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

UNIDAD
DE RESTITUCIÓN
DE TIERRAS

Bogotá D.C., Noviembre de 2020

TABLA DE CONTENIDO

1 ANTECEDENTES Y DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

La Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas- URT, 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 nueva Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital, así como, el Diseño de Controles en Entidades Públicas; en ese sentido se actualizó la *Guía para la Administración del Riesgo y Oportunidades de la URT* [1] incorporando los riesgos de seguridad digital y de acuerdo con lo establecido en el MSPI, se realizó la identificación y valoración de activos de información, se agruparon los activos, se identificaron riesgos asociados y de acuerdo con su valoración y criticidad se determinaron las acciones para la mitigación de los mismos. 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 ciberincidentes. 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."*[2]. 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 URT 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 URT. Dicha metodología contribuye al conocimiento y mejoramiento de la entidad, a elevar la productividad, a garantizar 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[3], 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

---

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

2 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/

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

DE LA REPÚBLICA - en la *"Guía para la Administración de los Riesgos y el Diseño de Controles en Entidades Públicas"* de octubre de 2018, 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

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 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 TERMINOS

- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **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).
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **Probabilidad:** es la posibilidad de que algo pueda suceder. La probabilidad puede ser definida, determinada y medida objetiva o subjetivamente, y puede expresarse de forma cualitativa o cuantitativa.
- **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.
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

5 OBJETIVO GENERAL

Gestionar los riesgos de seguridad de la información y seguridad digital para preservar la integridad, disponibilidad y confidencialidad de la información siguiendo la metodología establecida en la Unidad de Restitución de Tierras.

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 ACCIONES

7.1 Metodología

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.

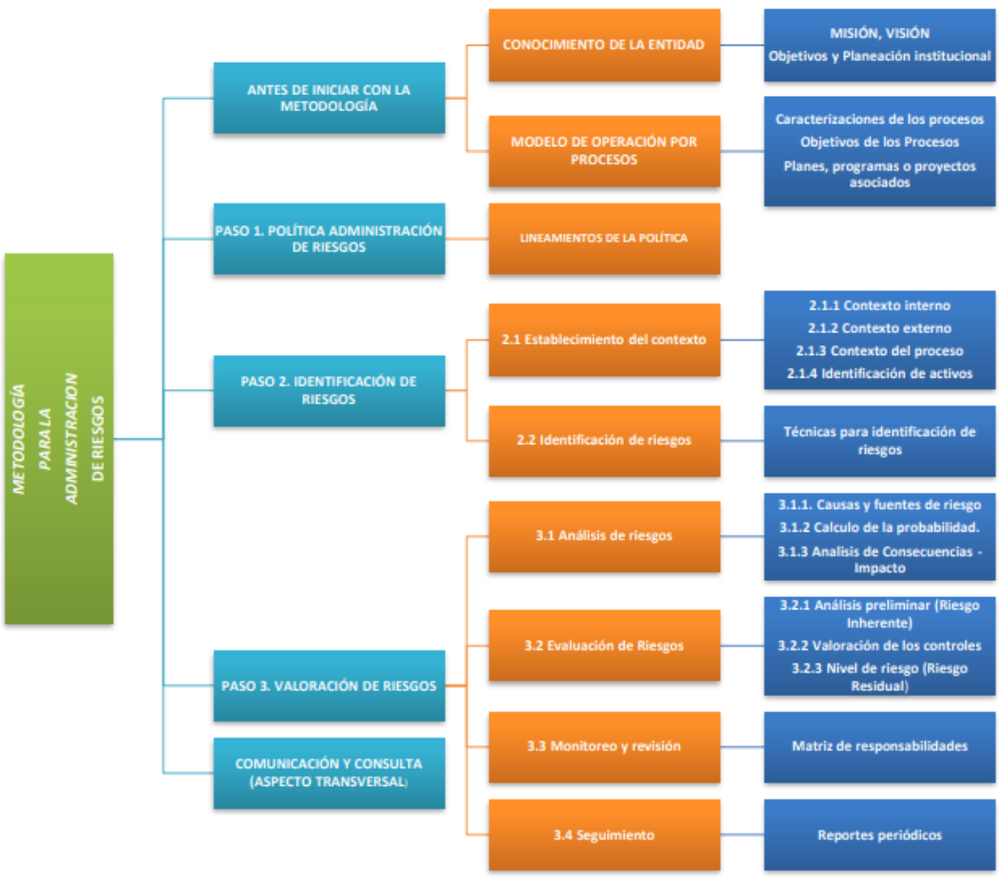

Ilustración 1 - Metodología para la administración del riesgo en la URT.[4]

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

7.2 Riesgos Identificados

A continuación, se encuentran los riesgos de Seguridad y privacidad de la Información identificados para la Unidad:

	RIESGO	DESCRIPCIÓN DEL RIESGO
1	Equipos con fallas en el datacenter de nivel central	Equipos con fallas debido a Mantenimiento Insuficiente causando Inoportunidad en la prestación de los servicios
2	Uso inapropiado de los equipos de las estaciones usuario de las oficinas	Uso inapropiado de los equipos debido a la deficiencia en la aplicación de políticas de seguridad causando fuga de información
3	Uso inadecuado de controles en el acceso físico a cajas fuertes que contienen token y claves	Uso inadecuado de controles en el acceso físico causando sanciones legales para la entidad.
4	Robo o perdida en Equipos Transportables que se utilizan en salidas a campo o trabajo en casa	Robo o perdida debido a negligencia, descuido o casos fortuitos causando exposición de información sensible
5	Equipos de oficina con Fallas o daños	Equipos de oficina con fallas o daños debido a desconocimiento en la manipulación de los elementos causando inoportunidad en la prestación de los servicios.
6	Cambios no autorizados en software o hardware con servicios de TI de los datacenter y la nube	Cambios no autorizados debido por no seguir lo dispuesto en el procedimiento Gestión de Cambios causando fallas en la prestación del servicio
7	Requerimientos con definiciones inadecuadas en el software de los servicios de TI de los datacenter	Requisitos de desarrollo y / o adquisición de software con definiciones inadecuadas causando resistencia en el uso de las aplicaciones
8	Sistemas de información con fallas en el acceso en los datacenter y en la nube	Sistemas de información con fallas en el acceso debido a inadecuados procedimientos de solicitud activación y desactivación de credenciales causando fuga y alteración de información
9	Instalación de software malicioso en las estaciones de usuario	Instalación de software malicioso debido a descarga e instalación no controlada, causando indisponibilidad de los servicios y/o perdida y/o fuga de información
10	Instalación de software malicioso en estaciones de usuario personal para trabajo en casa	Instalación de software malicioso debido a equipos no gobernados por la entidad causando Inoportunidad en la prestación de los servicios
11	Revelación de contraseñas de administrador	Revelación de contraseñas debido a Falta de control en la custodia causando robo, fraude o perdida de información afectando la prestación del servicio
12	Bases de datos con inadecuada administración en información en el datacenter y en la nube	Bases de datos con errores de configuración debido a inadecuada administración y definición de modelos de datos causando indisponibilidad de los sistemas de información
13	Perdida de información en el datacenter y en la nube	Perdida de datos debido a escasos respaldos e insuficientes controles de seguridad causando afectaciones de los sistemas de información
14	Fraude, fuga o revelación de información	Fraude, fuga o revelación de información, debido a información extraída de las Bases de datos y correo electrónico causando vulneración de los derechos de la población objeto de los procesos de restitución
15	Datos vulnerados en Información en datacenter y la Nube	Datos vulnerados debido a lineamientos, procedimientos y esquemas de gobierno de intercambio de información inadecuados causando Pérdida de la integridad, disponibilidad y confidencialidad de la información, vulnerando los derechos de las víctimas

7.3 Actividades del plan de tratamiento

Después de identificar en la tabla anterior los diferentes riesgos los cuales después de evaluar sus controles, la probabilidad y el impacto se encontraban en zonas no tolerables para la entidad, por la tanto se identifican las acciones adicionales para el tratamiento de los siguientes riesgos:

Riesgo	Acción a Desarrollar	Nivel aplicación	Evidencia/Entregable	Responsable	Fecha Inicio	Fecha Final
1	Gestionar para obtener los recursos económicos que garanticen el desarrollo de los mantenimientos, el cambio tecnológico y personal para el monitoreo de las plataformas de hardware	Nivel Central	PAA, Informes de monitoreo de los responsables	Jefe OTI, Ing., infraestructura, redes y seguridad	31/07/2020	12/31/2020
4	Incluir en el catálogo de servicios el CIFRADO DE EQUIPOS en la categoría de SEGURIDAD	Nivel Central y Territorial	Catálogo de servicios	Líder mesa de servicios y Oficial de Seguridad	01/01/2021	30/03/2021
	Ajustar el procedimiento de administrativa GL-PR-02 SALIDA DE BIENES DEL ALMACEN, para incluir el cifrado de equipos	Nivel Central y Territorial	Procedimiento ajustado	líder mesa de servicios	01/01/2021	30/04/2021
	Generar campaña sobre la necesidad de solicitar el cifrado de los equipos cuando sale de las instalaciones de la Unidad	Nivel Central y Territorial	Campaña y evidencia adjunta al GLPI con el cifrado del equipo	Líder UyA / Ingeniero de Seguridad	01/04/2021	30/06/2021
	Cifrar los discos duros de los equipos transportables solicitados: Responsable: ing. TI territorio y soporte	Nivel Central y Territorial	Pantallazos con identificación de equipo y cifrado	ingenieros territoriales **/** ingenieros de soporte	01/01/2021	31/12/2021
	Verificar de la eficacia en la implementación del control: Seguridad de la información	Nivel Central y Territorial	Reporte de implementación	Ingeniero de Seguridad	01/07/2021	31/08/2021
	Incluir en el curso de la escuela URT y evaluación sobre, el tema de uso de equipos transportables y discos portables.	Nivel Central y Territorial	Curso en la escuela de URT.	Líder de UyA Ingeniero de Seguridad y mesa de servicios	01/01/2021	30/06/2021
5	Actualizar los equipos de oficina acorde con los lineamientos definidos desde el nivel central (OCS, actualizaciones de Windows, antivirus, mantenimientos preventivos y correctivos, office 365, carpetas compartidas)	Nivel Central y Territorial	Informe de cumplimiento de lineamientos indicados y soportes en GLPI según corresponda	Ingenieros territoriales y soporte	01/01/2021	31/12/2021
	Incluir en el curso de la escuela URT y evaluación sobre el buen manejo y cuidado de equipos de oficina	Nivel Central y Territorial	Curso en la escuela de URT.	Líder de UyA Ingeniero de Seguridad y mesa de servicios	01/01/2021	30/06/2021
7	Ampliar los responsables de la validación y aprobación de las historias de usuario por parte del líder del proceso y el lideres funcionales	Nivel Central	Actas de reunión	Líder de sistemas de información	01/01/2021	31/03/2021
8	Unificar las bases de las diferentes áreas e implementar un sistema de información	Nivel Central	Sistema de información en producción	Líder de sistemas de información	01/01/2021	31/03/2021
	Realizar la desactivación de los usuarios a través de las interfaces de usuario de las diferentes aplicaciones que hacen parte de los servicios de TI.	Nivel Central	Registro en base de datos,	Mesa de servicio, Líder de información, Líder de Sistemas de Información	01/01/2021	31/12/2021

Riesgo	Acción a Desarrollar	Nivel aplicación	Evidencia/Entregable	Responsable	Fecha Inicio	Fecha Final
	Desarrollar las interfaces graficas de gestión de usuarios para los aplicativos que no tienen los niveles de seguridad adecuados	Nivel Central	módulos de seguridad implementados, pantallazos de las interfaces graficas en producción	Líder de Sistemas de información	01/01/2021	30/06/2021
10	Sensibilizar acerca de riesgos de seguridad en el trabajo en casa	Nivel Central y Territorial	Actas de Asistencia	Ingeniero de Seguridad	01/01/2021	30/06/2021
11	Ampliar la difusión del uso del gestor de contraseñas KeePass para los usuarios administradores	Nivel Central y Territorial	piezas de comunicación	Líder de UyA, Ingeniero de Seguridad	01/01/2021	30/09/2019
12	Lineamientos para la administración de las bases de datos	Nivel Central	Documento con el lineamiento. Copia de la Comunicación a los administradores para el estricto cumplimiento.	Líder de Información	01/01/2021	30/06/2021
	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	01/01/2021	30/06/2021
14	Implementación de DLP de acuerdo con el nivel de licenciamiento y funcionalidad asociada a Microsoft 365 E3	Nivel Central	Configuraciones en la plataforma	Servicios Tecnológicos	01/01/2021	30/06/2021
15	Definir y formalizar las políticas, lineamientos y procedimientos necesarios para la gestión de interoperabilidad en la Unidad.	Nivel Central	Documentos formalizados en el SIPG	Jefe OTI / Asesor transformación digital	01/01/2021	31/03/2021
	Definir el procedimiento de acceso incorporando la revisión Acuerdos de Confidencialidad u otros instrumentos, que incluyan el tratamiento de datos personales	Nivel Central	Protocolo y Procedimiento de intercambio	Profesional Gestión de Interoperabilidad	01/01/2021	31/03/2021
	Documentar la matriz de roles para el intercambio de información	Nivel Central	Matriz de roles para intercambio de información	Profesional Gestión de Interoperabilidad /Oficial de Seguridad	01/01/2021	31/03/2021
	Exigir la firma de Acuerdos de Confidencialidad o cualquier otro instrumento, con terceros, cuando implique intercambio de datos, en donde quede plasmado el tratamiento de los datos por parte del tercero.	Nivel Central	Acuerdos de confidencialidad o el instrumento	Gestor de Interoperabilidad	01/01/2021	31/03/2021
	Documentar la arquitectura de la plataforma de interoperabilidad y sus controles	Nivel Central	Arquitectura formalizada	Líder de información/ Líder de sistemas de información	01/01/2021	31/03/2021
	Realizar el Monitoreo periódico sobre la plataforma de interoperabilidad y el cumplimiento de los controles implementados	Nivel Central	Reportes de monitoreo	Profesional Gestión de Interoperabilidad/ líderes de sistemas de información, servicios Tecnológicos e Información	01/01/2021	30/06/2021

8 METAS

La meta es completar el 90% de las actividades establecidas en este plan.

9 RECURSOS

9.1 Presupuesto

Los recursos disponibles para su la ejecución de este plan están definidos en el componente asociado a proveer los servicios de tecnologías de la información a través del proyecto de inversión registrado en el BPIN BPIN2018011000177-Fortalecimiento y BPIN 2018011000454 - Restitución tierras y Territorios.

9.2 Requerimientos logísticos, técnicos y/o tecnológicos

Para la ejecución de este Plan se contemplan los recursos técnicos y tecnológicos, los cuales se encuentran plasmados en el Plan Anual de Adquisiciones del proceso de Gestión TI.

9.3 Recursos humanos

Para lograr los objetivos propuestos en el plan se requiere de la participación de todos los colaboradores de la OTI incluidos los Ingenieros en territorio para la ejecución y cumplimiento de las actividades. Adicionalmente para el cumplimiento de los lineamientos y procedimientos que se lleguen a formalizar se requerirá del compromiso y la colaboración de diferentes dependencias en la entidad.

10 ANÁLISIS DE RIESGOS

Los riesgos relacionados con la ejecución e implementación de los proyectos definidos en el Plan Estratégico de Tecnológicas de la Información PETI (2021-2022) se encuentran identificados dentro del mapa de riesgos del proceso Gestión de TI entre los que se resaltan: i)Indisponibilidad de los servicios de TI, ii) Deficiencia en la prestación de los servicios, iii) Afectación sobre los servicios de TI en beneficio propio, de un tercero, a cambio de una retribución económica y/o beneficio particular y los riesgos definidos de Seguridad Digital los cuales son tratados en este Plan.

11 INDICADORES

Se reportará periódicamente como indicador el porcentaje de avance de este Plan, la fórmula para calcular el indicador será: (*número de actividades completadas / actividades planeadas) x 100.*

12 EVALUACIÓN

Como mecanismo de seguimiento y evaluación 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. Adicionalmente se reportarán los avances y evidencias de las actividades asociados al Plan de Acción del proceso en la herramienta dispuesta para el seguimiento.

13 ANEXOS

N/A

14 PARTICIPANTES EN LA ELABORACIÓN

N/A

15 CONTROL DE CAMBIOS

- Relacionar las modificaciones que se realizan al documento cuando se emite una nueva versión de este

	NOMBRE:	CARGO / ROL:	FECHA	FIRMA:
ELABORADO POR:	Francisco Daza	Oficial de Seguridad de la Información	23/11/2020	**Original Firmado**
REVISADO POR:	Claudia Patricia Hernández	Jefe Oficina Asesora de Planeación	23/11/2020	**Original Firmado**
APROBADO POR:	Enrique Cusba García	Jefe Oficina de Tecnologías	23/11/2020	**Original Firmado**