PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIDAD
DE RESTITUCIÓN
DE TIERRAS

Bogotá D.C., Noviembre de 2020

TABLA DE CONTENIDO

1 ANTECEDENTES Y DESCRIPCIÓN DE LA SITUACIÓN ACTUAL 3
2 JUSTIFICACIÓN 4
3 CONTEXTO NORMATIVO 4
4 TERMINOS 4
5 OBJETIVO GENERAL 5
6 OBJETIVOS ESPECÍFICOS 5
7 ACCIONES 5
7.1 Diagnostico 6
7.2 Planificación 6
7.3 Implementación 7
7.4 Evaluación de Desempeño 8
7.5 Mejora Continua 8
8 METAS 8
9 RECURSOS 8
9.1 Requerimientos logísticos, técnicos y/o tecnológicos 9
9.2 Recursos Humanos 9
10 ANÁLISIS DE RIESGOS 9
11 INDICADORES 9
12 EVALUACIÓN 9
13 ANEXOS 9
14 PARTICIPANTES EN LA ELABORACIÓN 9
15 CONTROL DE CAMBIOS 9

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 en el Plan Estratégico de Tecnologías de la información, el cual debe contiene la proyección estratégica en el tiempo, que para el caso de la Unidad actualmente será de 2 años (2021-2022), 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:

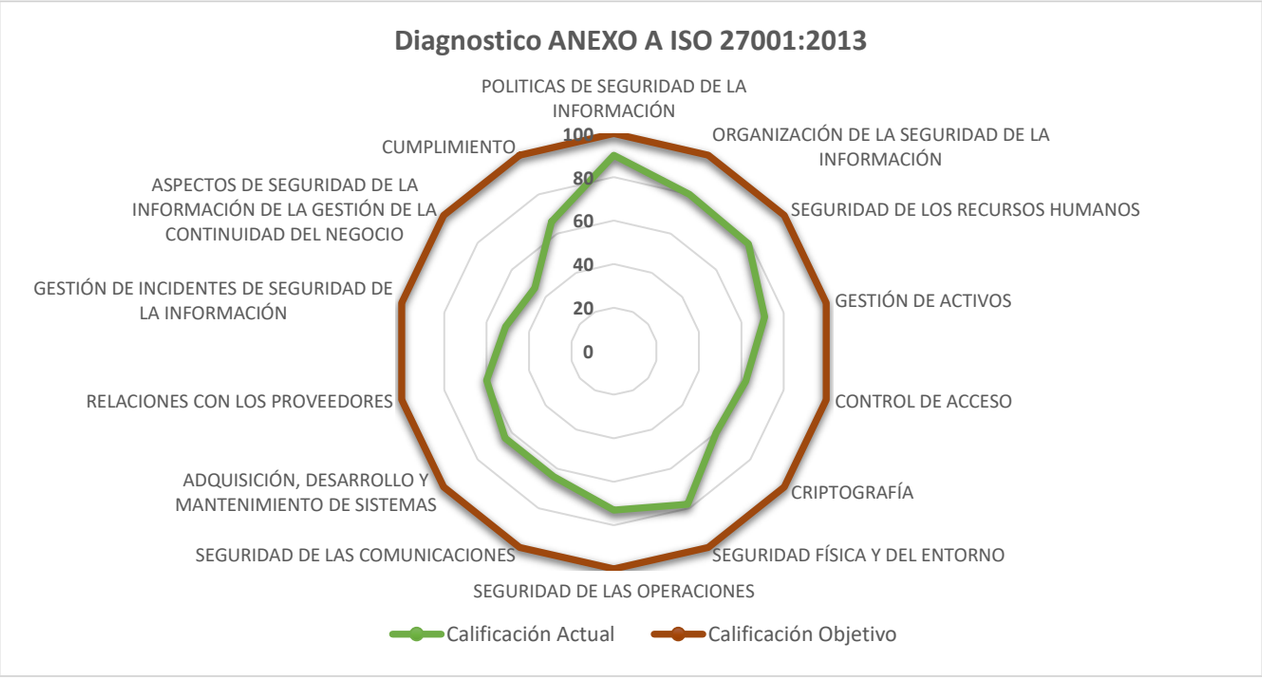

Ilustración 1 – Diagnostico Anexo A ISO 27001:2013

En cuanto al diagnóstico de FURAG frente a la política de Seguridad Digital del Modelo Integrado de Planeación y Gestión para la vigencia 2019 arrojo un avance del 88%, así mismo para el diagnóstico realizado por MinTIC arrojo un avance del 96% para la vigencia 2020.

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 en su versión 3 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 agrupados y asociados a los riesgos de seguridad digital 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 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. "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". 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

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 TERMINOS

- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000). MSPI: Modelo de Seguridad y Privacidad de la Información
- **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.
- **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.

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
- **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.
- **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).
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)
- **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).

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 URT 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 ACCIONES

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 URT, 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[1] 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

[1] Ministerio de Tecnologías de la Información y las Comunicaciones (Julio de 2016). Modelo de Seguridad. https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

propuesto para el desarrollo de las arquitecturas empresariales sectoriales, institucionales y territoriales, convirtiéndose en soporte de la Política de Gobierno Digital.

Este modelo contempla un ciclo de operación que consta de cinco (5) fases:

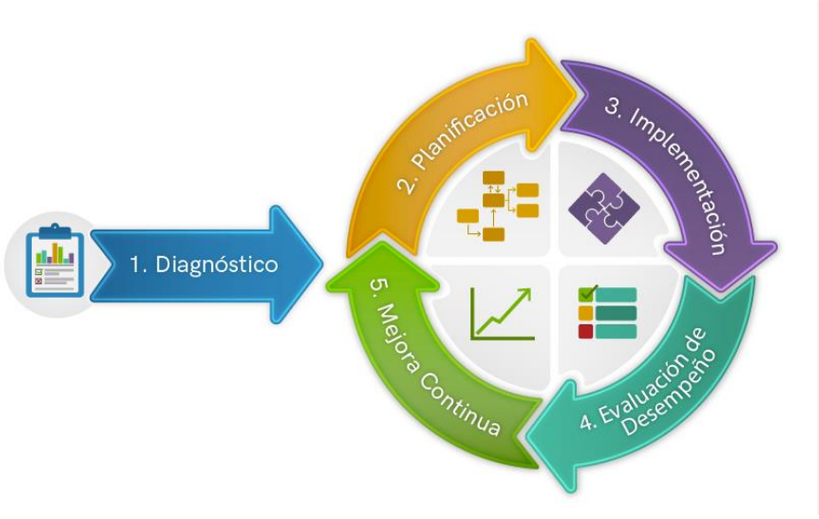

Ilustración 1 - Metodología MSPI

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.

7.1 Diagnostico

En esta fase se identifica el estado actual de la organización para determinar las actividades que se deben tener en cuenta para avanzar en la implementación y mejora del MSPI.

ACTIVIDADES	ENTREGABLES	ESTADO	FECHA FIN
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	No iniciada	Diciembre 2020

7.2 Planificación

La Unidad de Restitución de Tierras elabora este Plan de Seguridad y Privacidad de la Información teniendo en cuenta los resultados de la fase anterior, con el fin de determinar las actividades que estén encaminadas y alineadas a los objetivos misionales de la entidad. Teniendo en cuenta los procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados y las interrelaciones del modelo con otros procesos.

ACTIVIDADES	ENTREGABLES	ESTADO	FECHA FIN
Generar el plan de documentos de seguridad de la información a formalizar durante la vigencia.	Documento con la lista de Actividades y Fechas.	No iniciada	Marzo 2021
Publicar el Plan de Tratamiento de Riesgos de Seguridad Digital.	Documento con el Plan de Tratamiento de Riesgos	No iniciada	Enero 2021

ACTIVIDADES	ENTREGABLES	ESTADO	FECHA FIN
	aprobado y publicado en la página web.		
Formalizar el Plan de Sensibilización y Comunicación de Seguridad de la Información. 1. Segmentar en grupos focales. 2. Hacer encuesta de seguridad de la información 3. Fortalecer los contenidos orientados a grupos. Incluir actividades de sensibilización.	Documento con el Plan de Capacitación Sensibilización y Comunicación formalizado.	No iniciada	Marzo 2021
Revisar y actualizar la política de Protección de Datos Personales y establecer actividades que se detecten durante la actualización.	Documento y actividades detectadas durante la actualización.	No iniciada	Mayo 2021
Revisar y actualizar el plan de continuidad de negocio de TI.	Documento Plan Actualizado	No iniciada	Marzo 2021

7.3 Implementación

En esta fase la entidad llevará a cabo lo descrito en la Fase de Planificación donde se deberán implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos.

De acuerdo con la madurez del Subsistema de Gestión de Seguridad de la Información se establecerán los criterios que permitan medir la efectividad, eficiencia y eficacia de las acciones implementadas en seguridad de la información.

ACTIVIDADES	ENTREGABLES	ESTADO	FECHA FIN
Revisar y Actualizar la Política de Seguridad y Privacidad de la Información.	Política de Seguridad de la Información y Complementarias Actualizadas	No iniciada	Junio 2021
Implementar el Plan de Tratamiento de Riesgos.	Reportes de monitoreo del plan de tratamiento de riesgos.	No iniciada	Diciembre 2021
Implementar Plan de Sensibilización y Comunicación de Seguridad de la Información.	Reportes de avance del Plan de Capacitación y Sensibilización	No iniciada	Diciembre 2021
Implementar Plan de Continuidad del Negocio	Reportes de avance del Plan de Continuidad de Negocio	No iniciada	Noviembre 2021
Implementar el plan de documentos asociados a seguridad de la información.	Procedimientos de seguridad de la información en ejecución.	No iniciada	Octubre 2021
Actualizar Activos de Información.	Actualizar el inventario de activos de información.	No iniciada	Octubre 2021
Implementar Actividades de Protección de Datos detectadas en la planeación. (Incluir los avisos de privacidad y autorización de datos	Reporte de avance de la actividad	No iniciada	Septiembre 2021

ACTIVIDADES	ENTREGABLES	ESTADO	FECHA FIN
personales en los formularios y aplicaciones de la entidad).			
Actualizar la metodología de incidentes de seguridad de la entidad.	Metodología actualizada y formalizada	No iniciada	Junio 2021
Implementar método de prevención de fuga de la información (DLP).	Herramienta funcionando	No iniciada	Mayo 2021
Actualizar la matriz de riesgos de seguridad digital.	Riesgos actualizados.	No iniciada	Agosto 2021

7.4 Evaluación de Desempeño

El proceso de seguimiento y monitoreo del MSPI se realizará con base a los resultados que se calculen a través de los indicadores de seguridad de la información propuestos para la verificación de las acciones implementadas, así como las auditorías realizadas al SGSI.

ACTIVIDADES	ENTREGABLES	ESTADO	FECHA FIN
Incluir en el Plan de ejecución de auditorías las relacionadas con el SGSI.	Documento con el plan de ejecución de auditorías del SGSI articulado con OCI.	No iniciada	Mayo 2021
Revisar indicadores y los informes de auditoría relacionados con el SGSI.	Informe de Auditoria	No iniciada	Diciembre 2021

7.5 Mejora Continua

En esta fase la Unidad de Restitución de Tierras debe consolidar los resultados obtenidos en la fase de evaluación de desempeño, para diseñar el plan de mejoramiento dirigido a la seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

ACTIVIDADES	ENTREGABLES	ESTADO	FECHA FIN
Actualizar el Plan de Mejoramiento.	Plan de Mejoramiento Publicado	No iniciada	Diciembre 2021

8 METAS

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

9 RECURSOS

Los recursos disponibles para 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.

9.1 Requerimientos logísticos, técnicos y/o tecnológicos

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

9.2 Recursos Humanos

Para lograr los objetivos propuestos en el plan se requiere de una persona encargada de liderar las estrategias de seguridad de la información quien asegure el cumplimiento del plan, un ingeniero de seguridad quien es el encargado de administrar los recursos tecnológicos y colaboradores de OTI que participan en la ejecución y cumplimiento de las actividades. Adicionalmente para el cumplimiento de las políticas y demás planes se requiere del compromiso y la colaboración de toda 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.

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**