OFICINA DE CONTROL INTERNO

CLASE DE AUDITORÍA: INTERNA DE GESTIÓN

CLASE DE INFORME: DEFINITIVO

AUDITORÍA AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - MSPI

NÚMERO DE EXPEDIENTE SGD: 288/2023/EV

JEFE OFICINA CONTROL INTERNO:	DIEGO ESTEBAN ORTIZ DELGADO
AUDITOR:	HONORIO RIVERA CORTÉS
MODALIDAD DE LA AUDITORÍA:	VIRTUAL
FECHA DEL INFORME:	27 DE OCTUBRE DEL 2023

TABLA DE CONTENIDO

Pág.

1. OBJETIVOS DE LA AUDITORÍA

1.1 Objetivo General

Evaluar la implementación del Modelo de Seguridad y Privacidad de la Información MSPI, de acuerdo a los lineamientos de la Estrategia de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones Mintic y la norma NTC ISO / 27001:2013 en la PGN.
.

1.2 Objetivos Específicos

Para la evaluación de la implementación del MSPI se tendrá en cuenta aspectos contenidos en las siguientes guías establecidas por Mintic.

- G7 Guía de Gestión de Riesgos.
- G9 Guía de indicadores de Gestión para la seguridad de la información.
- G10 Guía para la preparación de las TIC para la continuidad del negocio.
- G12 Seguridad en la Nube.
- G20 Guía de Transición del IPv4 a IPv6 para Colombia
- G21 Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.

De igual forma aspectos contenidos en:

- Norma NTC-ISO/IEC 27001:2013
- Política de seguridad de la información de la PGN
- Resolución 036 de 2009

2. ALCANCE DE LA AUDITORÍA

Evaluar la gestión realizada en la implementación del Modelo de Seguridad y Privacidad de la información, por parte de la Oficina de Tecnología Innovación y Transformación Digital y la Oficina de Planeación durante el periodo comprendido entre el 1 de enero de 2022 y el 30 de septiembre de 2023.

3. CRITERIOS DE AUDITORÍA

Está auditoría interna de gestión se realizó con fundamento en:

- Artículos Nos. 209 y 269 de la Constitución Política de 1991.

- Ley No. 87 del 29 de noviembre de 1993 Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.

- Las funciones señaladas en los numerales 3 y 4, artículo 13, Decreto-Ley No.262 del 22 de febrero de 2000.

- El Modelo Estándar de Control Interno MECI, adoptado por la Entidad mediante Resolución No. 861 del 10 de septiembre de 2019.

- Resolución 910 de 2019, por medio de la cual se adopta la Política de Seguridad de la Información de la Procuraduría General de la Nación.

- Resolución 124 de 2020 por la cual se adopta el Modelo Integrado de Planeación y Gestión de la Procuraduría General de la Nación –MIPGN, y se establece su estructura de implementación y operación.

- Resolución 500 de 2021 por la cual se establecen los lineamientos y estándares para la estrategia de la seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

- Decreto 1078 de 2015 Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Mapa de Riesgos de Seguridad Digital de la PGN vigencias 2022 y 2023.

- Decreto No.1851 del 24 de diciembre de 2021 “Por el cual se modifican los Decretos Ley 262 y 265 de 2000 con el fin de reconfigurar la planta de personal de la Procuraduría General de la Nación, modificar el régimen de competencias internas, crear, fusionar cargos y determinar los funcionarios que los ocupaban a donde pasarán a ocupar los nuevos cargos que se creen, así como la reasignación o cambio de la estructura de funcionamiento y asignación de las diferentes funciones y cargos de los empleados y se dictan otras disposiciones”.

- Norma NTC-ISO/IEC 27001:2013

- Resolución 036 de 2009, Por medio de la cual se adopta el Sistema de Gestión de la Seguridad de la Información -SGSI - de la Procuraduría General de la Nación

- Plan Operativo Anual 2023 de la Oficina de Control Interno.

  Procesos, procedimientos y demás normas relacionadas con el MSPI.

4. RESULTADOS

4.1 Sistema de Gestión de Seguridad de la Información.

El SGSI de la Procuraduría General de la Nación fue adoptado mediante la resolución 036 del 18 de febrero de 2009, como herramienta de gestión para implementar y mantener la Política de Seguridad de la Información.

4.2 Políticas de Seguridad de la Información.

Las Políticas de Seguridad de la Información fueron adaptadas en la Procuraduría General de la Nación, mediante la resolución número 910 del 25 de septiembre de 2019, con estas buscan la adopción de un conjunto de medidas con las cuales se busca preservar la confidencialidad, integridad y disponibilidad de la información, que son los pilares básicos de la seguridad de la información.

4.3 Plan de Contingencias Logísticas y Emergencias de la PGN.

La Oficina de Planeación realizó la construcción del documento Plan de Contingencias Logísticas y Emergencias de la Procuraduría General de la Nación", cuyo objetivo es mantener la continuidad de las operaciones, ante la ocurrencia de alguna falla que provoque la paralización parcial o total de la Entidad. Este documento define también, el Plan de Recuperación de Desastres–DRP, basado en la norma ISO/IEC 24762, orientada a la recuperación de desastres, alineado con la norma ISO/IEC 22301, encaminada a la continuidad de negocio y con el Modelo de Seguridad y privacidad de la información – MSPI.

4.4 Plan de Recuperación de Desastres o Plan de Continuidad de TI.

La Oficina de Tecnología, Innovación y Transformación Digital construyo un documento el cual se actualiza cada vigencia, cuya última versión 3.0 se encuentra a 1 de septiembre de 2023, en el cual se documenta como recuperar las capacidades de tecnología y telecomunicaciones cuando se presenta una interrupción, el cual se debe armonizar con el Plan de Continuidad del Negocio de la Entidad.

4.5 Indicadores de Gestión del MSPI

Los indicadores de gestión su objetivo principal es la medición de la efectividad, eficiencia y eficacia de los componentes de implementación y gestión estipulados en el modelo de operación del marco de seguridad y privacidad de la información. Los cuales se constituyen en una herramienta de mejora continua, permitiendo tomar con sus resultados mejores decisiones.

La Oficina de Tecnología, Innovación y Transformación Digital de forma proactiva ha realizado la formulación de algunos indicadores, los cuales algunos de ellos se encuentran de igual forma propuestos en la guía de indicadores de gestión para la seguridad de la información de Mintic de la siguiente manera:

1. Organización de la seguridad de la información
2. Cubrimiento de Sistema de Gestión de Seguridad de la Información en activos de información
3. Tratamiento de eventos relacionados en el marco de Seguridad y Privacidad de la Información
4. Plan de sensibilización
5. Revisión de Políticas
6. Ejecución de Plan de mejoras
7. Aprendizajes de Incidentes
8. Ingeniería Social
9. Controles Físicos
10. Protección contra código malicioso

4.6 Pruebas de Vulnerabilidad a la Infraestructura Tecnológica

La Oficina de Tecnología, Innovación y Transformación Digital realizó pruebas para detectar vulnerabilidades a la plataforma de gestión de identidades, verificando las tecnologías utilizadas en el mismo, y de acuerdo a las vulnerabilidades detectadas se trató de explotar esos fallos de seguridad analizando el comportamiento de la plataforma.

De igual forma se realizó, pruebas para detectar vulnerabilidades a las plataformas de Regalias y del SIM, dando las respectivas recomendaciones para corregir las situaciones detectadas.

4.7 Centro Alterno de Datos

La entidad cuenta con un Centro de Datos alterno el cual se encuentra en Azure[1] y sirve como sitio de recuperación ante desastres.

En este centro de datos se encuentran alojados sistemas y servicios como:

1) Sigdea

[1] **Microsoft Azure** (anteriormente *Windows Azure* y *Azure Services Platform*) es una plataforma de computación en la nube creado por Microsoft para construir, probar, desplegar y administrar aplicaciones y servicios mediante el uso de sus centros de datos. Proporciona software como servicio (SaaS), plataforma como servicio (PaaS) e infraestructura como servicio (IaaS) y es compatible con muchos lenguajes, herramientas y marcos de programación diferentes, incluidos software y sistemas específicos de Microsoft y de terceros. Fuente: https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-azure/?cdn=disable

2) SIM
3) Hominis
4) SIAF

El modelo de operación del centro de datos alterno es asincrónico, por lo tanto, en caso de un desastre, aunque la replicación es asincrónica con tiempos replicación cortos, se requiere subir los servicios de manera manual.

Actualmente, la entidad se encuentra en proceso de contratación del licenciamiento necesario para automatizar el proceso ante un evento crítico.

De igual forma se cuenta con un centro de datos de nube privada, el cual está ubicado a las afueras de Bogotá y aloja servicios como:

1) Next Generation Firewall en Alta Disponibilidad
2) Balanceador de Cargas en Ata Disponibilidad
3) Correlacionador de eventos.
4) SIM
5) Sigdea
6) SIAF, Controlador de dominio
7) Almacenamiento Hitachi
8) Respaldo CommVault
9) Custodia y transporte de medios magnéticos
10) Canales de datos para acceso de todo el país a los servicios internos
11) Canal de internet para conexión con Azure
12) Servicios de administración y soporte en horario no hábil para todas las plataformas de la entidad.

Centro de Datos Azure, el cual cuenta con cuatro inquilinos para el IEMP, Regalías, Oficina de Tecnología, Oficina de Planeación y UGII.

Dentro de los sistemas en esta nube alojados se encuentran:

1) Insap
2) Cas Virtual
3) Hominis
4) Intranet
5) Página Web
6) Dokus

Centro de Datos propio, el cual está ubicado en las instalaciones de la entidad y cuenta con algunos servicios en producción como:

1) Uno de los controladores de dominio
2) Next Generation Firewall[2] en Alta Disponibilidad
3) Sandbox[3].
4) Reporteador de eventos de seguridad.
5) Switchs de Core[4].
6) Servicios de Telefonía
7) Servicios de conectividad (Datos e internet).

4.7.1 RTO (Tiempo Objetivo de Recuperación)

El tiempo objetivo de recuperación ha sido definido para los sistemas de información de la PGN, por parte de los funcionarios de la Oficina de Tecnología y fue definido con base en las entrevistas realizadas con los funcionarios de la entidad.

4.7.2 RPO (Punto Objetivo de Recuperación)

El punto objetivo de recuperación ha sido definido para los sistemas de información de la PGN, por parte de los funcionarios de la Oficina de Tecnología y fue definido con base en a las entrevistas realizadas con los funcionarios de la entidad.

De acuerdo a la elaboración del Plan de Continuidad de Desastres se realizó el siguiente análisis en lo relativo al RTO y RPO en la Procuraduría General de la Nación en la Tabla No.1 de los Procesos Críticos de la PGN y su RPO y RTO.

Tabla No.1 Procesos Críticos en la PGN y su RPO y RTO

Categoría (Función del Negocio)	Proceso Critico (servicios)	RPO	RTO	(días)	Prioridad de Recuperación
Sitio Web Corporativo	Todos	24H	24H	1	1
Sitio Web	Portal INTRANET / intranet	24H	24H	3	3

[2] Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.
Fuente: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html
[3] Un Sandbox en informática o un entorno de pruebas, es una máquina virtual aislada en la que se puede ejecutar código de software potencialmente inseguro sin afectar a los recursos de red o a las aplicaciones locales.
Fuente: https://www.proofpoint.com/es/threat-reference/sandbox.

[4] Los Switches Core son un tipo de conmutador de alta capacidad que generalmente se coloca dentro de la red troncal o núcleo físico de una red.
Fuente:https://www.google.com/search?q=que+es+Switchs+de+Core&rlz=1C1GCEU_esCO1046CO1046&oq=que+es+Switchs+de+Core&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIICAEQABgWGB7SAQk0OTIyajBqMTWoAgCwAgA&sourceid=chrome&ie=UTF-8&bshm=rimc/1

Sistemas de Información	SIM - Sistema de Información Misional (MISIONAL)	12H	12H	1	1
Sistemas de Información	SIRI - Sistema de Información de Registro de Sanciones y Causales de Inhabilidad (MISIONAL)	12H	4H	0,5	1
Sistemas de Información	HOMINIS	24H	72H	1	3
Sistemas de Información	ALFA/ histórico/ Sigdea	24H	72H	3	20
Sistemas de Información	MAPA PGN/histórico	72H	72H	2	15
Sistemas de Información	SIAF - Sistema de Información Administrativa y Financiera (SALIN-SIFIP)	8H	4H	2	9
Sistemas de Información	Total Quality Management (HOJAS DE VIDA) - Sistema TQM	12H	12H	3	6
Sistemas de Información	STRATEGOS (APOYO)	24H	24H	3	8
Sistemas de Información	MIGRACIONES	24H	12H	3	7
Sistemas de Información	SIGDEA PORTAL EMPLEADO	4H	1H	1	1
Sistemas de Información	SIGDEA SEDE ELECTRONICA	4H	1H	1	1
Sistemas de Información	SICN - Sistema de Indicadores de Cumplimiento Normativo /histórico	24H	12H	3	15
Sistemas de Información	ITA	24H	24H	3	10
Sistema Documental	Guías disciplinarias, Intervención y preventiva	48H	48H	4	20

Sistemas de Información	Plataforma Moodle/sin uso	48H	48H	4	20
Sistemas de Información	Seguimiento al plan de vacunación, (SERVICIOS DE ANALITICA - UGII)/ histórico Covid	72H	72H	72H	16
Sistemas de Información	Aranda (Mesa de Servicios)	24H	12H	3	17
Sistemas de Información	INSAP/ausencias - permisos	24H	12H	3	18
Sitio Web	Portal INTRANET	24H	24H	3	3
Servidores	Servidor HP (2 Enclosure Sinergy) 01 + 6 Blades	2H	4H	1	1
Servidores	Servidor HP (2 Enclosure Synergy) 02+ 7 blades	24H	12H	3	20
Servidores	HP Simplivity 4 nodos de Hyper convergencia	4H	8H	2	9
Servidores	Servidor DELL	2H	4H	1	6
Servidores	Servidor CommServ	24H	24H	2	8
Servidores	Media Agent -1	2H	4H	1	7
Servidores	Media Agent -2	24H	12H	2	1
Switches	Swich Core 1	48H	12H	2	8
Switches	Swich Core 2	48H	12H	2	6
Switches	Swich Distribución	48H	12H	2	7
Switches	Swich Acceso	48H	12H	2	3
Access Points	Puntos de Acceso Wireless	48H	12H	2	2
Pasarelas	Gateways para comunicación con PSTN	24H	12H	2	2
	Codecs de Videoconferencia	48H	12H	2	8
Appliance VoIP	Stack Avaya (Comunicaciones Unificadas)	48H	12H	3	5

Fuente: Plan de recuperación de desastres - DRP v3+.pdf, elaborado por la Oficina de Tecnología Innovación y Transformación Digital

4.8 Modelo de Gestión de Incidentes de Seguridad de la Información.

La Oficina de Tecnología, Innovación y Transformación Digital, elaboro un documento denominado Plan de Clasificación y Gestión de Incidentes de Seguridad versión 1.1 de fecha mayo de 2022, y actualizado al 8 de agosto de 2022, este plan describe los procesos de

planificación, preparación, clasificación, detección, análisis, contención, erradicación y recuperación junto con las actividades post-incidente que hacen parte de la gestión de incidentes de ciberseguridad que puedan afectar a los servicios desplegados sobre la infraestructura de la PGN, con este se busca que la entidad esté preparada para identificar eventos y detectar incidentes de seguridad que podrían interrumpir la operación de los servicios o impactar la integridad y/o confidencialidad de los activos de información; como también contar con la capacidad necesaria para responder de forma adecuada a la materialización de las amenazas y aprender de los incidentes que se han podido presentar en la Entidad.

Adicionado al anterior documento se diseñó el formato reportes de incidentes.

4.9 Procedimientos de seguridad de la información

La Oficina de Tecnología, Innovación y Transformación Digital ha construido tres procedimientos para el efecto de la siguiente forma:

Procedimiento de Notificación de Eventos de Seguridad; cuya última actualización se encuentra a 11 de septiembre de 2023, en el que se describe el siguiente objetivo: Definir los lineamientos referentes al reporte de eventos de seguridad de la información al personal encargado de la gestión de eventos e incidentes de seguridad de la entidad, con el fin de identificar y contener a tiempo cualquier situación que pueda afectar la confidencialidad, integridad y/o disponibilidad de la información de la Entidad.

Procedimiento para la destrucción de medios de almacenamiento; cuya última actualización se encuentra a 12 de abril de 2023, en el que se describe el siguiente objetivo: Definir los lineamientos para la destrucción de información y los métodos de borrado seguro que deben emplearse para que garantizan la confidencialidad de la información de la Entidad.

Procedimiento para la identificación y clasificación de activos de información; cuya última actualización se encuentra a 13 de septiembre de 2023, en el que se describe el siguiente objetivo: Establecer las actividades necesarias para la identificación y clasificación de los activos de información de la Procuraduría General de la Nación.

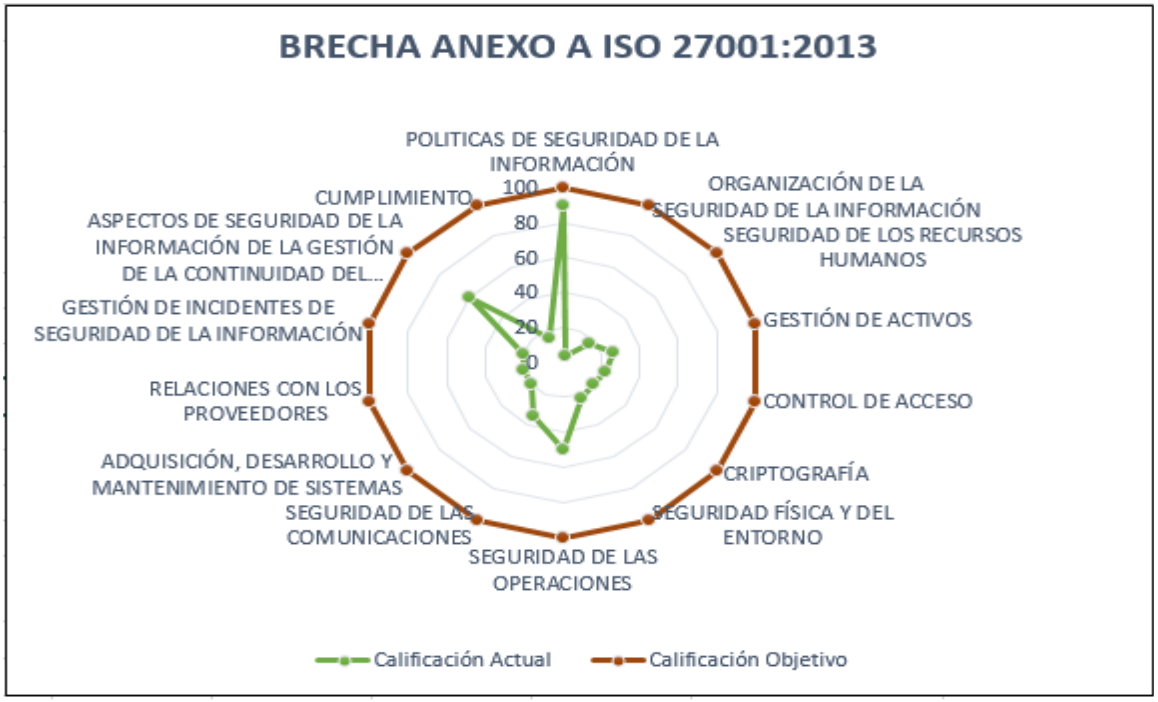
4.10 Diagnostico del Modelo de Seguridad y Privacidad de la Información.

La Oficina de Tecnología, Innovación y Transformación Digital se encuentra en construcción de un documento denominado análisis de brechas de la seguridad y privacidad de la información, el cual se encuentra fechado a agosto de 2023, en el que se describe el siguiente objetivo: El objetivo del presente documento es presentar el estado actual de la postura de la seguridad y privacidad de la información de la Procuraduría General de la Nación, con el fin de mejorar la seguridad de los activos de información a la vez que se cumple con los lineamientos

de la Política de Gobierno Digital. El análisis de brecha se basó en la documentación obtenida de parte de varios funcionarios de la entidad, junto con entrevistas y el diligenciamiento del Instrumento de evaluación del MSPI propuesto por el Ministerio de las TIC.

Este documento sugiere el uso los controles del Anexo A de la Norma ISO 27001:2013 para reducir los diferentes riesgos a los que están expuesto los activos de información de las Entidades. Partiendo de esta consideración, se realizó la identificación de la brecha entre los controles de los dominios del Anexo A y los implementados en la Entidad. De cual se desprende el resultado que se aprecia en la Grafica No. 1

Grafica No. 1 Brecha Anexo a ISO 27001:2013



Fuente: Informe GAP Análisis - En construcción.pdf elaborado por la Oficina de Tecnología e Innovación Digital

De acuerdo con el análisis efectuado en el documento se concluye oportunidades de mejora en varios de los controles, el que más se encuentra desarrollado es el que corresponde a las políticas de seguridad de la información.

De acuerdo con el ciclo del modelo PHVA, el documento arroja el resultado dado en la gráfica No. 2.

Grafica No. 2 Brecha Anexo a ISO 27001:2013

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2020	Planificación	40%	40%
	Implementación	15%	20%
	Evaluación de desempeño	2%	20%
	Mejora continua	0%	20%
TOTAL		57%	100%

Fuente: Informe GAP Análisis - En construcción.pdf elaborado por la Oficina de Tecnología e Innovación Digital

El documento concluye que la PGN muestra avances solo en la fase de planificación.

Dentro de las conclusiones elaboradas en el documento elaborado por la Oficina de Tecnología Innovación y Transformación Digital se encuentra las siguientes:

Se cuenta con el cuerpo normativo de las políticas de seguridad de la Información que incluye: políticas generales y políticas específicas aprobadas por la Entidad.

Se evidencia la realización de la clasificación de activos, del análisis de riesgos y la construcción de varios instrumentos de apoyo.

Se evidencia la realización del inventario de activos de información y su clasificación, al igual que el análisis de riesgos para los mismos.

La Entidad cuenta con un plan de recuperación de desastres –DRP, pero los planes no han sido probados.

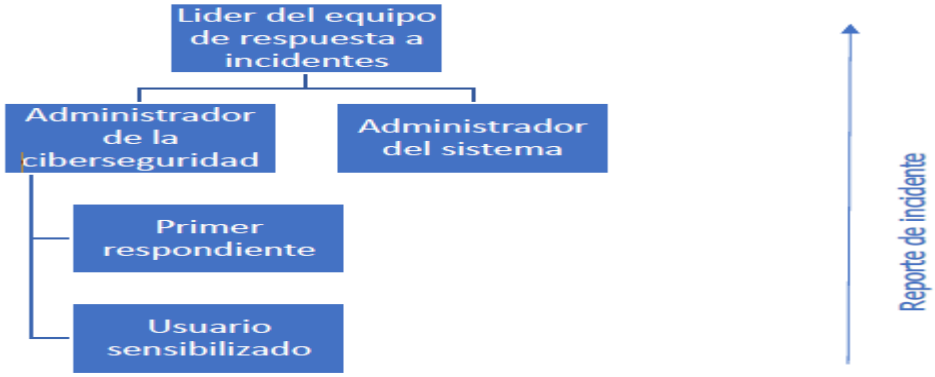
Aunque se cuenta con un plan básico de respuesta a incidentes de seguridad de la información, este no ha sido socializado ni probado.

4.11 Roles y Perfiles para la atención de Incidentes de Seguridad

La Oficina de Tecnología, Innovación y Transformación Digital realizó, mediante el documento, denominado Plan de Clasificación y Gestión de Incidentes de Seguridad, realizo un análisis de los roles y responsabilidades que pueden desempeñar diferentes funcionarios, en las diferentes etapas.

Entre ellos se definieron los roles que se detallan en la Figura 1.

Figura 1 Roles para la Atención de Incidentes de Seguridad



Fuente: Plan de Clasificación y Gestión de Incidentes de Seguridad.pdf Elaborado por la Oficina de Tecnología e Innovación Digital

4.12 Mapa de Riesgos de Seguridad Digital

La Oficina de Tecnología, Innovación y Transformación Digital realizó la construcción de mapa de Riesgos de la Seguridad Digital, en los cuales se incluyó el macroproceso Estratégico, el proceso de Tecnologías de la Información, y se contempló los subprocesos de: Soporte al Usuario, Administración Infraestructura Tecnológica, Administración Técnica de los Sistemas de Información.

4.13 Plan de Implementación del IPV6

La Oficina de Tecnología, Innovación y Transformación Digital celebro el contrato 134 de 2022, por medio del cual realizo la fase uno (1) correspondiente al diagnóstico y etapa preliminar con el diseño del proceso de transición a IPV6.

Se informa que las fases de implementación, pruebas y post- migración, están en proceso de contratación y se espera estar ejecutada para el 31 de diciembre de 2023.

4.14 Actividades de sensibilización desplegadas por la Oficina de Tecnología

Con estas actividades se busca implantar lineamientos para la construcción y mantenimiento del plan de capacitación, sensibilización y comunicación de la seguridad de la información, para así asegurar que este, cobije en su totalidad los funcionarios de la Entidad, asegurando que cada uno desempeñe sus roles y responsabilidades de seguridad y privacidad de la información dentro de la entidad.

La Oficina de Tecnología, Innovación y Transformación Digital ha venido realizando diferentes campañas, dentro de las cuales se encuentran: Plan de Comunicaciones, Capacitación y

Sensibilización del Personal, Boletines de Ciberseguridad y piezas graficas cuyos temas son el gestor de identidades, seguridad informática, Tips de Seguridad (hackeo entidades), doble factor de autenticidad, entre otros temas.

5. CONCLUSIONES

La Oficina de Control Interno, en cumplimiento al Plan de Acción 2023, ejecutó esta auditoría al Modelo de Seguridad y Privacidad de la Información - MSPI, para dar a conocer, mediante la evaluación independiente, el estado de la implementación del modelo en la PGN, la identificación y administración de los riesgos, e indicadores entre otros temas, con el fin de coadyuvar al mejoramiento continuo de los procesos para el cumplimiento de los objetivos institucionales.

Se evidencia que persisten las debilidades relacionadas con la operación del Comité de Seguridad de la Información establecido en el artículo octavo de la Resolución No. 036 de 2009[5]; y, con la designación y cumplimiento de funciones del Oficial de Seguridad determinadas en los artículos tercero y cuarto de la misma Resolución. Situaciones que merman el adecuado funcionamiento del Sistema.

6. RECOMENDACIONES

1. La Seguridad de la Información es un tema totalmente vigente y hace parte de los habilitadores transversales de la Política de Gobierno Digital establecida por el Decreto No. 1008 de 2018 y a la que hace referencia el Modelo Integrado de Planeación y Gestión - MIPG. Además, la Procuraduría General de la Nación adoptó el Modelo MIPGN, mediante la Resolución No. 124 de 2020[6], en donde, en el Anexo Técnico, recomienda tener en cuenta dicha Política, así como también la de Seguridad Digital, las cuales se pueden materializar, en lo que compete a la Seguridad de la Información, con una adecuada implementación del SGSI.

   Por lo anterior, se recomienda revisar la Resolución No. 036 de 2009 y realizar ajustes que permitan el cabal cumplimiento de los lineamientos, considerando lo siguiente:

   - Revisar el artículo tercero Oficial de Seguridad de la Información. Analizar las causas que han llevado a que no se haya realizado la designación y efectuar los ajustes a que haya lugar.

   - Revisar el artículo cuarto Funciones Generales del Oficial de Seguridad de la

[5] Por medio de la cual se adopta el Sistema de Gestión de la Seguridad de la Información -SGSI - de la Procuraduría General de la Nación.

[6] Por la cual se adopta el Modelo Integrado de Planeación y Gestión de la Procuraduría General de la Nación - MIPGN, y se establece su estructura de implementación y operación.

Información. Ajustar, de forma que las funciones sean realizables por una persona o, en su defecto, considerar conformar un equipo de trabajo, que pueda cumplir con las 15 actividades que actualmente están establecidas para este cargo.

- Revisar los artículos quinto, sexto y séptimo relacionados con el Comité de Seguridad de la Información. Analizar la pertinencia de la existencia de este o si se debe ajustar.

2. Presentar ante el Comité de Gestión y Desempeño, el Plan de Contingencias Logísticas y Emergencias de la PGN, para su aprobación, ejecución de pruebas, realizar la articulación con el Plan de recuperación de desastres o plan de continuidad de TI y realizar las capacitaciones a que haya lugar.

3. Presentar ante el Comité de Gestión y Desempeño, el Plan de Recuperación de desastres o Plan de Continuidad de TI, para su aprobación y realización de pruebas.

4. Continuar realizando las pruebas de vulnerabilidades a la infraestructura tecnológica, de acuerdo a un plan que se estipule para este efecto, y realizar las recomendaciones que se deriven de este ejercicio.

5. Continuar con el proceso de contratación con el objetivo de obtener el licenciamiento necesario para automatizar el proceso de subida de los servicios, del Centro de Datos Alterno.

6. Continuar con la ejecución de los procesos que permitan la implementación del IPV6 en la Procuraduría General de la Nación.

Teniendo en cuenta algunas de las recomendaciones anteriores, y por considerarlo de su interés, el presente informe se remite a la alta dirección de la Entidad.

HONORIO RIVERA CORTÉS
Funcionario de Control interno

Vo.Bo.

DIEGO ESTEBAN ORTIZ DELGADO
Jefe Oficina de Control Interno