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

UNIDAD
DE RESTITUCIÓN
DE TIERRAS

Bogotá D.C., agosto 2021

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐ **Fecha de aprobación**: 30/08/2021

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 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 **MC-GU-02 Guía para la Administración del Riesgo y Oportunidades de la UAEGRTD** [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 Administrativa Especial de Gestión de Restitución de Tierras Despojadas, 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 UAEGRTD, 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 UAEGRTD, 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 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 DE LA REPÚBLICA - en la *"Guía para la*

---

1. MC-GU-02 Guía para la administración del riesgo y oportunidades. Sistema de Información Strategos – Módulo documentos https://strategos.restituciondetierras.gov.co/STRATEGOS/files/mod_documentos/documentos/MC-GU-02/versiones/MC-GU-02.pdf

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 MC-GU-02 Guía para la administración del riesgo y oportunidades. Sistema de Información Strategos – Módulo documentos https://strategos.restituciondetierras.gov.co/STRATEGOS/files/mod_documentos/documentos/MC-GU-02/versiones/MC-GU-02.pdf

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

Ver definición de los términos en el Sistema de Información STRATEGOS.

- Riesgo
- Amenaza
- Vulnerabilidad
- Probabilidad
- Control o Medida
- Datos Personales
- Plan de continuidad del negocio
- Plan de tratamiento de riesgos
- Ciberseguridad
- Ciberespacio
- Activo
- Activo de Información

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.

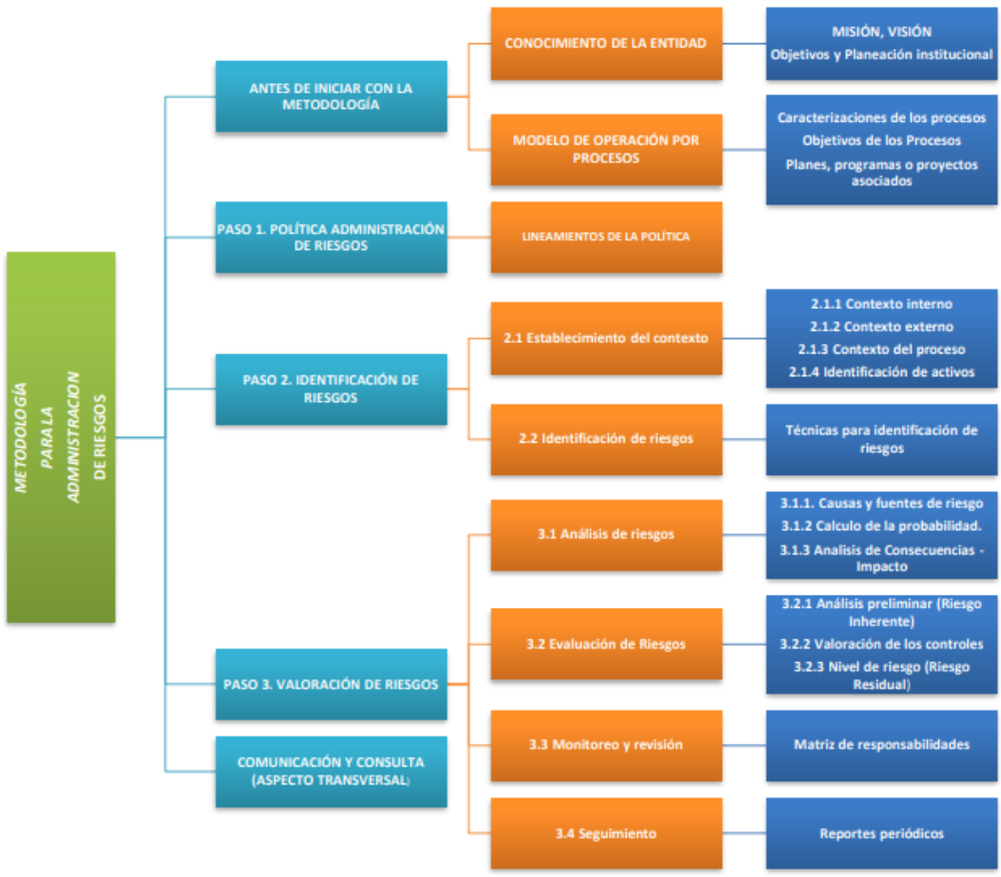

Ilustración 1 - Metodología para la administración del riesgo en la UAEGRTD.[4]

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 Centros de datos	Equipos con fallas debido a Mantenimiento Insuficiente causando Inoportunidad en la prestación de los servicios de TI
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 y/o mantenimiento insuficiente 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 exposición de información sensible
4	Robo o pérdida de equipos transportables por negligencia, descuido ó casos fortuitos, falta de cifrado de los equipos.	Robo o pérdida de equipos transportables debido a negligencia, descuido ó casos fortuitos, falta de cifrado de los equipos causando exposición de información sensible
5	Dispositivos de oficina con Fallas o daños	Dispositivos de oficina con fallas o daños debido a desconocimiento en la manipulación de los elementos causando inoportunidad en la prestación de los servicios.

[4] MC-GU-02 Guía para la administración del riesgo y oportunidades (Mayo 2020). Sistema de Información Strategos – Módulo documentos https://strategos.restituciondetierras.gov.co/STRATEGOS/files/mod_documentos/documentos/MC-GU-02/versiones/MC-GU-02.pdf

	RIESGO	DESCRIPCIÓN DEL RIESGO
6	Cambios no autorizados en Sistemas de información y Aplicaciones Centros de datos y Nube	Cambios no autorizados debido a deficiencia en la aplicación de procedimiento Gestión de Cambios causando Fallas en la prestación del servicio.
7	Requerimientos con definiciones inadecuadas en Sistemas de información y Aplicaciones Centros de datos y Nube.	Requisitos de desarrollo y / o adquisición de software con definiciones inadecuadas causando resistencia en el uso de las aplicaciones.
8	Fallas en el acceso en Sistemas de información y Aplicaciones de Centros de datos y Nube.	Fallas en el acceso debido a inadecuados procedimientos de solicitud activación y desactivación de credenciales causando fuga y alteración de información
9	Instalación de código malicioso en Estaciones Usuario	Instalación de Código malicioso debido a descarga de información sin control causando pérdida 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 cambios en el modelo de operación de la entidad causando Inoportunidad en la prestación de los servicios.
11	Fraude o fuga de información por revelación de contraseñas de administrador.	Fraude o fuga de información debido a Falta de control en la custodia causando Robo o fraude o perdida de información que pueda afectar la prestación del servicio.
12	Bases de datos con inadecuada administración en información en el Centro de datos y en la nube.	Bases de datos con inadecuada administración debido a errores de configuración y definición de modelos de datos causando indisponibilidad de los sistemas de información.
13	Pérdida de datos en información en el Centro de datos y en la nube.	Pérdida 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, por correos electrónicos y medios extraíbles.	Fraude, fuga o revelación de información, debido a información obtenida a través de los correos electrónicos y medios extraíbles causando vulneración de los derechos de la población objeto de los procesos de Restitución.
15	Obligaciones contractuales con Incumplimiento por personal no calificado en Recurso Humano de TI.	Obligaciones contractuales con Incumplimiento por personal no calificado debido a falta de capacidades técnicas y principios éticos causando inoportunidad en la prestación del servicio.
16	Pérdida de datos debido a escasa definición de lineamientos para la gestión de interoperabilidad en la UAEGRTD.	Pérdida de datos debido a escasa definición de lineamientos para la gestión de interoperabilidad en la UAEGRTD causando inoportunidad en la prestación del servicio.

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
2	Incluir en la inducción y prueba de conocimiento el módulo	Nivel Central y Territorial	Pantallazo de los temas incluidos en	Oficial de Seguridad de la Información	01/03/2021	30/06/2021

	de Seguridad de la información.		el módulo y preguntas en la prueba de conocimiento			
	Realizar campañas para sensibilizar a los colaboradores en materia de seguridad y privacidad de la información.	Nivel Central y Territorial	Actas de asistencia	Oficial de Seguridad de la Información y Uso Apropiación	01/03/2021	30/11/2021
3	Incluir en la inducción y prueba de conocimiento el módulo de Seguridad de la información	Nivel Central y Territorial	Pantallazo de los temas incluidos en el módulo y preguntas en la prueba de conocimiento	Oficial de Seguridad de la Información	01/03/2021	30/06/2021
	Realizar campañas para sensibilizar a los colaboradores en materia de seguridad y privacidad de la información.	Nivel Central y Territorial	Actas de asistencia	Oficial de Seguridad de la Información y Uso Apropiación	01/03/2021	30/11/2021
4	Incluir en el catálogo de servicios el CIFRADO DE EQUIPOS en la categoría de SEGURIDAD.	Nivel Central y Territorial	catálogo de servicios actualizado	líder mesa de servicios y Oficial de Seguridad	01/03/2021	30/06/2021
	Acordar los ajustes del procedimiento de administrativa GL-PR-06 PRESTACIÓN DEL SERVICIO DE SEGURIDAD, VIGILANCIA Y MEDIOS TECNOLOGICOS, para incluir el cifrado de equipos.	Nivel Central y Territorial	Evidencia de la aceptación del ajuste de GSOA	líder mesa de servicios	01/01/2021	30/04/2021
	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	01/01/2021	31/12/2021
	Verificar la eficacia en la implementación del control: Seguridad de la información.	Nivel Central y Territorial	Reporte de implementación	ingeniero de seguridad	01/07/2021	30/08/2021
	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	líder Uso y Apropiación /ingeniero de Seguridad	01/04/2021	30/06/2021
5	Realizar campaña sobre el buen manejo y	Nivel Central y Territorial	Campaña	líder Uso y Apropiación	01/01/2021	30/06/2021

	cuidado de equipos de oficina					
8	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	01/01/2021	31/07/2021
9	Realizar campañas para sensibilizar a los colaboradores en materia de seguridad y privacidad de la información.	Nivel Central y Territorial	Actas de asistencia	Oficial de Seguridad de la Información y Uso Apropiación	01/03/2021	30/11/2021
10	Sensibilizar acerca de riesgos de seguridad en el trabajo en casa	Nivel Central y Territorial	Actas de Asistencia	Oficial de Seguridad de la Información y Uso Apropiación	01/01/2021	30/10/2021
	Implementar 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	01/05/2021	31/12/2021
	Implementar 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	01/08/2021	31/12/2021
11	Sensibilizar acerca de riesgos de revelación /uso inadecuado de claves contraseñas	Nivel Central y Territorial	Actas de Asistencia	Oficial de Seguridad de la Información y Uso Apropiación	01/01/2021	30/06/2021
	Ampliar la difusión del uso del gestor de contraseñas KeePass para los usuarios administradores.	Nivel Central y Territorial	piezas de comunicación	líder uso y Apropiación/ ingeniero seguridad	01/01/2021	30/09/2021
12	Generar lineamientos para la administración y configuración de las bases de datos, (mínimos: diccionario de datos, diagrama entidad relación y script).	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	Líder de Información	01/01/2021	30/06/2021

			de datos productivas			
14	Implementación de DLP de acuerdo con el nivel de licenciamiento y funcionalidad asociada a Microsoft 365 E3.	Nivel Central y Territorial	Configuraciones en la plataforma	líder servicios tecnológicos/ Oficial de Seguridad	01/01/2021	30/06/2021
	Implementar fuentes únicas de información para preservar la integridad, confidencialidad y disponibilidad.	Nivel Central	Sistema de componentes de información	líder de información	01/04/2021	30/11/2021
16	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	líder de información	01/01/2021	31/03/2021
	Definir y formalizar las políticas, lineamientos y procedimientos necesarios para la gestión de interoperabilidad en la Unidad.	Nivel Central	Documentos formalizados en el SIPG	líder de información	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	líder de información	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 plasmadas la responsabilidad por el tratamiento de la información por parte del tercero.	Nivel Central	Acuerdos de confidencialidad o el instrumento	líder de información	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	31/05/2021
	Realizar el Monitoreo periódico sobre la plataforma de interoperabilidad y el cumplimiento de los controles implementados.	Nivel Central	Reportes de monitoreo	líderes de sistemas de información/ servicios Tecnológicos /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 y servicios de información de restitución y protección de tierras y territorios abandonados a través de los proyectos de inversión de la Entidad registrados en el Banco Nacional de Programas y Proyectos -BPIN para la vigencia 2021, a saber: i) proyecto "Fortalecimiento de la Gestión Administrativa de la Unidad de Restitución de Tierras Nacional" **BPIN** 2018011000177 – ii) Proyecto de "**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

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

MC-GU-02 Guía para la administración del riesgo y oportunidades.

14 PARTICIPANTES EN LA ELABORACIÓN

- Francisco Andrés Daza Cardona- Oficial de Seguridad- Oficina Tecnologías de la Información

15 CONTROL DE CAMBIOS

- Primera versión: inicial
- Segunda versión: producto de la actualización de la matriz de riesgos Junio 2021 y se integran riesgos sobre trabajo en casa.