los criterios diferenciales del Modelo de Seguridad y Privacidad de la Información, habilitador de la Estrategia de Gobierno Digital vigente expedida por el MINTIC.

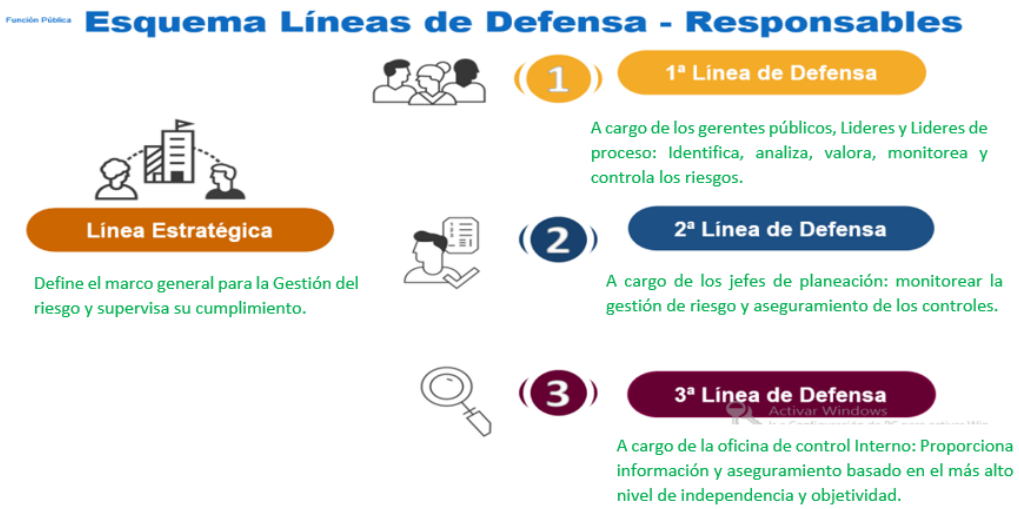


Imagen: Esquema de Líneas de Defensa
Fuente: Departamento Administrativo de la Función Pública

Los roles y responsabilidades para la gestión de riesgos se alinean con los establecido en el Modelo Integrado de Planeación y Gestión - MIPG, conforme la naturaleza y manual de funciones de la Entidad.

En caso de considerarse necesario, se definirán roles y responsabilidades específicos en los instrumentos que correspondan y en razón a disposiciones normativas, organizacionales, cambios y/o mejores prácticas que aporten a la mejora continua de la gestión de riesgos; sin embargo, en principio en la Entidad, se adoptan y se toman como referencia los que se encuentran ya definidos en los lineamientos vigentes.

4.4. NIVEL DE ACEPTACIÓN DEL RIESGO

Tipo de Riesgo	Zona de Riesgo	Nivel de Aceptación
Gestión	Baja	Se ASUMIRÁ el riesgo y debe incluirse en la matriz de riesgos institucional, se administrará por medio de las actividades propias del proceso y no será necesario establecer un Plan de Manejo del Riesgo.
	Moderada	Se ASUMIRÁ el riesgo y debe incluirse en la matriz de riesgos institucional, se administrará por medio de las actividades propias del proceso y no será necesario establecer un Plan de Manejo del Riesgo. Se debe realizar un monitoreo semestral a través del módulo de riesgos del aplicativo SIGECO.

Tipo de Riesgo	Zona de Riesgo	Nivel de Aceptación
	Alta	Se deben establecer acciones para REDUCIR EL IMPACTO y DISMINUIR LA PROBABILIDAD de materialización del riesgo, se debe establecer un Plan de Manejo de Riesgo y se debe hacer un monitoreo trimestral a través del módulo de riesgos del aplicativo SIGECO.
	Extrema	Se deben establecer acciones para REDUCIR EL IMPACTO y DISMINUIR LA PROBABILIDAD de materialización del riesgo, se debe establecer un Plan de Manejo de Riesgo y un Plan de Contingencia y se debe hacer un monitoreo mensual a través del módulo de riesgos del aplicativo SIGECO.

Tipo de Riesgo	Zona de Riesgo	Nivel de Aceptación
Corrupción	Baja	Ningún riesgo de corrupción podrá ser aceptado. se debe hacer monitoreo trimestral a través del módulo de riesgos del aplicativo SIGECO para evitar su materialización.
	Moderada	Ningún riesgo de corrupción podrá ser aceptado. Se deben establecer medidas para REDUCIR la probabilidad de ocurrencia del riesgo y hacer monitoreo trimestral a través del módulo de riesgos del aplicativo SIGECO para evitar su materialización.
	Alta	Ningún riesgo de corrupción podrá ser aceptado. Se deben establecer acciones para REDUCIR EL IMPACTO y DISMINUIR LA PROBABILIDAD de materialización del riesgo, se debe establecer un Plan de Manejo de Riesgo y hacer un monitoreo bimestral a través del módulo de riesgos del aplicativo SIGECO.
	Extrema	Ningún riesgo de corrupción podrá ser aceptado Se deberán establecer acciones para REDUCIR EL IMPACTO y DISMINUIR LA PROBABILIDAD de materialización del riesgo, se debe establecer un Plan de Manejo de Riesgo y un Plan de Contingencia y hacer un monitoreo mensual a través del módulo de riesgos del aplicativo SIGECO.

Tipo de Riesgo	Zona de Riesgo	Nivel de Aceptación
	Baja	El proceso podrá decidir si propone un Plan de Manejo del Riesgo o si lo ACEPTA, para lo cual como mínimo debe garantizar una copia de respaldo periódica de la información y planes de soporte y mantenimiento cuando se trate de dispositivos tecnológicos, lo cual debe estar documentado.

Tipo de Riesgo	Zona de Riesgo	Nivel de Aceptación
Seguridad de la Información y Seguridad Digital		Se debe hacer monitoreo según periodicidad definida*, buscando prevenir su materialización.
	Moderada	Se deben establecer medidas para REDUCIR LA PROBABILIDAD de ocurrencia del riesgo y se debe hacer monitoreo según periodicidad definida* buscando evitar su materialización.
	Alta	Se deben establecer acciones para DISMINUIR LA PROBABILIDAD y REDUCIR EL IMPACTO de materialización del riesgo, se debe establecer un Plan de Manejo de Riesgo y hacer monitoreo anual buscando evitar su materialización**.
	Extrema	Se deberán establecer acciones para DISMINUIR LA PROBABILIDAD Y REDUCIR EL IMPACTO de materialización del riesgo, se debe establecer un Plan de Manejo de Riesgo, un Plan de Contingencia y hacer monitoreo anual buscando evitar su materialización**.
	*Cada proceso podrá definir la periodicidad de monitoreo para los Riesgos Residuales en Zona Baja y Moderada, que no podrá ser superior a dos (2) años. En el caso **de ICC[18] o Riesgos asociados a incumplimientos normativos, de estándares certificados por la Entidad y/o posibles sanciones legales**, se deberá validar los controles, realizar monitoreo y seguimiento por lo menos **una (1) vez al año.** ** Si se identifican riesgos nuevos en las **Zonas Alta y Crítica** y la implementación de los controles para su mitigación demanda recursos y plazos extendidos, se deberá definir un plan de contingencia para ser aplicado inmediatamente en caso de su materialización, incluyendo responsables, plazo y evidencias, mientras se implementan los controles requeridos. Cuando la implementación de controles supera el valor de la posible materialización de un riesgo, se **ACEPTARÁ** el riesgo, para lo cual, se deberá analizar si es posible eliminar la causa y/o la vulnerabilidad. En todo caso se deberán implementar las medidas que haya disponibles para su mitigación.	

[18] Infraestructura Crítica Cibernética, ver en Definiciones.

4.5. LIDERAZGO Y COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección adquiere el compromiso de facilitar el cumplimiento de los objetivos sobre la gestión de los riesgos de *gestión, de corrupción, de seguridad de la información y de seguridad digital*, a través del establecimiento de políticas, roles y responsabilidades, así como, la adopción de medidas técnicas, administrativas, de talento humano, la asignación de recursos necesarios para que el proceso se desarrolle en la entidad de forma efectiva y el monitoreo, seguimiento y la toma de decisiones para la mejora continua.[19]

Conforme los lineamientos vigentes, ANH designará un **responsable de Seguridad Digital** que también es el responsable de la Seguridad de la Información, el cual debe pertenecer a un área de la Alta Dirección o Línea Estratégica que le permita de manera trasversal el acompañamiento a todos los procesos. Las responsabilidades de este y demás roles asociados son detalladas en los instrumentos para tal fin. [20]

4.6. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

La metodología institucional para la gestión del riesgo se basa en lo propuesto en la **NTC-ISO31000** la cual describe un proceso sistemático, lógico y detallado para identificar, analizar, evaluar y tratar los riesgos. La metodología inicia con el análisis del contexto interno y externo de la organización para pasar a la etapa de valoración de riesgo en la cual se identifica el riesgo, se analiza y se evalúa, para finalizar con a la etapa de tratamiento, todo esto enmarcado en el monitoreo constante y la comunicación y difusión de los riesgos al interior de la organización.

De igual manera en lo concerniente a seguridad de la información y seguridad digital, se siguen los lineamientos gubernamentales vigentes y las buenas prácticas en la materia[21].

Imagen: Proceso de la Gestión del Riesgo
Fuente: NTC ISO 31001:2018

[19] En cuanto a recursos se hace referencia al personal capacitado e idóneo, recursos económicos para implementación de controles y para la mejora continua. Adaptado del Modelo de Gestión de Riesgos de Seguridad Digital, su anexo 4 v4-2021 y Resolución 500 de 2021
[20] Conforme lo establece el Manual Operativo de MIPG en el numeral 3.2.1.4 Política de Seguridad de la información, en alineación con el MSPI vigente. Ver Guía de Roles y Responsabilidades MISP v4-2021 o la que se encuentre vigente
[21] Lineamientos de MINTIC para el MSPI y Norma ISO 27001 vigente

La Administración del Riesgo en el Ciclo PHVA

Para tener una adecuada Gestión del Riesgos, se debe entender que los riesgos están asociados a todas las actividades que se desarrollan en el ciclo PHVA (Planear, Hacer, Verificar y Actuar):

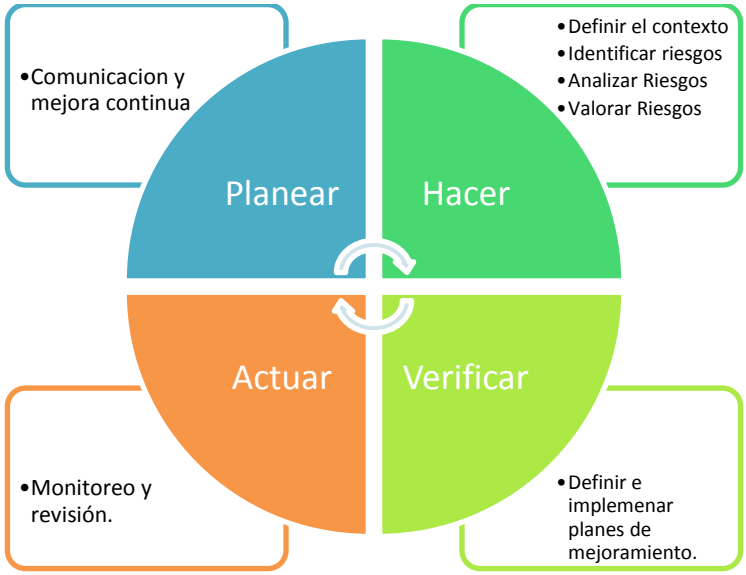


Imagen: Ciclo PHVA
Fuente: Autoría propia

Las entidades de la administración pública deben darle cumplimiento a su misión y visión, a través de sus objetivos institucionales, los cuales se desarrollan a partir del diseño y ejecución de los diferentes planes, programas y proyectos.

El cumplimiento de dichos objetivos puede verse afectada por factores tanto internos como externos que crean riesgos frente a todas sus actividades, razón por la cual se hace necesario contar con acciones tendientes a administrarlos.

El adecuado manejo de los riesgos favorece el desarrollo y crecimiento de la entidad, con el fin de asegurar dicho manejo es importante que se establezca el entorno y ambiente organizacional de la entidad, la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos.

Riesgos de seguridad de la información y seguridad digital

El Modelo Nacional de Riesgos de Seguridad Digital para entidades del sector público plantea el siguiente esquema:

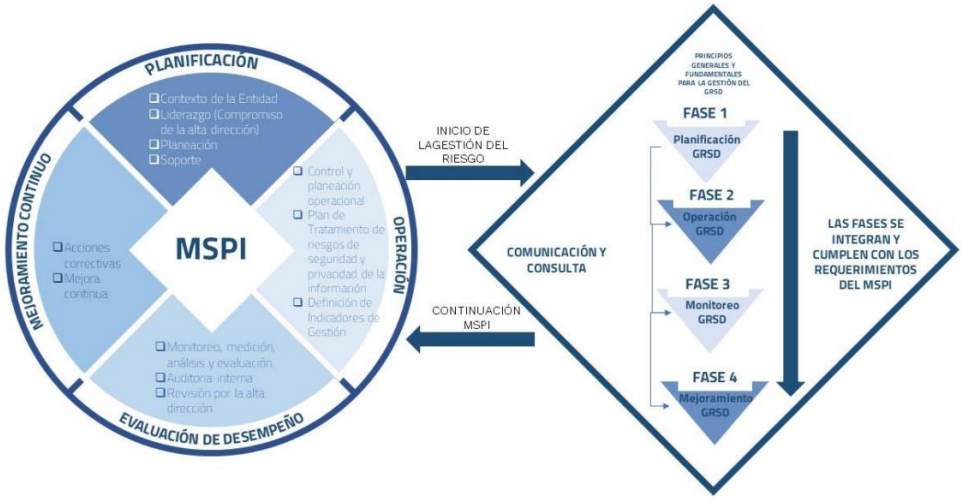


Imagen: Interacción entre el MSPI y el MGRSD
Fuente: Modelo Nacional de Gestión de Riesgos de Seguridad Digital - MINTIC

El criterio diferencial más relevante en la gestión de riesgos de seguridad de la información y seguridad digital es la necesidad de identificar los activos de información[22], las amenazas y las vulnerabilidades asociadas a estos.

[22] Activos de información en el marco del MSPI, los cuales difieren del Registro de Activos de Información que debe publicarse según la Ley de Transferencia 1712 de 2014. Conforme lo indicado en la Guía 5 para la gestión y clasificación de activos de información V1-2016, el inventario de activos de información "debe ser un documento clasificado como 'Confidencial', y no debe tener características que lo permitan modificar por los usuarios autorizados. Sólo debe tener acceso de modificación a este documento el líder del proceso con previa autorización del oficial de seguridad de la información o quien hagas sus veces.

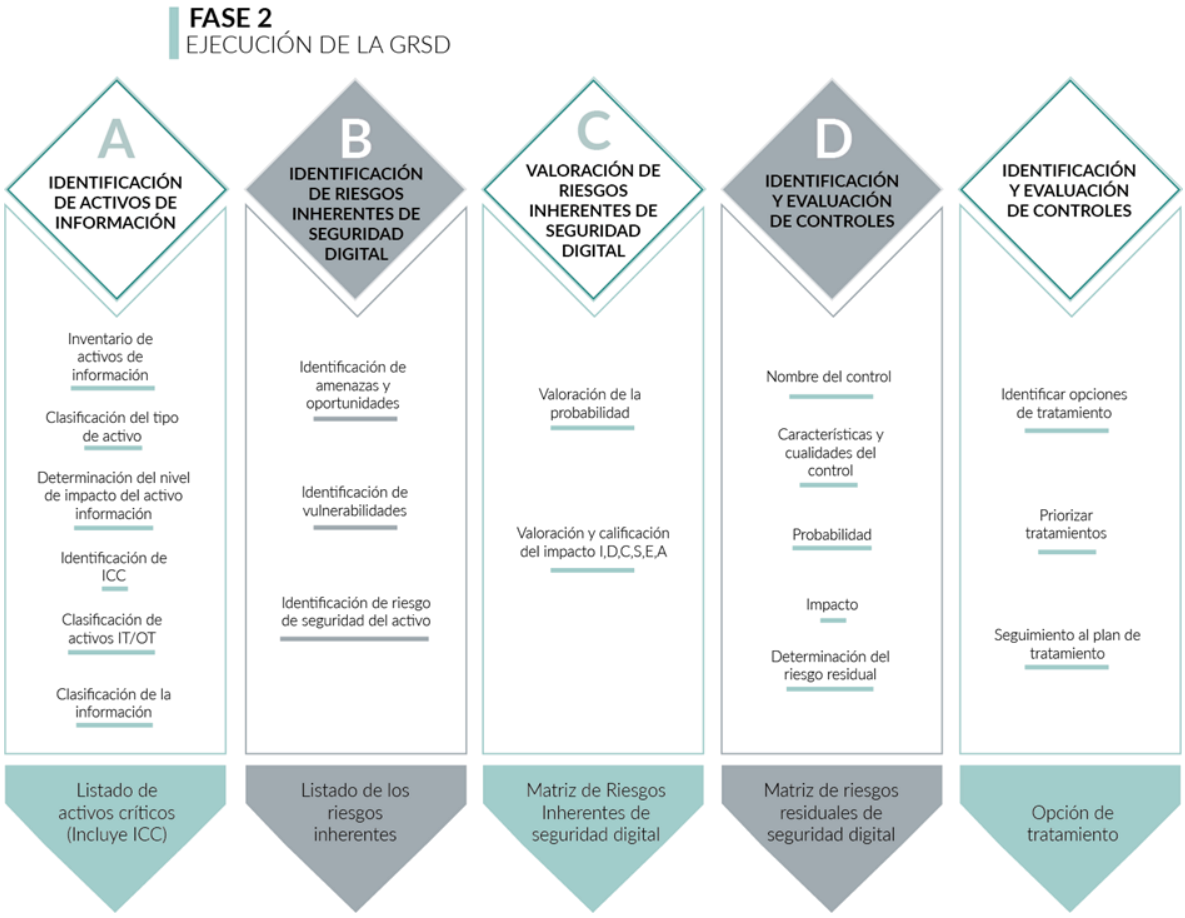


Imagen: Ejecución de la GRSD
Fuente: Modelo Nacional de Gestión de Riesgos de Seguridad Digital - MINTIC

4.6.1. SOFTWARE PARA LA GESTIÓN INTEGRAL DE RIESGOS

La Agencia Nacional de Hidrocarburos cuenta con la herramienta SIGECO (Disponible en: http://192.168.67.83/portal/index.php) la cual tiene un módulo de riesgos que suporta toda la gestión de los riesgos institucionales (Identificación, valoración, controles, planes de tratamiento y planes de contingencia) y que puede ser utilizada y consultada por todos los funcionarios y colaboradores de la entidad.

Así mismo, en lo relacionado a la gestión de riesgos de seguridad de la información y seguridad digital, dada su especificidad, se utilizará la herramienta informática disponible y, en su defecto, los instrumentos normalizados que se definan.

4.6.2. COMUNICACIÓN Y CONSULTA

En esta fase se busca promover la toma de conciencia y comprensión frente al riesgo, así como la obtención de información y retroalimentación para la toma de decisiones. La consulta de las partes interesadas ayudará a:

- Establecer el análisis del contexto
- Garantizar que las necesidades e interés de las partes interesadas sean tenidas en cuenta en la definición de riesgos.
- Identificar y analizar los riesgos desde diferentes puntos de vista.
- Apoyar la construcción de los planes de tratamiento de riesgos.

4.6.3. ALCANCE

Determinar el alcance permite adaptar la gestión de riesgo a las necesidades y la complejidad de la entidad, de esta forma se contribuye a una evaluación del riesgo eficaz y a un tratamiento apropiado del riesgo. Para definir el alcance se deben tener en cuenta:

- Los objetivos, naturaleza, características propias y los resultados esperados de la organización.
- Las herramientas y técnicas para la evaluación del riesgo.
- Los recursos, responsabilidades y registros a conservar.
- Los requisitos legales, reglamentarios y contractuales aplicables a la organización
- Las interfaces, intercambio de información e interoperabilidad con otras Entidades
- los resultados del análisis de riesgos y gestión de incidentes de seguridad digital
- los procesos de la Entidad, especialmente los que por sus criterios diferenciales se enmarquen en el Modelo de Seguridad y Privacidad de la Información[23]

En la implementación de la gestión de riesgos de seguridad de la información y seguridad digital, conforme el tamaño, naturaleza, misión y capacidad instalada en la Entidad, podrá definirse de manera gradual el alcance priorizando los procesos más críticos y misionales o en fases, que permitan, en suma, cubrir todos los procesos.

[23] Y en el marco del Sistema de Gestión de Seguridad de la Información -SGSI institucional (Resolución 266 de 2018) y las políticas vigentes.

4.6.4. ANÁLISIS DEL CONTEXTO INTERNO Y EXTERNO

En esta etapa se deben definir los factores internos y externos que se deben tener en cuenta para la administración del riesgo, ya que de estos factores se pueden establecer las causas de los riesgos a identificar.

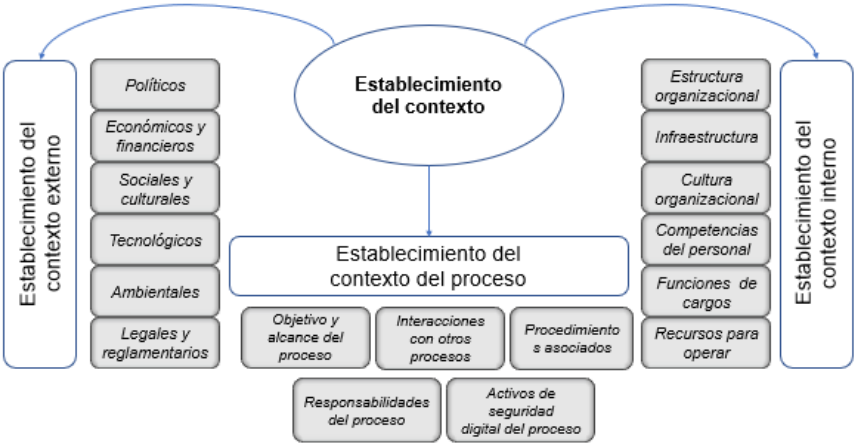


Imagen: Análisis del Contexto Interno y Externo
Fuente: Guía de administración de riesgos – DAFP

En la identificación del contexto interno y externo de la entidad, es necesario profundizar en los aspectos relacionados con seguridad digital, por lo tanto, se debe consultar el lineamiento vigente.[24]

Para el entendimiento del contexto interno a nivel de los procesos, se tendrá en cuenta la documentación normalizada, oficializada y vigente en el Sistema de Gestión de Calidad de la Entidad.

En la medida en que se van presentando cambios en el contexto, se pueden presentar nuevos eventos o riesgos que deben ser atendidos como parte del proceso[25].

4.6.5. IDENTIFICACIÓN DEL RIESGO

Riesgos de Gestión

En esta etapa se deben establecer las fuentes o factores de riesgos, sus causas y consecuencias. Para esto se deben tener en cuenta datos históricos, análisis de contexto interno y externo, informes de expertos y necesidades y expectativas de las partes interesadas.

[24] Consultar el Anexo 4 del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información v4-2021 o el que se encuentre vigente
[25] Anexo 4 del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información v4-2021 o el que se encuentre vigente

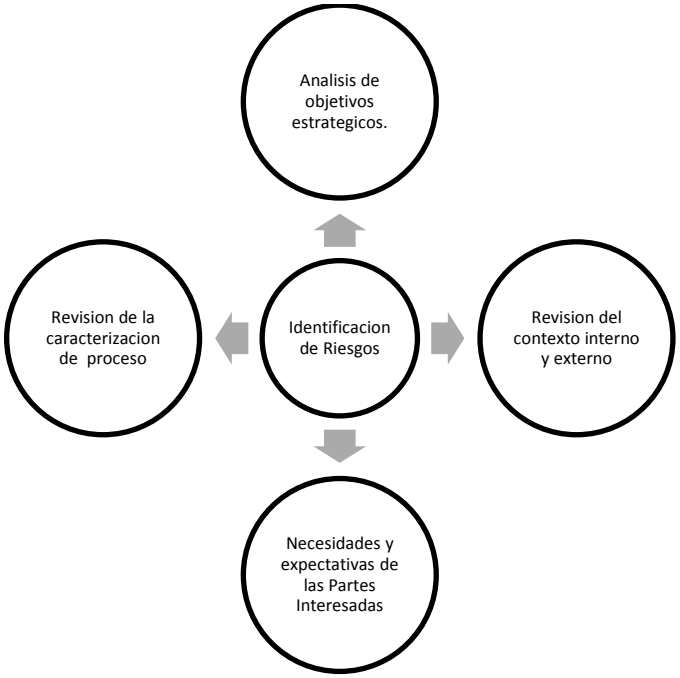


Imagen: identificación de riesgos
Fuente: Autoría propia

En la identificación de riesgos se busca establecer que sucesos pueden ocurrir en la organización que tengan un efecto sobre el logro de los objetivos, para ello se pueden utilizar unas preguntas claves para orientar la identificación de riesgos:

- ¿Qué puede suceder?: Identificar la afectación del cumplimiento del objetivo o actividad del proceso.
- ¿Cómo puede suceder?: Establecer las causas a partir de los factores determinados en el contexto.
- ¿Cuándo puede suceder?: Determinar de acuerdo con el desarrollo del proceso.
- ¿Qué consecuencias tendría su materialización?: Determinar los posibles efectos por la materialización del riesgo.

Ejemplo:

Objetivo: Abastecer de bienes y servicios corporativos oportunamente de acuerdo con las **necesidades de la compañía** en función del **cumplimiento de las metas organizacionales.**

- Riesgo: Realizar las compras de bienes y servicios desalineadas con las necesidades de la compañía.
- Riesgo: Realizar las compras sin cumplir con los estándares definidos en los manuales y procedimientos institucionales.
- Riesgo: Incumplimiento de parte de contratistas o proveedores a lo pactado en la orden de compra o contrato.
- Riesgo: Cerrar contratos de manera inoportuna y/o inadecuada.

Adicionalmente se debe tener en cuenta que:

- El riesgo y la causa debe estar escrito en un lenguaje común (que entienda toda la Organización).
- Evitar las negaciones o el impacto para expresar el riesgo
- El riesgo generalmente se redacta en infinitivo.
- Las causas son aquel evento que hace que el riesgo se materialice.
- Las causas no son una negación del control.

Riesgos de Corrupción

Un riesgo de corrupción es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo publico en beneficio propio de un tercero para poder identificar los riesgos es necesario determinar los factores que afectan positiva o negativamente el cumplimiento de la misión y los objetivos institucionales tanto a nivel externo como interno. Los riesgos de corrupción siempre se deben establecer sobre los procesos:

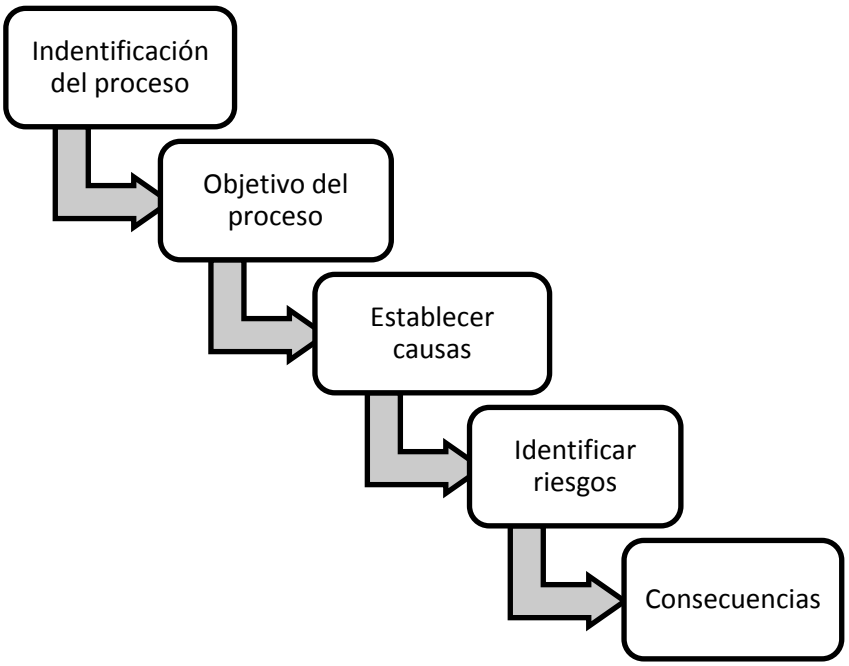


Imagen: Identificación de riesgos de corrupción sobre los procesos
Fuente: Autoría propia

Los riesgos de corrupción deben ser escritos de forma clara y precisa, en su redacción se deben tener presente los siguientes componentes:

***Acción u omisión* + *Uso del Poder* + *Desviación de la gestión de lo público* + *Beneficio Privado*.**

Ejemplo:

- *Posibilidad de Recibir o solicitar cualquier beneficio a nombre propio o de terceros con el fin de celebrar un contrato.*

Riesgos de seguridad de la información y seguridad digital

Se debe iniciar con la identificación y clasificación de los activos de información, incluyendo la identificación de infraestructuras críticas cibernéticas[26], aquellos activos conforme la Ley de Transparencia y de Protección de Datos Personales[27] y, los que requieren autenticación digital.

La identificación de activos de información comprende los siguientes pasos[28]:

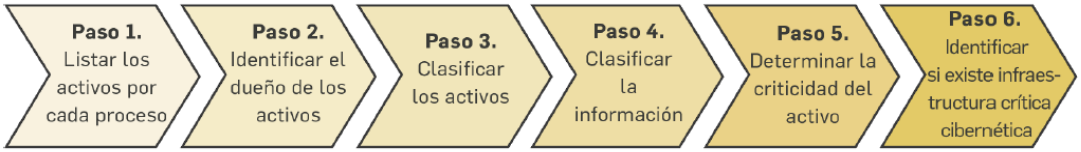


Imagen: Pasos para la identificación de activos
Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5-2020 - Función Pública

Esta identificación de los activos de información debe realizarse por parte de la ***Primera Línea de Defensa*** en cada proceso. El área responsable de liderar la implementación de la política de gobierno digital y/o los relacionado con seguridad de la información y seguridad digital realiza acompañamiento técnico y orientación en esta labor.

En la identificación del riesgo, se tienen en cuenta las propiedades de la seguridad de la información a saber ***Confidencialidad, Integridad y Disponibilidad*.**

De igual manera, se deben identificar las amenazas y vulnerabilidades, las causas y consecuencias. Es importante tener en cuenta que pueden existir varias causas y varias consecuencias para un riesgo; así como que, por cada causa debe realizarse el respectivo análisis de riesgo.

La identificación de todos estos aspectos sea basa en los lineamientos gubernamentales vigentes[29], los cuales se recomienda consultar para su respectiva aplicación. Complementariamente se pueden consultar otras guías gubernamentales relacionadas y las buenas prácticas vigentes[30]. Respecto a los formatos se deben utilizar los que se encuentren vigentes en el sistema de gestión de calidad de la Entidad.

Una vez identificados y clasificados los activos de información, se deben tener en cuenta los siguientes aspectos para la identificación del Riesgo de Seguridad de la Información/Seguridad Digital:

[26] Guía de Inventario y clasificación de activos de información e infraestructura crítica cibernética nacional v4-2021 – MINTIC o la que se encuentre vigente
[27] Ley 1712 de 2014 y Ley 1581 de 2012 respectivamente, o las que se encuentren vigentes en la materia
[28] Se hace claridad que el inventario de activos aquí mencionado se enmarca a la gestión de riesgos de seguridad digital, siendo interno y de carácter CONFIDENCIAL y, por ende, no debe confundirse con el Registro de Activos de Información que por Ley 1712 de 2014 debe publicarse.
[29] Actualmente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5-2020 - Función Pública y, Anexo 4 del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información v4-2021 – MINTIC con sus anexos y guías complementarias del MSPI. Es importante consultar su vigencia antes de aplicarlos.
[30] En cuanto a identificación de activos: la Guía 5 para la Gestión y Clasificación de Activos de Información V1-2016 del MSPI – MINTIC, en cuanto a Gestión de Riesgos: Guía 7 de gestión de riesgos V3-2016 del MSPI - MINTIC y, buenas prácticas como la ISO 27001. Dada la constante actualización de estos lineamientos, siempre deberá remitirse a aquellos que se encuentren vigentes al momento de la gestión

Criterios de selección de activos para análisis de Riesgos

Como mínimo, a los siguientes activos se les identificarán los riesgos:

- *A los que contengan o gestionen datos personales*
- *A los que requieran autenticación digital*[31]
- *A los que soporten o hagan parte de Infraestructuras Críticas Cibernéticas*
- *A los de valoración de criticidad MEDIA y ALTA*
- *A los que tengan alguna de las propiedades de seguridad de la información (Confidencialidad, Integridad, Disponibilidad) con clasificación en ALTA*
- *A los de valor estratégico para la Entidad y,*
- *A los que puedan derivar en sanciones legales o afectar la imagen de la Entidad*

Para los demás activos de información, la identificación de riesgos será potestativo del dueño del riesgo siempre y cuando, se garantice que se cuenta con copia de seguridad y controles de acceso de dichos o con planes de soporte y mantenimiento, según corresponda. Se deberá documentar cuando se decida no identificar riesgos para estos activos.

Agrupación

Para la identificación de los riesgos, los activos de información deben agruparse por tipo de activo, realizando el análisis de manera conjunta para cada tipo[32].

Técnica de identificación

Se tendrán como base para la identificación del riesgo, los historiales, estadísticas y/o diagnósticos existentes; al ser un proceso cíclico, en la medida que se documenten eventos o incidentes, estos deberán retroalimentar el siguiente ciclo. En la ausencia de estos datos, se realizará la técnica de juicio de expertos y/o lluvia de ideas con base en el conocimiento y experiencia de los participantes, para lo cual se podrá promediar la calificación propuesta por cada uno.

Descripción del Riesgo

Para estandarización en la descripción del Riesgo de seguridad de la información y seguridad digital, se tendrá en cuenta la siguiente estructura:

Propiedad(es) de seguridad de la información afectada(s) + amenaza a materializarse + vulnerabilidad presente

Ejemplos:

[31] Anexo 4 del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información v4-2021 – MINTIC

[32] No es necesario identificarle riesgos a cada activo de información.

- *Pérdida de confidencialidad e integridad por corrupción de los datos y acceso no autorizado debido a la asignación errada de los derechos de acceso*

- *Pérdida de disponibilidad por fallas en el suministro de energía debido a red energética inestable y ausencia de unidad de respaldo (UPS)*

No se recomienda incluir nombres de activos de información puntuales en la descripción del riesgo, por cuanto el análisis se hace agrupado por tipo de activo y un mismo riesgo puede aplicar a varios activos.

4.6.6. ANÁLISIS DEL RIESGO.

El análisis del riesgo busca establecer la probabilidad de ocurrencia y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente). El análisis del riesgo depende de la información obtenida en la fase de identificación de riesgos. En primer lugar, se deben analizar las causas que originan la materialización de los riesgos.

También es importante considerar las fuentes generadoras del riesgo, lo cual facilita la identificación, analizando si para estas fuentes existen debilidades o amenazas. Algunas fuentes son:

- *La presión de la competencia*
- *Los empleados*
- *Los clientes*
- *Las nuevas tecnologías*
- *Los cambios del entorno*
- *Leyes y regulaciones*
- *La globalización*
- *Las operaciones*
- *Los proveedores*[33].
- *Instalaciones eléctricas*
- *Los espacios de trabajo*
- *El almacenamiento y transporte*
- *El espionaje*
- *El terrorismo*
- *Los criminales de la computación, entre otras*

A nivel digital, las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas, por ende, es recomendable identificar todos los orígenes posibles y realizar un modelado de amenazas[34]. Así mismo, las vulnerabilidades, para que generen daño debe existir una amenaza para explotarla, por lo que, es importante realizar el análisis conjunto[35].

[33] Recuperado de http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/3IdentificaciondelosRiesgos_es.pdf
[34] Para esto se recomienda consultar como referente las fuentes, tipos y amenazas comunes sugeridas en la Guía 7 Gestión de Riesgos v3-2016 y Guía 1 Metodología de Pruebas de efectividad v1-2016– MINTIC o las que se encuentren vigentes y buenas prácticas en la materia.
[35] Se recomienda consultar las vulnerabilidades conocidas, según los tipos de activos sugeridas en la Guía 7 Gestión de Riesgos v3-2016 y Guía 1 Metodología de Pruebas de efectividad v1-2016– MINTIC o las que se encuentren vigentes y buenas prácticas en la materia.

Después se debe determinar la probabilidad de ocurrencia, en donde se establece la frecuencia con la que se ha presentado o puede presentarse el riesgo cuando no existen controles. Se mide en términos de la factibilidad o frecuencia con que el riesgo se podría llegar a materializar, teniendo en cuenta la presencia y exposición ante factores internos y externos. De acuerdo con un análisis cualitativo, se selecciona el grado de probabilidad de ocurrencia, en la ANH contamos con el software SIGECO en donde se establece la siguiente escala de probabilidad:

Probabilidad del riesgo:

Descripción	Frecuencia	Concepto
El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años. Para el tema de seguridad de la información aplica Menos de una vez cada 10 años.	SI ◉
El evento puede ocurrir en algún momento	Al menos de 1 vez en los últimos 5 años. Para el tema de seguridad de la información aplica Desde una vez cada 10 años hasta una vez cada 5 años	SI ○
El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años. Para el tema de seguridad de la información aplica Desde una vez cada 5 años hasta una vez cada año	SI ○
El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año. Para el tema de seguridad de la información aplica Desde un (1) evento/año hasta tres (3) eventos/año	SI ○
Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año. Para el tema de seguridad de la información aplica Más de tres (3) veces por año	SI ○

Fuente: Software SIGECO.

Una vez establecida la probabilidad se debe establecer el Impacto **antes de Controles** en donde se establece la magnitud de los efectos ocasionados con la materialización del riesgo cuando no existen controles. En el software SIGECO se establecen los siguientes criterios para determinar el impacto:

INSIGNIFICANTE (1)		
Descripción	**Tipo de impacto**	
Se tendrían que realizar ajustes a una actividad concreta del proceso.	Operativo	SI ○
Se afecta a una persona en particular	Confidencialidad de la Información	SI ○
Se afecta al grupo de funcionarios y contratistas del proceso.	Credibilidad o Imagen	SI ○
Se producen multas para la entidad.	Legal	SI ○

Fuente: Software SIGECO.

MENOR (2)		
Descripción	**Tipo de impacto**	
Se tendrían que realizar ajustes en los procedimientos del proceso.	Operativo	SI ○
Se afecta a un grupo de trabajo interno del proceso.	Confidencialidad de la Información	SI ○
Se afecta a todos los funcionarios y contratistas de la entidad.	Credibilidad o Imagen	SI ○
Se producen demandas para la entidad.	Legal	SI ○

MODERADO (3)		
Descripción	**Tipo de impacto**	
Se tendrían que realizar ajustes en la interacción de procesos.	Operativo	SI ○
Se afecta a los usuarios de la Sede Central de la entidad.	Credibilidad o Imagen	SI ○
Se producen investigaciones disciplinarias	Legal	SI ○
Se afecta a todo el proceso	Confidencialidad de la Información	SI ◉

MAYOR (4)		
Descripción	**Tipo de impacto**	
Se presentarían intermitencias o dificultades en la operación del proceso	Operativo	SI ○
Se afecta a los usuarios de las Direcciones Territoriales	Credibilidad o Imagen	SI ○
La afectación se da a nivel estratégico.	Confidencialidad de la Información	SI ○
Se producen investigaciones fiscales	Legal	SI ○

CATASTRÓFICO (5)		
Descripción	**Tipo de impacto**	
Se presentaría paro o no operación del proceso.	Operativo	SI ○
Se afecta a los usuarios de la Sede Central y de las Direcciones Territoriales.	Credibilidad o Imagen	SI ○
La afectación se da a nivel institucional	Confidencialidad de la Información	SI ○
Se producen intervenciones y o sanciones para la entidad por parte de un Ente de control u otro Ente regulador.	Legal	SI ○

Fuente: Software SIGECO.

En cuanto a **riesgos de seguridad de la información y seguridad digital**, se adoptan las siguientes tablas de referencia para establecer la probabilidad y el impacto, para lo cual debe tenerse en cuenta que la probabilidad e impacto se determinan con base en la amenaza, no en las vulnerabilidades:

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 podrá 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.

Imagen: Tabla de Probabilidad
Fuente: Guía de Administración de riesgos de gestión, corrupción y seguridad digital

Criterios de impacto para características de seguridad de la información

Nivel asignado	Valor del impacto	Integridad (I)	Disponibilidad (D)	Confidencialidad (C)	Tecnológico (T)	Reputacionales (R)	Cumplimiento (CU)	Operativos (O)	Social (S) Por ser entidad pública, la tolerancia es baja	Económica (E) Por tratarse de recursos públicos, la tolerancia es baja	Ambiental (A)
Insignificante	1	Sin afectación de la integridad	Sin afectación de la disponibilidad	Sin afectación de la confidencialidad	Se afecta a un usuario en particular.	Se afecta a un servidor o colaborador del proceso	Se producen amonestaciones verbales para la entidad	Se tendrían que realizar ajustes a una actividad concreta del proceso.	Afectación de hasta el 0,01% de la población objetivo	Sin afectación económica o no supera el valor de la caja menor	Sin Afectación medioambiental
Menor	2	Afectación leve de la integridad	Afectación leve de la disponibilidad	Afectación leve de la confidencialidad	Se afecta a un grupo de trabajo interno del proceso.	Se afecta a un grupo de servidores y colaboradores del proceso	Se producen amonestaciones escritas o demandas para la entidad.	Se tendrían que realizar ajustes en los procedimientos del proceso.	Afectación mayor al 0,01% hasta el 1 % de la población objetivo	Afectación desde el valor de la caja menor hasta el 4,99 % de la menor cuantía**	Afectación leve del MA requiere de hasta 1 semana de recuperación
Moderado	3	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	Se afecta a todo el proceso.	Se afecta a todos los servidores y colaboradores del proceso	Se producen investigaciones disciplinarias.	Se tendrían que realizar ajustes en la interacción de procesos.	Afectación mayor al 1% hasta el 4% de la población objetivo	Afectación desde el 5% de la menor cuantía** hasta el 0,1 % del presupuesto anual del área/ entidad	Afectación del MA requiere más de 1 hasta 3 meses de recuperación
Mayor	4	Afectación grave de la integridad de la información debido al	Afectación grave de la disponibilidad de la información debido al	Afectación grave de la confidencialidad de la información debido al interés particular de los	La afectación se da a nivel estratégico.	Se afecta a servidores y colaboradores de varios procesos	Se producen investigaciones fiscales.	Se presentarían intermitencias o dificultades en la operación del proceso	Afectación mayor al 4% y hasta el 20% de la población objetivo	Afectación mayor al 0,1% y hasta el 10 % del presupuesto anual del	Afectación del MA que requiere más de 3 meses hasta 2 años de recuperación

Editado por:	Revisado por:	Aprobado por:
NOMBRE: Laura Sierra Guerrero / Sandra Mireya Ramírez	NOMBRE: Cristian Javier Vargas del Campo	NOMBRE: Cristian Javier Vargas del Campo
CARGO: Contratista / Experto G3-5 Asesor	CARGO: Gerente de Planeación	CARGO: Gerente de Planeación

Criterios de impacto para características de seguridad de la información

Nivel asignado	Valor del impacto	Integridad (I)	Disponibilidad (D)	Confidencialidad (C)	Tecnológico (T)	Reputacionales (R)	Cumplimiento (CU)	Operativos (O)	Social (S) Por ser entidad pública, la tolerancia es baja	Económica (E) Por tratarse de recursos públicos, la tolerancia es baja	Ambiental (A)
		interés particular de los empleados y terceros	interés particular de los empleados y terceros	empleados y terceros						área/ entidad	
Catastrófico	5	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 confidencialidad de la información debido al interés particular de los empleados y terceros	La afectación se da a nivel institucional.	Se afecta a todos los servidores y colaboradores de la entidad.	Se producen intervenciones y o sanciones para la entidad por parte de un Ente de control u otro Ente regulador.	Se presentaría paro o no operación del proceso.	Afectación mayor al 20% de la población objetivo	Afectación mayor al 10 % del presupuesto anual del área/ entidad	Afectación del MA que requiere más de 2 años de recuperación

**según los parámetros establecidos en el Art. 2. Núm. 2 Lit. b. Ley 1150 de 2007.

Imagen: Tabla de Impacto
Fuente: Adaptación a partir de tablas del Modelo de Gestión de Riesgos de Seguridad Digital, MINTIC y Función Pública

El nivel de impacto será determinado con la presencia de cualquiera de los criterios, por lo que se debe tomar el que permita mejor asociación o defina mejor la afectación, ya sea cualitativa o cuantitativamente. Es importante dejar plasmado qué criterio se usó y al cambiar vigencias, cuáles fueron los valores de referencia para el caso del criterio social y económico. A continuación, aspectos a tener en cuenta para mejor claridad de algunos criterios.

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.

Imagen: Información de variables de impacto
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V5

Zona de Riesgo Inherente

Una vez establecida la probabilidad de ocurrencia del riesgo y su impacto, se determinará la zona de riesgo inicial o riesgo inherente. Este tipo de riesgo se entiende como aquel que existe de manera intrínseca en las actividades del proceso y permanecería así si no se toma ninguna acción para alterar la probabilidad o impacto por medio de los controles.

Zona de Riesgo	Color	Descripción
Baja		Genera menores efectos que pueden ser fácilmente remediados
Moderada		Se administra con procedimientos normales de control
Alta		Se requiere una pronta atención

Zona de Riesgo	Color	Descripción
Extrema-Critica		Se requiere una acción inmediata

Tabla: Clasificación del Riesgo
Fuente: Software SIGECO.

4.6.7. EVALUACIÓN DEL RIESGO

Permite comparar los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición de la entidad al mismo; de esta forma es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento.

Para facilitar la calificación y evaluación a los riesgos, a continuación, se presenta una matriz que contempla un análisis cualitativo, para presentar la magnitud de las consecuencias potenciales (impacto) y la posibilidad de ocurrencia (probabilidad).

	Insignificante	Menor	Moderado	Mayo	Catastrofico
Rara vez	BAJA 2	BAJA 3	MODERADA 0	ALTA 0	ALTA 0
Improbable	BAJA 0	BAJA 1	MODERADA 0	ALTA 0	EXTREMA 0
Posible	BAJA 0	MODERADA 0	ALTA 0	EXTREMA 0	EXTREMA 0
Probable	MODERADA 0	ALTA 0	ALTO 0	EXTREMA 0	EXTREMA 0
Casi seguro	ALTA 0	ALTA 0	EXTREMA 0	EXTREMA 0	EXTREMA 0

Imagen: Matriz de Calor - Riesgo Inherente
Fuente: Software SIGECO.

Para los riesgos seguridad de la información y seguridad digital:

Teniendo en cuenta la herramienta informática con la que cuenta la Entidad para la gestión de riesgos de seguridad de la información y seguridad digital, se adopta la siguiente matriz[27] de calor producto de combinación de probabilidad e impacto generando la criticidad del riesgo:

			Impacto				
			Insignificante	Menor	Moderado	Mayor	Catastrófico
			1	2	3	4	5
Probabilidad	1	Raro					
	2	Improbable					
	3	Posible					
	4	Probable					
	5	Casi Seguro					

Imagen: Matriz de Calor
Fuente: Software GPSecure

La valoración establecida y la criticidad podrá se actualizada y/o complementada según cambios organizativos, normativos y demás situaciones que lo ameriten.

4.6.8. DEFINICIÓN DE CONTROLES

Los controles son mecanismos que permiten mitigar las causas que podrían ocasionar la materialización de un riesgo, mejorando así la gestión del riesgo y el aumento de la probabilidad de alcanzar los objetivos y metas. Por lo tanto, para definir de forma adecuada los controles es necesario tener en cuenta los siguiente:

Implementación:

- **Control Manual:** existe presencia o intervención de una persona en la acción del control.
- **Control Automático:** la acción de control la realiza una aplicación o sistema de manera automática a través de un sistema programado.

Tipo de control:

- **Control preventivo:** Acción orientada a eliminar o reducir las causas del riesgo para prevenir su probabilidad ocurrencia. Ejemplo: Capacitación y sensibilización al personal sobre riesgos, listas de chequeo de cumplimiento de requisitos.

- **Control detectivo:** Acción orientada a identificar los eventos cuando ocurren. Ejemplo: Bloqueo por superar los intentos fallidos de acceso al sistema, sistema de detección de intrusos o software antivirus.

- **Control correctivo:** Orientado a asegurar que se tomen las acciones necesarias para revertir un evento no deseado, luego de su materialización, por ende, ataca el impacto frente a la materialización del riesgo. Ejemplo: Recuperación de archivos a partir de copias de seguridad.

Atributos informativos: Permite formalizar y complementar su documentación

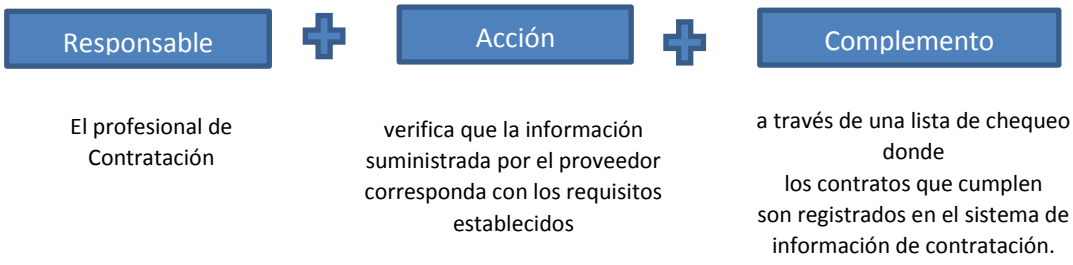
- Documentación (Documentado/Sin documentar)
- Frecuencia (Continua/Aleatoria)
- Evidencia[36]

Pasos para el diseño de controles

Con el fin de facilitar la adecuada redacción del control, se propone una estructura que permitirá entender su tipología y facilitará su valoración:

- **Responsable de ejecutar el control:** Identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.
- **Complemento:** corresponde a los detalles que permiten identificar claramente el objeto del control.

Ejemplo



En la descripción de los controles y su aplicación, es recomendable complementar con información relativa a la periodicidad y el soporte o evidencia de su ejecución. Así mismo, en la definición de los controles se deben

[36] Se debe propender porque el control cuente con evidencia de su ejecución

considerar los aspectos que permitan un diseño adecuado y que permitan su valoración respecto a la mitigación del riesgo[37].

Para la gestión de **riesgos de seguridad de la información y seguridad digita**l, se tomarán como base los controles basados en la norma vigente ISO/IEC 27001[38] y su Anexo A vigente; sin embargo, se podrán implementar nuevos controles de seguridad buscando que sean efectivos y eficaces para disminuir la probabilidad o el impacto del riesgo.[39] Es importante tener en cuenta que una actividad de control debe apuntar a mitigar la causa y, que una política por sí sola NO es un control.

4.6.9. VALORACIÓN DEL RIESGO RESIDUAL

La valoración del riesgo residual es el producto de confrontar los resultados de la evaluación del riesgo inherentes con los controles identificados.

Para la aplicación de los controles se debe tener en cuenta la naturaleza del control ya que esto es lo determinará si el control está enfocado en mitigar la probabilidad o el impacto del riesgo.

Mapa riesgo inherente

	Moderado	Mayor	Catastrófico
Rara vez	BAJA 0	BAJA 0	MODERADA 0
Improbable	BAJA 0	MODERADA 0	ALTA 0
Posible	MODERADA 0	ALTA 0	EXTREMA 0
Probable	MODERADA 0	ALTA 0	EXTREMA 0
Casi seguro	MODERADA 0	ALTA 0	EXTREMA 0

Mapa riesgo residual

	Moderado	Mayor	Catastrófico
Rara vez	BAJA 0	BAJA 0	MODERADA 0
Improbable	BAJA 0	MODERADA 0	ALTA 0
Posible	MODERADA 0	ALTA 0	EXTREMA 0
Probable	MODERADA 0	ALTA 0	EXTREMA 0
Casi seguro	MODERADA 0	ALTA 0	EXTREMA 0

Imagen: Mapa de Calor – Riesgo Inherente y Residual
Fuente: Aplicativo SIGECO

[37] Se recomienda consultar el capítulo de valoración de controles de la Guía de Administración del riesgo y el diseño de controles en entidades públicas – Riesgos de Gestión, Corrupción y Seguridad Digital v5-2020 o la que se encuentre vigente
[38] La norma ISO 27001 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización, se debe validar la versión vigente.
[39] Adaptado del Anexo 4 del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información v4-2021

Para los riesgos de seguridad de la información y seguridad digital:

La zona de riesgos permitirá establecer los pasos a seguir para el tratamiento de los riesgos:

Zona de Riesgo	Color	Descripción
Baja		Requiere monitoreo y seguimiento a través de actividades propias de la entidad y preferiblemente acciones de detección y prevención
Moderada		Se requiere medida a mediano plazo y adecuada, que permita disminuir los riesgos asociados a la seguridad digital
Alta		Se requiere una acción rápida, a corto plazo, por parte de la alta dirección para disminuir los riesgos asociados a la seguridad digital
Extrema		Se requiere una acción inmediata, para evitar la materialización de los riesgos asociados a la seguridad digital

NOTA: Siempre que el impacto sea valorado en nivel 4 (Mayor) se recomienda aplicar el tratamiento de Nivel Alto y, siempre que el impacto sea valorado en nivel 5 (Catastrófico) se recomienda aplicar el tratamiento de Nivel Extremo

Tabla: Zona de Riesgo

Fuente: Guía para la orientación de la GRSD en el Gobierno Nacional Entes Territoriales y Sector Publico

Las acciones a plantear se deben alinear con lo establecido en el Nivel de Aceptación del Riesgo.

4.6.10. TRATAMIENTO DEL RIESGO

El resultado obtenido a través de la valoración del riesgo es denominado también tratamiento del riesgo, ya que se "involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales acciones" así el desplazamiento dentro de la Matriz de Evaluación y Calificación determinará finalmente la selección de la opción de tratamiento del riesgo, así:

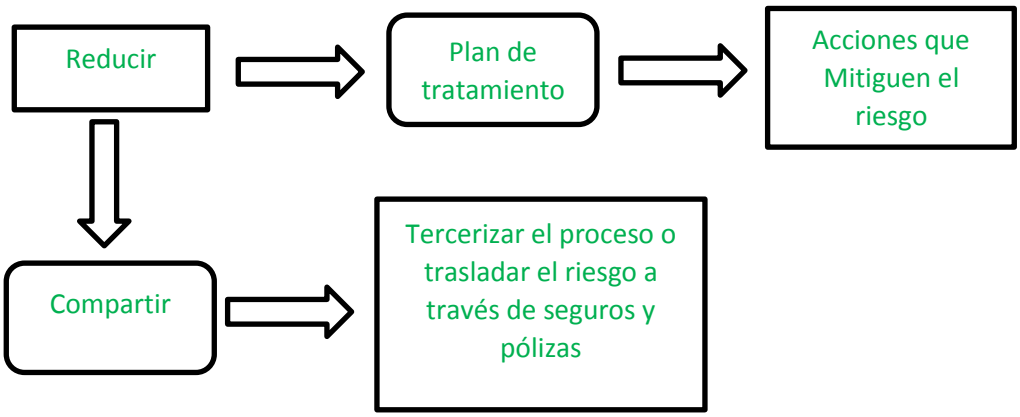


Imagen: tratamiento de riesgo

Fuente: Autoría propia

Aceptar: Después de realizar un análisis y considerar los niveles del riesgo, se determina asumir el mismo conociendo los efectos de su posible materialización. Generalmente, no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. Se recomienda consultar el campo Nivel de aceptación.

Reducir: Después de realizar un análisis y considerar que su nivel es alto se determina tratarlo mediante transferencia o mitigación del mismo. Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.

Compartir: Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.

Evitar: Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo. Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

Se considera el tratamiento de riesgos al proceso para modificar el riesgo[40], el cual no debe confundirse con el plan de contingencia, ya que este hace parte del Plan de Continuidad -BCP que, al igual que el Plan de Recuperación ante Desastres - DRP, se enmarcan como controles correctivos.

Cuando se decide reducir el riesgo, se debe especificar la acción, responsable, fecha de implementación/frecuencia y seguimiento. La Línea estratégica debe brindar los recursos para el tratamiento de los riesgos.

Al establecer el plan de tratamiento, se debe considerar la definición medidas de desempeño o indicadores por proceso, los cuales deben ser revisados por la línea estratégica - mínimo un (1) indicador de eficacia que indique el cumplimiento y uno (1) de efectividad -[41].

4.6.11. MONITOREO Y REVISIÓN

A través de las Tres Líneas de Defensa se debe realizar el monitoreo y revisión a la efectividad de los planes de tratamiento, determinando si se requieren actualizaciones, ajustes a los controles, cumplimiento de lo propuesto y evaluar la disminución o no del nivel del riesgo, con el fin de generar las recomendaciones para mejorar la gestión, así como la eficiencia y eficacia de los controles[42]. Los riesgos aceptados siempre serán susceptibles de monitoreo.

El responsable de seguridad de la información y seguridad digital, en lo pertinente, supervisará y acompañará el proceso de implementación de los planes de tratamiento, verificando que los responsables den cumplimiento a lo establecido en los mismos.

40 NTC GTC137, Numeral 3.8.1.
[41] Consultar Guía para la administración del riesgo y el diseño de controles en entidades públicas V5 o la que se encuentre vigente
[42] Anexo 4 del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información v4-2021

La periodicidad de monitoreo y revisión será la definida en el Nivel de aceptación respectiva (Riesgos de gestión y corrupción agregar eso) reportando las desviaciones al Comité de Gestión Institucional y Desempeño o el que haga sus veces.

4.6.12. MECANISMOS DE SEGUIMIENTO Y MEDICIÓN

Para realizar el seguimiento a las acciones de respuesta y efectividad en cuanto a riesgos de gestión y de corrupción, se tendrá como herramienta de seguimiento y gestión el Software SIGECO, tarea que se realizará junto con los facilitadores de proceso.

Para la gestión de riesgos de seguridad de la información y seguridad digital, dada su especificidad, se utilizará la herramienta informática disponible o los instrumentos definidos y normalizados para tal fin.

Conforme lo definido en los lineamientos, se utilizarán los indicadores establecidos en plan de tratamiento como medida de desempeño[43].

4.6.13. REPORTE DE LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

Con el propósito de consolidar la información relevante para su respectivo reporte a las autoridades o instancia que el Gobierno defina[44], los procesos deberán remitir al área o Responsable de seguridad de la información y seguridad digital, los activos identificados, vulnerabilidades, amenazas, riesgos, planes de tratamiento y servicios digitales críticos. Igualmente, las infraestructuras críticas cibernéticas -ICC- que hayan sido identificadas deben reportarse a las autoridades o instancias encargadas del tema en el Gobierno nacional, según como estas lo indiquen[45].

A nivel interno, se reportará al Comité de Gestión Institucional y Desempeño o el que haga sus veces, según agenda o requerimientos.

En la presentación de información se deberá considerar su respectiva clasificación (confidencial, clasificada o reservada) evitando exponer información sensible[46].

Todos los servidores públicos y colaboradores de la Entidad deben reportar si tienen conocimiento de la posible materialización de un riesgo a sus respectivos líderes de proceso, así como de la ocurrencia de un posible evento de seguridad de la información o seguridad digital -incluyendo los asociados al tratamiento de datos personales-, a través de la Mesa de Servicios de la Oficina de Tecnologías de la Información.

[43] Conforme Anexo 4 del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información v4-2021, Guía 16 de Evaluación del Desempeño v1-2017, Guía 9 de indicadores de Gestión para la Seguridad de la Información v3-2015 o las que se encuentren vigentes
[44] Para la generación de política pública, capacidades o asignación de recursos, así como la toma de decisiones.
[45] Anexo 4 del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información v4-2021, Guía 16 de Evaluación del Desempeño v1-2017, Guía 9 de indicadores de Gestión para la Seguridad de la Información v3-2015 o las que se encuentren vigentes
[46] Conforme lo indicado en la Guía 5 para la Gestión y Clasificación de Activos de Información que lo clasifica como Confidencial.

4.6.14. AUDITORÍAS

Le corresponde a las Unidades de Control Interno realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo conforme al Plan Anual de Auditoría aprobado por el Comité Institucional de Coordinación de Control Interno de la entidad.

La Oficina de Control Interno (tercera línea de defensa) debe realizar esta misma evaluación sobre la gestión del riesgo de seguridad de la información/seguridad digital, catalogándola como una unidad auditable más dentro de su Universo de Auditoría[47].

4.6.15. MEJORA CONTINUA

Se deben revisar y evaluar los hallazgos tanto de auditorías como de entes de control; así como, las falencias y los incidentes de seguridad de la información y seguridad digital, con el fin de definir acciones para la mejora continua de la gestión de riesgos[48]. Es importante documentar este tratamiento a fin de retroalimentar el proceso.

5. POLÍTICA DE ADMINISTRACIÓN DE OPORTUNIDADES DE MEJORA.

La Oportunidad de Mejora, es un elemento fundamental en el desarrollo de los Sistemas de Gestión y se entienden como todas aquellas situaciones convenientes que le permiten a la organización obtener o maximizar resultados favorables frente al cumplimiento de su gestión, logro de resultados, mejora de los productos y servicios, mejorar la satisfacción de las partes interesadas o mejorar la imagen institucional.

5.1. OBJETIVO

Establecer los parámetros necesarios para una adecuada identificación y gestión de las oportunidades de mejora del Sistema de Gestión Integral y Control de la ANH.

[47] Conforme Anexo 4 del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información v4-2021 o la que se encuentre vigente
[48] Ibidem

5.2. METODOLOGÍA PARA LA IDENTIFICACIÓN DE OPORTUNIDADES DE MEJORA

Las oportunidades de mejora son todas aquellas situaciones favorables que pueden ayudar a la organización a cumplir resultados previstos, mejorar la gestión, reducir riesgos y mejorar la satisfacción de las partes interesadas.

5.2.1. IDENTIFICACIÓN

Para la identificación se deben tener en cuenta las diferentes fuentes o elementos de entrada como el análisis del contexto interno y externo, las necesidades y expectativas de las partes interesadas y el análisis de indicadores.

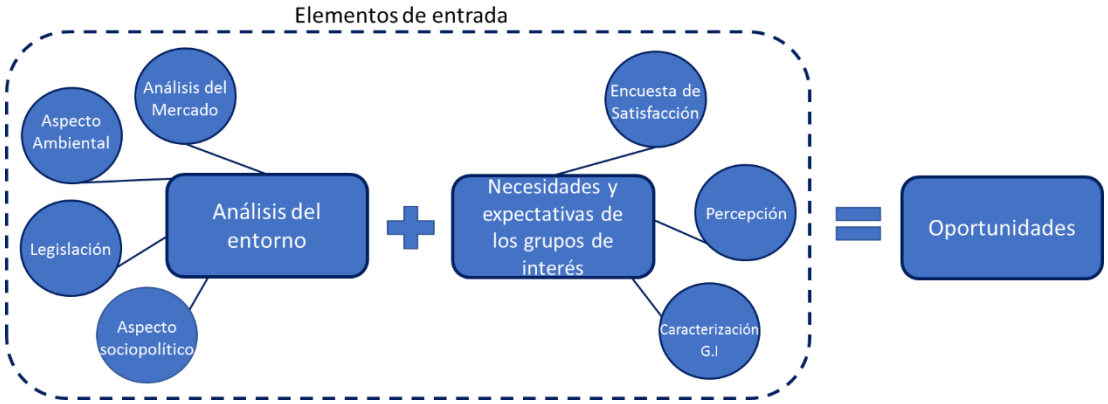


Imagen: Nombre imagen
Fuente: Fuente imagen

Las oportunidades se deben registrar en la matriz de identificación y gestión de oportunidades, la cual se encuentra disponible en SIGECO, allí se debe consignar lo siguiente:

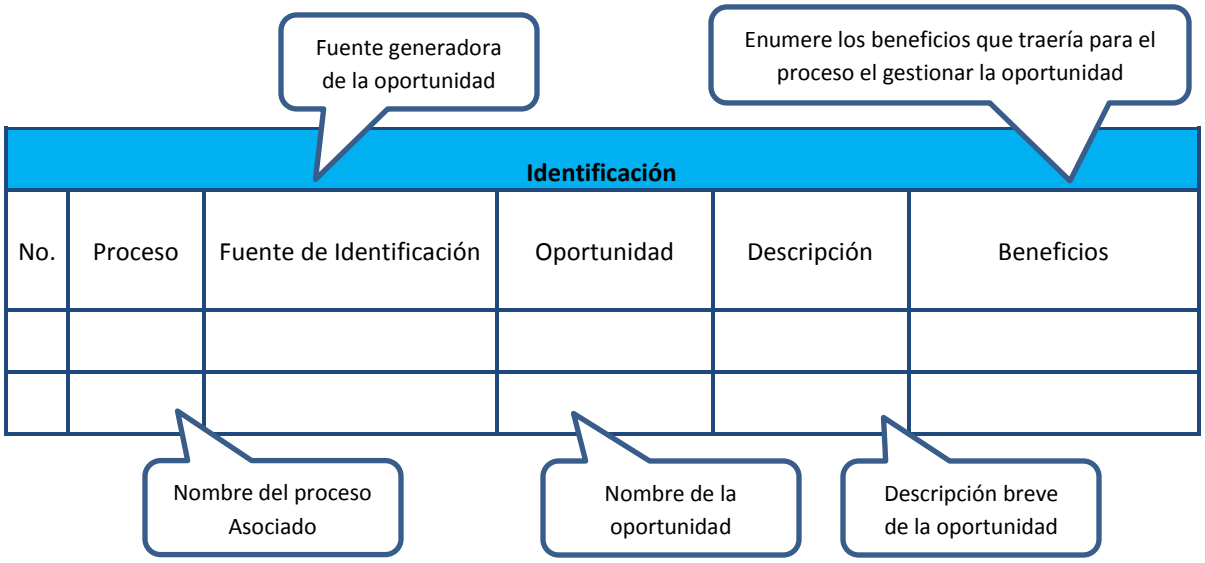


Imagen: Matriz de Identificación de Oportunidades
Fuente: Autoría Propia

5.2.2. VALORACIÓN

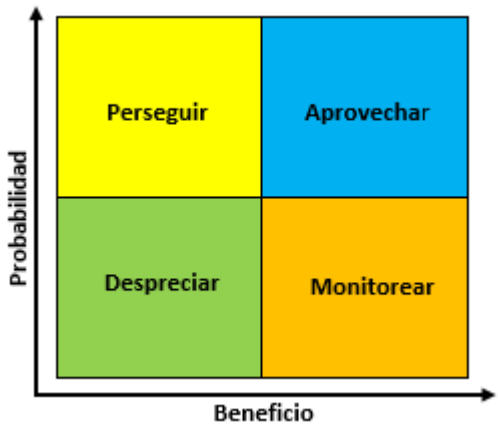
En este paso las oportunidades se valoran teniendo en cuenta dos parámetros principales que determinan su nivel de impacto en la organización. Las cuales parten de la **probabilidad** que la entidad tiene de gestionar la oportunidad y el **beneficio** que traería para la organización su implementación en diferentes frentes de la gestión institucional como impacto en la cadena de valor, innovación, satisfacción de las partes interesadas, mejora de procesos internos y mejora de la imagen.

Valoración de oportunidades							
Probabilidad	Rara	1	Puede darse solo en circunstancias excepcionales	**Beneficio**	Muy bajo	1	Representaría un beneficio casi nulo para la entidad.
	Improbable	2	Es probable que no suceda en la mayoría de las circunstancias		Bajo	2	Traería un beneficio bajo para la entidad
	Posible	3	Es posible que suceda bajo cualquier circunstancia		Moderado	3	Traería un beneficio moderado para la entidad
	Probable	4	Puede que suceda bajo cualquier circunstancia		Alto	4	Representa un benéfico alto para la entidad
	Casi seguro	5	Se espera que suceda		Muy alto	5	Impactaría positivamente la entidad y su gestión

Imagen: Valoración de oportunidades
Fuente: Autoría propia

5.2.3. CLASIFICACIÓN DE LA OPORTUNIDAD

Una vez valorada la oportunidad, bajo los parámetros establecidos, se procederá a clasificar la oportunidad según su grado de probabilidad y beneficio.



Fuente: Valoración de Oportunidad

Despreciar: Oportunidades de mejora que no son de gran impacto para la entidad.
Monitorear: Oportunidades que ofrecen un alto beneficio pero que su probabilidad de ocurrencia en baja. Se debe hacer seguimiento para aprovechar ya que son susceptibles de cambio de cuadrante.
Perseguir: Oportunidades que tienen una probabilidad alta de ejecución, pero su beneficio es bajo. Se deben evaluar la necesidad de ejecución teniendo en cuenta las capacidades institucionales
Aprovechar: Son oportunidades que presentan un beneficio y probabilidad alta por lo tanto su ejecución en obligatoria.

La clasificación es generada automáticamente por la matriz de identificación y gestión de oportunidades. En ella se diagrama el cuadrante en el que quedo ubicada la oportunidad según los datos ingresados por el usuario.

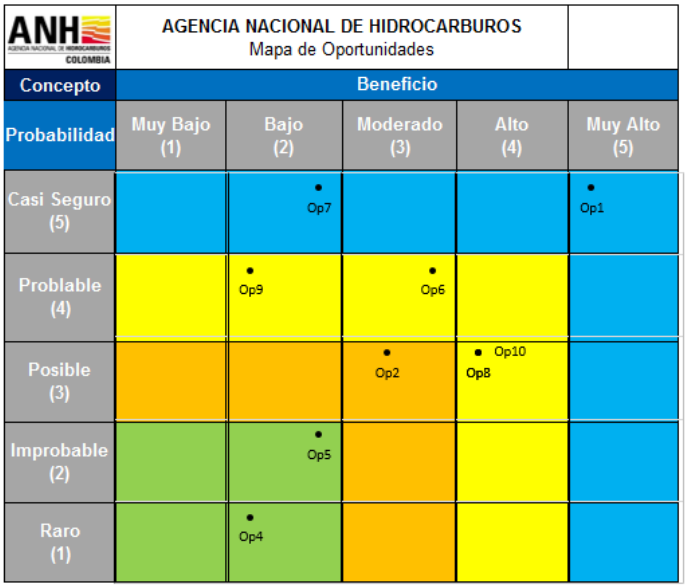


Imagen: Mapa de Oportunidades
Fuente: Autoría propia

Para aquellas oportunidades que están clasificadas en el cuadrante Aprovechar (Azul), será obligatorio realizar un plan de mejora encaminado a obtener los beneficios que trae para la organización la implementación de la oportunidad. Para ello se deberá consignar en la matriz de identificación y gestión de oportunidades lo siguiente:

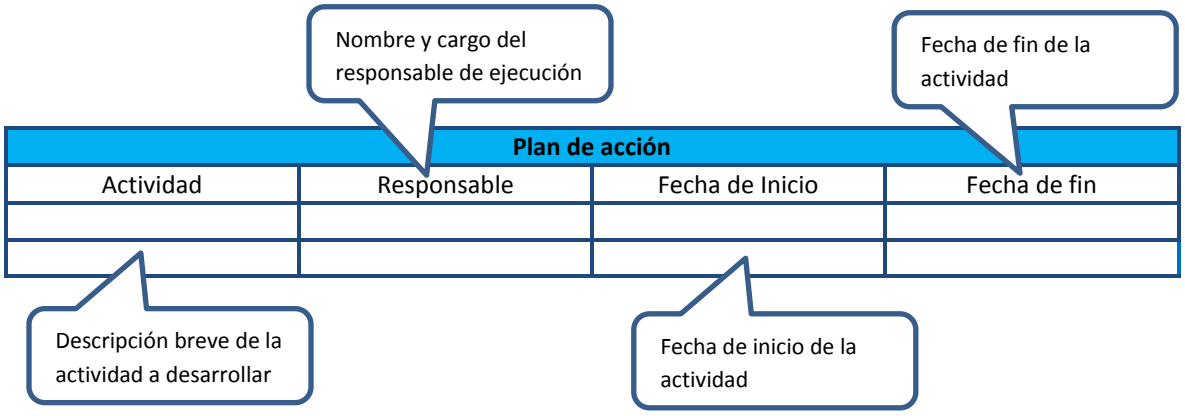


Imagen: Matriz de Identificación de Oportunidades
Fuente: Autoría Propia

Una vez consignada esta información en la matriz de identificación y gestión de oportunidades, será necesario formalizar el plan de mejoramiento en el aplicativo SIGECO, módulo de mejora. Para ello se seleccionará como fuente generadora del plan Análisis de oportunidades de mejora

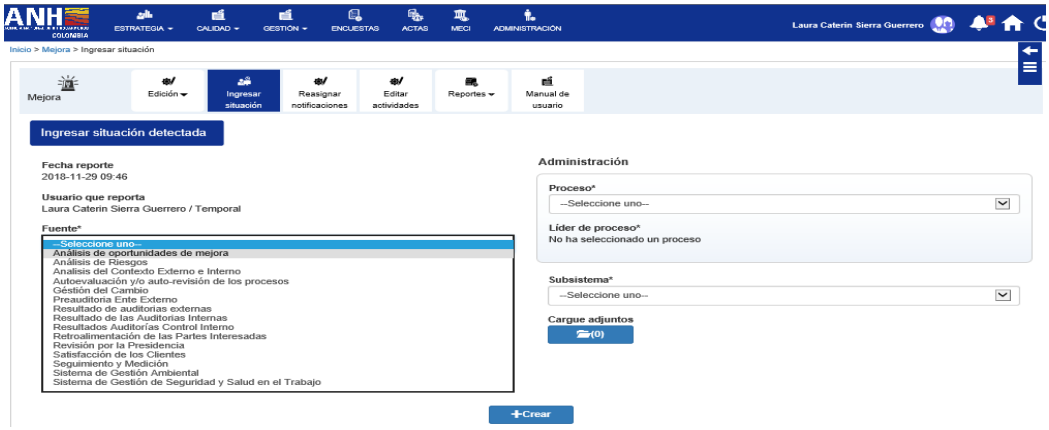


Imagen: Registro de Planes SIGECO
Fuente: SIGECO

6. BIBLIOGRAFIA.

- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN -ICONTEC. Norma Técnica Colombiana NTCISO31000. 2011
- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN -ICONTEC. HB 141 Guía para la Financiación del Riesgo. 2008.
- ISO TOOLS EXCELLENCE. Como integrar COSO, COBIT e ISO 27001. Tomado de: https://www.pmg-ssi.com/2016/10/como-integrar-coso-cobit-e-iso-27001/
- PRICEWATERHOUSECOOPERS. Administración de Riesgos Corporativos. 2005.
- CASALS & ASSOCIATES INC, PRICEWATERHOUSECOOPERS, USAID, Documento Mapas de Riesgo, octubre 2003.
- CASALS & ASSOCIATES INC USAID; Marco Conceptual, Programa Fortalecimiento de la Transparencia y la Rendición de Cuentas en Colombia. 2004.
- CEPEDA, GUSTAVO. Auditoría y Control Interno. McGraw Hill, 1997.
- DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA, Riesgos de Corrupción en la Administración Pública, Tercer Mundo, 2015.
- JIMENEZ, ENRIQUE Y MARTÍN, JOSÉ. El nuevo acuerdo de Basilea y la gestión de riesgo operacional. Universidad Business Review.2005.
- Guías, Manuales, Resoluciones y Decretos vigentes del Modelo de Seguridad y Privacidad de la Información – MSPI y Modelo de Gestión de Riesgos de Seguridad Digital - MGRSD emitidos por MINTIC
- Buenas prácticas vigentes en Seguridad y Privacidad de la Información (Normas ISO)

7. DOCUMENTOS ASOCIADOS

- ANH-GES-FR-01Matriz de identificación y valoración de oportunidades.
- ANH-GES-FR-02 - Matriz de Riesgos de Seguridad de la Información Digital.
- ANH-GES-FR-03 – Matriz de Inventario y Clasificación de Activos de Información.
- Glosario de Términos y Definiciones de Seguridad y Privacidad de la Información.

8. CONTROL DE CAMBIOS

FECHA	MOTIVO DEL CAMBIO	VERSIÓN
28/08/2018	Implementación	1
25/09/2018	Se incluye la Gestión de Oportunidades	2
29/11/2018	Se modifica la metodología de identificación y gestión de oportunidades	3
30/03/2020	Se incluye el nivel de aceptación de riesgo y diseño de controles	4
21/02/2023	Se incluye la gestión de riesgos de seguridad de la información y seguridad digital. Actualización de la Guía según cambios en lineamientos	5

Editado por:	Revisado por:	Aprobado por:
NOMBRE: Laura Sierra Guerrero / Sandra Mireya Ramírez	NOMBRE: Cristian Javier Vargas del Campo	NOMBRE: Cristian Javier Vargas del Campo
CARGO: Contratista / Experto G3-5 Asesor	CARGO: Gerente de Planeación	CARGO: Gerente de Planeación