INFORME DE SEGUIMIENTO MAPAS DE RIESGOS
SEGURIDAD DIGITAL

III CUATRIMESTRE 2022

OFICINA DE CONTROL INTERNO

DICIEMBRE 2022

1. INTRODUCCION

Dando cumplimiento a las funciones propias de la Oficina de Control Interno y al cronograma de auditorías se efectúo seguimiento a la matriz mapas de riesgos de seguridad digital; utilizando herramientas que permitieron recopilar la información sobre la implementación de controles, para evitar la materialización de estos, y evitar consecuencias y efectos no deseados en el cumplimiento de sus objetivos

La Oficina de Control Interno adelanta seguimiento a los Riesgos de seguridad digital, analizando las causas, revisando los riesgos y la efectividad de los controles incorporados en el Mapa de Riesgos de la presente vigencia

2. OBJETIVO GENERAL

Evaluar la correcta identificación, análisis y efectividad de los controles en la gestión de Riesgos de seguridad digital de la FND, con el fin de fortalecer las buenas prácticas de seguridad de la información como son: confidencialidad, integridad y disponibilidad y autenticidad de la información.

2.1 objetivos específicos

1. Verificar la aplicación de los lineamientos del MIPG, componente administración del riesgo y, Guía para la administración del riesgo y el diseño de controles en entidades públicas- Versión 5 de diciembre 2020, generada por el DAFP, capítulo 5 Lineamientos riesgos de seguridad de la información
2. Implementar planes y programas de prevención de los riesgos asociados a los procesos.
3. Evaluar si los controles definidos en la matriz de riesgos de seguridad digital son eficaces y eficientes y si las acciones implementadas por cada proceso para abordar los riesgos son adecuadas para el tratamiento de estos.

3. LÍDER DEL PROCESO

Gerencia de Tecnología - GTE

4. ALCANCE

Verificar el cumplimiento de las acciones establecidas por FND para la definición y tratamiento de los riesgos de seguridad digital para el período comprendido entre septiembre y diciembre del 2022.

5. METODOLOGÍA

El informe de seguimiento se obtiene de la información consolidada y suministrada por la GTE; haciendo especial énfasis en la implementación de controles, incluyendo la revisión, seguimiento y los soportes, el objetivo primordial de la administración de riesgos es crear una cultura de prevención y control.

El enfoque no se fundamenta únicamente en una metodología, sino que se convierte en parte esencial desde la planeación estratégica, debido a que existe la posibilidad de que se presenten eventos y circunstancias internas y externas que pueden afectar el cumplimiento de la misión.

Además, se tuvo en cuenta:

1. Documentos internos, como la política de seguridad de la información, la política de protección de datos
2. Informes de auditorías internas y/o externas.
3. Procedimientos de control interno.
4. Sistemas de información, entre otros.

6. ARTICULACIÓN CON EL MIPG

El seguimiento a los riesgos de seguridad digital de la FND es efectuado, bajo la 7ª Dimensión del Modelo Integrado de Planeación y Gestión, denominada “Control Interno”, que se realiza de conformidad con la actualización del Modelo Estándar de Control Interno- MECI, verificando los controles diseñados , el seguimiento en la evaluación de la política de seguridad digital y de la información, bajo los lineamientos y supervisión de la Alta Dirección y, definir tratamiento, manejo y seguimiento a los riesgos de seguridad digital que afectan el logro de los objetivos institucionales de la entidad, para lo cual la FND debe contar con mecanismos efectivos de evaluación de riesgos, para establecer el nivel de riesgo inherente y residual y diseñar actividades de control relevantes sobre los procesos de gestión de la seguridad, y de adquisición , desarrollo y mantenimiento de tecnologías, que contribuyan a la mitigación de los Riesgos de Seguridad digital, llevarlos a niveles aceptables para la consecución de los objetivos.

7. CRITERIOS DE AUDITORÍA

1. Ley 87 del 2003 “Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.

2. Art. 2 “Objetivos del Sistema de Control Interno. literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Literal f) definir y aplicar medidas para prevenir los riesgos; detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.”.

3. MIPG. Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG - Versión 4 - Marzo Dimensión 7 “Control Interno”

4. Guía para la administración de Riesgos DAFP- versión 5. diciembre 2020 generada por el DAFP, capítulo 5 Lineamientos riesgos de seguridad de la información con el fin de Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación que la FND pueda estar expuesta, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

8. LIMITACIONES

No se presentaron limitaciones para la realización del presente informe

9. EQUIPO AUDITOR

Carolina Navarrete /Clara Consuelo Ovalle

10. DESARROLLO

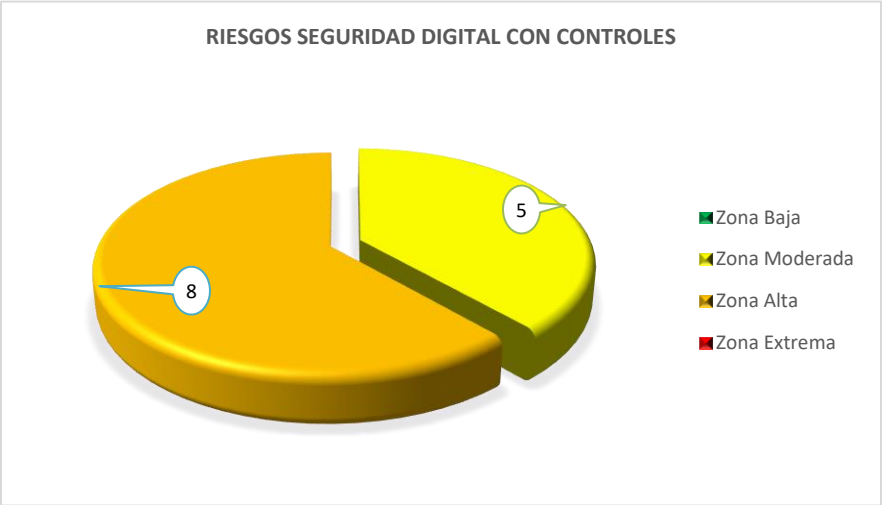
Para este periodo de análisis se formalizó el informe con base al seguimiento de los riesgos de seguridad digital que se efectúa a través de la Matriz de Riesgos III cuatrimestre consolidada 2022, estableciendo.

La Matriz MRSD refleja que la FND, determinó 13 riesgos de Seguridad digital, los cuales se relacionan a continuación. Con el fin de mitigar dichos riesgos la FND desde la GTE implementó treinta y un (31) controles como se relacionan a continuación:

10.1. Avances Matriz de Riesgos de Seguridad Digital

El proceso GTE cuenta con 13 Riesgos de Seguridad Digital, de los cuales ocho (8) se encuentra en zona de riesgos alta y cinco (5) en zona de riesgo moderada con controles. Implementaron 31 controles con el objetivo de disminuir el nivel de riesgo identificado en el proceso; sin embargo, los riesgos tecnológicos siempre van a estar en zonal alta de materialización de estos, por lo que se debe implementar controles aún más robustos y de esta manera blindar a la organización.

Gráfico No. 1. Riesgos Seguridad Digital



Fuente: Matriz de Riesgos de Seguridad Digital

Cuadro No 1. Riesgo Residual con Controles

RIESGOS	*ZONA BAJA*	*ZONA MOEDARADA*	*ZONA ALTA*	*ZONA EXTREMA*	*TOTAL*
Pérdida de bases de datos y fuentes de información			1		1
Ausencia de controles en los sistemas de información		1			1
Manipulación, modificación o alteración sin autorización de la información registrada en los sistemas de la FND			1		1
Errónea gestión de la infraestructura tecnológica de la FND		1			1
No cumplir con los lineamientos del Modelo de Seguridad y Privacidad de la Información y de las Políticas Gobierno Digital			1		1
No disponibilidad de los sistemas tecnológicos y los de información.		1			1
Insuficiencias operativas de software			1		1
Ataques Cibernéticos			1		1
Acceso a cuentas de correo FND		1			1
Perdida de equipos informáticos			1		1
Brechas de seguridad informática			1		1
Acceso a información no autorizada		1			1
Información errónea en sistemas de información			1		1
TOTAL	***0***	***5***	***8***	***0***	***13***

Fuente: Matriz de Riesgos de Seguridad Digital

Cuadro No 2. Controles Existentes

No.	*CONTROLES ESTABLECIDOS*
1	Copias de seguridad alojadas en Drive
2	Capacitaciones realizadas en las herramientas disponibles DE GOOGLE en la FND

3	Claves únicas para trabajadores. Manejo de información por áreas o procesos.
4	Actualizaciones y cambios periódicos de contraseñas
5	Cambios periódicos de contraseñas
6	Capacitar a los funcionarios para la solicitud de requerimientos
7	Actualización y mantenimiento de las herramientas.
8	Mantenimiento de los activos de la FND y proveedores
9	Ejecución al plan de trabajo de la Política digital
10	Entrega de informes y porcentaje de avances
11	Creación del PETI.
12	Plan de tratamiento de riesgos de seguridad digital.
13	Listado de activos físicos de tecnología
14	Listado de inventario intangible (Sistemas de Información)
15	Controles de fechas de terminación de contratos y acuerdos de Niveles de Servicios (ANS).
16	Aplicación de acuerdos de Niveles de Servicios (ANS)
17	Bitácora de sistemas de información de la FND con sus respectivos tiempos de vigencias.
18	Programación de actividades de renovación con sistema de alarmas
19	Constituir nuevas políticas de trabajo y políticas de seguridad digital (incluyendo modalidad de trabajo en casa).
20	Control centralizado de equipos informáticos.
21	Copias de seguridad alojadas en Drive
22	Equipos protegidos a partir de Antivirus
23	Eliminación de cuentas de correos electrónicos.
24	Backups de cuentas de correos electrónicos.
25	Listado de activos físicos de tecnología
26	Correos de asignación de equipos
27	Implementar políticas de seguridad de la información que aseguren la integridad de los sistemas de información de la FND
28	Cambios periódicos de contraseñas
29	Capacitar a los funcionarios para la solicitud de requerimientos
30	Acceso a funcionarios a sistemas de información mínimos necesarios.
31	*Backups de información para poder restaurar datos en caso de materialización del riesgo*

Fuente: Matriz de Riesgos de Seguridad Digital

11. RECOMENDACIONES

1. *Incluir en la matriz de riesgos de Seguridad Digital los siguientes riesgos:*

ITEM	***RIESGOS***
1	Los contratistas trabajan con equipos propios, los cuales no tienen ningún tipo de restricción y se conectan a la red de Federación, evidenciando el riesgo de pérdida de la información y teniendo como consecuencia impacto en la imagen reputacional.
2	Los contratistas no tienen correo con dominio de FND, evidenciando como riesgo pérdida de información y como consecuencia impacto en la imagen reputacional.
3	No se cumple con la infraestructura necesaria para los data center y áreas seguras, evidenciando el riesgo de no garantizar la seguridad de la información contenida y teniendo como consecuencia impacto económico en la organización.
4	No tienen segregadas las redes, por lo tanto, los invitados también se pueden conectar a la red de Federación, evidenciando el riesgo de hacking de la información y teniendo como consecuencia impacto en la imagen reputacional.
5	No se han definido claramente los mecanismos de redundancia para los equipos críticos con los proveedores, evidenciando como riesgo pérdida de la información o demora en los servicios si hay incidentes críticos, teniendo como consecuencia impacto económico en la organización.

6	No se han definido con los proveedores claramente los requisitos de seguridad requeridos para la prestación de los servicios, evidenciando el riesgo de pérdida de la información y teniendo como consecuencia impacto económico en la organización.

2. *Realizar por parte del área de GTE mesas de trabajo con las dependencias con el fin de identificar riesgos de seguridad de la información propios de cada proceso.*

3. *Generar y/o robustecer y/o fortalecer los mecanismos de seguridad que existen por parte de la Gerencia de tecnología con el fin de identificar, analizar, valorar y tratar los riesgos, amenazas y vulnerabilidades del entorno digital y, que constituyan las herramientas para la protección del sistema, apoyándose en las normas internas en seguridad digital con que cuenta la Institución. (prevención, detección, recuperación).*

12. CONCLUSION

Del seguimiento efectuado al mapa de riesgos de seguridad digital de la entidad, se concluye que para el III Cuatrimestre 2022, no se materializó ningún riesgo; sin embargo, es importante tener en cuenta por parte del responsable de GTE, la incorporación de nuevos mecanismos de control y proponer estrategias para la ejecución de planes de acción para mitigar los riesgos generados en el entorno digital, que se encuentran en ***nivel de riesgo alto y extremo****.*

Atentamente

CLARA CONSUELO OVALLE JIMÉNEZ
Jefe Oficina Control Interno

Elaboro:	Revisó:	Aprobó
Carolina Navarrete/Clara Ovalle	Clara Ovalle Jiménez	Clara Ovalle Jiménez
Fecha: Diciembre 2022	Fecha: Diciembre 2022	Fecha: Diciembre 2022