ADR
Agencia de Desarrollo Rural

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

El campo es de todos

Minagricultura

ADR Agencia de Desarrollo Rural	**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**	El campo es de todos · Minagricultura

HISTORIAL DE VERSIONES

VERSIÓN	FECHA	DESCRIPCIÓN
0.1	Diciembre 2019	Primera versión del documento.
1.0	Junio 2020	Ajustes relacionados con la autoevaluación del modelo de Seguridad y Privacidad de la Información de MinTIC
2.0	Agosto 2020	Ajustes relacionados con las observaciones el Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural

HISTORIAL DE APROBACIONES

ELABORÓ		REVISÓ		APROBÓ	
Cargo	Profesional Especializado	Cargo	Profesional Especializado	Cargo	Jefe de Of. / Cód: G1-Grado 5
Nombre	Catherine Suárez	Nombre	Paola Ambrosio	Nombre	Víctor Mondragón
Dependencia	Oficina Tecnologías de la Información.	Dependencia	Oficina Tecnologías de la Información.	Dependencia	Oficina Tecnologías de la Información.
Fecha	30/04/2020	Fecha	05/06/2020	Fecha	10/06/2020

ADR Agencia de Desarrollo Rural	**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**	El campo es de todos Minagricultura

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

LISTA DE TABLAS

1. INTRODUCCIÓN

Teniendo en cuenta lo expresado en la resolución 1602 del 2017, "Por la cual crea el Comité Institucional de Desarrollo Administrativo de la Agencia de Desarrollo Rural, como instancia orientadora del Modelo Integrado de Planeación y Gestión y se establece su reglamentación" y en su lugar se integra el Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural." En su artículo Tercero. Funciones del comité institucional de gestión y desempeño de la agencia de desarrollo rural, numeral 6 - "Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información".

Adicionalmente, dando cumplimiento a lo establecido en el Decreto 612 de 2018 "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", en el Artículo 1. Adicionar al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, los siguientes artículos: "2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año: ítem 12. Plan de Seguridad y Privacidad de la Información.

Es por esto, que la Agencia de Desarrollo Rural (ADR), ha adelantado cambios organizacionales, para orientar estratégicamente sus actividades con el apoyo de las tecnologías de la información y las comunicaciones, dentro de esos cambios se tiene: el posicionamiento de una Oficina de Tecnologías de la Información (OTI) como una oficina estratégica al interior de la entidad, la definición de directrices relacionados con Transformación Digital y los avances en la implementación de las Políticas de Gobierno Digital y Seguridad Digital, por lo tanto, este documento tiene como fin presentar un plan de acción para el establecimiento, implementación, operación, monitoreo, revisión y mejora continua de la Seguridad y Privacidad de la Información.

2. OBJETIVO DEL DOCUMENTO.

Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, con las cuales se busca desarrollar, verificar y aplicar la mejora continua en la Seguridad de la Información en la Agencia de Desarrollo Rural - ADR.

2.1. OBJETIVOS ESPECIFICOS

- Identificar las necesidades y requerimientos la Agencia de Desarrollo Rural-ADR para tener en cuenta en la implantación del MSPI, definido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)
- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la información
- Establecer el estado actual y nivel de madurez de los procesos de seguridad y privacidad de la información. identificando vulnerabilidades, amenazas, y riesgos
- Establecer y documentar el gobierno de gestión de seguridad de la información, alineado con el gobierno de TI
- Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.
- Establecer lineamientos que permitan continuar con la gestión de la seguridad de la información al interior de la entidad. Evaluar y alinear el Modelo de seguridad y privacidad de la información1 con el fin de dar cumplimiento a los marcos regulatorios identificados. Planear programas y planes de auditoria para el monitoreo y mejora continua Generar conciencia para el cambio organizacional requerido para la apropiación de la Seguridad y Privacidad de la Información como eje transversal.
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

[1] https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

3. ALCANCE

El Plan de Seguridad y Privacidad de la Información se aplica para todos los procesos del ADR, a todos los funcionarios, contratista y demás colaboradores que debido al cumplimiento de sus funciones utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación.

Así mismo, la aplicación de la Política a toda la información creada, procesada o utilizada en la ADR sin importar el medio, formato o presentación o lugar en el cual se encuentre. Utilizando como guía la norma ISO-IEC- 27001:2013 y la metodología MSPI de MINTIC, en un periodo de 2 años. (Fase I -2019, Fase 2 -2021)

4. TERMINOS Y DEFINICIONES[2]

- **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) (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016).
- **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. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016).
- **Activo:** Cualquier cosa que tenga valor para la organización. Existen diversos tipos de activos en una organización como: información, software, programas de computador, físicos como los computadores, servicios, la gente y sus aptitudes, habilidades, y experiencia, intangibles como Reputación o Imagen. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2018)
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria.(ISO/IEC 27000) (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016).
- **Ciberseguridad:** Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que

[2] https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio (Departamento Nacional de Planeación, 2016).

- **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) (Departamento Nacional de Planeación, 2016).
- **Confidencialidad:** Se refiere a que la información solo puede ser conocida por individuos autorizados. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2018)
- **Continuidad de negocio:** Proceso general de gestión que identifica amenazas potenciales a una organización y el impacto que se podría causar a la operación de negocio que en caso de materializarse. La gestión de la continuidad del negocio provee un marco de trabajo para la construcción de la resiliencia organizacional, con capacidad de respuesta efectiva que salvaguarde los intereses de las partes interesadas, reputación, marca y actividades de creación de valor. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2018)
- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016).
- **CSIRT**: Equipo de Respuesta a Incidentes de Seguridad cibernética, por su sigla en inglés. Se refiere a una institución definida y concreta que tiene la responsabilidad de proveer capacidades de gestión de incidentes a una organización/sector en especial. Su objetivo es minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta y recuperación efectiva, así como trabajar en pro de prevenir la ocurrencia de futuros incidentes (Departamento Nacional de Planeación, 2020)
- **Datos Abiertos:** En 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) (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3). (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)
- **Declaración de Aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.(ISO/IEC 27000). (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)
- **Disponibilidad de la información:** Se refiere a la seguridad que la información puede ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2018)
- **Incidente:** cualquier evento adverso real o sospechado, intencionado o no intencionado, que puede cambiar el curso esperado de una actividad en el entorno digital. (Departamento Nacional de Planeación, 2020)
- **Incidente digital:** evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el entorno digital y que genera impactos sobre los objetivos. (Departamento Nacional de Planeación, 2016)
- **Integridad:** Se refiere a la garantía de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2018)
- **ISO27001:** Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. (NTC-ISO/IEC 27001:2013, 2013)
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Lineamiento**: Es una directriz o disposición obligatoria para efecto de este manual que debe ser implementada por las entidades públicas para el desarrollo de la política de gobierno digital. Los lineamientos pueden ser a través de estándares, guías, recomendaciones o buenas prácticas. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2018)
- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000). (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000). (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)
- **Seguridad digital**: Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (Departamento Nacional de Planeación, 2020)
- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3) (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)
- **Vulnerabilidad** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000). (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)

5. NORMATIVIDAD

La actualización del siguiente Plan de Seguridad y Privacidad de la Información para la Agencia de Desarrollo Rural (ADR), se define teniendo en cuenta las principales normas relacionadas con el accionar misional de la Entidad, el Sector Agropecuario y Pesquero, el Sector de las Tecnologías de la Información y las Comunicaciones asociada a los temas de la Política de Gobierno Digital, Arquitectura de Información, el Modelo de Gestión Estratégica de TI y el Modelo integrado de Planeación y Gestión (MIPG).

- **Constitución Política de Colombia**; Artículos 11, 12, 13, 14, 17, 21, 22, 24, 29, 44, entre otros, Art. 15 de julio de 1991. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución".
- **Ley 1712 de 2014**: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
- **Ley Estatutaria 1581 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013: "**Por la cual se dictan disposiciones generales para la protección de datos personales".
- **Ley 1437 de 2011: "**Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo".
- **Ley 1273 de 2009: "**Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado "de la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
- **Ley 1341 de 2009: "**Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones"**.**
- **Ley 1150 de 2007: "**Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos contenidos de la norma".
- **Ley 527 de 1999 (Comercio Electrónico)** Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Se tratan conceptos como: mensaje de datos (artículos 2º y 5º), el principio de equivalencia funcional

(artículos 6º, 8º, 7º, 28º, 12º y 13º), la autenticación electrónica (artículo 17º), la firma electrónica simple (artículo 7º), la firma digital (artículo 28º), y la firma electrónica certificada (artículo 30º, modificado por el artículo 161 del Decreto Ley 019 de 2012)

- **Decreto 612 de 2018**: "Por el cual se fijan las directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las entidades del estado".
- **Decreto 1008 de 2018**: "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", en el artículo 2.2.9.1.1.3., incluye la seguridad de la información entre los principios de la Política de Gobierno Digital; de igual manera, en el artículo 2.2.9.1.2.1. se establece que la Política de Gobierno Digital se desarrollará a través de componentes y habilitadores transversales3, y respecto de estos últimos indica que son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital".
- **Decreto 2693 de 2012: "**Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones".
- **Decreto 2578 de 2012: "**Por medio del cual se reglamenta el Sistema Nacional de Archivos. Incluye "El deber de entregar inventario de los documentos de archivo a cargo del servidor público, se circunscribe tanto a los documentos físicos en archivos tradicionales, como a los documentos electrónicos que se encuentren en equipos de cómputo, sistemas de información, medios portátiles" entre otras disposiciones".
- **Decreto 2609 de 2012: "**Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos".
- **Resolución No. 0409 de 2019: "**Por la cual se adopta la política de seguridad y privacidad de la información de la Agencia de Desarrollo Rural - ADR y se definen lineamientos frente al uso y manejo de la información"
- **CONPES 3854 de 2020.** Política Nacional De Confianza Y Seguridad Digital
- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital.
- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.

[3] Entiéndase por habilitadores transversales de la Política de Gobierno Digital: Arquitectura, Seguridad y privacidad y Servicios Ciudadanos Digitales, como elementos de base que permiten el desarrollo de los componentes de la política.

Adicionalmente, la ADR sigue estándares y buenas prácticas utilizados en TI, bajo las Normas ISO 9001, ISO 27001, ISO 22301, ISO 31000, OCTAVE allegro, la NTC 5854 para accesibilidad de páginas web, ITIL, TOGAF, COBIT, entre otras.

- **ISO/IEC 27001:2013:** Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información

6. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN POLÍTICA DE TRATAMIENTO DE PROTECCIÓN DE DATOS

La Agencia de Desarrollo Rural - ADR, adopta en términos de la Resolución No. 04092 del 03-07-2019 “política de seguridad y privacidad de la información”, con el objetivo establecer mecanismos y procedimientos para la divulgación y socialización oportuna, eficaz y efectiva de las decisiones, comunicados, recomendaciones, políticas y en general toda actuación que adopte la Entidad en el marco de su misión, visión y funciones constitucionales y legales que deban ser de conocimiento al público en general o a sus servidores públicos y colaboradores.

Al cumplimiento del pacto por la transformación digital a partir de la ley 1955 de 2019 PND 2018 - 2022, armonizando los postulados y sus objetivos, como estrategia transversal establecida por el Plan Nacional de Desarrollo y con los objetivos del Ministerio de Ciencia, Tecnología e Innovación en relación con el desarrollo del conocimiento científico, tecnológico y de innovación, en aras de la modernización del Estado.

7. MANEJO DE LA INFORMACIÓN EN LA AGENCIA DE DESARROLLO RURAL - ADR

La Ley 1955 de 2019: “Por el cual se expide el Plan Nacional de Desarrollo 2018-2022 - “Pacto por Colombia, Pacto por la Equidad”, está compuesto por objetivos de política pública denominados pactos, concepto que refleja la importancia del aporte de todas las facetas de la sociedad en la construcción de una Colombia equitativa; dichos pactos contienen estrategias transversales como el “Pacto por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento” (numeral 7° del artículo 3°), lo cual es coherente con los objetivos generales y específicos del Ministerio de Ciencia, Tecnología e Innovación, en relación con el desarrollo del conocimiento científico, tecnológico y de innovación, en aras de la modernización del Estado, según lo establecido en el artículo 126 de la Ley 1955 de 2019, que modificó parcialmente el artículo 2 de la Ley 1951 de 20194.

A causa de dicho pacto que tiene como objetivo el uso y aprovechamiento de las TIC para mejorar la provisión de servicios digitales de confianza, el desarrollo de procesos internos eficientes, la toma de decisiones basadas en datos confiables y actualizados, el empoderamiento de los ciudadanos y el impulso en el desarrollo de territorios y ciudades inteligentes, logrados a partir de la consolidación de un Estado y ciudadanos competitivos, proactivos, e innovadores, que generan valor público en un entorno de confianza digital[5]

---

[4] Por la cual crea el Ministerio de Ciencia, Tecnología e Innovación, se fortalece el Sistema Nacional de Ciencia, Tecnología e Innovación y se dictan otras disposiciones”.

[5] [5] Manual de Gobierno Digital, consultado en https://mintic.gov.co/portal/604/articles-61775_recurso_2.pdf

Que por consiguiente, la aplicación de este pacto por el buen uso de las Tecnologías de la información y la comunicación - TIC, permitirá a las entidades públicas mejorar su funcionamiento y su relación con otras entidades, con los ciudadanos y agentes del sector, fortaleciendo la relación con el Estado en un entorno confiable, que permita la apertura y aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, la participación en el diseño de servicios y programas, así como la identificación de soluciones a problemáticas de interés común, todo esto en el marco de la eficiencia en la prestación del servicio público.

Dado lo anterior, se hace necesario adoptar mediante el presente acto administrativo, Resolución No. 409 de 3 de julio 2019*; "Por la cual se adopta la política de seguridad y privacidad de la información de la Agencia de Desarrollo Rural- ADR y se definen lineamientos frente al uso y manejo de la información*", con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), así como definir los lineamientos frente al uso y manejo de la información en la Agencia de Desarrollo Rural, armonizando los postulados y objetivos del pacto por la transformación digital, como estrategia transversal establecida por el Plan Nacional de Desarrollo.

8. ESTABLECIMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Las funciones del comité de Seguridad de la Información serán asumidas por el comité institucional de gestión y desempeño – MIPG, mediante la resolución 1602 de 2017 "*Por la cual crea el Comité Institucional de Desarrollo Administrativo de la Agencia de Desarrollo Rural, como instancia orientadora del Modelo Integrado de Planeación y Gestión y se establece su reglamentación*" y en su lugar se integra el Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural.

9. METODOLOGÍA DE IMPLEMENTACIÓN DEL PLAN

Con el fin de efectuar el proceso de implementación del presente Plan , se hará uso de la metodología del Modelo de Seguridad y Privacidad planteado por MinTIC,[6] mediante el ciclo de funcionamiento del modelo de operación, a través de la descripción detallada de cada una de las cinco (5) fases que lo comprenden. Estas, contienen objetivos, metas y herramientas (guías) que permiten que la seguridad y privacidad de la información sea un modelo de gestión sostenible dentro de las entidades.

[6] https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Ilustración 1. Ciclo de operación MSPI

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

De la autoevaluación publicada por MINTIC por medio del Instrumento de Evaluación MSPI[7], se obtuvieron los siguientes resultados para el 2019.

Tabla 1. Autoevaluación MSPI 2019

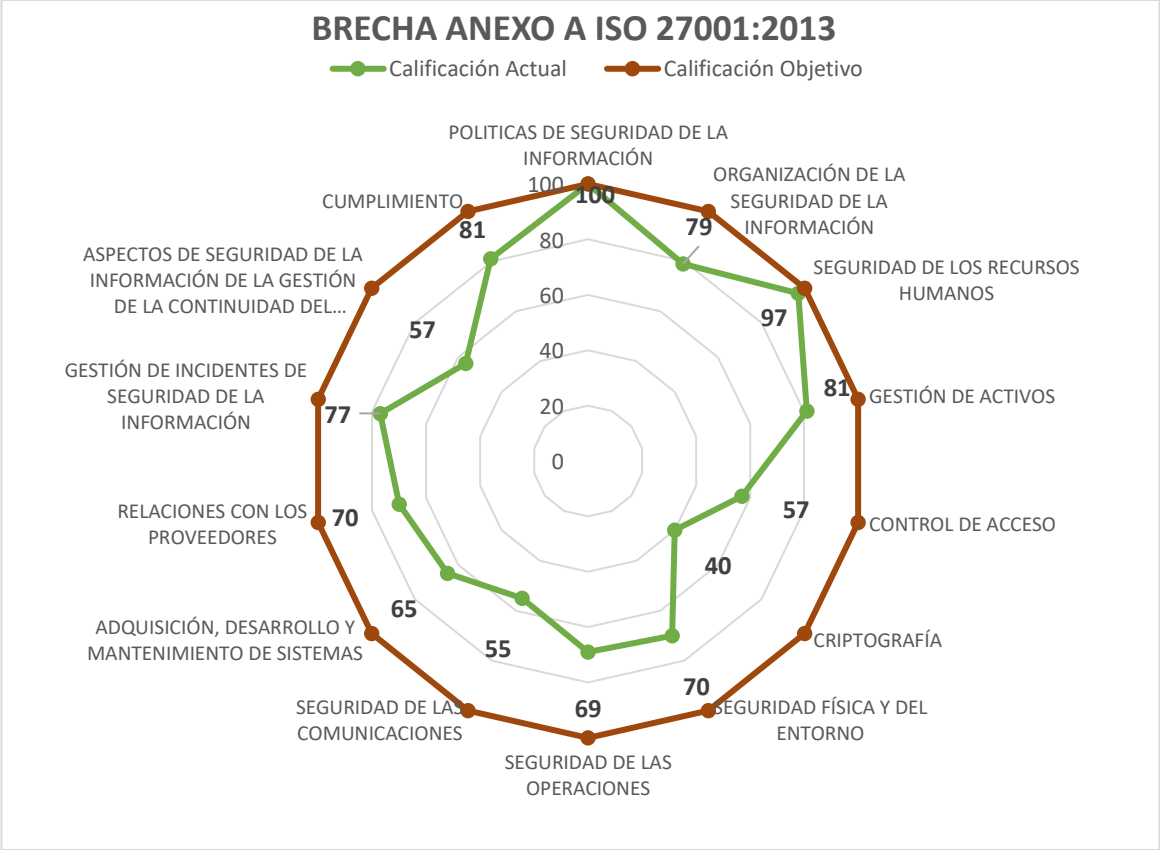
Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2018	Planificación	26%	40%
2019	Implementación	12%	20%
2020	Evaluación de desempeño	8%	20%
2021	Mejora continua	6%	20%
TOTAL		52%	100%

Fuente OTI: Instrumento de Evaluación MSPI-ADR abril 2019

Para el 2020 se realizó el autodiagnóstico con corte de mayo con los siguientes resultados:

[7] https://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx

Ilustración 2. Autodiagnóstico MSPI 2020



Fuente OTI: Instrumento de Evaluación MSPI-ADR mayo 2020

En la siguiente tabla se presentan los resultados discriminados por cada una de las fases de implementación

Tabla 2. Autoevaluación MSPI 2019

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2018	Planificación	32%	40%
2019	Implementación	13%	20%
2020	Evaluación de desempeño	9%	20%
2021	Mejora continua	14%	20%
TOTAL		68%	100%

Fuente OTI: Instrumento de Evaluación MSPI-ADR mayo 2020

10. IDENTIFICACIÓN NECESIDADES Y EXPECTATIVAS DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Todo el equipo de la Agencia de Desarrollo Rural-ADR, es responsable de la seguridad de la información. Adicionalmente existen los siguientes roles y responsabilidades específicas dentro del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.

- **Presidencia**

- Responsable por el direccionamiento estratégico e impulso del Modelo de Seguridad y Privacidad de la Información. Requiere el compromiso, recursos y asignación de responsabilidades para la gestión de seguridad y privacidad de la información. de la misma forma debe contar con la aprobación de este direccionamiento y los resultados por parte del Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural.
- Como parte de la gestión de la presidencia para seguridad de la información se encuentran las siguientes responsabilidades:
- Aprobación y verificación del cumplimiento de las políticas de seguridad de la información
- Hacer que los miembros del Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural sean conscientes de la criticidad de los activos de información de la ADR y de su criticidad en el desarrollo de la misión de la Entidad.
- Divulgar las responsabilidades de seguridad de la información de la ADR, con base en los lineamientos del Modelo de Seguridad y Privacidad de la Información.

- **Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural.**

Con la Resolución 1602 del 6 de diciembre de 2017 “Por la cual se deroga la Resolución No. 731 de 2017 "Por la cual crea el Comité Institucional de Desarrollo Administrativo de la Agencia de Desarrollo Rural, como instancia orientadora del Modelo Integrado de Planeación y Gestión y se establece su reglamentación" y en su lugar se integra el Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural.

El Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural, tendrá a su cargo las siguientes funciones:

- Aprobar y hacer seguimiento, por lo menos una vez cada tres meses, a las acciones y estrategias adoptadas para la operación del Modelo Integrado de Planeación y Gestión - MIPG de la Agencia de Desarrollo Rural.

- Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del Modelo Integrado de Planeación y Gestión - MIPG de la Agencia de Desarrollo Rural.
- Proponer al Comité Sectorial de Gestión y el Desempeño institucional, iniciativas que contribuyan al mejoramiento en la implementación y operación del Modelo Integrado de Planeación y Gestión - MIPG.
- Presentar los informes que el Comité Sectorial de Gestión y el Desempeño Institucional y los organismos de control requieran sobre la gestión y el desempeño de la entidad.
- Adelantar y promover acciones permanentes de autodiagnóstico para facilitar la valoración interna de la gestión.
- Las demás que tengan relación directa con la implementación, desarrollo y evaluación del Modelo.
- Teniendo en cuenta el numeral 6. “Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información” se tienen las siguientes responsabilidades:
  - ✓ Definir la estrategia, el gobierno y la dirección de la gestión de la seguridad de la información.
  - ✓ Aprobar la política de seguridad y privacidad de la información.
  - ✓ Promover la gestión de la seguridad de la información mediante el compromiso de la dirección y la asignación de los recursos adecuados.
  - ✓ Estudiar y aprobar las iniciativas de seguridad de la información que le sean propuestas.

  - **Responsable del funcionamiento del Modelo de Seguridad y Privacidad de la Información**

El responsable del funcionamiento del Modelo de Seguridad y Privacidad de la Información en la Agencia de Desarrollo Rural-ADR, es del jefe de la Oficina de Tecnologías de la Información y sus principales responsabilidades son:

- Asegurar la disponibilidad de los recursos necesarios para la definición, la implementación y el mantenimiento del Modelo de Seguridad y Privacidad de la Información.
- Revisar periódicamente los documentos y controles del Modelo de Seguridad y Privacidad de la Información para asegurar que el
- El Modelo de Seguridad y Privacidad de la Información logre los resultados previstos.
- Analizar la gestión de los incidentes de seguridad que le sean escalados y ponerse en contacto con las autoridades correspondientes.
- Definir lineamientos que den guía al profesional de seguridad de la información.

- **Profesional de seguridad de la información**

Que las actividades del profesional de Seguridad Digital y Seguridad de la Información serán coordinadas y aprobadas por el jefe de la Oficina de las Tecnologías de Información.

Que corresponden al profesional de Seguridad Digital y Seguridad de la Información desarrollar las siguientes funciones:

- Asesorar al Comité Institucional de Gestión y Desempeño en la planificación, diseño, implementación, operación, revisión y mejora continua del Modelo de seguridad de la información en la entidad, sus políticas, lineamientos y controles, conforme a los requerimientos legales y buenas prácticas de normas técnicas.
- Apoyar al Comité Institucional de Gestión y Desempeño en las actividades de implementación del Modelo de Privacidad y Seguridad de la Información de la estrategia de Gobierno Digital del Ministerio de Tecnología de la Información
- Apoyar el Comité Institucional de Gestión y Desempeño en las actividades de implementación de la estrategia de ciber seguridad definida por el Ministerio de Defensa Nacional.
- Apoyar al Comité Institucional de Gestión y Desempeño en las actividades de divulgación y promoción de la importancia de la política de seguridad digital, los beneficios de la seguridad de la información para la entidad y las implicaciones de la no conformidad con los requisitos de seguridad de la información de la Agencia de Desarrollo Rural-ADR, mediante la elaboración de propuestas de programas de toma de conciencia y formación en seguridad de la información.
- Velar por el cumplimiento de los requisitos del Modelo de seguridad de la información, base de datos y sistemas de comunicaciones informáticos.
- Coordinar las acciones necesarias para identificar controlar, reducir y evaluar incidentes de seguridad de la información.
- Preparar los informes del estado de la seguridad de la información y la efectividad de los controles de la seguridad, para realizar la revisión periódica del estado del sistema y acompañar a la entidad en la evaluación de este para asegurar que el Modelo de seguridad de la información permanezca conforme a las necesidades de la entidad, y se identifiquen mejoras sobre el mismo.
- Proponer, diseñar y fomentarla implementación de mejoras a los controles y herramientas de seguridad de la información necesarias para el fortalecimiento de la seguridad de la información en la entidad, y el adecuado tratamiento de los incidentes de seguridad de la información detectados.
- Coordinar con los propietarios de los activos de información y los dueños de procesos las acciones para el cumplimiento del Modelo de Seguridad y Privacidad de la Información.

- Apoyar a los funcionarios y contratistas para que cumplan con las responsabilidades de su rol frente al Modelo de Seguridad y Privacidad de la Información

  - **Propietario de los activos de información**

- Es el funcionario, contratista, colaborador o área de la Agencia de Desarrollo Rural-ADR, al cual se le ha asignado la responsabilidad formal sobre un activo de información. Sus principales responsabilidades son:
- Cumplir con la política de seguridad de la información aprobada por el comité designado para la seguridad de la información.
- Identificar, establecer el alcance y el valor o criticidad de los activos de información de los cuales es propietario
- Clasificar los activos de información siguiendo la metodología de identificación y clasificación de activos donde “Los líderes de los procesos, deberán identificar y asignar un custodio para uno de los activos de Información identificados; el custodio debe ser el Presidente, Vicepresidente o Jefe del área o dependencia en donde se realiza el levantamiento de los activos de información, para el caso de las UTT el custodio es el Director de la UTT”, aprobada y verificada el responsable del funcionamiento del Modelo de Seguridad y Privacidad de la Información
- Identificar, definir y evaluar los riesgos a los que pudieran estar expuestos los activos de información de los cuales es propietario.
- Definir los requerimientos de seguridad de los activos de información en relación con su confidencialidad, integridad y disponibilidad.
- Informar los requerimientos y controles requeridos por los activos de información a los custodios y usuarios de los activos de información.
- Efectuar una verificación periódica de la correcta ejecución de los controles requeridos sobre los activos de información bajo su responsabilidad.
- Conocer la valoración actual del riesgo y verificar si se encuentra dentro del nivel de riesgo aceptable definido por la ADR.
- Gestión inmediata para el tratamiento definido en el Modelo de Seguridad y Privacidad de la Información cuando el riesgo se encuentre en una calificación por fuera del nivel de riesgo aceptable.
- Cumplir con el reporte formal del riesgo a la Oficina de Planeación, cuando se detecte que su valoración supera el nivel de riesgo aceptable.
- Seguimiento permanente a la aplicación de los controles requeridos para el tratamiento del riesgo hasta que se constate que el nivel se encuentra dentro del nivel de riesgo aceptable

- **Custodio de los activos de información**

Es el funcionario, contratista o área de la Agencia de Desarrollo Rural-ADR, responsable de administrar y hacer efectivos los controles que el propietario del activo de información haya definido. Sus principales responsabilidades son:

- Implementar y mantener los controles requeridos en los contenedores donde estén almacenados los activos de información que se encuentren a su cargo.
- Administrar los recursos donde residen los activos de información dando los permisos definidos por el propietario del activo a los usuarios interesados.
- Proteger los activos de información presentes en los contenedores a su cargo en la situación que corresponda: almacenamiento, transporte y procesamiento.

- **Líder de procesos**

Es el funcionario, contratista o área de la Agencia de Desarrollo Rural-ADR, al cual se le ha asignado la responsabilidad formal sobre un proceso de la entidad. Sus principales responsabilidades son:

- Apoyar la identificación de los activos de información que intervienen en el proceso correspondiente.
- Validar los activos de información identificados junto con las características básicas de cada uno de ellos.
- Apoyar y validar la identificación y designación de los propietarios de los activos de la información de su proceso.

- **Usuario de la información**

- Es el funcionario o contratista de la Agencia de Desarrollo Rural-ADR, que utiliza la información para desempeñar sus funciones. Sus principales responsabilidades son:
- Utilizar los activos de información exclusivamente para el desempeño de sus funciones y obligaciones dentro y fuera de la Agencia de Desarrollo Rural-ADR.
- Conocer la clasificación de los activos de información que maneja.
- Preservar la seguridad de la información utilizada en el desempeño de sus funciones y obligaciones.
- No divulgar la información clasificada sin autorización del propietario del activo de información.
- Procurar el buen manejo de todos los activos, buscando protegerlos en relación con los principios de seguridad.

11. PRESUPUESTO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020-2021

A continuación, se presenta el presupuesto estimado para la implementación de este plan.

Tabla 2. Presupuesto Plan MSPI 2019 - 2020

DESCRIPCIÓN	PRODUCTO	CANTIDAD	UNIDAD	VALOR TOTAL AÑO 2020 AJUSTADO POR PRESUPUESTO
Licenciamiento	Certificado Digital sitio seguro (SSL)	1	Unidad	1.642.359
Servicios especializados	Especialista Seguridad de la informática	1	Unidad x 12 meses	110.400.000
TOTAL				**112.042.359**

DESCRIPCIÓN	PRODUCTO	CANTIDAD	UNIDAD	VALOR TOTAL AÑO 2021
Servicio de WiFi	Solución WIFI equipos sede principal mes	16	Unidad	35.943.095
	Instalación eléctrica y red	1	Unidad	52.994.174
	Solución WIFI equipos UTT mes	13	Unidad	29.203.765
TOTAL				**118.141.034**

DESCRIPCIÓN	PRODUCTO	CANTIDAD	UNIDAD	VALOR TOTAL AÑO 2021
Servicio de antivirus	Licencias de Kaspersky Endpoint Security Advanced para estaciones de trabajo	750	Unidad	184.047.806
	Licencias de Kaspersky Security Hybrid Cloud en plataforma	47	Unidad	31.948.154
	Soporte técnico y alcance de los servicios	1	Unidad	37.522.476
TOTAL				**253.518.436**

DESCRIPCIÓN	PRODUCTO	CANTIDAD	UNIDAD	VALOR TOTAL AÑO 2021
Licenciamiento	Certificado Digital sitio seguro (SSL)	1	Unidad	1.642.359
Ethical Hacking y Retesting	software Ethical Hacking y Retesting	1	Unidad	65.672.915
Licenciamiento IPV6 membresía LACNIC	AÑO LACNIC	1	Unidad	2.400.000
Solución adquisición equipos Activos	Switch 48 Puertos	23	Unidad	417.796.037
Servicios especializados	Especialista Seguridad de la informática	1	Unidad x 12 meses	**114.595.200**
TOTAL				**602.106.511**
TOTAL 2021				**$ 973.765.981,00**

Fuente: OTI

12. CRONOGRAMA

A continuación, se presenta el cronograma de actividades proyectadas en el siguiente plan.

Tabla 3. Cronograma actividades Plan MSPI 2019 – 2020

CRONOGRAMA LISTA DE TAREAS MODELO DE SEGUDIDAD Y PRIVACIDAD DE LA INFORMACIÓN					
GESTION	**LINEAMIENTO MINTIC**	**TAREA**	**INICIO DE TAREA**	**FINAL DE TAREA**	**ASIGNADO A**
Inicio	No Aplica	Reunión de inicio del Modelo de Seguridad de la información	27/05/2019	27/05/2019	Profesional especializado seguridad informática
Política general	Guía 2 - Política General MSPI v1	Elaborar Política de seguridad y privacidad de la información	01/04/2019	30/04/2019	Profesional especializado seguridad informática
		Oficio para firma del presidente o memoria justificativa	01/06/2019	05/06/2019	Profesional especializado seguridad informática
		Aprobación de la política de seguridad y privacidad de la información por parte de la presidencia	15/06/2019	03-07-2019	Profesional especializado seguridad informática

CRONOGRAMA LISTA DE TAREAS MODELO DE SEGUDIDAD Y PRIVACIDAD DE LA INFORMACIÓN					
GESTION	**LINEAMIENTO MINTIC**	**TAREA**	**INICIO DE TAREA**	**FINAL DE TAREA**	**ASIGNADO A**
		Publicación de política de seguridad y privacidad de la información ADR	05-07-2019	15-07-2019	Profesional especializado seguridad informática
Seguridad del recurso humano	Guía 14 - Plan de comunicación, sensibilización, capacitación	Plan de socialización de seguridad y privacidad de la información 2019	05/06/2019	31-07-2019	Profesional especializado seguridad informática
		Plan de socialización de seguridad y privacidad de la información 2020	30-04-2020	30-05-2020	Profesional especializado seguridad informática
Gestión de activos	Guía para la Gestión y Clasificación de Activos de Información.	Actualización de registro de activos de la información de la vigencia anterior y publicar	15-08-2019	20-07-2019	Equipo interdisciplinario Activos
		Actualizar formato de levantamiento de activos de información para seguridad digital	01-08-2019	30/09/2019	Equipo Activos
		Levantamiento de activos de información para seguridad digital	01/04/2020	30/08/2020	Equipo Activos
		Publicación de activos de la información para seguridad digital aprobados por comité	01-10-2020	30/10/2020	Equipo Activos
Gestión de riesgos de seguridad digital	Guía 7 - Gestión de Riesgos	Actualización de lineamientos de riesgos	01-04-2020	30/06/2020	Equipo de Gestión de Riesgos
		Identificación, Análisis y Evaluación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital	01-08-2020	30/08/2020	Equipo de Gestión de Riesgos
		Aceptación de Riesgos Identificados	01-09-2020	30/09/2020	Equipo de Gestión de Riesgos
		Publicación Matriz de riesgos	01-10-2020	30/10/2020	Equipo de Gestión de Riesgos

CRONOGRAMA LISTA DE TAREAS MODELO DE SEGUDIDAD Y PRIVACIDAD DE LA INFORMACIÓN					
GESTION	**LINEAMIENTO MINTIC**	**TAREA**	**INICIO DE TAREA**	**FINAL DE TAREA**	**ASIGNADO A**
		Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	01-11-2020	30/11/2020	Equipo de Gestión de Riesgos
		Evaluación de riesgos residuales	01-11-2020	30/11/2020	Equipo de Gestión de Riesgos
		Actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo con los cambios solicitados.	01-12-2020	30/12/2020	Equipo de Gestión de Riesgos
Gestión de incidentes de seguridad de la información	Guía 21 - Gestión de Incidentes	Actualizar procedimiento gestión de incidentes de seguridad de la información	01/04/2019	30/04/2019	Profesional especializado seguridad informática
		Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	01/09/2019	15/12/2019	Profesional especializado seguridad informática
		Gestionar los incidentes de Seguridad de la Información identificados 2019	01-07-2019	31-12-2019	Profesional especializado seguridad informática
		Gestionar los incidentes de Seguridad de la Información identificados 2020	01-01-2020	31-12-2020	Profesional especializado seguridad informática
Procedimiento de seguridad de la información	Guía 3 - Procedimiento de Seguridad de la Información	Documento para ingreso seguro a los sistemas de información	01-07-2020	31/07/2020	Grupo de profesionales OTI
		Crear documento de gestión de usuarios y contraseñas	01-07-2020	31/07/2020	Grupo de profesionales OTI
		Política de gestión de control de acceso en el manual de políticas del Modelo de Seguridad y Privacidad de la Información	01-07-2020	31/07/2020	Profesional especializado seguridad informática

CRONOGRAMA LISTA DE TAREAS MODELO DE SEGUDIDAD Y PRIVACIDAD DE LA INFORMACIÓN					
GESTION	LINEAMIENTO MINTIC	TAREA	INICIO DE TAREA	FINAL DE TAREA	ASIGNADO A
		Crear documento de controles criptográficos y procedimiento de gestión de llaves criptográficas	01-08-2020	31/08/2020	Grupo de profesionales OTI
		Política de criptografía en manual de políticas manual de políticas del Modelo de Seguridad y Privacidad de la Información	01-08-2020	31/08/2020	Profesional especializado seguridad informática
		Crear documento de mantenimiento preventivo de equipos	01/05/2020	01/06/2020	Grupo de profesionales OTI
		Crear documento de protección contra códigos maliciosos	01/05/2020	01/06/2020	Grupo de profesionales OTI
		Crear documento de separación de ambientes	01/05/2020	01/06/2020	Grupo de profesionales OTI
		Crear documento de gestión de capacidad infraestructura	01/05/2020	01/06/2020	Grupo de profesionales OTI
		Crear documento de aseguramiento de servicios en la red	01/05/2020	01/06/2020	Grupo de profesionales OTI
		Crear documento de transferencia de información	01/06/2020	01/07/2020	Grupo de profesionales OTI
		Documento para el tratamiento de la seguridad en los acuerdos con los proveedores	01/06/2020	01/07/2020	Grupo de profesionales OTI
		Revisar documento adquisición, desarrollo y mantenimiento de software	01/06/2020	01/07/2020	Grupo de profesionales OTI
Aspectos de seguridad de la información de la gestión de continuidad de negocio	Guía 10 - Continuidad de Negocio	Crear documento de gestión de la continuidad de negocio y el plan	01/10/2020	30/12/2020	Grupo de profesionales OTI
	Guía 11 - Análisis de Impacto de Negocio	Análisis de impacto de negocio BIA	01/10/2020	30/12/2020	Grupo de profesionales OTI

CRONOGRAMA LISTA DE TAREAS MODELO DE SEGUDIDAD Y PRIVACIDAD DE LA INFORMACIÓN					
GESTION	**LINEAMIENTO MINTIC**	**TAREA**	**INICIO DE TAREA**	**FINAL DE TAREA**	**ASIGNADO A**
Roles y responsabilidades	Guía 4 - Roles y responsabilidades	Roles y responsabilidades de seguridad y privacidad de la información	01-07-2020	31-07-2020	Profesional especializado seguridad informática
Seguridad en la nube	Guía 12 - Seguridad en la Nube	Aseguramiento de la información en la nube	01/06/2020	30/06/2020	Grupo de profesionales OTI
Protocolo IPv4_IPv6	Guía 19 - Aseguramiento de protocolo IPv4_IPv6	Situación actual de la red	01-08-2019	31-12-2019	Profesional especializado seguridad informática Grupo de profesionales OTI
		Inventario de equipos activos	01-08-2020	31-12-2020	Profesional especializado seguridad informática Grupo de profesionales OTI
		Topología de red y direccionamiento actual	01-08-2020	31-12-2020	Profesional especializado seguridad informática Grupo de profesionales OTI
	Guía 20 - Transición IPv4_IPv6	Plan diagnostico IPV6	01-08-2019	31-12-2019	Profesional especializado seguridad informática
		Plan de adopción del protocolo ipv6	01-08-2019	31-12-2019	Profesional especializado seguridad informática
		Adquisición de direccionamiento ante LACNIC y sistema autónomo	01-11-2019	31-12-2019	Profesional especializado seguridad informática

CRONOGRAMA LISTA DE TAREAS MODELO DE SEGUDIDAD Y PRIVACIDAD DE LA INFORMACIÓN					
GESTION	**LINEAMIENTO MINTIC**	**TAREA**	**INICIO DE TAREA**	**FINAL DE TAREA**	**ASIGNADO A**
		Ejecutar plan de adopción de protocolo IPV6 (implementación de ipv6 ADR)	01-03-2020	31-12-2020	Profesional especializado seguridad informática Grupo de profesionales OTI
Controles de seguridad de la información	Guía 8 - Controles de Seguridad de la Información	Evaluación inicial de controles	01-08-2020	31-08-2020	Equipo de Gestión de Riesgos
		Declaración de aplicabilidad			
Vulnerabilidades	Guía 1 Metodológica de Pruebas de Efectividad	Definir lineamientos para ejecutas las pruebas de vulnerabilidades	01-08-2020	31-09-2020	Equipo de Gestión de Riesgos
		Definir estudios previos y procesos de contratación para realizar el análisis de vulnerabilidades teniendo en cuenta el alcance	01-01-2021	31-01-2021	Equipo de Gestión de Riesgos
		Ejecución de las pruebas de vulnerabilidades de acuerdo con el alcance y la metodología establecida	01-10-2020	31-10-2020	Auditoría externa
		Ejecutar plan de remediación	01-10-2020	31-10-2020	Equipo de Gestión de Riesgos
Indicadores del modelo de seguridad y privacidad de la información	Guía 9 - Indicadores Gestión de Seguridad de la Información	Realizar la evaluación de indicadores para medir	01/08/2020	30/08/2020	Profesional especializado seguridad informática Grupo de profesionales OTI
		Entregar informe mensual de indicadores	01/09/2020	31/12/2020	Profesional especializado seguridad informática Grupo de profesionales OTI

CRONOGRAMA LISTA DE TAREAS MODELO DE SEGUDIDAD Y PRIVACIDAD DE LA INFORMACIÓN					
GESTION	LINEAMIENTO MINTIC	TAREA	INICIO DE TAREA	FINAL DE TAREA	ASIGNADO A
Protección de datos personales	SIC	Revisar política de datos personales vigente	01/08/2020	30/08/2020	Profesional especializado seguridad informática
		Actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	01/10/2020	30/10/2020	Profesional especializado seguridad informática
Auditoria	Guía 15 - Auditoria	Solicitar por medio de oficio a la oficina de planeación, control interno y al Comité de Coordinación del Sistema de Control Interno, la programación autoría del MSPI	15/02/2021	27/02/2021	Jefe de la Oficina de Tecnologías de la información
Evaluación de desempeño	Guía 16 - Evaluación de Desempeño	Solicitar por medio de oficio a la oficina de planeación y control interno la revisión y seguimiento del MSPI	16/03/2021	27/03/2021	Jefe de la Oficina de Tecnologías de la información
Mejora continua	Guía 17 - Mejora continua	Solicitar por medio de oficio a la oficina de planeación y control interno el acompañamiento Planes de mejoras propuestos	01/06/2021	19/06/2021	Jefe de la Oficina de Tecnologías de la información

Fuente: OTI

13. INDICADOR

A continuación, se presenta el indicador proyectado para la evaluación del siguiente plan.

Tabla 4. Indicador Plan MSPI 2019 – 2020

ID de la métrica	**IND_OTI_SEG_01**
Nombre del indicador	PLAN DE SEGURIDAD DE LA INFORMACION
Propósito del indicador	El indicador permite medir la ejecución de las actividades relacionadas en el plan en seguridad de la información por parte de la ADR . Estas mediciones se podrán realizar por medio de auditorías especializadas en el tema o de forma aislada por parte de los responsables de las actividades
Objetivo de control o controles asociados	El objetivo del indicador es establecer la efectividad de un plan de seguridad de la información previamente definido como medio para el control de SI.
Destinatario	OTI
Formula	número de actividades programadas del plan de SI /número de actividades realizadas del plan de SI
Escala	Porcentaje
Nivel para el cumplimiento	80%
Frecuencia de medición	Anual
Fuente de datos	Oficial de Seguridad de la Información, auditorías internas
MEDICIÓN	
$IND\ OTI\ SEG\ 01 = \frac{Numero\ de\ actividades\ programadas\ en\ el\ plan\ SI}{Numero\ de\ actividades\ realizadas\ del\ plan\ SI}$	
NIVEL DE CUMPLIMIENTO	Medición anual con corte diciembre

Fuente: OTI

14. BIBLIOGRAFIA

Departamento Nacional de Planeación (DNP). (03 de mayo de 2019). *Bases Del Plan Nacional de Desarrollo 2018-2022.* Obtenido de https://colaboracion.dnp.gov.co/CDT/Prensa/BasesPND2018-2022n.pdf

Departamento Nacional de Planeación. (11 de Abril de 2016). *CONPES 3854 Política Nacional de Seguridad Digital.* Recuperado el 12 de Septiembre de 2019, de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Departamento Nacional de Planeación. (1 de Julio de 2020). *CONPES 3995 POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL*. Recuperado el 1 de 12 de 2017, de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (29 de Julio de 2016). *Modelo de Seguridad y Privacidad.* Recuperado el 3 de 10 de 2017, de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (Junio de 2018). *Manual de Gobierno Digital.* Recuperado el 2019, de https://www.gobiernodigital.gov.co/623/articles-81473_recurso_1.pdf

NTC-ISO/IEC 27001:2013. (11 de Diciembre de 2013). *Norma Técnica Colombiana NTC-ISO/IEC 27001:2013.* Recuperado el 1 de Septiembre de 2018, de 2013-12-11: https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion/