SISTEMA DE GESTIÓN INTEGRADO

| PROCESO GOBERNABILIDAD TICS | |
|---|---|
| SUBPROCESO O ACTIVIDAD<br>SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN | CÓDIGO |
| PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL | |

# Plan de tratamiento de Riesgos de Seguridad Digital

## Instituto Colombiano Agropecuario - ICA

## Febrero 2023

*Aprobado en Sesión II – 2023. Comité Institucional de Gestión y Desempeño (Ordinaria) del 15 de Mayo de 2023.*

# TABLA DE CONTENIDO

## INTRODUCCIÓN

El Instituto Colombiano Agropecuario – ICA, establece el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información, Seguridad Digital y continuidad de la Operación de los Servicios de la Entidad, con el cual busca mitigar los riesgos presentes en el análisis de riesgos en relación a la perdida de la Confidencialidad, Integridad y Disponibilidad de los activos de información, con el fin de evitar escenarios que impidan el logro del os objetivos de la entidad; el Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes y posibles eventos que puedan llegar a materializarse.

La estrategia que la Entidad requiere es de carácter preventivo, el cual se basa en comprender el concepto de riesgo, así como el contexto en el que se desarrolla y las acciones planteadas que permitirán reducir la materialización del riesgo, para lo cual se requiere la destreza en la identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos con una mayor objetividad, dando a conocer a la entidad aquellas situaciones y/o escenarios que puedan comprometer el cumplimiento de los objetivos del Instituto Colombiano Agropecuario “ICA”.

Lo anterior dando cumplimiento a:

- La normativa establecida por el estado colombiano.
- CONPES 3854 de 2016.
- Modelo de Seguridad y Privacidad de MINTIC.
- Decreto 1008 de 14 de junio 2018.
- Adopción las buenas prácticas y los lineamientos de los estándares ISO 27001:2022, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

## 1. TERMINOS Y DEFINICIONES

- **Acceso lógico:** Es un acceso en red a través de la ICAnet de la Entidad o de Internet.

- **Activos de Información:** Los activos de información son datos o información propietaria en medios electrónicos, impreso o entre otros medios, considerados sensitivos o críticos para los objetivos del proceso.

- **Almacenamiento:** Se refiere a la forma en la que se almacena el activo, como en medios magnéticos, salas, cajas, PC’s, Servidores, CD’s, DVD, USB, Cintas magnéticas, etc.

- **Área solicitante[1]:** Es la dependencia del Instituto Colombiano Agropecuario ICA que solicita al Funcionario competente y/u ordenador del gasto, la contratación de Bienes o Servicios para satisfacer necesidades o solucionar problemas.

- **Autorización[2]:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

[1] **Fuente**: Definiciones - Manual de Contratación GRFT-GC-MP-001
[2] Fuente: Definiciones Ley 1581 de 2012

- **Base de Datos[3]:** Conjunto organizado de datos personales que sea objeto de Tratamiento;

- **Cifrado:** Es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación (letras, símbolos o números) del contenido que solo pueden comprenderse si se dispone de la clave necesaria para descifrarlos).

- **Clasificación de la Información:** Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulado por la Entidad. Tiene como objetivo asegurar que la información tenga el nivel de protección adecuado. La información debe clasificarse en términos de sensibilidad e importancia para la Entidad.

- **Complementario**: Hace referencia a todo aquel elemento, objeto, individuo o fenómeno que se caracteriza por unirse a otro elemento para completarlo y, en lo posible, mejorarlo.

- **Confidencialidad**: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- **Contraseña**: Código secreto que se introduce en una máquina para poder accionar un mecanismo o para acceder a ciertas funciones informáticas.

- **Contratista**: Persona natural o jurídica que se vincula a la entidad con el objeto de prestar al Instituto un bien o un servicio determinado.

- **Control o Medida:** Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

- **Creación:** Se refiere a la concepción de documentos o datos, el momento en el cual se origina el contenido (digital o físico) de un medio de información.

- **Custodio**: Persona delegada para ejercer el cuidado o vigilancia sobre un activo que le ha sido encargado.

- **Dato personal[4]:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

- **Disponibilidad**: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

- **Destrucción:** Se refiere a la actividad para la destrucción de la información que se maneja sobre el activo en el momento en el que este finaliza su ciclo de vida:

  - Incineración: Destrucción de información exponiéndola a altas temperaturas para quemarla.

  - Borrado Seguro: Aplica solo para medio magnéticos, es un borrado a bajo nivel.

[3] Fuente: Definiciones Ley 1581 de 2012
[4] Fuente: Definiciones Ley 1581 de 2012

- Trituración: Esto aplica más que todo a la destrucción de papel por medio de máquinas trituradoras.

- **Dominio**: Áreas en las que se desarrolla la NTC/ISO 27001.

- **Encargado del Tratamiento[5]:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

- **Etiquetado**: Colocar una etiqueta o rótulo para identificar un elemento.

- **Evento de Seguridad de la Información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

- **Excepciones**: Todo aquello que se excluye de la generalidad o regla común.

- **ICAnet:** Hace referencia a la Intranet del Instituto Colombiano Agropecuario – ICA.

- **Incidente de seguridad de la Información:** Un evento o serie de eventos de seguridad de la Información no deseados o inesperados, que tiene una la probabilidad significativa de comprometer las operaciones del negocio o amenazar la seguridad de la información de los activos críticos que almacenen, procesen y/o gestionen información.

- **Integridad**: Propiedad de Salvaguardar la exactitud y estado completo de los activos.

- **Inventario de activos:** Listado de recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.)

- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.

- **Lineamientos**: Describe en orden numérico y de acuerdo a su importancia las directrices específicas establecidas para la aplicación de la política.

- **Medio Removible:** Dispositivos de almacenamiento independientes del computador que pueden ser transportados libremente. Los dispositivos móviles más comunes son: Memorias USB, discos duros extraíbles, DVD y CD.

- **Política de seguridad de la información:** Establece a alto nivel los objetivos y metas relacionados con la seguridad de la información.

- **Probabilidad:** Es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.

- **Programas Utilitarios**: Los utilitarios o utilidades, son programas diseñados para realizar una función determinada, por ejemplo, un editor, un depurador de código o un programa para recuperar datos perdidos o borrados accidentalmente en el disco duro.

[5] Fuente: Definiciones Ley 1581 de 2012

- **Propietario de la información**: Es el responsable de definir el nivel de clasificación de la información, dar las directrices de uso del activo, autorizar privilegios y definir el ciclo de vida del mismo.

- **Responsable del Tratamiento[6]:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

- **Riesgo:** Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

- **Rol:** El papel que desempeña un individuo o un grupo en una actividad determinada.

- **Seguridad de la Información:** Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

- **Servidor Público**: Es una persona que desempeña un empleo público. Se trata de un trabajador que cumple funciones en el organismo del estado.

- **Sistema de procesamiento de información**: Es un sistema que transforma los datos en información organizada, significativa y útil.

- **Teletrabajador:** Es la persona que utiliza las tecnologías de la información y comunicación como medio para realizar su actividad laboral fuera del local del empleador, en el marco de un contrato de trabajo o de una relación laboral dependiente, en la cual le sean garantizados todos sus derechos laborales.

- **Teletrabajo:** Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo[7].

- **Titular[8]**: Persona natural cuyos datos personales sean objeto de Tratamiento.

- **Token de seguridad:** (también token de autenticación o token criptográfico) es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación. Los tokens electrónicos se usan para almacenar claves criptográficas como firmas digitales o datos biométricos, como las huellas digitales.

- **Transporte de datos:** Considera las diferentes formas en la que se transporta la información de un lado a otro y los cuidados que se debe tener en este proceso, según su nivel de clasificación.

- **Tratamiento[9]:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

- **Usuario**: Es un individuo que utiliza una computadora, un sistema operativo o cualquier sistema informático. Por lo general es una única persona.

---

[6] Fuente: Definiciones Ley 1581 de 2012
7 Fuente: Definiciones Ley 1221 de 2008
[8] Fuente: Definiciones Ley 1581 de 2012
[9] Fuente: Definiciones Ley 1581 de 2012

- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

- **VPN**: (Virtual Private Network) Es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.

## 2. OBJETIVO

- Definir y aplicar los lineamientos para tratar de manera integral los Riesgos de Seguridad y Privacidad de la información, Seguridad Digital y continuidad de la Operación de los Servicios de la Entidad, que pueda afectar al Instituto Colombiano Agropecuario "ICA", con el fin de alcanzar los objetivos, la misión y la visión institucional, preservando la Confidencialidad, Integridad y Disponibilidad de la información.

- Gestionar Riesgos de Seguridad y Privacidad de la información identificados de acuerdo al tratamiento establecido.

- Fortalecer y apropiar el conocimiento al interior de los procesos referente a la gestión de Riesgos Seguridad y Privacidad de la información.

- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.

## 3. ALCANCE

El alcance del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información, Seguridad Digital y continuidad de la Operación de los Servicios de la Entidad y eventos de seguridad debe gestionarse a través de la integración de los procesos de la entidad para adoptar buenas prácticas que contribuyan a la toma de decisiones con el fin de prevenir eventos e incidentes que se tornan en riesgos que puedan afectar el cumplimiento de los objetivos de Instituto Colombiano Agropecuario "ICA".

Estos lineamientos deben poder identificar, analizar, tratar, evaluar y monitorear los Riesgos de Seguridad y Privacidad de la Información en la Entidad.

El Plan de Tratamiento de Riesgo tendrá en cuenta aquellos niveles definidos en la Guía para la Administración de Riesgos adoptada por la entidad al igual que los Riesgos serán aceptados por la Entidad.

## 4. POLITICA DE ADMINISTRACION DE RIESGOS

La alta dirección del Instituto Colombiano Agropecuario ICA, manifiesta su compromiso con la identificación, evaluación y administración de los riesgos que se encuentran presentes en el desarrollo de las actividades establecidas para el cumplimiento de los objetivos encomendados y su misión institucional.

La alta dirección designara un líder responsable por el monitoreo y control de los riesgos que se identifiquen en la entidad a través de los métodos establecidos como la matriz de riesgos por proceso y el mapa de riesgos de la entidad, el líder de riesgos tendrá las siguientes funciones generales; divulgar a todos los funcionarios del Instituto a través de los medios masivos de comunicación, charlas informativas, sesiones de capacitación y socialización de la metodología y política de administración de riesgos establecida.

De la misma forma dará los lineamientos para que al interior de cada uno de los procesos, se aplique la metodología y se actualice la matriz y mapa de riesgos en periodos establecidos por la alta dirección.

Los niveles de riesgo de la entidad estarán controlados de la siguiente manera:
• Nivel de riesgo EXTREMO. Se debe informar a la alta dirección, se requiere acción inmediata y son controlados por el Comité de Coordinación del Sistema de Control Interno y del Sistema de Gestión de la Calidad.

• Nivel de riesgo ALTO. Se debe informar a los responsables de proceso y/o subgerentes y se deben establecer planes para tratar el riesgo y para su control.

• Nivel de riesgo MODERADO. Se deben establecer puntos de control que permitan mitigarlo. Para el control y seguimiento, es trabajo y compromiso de los responsables de proceso y/o subgerentes.

• Nivel de riesgo BAJO. Se deben controlar por los responsables de cada una de las actividades.

Todos los funcionarios del Instituto Colombiano Agropecuario deben conocer la metodología para la identificación y evaluación de riesgos de la entidad y se formaran los analistas de riesgos que se encargaran de aplicar y actualizar las herramientas para la administración y control de los riesgos.

La Administración de Riesgos en el ICA, tendrá un carácter prioritario y estratégico, fundamentada en el modelo de operación por procesos. Son los responsables de los procesos los encargados de implementar los controles, verificar su efectividad, proponer cambios, velar por su adecuada documentación y socialización al interior de cada proceso para disminuir la vulnerabilidad ante los factores de riesgo.

El ICA mantendrá el control adecuado sobre los procesos del Instituto, para esto incorporará gradualmente los principios, conceptos y criterios de las mejores prácticas internacionales aplicables a la administración de los riesgos con el fin de adaptarlos a la naturaleza y realidad de la entidad, con la disponibilidad de recursos necesarios para este fin.

A través del mejoramiento continuo de los procesos definidos en el Sistema de Gestión de la Calidad, buscará la eficacia de los controles que conlleven a la eliminación y mitigación de los riesgos identificados para dar cumplimiento a los lineamientos estratégicos del Instituto Colombiano Agropecuario.

Los líderes de los procesos son los responsables de mantener actualizados los registros relativos al reporte y la evaluación de los riesgos, la necesidad de efectuar actualización y/o modificación a los procedimientos y planes de acción, reportarlos al líder de los riesgos semestralmente o en el evento que se materialice un riesgo para su revisión de los controles para identificar los posibles cambios en la entidad.

Los responsables del manejo de los riesgos de la institución son todos los funcionarios de la entidad a través del ejercicio del autocontrol a sus actividades.

El ICA provendrá siempre con la participación de todos los funcionarios por dar cumplimiento a los requisitos ambientales y sanitarios establecidos, para garantizar un ambiente de trabajo seguro, para proteger la salud e integridad física del equipo humano y que conlleven a la protección del medio ambiente.

## 5. METODOLOGIA

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información, Seguridad Digital y continuidad de la Operación de los Servicios del Instituto colombiano Agropecuario "ICA", contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera:

| GESTIÓN | ACTIVIDAD | TAREA | RESPONSABLE DE LA TAREA | RECURSOS | FECHAS PROGRAMADAS | |
|---|---|---|---|---|---|---|
| | | | | | FECHA INICIO | FECHA FIN |
| **Gestión de Riesgos.** | Definir lineamiento para la identificación de Riesgos de Seguridad. | Actualización de la Guía para la Administración en el capítulo de Riesgos de Seguridad Digital y el instrumento para diligenciamiento de Riesgos de Seguridad Digital. | Oficina de Tecnologias de la Información. | Recursos Humanos<br>Recursos Técnicos | mar-23 | abr-23 |
| | | Aprobación y publicación de la Guía para la Administración en el capítulo de Riesgos de Seguridad Digital. | Oficina Asesora de Planeación - OAP. | Recursos Humanos | mar-23 | abr-23 |
| | Identificación de Riesgos de Seguridad Digital. | Identificación, Análisis y Evaluación de Riesgos de Seguridad Digital. | Oficina de Tecnologias de la Información.<br>Dueños y líderes de los Procesos. | Recursos Humanos | abr-23 | jun-23 |
| | Aceptación y aprobación de Matriz de Riesgos de Seguridad Digital y Planes de Tratamiento. | Aceptación y aprobación de la Matriz de Riesgos de Seguridad Digital. | Dueños y líderes de los Procesos. | Recursos Humanos<br>Recurso Financiero | abr-23 | jun-23 |
| | Publicación de la Matriz de Riesgos de Seguridad Digital. | Publicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. | Oficina Asesora de Planeación - OAP. | Recursos Humanos | jul-23 | jul-23 |
| | Seguimiento al Tratamiento de Riesgos de Seguridad Digital. | Seguimiento al estado de los planes de tratamiento de Riesgos de Seguridad Digital identificados y verificación de evidencias. | Oficina de Tecnologias de la Información. | Recursos Humanos<br>Recurso Financiero | jul-23 | dic-23 |
| | Evaluación de Riesgos residuales de Seguridad Digital. | Evaluación de Riesgos residuales de Seguridad Digital. | Oficina de Tecnologias de la Información.<br>Oficina Asesora de Planeación - OAP. | Recursos Humanos<br>Recurso Financiero | jul-23 | dic-23 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Mejoramiento | Identificar las oportunidades de mejora, acorde a los resultados obtenidos durante la evaluación de riesgos Residuales | Oficina de Tecnologias de la Información.<br><br>Oficina Asesora de Planeación - OAP. | Recursos Humanos | jul-23 | dic-23 |
| | Monitoreo y Revisión | Generación, presentación y reportes de indicadores. | Oficina de Tecnologias de la Información. | Recursos Humanos | jul-23 | dic-23 |

Tabla 1 Metodología

Los controles seleccionados serán confrontados con los estándares ISO 27001:2022 y su anexo A; a fin de determinar las falencias del Instituto Colombiano Agropecuario “ICA”.

## 5.1. METODOLOGIA PARA LA GESTION DE RIESGOS DE SEGURIDAD DIGITAL

La metodología para la identificación, análisis, valoración y tratamiento de los riesgos de seguridad digital, al igual que los riesgos de corrupción, de calidad y ambientales, se enmarca en la estructura establecido por la Norma Técnica Colombiana NTC-ISO 31000:2018 (Figura 1).

- **IDENTIFICACIÓN DEL RIESGO DE SEGURIDAD DIGITAL**

Para la gestión de Riesgos de Seguridad Digital se requiere realizar un conjunto de actividades coordinadas dentro del ICA para abordar los riesgos. Estas actividades ayudan a asegurar que las medidas de gestión de riesgos de seguridad digital sean apropiadas para el riesgo y los objetivos del proceso. Los Riesgos se identifican por procesos y no por activos.

- a. Identificación de tipo de proceso.
- b. Identificación del proceso.
- c. Identificación del subproceso/dirección técnica.
- d. Identificación del tipo de vulnerabilidad
- e. Vulnerabilidad o causa raíz
- f. Identificación del tipo de amenaza
- g. Amenaza o causa inmediata.
- h. Tipo de riesgo
- i. Descripción del riesgo
- j. Clasificación del riesgo.

- **IDENTIFICACIÓN DEL RIESGO DE SEGURIDAD DIGITAL**

Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar de estimar la zona de riesgo inicial (RIESGO INHERENTE).

- a. Análisis de probabilidad
- b. Análisis de impacto
- c. Evaluación del riesgo inherente
- d. Nivel del riesgo inherente

- **EVALUACION DEL RIESGO DE SEGURIDAD DIGITAL**

Se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona del riesgo final (RIESGO RESIDUAL).

- a. Descripción de los controles existentes.
- b. Valoración de los controles.
- c. Nivel del riesgo residual.

- **PLAN DE TRATAMIENTO DEL RIESGO DE SEGURIDAD DIGITAL**

a. Opción de tratamiento

- **MONITOREO Y REVISION DEL RIESGO**

La entidad debe asegurar el logro de sus objetivos, anticipándose a los eventos negativos relacionados con la gestión de riesgos de la entidad. El modelo integrado de planeación y gestión (MIPG), en la dimensión 7 “Control interno”, desarrolla a través de las líneas de defensa la responsabilidad de la gestión del riesgo y control. Las líneas de defensa son un modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control en una entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos.

### 5.2. OPORTUNIDAD DE MEJORA

No sólo deberá centrarse en los riesgos identificados, sino que este análisis del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

## 6. RECURSOS

En el marco de la Gestión de Riesgos de Seguridad y Privacidad de la Información se establece los siguientes recursos para abordar la gestión de riesgos:

| RECURSOS | DEFINICIÓN |
|---|---|
| Humanos | La Oficina de Tecnologías de la Información “OTI” a través del personal de Seguridad de la Información serán los responsables de:<br>- coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en materia de Seguridad y Privacidad de la Información lo cual contribuye a la mejora continua. |
| Técnicos | Se basa en los instrumentos definidos como:<br>- Guía para la administración de riesgos.<br>- Instrumento para la gestión de riesgos (Matriz de riesgos SGSI).<br>- Guía para la administración del riesgo y el diseño de controles en entidades públicas.<br>- Manual Operativo del Modelo Integrado de Planeación y gestión – Política de Seguridad Digital y Política de Gobierno Digital. |
| Logísticos | Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos. |

| | |
|---|---|
| Financiero | Gestión financiera para la adquisición de logísticos, recursos humanos, técnicos, entre otros. |

## 7. PRESUPUESTO

La estimación y asignación del presupuesto para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el Plan de Tratamiento.

## 8. NORMAS APLICABLES

- NTC/ISO 27001:2022.
- NTC/ISO 27005:2009.
- GTC/ISO 27002:2022.
- NTC-ISO 31000:2018.
- Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI y Política de Gobierno Digital.
- Guía para la administración del riesgo y diseño de controles en entidades públicas.
- Manual Operativo del Modelo Integrado de Planeacion y Gestión – Política de Seguridad Digital y Política de Gobierno Digital

## 9. DOCUMENTOS ASOCIADOS

- Procedimiento de Identificación, Valoración y Clasificación de Activos de Información.
- Guía Administración de Riesgos.
- Manual de Políticas de Seguridad y Privacidad de la Información.
- Manual del Sistema de Gestión de Seguridad de la Información – SGSI.
- Plan de Cultura y Sensibilización de Seguridad y Privacidad de la Información.

| Versión | Descripción del cambio | Fecha |
|---|---|---|
| 1 | Creación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. | 28-Feb-2022 |
| 1.1 | Actualización del documento | Feb- 2023 |

| Nombre de quien Elabora: | Nombre de quien Revisa: | Nombre de quien Aprueba: |
|---|---|---|
| Danny Peter Gutierrez Beltran | Carlos Alberto Pinto Hurtado | Carlos Alberto Pinto Hurtado |
| **Firma:** | **Firma** | **Firma** |
| **Cargo:**<br>Líder de Seguridad de la Información Oficina de Tecnología de Información. | **Cargo:**<br>Jefe de Oficina de Oficina de Tecnología de Información | **Cargo:**<br>Jefe de Oficina de Oficina de Tecnología de Información |