PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INSTITUTO NACIONAL DE SALUD

Jefe de Oficina de Tecnología de la Información y Comunicaciones

Carlos Andrés López Fernández

Elaborado por:	Revisado por:	Aprobado por:
Sergio Andrés Ramos Pahuana Profesional Contratista OTIC Jesús David Diaz Quiceno Profesional Contratista OTIC	Carlos Andrés López Fernández Jefe OTIC	Carlos Andrés López Fernández Jefe OTIC Comité Institucional de Gestión y Desempeño Fecha Realización: 30/12/2025

Fecha de elaboración:

www.ins.gov.co
@INSColombia @insaludcolombia Instituto Nacional de Salud de Colombia
Avenida Calle 26 # 51 - 20 / Bogotá D.C. - Colombia PBX: (601) 220 77 00 / exts. 1101 - 1214 contactenos@ins.gov.co

1. INTRODUCCION

El presente documento define las medidas que se desarrollarán e implementarán durante la vigencia 2026 del plan de tratamiento de riesgos de Seguridad y Privacidad de la Información y Seguridad Digital en el Instituto Nacional de Salud – INS, medidas que permitan mitigar los riesgos presentes (perdida de confidencialidad, integridad, disponibilidad y privacidad en los activos de información), evitando situaciones que generen incertidumbre en el cumplimiento de los objetivos de la Entidad.

Las tendencias tecnológicas de los últimos años han permitido crear de manera exponencial cantidades de información, cambiando la manera de ver las cosas por parte de todos aquellos quienes tienen acceso a esta. Particularmente en las entidades de la administración pública, se hace necesario contar con la conciencia del poder de la información, el alcance que tiene la misma y principalmente la entrega de esta de manera oportuna y eficiente a la ciudadanía.

En este contexto, bajo la perspectiva de tener información disponible en activos de información vulnerables, surge la necesidad de establecer lineamientos que permitan una adecuada administración del riesgo, integrándola como parte del Instituto Nacional de Salud - INS. Este proceso involucra actividades de identificar, analizar, controlar y mitigar los riesgos de seguridad de la información que podrían afectar negativamente el logro de los objetivos estratégicos de la Entidad.

En este sentido, el presente documento se convierte en una necesidad casi imperativa, dado que la materialización de los riesgos de seguridad de la información puede obstaculizar el cumplimiento adecuado, efectivo y óptimo de los objetivos institucionales tanto internos como los dirigidos a la ciudadanía, para los cuales fue concebida la Entidad.

Desde esta perspectiva, la gestión de los Riesgos de Seguridad y Privacidad de la Información se presenta como una herramienta vital para el desarrollo, implementación y mejora continua de la Entidad frente a la prestación de servicio y la entrega de información, partiendo de la protección del valor de la organización a partir de la seguridad de la información, tanto física como digital.

Al tener una visión clara de los riesgos que pueden afectar la seguridad de la información, la entidad puede establecer controles y medidas efectivas, viables y transversales, con el propósito de preservar la disponibilidad, integridad y confidencialidad de su información. Para lograrlo, es esencial definir los lineamientos que se deben seguir para el análisis y evaluación de los riesgos de la Entidad. Todo esto, cumplimiento con la normativa establecida por el estado Colombiano y adoptando las buenas prácticas de los estándares que sirven como guía.

Las actividades se definieron teniendo en cuenta la metodología de gestión de riesgos adoptada por la entidad en cuanto a la seguridad y privacidad de la información y seguridad digital y basados en la Guía para la gestión integral del riesgo en entidades públicas, proporcionando las herramientas necesarias para identificar sus características y definir los pasos a seguir para su ejecución.

2. MARCO NORMATIVO

A continuación, se referencian las normas y leyes colombianas que aplican en el ámbito de Seguridad y Privacidad de la información; si cualquier disposición de estas condiciones pierde validez por cualquier razón, todas las demás conservan su fuerza obligatoria:

Constitución Política de Colombia

- **Artículos** 15, 20, 23 y 74.

Leyes

- **Ley 23 de 1982.** Sobre derechos de autor
- **Ley 44 de 1993.** Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- **Ley 527 de 1999.** Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 594 de 2000.** Por medio de la cual se expide la Ley General de Archivos.
- **Ley 962 de 2005.** Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
- **Ley 1266 de 2008.** Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1221 del 2008.** Por la cual se establecen normas para promover y regular el teletrabajo y se dictan otras disposiciones.
- **Ley 1273 de 2009.** Por medio de la cual se modifica el Código Penal, se 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 1450 de 2011.** Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.

- **Ley 1437 de 2011.** Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1712 de 2014.** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Ley 1753 de 2015.** Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país”.
- **Ley 1755 de 2015.** Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- **Ley 2052 de 2020.** Por medio de la cual se expide el código general disciplinario.
- **Ley 1915 de 2018.** Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- **Ley 2088 de 2021.** Por la cual se regula el trabajo en casa y se dictan otras disposiciones.

Decretos

- **Decreto 2364 de 2012.** Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- **Decreto 884 de 2012.** por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
- **Decreto 2609 de 2012.** Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- **Decreto 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **Decreto 1074 de 2015.** Por medio del cual se expide el Decreto reglamentario del sector comercio, industria y turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- **Decreto 1078 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1081 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- **Decreto 1068 de 2015.** por medio del cual se expide el Decreto Único Reglamentario del Sector Hacienda y Crédito Público.
- **Decreto 728 de 2017.** Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
- **Decreto 1499 de 2017.** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

- **Decreto 612 de 2018.** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- **Decreto 1008 del 2018.** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 2106 de 2019.** Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- **Decreto 620 de 2020.** por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- **Decreto 88 de 2022.** Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea
- **Decreto 338 de 2022.** Por el cual se adiciona el Titulo 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- **Decreto 767 de 2022.** Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Resoluciones

- **Resolución 1519 de 2020.** “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- **Resolución 500 de 2021.** 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
- **Resolución 746 de 2022.** Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021.

- **Resolución 460 de 2022.** Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.
- **Resolución 02277 DE 2025.** Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.
- **Resolución 1457 de 2025.** Por la cual se actualiza la Política de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Instituto Nacional de Salud - INS, como uno de los elementos habilitadores de la Política de Gobierno Digital, y se deroga la Resolución 0839 de 2025.
- **Resolución 0457 de 2020.** Por medio de la cual se adiciona el anexo No. 02 de la Resolución 1607 de 2014 y se actualiza la Política de Tratamiento de Datos Personales del INS.

Otras

- **Decisión Andina 351 de 1993.** Régimen común sobre derecho de autor y derechos conexos
- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital.
- **CONPES 3995 de 2020**. Confianza y Seguridad Digital
- **CONPES 3995 de 2020.** Política Nacional de Confianza y Seguridad Digital.
- **CONPES 4144 de 2025.** Política nacional de Inteligencia Artificial
- **Directiva 26 de 2020.** Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones del artículo 23 de la ley 1712 de 2014.
- **Directiva Presidencial 02 de 2022.** Reiteración de la política pública en materia de seguridad digital.

3. OBJETIVOS

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de seguridad y privacidad de la información y seguridad digital a los que el INS pueda estar expuesto, de acuerdo con el contexto establecido en la Entidad, y a los requisitos legales, reglamentarios, regulatorios y de las demás normas técnicas colombianas.

4. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad de la Información abarca la identificación, análisis y valoración de los riesgos asociados a los activos que custodian los procesos de la Entidad.

El alcance incluye a todos los funcionarios, contratistas y terceros que interactúan con los sistemas y datos de la entidad. Las actividades se centran en la definición de controles para proteger la confidencialidad, integridad y disponibilidad de la información, priorizando los riesgos que puedan afectar el cumplimiento de los objetivos misionales.

El plan se desarrollará durante 2026, siguiendo el ciclo PHVA y conforme a la Guía para la gestión integral del riesgo en entidades públicas, Versión 7, y la Política de Seguridad y privacidad de la Información de la entidad.

5. DIAGNÓSTICO DE NECESIDADES

En el marco de la actualización de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 del DAFP, se realizó un análisis detallado de los criterios actuales en materia de riesgos en la Entidad, y producto de este ejercicio se realizó la actualización de la metodología y el instrumento para la gestión de los riesgos de seguridad digital, adicionalmente, en vigencias anteriores, no se habían identificado riesgos asociados a la seguridad y privacidad de la información y seguridad digital, lo que representa una brecha significativa frente a las exigencias actuales en materia de protección de la información y ciberseguridad.

Con la ausencia de estos riesgos en ciclos previos no fue posible identificar amenazas y vulnerabilidades que comprometan la confidencialidad, integridad y disponibilidad de la información, afectando la confianza ciudadana y el cumplimiento normativo. Adicionalmente, la transición de la norma ISO 27001:2013 a ISO 27001:2022 introduce nuevos requisitos orientados a la gestión proactiva de riesgos, la resiliencia organizacional y la protección frente a amenazas emergentes, lo que exige una adaptación inmediata de los controles y procesos internos.

Por estas razones, se hace indispensable la formulación e implementación de un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, que permita:

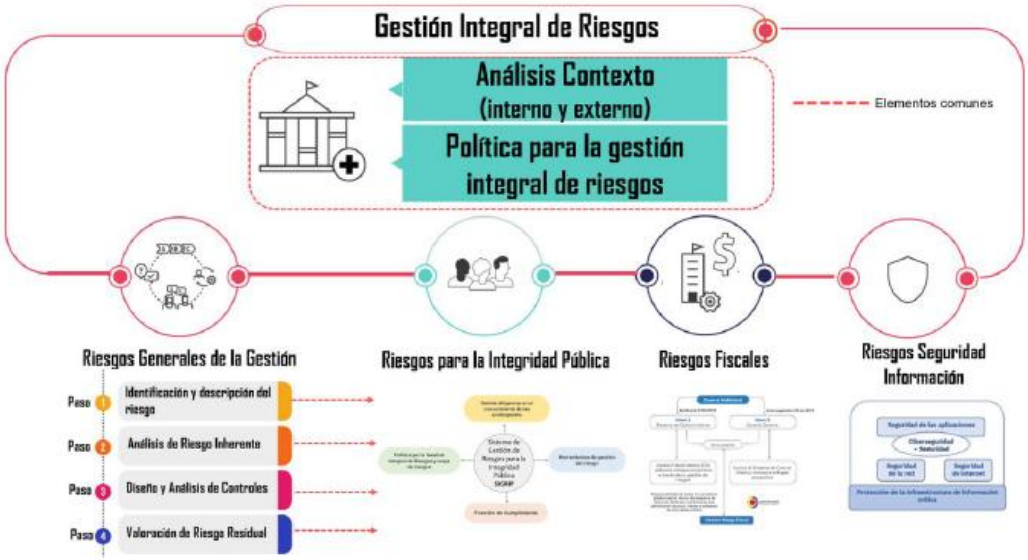
- Identificar, evaluar y priorizar los riesgos relacionados con la seguridad digital y la protección de datos personales.
- Definir estrategias y controles alineados con la nueva versión de la norma ISO 27001:2022 y la normativa nacional vigente.
- Integrar el tratamiento de riesgos en el Sistema de Gestión de Seguridad de la Información (SGSI) para garantizar su efectividad.
- Fortalecer la cultura organizacional mediante capacitación y sensibilización sobre riesgos tecnológicos y normativos.

Este plan será un componente esencial para consolidar la gestión integral del riesgo en la entidad, asegurando la protección de los activos de información y la continuidad de los servicios frente a un entorno cada vez más complejo y dinámico.

6. DESARROLLO DEL PLAN

6.1 Desarrollo Metodológico

El INS, acogerá la metodología establecida por el Departamento Administrativo de la Función Pública, descrita en la Guía para la gestión integral del riesgo en entidades públicas versión 7.



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2025.

Para dar cumplimiento a las etapas establecidas en dicha metodología se establece el siguiente cronograma de actividades, el cual se le hará seguimiento a través del plan de acción Institucional:

Actividades	Tareas	Responsable de la Tarea	Fecha Inicio	Fecha Final
Revisión de los lineamientos de riesgos de seguridad y privacidad de la información y seguridad digital	Revisar y/o actualizar la política, metodología y lineamientos de la gestión de riesgos de seguridad y privacidad de la información y seguridad digital.	Oficina Asesora de Planeación. Referente de seguridad y privacidad de la Información.	2-feb-26	31-mar-26
Identificación de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital	Acompañar en la identificación y/o actualización del Contexto interno y externo de los procesos en lo referente a la Seguridad y Privacidad de la Información y Seguridad Digital	Referente de seguridad y privacidad de la Información Líderes de los procesos	01 abr-26	30-jun-26
	Acompañar en la identificación, análisis y evaluación de los Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital.	Referente de seguridad y Privacidad de la Información Líderes de los procesos	01 abr-26	30-jun-26
Aceptación y aprobación de Riesgos Identificados	Solicitar la aceptación y aprobación de los riesgos identificados y los planes de tratamiento	Referente de seguridad y Privacidad de la Información Líderes de los procesos	01 abr-26	30-jun-26
Seguimiento y fase de tratamiento	Realizar seguimiento a la implementación de controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)	Referente de seguridad y privacidad de la Información	01-jul-26	23-dic-26

Gestión de Vulnerabilidades	Ejecutar las pruebas de vulnerabilidades y pentest	Referente de seguridad y Privacidad de la Información	02-feb-26	30-jun-26
	Realizar seguimiento a los planes de remediación sobre los sistemas y plataforma de acuerdo con los resultados del análisis de vulnerabilidades y pentest	Referente de seguridad y privacidad de la Información Líderes de las líneas de infraestructura y sistemas de información	02-feb-26	30-jun-26
Entrenamiento	Realizar pruebas de Ingeniería Social	Referente de seguridad y privacidad de la Información	02-feb-26	23-dic-26

7. DISTRIBUCIÓN PRESUPUESTAL DE LOS PROYECTOS DE INVERSIÓN

El Instituto, para la gestión de riesgos de Seguridad y Privacidad de la información y Seguridad Digital, dispondrá de los siguientes recursos:

Recursos	Variable
Humanos	Responsables de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la gestión de riesgos de seguridad y privacidad de la información y seguridad digital.
Técnicos	Guía para la gestión integral del riesgo en entidades públicas, en su última versión. Herramienta para la gestión de riesgos.
Logísticos	Cronograma para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos con los procesos de la entidad.

Recursos	Variable
Financieros	El Presupuesto que implique la ejecución de los planes de tratamiento de riesgos de Seguridad y Privacidad de la Información y Seguridad Digital identificados en la entidad, corresponderá al dueño del riesgo (líder del proceso), quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos.

8. INDICADORES

La medición se realizará a través de un indicador orientado principalmente a determinar el porcentaje de ejecución de los controles definidos para mitigar los riesgos identificados en los diferentes procesos de la entidad.

9. HOJA DE RUTA DE IMPLEMENTACIÓN DEL PLAN

Ver hoja de ruta del plan

10. CONTROL DE CAMBIOS.

Versión	Fecha de actualización			Descripción de los cambios
	aaaa	mm	dd	
1.0	2024	01	12	Versión inicial del documento
2.0	2024	12	28	Actualización 2025
3.0	2025	07	04	Actualización 2025
4.0	2025	12	30	Actualización 2026

HOJA DE RUTA PLANES INSTITUCIONALES

Recomendación general: Diligenciar en minúscula, revisar escritura y ortografía antes de enviar, con la pestaña revisar y ortografía.

FECHA DE DILIGENCIAMIENTO	29/12/25	NOMBRE DE QUIEN DILIGENCIA	SERGIO ANDRÉS RAMOS PAHUANA

CÓDIGO DE LA ACTIVIDAD/TAREA DEL PLAN DE ACCIÓN ASOCIADO	NOMBRE DEL PLAN	CATEGORIA/COMPONENTE/PRODUCTO	SUBCATEGORIA/SUBCOMPONENTE /ACCIÓN ESTRATÉGICA	TAREA	ENTREGABLE	PROCESO RESPONSABLE	LÍDER DEL PROCESO	RESPONSABLE DEL REPORTE DE LA TAREA	META TOTAL	UNIDAD META AVANCE FÍSICO	FUNCIÓN PARA CALCULAR EL AVANCE DE LA META	FRECUENCIA DE MEDICIÓN DE AVANCE	METAS FÍSICAS PARCIALES	FECHA INICIO	FECHA FINALIZACIÓN
140114/1401142	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Revisión de los lineamientos de riesgos de seguridad y privacidad de la información y seguridad digital	N/A	Revisar y/o actualizar la política, metodología y lineamientos de la gestión de riesgos de seguridad y privacidad de la información y seguridad digital.	Documento actualizado	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	1	NÚMERO	SUMA	ANUAL	N/A	2/02/26	31/03/26
140114/1401142	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Identificación de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital	N/A	Acompañar en la identificación y/o actualización del Contexto interno y externo de los procesos en lo referente a la Seguridad y Privacidad de la Información y Seguridad Digital	Formato FOR-I302.0000-037 diligenciado	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	1	NÚMERO	SUMA	ANUAL	N/A	1-abr-26	30/09/26
140114/1401142	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Identificación de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital	N/A	Acompañar en la identificación, análisis y evaluación de los Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital.	Formato FOR-I302.0000-037 diligenciado	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	1	NÚMERO	SUMA	ANUAL	N/A	1-abr-26	30/09/26
140114/1401142	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Aceptación y aprobación de Riesgos Identificados	N/A	Solicitar la aceptación y aprobación de los riesgos identificados y los planes de tratamiento	Correo de solicitud de aprobación	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	1	NÚMERO	SUMA	ANUAL	N/A	1-abr-26	30/09/26
140114/1401142	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Seguimiento y fase de tratamiento	N/A	Realizar seguimiento a la implementación de controles y planes de tratamiento de los riesgos identificados (verificación de evidencias)	Formato FOR-I302.0000-037 diligenciado	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	3	NÚMERO	SUMA	CUATRIMESTRAL	N/A	1-jul-26	23/12/26
140114/1401142	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Gestión de Vulnerabilidades	N/A	Ejecutar las pruebas de vulnerabilidades y pentest	Informes de pruebas realizadas	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	4	NÚMERO	SUMA	TRIMESTRAL	N/A	2-feb-26	30/09/26
140114/1401142	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Gestión de Vulnerabilidades	N/A	Realizar seguimiento a los planes de remediación sobre los sistemas y plataforma de acuerdo con los resultados del análisis de vulnerabilidades y pentest	Herramienta de seguimiento de los planes de vulnerabilidades Informe de los planes de remediación	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	4	NÚMERO	SUMA	TRIMESTRAL	N/A	2-feb-26	30/09/26
140114/1401142	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Entrenamiento	N/A	Realizar pruebas de Ingeniería Social	Informes de pruebas realizadas	TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN	Carlos Andres Lopez Fernandez	Sergio Andrés Ramos Pahuana	2	NÚMERO	SUMA	SEMESTRAL	N/A	2-feb-26	23/12/26