

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



UNIDAD
DE RESTITUCIÓN
DE TIERRAS

Bogotá D.C., noviembre de 2019



 UNIDAD DE RESTITUCIÓN DE TIERRAS	UNIDAD ADMINISTRATIVA ESPECIAL DE GESTIÓN DE RESTITUCIÓN DE TIERRAS DESPOJADAS	PÁGINA: 2 DE 9
	PROCESO: NOMBRE DEL PROCESO AL QUE PERTENECE SEGÚN MAPA DE PROCESOS	CÓDIGO: ALFANUMÉRICO
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 1.0

TABLA DE CONTENIDO

1	ANTECEDENTES Y DESCRIPCIÓN DE LA SITUACIÓN ACTUAL.....	3
2	RELACIÓN CON EL PLAN DE ACCIÓN Y/O PLAN INSTITUCIONAL	3
3	JUSTIFICACIÓN	3
4	MARCO NORMATIVO	4
5	MARCO CONCEPTUAL	4
6	OBJETIVO	4
7	ALCANCE	4
8	DESCRIPCIÓN DE ACTIVIDADES	4
9	METAS.....	8
10	CRONOGRAMA DE ACTIVIDADES	8
11	ENTREGABLES	8
12	PRESUPUESTO	8
13	REQUERIMIENTOS LOGÍSTICOS, TÉCNICOS Y/O TECNOLÓGICOS	8
14	METAS E INDICADORES	8
15	RESPONSABLE DE LA SUPERVISIÓN Y SEGUIMIENTO	8
16	EVALUACIÓN	9
17	PARTICIPANTES EN LA ELABORACIÓN	9
18	CONTROL DE CAMBIOS	9

 UNIDAD DE RESTITUCIÓN DE TIERRAS	UNIDAD ADMINISTRATIVA ESPECIAL DE GESTIÓN DE RESTITUCIÓN DE TIERRAS DESPOJADAS	PÁGINA: 3 DE 9
	PROCESO: NOMBRE DEL PROCESO AL QUE PERTENECE SEGÚN MAPA DE PROCESOS	CÓDIGO: ALFANUMÉRICO
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 1.0

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 los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI generado 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 hace 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 RELACIÓN CON EL PLAN DE ACCIÓN Y/O PLAN INSTITUCIONAL

Este plan se encuentra relacionado con el Plan de Seguridad y Privacidad de la información el cual tiene como objetivo: *preservar la integridad, disponibilidad y confidencialidad de la información a partir de la adopción y optimización del Modelo de Seguridad y Privacidad de la Información (MSPI) el cual está enmarcado en la Norma ISO 27001:2013*".

Así mismo está alineado con la Política de Seguridad de la Información² donde en el "Artículo 4 Objetivos" se menciona: "Minimizar el riesgo de los procesos misionales de la Unidad".

3 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. "La ciberdelincuencia tiene tal penetración que sabemos que cerca del 80% de las empresas en el mundo han sido o son hackeadas, y tardan casi 200 días en darse cuenta de que han sido vulneradas, y no siempre es por agentes del exterior, ya que casi el 28% de los ataques son internos"³. Por ello, es necesario implementar y mantener un Subsistema de Seguridad de la Información (SGSI) que permita mitigar los riesgos en la URT, a través de la planeación de un conjunto de proyectos y actividades encaminadas a la consecución de la misión.

Por otra parte, con el objeto de dar cumplimiento al marco de gobierno impartido en el CONPES 3854 del 11 de abril de 2016, donde se establece sean desarrolladas medidas que aseguren la información de los ciudadanos frente a las amenazas informáticas, así como la Política de Gobierno Digital, en el cual se definen las acciones tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada donde se debe realizar la gestión de riesgos de seguridad digital para los activos de información críticos de la entidad.

1 Unidad de Restitución de Tierras (23 de diciembre de 2019). Resolución 00925 <https://bit.ly/35czFon>.

2 Unidad de Restitución de Tierras (marzo de 2019) Guía para la administración del riesgo y oportunidades. <https://bit.ly/37E4xiQ>

3 Seguridad en América (25 de mayo de 2018). Una tercera parte de ataques cibernéticos surgen del interior de las organizaciones. México. <https://bit.ly/35tlpHQ>

 <p>UNIDAD DE RESTITUCIÓN DE TIERRAS</p>	UNIDAD ADMINISTRATIVA ESPECIAL DE GESTIÓN DE RESTITUCIÓN DE TIERRAS DESPOJADAS	PÁGINA: 4 DE 9
	PROCESO: NOMBRE DEL PROCESO AL QUE PERTENECE SEGÚN MAPA DE PROCESOS	CÓDIGO: ALFANUMÉRICO
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 1.0

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, 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 de los Riesgos y el Diseño de Controles en Entidades Públicas” de octubre de 2018, los lineamientos 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.

4 MARCO NORMATIVO

Ver Normograma en el Sistema de Información STRATEGOS

5 MARCO CONCEPTUAL.

Ver Términos en el Sistema de Información STRATEGOS.

6 OBJETIVO

Implementar, y evaluar acciones efectivas para abordar los riesgos de seguridad de la información identificados en la Unidad de Restitución de Tierras, en procura de la mejora continua y de la salvaguarda de la información en atención a la Política de Seguridad y Privacidad de la Información establecida en la resolución 0925 de 2016.

7 ALCANCE

Definir en este plan las actividades que harán parte del tratamiento de riesgos de seguridad digital Información en el marco de la implementación y mejora del Subsistema de Gestión de Seguridad de la Información (SGSI) donde el alcance definido es para los riesgos relacionados a los grupos de activos de información críticos de la Unidad de Restitución de Tierras identificados en durante la vigencia el 2019, siguiendo lo establecido en la Guía para la Administración del Riesgo y Oportunidades de la entidad para la vigencia 2020.

8 DESCRIPCIÓN DE ACTIVIDADES

8.1 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:

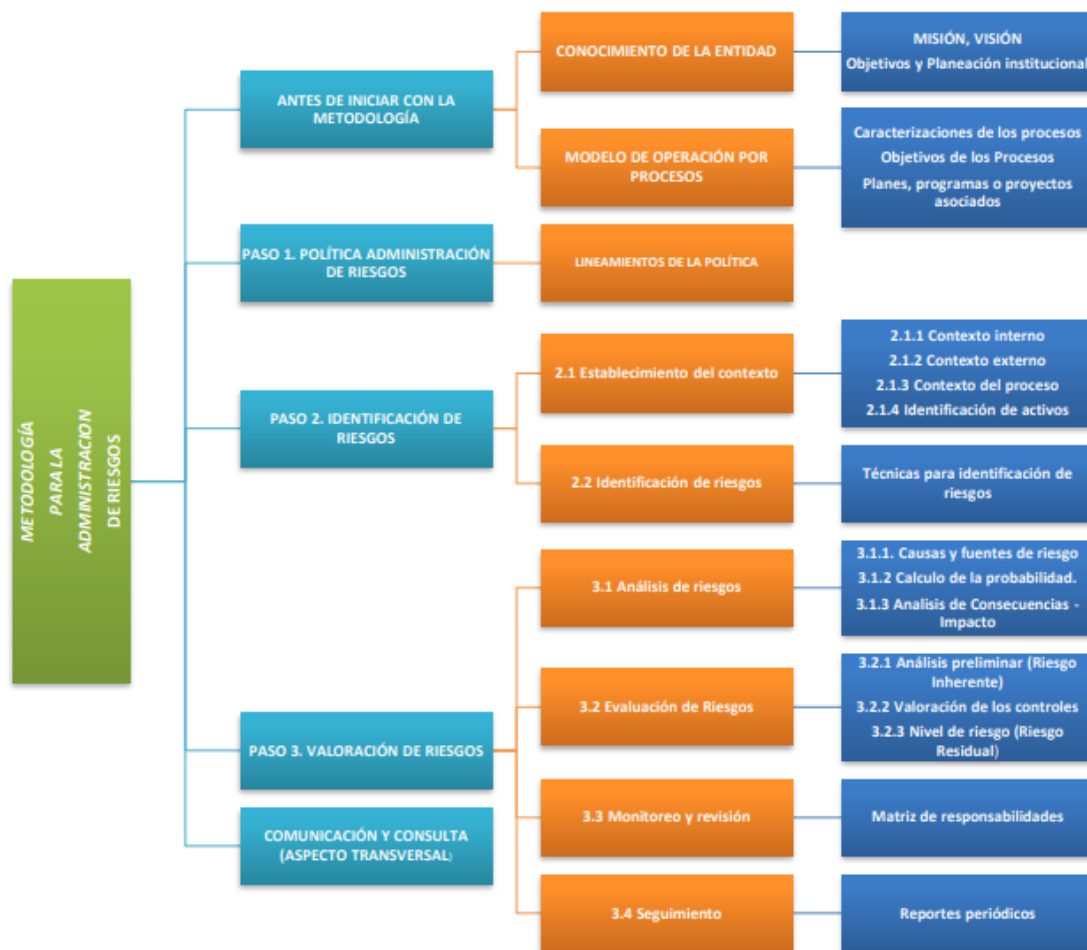


Ilustración 1 - Metodología para la administración del riesgo en la URT.⁴

8.2 Riesgos Identificados

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

RIESGO	DESCRIPCIÓN DEL RIESGO
Equipos con fallas en HW-Datacenter NC	Equipos con fallas debido a Mantenimiento Insuficiente causando Inoportunidad en la prestación de los servicios
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
Uso inadecuado de controles en el acceso físico cajas fuertes que contienen token y claves	Uso inadecuado de controles en el acceso físico causando sanciones legales para la entidad.
Robo o pérdida de equipos transportables en Equipos Transportables que se utilizan en salidas a campo	Robo o pérdida de equipos transportables debido a Negligencia o descuido causando exposición de información sensible
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.
Instalación no autorizada de software en SW Datacenter NC	Instalación no autorizada de software debido a Ausencia en la gestión de Cambios causando Fallas en la prestación del servicio

⁴ Unidad de Restitución de Tierras (marzo de 2019) Guía para la administración del riesgo y oportunidades. <https://bit.ly/37E4xjQ>



Requerimientos con definiciones inadecuadas en SW Datacenter NC	Requisitos de desarrollo y / o adquisición de software con definiciones inadecuadas causando resistencia en el uso de las aplicaciones
Sistemas de información con fallas en el acceso en SW Datacenter NC	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
Posibilidad de instalación de código malicioso en SW Estaciones Usuario	Posibilidad de instalación de código malicioso debido a Descarga de información sin control causando Perdida y/o fuga de información
Instalación de software malicioso en SW Estaciones Usuario	Instalación de software malicioso debido a Sistemas desprotegidos ante acceso no autorizado causando Inoportunidad en la prestación de los servicios
Revelación de contraseñas en INF-FIS de Claves de Administrador	Revelación de contraseñas debido a Falta de control en la custodia causando Robo o fraude o pérdida de información que pueda afectar la prestación del servicio
Bases de datos con inadecuada administración en información en el Datacenter	Bases de datos con inadecuada administración debido a errores de configuración y definición de modelos de datos causando indisponibilidad de los sistemas de información
Perdida de información en información en el Datacenter	Perdida de información debido a escasos respaldos e insuficientes controles de seguridad causando afectaciones de los sistemas de información
Fraude fuga o revelación de información. de información fuera del Datacenter	Fraude fuga o revelación de información. debido a información extraída de las Bases de datos unificadas y entregadas a procesos internos de restitución causando Vulneración de los derechos de la población objeto de los procesos de Restitución
Obligaciones contractuales con incumplimiento por personal no calificado en Recurso Humano Critico	Obligaciones contractuales con incumplimiento por personal no calificado debido a falta de capacidades técnicas y principios éticos causando inoportunidad en la prestación del servicio


8.3 Actividades del plan de tratamiento

Después de identificar los diferentes riesgos se resume en este documento las actividades planteadas para el plan de tratamiento de riesgos:

Acción a Desarrollar	Nivel aplicación	Evidencia/Entregable	Responsable	Fecha Inicio	Fecha Final
Gestionar los mantenimientos necesarios en la infraestructura tecnológica y personal para el monitoreo de las plataformas.	Nivel Central	Informes de monitoreo y de contrato de mantenimiento por parte de los responsables	Ing. Infraestructura, redes y seguridad.	ene-2020	nov-2020
Socializar el lineamiento a Ing. territoriales y soporte para que se realice el cifrado de información. Para los usuarios socializar el uso de la herramienta de cifrado.	Nivel Central y Territorial	Actas Correos donde se evidencie la instrucción.	Líder de Mesa de servicios	ene-2020	marzo-2020
Generar campaña sobre la necesidad de solicitar el cifrado de los equipos cuando sale de las instalaciones de la Unidad Responsable Líder UyA / seguridad.	Nivel Central y Territorial	Campaña y evidencie adjunta al GLPI con el cifrado del equipo	Líder UyA / Seguridad	ene-2020	marzo-2020
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	ene-2020	mar-2020



Acción a Desarrollar	Nivel aplicación	Evidencia/Entregable	Responsable	Fecha Inicio	Fecha Final
Verificar de la eficacia en la implementación de los controles de Seguridad de la información.	Nivel Central y Territorial	Reporte de implementación	Oficial de Seguridad	mar-2020	jun-2020
Actualizar contexto, revisión y actualización de nuevos riesgos	Nivel Central	Matriz de Riesgos Actualizada	Jefe OTI y Lideres OTI	Jun-2020	Jul-2020
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	ene-2020	dic-2020
Realizar el Primer Monitoreo al plan de tratamiento de riesgos de seguridad digital.	Nivel Central	Acta de reunión	Jefe OTI y Lideres OTI	abr-2020	abr-2020
Realizar el Segundo Monitoreo al plan de tratamiento de riesgos de seguridad digital.	Nivel Central	Acta de reunión	Jefe OTI y Lideres OTI	ago-2020	ago-2020
Realizar el Tercer Monitoreo al plan de tratamiento de riesgos de seguridad digital.	Nivel Central	Acta de reunión	Jefe OTI y Lideres OTI	dic-2020	dic-2020
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 y/o Herramienta de monitoreo y/o Informe.	Líder sistemas de información	ene-2020	dic-2020
Unificar las bases de las diferentes áreas para la implementación de un sistema de información.	Nivel Central	Modelo de bases unificadas	Líder sistema información/ Financiera/ contratos/talento humano	jun-2020	sep-2020
Actualizar los procedimientos de pruebas software de acuerdo con la incorporación de nuevos componentes de inteligencia artificial y demás tecnologías emergentes.	Nivel Central y Territorial	Guion de pruebas actualizado	Líder de Sistemas de Información	jun-2020	nov-2020
Ampliar la difusión del uso (Keepass) para los usuarios específicos.	Nivel Central y Territorial	Piezas de comunicación	Ingeniero de Seguridad UyA	ene-2020	mar-2020
Verificar la eficacia de la adecuada aplicación del procedimiento de gestión de cambios.	Nivel Central y Territorial	Evidencias de la aplicación del procedimiento	Líder de Servicios Tecnológicos Líder de Sistemas de Información Líder de Información Líder de Mesa de Servicios	feb-2020	mar-2020
Incluir actividades en los diferentes planes si se han materializado nuevos riesgos. Identificar e incluir en la matriz de riesgos.	Nivel Central	Planes y Matriz actualizados	Líder de Servicios Tecnológicos Líder de Sistemas de Información Líder de Información Líder de Mesa de Servicios Oficial de Seguridad de la Información	nov-2020	dic-2020

 UNIDAD DE RESTITUCIÓN DE TIERRAS	UNIDAD ADMINISTRATIVA ESPECIAL DE GESTIÓN DE RESTITUCIÓN DE TIERRAS DESPOJADAS	PÁGINA: 8 DE 9
	PROCESO: NOMBRE DEL PROCESO AL QUE PERTENECE SEGÚN MAPA DE PROCESOS	CÓDIGO: ALFANUMÉRICO
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 1.0

9 METAS

La meta es completar el 100% de las actividades establecidas en este plan.

10 CRONOGRAMA DE ACTIVIDADES

Ver numeral 8 Descripción de Actividades.

11 ENTREGABLES

Ver numeral 8 Descripción de Actividades.

12 PRESUPUESTO

Los recursos disponibles para su desarrollo 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.

13 REQUERIMIENTOS LOGÍSTICOS, TÉCNICOS Y/O TECNOLÓGICOS

Para la actualización del Plan de Tratamiento de Riesgos de Seguridad Digital se contemplan los recursos humanos, técnicos y presupuestales dispuestos en el proyecto de inversión de la Unidad para el componente tecnológico, los cuales se encuentran plasmados en el Plan Anual de Adquisiciones.


14 METAS E INDICADORES

Metas: Ver numeral 9.

El indicador para medir este plan será el porcentaje de avance del cronograma = (Número actividades ejecutadas/Número actividades planeadas) x 100.

15 RESPONSABLE DE LA SUPERVISIÓN Y SEGUIMIENTO

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

 UNIDAD DE RESTITUCIÓN DE TIERRAS	UNIDAD ADMINISTRATIVA ESPECIAL DE GESTIÓN DE RESTITUCIÓN DE TIERRAS DESPOJADAS	PÁGINA: 9 DE 9
	PROCESO: NOMBRE DEL PROCESO AL QUE PERTENECE SEGÚN MAPA DE PROCESOS	CÓDIGO: ALFANUMÉRICO
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 1.0

16 EVALUACIÓN

Como mecanismos de seguimiento y evaluación a la gestión de los proyectos actualizados, se establecieron indicadores con el fin de monitorear de manera periódica el avance de las líneas de acción definidas para el cumplimiento de las actividades establecidas en este plan.

17 PARTICIPANTES EN LA ELABORACIÓN

Equipo Oficina Tecnologías de la Información

18 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	18/11/2019	
REVISADO POR:	Claudia Patricia Hernández	Jefe Oficina Asesora de Planeación	18/11/2019	
APROBADO POR:	Enrique Cusba García	Jefe Oficina de Tecnologías	18/11/2019	