PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

UNIDAD
DE RESTITUCIÓN
DE TIERRAS

Bogotá D.C., Diciembre 2021

TABLA DE CONTENIDO

1 ANTECEDENTES Y DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

De acuerdo con lo establecido en la política de Gobierno Digital, se genera un nuevo enfoque en donde no sólo el Estado sino también los diferentes actores de la sociedad son parte fundamental para el desarrollo integral del Gobierno Digital en Colombia, donde las necesidades y problemáticas van a definir el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público. En este sentido, y siguiendo el objetivo de la política: *"Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital"*, y en concordancia con la *"Guía para la Construcción del PETI – Planeación de la Tecnología para la Transformación Digital"* publicada por el Ministerio de Tecnologías de la Información y las Comunicaciones en el año 2019, el PETI es parte integral de la estrategia de las entidades públicas y uno de los principales instrumentos que permiten identificar su visión, objetivos, las estrategias y los proyectos para lograr los resultados esperados, dentro de un proceso de transformación que involucre tecnologías digitales. En tal sentido, el PETI se convierte en la hoja de ruta para una entidad, sector o territorio, en materia de TI alineado a los objetivos institucionales.

Así mismo y de acuerdo con lo indicado en el Marco de Referencia de Arquitectura Empresarial, la Oficina de Tecnologías de la Información, debe contar con una estrategia de TI documentada, que contenga la proyección estratégica en el tiempo, que para el caso de la Unidad actualmente será hasta la vigencia 2022, y deberá ser actualizado permanentemente debido a los cambios de la estrategia del sector o de la Entidad, la normatividad y el desarrollo tecnológico.

En este sentido dentro del PETI se ha establecido una línea de acción enfocada a la *"Optimizar el Subsistema de Gestión de Seguridad de la Información",* para lo cual se hace necesario establecer un Plan de Seguridad y Privacidad de la Información que guie las líneas para la consecución de los objetivos frente a las estrategias que se plantean en este documento.

Cabe resaltar que, en el mes de octubre de 2020, al realizar una medición de los avances en la entidad se realizó un diagnóstico utilizando la herramienta dispuesta por MinTIC, para determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad, cuyo resultado para la efectividad de los controles se encuentra en un 67% repartido de la siguiente manera:

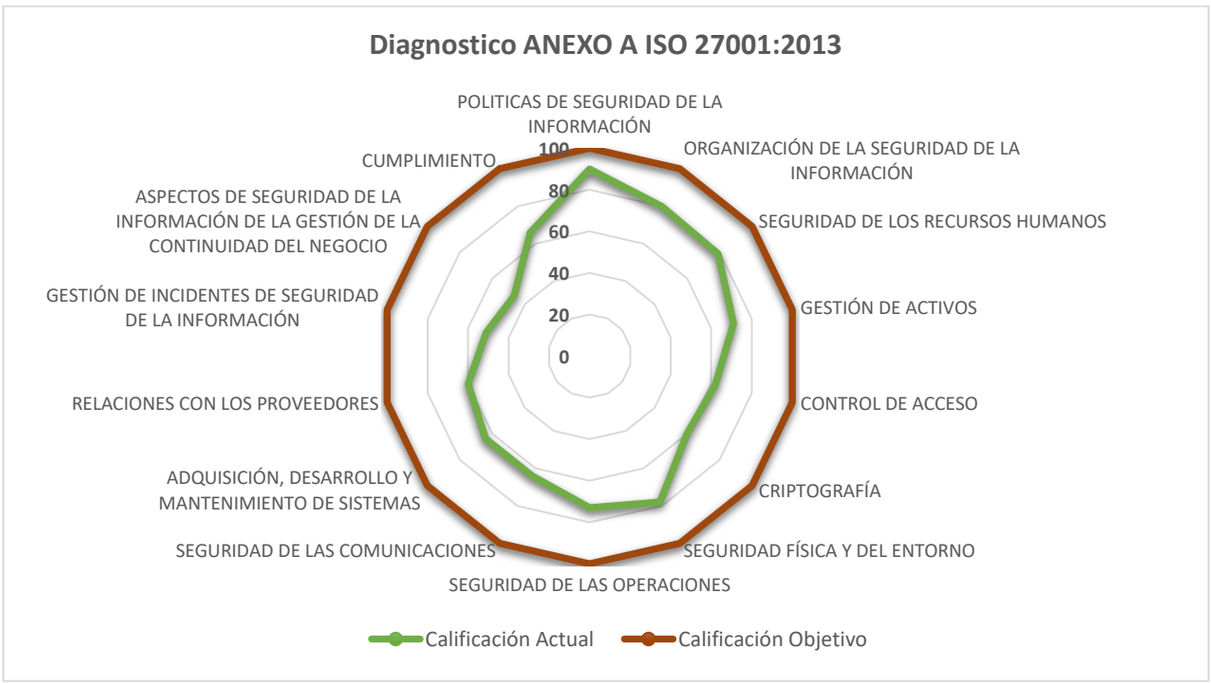

Ilustración 1 – Diagnostico Anexo A ISO 27001:2013

En cuanto al diagnóstico de FURAG frente a la política de Seguridad Digital del Modelo Integrado de Planeación y Gestión para la vigencia 2020 arrojo un avance del 80%.

Actualmente la entidad cuenta con una Política general que integra a los subsistemas de gestión, la cual se encuentra debidamente formalizada, donde se establecieron los objetivos y el compromiso de la alta dirección, adicionalmente se cuenta con las políticas complementarias de Seguridad y Privacidad de la Información donde se detallan los lineamientos y las actuaciones que deben seguir los colaboradores para mantener una adecuada seguridad de la información en la entidad.

Para dar alcance a lo estipulado en la Política de seguridad digital frente al Plan de Tratamiento de Riesgos, se definió adoptar la metodología definida por el Departamento Administrativo de la Función Pública siguiendo lo descrito en la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, basándose en una integración adecuada entre el Modelo de Seguridad y Privacidad de la Información (MSPI) y el enfoque por procesos, permitiendo identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos de información identificados. Actualmente se cuenta con el Plan de Tratamiento de Riesgos basado en esta metodología.

Respecto a la gestión de los activos de Información se identifican y actualizan periódicamente, estos se encuentran asociados a los riesgos de seguridad de la información identificados.

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 esta. 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. *"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".* 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.

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."

Asi mismo de acuerdo con lo establecido en el Decreto 612 de 2018, la creación del Plan de Seguridad y Privacidad de la Información 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 2021, 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

Ver definición de los términos en el Sistema de Información STRATEGOS

5 OBJETIVO GENERAL

Implementar, y evaluar acciones efectivas a través de la elaboración del Plan de Seguridad y Privacidad de la Información para fortalecer el Subsistema de Gestión de Seguridad de la Información en la Unidad de Restitución de Tierras, en procura de la mejora continua y de la salvaguarda de la información.

6 OBJETIVOS ESPECÍFICOS

- Establecer las principales líneas de actuación a seguir en el corto y mediano plazo para la implementación y mantenimiento del SGSI.
- Definir las actividades para implementar los controles, procedimientos, políticas necesarias para realizar un adecuado tratamiento de los riesgos de seguridad y privacidad de la información en todos los procesos de la UAEGRTD de acuerdo con la criticidad de los activos de información relacionados.

- Definir los indicadores, metas y recursos necesarios para la consecución del plan.
- Definir acciones para la evaluación y el monitoreo del plan.

7 DESCRIPCIÓN DE ACTIVIDADES

Definir el plan de seguridad y privacidad de la Información en el marco de la implementación y mejora del Subsistema de Gestión de Seguridad de la Información (SGSI) para la UAEGRTD, utilizando como guía la norma ISO-IEC- 27001:2013 y Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC para proteger la confidencialidad, integridad y disponibilidad de la información contenida en los activos críticos de la Unidad de Restitución de Tierras.

La Unidad de Restitución de Tierras ha adoptado el MSPI como guía para la construcción del Subsistema de Gestión de Seguridad de la Información (SGSI), este modelo está basado en el Marco de Referencia de Arquitectura TI el cual fue propuesto para el desarrollo de las arquitecturas empresariales sectoriales, institucionales y territoriales, convirtiéndose en soporte de la Política de Gobierno Digital.

El MSPI permite que las Entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información. Este modelo contempla un ciclo de operación que consta de cinco (5) fases:

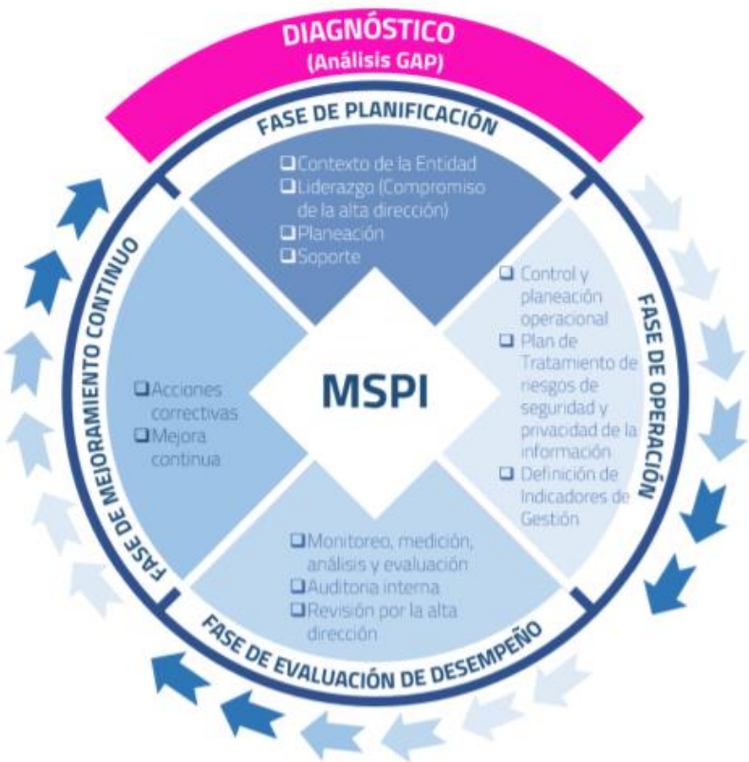

Ilustración 1 - Metodología MSPI

1. **Diagnóstico**: Realizar un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 4 de mejora continua.

2. **Planificación**: Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.
3. **Operación**: Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.
4. **Evaluación** de desempeño: Determinar el sistema y forma de evaluación de la adopción del modelo.
5. **Mejoramiento Continuo**: Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

8 METAS

A continuación, se presentan las actividades de acuerdo con cada fase, la responsabilidad de la ejecución de estas se encuentra a cargo de la Oficina de Tecnologías de la Información:

No.	Fase	ACTIVIDADES	ENTREGABLES	FECHA
1	**Diagnostico**	Identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, tener en cuenta la auditoria, diagnósticos de FURAG y MinTIC.	Herramienta de diagnostico	dic-21
2	**Planificación**	Generar el plan de actualización documental de seguridad de la información. (políticas, procedimientos, guías, etc.)	Documento con la lista de Actividades y Fechas.	feb-22
3	**Planificación**	Generar el Plan de Capacitación y Sensibilización actualizado.	Documento con el Plan de Capacitación Sensibilización y Comunicación formalizado.	feb-22
4	**Planificación**	Revisar y actualizar el plan de continuidad de negocio de TI.	Documento Plan Actualizado	mar-22
5	**Operación**	Adquirir certificados SSL para la vigencia.	Acta de Entrega de SSL	abr-22
6	**Operación**	Identificar y actualizar activos de información en los procesos.	Matrices de Activos Diligenciadas	may-22
7	**Operación**	Revisar y Actualizar la Política de Seguridad y Privacidad de la Información.	Política de Seguridad de la Información y Complementarias Actualizadas	jun-22
8	**Operación**	Identificar y actualizar riesgos de seguridad de la información en los procesos.	Riesgos de Seguridad actualizados	jul-22
9	**Operación**	Implementar proyecto de Ethical Hacking	Informe ejecutivo y detallado.	jul-22
10	**Operación**	Gestionar y mantener la infraestructura de seguridad perimetral de La Unidad.	Infraestructura actualizada y en operación.	ago-22
11	**Operación**	Optimizar los métodos de prevención de fuga de la información (DLP) en correo electrónico.	Reporte de configuración y usuarios a los que aplica.	sep-22
12	**Operación**	Gestionar renovación y actualización del sistema de respaldo.	Infraestructura actualizada y en operación.	oct-22

13	**Evaluación**	Realizar auditoría interna donde se tengan en cuenta temas de seguridad de la información.	Informes de auditoria	nov-22
14	**Mejora Continua**	Revisar resultados auditoría interna, FURAG, y diagnósticos.	Reporte con las brechas identificadas.	nov-22
15	**Operación**	Implementar el plan de actualización documental asociados a seguridad de la información.	Reporte de avance del plan	nov-22
16	**Operación**	Implementar Plan de Sensibilización y Comunicación de Seguridad de la Información.	Reporte de avance del plan	dic-22
17	**Operación**	Implementar Plan de Continuidad del Negocio	Reporte de avance del plan	dic-22
18	**Mejora Continua**	Actualizar los planes de mejoramiento de seguridad de la información.	Planes de mejoramiento en el sistema.	dic-22
19	**Operación**	Gestionar renovación y actualización del licenciamiento de Antivirus	Infraestructura actualizada y en operación.	dic-22

9 RECURSOS

9.1 Presupuesto

Los recursos disponibles para la implementación del Plan 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.

9.2 Requerimientos logísticos, técnicos y/o tecnológicos

➢

Para la actualización del Plan 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 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 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 de este.

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.