INFORME DE SEGUIMIENTO A LA GESTIÓN DE RIESGOS EN LA AGENCIA NACIONAL DE CONTRATACIÓN PÚBLICA - COLOMBIA COMPRA EFICIENTE
Junio a noviembre de 2023

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, efectúo seguimiento a la gestión de riesgos de la Entidad, correspondiente al periodo comprendido entre junio y noviembre de 2023.

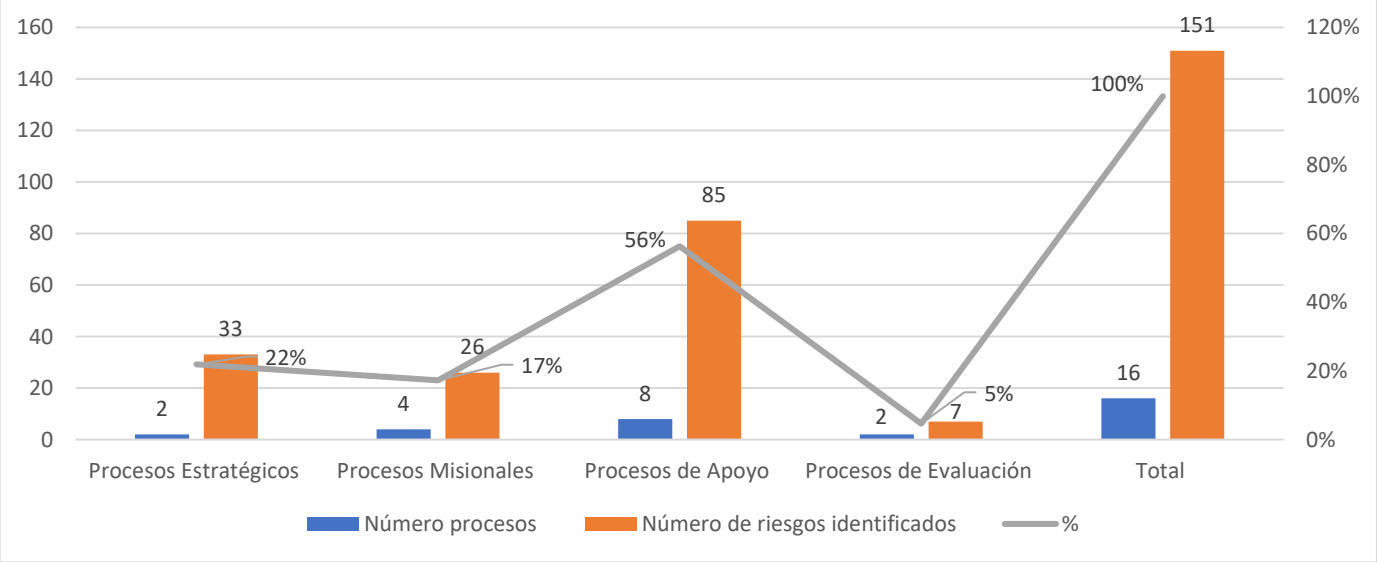
A continuación, se detalla el seguimiento en los literales a y b de este informe.

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, entre junio y noviembre de 2023, la Entidad identificó 151 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.

A continuación se presenta la gráfica No. 1 donde se permite observar el número de riesgos identificados por tipo de proceso:

Gráfica 1. Cantidad de riesgos identificados por tipo de proceso

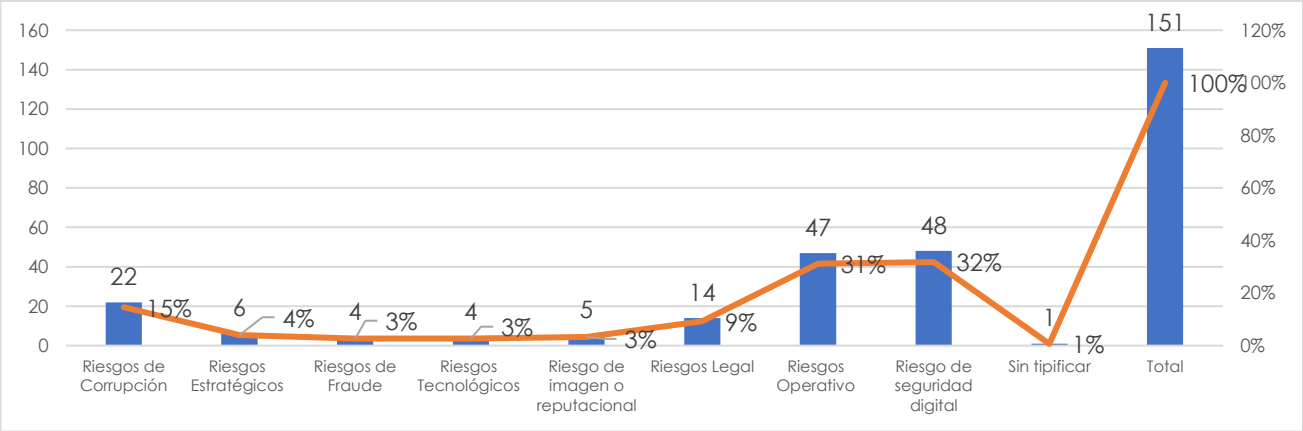


Fuente: Elaboración propia equipo de Control Interno con base en la información suministrada por la Segunda Línea de Defensa a noviembre de 2023 – Reporte Suite Empresarial

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 32%; en contraste, con los riesgos de fraude y tecnológicos que presentan el 3% del total de los riegos; es importante mencionar que teniendo en cuenta la matriz de riesgos por procesos descargada de la "*Suite Empresarial*" para los riesgos de gestión, se identificaron 103 riesgo y cotejado con la información suministrada por la segunda línea de defensa la cual reporta 102,

revisada la información se identificó que el riesgo denominado "*Perdida de la confidencialidad de la información almacenada en la nube por accesos no autorizados*" se encuentra en la matriz de riesgos de gestión y en la matriz de riesgos de seguridad digital.

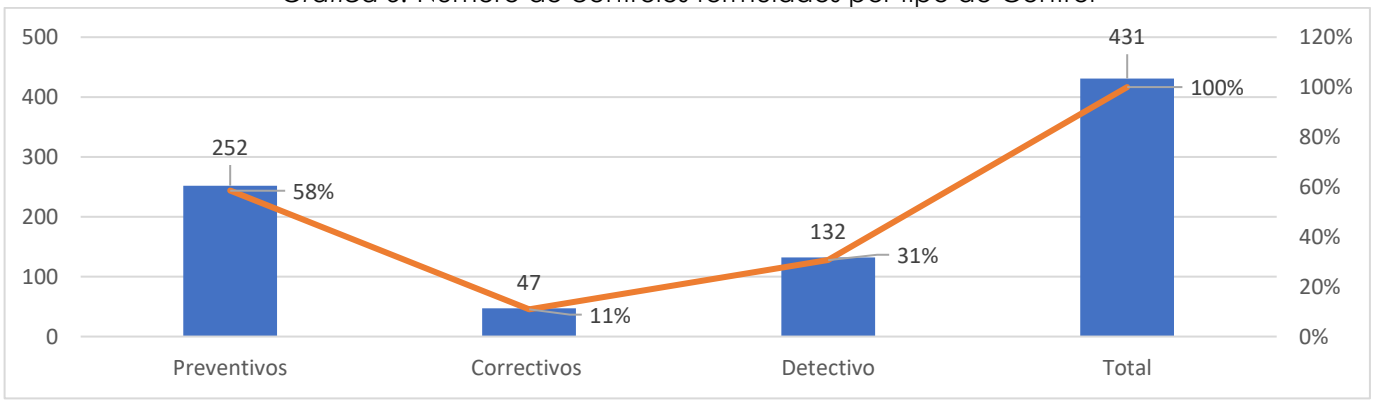
Gráfica 2. Número de riesgos identificados por clase de riesgo



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 2023 – Reporte Suite Empresarial.

Se definió un total de 431 controles para los 151 riesgos, de los cuales 252 de estos, corresponde a controles preventivos, la gráfica No. 3 muestra el número de controles formulados, según tipo:

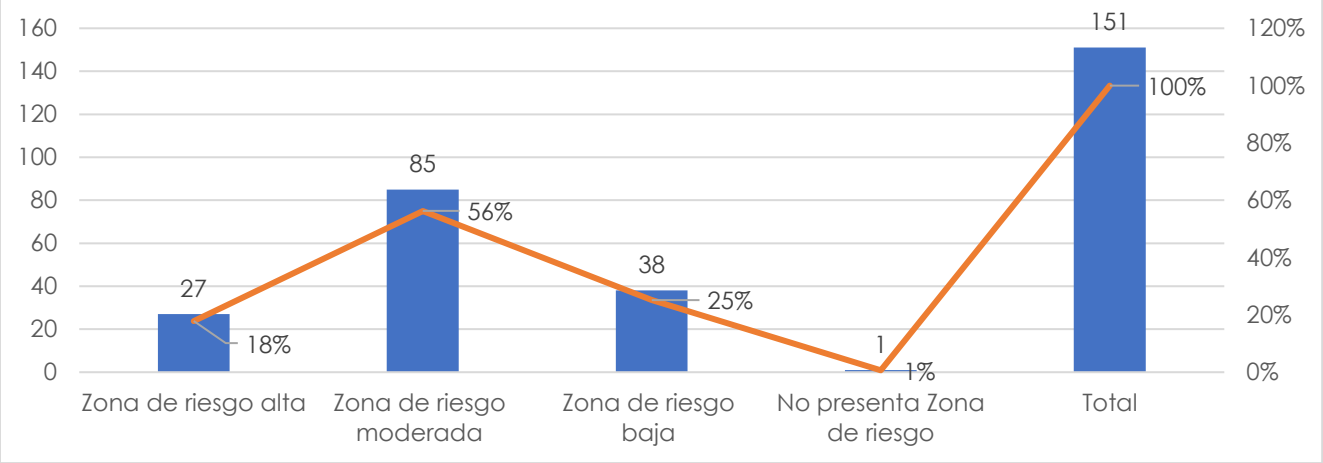
Gráfica 3. Número de controles formulados por tipo de Control



Fuente: Elaboración propia equipo de Control Interno con base en la información suministrada por la Segunda Línea de Defensa a noviembre de 2023 - Reporte Suite Empresarial

Revisados y evaluados los controles, a continuación, se presenta la zona de riesgo residual donde se ubican los 151 riesgos identificados:

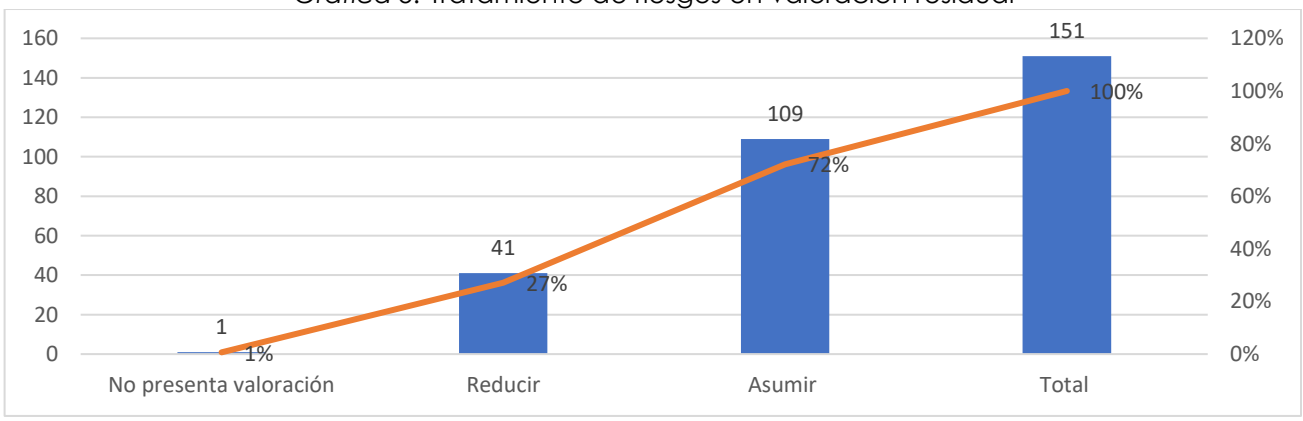
Gráfica 4. Número de riesgos por zona de riesgo residual



Fuente: Elaboración propia equipo de Control Interno con base en la información suministrada por la Segunda Línea de Defensa a noviembre de 2023 – 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 asumieron el 72% 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 2023 – 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 y noviembre de 2023, se observa lo siguiente:

Con base en la información suministrada por la segunda línea de defensa sobre la materialización de los riesgos en sus reportes mensuales, se evidenció lo siguiente:

Tabla 1. Riesgos materializados

Proceso	Riesgo materializado	junio	julio	agosto	septiembre	octubre	Total Materialización
Relacionamiento Estado Ciudadano	Inoportunidad en el cumplimiento de los términos legales de respuesta de las PQRSD		1	1	1	1	**4**
	Documentos y registros asociados a las PQRS inexistentes, cruzados e incompletos que no permiten la trazabilidad del trámite tanto de petición como de respuesta.			1			**1**
Operaciones SECOP II	Fallas en la ejecución de las formaciones planeadas por el grupo de uso y apropiación	1					**1**
Gestión de Tecnologías de la Información	Posibilidad de falla en la implementación en producción de un producto de Software con problemas de calidad y estabilidad	1					**1**
Normativa de la contratación en la administración pública	Inoportunidad en las respuestas de conceptos jurídicos de carácter general	1					**1**
Total		**3**	**1**	**2**	**1**	**1**	**8**

Fuente: Elaboración propia equipo de Control Interno con base en la información suministrada por la Segunda Línea de Defensa a noviembre de 2023.

Durante el periodo evaluado se materializó en cuatro (4) oportunidades el riesgo *"Inoportunidad en el cumplimiento de los términos legales de respuesta de las PQRSD"*, de esta manera se observa que el plan de tratamiento no ha sido efectivo.

A la fecha del presente informe, no se cuenta con el monitorio que realiza la segunda línea de defensa correspondiente al mes de noviembre del año en curso.

De acuerdo con el seguimiento realizado por la segunda línea de defensa y los trabajos elaborados por Control Interno, 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.

Revisado la matriz de riesgos de seguridad digital de acuerdo con los riesgos que presentan tratamiento, se identificó lo siguiente:

Tabla 2. Riesgo de Seguridad Digital que Presentan Tratamiento

ÍTEM	RIESGO	DESCRIPCIÓN DEL CONTROL	OBSERVACIÓN
R-GTI-38	Perdida de confidencialidad de la información almacenada en la nube por accesos no autorizados.	Verificar la matriz de roles y perfiles.	Se evidenció que en la matriz de roles y perfiles se encuentra desactualizada, ya que mencionan como jefe directo al Exsubdirector de IDT.
R-GTI-41	Perdida de confidencialidad de los servicios por ausencia de control de acceso.	Verificar la matriz de roles y perfiles.	Se evidenció que la "*política de roles y responsabilidades para la seguridad y privacidad de la información.docx*" corresponde a un documento preliminar con corte de 30 de noviembre lo cual no se cumple con la acción programada.
R-GTI-44	Perdida de confidencialidad de los componentes de red de la ANCP-CCE, permitiendo acceso a información clasificada afectando la prestación de servicios internos.	Verificar la matriz de roles y perfiles.	Se evidenció que la "*política de roles y responsabilidades para la seguridad y privacidad de la información.docx*" corresponde a un documento preliminar con corte de 30 de noviembre lo cual no se cumple con la acción programada.
R-GTI-46	Perdida de integridad en la infraestructura de almacenamiento por modificación de la información personal no autorizado o error humano.	Controlar el acceso por segmento de red, únicamente se permite el acceso desde los equipos de infraestructura o VPN.	Se evidenció el documento denominado "*actividades-bcp_portalweb.xlsx*", así mismo. no se adjuntan las evidencias de las actividades del minutograma relacionadas en la hoja "minutograma web".
R-GTI-47	Perdida de confidencialidad de la infraestructura de almacenamiento, ocasionando la exposición de información sensible por acceso no autorizado.	Verificar la matriz de roles y perfiles.	Se evidencia el documento de políticas debe contener los requisitos para que los usuarios internos y externos puedan crear contraseñas seguras, como por ejemplo, longitud mínima, complejidad, caracteres permitidos entre otros, sin embargo, el documento evidenciado corresponde a una versión preliminar de solo una hoja, sin atributos de calidad y sin firmas.
R-GTI-48	Perdida de disponibilidad de la infraestructura de almacenamiento por fallas en los dispositivos.	Monitorear del desempeño de los recursos de máquinas en toda la infraestructura interna y externa.	Sin novedad
R-GTI-48	Perdida de disponibilidad de la infraestructura de almacenamiento por fallas en los dispositivos.	Monitorear del desempeño de los recursos de máquinas en toda la infraestructura interna y externa.	No se observa un plan de capacidad donde se realice un análisis de infraestructura tecnológica en el cual se proyecte que los recursos aprovisionados sean suficientes para atender la demanda de servicios por parte de los usuarios internos y externos, además de identificar oportunidades de mejora en la infraestructura, solamente se adjunta un pantallazo de un recurso de AZURE denominado "*load balancing*".

Fuente: Elaboración propia equipo de Control Interno con base en la información suministrada por la Subdirección de IDT sobre los riesgos de seguridad digital a noviembre de 2023.

Revisado el cumplimento 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 3. Realización Subcomités de Control Interno

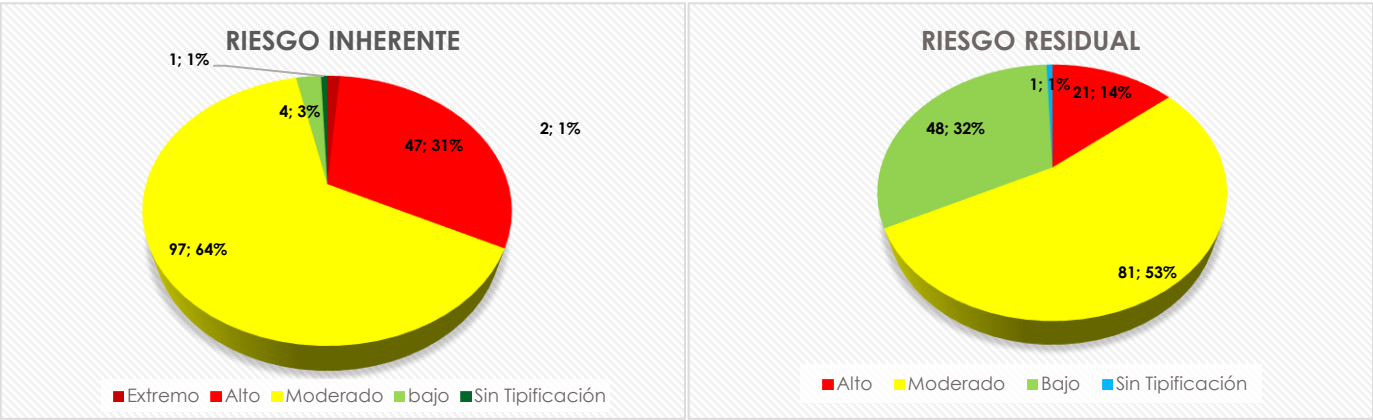
Áreas	Fecha Subcomité de Control Interno	Observación
Dirección General	No se realizaron Subcomités	No se evidencia la realización de los Subcomités de Control Interno durante el periodo evaluado.
Subdirección de Información y Desarrollo Tecnológico	16/06/2023 14/08/2023 08/11/2023	Sin novedad
Subdirección de Estudios de Mercados y Abastecimiento Estratégico	1/06/2023 28/09/2023	Sin novedad
Subdirección de Negocios	18/07/2023	Se evidenció que en el subcomité realizado por la Sub. de Negocios no se trataron los riesgos del proceso.
Subdirección de Gestión Contractual	16/06/2023 20/09/2023	Sin novedad
Secretaría General	05/07/2023 10/08/2023	La Asesora de Control Interno no fue invitada.

Fuente: Elaboración propia equipo de Control Interno con base en la información suministrada por la Primera Línea de Defensa a noviembre de 2023.

Resultado de la revisión de las actas de los subcomités de Control Interno, se observó que no se han realizado periódicamente para evidenciar las desviaciones oportunas sobre la gestión de los aspectos citados en la Resolución 270 de 2021.

A continuación, se presenta un comparativo 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 2023.

Teniendo en cuenta la situación identificada frente a la efectividad de los controles, se materializaron riesgos que requieren revisión y tratamiento.

No se observó que se haya actualizado la Política de Riesgos acorde con los lineamientos de la "*Guía para la Administración del Riesgo y el diseño de controles en entidades públicas*" Versión 6 emitida por el Departamento de la Función Pública DAFP.

RECOMENDACIONES DE CONTROL INTERNO

Conforme el seguimiento efectuado a la Gestión de Riesgos en la ANCP-CCE, correspondiente al periodo comprendido entre junio y noviembre de 2023, el Asesor Experto con funciones de Control Interno recomienda:

1. Validar la información que se encuentra en la Suite Empresarial, para evitar duplicidad de los riesgos.

2. Actualizar la política de riesgos incluyendo aspectos relacionados con los riegos de fraude y fiscales.

3. Se reitera qué una vez evidenciado la materialización de riesgos por la primera línea de defensa, reportarlos oportunamente para el tratamiento correspondiente.

4. 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.

5. 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.

Con relación a los Riesgos de Seguridad Digital Se recomienda lo siguiente:

6. Análisis de Riesgos: Realizar y actualizar de manera continua el análisis de riesgos para identificar y evaluar las amenazas potenciales a los activos de información y de esta manera establecer los controles de seguridad.

7. Política de Seguridad de la Información (PSI): Desarrollar, comunicar y socializar una PSI clara y comprensible para todos los funcionarios de la Agencia, con el compromiso de que desde la dirección general se respalde y promueva activamente la política al interior de la Agencia.

8. Nombramiento de un Responsable de Seguridad: Mantener constantemente designado al Responsable de Seguridad de la Información (RSI) para supervisar, coordinar e implementar todas las actividades relacionadas con la seguridad de la información.

9. Controles de Acceso: Mantener e implementar controles de acceso robustos para garantizar que solo los funcionarios autorizados tengan acceso a los activos de información de la Agencia, mediante la gestión

de contraseñas seguras, autenticación multifactor y revisión regular de privilegios sobre la infraestructura tecnológica.

10. Capacitación: Definir y realizar jornadas de capacitación constantes que proporcionen la concientización de los funcionarios de la Agencia sobre las amenazas digitales y las mejores prácticas de seguridad.

11. Gestión de Activos: Mantener actualizado el inventario de activos de información y de acuerdo con su clasificación aplicar medidas de seguridad proporcionales.

12. Gestión de Incidentes: Mantener y actualizar el plan de respuesta a incidentes que incluya procedimientos claros y entendibles para identificar, informar, documentar y gestionar incidentes de seguridad de la información. Es importante llevar a cabo ejercicios planeados de simulacros periódicos para evaluar la eficacia del plan.

13. Auditorías y Revisiones: Realizar auditorías internas y revisiones constantes para asegurar el cumplimiento continuo con los controles de seguridad establecidos. Esto permite la corrección de cualquier desviación encontrada de manera oportuna.

14. Actualizaciones y Parches de seguridad: Implementar un proceso efectivo para gestionar y aplicar actualizaciones de seguridad y parches en todos los sistemas y software de la infraestructura de la Agencia, realizando un análisis de viabilidad sobre el impacto que estas puedan tener sobre las aplicaciones existentes.

15. Monitorización Continua: Implementar herramientas de seguridad de la información para detectar posibles amenazas en tiempo real para asegurar un sistema de monitorización continua sobre la infraestructura tecnológica de la Agencia, permitiendo identificar y responder rápidamente a eventos de seguridad.

Firmado digitalmente por JUDITH ESPERANZA GÓMEZ ZAMBRANO
Fecha: 2023.12.21 16:05:03 -05'00'

Aprobó	Judith Esperanza Gómez Zambrano
Revisó	Judith Esperanza Gómez Zambrano
Elaboró	Jesús Gabriel Montoya Ramos
Fecha:	Diciembre 2023
Código de informe:	22-2

CONTROL DE CAMBIOS DEL DOCUEMNTO					
VERSION	**AJUSTES**	**FECHA**	**VERSIÓN ACTUAL**		**01**
01	Creación y estandarización de formato	01/07/2021	**Elaboró**	Judith Gómez	Asesora Experta con funciones de Control Interno
			Revisó	Judith Gómez	Asesora Experta con funciones de Control Interno
			Aprobó	Judith Gómez	Asesora Experta con funciones de Control Interno