

INFORME DE SEGUIMIENTO A LA GESTIÓN DE RIESGOS EN LA AGENCIA NACIONAL DE CONTRATACIÓN PÚBLICA - COLOMBIA COMPRA EFICIENTE
 Junio a noviembre de 2022

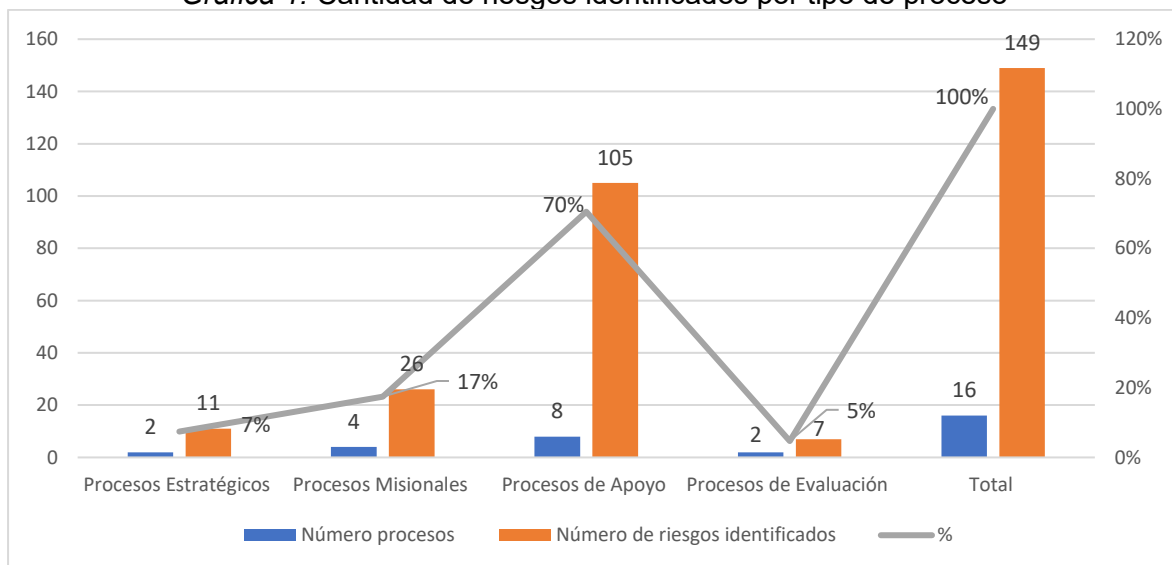
El Asesor(a) Experto(a) con Funciones de Control Interno, juntamente con el equipo de trabajo, en cumplimiento de lo establecido en el Decreto 1499 de 2017 y en armonía con los roles de Liderazgo Estratégico y Enfoque hacia la Prevención asignados a las Oficinas de Control Interno o quienes hagan sus veces a partir del Decreto 648 de 2017, efectuó seguimiento a la gestión de riesgos de la Entidad, correspondiente al periodo comprendido entre junio a noviembre de 2022.

A continuación, se detalla el seguimiento en los literales a y b de este informe.

a) Contextualización de la Gestión de Riesgos en la Agencia Nacional de Contratación Pública – Colombia – Compra Eficiente ANCP-CCE durante el periodo evaluado

En cumplimiento de las etapas de identificación y valoración de riesgos, con corte a noviembre de la vigencia 2022, la Entidad identificó 149 riesgos de proceso, corrupción y seguridad digital, distribuidos entre los dieciséis (16) procesos que conforman el Mapa de Procesos vigente, publicado en la página web de la ANCP-CCE. En seguida se presenta la gráfica No. 1 que permite observar el número de riesgos identificados por tipo de proceso:

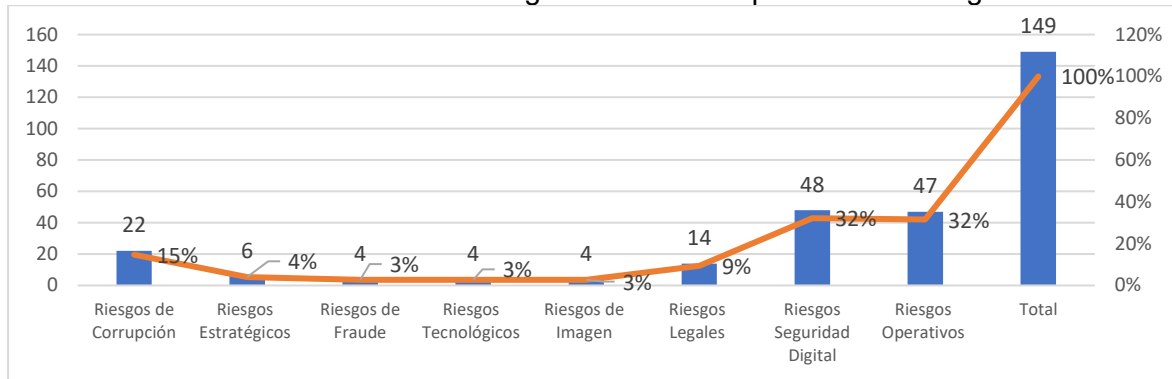
Gráfica 1. Cantidad de riesgos identificados por tipo de proceso



Fuente: Elaboración propia equipo de Control Interno con base en la información suministrada por la Segunda Línea de Defensa a noviembre de 2022 – Reporte Suite Empresarial

La gráfica No. 2, muestra que la mayor cantidad de riesgos identificados por parte de la Entidad corresponde a riesgos de seguridad digital con el 48%; en contraste, con los riesgos de fraude, tecnológicos y de imagen que presen tal el 4% del total de los riesgos.

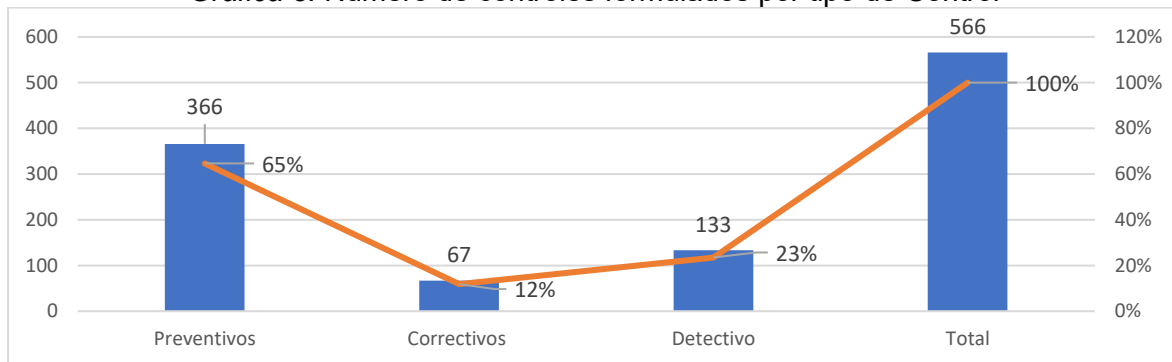
Gráfica 2. Número de riesgos identificados por clase de riesgo



Fuente: Elaboración propia equipo de Control Interno con base en la información suministrada por la Primera y Segunda Línea de Defensa Subdirección de Información y Desarrollo Tecnológico IDT a noviembre de 2022 – Reporte Suite Empresarial

Se definió un total de 566 controles para los 149 riesgos, de los cuales cuarenta y ocho (48) de estos, corresponde a los riesgos de seguridad digital, la gráfica No. 3 muestra el número de controles formulados, según tipo:

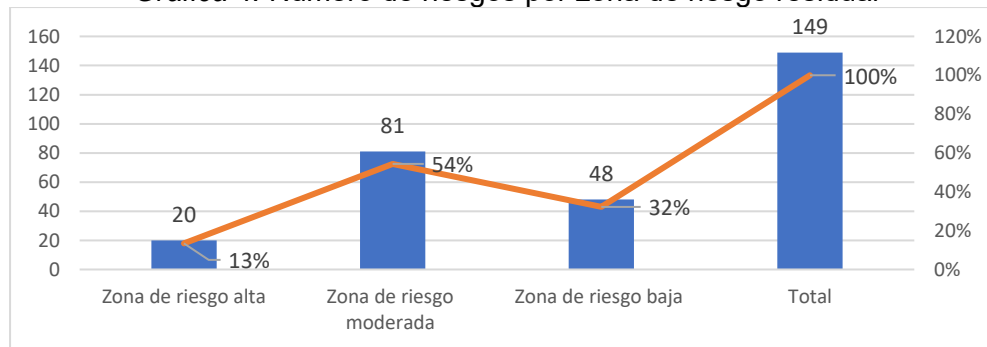
Gráfica 3. Número de controles formulados por tipo de Control



Fuente: Elaboración propia equipo de Control Interno con base en la información suministrada por la Segunda Línea de Defensa a noviembre de 2022- Reporte Suite Empresarial

Una vez evaluados los controles, en seguida se presenta la zona de riesgo residual donde se ubican los 149 riesgos identificados:

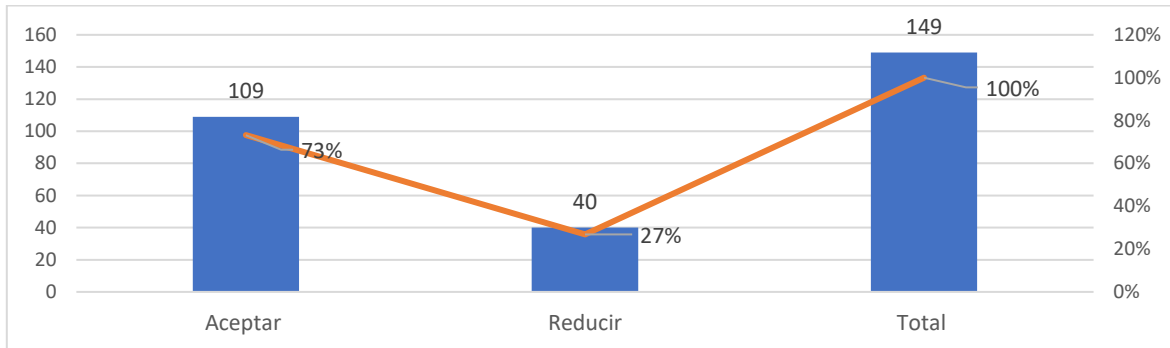
Gráfica 4. Número de riesgos por zona de riesgo residual



Fuente: Elaboración propia equipo de Control Interno con base en la información suministrada por la Segunda Línea de Defensa a noviembre de 2022 – Reporte Suite Empresarial

De conformidad con la tolerancia del riesgo definida por la ANCP-CCE en la Política del Sistema de Administración y Gestión de Riesgos se aceptaron el 87% de los riesgos identificados, como se presenta a continuación:

Gráfica 5. Tratamiento de riesgos en valoración residual



Fuente: Elaboración propia equipo de Control Interno con base en la información suministrada por la Primera y Segunda Línea de Defensa a noviembre de 2022 – Reporte Suite Empresarial

b. Resultados seguimiento a la gestión de riesgos en la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente ANCP-CCE

Verificados los soportes y demás evidencias que sustentaron la gestión de riesgos en la Entidad, a la luz de la aplicación de la Metodología para la Administración del Riesgo, y en cumplimiento de la Política del Sistema de Administración y Gestión de Riesgos de la ANCP-CCE, en el periodo comprendido entre junio a noviembre de 2022, se resalta lo siguiente:

- De los 149 riesgos residuales, treinta y cuatro (34) como calificados como “*Altos*” y “*Moderados*”, correspondiente al 23% que cuentan con plan de tratamiento y con definición de reducir el riesgo según información suministrada por la segunda línea de defensa incluida la Subdirección de Información y Desarrollo Tecnológicos IDT con los riesgos de seguridad digital, en el periodo evaluado.

Durante el período evaluado se materializaron los siguientes riesgos:

Tabla 1. Riesgos materializados

Proceso	Riesgo materializado	jun-22	jul-22	ago-22	sep-22	oct-22	nov-22	Total Materialización	Plan de Tratamiento
Servicio y Atención al Ciudadano	Inoportunidad en las respuestas de conceptos jurídicos de carácter general			1	1			2	No se evidencia plan de Tratamiento
	Inoportunidad en el cumplimiento de los términos legales de respuesta de las PQRSD					1		1	Se evidencia plan de Tratamiento

Proceso	Riesgo materializado	jun-22	jul-22	ago-22	sep-22	oct-22	nov-22	Total Materialización	Plan de Tratamiento
Operaciones SECOP	Disminución de los procesos y transacciones en las plataformas del sistema de compra pública					1		1	Se evidencia plan de Tratamiento
	Inoportunidad en el cumplimiento de los términos legales de respuesta de las PQRSD		1					1	Se evidencia plan de Tratamiento
Abastecimiento Estratégico	Inoportunidad en el cumplimiento de los términos legales de respuesta de las PQRSD			1				1	Se evidencia plan de Tratamiento
Normativa de la contratación	Inoportunidad en el cumplimiento de los términos legales de respuesta de las PQRSD			1	1			2	Se evidencia plan de Tratamiento
Total		0	1	3	2	2	0	8	

Fuente: Elaboración propia equipo de Control Interno con base en la información suministrada por la Primera y Segunda Línea de Defensa. Archivos cargados en TEAMS – RAE Seguimientos mensuales a los riesgos junio a noviembre de 2022.

Durante el periodo evaluado, no se observó la materialización de riesgos de corrupción.

Frente a los riesgos de seguridad digital de acuerdo con la información suministrada por la Subdirección de Información y Desarrollo Tecnológico IDT estos no se han materializado.

Se reitera que no se evidencia que se haya realizado el reporte de la gestión del riesgo de seguridad digital al interior de la Entidad como lo señala el numeral 4.3.2 del “Anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Pública”, de la “Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas” del DAFP V5”, así como lo definido en el numeral 4.1.4 relacionado con la definición de los roles.

Revisado el mapa de riesgos de seguridad digital, frente al “Anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Pública” se observó lo siguiente:

En contexto del proceso de Gestión de Información presenta fecha de elaboración 2/12/2020.

No se evidencia el alcance para aplicar la gestión de riesgos de seguridad digital.

Revisado los planes de tratamiento en SharePoint, se evidenciaron documentos preliminares, en los formatos Word y PowerPoint que no contienen información (en blanco) como por ejemplo el de los riesgos No. 41 y 44 “Clasificación activos de información”, “Procedimiento Gestión de Accesos”, para el riesgo No. 48 se encontró el documento “CCE-GTI-IDI-02 POLÍTICAS



INTERNAS DE NAVEGACIÓN EN INTERNET CORPORATIVO 17-09-2021 (1)”, y para los riesgos No. 46 y 38 el documento “Procedimiento Gestion de Accesos”.

En la matriz de riesgos de seguridad digital, no se evidenció que se identificaran los riesgos a partir de cada uno de los activos de información, se observó que se señala como “Grupo de activos” y se clasifican en “Información”, lo que no permite realizar el análisis de vulnerabilidades efectivamente. Lo anterior no cumple con los lineamientos definidos en el Anexo 4 citado anteriormente.

Al revisar la documentación enviada por la subdirección de IDT, no se evidenció el seguimiento a los riesgos definidos en la matriz remitida, como se comentó anteriormente la información en SharePoint no permite establecer el cumplimiento de las actividades del plan de tratamiento.

No se observó que dentro de la estructura de la subdirección de IDT, se haya constituido un grupo interno independiente de las demás actividades, que permita realizar la adecuada gestión de riesgos de seguridad digital.

Revisado el cumplimiento del Capítulo 5 de la Resolución 270 de 2021 frente al Subcomité Institucional de Coordinación del Sistema de Control, y el monitoreo de los riesgos que debe realizar la primera línea de defensa, se revisaron las actas de dichos espacios, encontrado lo siguiente:

Tabla 2. Realización Subcomités de Control Interno

Áreas	Fecha Subcomité	Observación
Dirección General	07/07/2022 06/10/2022	Sin novedad
Subdirección de Información y Desarrollo Tecnológico	29/06/2022 11/11/2022	Sin novedad
Subdirección de Estudios de Mercados y Abastecimiento Estratégico	07/06/2022 22/06/2022 25/07/2022 13/10/2022	Sin novedad
Subdirección de Negocios	19/07/2022 15/09/2022	No se evidencia el seguimiento a los riesgos, en el acta correspondiente al 15/09/2022.
Subdirección de Gestión Contractual	5/08/2022	Sin novedad
Secretaría General	23/06/2022	No se evidencia el seguimiento a los riesgos, en el acta correspondiente al 23/06/2022.

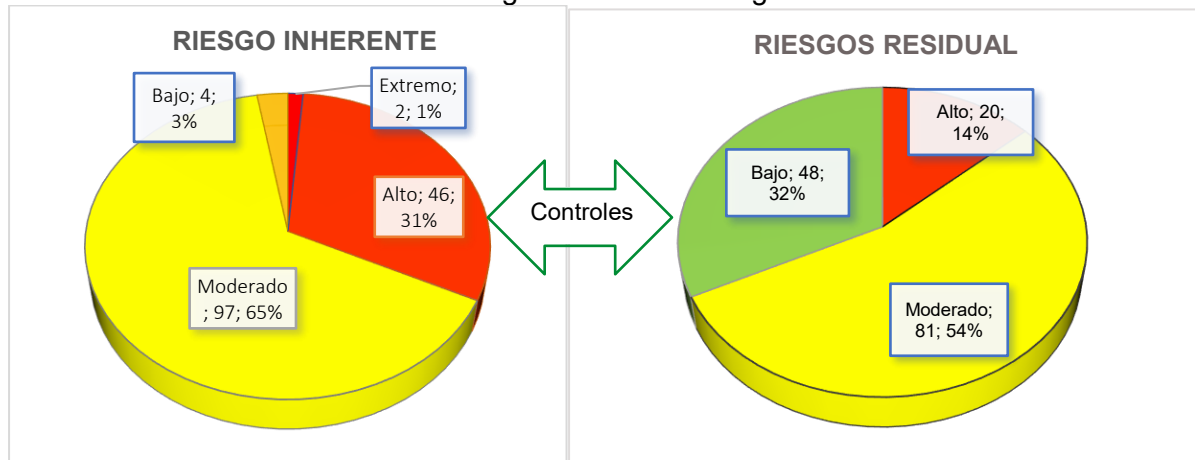
Fuente: Elaboración propia equipo de Control Interno con base en la información suministrada por la Primera Línea de Defensa junio a noviembre de 2022.

En el desarrollo del ejercicio de aseguramiento al Acuerdo Marco de Precios para el suministro, adquisición y dispensación de medicamentos, se evidencio la materialización de un riesgo no identificado en la matriz de riesgos del Proceso de Gestión de Agregación de Demanda - Procedimiento “Estructuración e Acuerdo Marco de Precios y otros Instrumentos de Agregación de Demanda. CCE-GAD-PLR-01 V7”, el cual no se reportó oportunamente en cumplimiento del Manual Metodológico de Administración de Riesgos V4 el cual hace parte de la Política del Sistema de Administración de Riesgo 2021.



A continuación, se presenta un comparativos de los riesgos inherentes frente a los residuales que muestran la valoración de los controles:

Gráfica 6. Riesgo Inherente - Riesgo Residual



Fuente: Elaboración propia equipo de Control Interno con base en la información suministrada por la Primera Línea de Defensa a noviembre de 2022.

No obstante, la situación identificada frente a la efectividad de los controles, se materializaron riesgos que requieren revisión y tratamiento.

Con ocasión al seguimiento realizado con corte a mayo de la vigencia 2022, en el periodo evaluado se identificaron avances en la gestión de riesgos tales como:

Uso de la “Suite VISIÓN EMPRESARIAL PENSEMOS” ha permitido que se adelante la gestión de riesgos de forma tal que permite evidenciar la trazabilidad de cada una de las etapas del tema evaluado.

En conclusión, el equipo de control interno evidenció exposición alta sobre los activos de información, debido a las debilidades identificadas frente a la gestión de riesgos de seguridad digital.

RECOMENDACIONES DE CONTROL INTERNO

Conforme el seguimiento efectuado a la gestión de riesgos en la ANCP-CCE, correspondiente al periodo comprendido junio a noviembre de 2022, el Asesor Experto con funciones de Control Interno recomienda:

1. Una vez evidenciado la materialización de riesgos por la primera línea de defensa, reportarlos oportunamente para el tratamiento correspondiente.
2. Revisar los riesgos de seguridad digital para que se ajusten a lo definido en el Modelo de Seguridad y Privacidad de la Información.
3. Los documentos que soportan la ejecución del plan de tratamiento de los riesgos de seguridad digital deben contener la información que se cita en el nombre del archivo, así como la trazabilidad del cumplimiento.

4. Documentar el monitoreo que se realiza a los riesgos de seguridad digital.
5. Revisar que el mapa de riesgos de seguridad digital se realice a partir de los activos de información definido por los líderes de proceso.
6. En el marco del de Modelo de Seguridad y Privacidad de la Información, definir los roles citados en el anexo No. 4 *“Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Pública”*, de la *“Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas” del DAFP V5*, así como la conformación del grupo interno para el desarrollo efectivo del modelo y los riesgos.
7. Se reitera realizar el reporte al interior de la entidad y línea estratégica de los riesgos de seguridad digital como lo cita el numeral 4.3.2 y definir formalmente los roles que establece el numeral 4.1.4 del Anexo No. 4.
8. Se reitera a la primera línea de defensa, fortalecer la realización de los Subcomités de Control Interno, a través de un adecuado monitoreo de los riesgos y el seguimiento a los puntos de control establecidos en cada una de las caracterizaciones de los procesos y a las demás herramientas de gestión, en cumplimiento de las funciones definidas en la Resolución 270 de 2021.
9. Como se ha señalado en diferentes evaluaciones, es necesario fortalecer el Esquema de Líneas de Defensa de manera permanente con el fin de consolidar la gestión de riesgos en la ANCP-CCE.

Aprobó: Judith Esperanza Gómez Zambrano
Asesora Experta con Funciones de Control Interno

Revisó: Judith Esperanza Gómez Zambrano
Asesora Experta con Funciones de Control Interno

Elaboró: Judith Esperanza Gómez Zambrano
Asesora Experta con Funciones de Control Interno

Jesús Gabriel Montoya Ramos
Analista

Diciembre 2022

Código Informe: 22 - 2



DEPARTAMENTO
NACIONAL DE PLANEACIÓN

Agencia Nacional de Contratación Pública - Colombia Compra Eficiente

Tel. [601] 7956600 • Carrera 7 No. 26 - 20 Piso 17 • Bogotá - Colombia



www.colombiacompra.gov.co