INFORME DE SEGUIMIENTO MAPAS DE RIESGOS
SEGURIDAD DIGITAL

I CUATRIMESTRE 2021

OFICINA DE CONTROL INTERNO

BOGOTA, MAYO 2021

TABLA DE CONTENIDO

- **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 el Gobierno Nacional a través del Ministerio de las Tics, generó la política de Seguridad Digital, la cual impulsa a la generación de confianza en el entorno digital y mejorar; por lo tanto su uso , busca incrementar que las Entidades se vean obligadas a tener una adecuada gestión sobre los riesgos de seguridad digital, para evitar la materialización de los mismos y evitar consecuencias y efectos no deseados tanto económicos como sociales para el país y para la Organización.

Así mismo, la FND debe tener en cuenta la 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 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.

2. OBJETIVO GENERAL

a. Evaluar la correcta identificación, análisis y efectividad de los controles en la gestión de Riesgos de seguridad digital de la FND, durante el periodo comprendido entre enero-abril de 2021

b. Proporcionar a la Alta Dirección, información sobre los aspectos relevantes detectados en el seguimiento, con el fin de que permita fortalecer a la entidad en las Políticas de administración del riesgo de seguridad digital y a los sistemas que se articulan con Modelo Integral de Planeación y Gestión – MIPG -

2.1 OBJETIVOS ESPECIFICOS

- Verificar la aplicación de los lineamientos del MIPG, componente administración del riesgo.
- Implementar planes y programas de prevención de los riesgos asociados a los procesos.
-

- 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 – con acompañamiento de la Oficina Asesora de Planeación

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 el 01 de enero y el 30 abril de 2021.

5. METODOLOGÍA

El informe de seguimiento se obtiene de la información consolidada y suministrada por la Oficina de Planeación y 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 marco general para la gestión del riesgo y el control está a cargo de la Alta Dirección, en el que participa toda la FND desde el esquema de las Líneas de Defensa.

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.

- ✓ Documentos internos, como la política de seguridad de la información, la política de protección de datos
- ✓ Informes de auditorías internas y/o externas.
- ✓ Procedimientos de control interno.
- ✓ 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

- ✓ 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 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.”.
  Art. 9 “Asesorar a la dirección en la continuidad del proceso administrativo, la revaluación de los planes establecidos y en la introducción de los correctivos necesarios para el cumplimiento de las metas u objetivos previstos”.
- ✓ MIPG. Versión 3, diciembre 2019, del Consejo para la Gestión y Desempeño Institucional. Dimensión 7 “Control Interno”
- ✓ Guía para la administración de Riesgos DAFP- versión 5. diciembre 2020

8. LIMITACIONES

No se presentaron limitaciones para la realización del presente informe

9. EQUIPO AUDITOR

Carolina Navarrete y Clara Consuelo Ovalle

10. DESARROLLO

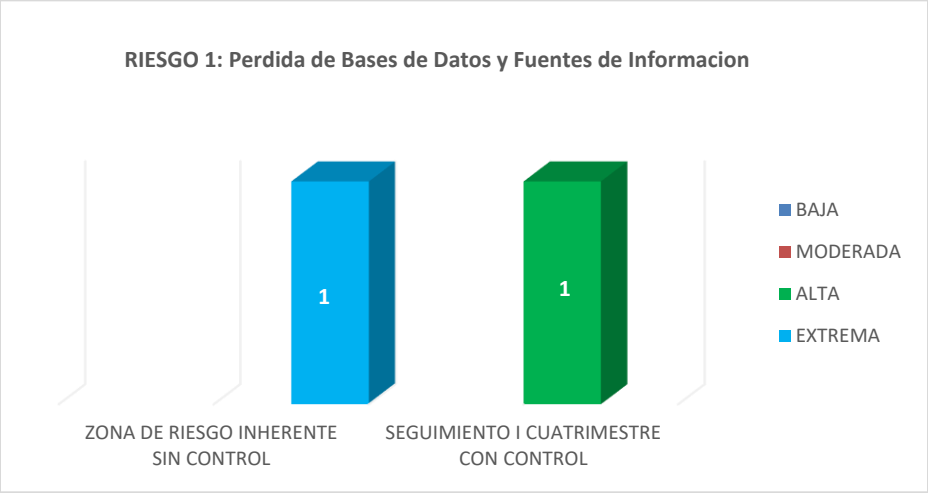
Para este periodo de análisis se formalizó el informe con base al seguimiento de los riesgos de seguridad digital que se efectúa a través de la Matriz de Riesgos I cuatrimestre consolidada 2021 y remitida por la Oficina Asesora de Planeación pudiendo establecer:

La Matriz MRSD refleja que la FND, determino-10 riesgos de Seguridad digital, los cuales se relacionan a continuación. Con el fin de mitigar dichos riesgos la FND desde la GTE implementó diez y nueve (19) controles como se relacionan a continuación:

NOMBRE DEL RIESGO - SEGURIDAD DIGITAL- FND	ZONA BAJA	ZONA MODERADA	ZONA ALTA	ZONA EXTREMA
Pérdida de Bases de Datos y Fuentes de Información	0	0	1	0
Ausencia de Controles en los Sistemas de Información	0	0	1	0
Manipulación, Modificación o Alteración sin Autorización de la Información Registrada en los Sistemas de la FND	0	0	1	0
Errónea Gestión de la Infraestructura Tecnológica de la FND	0	0	1	0
No Cumplir con los Lineamientos del Modelo de Seguridad y Privacidad de la Información y de las Políticas Gobierno Digital	0	0	1	0
No Disponibilidad de los Sistemas Tecnológicos y los de Información.	0	0	1	0
Insuficiencias Operativas de Software	0	0	1	0
Ataques Cibernéticos	0	0	1	0
Acceso a Cuentas de Correo FND	0	0	1	0
Pérdida de Equipos Informáticos	0	0	1	0
TOTAL	**0**	**0**	**10**	**0**

No.	CONTROLES
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	Bitácora de sistemas de información de la FND con sus respectivos tiempos de vigencias.
17	Programación de actividades de renovación con sistema de alarmas
18	Constituir nuevas políticas de trabajo y políticas de seguridad digital (incluyendo modalidad de trabajo en casa).
19	Control centralizado de equipos informáticos.

Riesgo No. 1 “pérdida de bases de datos y fuentes de información”



Controles establecidos por GTE.

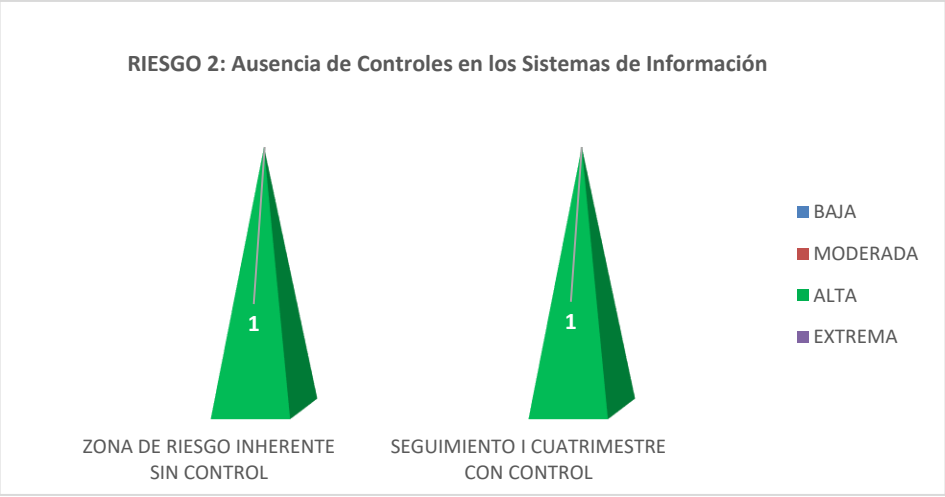
1. Copias de seguridad alojadas en Drive

2. Capacitaciones realizadas en las herramientas disponibles DE GOOGLE en la FND

Recomendación:

- ✓ Revisar las copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada por el proceso.

Riesgo No. 2 “**Ausencia de Controles en los Sistemas de Información**”



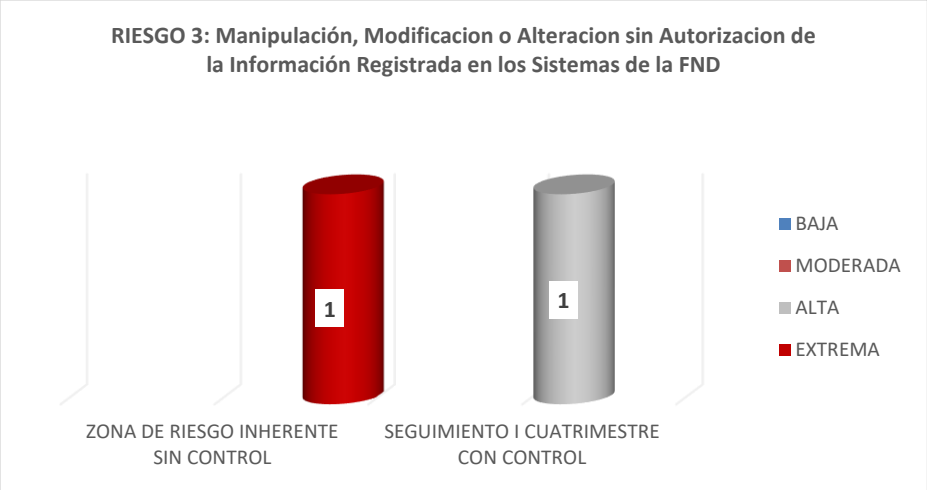
Controles establecidos por GTE.

1.Claves únicas para trabajadores. Manejo de información por áreas o procesos.
2.Actualizaciones y cambios periódicos de las contraseñas.

Recomendación

- ✓ Continuar con los controles existentes y evidenciar que estas actualizaciones y cambios periódicos en las contraseñas se realicen; es pertinente, que el mismo sistema arroje mensaje de alerta para que la tarea de actualización y cambio de contraseña se ejecute.

Riesgo No. 3 "**Manipulación, Modificación o alteración sin autorización de la Información Registrada en los Sistemas de la FND**"



Controles establecidos por GTE.

1.Actualizaciones

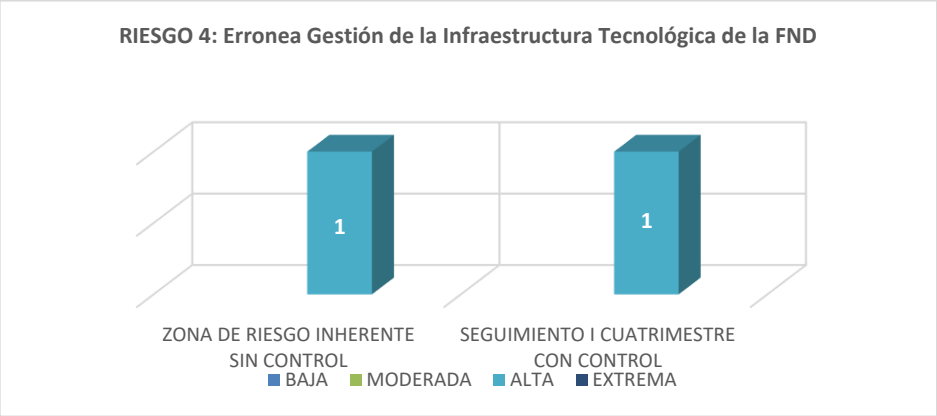
2.Cambios periódicos de contraseñas

3. Capacitar a los funcionarios para la solicitud de requerimientos

Recomendación

- ✓ Que los cambios de las contraseñas sean realizados por los usuarios periódicamente y que estos se ejecuten de acuerdo con el protocolo que la gerencia de tecnología establezca para tal actividad (programa de actualización periódica de contraseñas), con el fin de evitar vulnerabilidades y/o debilidades en los sistemas de la FND.

Riesgo No. 4 "**Errónea Gestión de la Infraestructura Tecnológica de la FND**"



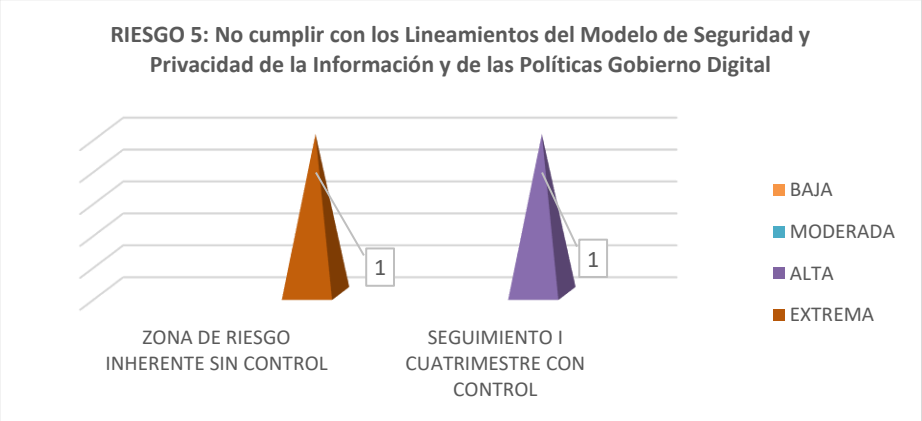
Controles establecidos por GTE.

1.Actualizacion y mantenimiento de las herramientas.
2.Mantenimiento de los activos de la FND y los proveedores.

Recomendación

- ✓ Consecución de insumos para el área de tecnología acorde con las necesidades actuales de cada área; mantenimiento oportuno de los sistemas por parte del proveedor, soporte inmediato y solución de fallas para que los sistemas no presenten altibajos y que la prestación de servicios sea de 100/100).

Riesgo No.5 "**No cumplir con los Lineamientos del Modelo de Seguridad y Privacidad de la Información y de las Políticas Gobierno Digital**"



Controles establecidos por GTE.

1.Ejecucion al plan de trabajo de la Política digital

2.Entrega de informes y porcentaje de avances

3. Creación del PETI.

4. Plan de tratamiento de riesgos de seguridad digital.

Observación:

- ✓ La FND, no esta dando cumplimiento a la implementación del modelo de seguridad digital y privacidad de la información, para preservar la confidencialidad, integridad, disponibilidad d ellos activos de información, garantizando su buen uso y la privacidad de los datos.

Lo anterior, debido a:

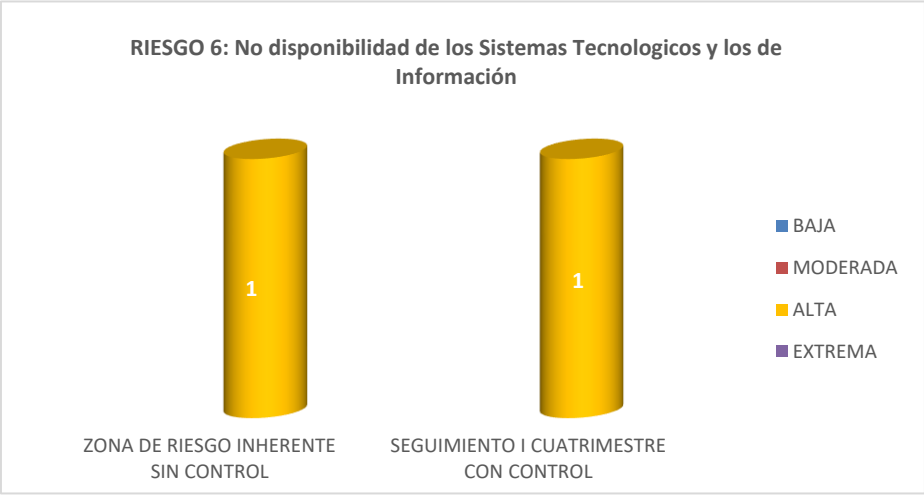
1. El PETI, no esta aprobado por el comité de gestión y desempeño, es decir, mientras no se apruebe no se puede ejecutar por parte GTE.

2. La FND viene construyendo un plan de tratamiento de riesgos de seguridad digital, orientado a gestionar los riesgos de seguridad digital asociados a los servicios de tecnologías de información y comunicaciones, que apoyan el desarrollo de las diferentes actividades asociadas al modelo de operación por procesos adoptados en la entidad, sim embargo hace falta la revisión por parte de la Oficina de planeación y posterior aprobación del comité de gestión y desempeño

Recomendación

- ✓ Dar cumplimiento con los lineamientos establecidos por Gobierno Digital- Mintic, con el acompañamiento de la Oficina de Planeación con el fin de articula esfuerzos, recursos metodologías y estrategias para asegurar su implementación.

Riesgo No.6 "**No disponibilidad de los Sistemas Tecnológicos y los de Información**"



Controles establecidos por GTE.

1. Listado de activos físicos de tecnología

2. Listado de inventario intangible (Sistemas de información)

3. Controles de fechas de terminación de contratos y+AA31cuerdos de Niveles de Servicios (ANS).

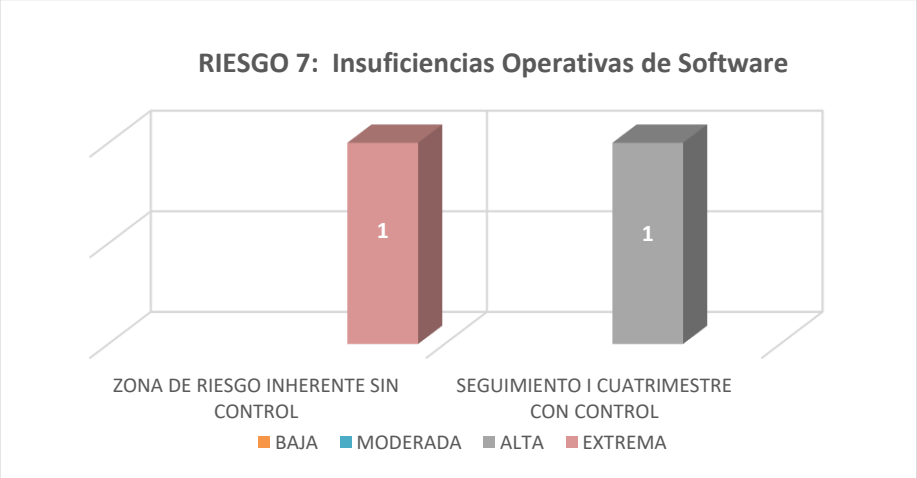
Observaciones:

Se evidencia, que en la FND algunos correos de los colaboradores que se retiraron o terminaron sus contratos de la Institución todavía aparecen como si estuviesen activos, no están deshabilitados del correo institucional.

Recomendación:

- ✓ Realizar exhaustivo check-list, de cuentas activas con dominio FND, frente a los contratos que se encuentren en ejecución (contratistas) los cuales deben tener cuenta activa con dominio FND; y anular las cuentas con dominio FND de colaboradores que no prestan servicios a la institución (cuentas de correo).

Riesgo No.7 “**Insuficiencias Operativas de Software**”



Controles establecidos por GTE.

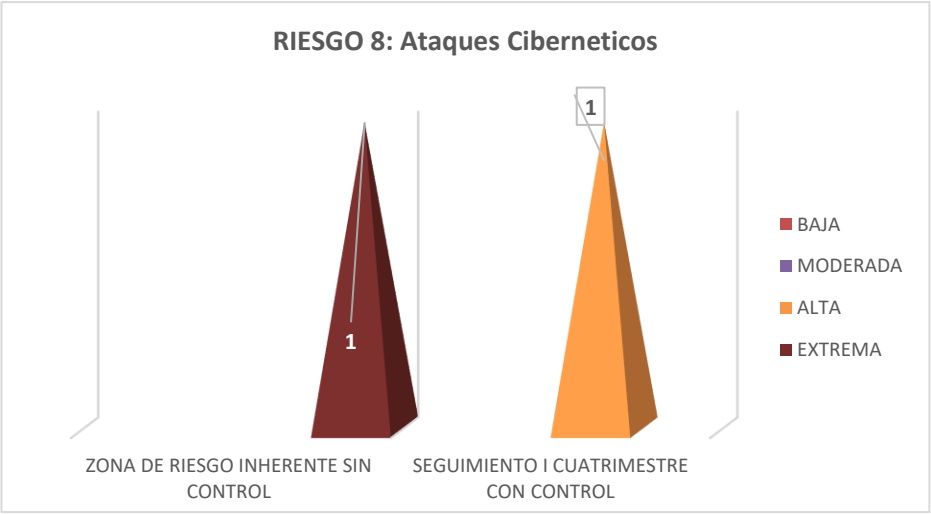
1. Bitácora de sistemas de información de la FND con sus respectivos tiempos de vigencias.

2. Programación de actividades de renovación con sistema de alarmas+AA31.

Recomendación:

- ✓ Seguir trabajando en aras de volver más robusto los sistemas de la FND.

Riesgo No.8 “**Ataques cibernéticos**”



Controles establecidos por GTE.

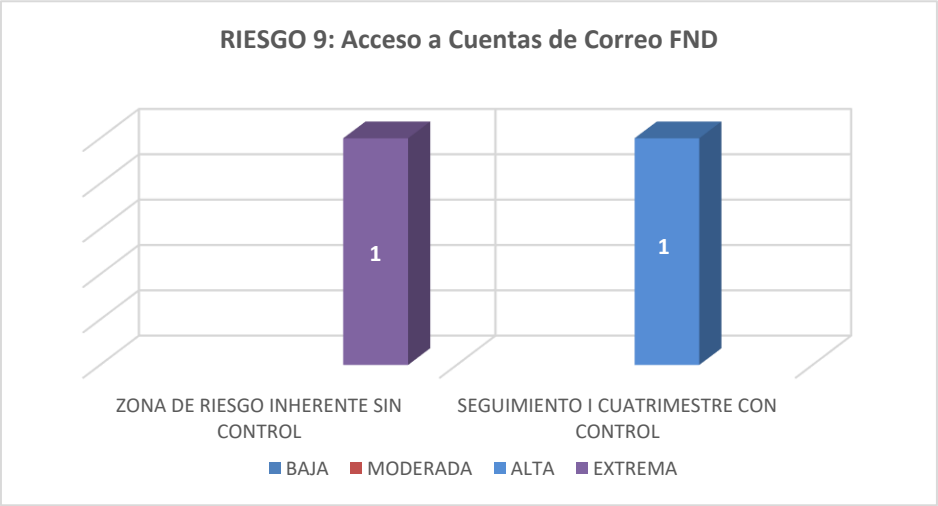
1. Constituir nuevas políticas de trabajo y políticas de seguridad digital (incluyendo modalidad de trabajo en casa).
2. Control centralizado de equipos informáticos.

Recomendación

✓ Control modalidad de trabajo en casa (Home working)

Estudiar por parte del proceso GTE, la implementación de una política y medidas de seguridad de soporte, para proteger, salvaguardar la información a la que se tiene acceso, y que es procesada o almacenada en los sitios en los que se realiza el trabajo en casa, por parte de los colaborares.

Riesgo No 9 "**Acceso a Cuentas de Correo FND**"



Controles establecidos por GTE.

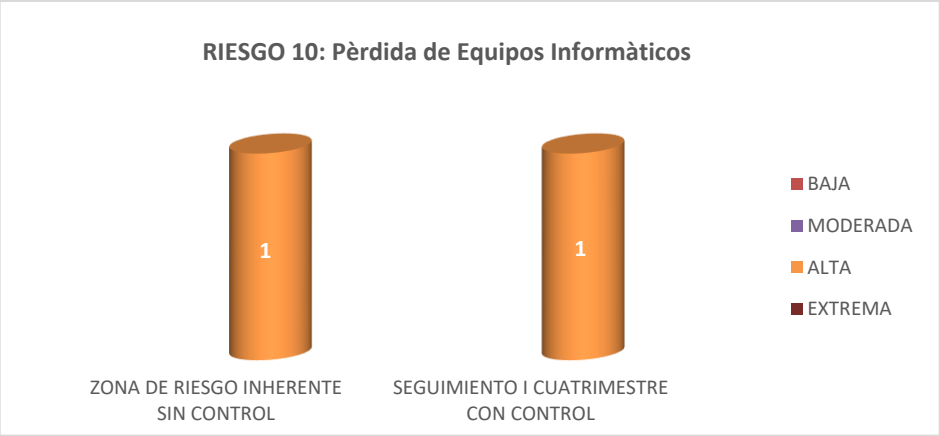
1. Constituir nuevas políticas de trabajo y políticas de seguridad digital (incluyendo modalidad de trabajo en casa).
2. Control centralizado de equipos informáticos

Recomendación

✓ Estudiar por parte del proceso GTE implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza el trabajo en casa, por parte de los colaboradores.

✓ Realizar exhaustivo check-list, de cuentas activas con dominio FND, frente a los contratos que se encuentren en ejecución (contratistas) los cuales deben tener cuenta activa con dominio FND; y anular las cuentas con dominio FND de colaboradores que no prestan servicios a la institución (cuentas de correo).

Riesgo No 10 "**Pérdida de equipos informáticos"**



Controles establecidos por GTE.

- Constituir nuevas políticas de trabajo y políticas de seguridad digital (incluyendo modalidad de trabajo en casa).
- Control centralizado de equipos informáticos

Recomendación

Estudiar por parte del proceso GTE implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza el trabajo en casa, por parte de los colaboradores.

10. OBSERVACIONES

1. En la Matriz, los controles establecidos no permiten disminuir el nivel de riesgo identificados en el proceso, ya que, con estos, el total de riesgos se encuentran en nivel alto

NOMBRE DEL RIESGO -SEGURIDAD DIGITAL- FND	ZONA BAJA	ZONA MODERADA	ZONA ALTA	ZONA EXTREMA
Pérdida de Bases de Datos y Fuentes de Información	0	0	1	0
Ausencia de Controles en los Sistemas de Información	0	0	1	0
Manipulación, Modificación o Alteración sin Autorización de la Información Registrada en los Sistemas de la FND	0	0	1	0
Errónea Gestión de la Infraestructura Tecnológica de la FND	0	0	1	0
No Cumplir con los Lineamientos del Modelo de Seguridad y Privacidad de la Información y de las Políticas Gobierno Digital	0	0	1	0
No Disponibilidad de los Sistemas Tecnológicos y los de Información.	0	0	1	0
Insuficiencias Operativas de Software	0	0	1	0
Ataques Cibernéticos	0	0	1	0
Acceso a Cuentas de Correo FND	0	0	1	0
Pérdida de Equipos Informáticos	0	0	1	0
TOTAL	**0**	**0**	**10**	**0**

Fuente: Matriz de Riesgos. OAP-FND

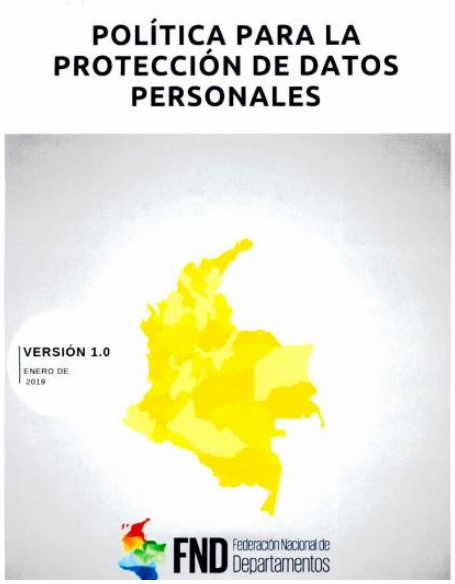
2. La FND cuenta con un plan de tratamiento de riesgos y seguridad digital, en construcción.

3. La FND su política de seguridad de la información se encuentra desactualizada, tiene fecha octubre 2018.

4. La política de tratamiento de datos personales, su última actualización fue en enero de 2019, cuyo propósito es establecer los criterios y lineamientos legales y corporativos bajo los cuales la FND realiza el tratamiento de la información.

5. Se evidencia en la página web de la FND contenido duplicado

- Documento desactualizado “Política para la protección de datos personales”.



- Documentos desactualizados

6. RECOMENDACIONES

- ✓ Revisar la página web, con el acompañamiento de la Oficina de Comunicaciones, con el fin de evitar la duplicidad de contenido y optimizar los enlaces internos y enlaces externos.

- ✓ 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)

- ✓ Tener en cuenta por parte de la GTE y con el acompañamiento de la Oficina Asesora de Planeación, y de la GAF, la Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas, Versión 5 de diciembre 2020 emitida conjuntamente entre el Departamento Administrativo de la Función Pública y la Secretaría de Transparencia de la Presidencia de la República, específicamente en las secciones de Análisis del contexto (con un enfoque hacia el entorno digital), identificación de activos, catálogos de amenazas y vulnerabilidades para el análisis de riesgos de seguridad digital, controles para la mitigación de los riesgos de seguridad digital, el reporte de riesgos de seguridad digital y otros aspectos adicionales para llevar a cabo una gestión del riesgo de seguridad digital adecuada, como herramienta para la toma de decisiones y para determinar la efectividad del control de seguridad digital en la Institución

- ✓ Tener en cuenta las recomendaciones realizadas por la Oficina de Control Interno para el proceso de seguridad digital, como resultado del seguimiento en el periodo Enero a abril 2021.

- ✓ Revisar por parte de la Oficina de Planeación y la GTE el plan de tratamiento de riesgos de seguridad digital con el apoyo de GAF, y actualizar las políticas de seguridad de la información y tratamiento de datos personales, las cuales deben ser llevadas a Comité de Gestión y Desempeño, para su aprobación, publicación y comunicación a los colaboradores y partes interesadas.

- ✓ Aplicar por parte de la GTE, medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la FND, teniendo en cuenta los diferentes riesgos de trabajar en sitios diferentes de dichas instalaciones.

- ✓ Revisar periódicamente los indicadores de gestión de seguridad digital, con el fin que reflejen el cumplimiento de las políticas y objetivos institucionales.

7. CONCLUSIONES

Del seguimiento efectuado al mapa de riesgos de seguridad digital de la entidad, se concluye que en el periodo enero a abril del 2021, no se materializó ningún riesgo de seguridad digital; 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.

Frente a la efectividad de los controles implementados en la matriz, es necesario que el líder del proceso de GTE con el acompañamiento de la Oficina de Planeación y de la GAF, revise los controles expuestos y genere nuevos y/o robustecer los existentes en aras de ser fuertes en sus sistemas y así evitar la materialización de riesgos.

El MRSD cuenta con 10 riesgos identificados, de los cuales se concluye que de los seis (6) riesgos de Zona extrema bajaron a zona **Alta** y se mantienen cuatro en la zona alta.

	Riesgo Inherente (Sin Control)	***Zona Riesgo***	***Riesgo Residual (Con Control)***
EXTREMA	6	EXTREMA	0
ALTA	4	ALTA	10
MODERADA	0	MODERADA	0
BAJA	0	BAJA	0

Atentamente

CLARA CONSUELO OVALLE JIMÉNEZ
Jefe Oficina Control Interno

Preparó:	Revisó:	Aprobó
Carolina Navarrete/Clara Ovalle	Clara Ovalle Jiménez	Clara Ovalle Jiménez
Fecha: mayo 2021	Fecha: mayo 2021	Fecha: mayo 2021