ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

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

2021

ARCHIVO GENERAL DE LA NACIÓN JORGE PALACIOS PRECIADO

La cultura es de todos Mincultura

ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

Titulo	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
Fecha actualización:	Septiembre del 2020				
Sumario	plan comprende las directrices trazadas en el Modelo de Gestión de Riesgos de Seguridad Digital, establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC, en consonancia con las buenas prácticas definidas en ISO/IEC 27001 y NTC-ISO-IEC 27001, en plena conexidad con la implementación de lo dispuesto en la legislación vigente sobre protección y tratamiento de datos personales.				
Palabras claves:	Políticas, Buenas prácticas, Controles, Guía				
Formato:	PDF		Lenguaje:		Español
Código:	GIT-M-02	Versión:	3	Estado:	
Categoría:	Documento Técnico				
Autor:	Jaime Alberto Duarte Hoyos				
Revisó:	Omar Villarreal Osorio				
Presentación aprobación					
Aprobó:	Comité Institucional de Gestión del Desempeño				
Información Adicional:					

CONTENIDO

INTRODUCCIÓN

Esta metodología define el análisis, evaluación y tratamiento de riesgos de Seguridad de la Información, tomando como base la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública (DAFP) y la "Guía de Gestión de Riesgos" del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), realizando la identificación, análisis, valoración, tratamiento de los riesgos e identificación de las vulnerabilidades y amenazas asociadas a los riesgos conforme a la norma ISO/IEC 27005:2011 Tecnologías de la información- Técnicas de Seguridad- Administración de riesgos de Seguridad de la Información.

1. PROPÓSITO.

El presente Plan establece las acciones específicas para liderar la implementación del Modelo de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en la Archivo General de la Nación -AGN, con el fin de preservar la confidencialidad, integridad, disponibilidad y no repudio de la información; así como, la protección de la privacidad en el marco del Sistema de Gestión de Seguridad de la Información del AGN

2. ALCANCE.

El plan comprende las directrices trazadas en el Modelo de Gestión de Riesgos de Seguridad Digital, establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC, en consonancia con las buenas prácticas definidas en ISO/IEC 27001 y NTC-ISO-IEC 27001, en plena conexidad con la implementación de lo dispuesto en la legislación vigente sobre protección y tratamiento de datos personales.

El alcance Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se fija para la vigencia 2021

3. DEFINICIONES.

- **Activos de Información.** Todo aquel elemento de información, recibido, gestionado o producido, que posee valor para la entidad y, por lo tanto, debe protegerse para el logro de la misión. Serán activos de información críticos aquellos que son imprescindibles o su valor es clave para la operación de la entidad. Cuando se trate de activos informáticos, se entenderán como aquellos dispositivos tecnológicos que permiten la emisión, transmisión, procesamiento y recepción de información.

- **Acuerdo de confidencialidad.** Conocido también como acuerdo de no divulgación, es un documento formal entre al menos dos partes interesadas, para compartir información considerada como confidencial, pero restringida para el uso público.

- **Acuerdo de Nivel de Servicio (ANS).** Documento que contiene las especificaciones o características de un servicio que se será entregado por un proveedor y su cliente o usuario. Entre

dos o más áreas de una entidad, se conoce como Acuerdo de Nivel Operacional (OLA1).

- **Agente de amenaza.** Entidad humana o no humana que explota una vulnerabilidad.
- **Anti Rootkits.** Aplicativo de software que busca bloquear un rootkits o código malicioso que permite el acceso privilegiado a una computadora de manera oculta al administrador, buscando dañar el funcionamiento normal del sistema operativo y algunas aplicaciones.
- **Bluetooth.** Especificación tecnológica para redes inalámbricas, permite transmisión de voz y datos entre dispositivos.
- **Cibernético.** Ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas.
- **Cifrado.** Método que permite aumentar la seguridad de la información de un archivo o mensaje mediante la codificación de su contenido, para que sólo pueda leerlo por el usuario autorizado y que posea la contraseña de cifrado para descodificarlo.
- **Cloud Computing.** Concepto tecnológico que se basa en que las aplicaciones software y los equipos hardware con capacidad de proceso y almacenaje de datos están ubicados en un Datacenter que permite a los usuarios acceder a las aplicaciones y servicios disponibles a través de Internet o como se conoce coloquialmente, a través de “la Nube” de Internet (Guía 12 Seguridad en la Nube, MinTIC).
- **Confidencialidad.** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 27001).
- **Custodia.** Acción de guardar con cuidado y vigilancia una información o mensaje.
- **Disponibilidad.** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. (ISO/IEC 27001).
- **Hardware.** Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.
- **IoT.** Sigla en inglés para Internet de las Cosas, que comprende la tecnología en la que se interconectan dispositivos u objetos cotidianos, mediante internet.
- **Infraestructura.** Conjunto de activos o recursos técnicos, servicios o instalaciones que se consideran necesarios para el desarrollo normal de procesos o actividades.
- **Integridad.** Propiedad de salvaguardar la exactitud y estado completo de los activos. (ISO/IEC 27001).
- **NFC (Near Field Communication).** Tecnología de comunicación inalámbrica de corto alcance

[1] Operational Level Agreement (OLA), ITIL

que facilita el intercambio de información entre dispositivos como smartphones y tablets.

- **No Repudio**. Es la garantía de que no puedan ser negados los mensajes en una comunicación electrónica (Guía 3 Cero papeles, MinTIC). Esto permite vincular al autor con la responsabilidad derivada de sus actuaciones y certificar que los datos o información provienen de la fuente que dice ser.

- **OT**. Sigla en inglés para Tecnología Operacional y comprende los dispositivos, redes y software asociados a procesos industriales, como tareas robotizadas, redes inteligentes, entre otros. Al software que permite controlar y supervisar estos procesos industriales, se le conoce como SCADA.

- **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, ISO 22301 de 2012 y la NTC 5722 de 2009).

- **Privacidad.** Derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar, que genera la obligación de proteger dicha información en observancia del marco legal vigente.

- **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).

- **Riesgo de corrupción.** Posibilidad que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

- **Riesgo inherente.** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

- **Riesgo institucional.** Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:

    - Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.
    - Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.
    - Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.
    - Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.

- **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.

- **Valoración del riesgo**: establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización.

- **Seguridad de la información.** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Software.** Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora2.

- **T.I. Tecnología de la Información**, generalmente se conoce así al área o dependencia que administra la tecnología en una entidad. Para el presente documento, OTI o TI hacen referencia a la Oficina de Tecnología de la Información del AGN.

- **WiFi**. Tecnología que permite la interconexión inalámbrica de dispositivos electrónicos a internet.

4. OBJETIVOS.

4.1. OBJETIVO GENERAL.

Establecer las actividades y metodologías para una adecuada Gestión de Riesgos de Seguridad y Privacidad de la Información, a partir de su identificación, evaluación, tratamiento y seguimiento.

4.2. OBJETIVOS ESPECÍFICOS.

A través de las acciones a ejecutar se pretende:

- Aumentar la probabilidad de alcanzar los objetivos estratégicos y de los procesos.
- Concienciar a todos los funcionarios de Carrera Administrativa, Provisionalidad, Contratistas, Pasantes del AGN, Áreas, Procesos, Proveedores y/o externos en general, sobre la necesidad e importancia de administrar de manera adecuada los riesgos asociados a la gestión del proceso propio del área.
- Fomentar el compromiso de todos los funcionarios de Carrera Administrativa, Provisionalidad, Contratistas, Pasantes, del AGN, Áreas, Procesos, Proveedores y/o externos en general, la formulación e implementación de controles y acciones encaminadas a prevenir y gestionar los riesgos.
- Establecer, mediante una adecuada administración de riesgos informáticos, una base confiable para la toma de decisiones y la planificación institucional.
- Socializar la necesidad constante de identificar y tratar los Riesgos de Seguridad y Privacidad de la Información, en todos los niveles del AGN.
- Involucrar y comprometer a todos los funcionarios de Carrera Administrativa, Provisionalidad, Contratistas, pasantes y/o del AGN, en la búsqueda de las acciones encaminadas a prevenir y administrar los riesgos.

2 Definición según la Real Academia de la Lengua Española -RAE, recuperado de http://dle.rae.es/?id=YErlG2H el 2 de abril de 2018

- Proteger los recursos del estado.
- Asignar y usar eficazmente los recursos para el tratamiento de riesgos Informáticos.
- Establecer el Mapa de Riesgos y la Matriz de Riesgos de Seguridad de la Información.

5. CONTEXTO ORGANIZACIONAL.

El Archivo General de la Nación es la entidad encargada de formular y liderar la Política de Archivos y de Gestión Documental en el territorio nacional, referente de la gestión pública para salvaguardar y difundir el patrimonio documental como herramienta para la transparencia y el acceso a la información pública

De conformidad con el Decreto 2126 de 2012, la estructura orgánico funcional del Archivo General de la Nación, está así:

1) Consejo Directivo.
2) Dirección General
    1) Grupo de Sistemas.
    2) Oficina Asesora de Planeación
    3) Oficina de Control Interno
    4) Oficina de Comunicaciones
    5) Oficina Asesora Jurídica
    6) Secretaria General
        i) Grupo de Archivo y Gestión Documental
        ii) Grupo de Recursos Físicos
        iii) Grupo de Gestión Financiera
    7) Subdirección del Sistema Nacional de Archivo
        i) Grupo de Articulación y desarrollo del SNA
        ii) Grupo de Inspección y Vigilancia
    8) Subdirección de Tecnologías de la Información Archivística y Documento Electrónico.
        i) Grupo de Documentos Electrónicos y Preservación Digital
        ii) Grupo de Innovación y Apropiación de Tecnologías de la Información Archivística
    9) Subdirección de Gestión del Patrimonio Documental.
        i) Grupo de Conservación y Restauración del Patrimonio Documental
        ii) Grupo de Investigación y Fondos Documentales Históricos
        iii) Grupo de Organización Descripción y Reprografía
        iv) Grupo de Evaluación Documental y Transferencias Secundarias
        v) Vicepresidencia de Operaciones, Regalías y Participaciones.
        vi) Órganos de Asesoría y Coordinación
    10) Subdirección de Asistencia Técnica y Proyectos Archivísticos
        i) Grupo de Gestión de Proyectos Archivísticos
        ii) Grupo de Asistencia Técnica Archivística
        iii) Grupo de Administración Integral

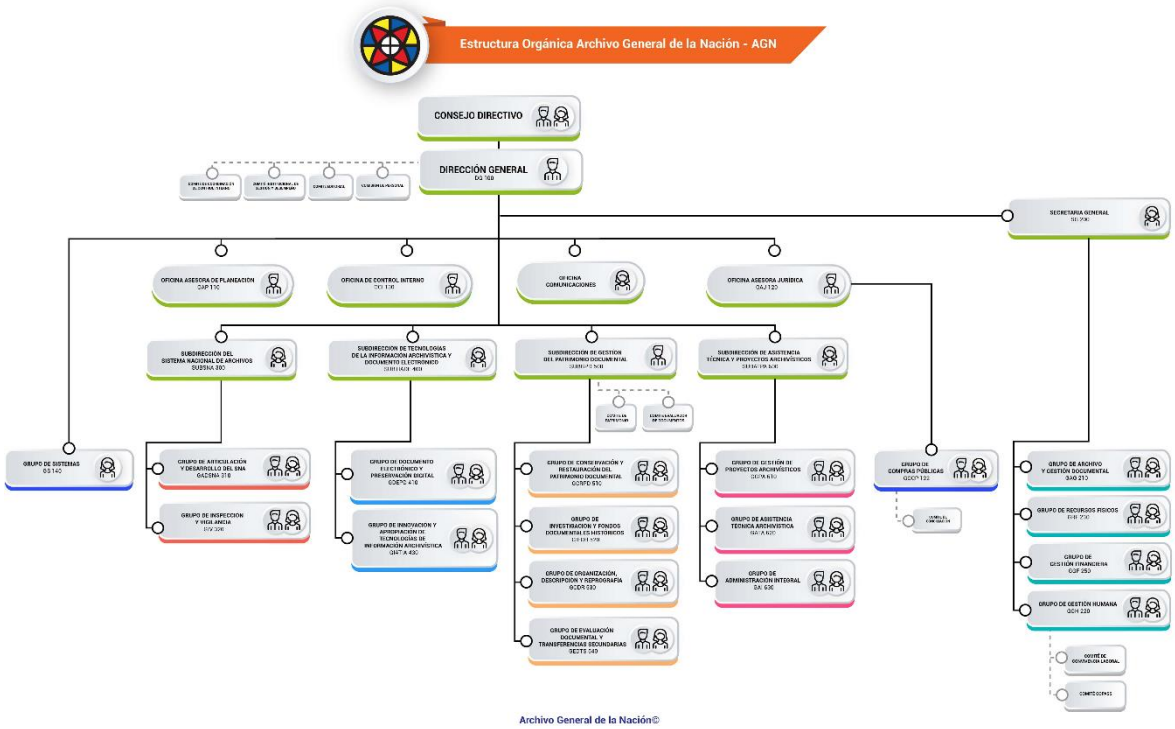

Imagen 1. Organigrama AGM

Es necesario aclarar, que según Resolución 339 de 2020 *"Por la cual se suprime un grupo interno de trabajo, se conforman los Grupos Internos de Trabajo en el Archivo General de la Nación Jorge Palacios Preciado y se establecen sus funciones"*, se suprime el Grupo de Administración Integral adscrito a la Subdirección de Asistencia Técnica y Proyectos Archivísticos creado mediante Resolución N° 102 del 22 de febrero de 2019 y se conforman los siguientes grupos internos de trabajo:

1. SECRETARÍA GENERAL:
1.1 Grupo de Archivo y Gestión Documental.
1.2 Grupo de Gestión Humana.
1.3 Grupo de Recursos Físicos.
1.4 Grupo de Gestión Financiera.
1.5 Grupo de Sistemas.
2. OFICINA ASESORA JURÍDICA:
2.1. Grupo de Gestión de Compras Públicas
3. SUBDIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN ARCHIVÍSTICA Y DOCUMENTO ELECTRÓNICO:
3.1. Grupo de Documentos Electrónicos y Preservación Digital.
3.2. Grupo Innovación y Apropiación de Tecnologías de Información Archivística.
4. SUBDIRECCIÓN DE ASISTENCIA TÉCNICA Y PROYECTOS ARCHIVÍSTICOS:
4.1 Grupo de Gestión de Proyectos Archivísticos.
4.2 Grupo de Asistencia Técnica Archivística.
5. SUBDIRECCIÓN DE GESTIÓN DEL PATRIMONIO DOCUMENTAL:

5.1 Grupo de Conservación y Restauración del Patrimonio Documental.
5.2 Grupo de Investigación y Fondos Documentales Históricos.
5.3 Grupo de Organización, Descripción y Reprografía.
5.4 Grupo de Evaluación Documental y Transferencias Secundarias.
6. SUBDIRECCIÓN DEL SISTEMA NACIONAL DE ARCHIVOS:
6.1 Grupo de Articulación y Desarrollo del Sistema Nacional de Archivos.
6.2 Grupo de Inspección y Vigilancia.

Del mismo modo, según resolución 365 de 2020 "*Por la cual se modifica parcialmente la Resolución N° 339 del 21 de agosto de 2020 "Por la cual se suprime un grupo interno de trabajo, se conforman los Grupos Internos de Trabajo en el Archivo General de la Nación Jorge Palacios Preciado y se establecen sus funciones",* se crea el Grupo de Servicio al Ciudadano.

Para la organización de la seguridad de la información, el AGN entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de Gestión de Seguridad y Privacidad de la Información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado, la sociedad y las empresas del sector, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con su misión y visión.

Así las cosas, en aras de cumplir con este compromiso, las directrices, normas y buenas prácticas en la materia, se ha establecido el Comité Institucional de Gestión y Desempeño del AGN, se ha adoptado el Sistema de Gestión de Seguridad de la Información -SGSI, se ha declarado y definido la Política General de Seguridad y Privacidad de la Información, así como se ha establecido el Manual de Políticas Específicas de Seguridad y Privacidad de la Información y, la Política de Protección de Datos Personales.

En tal sentido, se han implementado herramientas y controles de seguridad informática que permiten dar cumplimiento a las políticas establecidas, salvaguardando la confidencialidad, integridad, disponibilidad y no repudio de la información de la entidad.

Como responsable de liderar la implementación del SGSI, se ha designado el Rol de Oficial de Seguridad de la Información

6. ANÁLISIS DE RIESGOS.

El análisis del riesgo Informático busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, evaluándolos con el fin de obtener información para calificar su nivel.

Se han establecido dos aspectos: probabilidad e impacto, para tener en cuenta en el análisis de los riesgos identificados.

Por probabilidad se entiende la posibilidad de ocurrencia del riesgo y puede ser medida con criterios de frecuencia si se ha materializado, o de factibilidad teniendo en cuenta la presencia de factores internos y externos, que pueden propiciarlo, aunque éste no se haya materializado.

El impacto se mide por las consecuencias que puede ocasionar a la Entidad la materialización del riesgo. Los pasos para el análisis de los riesgos son:

6.1. CALIFICACIÓN DEL RIESGO.

Para la definición del impacto se debe tener en cuenta la clasificación del riesgo (estratégico, operativo, financieros, cumplimiento, tecnología, imagen) de acuerdo con la clase del riesgo y la magnitud del impacto se debe determinar el nivel en el que se encuentra.

6.2. EVALUACIÓN DEL RIESGO.

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.

Con la evaluación del riesgo, previa a la formulación de controles, se obtiene la ubicación del riesgo en la matriz de evaluación; esto se denomina evaluación del riesgo inherente.

6.2.1. DESARROLLO PRÁCTICO – ANÁLISIS.

Formato de Análisis de riesgos, el cual hace parte del proceso Administración del Sistema Integrado de Gestión de Calidad, donde se debe relacionar la siguiente información:

- Riesgo**:** Relacionar el riesgo redactado en el mapa de riesgos**.**
- Calificación de probabilidad: de acuerdo con la información cuantitativa y cualitativa generada por el análisis de los Riesgos.
- Calificación de impacto: de acuerdo con la información cuantitativa y cualitativa generada por el análisis de los Riesgos.
- Clasificación del riesgo: Ver componentes de la identificación del riesgo, en el apartado de clasificación de los riesgos.
- Evaluación: surge del cruce de los resultados cuantitativos de la calificación para probabilidad e impacto.

6.3. VALORACIÓN DE LOS RIESGOS.

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo. Lo anterior de acuerdo con los formatos Identificación y evaluación de controles y Valoración del riesgo.

6.4. SEGUIMIENTO DE RIESGOS.

La Oficina de Control Interno, realizará seguimiento a todo el componente de administración de riesgos y verificará aspectos como:

- Cumplimiento de las políticas y directrices para la administración del riesgo: metodología de Administración del Riesgo (diseño y funcionamiento).
- Administración de los riesgos por proceso e institucionales: calificación y evaluación, efectividad de los controles y cumplimiento de las acciones.

Los resultados de la evaluación y las observaciones de Control Interno, deben ser presentados a la Dirección General, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo en el AGN.

7. MAPA DE RIESGOS.

Una vez se tenga toda la información relacionada en los numerales anteriores, se documentará la información en el formato Mapa de riesgos del AGN.

Los responsables de procesos y sus equipos de trabajo deben garantizar que la información de los riesgos sea adecuada, coherente, pertinente y vigente. Cualquier ajuste que se deba realizar de esta información, debe ser notificado al oficial de seguridad.

8. DESARROLLO DEL PLAN.

8.1. HORIZONTE DEL PLAN.

Para 2021, se establecen las actividades de acuerdo con el enfoque en Riesgos, realizando el respectivo cruce entre lo establecido en el Modelo de Seguridad y Privacidad de la Información, la Política de Gobierno Digital (antes Gobierno en Línea) del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, la matriz de autodiagnóstico del Modelo Integrado de Planeación y Gestión – MIPG del Departamento Administrativo de la Función Pública – DAFP y las buenas prácticas aplicables. De igual manera se tiene en cuenta los siguientes recursos disponibles:

- ✓ Talento Humano especializado
- ✓ Infraestructura tecnológica.
- ✓ Capacidad instalada en términos de cultura de seguridad organizacional y capacitación del personal.
- ✓ Presupuesto destinado para Implementación del SGSI.

Con base en lo anterior, se cuenta con recursos para plasmar acciones de mejora que permitan enfocar a la entidad hacia la meta establecida, considerando actividades concretas, medibles y alcanzables, que admitan la mejora continua.

8.2. CRONOGRAMA.

Se establece el siguiente cronograma, detallando en el plan de trabajo las acciones, los responsables y el plazo de ejecución.

Id	Actividades de Mejora	Responsable	Plazo
1	Diseño de políticas de gestión de riesgos informáticos.	Oficial de Seguridad de la Información.	28-02-2021
2	Actualizar los activos de Información del AGN.	Oficial de Seguridad de la Información.	30-04-2021
3	Elaboración Pentesting	Oficial de Seguridad de la Información	30-06-2021 30-11-2021
	Análisis de vulnerabilidades	Oficial de Seguridad de la	31-07-2021

Id	Actividades de Mejora	Responsable	Plazo
	informáticas	Información	
4	Evaluación de Riesgos.	Comité Técnico de Seguridad de la Información	30-10-2021
5	Implementación de Controles.	Especialista Seguridad de la Información.	30-10-2021
6	Seguimiento a cronograma y documentación.	Coordinador Grupo de Sistemas.	30-10-2021

9. CONTROL DE CAMBIOS

FECHA	VERSIÓN	PROYECTÓ	REVISÓ	APROBÓ	DESCRIPCIÓN
23-05-2018	1.0	Heilin Guarnizo Rodriguez.	Manuel Gomez Patiño.	Erika Rangel Palencia	Versión inicial
18-02-2019	2.0	Heilin Guarnizo Rodriguez.	Manuel Gomez Patiño.	Manuel Gomez Patiño.	Actualización
30-11-2020	3.0	Jaime Alberto duarte	Omar Villarreal Osorio	Omar Villarreal Osorio	Actualización