MINISTERIO DE DEFENSA NACIONAL

FONDO ROTATORIO DE LA POLICÍA

SEGUIMIENTO IMPLEMENTACIÓN DE SEGURIDAD EN LA WEB
OFICINA DE CONTROL INTERNO

Bogotá, D.C. 2021 /12/31

Elaboró:	Revisó:	Aprobó:
Sandra A. Blanco G. **Prof. Admin. Sistemas** **Auditora**	**Omar Antonio Pereira Góez** **Economista** **Jefe de la Of. de Control Interno**	**Omar Antonio Pereira Góez** **Economista** **Jefe de la Of. de Control Interno**

TABLA DE CONTENIDO

Introducción

La proyección de la transformación digital de productos y servicios prestados por la entidades, traen consigo la necesidad de implementación y adopción de buenas prácticas, que garanticen la seguridad en la web.

El Congreso de la República a través de la Ley 1712 de 2014 regularizó el derecho de acceso a la información pública, así mismo, en el parágrafo del artículo 16 del decreto 2106 de 2019 del DAFP, se dictaron normas para simplificar, suprimir, reformar trámites, procesos y procedimientos, para lo cual las entidades deben disponer de una estrategia de seguridad digital siguiendo los lineamientos emitidos por el Ministerio de tecnologías a través del Modelo de Seguridad y privacidad de la Información – MSPI, la guía de gestión de riesgos de seguridad de la información y los estándares para la estrategia de seguridad digital.

Las políticas, procesos, procedimientos, guías, manuales y formatos generados por la entidad, deben garantizar el cumplimiento del ciclo PHVA, adoptando medidas eficientes de seguridad digital y gestión de incidentes, alineadas al Modelo de Seguridad de la información y al Modelo de Gestión de riesgos de Seguridad Digital, el cual tiene por objetivo “brindar un marco de gestión de riesgos de seguridad digital en el cual se identifiquen las amenazas y vulnerabilidades a las que una entidad pueda estar expuesta al momento de llevar a cabo actividades socio económicas en el entorno digital”.

A través de la resolución 1519 de 2020 generada por el Ministerio de Tecnologías, se establecieron las condiciones técnicas mínimas y de Seguridad Digital, que deben ser adoptadas por las entidades, con plazos de cumplimiento así:

Resolución 1519 de 24 de agosto de 2020 del Ministerio de Tecnologías y las Comunicaciones			
Artículo	**Título**	**Cumplimiento**	**Fecha de cumplimiento**
3	Directrices de accesibilidad web	AA de la Guía de Accesibilidad de Contenidos Web (Web Content Accesibillity Guidelines - WCAG) en la versión 2.1, expedida por el World Web Consortium (W3C)	Enero 1 de 2022
		Anexo 1 de la presente resolución aplicable en todos los procesos de actualización, estructuración, reestructuración, diseño, rediseño de sus portales web y sedes electrónicas, así como de los contenidos existentes en ésas	
4	Estándares de publicación y divulgación de contenidos e información	Dar cumplimiento a los estándares de publicación y divulgación de contenidos e información aplicable a sus sitios web y sede electrónica, establecidos en el Anexo 2 de la presente resolución.	Abril 1 de 2021
		Desarrollar el formulario electrónico para PQRSD, requisitos generales y campos mínimos que se señalen en el Anexo 2 de la presente resolución	
5	Información digital archivada	Garantizar condiciones de conservación y/o archivo para posterior consulta, de la documentación digital disponible en sitios web, conforme con las Tablas de Retención Documental aprobadas acorde con los lineamientos del Archivo General de la Nación.	
6	Condiciones mínimas técnicas y de seguridad digital	Los sujetos obligados deberán observar las condiciones mínimas técnicas y de seguridad digital que se definen en el Anexo 3 de la presente resolución.	
7	Condiciones mínimas de publicación de datos abiertos	Los sujetos obligados deberán publicar sus datos abiertos y federarlos al Portal Datos Abiertos del Estado colombiano -datos.gov.coconforme con las directrices referidas en el Anexo 4 de la presente resolución.	

Este seguimiento se realiza específicamente al cumplimiento del artículo 6 – anexo 3 de la resolución 1519 de 2020.

1. Objetivo

Realizar el seguimiento y verificación de las actividades ejecutadas en la entidad en función del cumplimiento de seguridad en la web, establecida por el Ministerio de Tecnologías de la Información y las comunicaciones.

2. Contenido del Informe

2.1. Alcance

Este documento contiene el seguimiento a las actividades realizadas por el Fondo Rotatorio de la Policía Nacional, al corte del mes de diciembre de 2021, con respeto al cumplimiento de los lineamientos para la publicación y divulgación de la información pública, establecida en la ley 1712 de 2014, el cumplimiento de la implementación de los criterios de estandarización de contenidos e información, accesibilidad web, seguridad digital, datos abiertos y formulario electrónico para PQRSD, establecidos en la resolución 1519 de 2020; así como el avance de la implementación de la seguridad digital, establecida en la resolución 500 del 10 de marzo de 2021.

2.2. Marco Legal

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.

La Resolución 001519 del 24 de agosto de 2020 – Por la cual se definen los estándares y directrices para publicar la información señalada en la ley 1712 del 2014 y se definen los requisitos materia de acceso a la información publicada, accesibilidad web, seguridad digital, y datos abiertos.

La Resolución 00500 de 2021 – Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

El decreto 2106 de 2019 - Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.

Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.

Guía para la Administración de Riesgos y el Diseño de Controles en Entidades Públicas - en su anexo 4 denominado “Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas”.

3. Resultados de la verificación

De acuerdo al lineamiento del MSPI es importante que la entidad revise y/o complemente los siguientes temas:

3.1. Proceso de Valoración de Riesgos de Seguridad de la Información

- Identificación de riesgos de seguridad de la información física y electrónica, que puedan generar perdida de confidencialidad, integridad, disponibilidad, privacidad de la información,
- Identificación de riesgos relacionados con continuidad de la operación de la Entidad.
- Identificación de los dueños de los riesgos
- Definición de los criterios para la valoración de las consecuencias de la materialización de los riesgos y la probabilidad de su ocurrencia
- Determinación del apetito de riesgo de la entidad
- Definición de los criterios de aceptación de los riesgos
- Priorización de los riesgos para su tratamiento

3.2. Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información

- Articulación con las dependencias de la entidad, los roles y responsabilidades, para el cumplimiento de la seguridad de la información
- Presentación dentro del comité de Gestión y Desempeño el monitoreo y reporte de seguimiento del cumplimiento de cada una de las responsabilidades de seguridad de la información, de las diferentes dependencias de la entidad.
- Asignación al responsable de Seguridad de la Información a un área estratégica de la entidad, que no sea el grupo de telemática.
- Inclusión como miembro del comité de gestión institucional con voz y voto y en el comité de control interno con voz
- Validación de las Funciones del Responsable de Seguridad de la Información para la entidad. Adicionalmente a liderar la implementación del Modelo de Seguridad y Privacidad de la Información de la Entidad, debe velar por el cumplimiento de:
    - Fomentar la implementación de la Política de Gobierno Digital
    - Asesorar a la Entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y privacidad de la Información para la entidad de conformidad con la regulación vigente.
    - Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación actual de la entidad.
    - Realizar la estimación, planificación y cronograma de la implementación del Modelo de Seguridad y privacidad de la Información.

- Liderar la implementación y hacer seguimiento a las tareas y cronograma definido.
- Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del Modelo de Seguridad y privacidad de la Información.
- Realizar el acompañamiento a los procesos y /o proyectos en materia de seguridad y privacidad de la información.
- Liderar y brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia.
- Proponer la formulación de políticas y lineamientos de seguridad y privacidad de la información.
- Definir e implementar en coordinación con las dependencias de la Entidad, las estrategias de sensibilización y divulgaciones de seguridad y privacidad de la información para servidores públicos y contratistas.
- Apoyar a los procesos de la Entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información.
- Definir, socializar e implementar el procedimiento de Gestión de Incidentes de seguridad de la información en la entidad.
- Efectuar acompañamiento a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en seguridad y privacidad de la información.
- Poner en conocimiento de las dependencias con competencia funcional, cuando se detecten irregularidades, incidentes o prácticas que atentes contra la seguridad y privacidad de la información de acuerdo con la normativa vigente.

3.3. Plan de tratamiento de riesgos de Seguridad de la Información

- Los dueños de los riesgos deben realizar la aprobación formal del plan de tratamiento de riesgos
- Presentar al Comité Institucional y de Desempeño la aprobación del plan de tratamiento de riesgos.

3.4. Competencia, Toma de conciencia y comunicación.

- Asegurar que las personas cuenten con los conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del modelo de seguridad y privacidad de la información.
- Involucrar al 100% de los funcionarios de la entidad en la implementación y gestión del MSPI.

3.5. Planificación e Implementación:

- Documentar por cada proceso responsable, la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos.
- Solicitar al Comité Institucional la aprobación de la planificación e implementación del plan de tratamiento de riesgos.

3.6. Revisión por la Dirección.

- Tratar y aprobar los temas de seguridad y privacidad de la información, seguridad digital y la Política y el Manual de Políticas de Seguridad y Privacidad de la información en el comité institucional de gestión y desempeño, o cuando el director lo determine.

3.7. Mejora.

- Elaborar un plan de mejoramiento continuo que involucre acciones correctivas, optimización de procesos o controles y mejorar el nivel de madurez del Modelo de Seguridad y privacidad de la Información.

5. Conclusiones y/o Recomendaciones

5.1. Conclusiones

El Fondo Rotatorio se encuentra comprometido en certificarse en el Sistema de Gestión de Seguridad de la Información ISO 27001:2013, ha realizado avances en temas relacionados con tecnología, para lograr con la implementación del modelo de seguridad y privacidad de la Información debe enfocar sus esfuerzos en involucrar a todos los responsables del manejo de la información física y digital.

La ley 1519 de 2020 exige el cumplimiento de las condiciones mínimas técnicas de seguridad digital a partir del primero de abril de 2021, teniendo en cuenta que estos plazos ya vencieron, la entidad debe documentar los controles existentes y agilizar en el cumplimiento de los controles que se encuentren en proceso de implementación.

5.2. Recomendaciones

- Formalizar las responsabilidades del oficial de seguridad de la Información, indicadas en el Modelo de Seguridad y privacidad de la información, definido por el Ministerio de Tecnologías de la información y las Comunicaciones
- Se sugiere avanzar en la adopción del Modelo de Seguridad y privacidad de la Información, definido por MinTic en febrero de 2021, el cual es un habilitador transversal de seguridad y privacidad de la información y que además de

apoyar la estrategia de gobierno digital, define la implementación de controles de seguridad físicos y lógicos para la efectiva gestión de los activos de información, infraestructura crítica, riesgos e incidentes de seguridad y privacidad de la información.

- De acuerdo a lo establecido en el MSPI se recomienda que el responsable de seguridad de la información sea independiente, organizacional y técnicamente de la coordinación de telemática.
- Establecer indicadores de medición de la gestión y cumplimiento en el avance de implementación del Modelo de Seguridad y Privacidad de la Información, de acuerdo a la pertinencia, funcionalidad, disponibilidad, confiabilidad y utilidad.
- Implementar la obligatoriedad de acceso a la Forponet con el uso de reCAPTCHA.
- Realizar desconexión automática de la sesión de la Forponet, la cual permanece activa si validación de tiempo de desconexión.
- Exigir validaciones de seguridad relacionadas con el control de la autenticación, definición de roles y privilegios y separación de funciones, tanto en las aplicaciones a la medida existentes como en los nuevas soluciones de software proyectadas para ser adquiridas por la entidad.
- Revisar y eliminar configuraciones y credenciales por defecto, además de deshabilitar métodos *HTTP* peligrosos como *put, delete, trace* y en la medida de lo posible restringir la administración remota.
- Para los nuevos desarrollos exigir la integridad de instrucciones tales como *input*, el paso de parámetros sensibles, uso de *Secure y HttpOnly*.
- Mantener actualizado el software, *frameworks y plugins* de los sitios web.
- Almacenar, proteger y monitorear los log de auditoría
- Revisar y en la medida de posible aplicar las recomendaciones de seguridad de la guía de desarrollo seguro de aplicaciones y Servicios Web Seguros de la *Open Web Application Security Project* (OWASP).
- Controlar el escalamiento de privilegios en los Sistemas Operativos, servidor web y Bases de datos que hacen parte de la infraestructura del portal web.
- Cumplir con la estandarización de código fuente para portales web y adoptar validaciones *HTML y CCS*, siguiendo las buenas prácticas del *W3C (World Web Wide Consortium*).
- Implementar un sistema de control de versiones
- Revisar y gestionar las vulnerabilidades relacionadas con:
    - Cookies
    - Configuraciones por defecto
    - Validaciones relacionadas con caracteres válidos en los datos del front-end
    - Reglas que garantizan la seguridad de las cabeceras del protocolo HTTP.