PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

Culturas

ICANH

CONTENIDO

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026 del Instituto Colombiano de Antropología e Historia (ICANH) tiene como objetivo identificar, analizar y tratar los riesgos asociados a la seguridad y privacidad de la información institucional, mediante la definición e implementación de acciones orientadas a su mitigación y control.

Este plan adopta un enfoque preventivo y sistemático, orientado a comprender el contexto y la naturaleza de los riesgos, así como a diseñar y ejecutar medidas que reduzcan su probabilidad de ocurrencia y el impacto potencial sobre los procesos misionales, estratégicos y de apoyo del ICANH. En este sentido, se estructura a partir de estrategias para la identificación, análisis, evaluación, tratamiento y monitoreo continuo de los riesgos, promoviendo la anticipación y la toma de decisiones objetivas frente a situaciones que puedan comprometer el logro de los objetivos institucionales en el ámbito de las Tecnologías de la Información y las Comunicaciones (TIC).

Con el propósito de garantizar la protección de la información, el plan establece controles específicos orientados a preservar la confidencialidad, integridad y disponibilidad de los activos de información. Asimismo, se encuentra alineado con la normativa nacional vigente, incluyendo el CONPES 3995 de 2020, el Decreto 1008 de 2018 y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones. De manera complementaria, incorpora buenas prácticas y estándares internacionales, en particular la norma ISO/IEC 27001, como marco de referencia para fortalecer la gestión de riesgos y robustecer el sistema de seguridad de la información institucional.

2. OBJETIVO GENERAL

Desarrollar e implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del ICANH, alineado con el propósito misional de la entidad, con el fin de definir y ejecutar las acciones necesarias para asegurar la protección de la información institucional, mediante la aplicación de una metodología

de gestión de riesgos que permita identificar, analizar, evaluar y mitigar los riesgos asociados a la seguridad y privacidad de los datos.

3. DEFINICIONES

- ***Aceptación del Riesgo:*** Decisión informada de asumir un riesgo, una vez analizadas sus consecuencias y determinado que su nivel es tolerable para la organización.

- ***Acción correctiva:*** Actividad implementada para eliminar la causa de una no conformidad detectada y prevenir su recurrencia.

- ***Acción preventiva:*** Actividad orientada a eliminar la causa de una posible no conformidad o situación no deseada, con el fin de evitar su ocurrencia.

- ***Administración de riesgos:*** Conjunto de etapas y actividades orientadas a la identificación, análisis, evaluación, tratamiento y seguimiento de los riesgos, con el propósito de reducir su impacto sobre la organización.

- ***Amenaza:*** Causa potencial de un incidente no deseado que puede generar daños a un activo de información, un sistema o a la organización (ISO/IEC 27000).

- ***Análisis del riesgo:*** Proceso sistemático para comprender la naturaleza del riesgo y determinar su nivel, considerando la probabilidad de ocurrencia y el impacto asociado (ISO/IEC 27000).

- ***Causa:*** Factor interno o externo que puede generar la materialización de un riesgo.

- ***Confidencialidad:*** Propiedad de la información que garantiza que solo sea accesible a personas, entidades o procesos debidamente autorizados.

- ***Disponibilidad:*** Propiedad de la información que asegura su acceso y utilización cuando sea requerida por un usuario autorizado.

- ***Integridad:*** Propiedad de la información que garantiza su exactitud, completitud y protección contra modificaciones no autorizadas.

- ***Modelo de Seguridad y Privacidad de la Información (MSPI):*** Conjunto de lineamientos, políticas, procesos y controles definidos por una entidad para gestionar de manera integral la seguridad y privacidad de la información, de acuerdo con los lineamientos del MinTIC.

- ***Riesgo:*** Posibilidad que una amenaza pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. ISO Guía 73:2002.

- ***Riesgo Inherente:*** Nivel de riesgo existente antes de aplicar controles o medidas de mitigación, derivado de la exposición natural de los activos de información a amenazas y vulnerabilidades.

- ***Vulnerabilidad:*** Debilidad, falla u omisión en un activo, proceso o control que puede ser explotada por una amenaza.

- ***SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO/IEC 27001: 20005]:*** la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos).

4. ALCANCE:

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del ICANH aplica a todos los funcionarios, contratistas y terceros que, en el desarrollo de sus funciones, interactúan con los activos de información institucionales. Su alcance comprende los procesos misionales, estratégicos, de apoyo y de evaluación de la entidad, así como las actividades asociadas al ciclo de vida de la información, con el propósito de garantizar la gestión integral de los riesgos y la protección de la confidencialidad, integridad y disponibilidad de la información, en cumplimiento de la normativa vigente y los lineamientos de seguridad digital aplicables. Asimismo,

promueve la adopción de buenas prácticas y el fortalecimiento de una cultura organizacional orientada a la seguridad y privacidad de la información.

5. MARCO NORMATIVO

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del ICANH se fundamenta en el siguiente marco normativo, el cual establece los lineamientos legales, técnicos y de política pública aplicables a la gestión de la seguridad de la información, la protección de datos personales y la seguridad digital en las entidades públicas:

- **Ley 1581 de 2012:** Establece el Régimen General de Protección de Datos Personales y regula el tratamiento de datos, así como la adopción de políticas y medidas para su protección en entidades públicas y privadas.
- **Ley 1712 de 2014:** Ley de Transparencia y del Derecho de Acceso a la Información Pública, que regula el acceso y protección de la información pública.
- **Decreto 1083 de 2015** "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".
- **Decreto 1008 de 2018:** Establece los lineamientos para la Política de Gobierno Digital, incluyendo principios de seguridad de la información y gestión de riesgos digitales.
- **Resolución 500 de 2021:** Adopta los estándares y lineamientos para la estrategia de seguridad digital y el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
- **Documento CONPES 3995 de 2020:** Política Nacional de Confianza y Seguridad Digital, que promueve la protección de datos e infraestructura crítica, fortaleciendo la gestión de riesgos en el entorno digital.
- **Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital del Departamento Administrativo de la Función Pública (DAFP):** Define lineamientos para gestionar riesgos de seguridad digital en entidades públicas.

- **Decreto 767 de 2022:** Lineamientos generales de la Política de Gobierno Digital, promoviendo la transformación digital con inclusión de estándares de ciberseguridad.
- **Modelo Integrado de Planeación y Gestión (MIPG):** Marco de referencia para la gestión institucional, que integra la seguridad de la información como un elemento transversal para el logro de resultados y la generación de valor público.
- **ISO/IEC 27001:** Norma internacional para el establecimiento, implementación, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI).

6. DIAGNÓSTICO Y JUSTIFICACIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del ICANH se formula a partir de la identificación y análisis de riesgos sobre los activos de información institucionales, así como de evaluaciones previas realizadas en el marco del MSPI y la norma ISO/IEC 27001. Estos ejercicios evidenciaron riesgos que afectan la confidencialidad, integridad y disponibilidad de la información, asociados a vulnerabilidades técnicas, brechas en la implementación de controles, necesidades de actualización documental y normativa, y oportunidades de mejora en el seguimiento y la gestión de incidentes.

Adicionalmente, los análisis de vulnerabilidades y la evaluación de riesgos sobre la infraestructura y los sistemas de información identificaron escenarios relacionados con exposición a amenazas cibernéticas, control de accesos, continuidad de servicios y cumplimiento de requisitos legales. Por lo anterior, el plan es necesario para priorizar y ejecutar acciones de tratamiento de forma sistemática, fortalecer el gobierno de seguridad de la información, reducir la probabilidad e impacto de incidentes y asegurar la continuidad operativa y el cumplimiento normativo, en coherencia con la Política de Gobierno Digital y la Política Nacional de Confianza y Seguridad Digital.

7. ETAPAS

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del ICANH se fundamenta en un enfoque sistemático de gestión de riesgos, soportado en políticas, lineamientos y controles definidos a partir de la evaluación de los riesgos asociados a los activos de información institucionales. Este enfoque permite determinar el nivel de seguridad de la información de la entidad y orientar la toma de decisiones para su protección.

Con el propósito de identificar, analizar, evaluar, tratar y monitorear los riesgos de seguridad y privacidad de la información, el plan se desarrolla a través de las siguientes etapas:

7.1 IDENTIFICACIÓN DE LA INFORMACIÓN

Consiste en la identificación y clasificación de los activos de información más relevantes del ICANH, considerando aquellos que inciden directamente en los productos y servicios institucionales y que reflejan el cumplimiento de la misión de la entidad. Esta etapa incluye la valoración del impacto potencial sobre la confidencialidad, integridad y disponibilidad de la información, como base para la gestión del riesgo.

7.2 IDENTIFICACION DE LOS RIESGOS

En esta etapa se identifican los riesgos asociados a los activos de información, teniendo en cuenta las amenazas, vulnerabilidades y posibles impactos que puedan afectar la seguridad y privacidad de la información institucional. Para este propósito, se consideran las siguientes categorías de riesgo:

- **Riesgos sobre la confidencialidad de la información:** Comprende los riesgos a la pérdida o revelación de la misma. Cuando se habla de información reservada institucional se hace alusión a aquella que por la razón de ser de la entidad solo puede ser conocida y difundida al interior de la misma; así mismo, la sensibilidad de la información depende de la importancia que esta tenga para el desarrollo de la misión de la entidad.

- **Riesgos de Imagen:** Relacionados con la percepción, credibilidad y confianza de la ciudadanía, los grupos de interés y otras entidades frente al ICANH, como consecuencia de incidentes de seguridad o uso inadecuado de la información.

- **Riesgos Operativos:** Derivados del funcionamiento y la operación de los sistemas de información institucionales, de la definición y ejecución de los procesos, de la estructura organizacional y de la articulación entre dependencias. En esta categoría se incluyen los procesos de apoyo que soportan la operación de la entidad.

- **Riesgos Legales:** Asociados al incumplimiento de disposiciones legales, reglamentarias y contractuales aplicables a la gestión de la información, incluyendo obligaciones relacionadas con la función administrativa, la ejecución presupuestal y la normatividad vigente.

- **Riesgos de Tecnología:** Relacionados con la capacidad tecnológica del ICANH para soportar sus procesos actuales y futuros, garantizar la continuidad de los servicios de TI y cumplir con los objetivos misionales, considerando aspectos como infraestructura, software, obsolescencia tecnológica y disponibilidad de recursos.

7.3 ESTIMACIÓN EL IMPACTO

Una vez identificados los riesgos de seguridad y privacidad de la información, se procede a estimar el impacto potencial que tendría su materialización sobre los activos de información del ICANH. Esta estimación permite dimensionar el nivel de afectación que un riesgo puede generar sobre la entidad y constituye un insumo fundamental para la priorización y el tratamiento de los riesgos.

La evaluación del impacto se realiza considerando los efectos en términos de confidencialidad, integridad y disponibilidad de la información, así como las posibles consecuencias en el ámbito operativo, legal, institucional y reputacional. Para ello,

se emplea una escala cualitativa de cinco niveles, que permite clasificar el impacto de acuerdo con la severidad de sus consecuencias.

La Tabla 1. Impacto de Riesgos de Gestión establece los tipos de impacto evaluados (confidencialidad de la información, credibilidad o imagen, legal y operativo), junto con los niveles de impacto definidos y su respectiva descripción, la cual detalla el grado de afectación que tendría la entidad en caso de materializarse el riesgo.

TABLA DE IMPACTO			
TIPO	**NIVEL**	**DESCRIPTOR**	**DESCRIPCIÓN** En caso que el riesgo se materialice el impacto y afectación sería…
CONFIDENCIALIDAD EN LA INFORMACIÓN	1	INSIGNIFICANTE	Se afecta a una persona en particular.
	2	MENOR	Se afecta a un grupo de trabajo interno del proceso.
	3	MODERADO	Se afecta a todo el proceso.
	4	MAYOR	La afectación se da a nivel estratégico.
	5	CATASTRÓFICO	La afectación se da a nivel institucional.
CREDIBILIDAD O IMAGEN	1	INSIGNIFICANTE	Se afecta al grupo de funcionarios y contratistas del proceso.
	2	MENOR	Se afecta a todos los funcionarios y contratistas de la entidad.
	3	MODERADO	Se afecta a los usuarios de la Sede Central de la entidad.
	4	MAYOR	Se afecta a los usuarios de las Direcciones Territoriales.
	5	CATASTRÓFICO	Se afecta a los usuarios de la Sede Central y de las Direcciones Territoriales.
LEGAL	1	INSIGNIFICANTE	Se producen multas para la entidad.
	2	MENOR	Se producen demandas para la entidad.
	3	MODERADO	Se producen investigaciones disciplinarias.
	4	MAYOR	Se producen investigaciones fiscales.
	5	CATASTRÓFICO	Se producen intervenciones y o sanciones para la entidad por parte de un Ente de control u otro Ente regulador.
OPERATIVO	1	INSIGNIFICANTE	Se tendrían que realizar ajustes a una actividad concreta del proceso.
	2	MENOR	Se tendrían que realizar ajustes en los procedimientos del proceso.
	3	MODERADO	Se tendrían que realizar ajustes en la interacción de procesos.
	4	MAYOR	Se presentan intermitencias o dificultades en la operación del proceso
	5	CATASTRÓFICO	Se presentaría paro o no operación del proceso.

Tabla 1. Impacto de Riesgos de Gestión.

Por su parte, la Tabla 2. Criterios para definir el nivel de impacto describe de manera transversal los efectos esperados para cada nivel de impacto, desde escenarios

insignificantes, con afectaciones mínimas y localizadas, hasta escenarios catastróficos, que comprometen de manera grave la operación institucional, la imagen de la entidad y el cumplimiento de sus obligaciones legales.

Valor	Nivel	Descripción del impacto
1	INSIGNIFICANTE	Se afecta a un funcionario al interior del instituto, no afecta la imagen del instituto ni la de ningún proceso por lo cual no se presentan riesgos operativos
2	MENOR	Impacta la imagen del Instituto, se afecta a un grupo de usuarios de un proceso y por ende el funcionamiento, pueden existir demandas legales, Se tendrían que realizar ajustes en los procedimientos del proceso.
3	MODERADO	Se afecta la imagen de la institución, afecta a terceros, se producen investigaciones disciplinarias y se tendrían que realizar ajustes en la interacción de procesos.
4	MAYOR	Existe afectación a nivel de confidencialidad de la información a nivel estratégico, afecta la imagen de toda la institución, se pueden producir investigaciones a nivel fiscal y a nivel operativo se presentan intermitencia en los procesos.
5	CATASTRÓFICO	La confidencialidad afectara toda la institución, la imagen se ve afectada a nivel nacional, se producen sanciones por los entes de control a la entidad por parte de los entes de control, se puede presentar paro a nivel de los procesos.

Tabla 2. Criterios para definir el nivel de impacto.

Finalmente, la Tabla 3. Escala de Valoración de Riesgos presenta la equivalencia entre los niveles cualitativos de impacto y su correspondiente valor numérico, el cual será utilizado para el cálculo del nivel de riesgo y la priorización de las acciones de tratamiento, conforme a la metodología definida por el ICANH.

Escala	Valor
INSIGNIFICANTE	1
MENOR	2
MODERADO	3
MAYOR	4
CATASTRÓFICO	5

Tabla 3. Escala de Valoración de Riesgos

7.4 ESTIMACIÓN DE LA PROBABILIDAD EN EL RIESGO

En esta etapa se realiza la estimación del nivel de riesgo, considerando de manera conjunta el impacto potencial y la probabilidad de ocurrencia de cada riesgo identificado. Mientras el impacto hace referencia a la magnitud de las consecuencias derivadas de la materialización del riesgo, la probabilidad se asocia a la frecuencia o posibilidad con la que dicho evento puede ocurrir.

Para la determinación del nivel de riesgo, se utiliza la siguiente fórmula:

Riesgo = Impacto × Probabilidad

- **Estimación de la probabilidad**

La probabilidad de ocurrencia se evalúa con base en criterios cualitativos que consideran la factibilidad del evento y su frecuencia histórica o esperada. Para ello, se adopta una escala de cinco niveles, descrita en la Tabla 4. Escala para calificar la probabilidad del riesgo, que clasifica los eventos desde raros hasta casi seguros, asignándoles un valor numérico entre 1 y 5.

Esta escala permite establecer un criterio uniforme para valorar la probabilidad de ocurrencia de los riesgos, teniendo en cuenta tanto eventos pasados como escenarios potenciales que puedan afectar la seguridad y privacidad de la información del ICANH.

TABLA DE PROBABILIDAD			
Valor	**DESCRIPTOR**	**DESCRIPCIÓN (FACTIBILIDAD)**	**FRECUENCIA**
1	**RARO**	El evento puede ocurrir solo encircunstancias excepcionales	No se ha presentado en los últimos 5 años.
2	**IMPROBABLE**	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
3	**POSIBLE**	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.

4	**PROBABLE**	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
5	**CASI SEGURO**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Tabla 4. Escala para calificar la probabilidad del riesgo.

- **Matriz de calificación y evaluación del riesgo**

Una vez definidos los valores de impacto y probabilidad, se procede a calcular el nivel de riesgo mediante la Matriz de Calificación, Evaluación y Respuesta a los Riesgos (Tabla 5), la cual resulta de la multiplicación de ambos factores. Esta matriz permite visualizar de manera clara la severidad del riesgo y facilita su clasificación y priorización para la toma de decisiones.

El resultado obtenido refleja el nivel de exposición al riesgo y sirve como insumo para definir las acciones de tratamiento más adecuadas, de acuerdo con la capacidad de respuesta y el apetito de riesgo de la entidad.

CONCEPTO		IMPACTO				
PROBABILIDAD		INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
	VALOR	1	2	3	4	5
RARO (1)	1	1	2	3	4	5
IMPROBABLE (2)	2	2	4	6	8	10
POSIBLE (3)	3	3	6	9	12	15
PROBABLE (4)	4	4	8	12	16	20
CASI SEGURO (5)	5	5	10	15	20	25

Tabla 5. Matriz de Calificación, Evaluación y respuesta a los Riesgos.

- **Determinación de la zona de riesgo**

Posterior a la calificación del riesgo, se determina la zona de riesgo en la que se ubica cada riesgo identificado, conforme a los rangos establecidos en la *Tabla 6. Evaluación de Zona de Riesgos*. Estas zonas permiten clasificar los riesgos en función de su severidad, de la siguiente manera:

- **Zona de riesgo baja:** Riesgos con impacto reducido y controlable, que pueden ser aceptados o monitoreados.
- **Zona de riesgo moderada:** Riesgos que requieren acciones de control y seguimiento periódico.
- **Zona de riesgo alta:** Riesgos que demandan la definición e implementación de acciones de tratamiento prioritarias.
- **Zona de riesgo extrema:** Riesgos críticos que requieren atención inmediata y acciones de tratamiento urgentes para evitar impactos severos sobre la entidad.

ZONA	VALOR
ZONA DE RIESGO BAJA	Mayor de 0 y menor de 5
ZONA DE RIESGO MODERADA	Mayor o igual a 5 y menor de 10
ZONA DE RIESGO ALTA	Mayor o igual a 10 menor de 20
ZONA DE RIESGO EXTREMA	Mayor o igual a 20

Tabla 6. Evaluación Zona de Riegos.

La clasificación por zonas facilita la priorización de los riesgos y orienta la definición de las estrategias de tratamiento, asegurando una gestión eficiente y coherente con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y las mejores prácticas internacionales.

- **Acciones de tratamiento del riesgo**

Teniendo en cuenta el nivel de riesgo determinado en la etapa de evaluación, se definen las acciones de tratamiento a aplicar, las cuales permiten reducir, aceptar, transferir o evitar los riesgos identificados, de acuerdo con su severidad y el apetito de riesgo del ICANH. Estas acciones se describen a continuación:

Zona	Acción requerida
ZONA DE RIESGO EXTREMA	Evitar el riesgo empleando controles que busquen reducir el nivel de probabilidad. Reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa. Compartir o transferir el riesgo mediante la ejecución de pólizas.
ZONA DE RIESGO ALTA	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado. Compartir o transferir el riesgo.
ZONA DE RIESGO MODERADA	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor. Compartir el riesgo.
ZONA DE RIESGO BAJA	Mitigar el riesgo mediante medidas momentáneas y efectivas del proceso que permitan prevenirlo o llevarlo a la zona de riesgo bajo. Asumir el riesgo.

Tabla 7. Dimensión del Riego.

8. MATRIZ DE RIESGOS Y SEGURIDAD DE LA INFORMACIÓN

La valoración de los activos de información del ICANH se consolida en la Matriz de Riesgos y Seguridad de la Información, la cual permite identificar, analizar y gestionar los riesgos asociados a la seguridad y privacidad de la información, considerando las dimensiones de confidencialidad, integridad y disponibilidad, así como los impactos operativos, legales, tecnológicos y reputacionales.

La matriz constituye una herramienta fundamental para la gestión del riesgo, ya que integra de manera estructurada los elementos necesarios para su identificación, análisis, tratamiento y seguimiento.

8.1 IDENTIFICACIÓN DEL RIESGO

Tipos de activos de información

- ***Información y datos de la entidad:*** Incluye la información almacenada o procesada de forma física o electrónica, tales como bases de datos, archivos, contratos, documentación de sistemas de información, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos y de soporte, planes de continuidad del negocio, informes y evidencias de auditoría, entre otros.
- ***Sistemas de información y aplicaciones de software:*** Comprende aplicaciones, interfaces, software de sistema, herramientas de desarrollo y demás utilidades que soportan los procesos institucionales.
- ***Dispositivos de tecnologías de información (hardware):*** Equipos de cómputo, servidores y dispositivos tecnológicos que, por su criticidad, son considerados activos de información, no solo activos físicos.
- ***Soporte para almacenamiento de información:*** Dispositivos y medios utilizados para el almacenamiento de información, tales como memorias USB, discos duros, SAN, NAS y otros dispositivos de respaldo.
- ***Servicios:*** Servicios de computación y comunicaciones que soportan la operación institucional, como conectividad a Internet, servicios de red, correo electrónico, servicios en la nube, intranet y directorios compartidos.

Activo de Información:

Se entiende como activo de información cualquier elemento que contenga, genere, gestione o procese información y que tenga valor para la entidad, por lo cual debe ser protegido.

Ejemplos: bases de datos personales, página web institucional, correo electrónico, unidades de respaldo, servidores de archivos, enlaces de datos principales y de respaldo, firewall perimetral, servicios VPN, entre otros.

Propiedades afectadas por el riesgo

Los riesgos de seguridad de la información se analizan considerando la afectación de una o más de las siguientes propiedades:

- ✓ **Confidencialidad:** Propiedad que garantiza que la información no sea divulgada a personas, entidades o procesos no autorizados.
- ✓ **Disponibilidad:** Propiedad que asegura que la información sea accesible y utilizable cuando sea requerida por un usuario autorizado.
- ✓ **Integridad:** Propiedad que garantiza la exactitud, completitud y confiabilidad de la información.

Descripción del Riesgo:

Corresponde a la descripción de las características generales del riesgo identificado, incluyendo la forma en que se manifiesta y las condiciones bajo las cuales puede materializarse.

Responsable de determinar la materialización del riesgo:

Es el responsable del proceso, gestor de TI o supervisor designado por la entidad, encargado de identificar y reportar la posible materialización del riesgo.

Amenazas:

Situación potencial de un incidente no deseado que puede ocasionar daño a un activo de información, a un sistema o a la organización (ISO/IEC 27000:2018).

Vulnerabilidades:

Debilidad, deficiencia o ausencia de controles que puede ser explotada por una o más amenazas para afectar los activos de información.

8.2 ANÁLISIS DEL RIESGO INHERENTE

El análisis del riesgo inherente se realiza sin considerar la existencia de controles, y permite estimar el nivel inicial de exposición al riesgo.

Probabilidad: Es la medida para estimar la ocurrencia del riesgo y se mide con criterios de Frecuencia, si se ha materializado cierto número de veces en un tiempo determinado) o de factibilidad; teniendo en cuenta la presencia de factores internos y externos, que pueden propiciar el riesgo, aunque este no se haya materializado.

Impacto: Son las consecuencias potenciales que genera el hecho que se materialice el riesgo.

- **Insignificante:** Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
- **Menor:** Si el hecho llegara a presentarse, tendría bajo impacto efecto sobre la entidad.
- **Moderado:** Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
- **Mayor:** Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
- **Catastrófico:** Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Zona de Riesgo: Representa la clasificación del riesgo según su nivel de severidad, ubicándolo en una de las siguientes zonas: baja, moderada, alta o extrema, de acuerdo con la matriz de evaluación definida.

Zona de Riesgo Baja
Zona de Riesgo Moderado
Zona de Riesgo Alta
Zona de Riesgo Extrema

Tabla 8. Zonas de Riego.

8.3 IDENTIFICACIÓN DE CONTROLES

Opciones de manejo del riesgo: Las opciones de manejo del riesgo, representan las posibilidades que se tienen para administrar el riesgo, a través de controles, luego de determinar la probabilidad e impacto del riesgo inherente.

- **Aceptar el riesgo:** No se adoptan medidas adicionales, al considerarse que el riesgo es tolerable.
- **Reducir el riesgo:** Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.
- **Evitar el riesgo:** Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.
- **Compartir el riesgo:** Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este.

Zonas de riesgo y opciones de riesgo: Para nuestro caso se aplicarán las siguientes opciones en el manejo del riesgo:

Zona	Acción
Zona de Riesgo Baja	Reducir el Riesgo
Zona de Riesgo Moderado	Reducir el Riesgo
Zona de Riesgo Alta	Compartir el Riesgo
Zona de Riesgo Extrema	Compartir el Riesgo

Tabla 9. Zonas de Riego y acción.

Descripción del control: Corresponde a la descripción de los controles existentes o propuestos que permiten mitigar el riesgo identificado.

Responsable de ejecutar el control: Persona o dependencia responsable de implementar y mantener los controles definidos.

8.4 RIESGO RESIDUAL

El riesgo residual corresponde al nivel de riesgo que permanece una vez implementados los controles definidos para mitigar el riesgo inherente.

- ***Probabilidad:*** Representa la probabilidad residual, de materialización del riesgo, una vez evaluados los controles establecidos en el proceso, que contrarrestan la probabilidad de materialización del riesgo inherente.
- ***Impacto:*** Representa el impacto residual, de materialización del riesgo, una vez evaluados los controles establecidos en el proceso; que contrarrestan el impacto de la materialización del riesgo inherente.
- ***Zona de riesgo residual:*** Es la nueva zona de riesgo, después de evaluar los controles establecidos por el proceso para mitigar el riesgo inherente.

9. FORMULACIÓN DEL PLAN DE TRATAMIENTOS RIESGOS Y SEGURIDAD DE LA INFORMACIÓN

La formulación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información comprende la definición de acciones orientadas a gestionar los riesgos identificados, mediante la identificación de controles existentes, la implementación de nuevos controles y/o el fortalecimiento de controles actuales, de acuerdo con el nivel de riesgo, la criticidad de los activos de información y la disponibilidad de recursos institucionales.

En este sentido, el plan establece medidas de tratamiento que buscan reducir la probabilidad de ocurrencia y/o el impacto de los riesgos, así como definir responsables, plazos, evidencias y mecanismos de seguimiento que permitan verificar su efectividad y garantizar la mejora continua de la gestión del riesgo.

9.1 OPCIONES EN EL MANEJO DEL RIESGO:

Para el tratamiento de los riesgos, se contemplan las siguientes opciones:

- **Aceptar el riesgo:** Decisión informada de mantener el riesgo en un nivel tolerable para la entidad, sin implementar controles adicionales, o manteniendo los controles existentes, previa evaluación y aprobación correspondiente.
- **Reducir el riesgo:** Implementar o fortalecer controles que permitan disminuir la probabilidad de ocurrencia y/o el impacto del riesgo, con el fin de llevarlo a un nivel aceptable para la entidad.
- **Evitar el riesgo:** Eliminar la fuente del riesgo mediante la suspensión, modificación o no ejecución de la actividad que lo origina, cuando el nivel de riesgo sea inaceptable y no sea viable su mitigación con controles razonables.
- **Compartir el riesgo:** Distribuir o transferir parte del riesgo a un tercero mediante mecanismos contractuales, acuerdos, pólizas u otros instrumentos. En todo caso, la entidad conserva la responsabilidad sobre la gestión y supervisión del riesgo.

10. RESULTADOS DE LA VIGENCIA ANTERIOR

Durante la vigencia 2025, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información registró avances en la implementación de las acciones orientadas al fortalecimiento de los controles de seguridad, la gestión de riesgos y el cumplimiento de los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI). En particular, se consolidó la actualización del instrumento de evaluación de los controles del Anexo A de la norma ISO/IEC 27001:2022, se realizó el análisis de vulnerabilidades a la infraestructura tecnológica, se gestionaron y atendieron incidentes de seguridad de la información, y se efectuó la evaluación de riesgos de seguridad de la información del ICANH mediante el uso de herramientas de seguridad informática. Asimismo, se fortaleció el marco documental asociado a la seguridad de la información.

Como lecciones aprendidas, se evidenció la necesidad de fortalecer la planeación anticipada de las actividades y consolidar mecanismos de seguimiento más

sistemáticos, aspectos que fueron incorporados en la formulación del plan para la vigencia 2026.

a. Resultados del indicador asociado al plan institucional de la vigencia anterior

El indicador del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2025 registró un cumplimiento del 100%, calculado como (Acciones ejecutadas / Acciones planificadas) × 100. Este resultado evidencia que la totalidad de las actividades definidas en el plan fueron ejecutadas conforme al cronograma establecido y soportadas con las evidencias correspondientes, sin reportarse actividades pendientes al cierre de la vigencia.

11. GESTIÓN PLAN VIGENCIA ACTUAL

a. Metodología

La gestión del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del ICANH para 2026 se realizará mediante una metodología sistemática y cíclica, alineada con el MSPI, la norma ISO/IEC 27001 y el Sistema Integrado de Gestión. El proceso inicia con la revisión y validación de la matriz de riesgos, la priorización de riesgos con base en su nivel (impacto × probabilidad) y la criticidad de los activos de información, y la definición de acciones de tratamiento con responsables, cronograma y evidencias. Posteriormente, se ejecutarán acciones como la remediación de vulnerabilidades, el fortalecimiento de controles, la actualización normativa y la gestión documental, en articulación con las áreas responsables y la Oficina de Tecnologías. El avance se verificará de manera periódica mediante la matriz de seguimiento y la evaluación de la efectividad de los controles implementados, soportado en fuentes y evidencias como la matriz de riesgos, informes técnicos, reportes de incidentes y registros asociados. La ejecución y el seguimiento estarán a cargo del Oficial de Seguridad de la Información, la Oficina de Tecnologías, los responsables de proceso y la Oficina Asesora de Planeación.

b. Ejecución – Cronograma

La ejecución del plan se realizará conforme al cronograma definido en la matriz de seguimiento del Plan de Tratamiento de Riesgos de Seguridad de la Información, en la cual se establecen las actividades, responsables, periodos de ejecución, fechas de inicio y finalización para cada acción de tratamiento.

Las actividades se desarrollarán a lo largo de la vigencia 2026, con hitos trimestrales y semestrales según la naturaleza de cada acción.

No.	Actividad	Descripción	Nombre del responsable	Cargo responsable	Mes de ejecución												Fecha inicia	Fecha final	Evidencia de la actividad
					Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic			
01	Realizar seguimiento periódico a la matriz de riesgos de seguridad y privacidad de la información.	Verificar trimestralmente el estado de los riesgos identificados en la matriz de riesgos de seguridad y privacidad de la información del ICANH, evaluando el avance en la implementación de los controles definidos, la efectividad de los tratamientos aplicados y el registro de evidencias, con el fin de garantizar una gestión oportuna y continua del riesgo.	Sandra Silva - Edwin Fabián Olivos	Oficial de Seguridad de la Información - Profesional Especializado			x			x			x			x	1/03/2026	30/12/2026	• Matriz de riesgos de seguridad y privacidad de la información actualizada • Evidencias documentales de implementación de controles (capturas, reportes, configuraciones)
02	Implementar acciones de remediación a las vulnerabilidades de seguridad identificadas en la infraestructura tecnológica y los sistemas de información.	Ejecutar y realizar seguimiento trimestral a las acciones de remediación de las vulnerabilidades identificadas en la infraestructura tecnológica y los sistemas de información del ICANH, priorizando aquellas de mayor riesgo, con el fin de fortalecer los controles de seguridad, reducir la exposición y prevenir incidentes de seguridad de la información.	Sandra Silva - David Jiménez	Oficial de Seguridad de la Información - Profesional Especializado			x			x			x			x	1/03/2026	30/12/2026	• Informes de análisis de vulnerabilidades (escaneos, diagnósticos) • Informes trimestrales de seguimiento a la remediación
03	Implementar y fortalecer los controles de seguridad de la información conforme a la norma ISO/IEC 27001 (Anexo A).	Implementar y fortalecer progresivamente los controles de seguridad de la información del Anexo A de la norma ISO/IEC 27001:2022, con el fin de reducir los riesgos identificados y fortalecer el nivel de madurez del Modelo de Seguridad y Privacidad de la Información (MSPI) del ICANH.	Sandra Silva - Edwin Fabián Olivos	Oficial de Seguridad de la Información - Profesional Especializado			x			x			x			x	2/03/2026	31/12/2026	• Matriz de controles ISO/IEC 27001 Anexo A implementados • Evidencias de adopción de controles (procedimientos, configuraciones, registros).
04	Actualizar la Política de Seguridad de la Información y Privacidad de la Información	Revisar, actualizar y socializar la Política de Seguridad de la Información del ICANH, garantizando su alineación con la normatividad vigente, el Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma ISO/IEC 27001:2022, con el propósito de fortalecer el marco institucional de gobierno de la seguridad de la información.	Sandra Silva - Edwin Fabián Olivos	Oficial de Seguridad de la Información - Profesional Especializado											x		1/11/2026	30/11/2026	• Versión actualizada de la Política de Seguridad y Privacidad de la Información
05	Actualizar los documentos, lineamientos y procedimientos asociados a la seguridad y privacidad de la información.	Revisar, actualizar y versionar los documentos, lineamientos y procedimientos asociados a la seguridad de la información del ICANH, incorporando ajustes normativos, técnicos y del contexto institucional, y gestionar su aprobación y publicación oficial.	Sandra Silva - Edwin Fabián Olivos	Oficial de Seguridad de la Información - Profesional Especializado						x						x	1/06/2026	30/12/2026	• Documentos, lineamientos y procedimientos actualizados y versionados.
				Total actividades planeadas por mes	0	0	3	0	0	4	0	0	3	0	1	4			
				Total actividades planeadas por trimestre	3			4			3			5					

Tabla 10. Matriz de seguimiento Plan de Tratamiento de Riesgos.

c. Seguimiento y evaluación

El seguimiento y la evaluación del Plan de Tratamiento de Riesgos se realizará de manera periódica para medir el avance y la efectividad de las acciones implementadas. La medición se efectuará mediante indicadores de ejecución y cumplimiento, tales como el porcentaje de acciones ejecutadas, el porcentaje de controles implementados y el número de riesgos mitigados; como indicador general se aplicará la fórmula (Acciones ejecutadas / Acciones planificadas) × 100. El seguimiento se soportará en evidencias como informes trimestrales y semestrales, actas y registros de ejecución, documentos actualizados y evidencias técnicas de implementación. Se realizará seguimiento interno trimestral a cargo del Oficial de Seguridad de la Información y la Oficina de Tecnologías, y seguimiento institucional por parte de la Oficina Asesora de Planeación. Los resultados se consolidarán en la matriz institucional de planes y se reportarán conforme al calendario institucional.

CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
Versión	Fecha	Descripción general del cambio
01	2023-03-15	Elaboración del documento
02	2025-01-15	Actualización del documento
03	2025-01-23	Actualización y ajuste integral del documento para la vigencia 2026.

ELABORÓ	REVISÓ	APROBÓ
Cargo: Profesional Especializado Oficina de Tecnologías	**Cargo:** Asesor de Oficina de Tecnologías Contratista Oficina Asesora de Planeación	**Cargo:** Asesor de Oficina de Tecnologías
Fecha: 10-01-2025	**Fecha: 15-01-2025**	**Fecha: 15-01-2025**