PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACÍON 2022

UNIDAD DE RESTITUCIÓN DE TIERRAS

Bogotá D.C., Diciembre 2021

TABLA DE CONTENIDO

1 ANTECEDENTES Y DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

La Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas- UAEGRTD, como entidad pública consciente de la importancia que representa su gestión al servir de órgano administrativo para la restitución de tierras en el país, se ha comprometido con la responsabilidad de salvaguardar la información a través de la implementación del Sistema de Gestión en Seguridad de la Información- SGSI, siguiendo a través del Plan de Seguridad y Privacidad de la Información los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI dispuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTic.

Tras los nuevos elementos que se contemplan en el Modelo Integrado de Planeación y Gestión (MIPG), frente a la dimensión de Gestión con Valores para el Resultado, donde se establece la Política de Seguridad Digital y la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - Diciembre de 2020; se deben seguir los lineamientos para la Administración del Riesgo y Oportunidades en la UAEGRTD incorporando los riesgos de seguridad de la información y de acuerdo con lo establecido en el MSPI, se realizó la identificación y valoración de activos de información, se identificaron riesgos asociados y de acuerdo con su valoración y criticidad se determinaron las acciones para la mitigación de los mismos. Por lo tanto, las actividades identificadas durante este ejercicio harán parte del presente plan.

2 JUSTIFICACIÓN

La información producida en la gestión que adelantan las organizaciones en los diferentes ámbitos del sector hace parte de los activos más importantes para las instituciones que intervienen en el tratamiento de la misma. Para el caso de la Unidad de Restitución de Tierras, la información que se produce y gestiona resulta ser especialmente sensible teniendo en cuenta la labor que tiene la Entidad de “conducir a las víctimas de abandono y despojo, a través de la gestión administrativa para la restitución de sus tierras y territorios, a la realización de sus derechos sobre los mismos, y con esto aportar a la construcción de la paz en Colombia”.

Teniendo en cuenta la complejidad de los casos que se gestionan en la Unidad de Restitución de Tierras, la información se convierte en un atractivo para los profesionales dedicados al robo de información y debido a los nuevos riesgos por la pandemia. *“En el primer semestre de 2020 el CAI Virtual de la Policía Nacional atendió 21.005 ciber incidentes. El incremento por delitos informáticos fue de un 59%, esto equivale a 6.340 denuncias más que el año anterior. Precisamente, Los cibercriminales están aprovechando el interés que genera la crisis del coronavirus para desplegar sus redes y aprovecharse de esta pandemia con fines de cometer ciberdelitos.”*[1]. Por ello, es necesario mejorar constantemente el Subsistema de Seguridad de la Información (SGSI) y que pueda responder a la gestión de los nuevos riesgos en la Unidad, a través de la planeación de un conjunto de proyectos y actividades encaminadas a salvaguardar la información.

Por otra parte, la Política de Seguridad Digital del Modelo Integrado de Planeación y Gestión, se definen las acciones tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada, a través de la gestión de riesgos de seguridad digital para los activos de información críticos de la entidad.

La UAEGRTD ejecuta sus actividades bajo un enfoque de gestión por procesos y su enfoque basado en riesgos. El cumplimiento tanto de sus objetivos de proceso como estratégicos puede verse afectada por riesgos tanto positivos como negativos, con la finalidad de mitigarlos, se hace necesario contar con una metodología encaminada a administrar y prevenir su ocurrencia al interior de la UAEGRTD. Dicha metodología contribuye al conocimiento y mejoramiento de la entidad, a elevar la productividad, a garantizar

1 Cámara Colombiana de Informática y Telecomunicaciones (23 de julio de 2020). COVID-19 el foco de los ciberdelincuentes. https://www.ccit.org.co/articulos-tictac/covid-19-el-foco-de-los-ciberdelincuentes/

la eficiencia y eficacia de los procesos organizacionales y permite la definición de estrategias de mejoramiento continuo, brindándole un manejo sistémico a la entidad.

La administración de riesgos y de las oportunidades se desarrollan a través de la aplicación de esta Guía , en la cual se adaptan los lineamientos emitidos por el DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA –DAFP, MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES y la SECRETARIA DE TRANSPARENCIA DE LA PRESIDENCIA DE LA REPÚBLICA - en la *"Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - Diciembre de 2020",* los lineamiento contemplados en la Ley 1474 de 2011, y la Versión 2 del Modelo Integrado de planeación y gestión el cual incluye el Modelo de las Líneas de Defensa. Esta guía define los roles, responsabilidades, actuaciones y políticas a seguir para coadyuvar a la consecución de los objetivos institucionales que se pretenden alcanzar.

Vale la pena resaltar que el adecuado manejo de los riesgos y oportunidades favorece el desarrollo, la sostenibilidad y el logro de los objetivos institucionales en el marco de la política de restitución de tierras y por ende los fines esenciales del Estado por cuanto se procura la anticipación de la entidad a la ocurrencia de dichos eventos.

3 CONTEXTO NORMATIVO

La Unidad cuenta con el Plan Estratégico Institucional como herramienta estratégica para orientar la gestión en pro del cumplimiento de la misión y visión de la Unidad, en el que se definió una de las líneas estratégicas orientada a fortalecer el uso y aprovechamiento de las tecnologías y la información, como insumos esenciales en el logro de los objetivos estratégicos y la apropiación de una cultura digital.

Así mismo, en esta dimensión la información es un elemento fundamental en los procesos que requiere una constante transformación con un énfasis en la inteligencia del dato, con el propósito de generar información veraz, oportuna y confiable para la toma de decisiones en la Unidad.

Por otra parte, el artículo 147 de la Ley 1955 de 2019, mediante la cual se expide el Plan Nacional de Desarrollo 2018-2022 "Pacto por Colombia, Pacto por la Equidad", establece lo siguiente:

"Las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones. En todos los escenarios la transformación digital deberá incorporar los componentes asociados a tecnologías emergentes, definidos como aquellos de la Cuarta Revolución Industrial, entre otros.

Las entidades territoriales podrán definir estrategias de ciudades y territorios inteligentes, para lo cual deberán incorporar los lineamientos técnicos en el componente de transformación digital que elabore el Ministerio de Tecnologías de la Información y las Comunicaciones.

Los proyectos estratégicos de transformación digital se orientarán por los siguientes principios:

1. Uso y aprovechamiento de la infraestructura de datos públicos, con un enfoque de apertura por defecto.
2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.
3. Plena interoperabilidad entre los sistemas de información públicos que garantice el suministro e intercambio de la información de manera ágil y eficiente a través de una plataforma de interoperabilidad. Se habilita de forma plena, permanente y en tiempo real cuando se requiera, el intercambio de información de forma electrónica en los estándares definidos por el Ministerio TIC, entre entidades públicas. Dando cumplimiento a la protección de datos personales y salvaguarda de la información.

4. Optimización de la gestión de recursos públicos en proyectos de Tecnologías de la Información a través del uso de los instrumentos de agregación de demanda y priorización de los servicios de nube.
5. Promoción de tecnologías basadas en software libre o código abierto, lo anterior, sin perjuicio de la inversión en tecnologías cerradas. En todos los casos la necesidad tecnológica deberá justificarse teniendo en cuenta análisis de costo-beneficio.
6. Priorización de tecnologías emergentes de la Cuarta Revolución Industrial que faciliten la prestación de servicios del Estado a través de nuevos modelos incluyendo, pero no limitado a, tecnologías de desintermediación, DLT (Distributed Ledger Technology), análisis masivo de datos (Big data), inteligencia artificial (AI), Internet de las Cosas (IoT), Robótica y similares.
7. Vinculación de todas las interacciones digitales entre el Estado y sus usuarios a través del Portal Único del Estado colombiano.
8. Implementación de todos los trámites nuevos en forma digital o electrónica sin ninguna excepción, en consecuencia, la interacción del Ciudadano-Estado sólo será presencial cuando sea la única opción.
9. Implementación de la política de racionalización de trámites para todos los trámites, eliminación de los que no se requieran, así como en el aprovechamiento de las tecnologías emergentes y exponenciales.
10. Inclusión de programas de uso de tecnología para participación ciudadana y Gobierno abierto en los procesos misionales de las entidades públicas.
11. Inclusión y actualización permanente de políticas de seguridad y confianza digital.
12. Implementación de estrategias público-privadas que propendan por el uso de medios de pago electrónicos, siguiendo los lineamientos que se establezcan en el Programa de Digitalización de la Economía que adopte el Gobierno nacional.
13. Promoción del uso de medios de pago electrónico en la economía, conforme a la estrategia que defina el Gobierno nacional para generar una red masiva de aceptación de medios de pago electrónicos por parte de las entidades públicas y privadas.

PARÁGRAFO. Los trámites y servicios que se deriven de los anteriores principios podrán ser ofrecidos tanto por personas jurídicas privadas como públicas, incluyendo a la entidad que haga las veces de articulador de servicios ciudadanos digitales, o la que defina el Ministerio TIC para tal fin."

Por su parte, el artículo 148 de la misma ley, señala lo siguiente:

"Gobierno Digital como Política de Gestión y Desempeño Institucional. Todas las entidades de la administración pública deberán adelantar las acciones que señale el Gobierno nacional a través del Ministerio de Tecnologías de la Información y las Comunicaciones para la implementación de la política de Gobierno Digital.

Esta política liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones contemplará como acciones prioritarias el cumplimiento de los lineamientos y estándares para la Integración de trámites al Portal Único del Estado Colombiano, la publicación y el aprovechamiento de datos públicos, la adopción del modelo de territorios y ciudades inteligentes, la optimización de compras públicas de tecnologías de la información, la oferta y uso de software público, el aprovechamiento de tecnologías emergentes en el sector público, incremento de la confianza y la seguridad digital y el fomento a la participación y la democracia por medios digitales.

El Gobierno implementará mecanismos que permitan un monitoreo permanente sobre el uso, calidad, nivel de satisfacción e impacto de estas acciones."

Por otro lado, el día 8 de noviembre de 2019 fue expedido el documento Conpes 3975 que consagra la "Política Nacional para la Transformación Digital e Inteligencia Artificial. Dicho documento, dentro de su numeral 5.1 - Plan de Acción, incluye una actividad relacionada con la mejora de la política de gobierno digital con el fin de abordar la adopción y explotación de la transformación digital en el sector público. Particularmente se señala lo siguiente:

*"**Línea de acción 3. Mejorar el desempeño de la política de gobierno digital, para abordar la adopción y explotación de la transformación digital en el sector público**.*

En primer lugar, el Ministerio de las Tecnologías de Información y las Comunicaciones desarrollará los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital, con el fin que puedan enfocar sus esfuerzos en este tema. Estos lineamientos se publicarán por medio de una actualización al Manual de gobierno digital y serán revisados y actualizados periódicamente. Esta acción iniciará en noviembre de 2019 y finalizará en marzo de 2020."

En ese sentido la Política de Gobierno Digital cuenta con un habilitador transversal llamado Seguridad y Privacidad de la Información el cual: *"Busca las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información de las entidades del Estado, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se desarrolla a través del Modelo de Seguridad y Privacidad de la Información, que orienta la gestión e implementación de la seguridad de la información en el Estado."*

La Gestión de Riesgos de Seguridad de la Información es parte fundamental para lograr el cumplimiento de la política y de acuerdo con lo establecido en el Decreto 612 de 2018, la creación del *Plan de Tratamiento de Riesgos de Seguridad Digital* debe estar alineado con la Planeación Estratégica Institucional y debe ser formulado, aprobado, publicado en la página web institucional y ejecutado de manera anual por cada una de las áreas responsables para la vigencia, en conjunto con la programación del Plan de Acción Institucional. Todos los planes institucionales estarán elaborados bajo los lineamientos dispuestos por las entidades responsables tales como el Departamento Administrativo de la Función Pública, Ministerio de Tecnologías de la Información y las Comunicaciones, Secretaria de Transparencia, Ministerio de Hacienda y Crédito Público, Archivo General de la Nación entre otros.

4 TÉRMINOS

Definidos en el sistema Strategos

5 OBJETIVO GENERAL

Mitigar los riesgos de seguridad de la información para preservar la integridad, disponibilidad y confidencialidad de la información definiendo el Plan de Tratamiento de Riesgos.

6 OBJETIVOS ESPECÍFICOS

- Tratar de manera integral los riesgos de Seguridad y Privacidad de la Información para alcanzar los objetivos, la misión y la visión institucional.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.

7 DESCRIPCIÓN DE ACTIVIDADES

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, el conocimiento de esta desde un punto de vista estratégico, de la aplicación de tres (3) pasos básicos para su desarrollo y de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada. A continuación, se puede observar la estructura completa con sus desarrollos básicos que se ilustran en la siguiente figura.

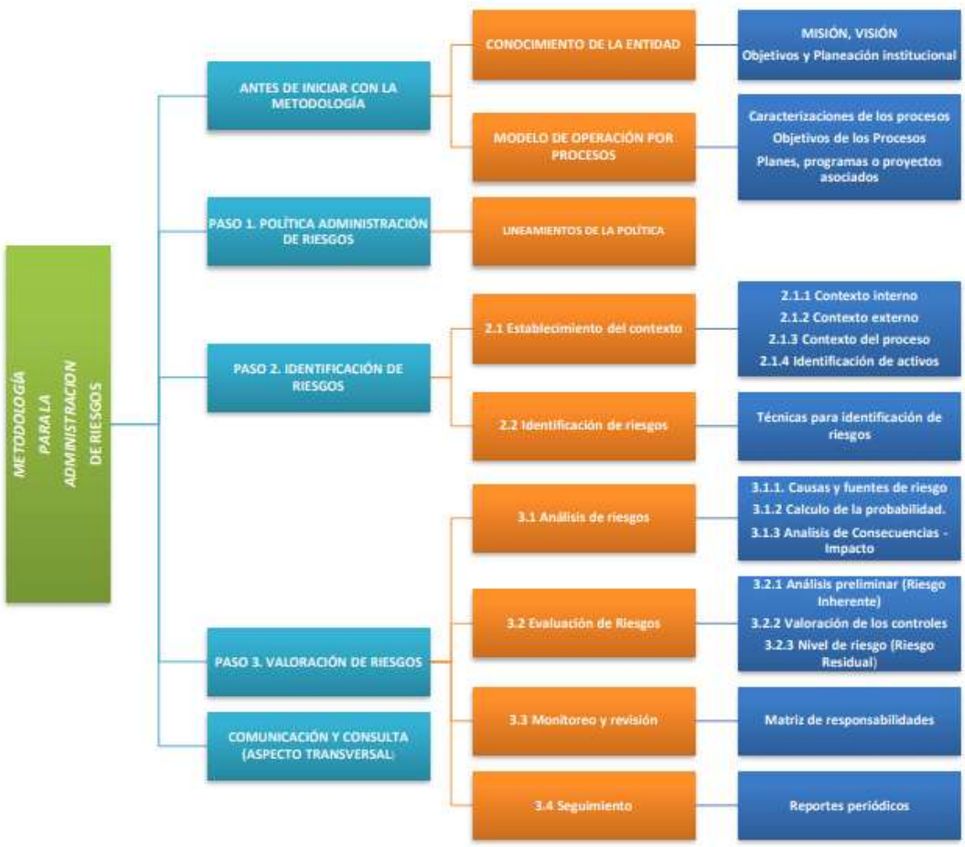

Ilustración 1 - Metodología para la administración del riesgo en la UAEGRTD.[2]

8 ACCIONES Y METAS

Después de realizar los pasos de la metodología establecida en La Unidad y donde después de evaluar sus controles, se detectaron algunos riesgos que por su probabilidad y el impacto que pueden generar se encuentran en zonas no tolerables para la entidad, por la tanto se identifican las acciones adicionales para el tratamiento de los riesgos los cuales se presentan a continuación en la siguiente tabla:

Riesgo	Acción a Desarrollar	Nivel aplicación	Evidencia/ Entregable	Responsable	Fecha Final
Uso inapropiado de los equipos de las estaciones usuario de las oficinas	Incluir en la inducción y prueba de conocimiento el módulo de Seguridad de la información.	Nivel Central y Territorial	Reportes con el resultado de la inducción	Oficial de Seguridad de la Información	mar-22
Uso inapropiado de los equipos de las estaciones usuario de las oficinas	Realizar campañas para sensibilizar a los colaboradores en materia de seguridad y privacidad de la información para el cuidado de equipos de oficina	Nivel Central y Territorial	Piezas de comunicación	Líder Uso Apropiación	mar-22

[2] Intranet de la Unidad de Restitución de Tierras (Mayo de 2020). Guía para la administración del riesgo y oportunidades. https://bit.ly/37E4xjQ

Uso inadecuado de controles en el acceso físico a cajas fuertes que contienen token y claves	Incluir en la inducción y prueba de conocimiento el módulo de Seguridad de la información	Nivel Central y Territorial	Reportes con el resultado de la inducción	Oficial de Seguridad de la Información	mar-22
Uso inadecuado de controles en el acceso físico a cajas fuertes que contienen token y claves	Realizar campañas para sensibilizar a los colaboradores en materia de seguridad y privacidad de la información para el cumplimiento de la política de control de acceso	Nivel Central y Territorial	Piezas de comunicación	Líder Uso Apropiación	jun-22
Robo o perdida de equipos transportables por Negligencia, descuido ó casos fortuitos	Generar campaña sobre la necesidad de solicitar el cifrado de los equipos cuando sale de las instalaciones de la Unidad.	Nivel Central y Territorial	Piezas de comunicación	Líder Uso Apropiación	mar-22
Robo o perdida de equipos transportables por Negligencia, descuido ó casos fortuitos	Cifrar los discos duros de los equipos transportables solicitados.	Nivel Central y Territorial	Pantallazos con identificación de equipo y cifrado	Ingenieros territoriales / ingenieros de soporte	jun-22
Robo o perdida de equipos transportables por Negligencia, descuido ó casos fortuitos	Verificar la eficacia en la implementación del control cifrado de equipos transportables.	Nivel Central y Territorial	Reporte de revisión	Ingeniero de seguridad	sep-22
Dispositivos de oficina con Fallas o daños	Realizar campañas para sensibilizar a los colaboradores en materia de seguridad y privacidad de la información para el cuidado de equipos de oficina	Nivel Central y Territorial	Piezas de comunicación	Líder Uso Apropiación	mar-22
Fallas en el acceso en Sistemas de información y Aplicaciones de Centros de datos y Nube	Realizar proceso centralizado para desactivación de usuarios en los sistemas de información y aplicaciones	Nivel Central	Herramienta de desactivación operando	Líder de sistemas de información/ Información	sep-22
Instalación de código malicioso en Estaciones Usuario	Realizar campañas para sensibilizar a los colaboradores en materia de seguridad y privacidad de la información para minimizar las amenazas de malware	Nivel Central y Territorial	Piezas de comunicación	Líder Uso Apropiación	jun-22
Instalación de software malicioso en estaciones de usuario personal para trabajo en casa	Realizar campañas para sensibilizar acerca de los riesgos de seguridad en el trabajo en casa	Nivel Central y Territorial	Piezas de comunicación	Líder Uso Apropiación	mar-22

Instalación de software malicioso en estaciones de usuario personal para trabajo en casa	Mantener la solución de escritorios virtuales y entregar a los colaboradores definidos un computador virtual	Nivel Central	Reporte de asignación de los escritorios virtuales	Ingeniero de infraestructura	sep-22
Instalación de software malicioso en estaciones de usuario personal para trabajo en casa	Mantener y mejorar el control de acceso de red (NAC) para validar los parámetros necesarios para el acceso a través de los equipos personal	Nivel Central	Reporte de validación de equipos personales a través del NAC	Ingeniero de Seguridad	sep-22
Fraude o fuga de información por revelación de contraseñas de administrador	Realizar campañas para sensibilizar acerca de riesgos de revelación /uso inadecuado de claves contraseñas	Nivel Central y Territorial	Piezas de comunicación	Líder Uso Apropiación	jun-22
Fraude o fuga de información por revelación de contraseñas de administrador	Ampliar la difusión del uso del gestor de contraseñas KeePass para los usuarios	Nivel Central y Territorial	Piezas de comunicación	líder uso y Apropiación	jun-22
Bases de datos con inadecuada administración en información en el Centro de datos y en la nube	Actualizar los lineamientos para la administración y configuración de las bases de datos frente al cumplimiento (mínimos: diccionario de datos, diagrama entidad relación y script).	Nivel Central	Documento actualizado	Líder de Información	sep-22
Bases de datos con inadecuada administración en información en el Centro de datos y en la nube	Solicitar respaldos de las configuraciones y la información de las bases de datos productivas.	Nivel Central	Prueba de restauración de la configuración y la información de las bases de datos productivas	Líder de Información	dic-22
Fraude, fuga o revelación de información, por correos electrónicos y medios extraíbles	Mantener el módulo de DLP de acuerdo con el nivel de licenciamiento y funcionalidad asociada a Microsoft 365 E3.	Nivel Central y Territorial	Configuraciones en la plataforma	Profesional especializado servicios tecnológicos	sep-22
Fraude, fuga o revelación de información, por correos electrónicos y medios extraíbles	Implementar fuentes únicas de información para preservar la integridad, confidencialidad y disponibilidad.	Nivel Central	Sistema de componentes de información	Líder de información	dic-22
Perdida de datos debido a escasa definición de lineamientos para la gestión de interoperabilidad en la UAEGRTD	Revisar y actualizar la documentación (arquitectura, procedimientos, guías, etc.) definida para el intercambio de información	Nivel Central	Documentación actualizada	Líder de información	dic-22
Perdida de datos debido a escasa definición de lineamientos para la gestión de	Realizar el monitoreo periódico sobre la plataforma de interoperabilidad y el cumplimiento de los	Nivel Central	Reportes de monitoreo	Líderes de sistemas de información/ servicios Tecnológicos /información	dic-22

interoperabilidad en la UAEGRTD	controles implementados.				

9 RECURSOS

- Presupuesto

Los recursos disponibles para la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad De la Información están definidos en el componente asociado a proveer los servicios de tecnologías de la información, a través del proyecto de inversión registrado en el proyecto Implementación de mecanismos para el acceso de las victimas a la ruta de restitución y protección de tierras y territorios a nivel nacional BPIN 2021011000036 y el proyecto Contribución a la mejora de la Gestión del Proceso de Protección y Restitución de las Tierras y Territorios Despojados o Abandonados Forzosamente a Nivel Nacional BPIN 2019011000064.

- Requerimientos logísticos,técnicos y /o Tecnológicos

Para la actualización del Plan de Tratamiento de Riesgos de Seguridad y Privacidad De la Información, se contemplan los recursos humanos, técnicos y presupuestales dispuestos en el proyecto de inversión de la Unidad para el componente tecnológico.

10 RESPONSABLE DE LA SUPERVISIÓN Y SEGUIMIENTO

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Entidad tiene como responsable de su ejecución y seguimiento a la Oficina de Tecnologías de la Información en cabeza de su Jefe de Oficina, así como del Subcomité de Gestión de Gobierno y Seguridad Digital de la Unidad.

11 EVALUACIÓN

El seguimiento del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se verá reflejado con las actividades reportadas con los instrumentos de planeación incluyendo el Plan de Acción y en el Plan Anual de Adquisiciones, el cual incluye actividades donde se deben adquirir elementos y servicios para el desarrollo y ejecución del mismo.

Adicionalmente, se realizarán reuniones de seguimiento periódicas donde se reporte el seguimiento mediante el indicador con el fin de monitorear el avance de las actividades definidas para el cumplimiento de este plan.

12 ANEXOS

No aplica.

13 PARTICIPANTES EN LA ELABORACIÓN

Enrique Cusba Garcia- Jefe Oficina Tecnologías de la Información
Francisco Andrés Daza Cardona – Oficial de Seguridad de la Información - Oficina Tecnologías de la Información

14 CONTROL DE CAMBIOS

Versión 2.0 se actualiza el documento conforme a las nuevas iniciativas y ajustes en los proyectos existentes.