ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

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

2022

ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

CONTENIDO

Titulo	**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**				
Fecha actualización:	Noviembre del 2021				
Sumario	El plan comprende las directrices trazadas en el Modelo de Gestión de Riesgos de Seguridad y Privacidad de la Información, 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:	4	Estado:	
Categoría:	Documento Técnico				
Autor:	Jaime Alberto Duarte Hoyos				
Revisó:	Omar Villarreal Osorio				
Presentación aprobación					
Aprobó:	Comité Institucional de Gestión del Desempeño				
Información Adicional:					

INTRODUCCIÓN

Este plan define el análisis, evaluación y tratamiento de los riesgos de seguridad y privacidad 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. OBJETIVOS.

1.1. OBJETIVO GENERAL.

Realizar el tratamiento de riesgos de seguridad y privacidad de la información alineado con la guía metodológica para la gestión del riesgo del DAFP adoptada por el Archivo General de la Nación.

1.2. OBJETIVOS ESPECÍFICOS.

- Realizar el plan de trabajo específico vigencia 2022, conforme a los resultados obtenidos de las auditorías realizadas en la vigencia 2018 y de los mapas de riesgos institucionales.
- Alinear los procesos de información del Archivo General de la Nación con los de datos personales dando cumplimiento a la ley 1581 de 2012 y demás normas concordantes.
- Aportar avances al modelo integrado de planeación y gestión en sus políticas gobierno digital, seguridad digital, transparencia, acceso a la información pública y lucha contra la corrupción entre otras.
- Gestionar los riesgos de seguridad y privacidad de la información buscando la integración de la metodología del DAFP

2. ALCANCE.

La vigencia del presente plan es 2022 y aplica para los 14 procesos que hacen parte del mapa de procesos definido en el sistema de gestión de calidad del Archivo General de la Nación, siendo un (1) proceso estratégico, siete (7) procesos de apoyo, cuatro (5) procesos misionales, un (1) proceso de evaluación independiente.

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).

[1] Operational Level Agreement (OLA), ITIL

- **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 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. ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

El análisis del riesgo de seguridad de la información 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:

4.1. 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.

4.2. 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.

---

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

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.

4.2.1. 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.

4.3. 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.

4.4. SEGUIMIENTO DE RIESGOS.

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

- Cumplimiento de las políticas y directrices para la administración del riesgo en seguridad y privacidad de la información.
- Administración de los riesgos de seguridad y privacidad de la información 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, serán presentadas a la Dirección General, en el momento que lo considere pertinente, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración de estos riesgos en el AGN.

5. MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

El Archivo General de la Nación en su mapa de riesgos tiene definidos los riesgos tecnológicos y de seguridad digital, los cuales serán el objeto de tratamiento para mantener la integridad y confidencialidad de la información.

Riesgo / amenaza	Tipología ó clasificación de riesgos	Causas ó vulnerabilidad		Descripción del control
Afectación de la plataforma tecnológica de canales de datos, canal de Internet y Networking	Riesgos tecnológicos	**1**	Corte de energía eléctrica, fluctuaciones de tensión, ruido eléctrico, subtensión, sobretensión, interrupciones y siniestros eléctricos.	El coordinador del grupo de sistemas cada vez que ocurre una falta de fluido eléctrico verifica en el centro de datos la activación de las UPS´s con el fin de garantizar la disponibilidad de la operación de la infraestructura tecnológica y los sistemas de información. En caso de no funcionar las UPS´s el Coordinador del Grupo de Sistemas de manera inmediata informara mediante correo electrónico la falla al proveedor con el fin de solventar el inconveniente presentado. Por otro lado, solicitara al Coordinador del Grupo de Recursos Físicos mediante un correo electrónico la activación de plan de contingencia alterno de energía. Como evidencia estará los correos electrónicos enviados y el informe de incidentes.
		2	Falta de mantenimiento a los sistemas de suministro y respaldo de energía (UPS)	El profesional asignado por el coordinador del grupo de sistemas verificara la elaboración del mantenimiento realizado a la UPS cada vez que esta se haga, de acuerdo con el cronograma realizado; con el fin de garantizar su funcionabilidad en caso de falla del fluido eléctrico; dejando como evidencia la hoja de vida actualizada de las UPS´s . En caso de no haberse realizado el mantenimiento por parte del proveedor, el funcionario informará al coordinador del grupo de sistemas mediante correo electrónico
		3	Falta de mantenimiento a los sistemas de climatización del centro de datos (Aires acondicionados)	El profesional asignado por el coordinador del grupo de sistemas verificara la elaboración del mantenimiento a los sistemas de climatización del Centro de datos realizado por parte del personal del Grupo de Recursos físicos esto acorde con el cronograma realizado; con el fin de garantizar su funcionamiento y evitar sobrecalentamiento del centro de datos eléctrico; dejando como evidencia la hoja de

Riesgo / amenaza	Tipología ó clasificación de riesgos	Causas ó vulnerabilidad		Descripción del control
				vida actualizada del sistema de climatización. En caso de no haberse realizado el mantenimiento por parte de Recursos físicos el funcionario informará al coordinador del grupo de sistemas mediante correo electrónico
		4	Falta de un plan detallado de mantenimiento de los servidores	La Mesa de Servicios realizará el mantenimiento a los servidores cada semestre con el fin de garantizar su funcionamiento, evitar fallas que ocasiona perdida en la información de la entidad, dejando como evidencia la actualización de las hojas de vida de cada uno de ellos; en caso de no realizarse el funcionario responsable de los mantenimientos deberá informar al coordinador del grupo de sistemas el motivo por el cual no se realizaron
		5	Falta de un plan de backups a nivel de networking en la entidad.	El profesional asignado debe ejecutar periódicamente los backups de estos equipos o según sea el procedimiento cuando estos cambien de configuración, para mantener la topología lógica lo más actualizada posible.
		6	Falta de Datacenter Alterno.	El coordinador del grupo de sistemas debe plantear la propuesta de crear un datacenter alterno el cual se debe ubicar en instalaciones físicas fuera de las del archivo o en la nube; debe proteger con mucha más seguridad del robo de datos, y de pérdidas por malware o por fallos del propio servidor. También se realizan copias de seguridad que permiten recuperar los datos en el caso de que la empresa tenga un fallo en su sistema. Para las áreas más críticas de la entidad, así como los servicios que no pueden estar fuera de operación.
Perdida de la integridad de la información	Riesgos de seguridad digital	**1**	Falta de actualización a la política de configuración del firewall.	El profesional, administrador de la red de datos de la Entidad, registra en el formato de bitácora del centro de cómputo, las novedades de acuerdo a la demanda del proceso, esta actividad deberá realizarse cada semestre, con el fin de mantener actualizada la política de firewall. En caso de no registrar en la bitácora se verifica el log del firewall.

Riesgo / amenaza	Tipología ó clasificación de riesgos	Causas ó vulnerabilidad		Descripción del control
		2	Desconocimiento por parte de los usuarios de los lineamientos y compromisos de seguridad de la información	El Oficial de Seguridad de la Información realiza dos sensibilizaciones en el año, con temas de seguridad de la información, con el fin de reforzar el conocimiento frente a las políticas de seguridad de la información y prevenir daños que pueden afectar la información de la Entidad, dejando evidencia a través de listados de asistencia. En caso de no poderse realizar la socialización se enviará por correo electrónico el Boletín informativo de seguridad de la información; dejando como evidencia las listas de existencia y copia de los boletines informativos
		3	Fallas en la asignación de roles y permisos	El profesional asignado por el Coordinador del Grupo de Sistemas verifica en el sistema de información, servidores y bases de datos cada vez que es solicitado por el Coordinador de un Grupo solicite vía correo electrónico al Coordinador del Grupo de Sistemas utilizando el formato preestablecido , los roles y permisos para el funcionario que así lo requiera, en caso de no poderse realizar el Coordinador de Sistemas responderá mediante correo electrónico el motivo por el cual no fue creado el rol y asignado los permisos; dejando como evidencia los correos electrónicos
Perdida de la Disponibilidad de la Información	Riesgos de seguridad digital	**1**	Aumento de ataques Informáticos sobre la infraestructura del AGN	El profesional asignado por el coordinador del Grupo de Sistemas verificara la instalación de los parche de actualización del sistema operativo , antivirus cada vez que las empresas proveedoras de los mismos los emitan, esto con el fin de minimizar los ataques cibernéticos a la entidad , protegiendo de esta forma la disponibilidad , integridad y confiabilidad de la información, de no hacerlo elaborará un informe el cual será dirigido al Coordinador del Grupo de Sistemas explicando el porqué. Dejando como evidencia el correo con el informe o el formato de actualización de antivirus y Sistemas Operativos

Riesgo / amenaza	Tipología ó clasificación de riesgos	Causas ó vulnerabilidad		Descripción del control
		2	Falta de un plan detallado de mantenimiento a los equipos de cómputo	El profesional o técnico de la mesa de servicios , realizará dos mantenimientos preventivos y/o correctivos en el año a todos y cada uno de los equipos de cómputo propios de la Entidad diligenciando el formato propio de la hoja de vida de cada equipo, consignando en ellos las novedades con el fin de prevenir daños en los equipos; en caso de no realizarse el mantenimiento programado, el funcionario responsable informara al Coordinador del Grupo de Sistemas el motivo por el cual no fue posible la labor. Dejando como evidencia el historial actualizado de los equipos de cómputo o el informe detallado en caso de no haberse realizado el mantenimiento

6. DESARROLLO DEL PLAN.

Para 2022, 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
- ✓ 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.

6.1. 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.	Grupo de sistemas.	28-02-2022
2	Actualizar los activos de Información del AGN.	Grupo de sistemas.	30-04-2022
3	Elaboración Pentesting (por un tercero)	Grupo de sistemas	30-06-2022 30-11-2022
5.	Elaboración ingeniería social (por un tercero)	Grupo de sistemas	30-06-2022 30-11-2022
6	Elaboración de hacking ético y penetración (por un tercero)	Grupo de sistemas	30-06-2022 30-11-2022
7	Análisis de vulnerabilidades informáticas	Grupo de sistemas	31-07-2022
8	Evaluación de Riesgos.	Grupo de sistemas	30-10-2022

ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

7. CONTROL DE CAMBIOS

VERSIÓN	FECHA APROBACIÓN	RESPONSABLE	DESCRIPCIÓN
1	23-05-2018	Manuel Gómez Patiño.	Versión inicial
2	18-02-2019	Laura Ruiz Gómez.	Actualización
3	30/03/2021	Omar Villarreal Osorio	Actualización
4	23/12/2021	Omar Villarreal Osorio	Actualización