INFORME DE SEGUIMIENTO MAPAS DE RIESGOS
SEGURIDAD DIGITAL

I CUATRIMESTRE 2022

OFICINA DE CONTROL INTERNO

BOGOTA, MAYO 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

- 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
- 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 –

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 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:

- 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.”.

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

- 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

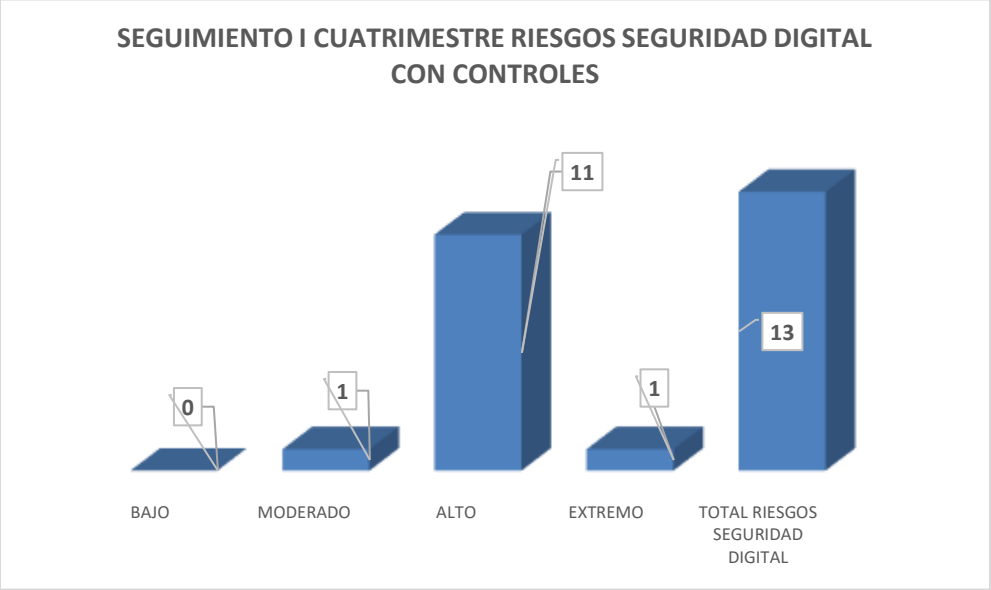
Carolina Navarrete /Clara Consuelo Ovalle

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 I cuatrimestre consolidada 2022, estableciendo.

La Matriz MRSD refleja que la FND, determino 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:

Gráfico No. 1. Riesgos Seguridad Digital con Controles



Fuente: Oficina Control Interno

Nota: El proceso GTE cuenta con 13 Riesgos de Seguridad Digita, de los cuales 1 se encuentra en zona de riesgos extrema, 11 se encuentran en zona de riesgo alta y 1 en zona de riesgo moderada con controles.

Cuadro No 1. Controles Establecidos -GTE

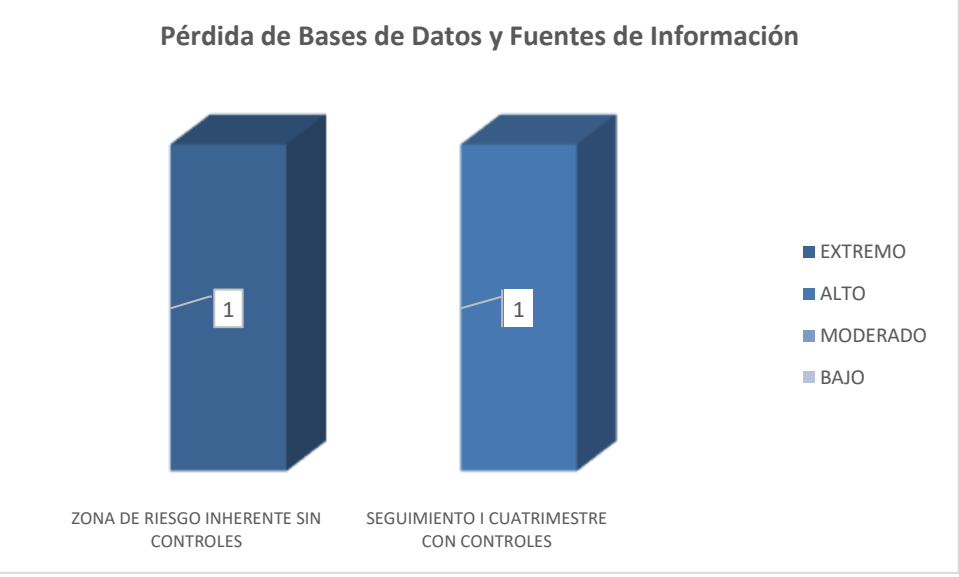
No.	CONTROLES
1	Copias de seguridad alojadas en Drive
2	Capacitaciones realizadas en las herramientas disponibles DE GOOGLE en la FND
3	Claves únicas para trabajadores. Manejo de información por áreas o procesos.
4	Actualizaciones y cambios periódicos de contraseñas
5	Cambios periódicos de contraseñas
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	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: Oficina Control Interno

Nota: El proceso de GTE, implemento 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.

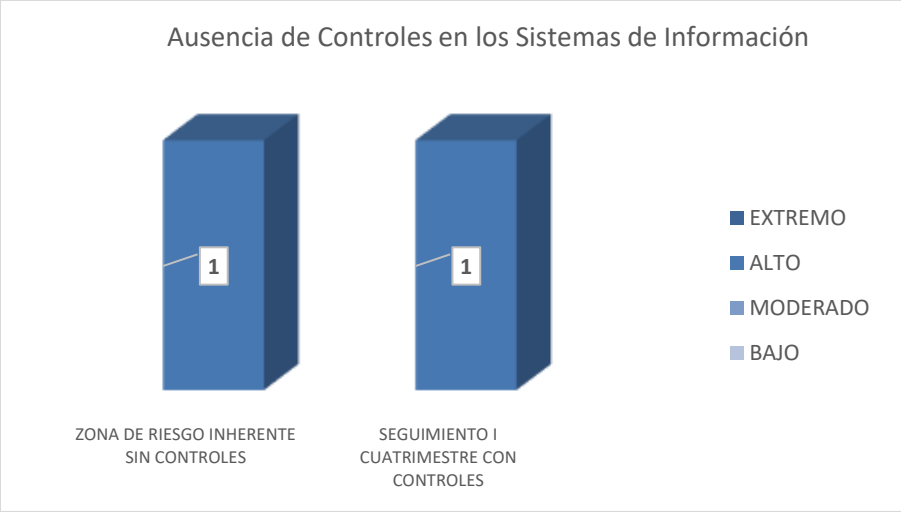
Riesgo No. 1 “pérdida de bases de datos y fuentes de información”



Fuente: Oficina Control Interno

Nota: Revisar las copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente.

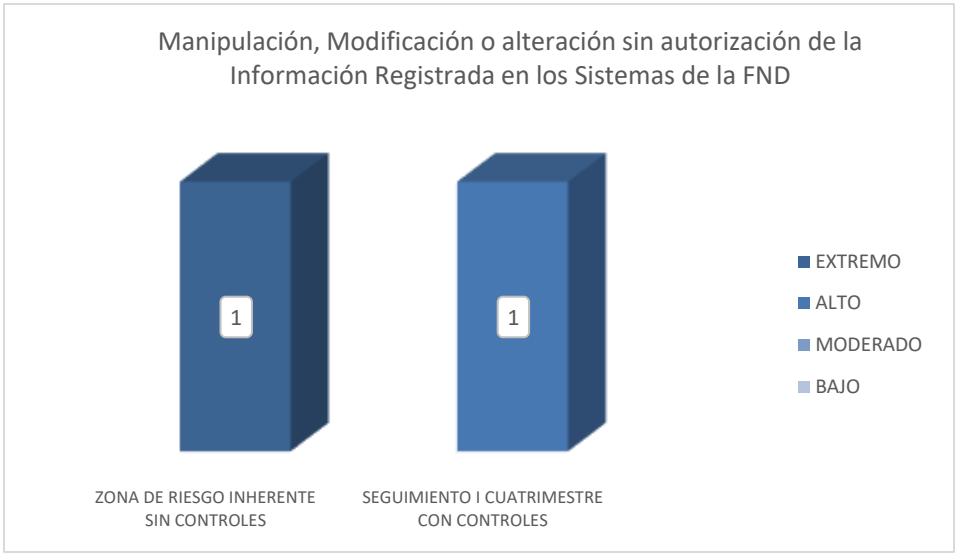
Riesgo No. 2 "Ausencia de Controles en los Sistemas de Información"



Fuente: Oficina Control Interno

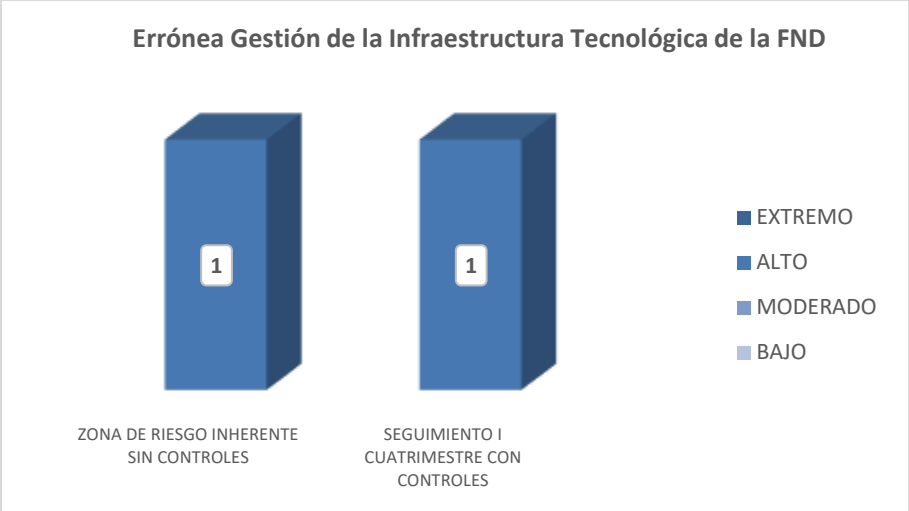
Nota: Continuar con los controles existentes y evidenciar que estas actualizaciones y cambios periódicos en las contraseñas se realicen; es pertinente, que el mismo sistema arroje mensaje de alerta para que la tarea de actualización y cambio de contraseña se ejecute.

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



Nota: Verificar 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"



Fuente: Oficina Control Interno

Nota: Continuar con la verificación del estado de actualización de todos los dispositivos y aplicaciones.

Nota: 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"

Fuente: Oficina Control Interno

Nota: Continuar con el cumplimiento de los lineamientos establecidos por Gobierno Digital- Mintic.

- Se llevo a Comité de Gestión y desempeño el PETI, para su aprobación
- Continuar con la aplicabilidad y ejecutar el plan de tratamiento de riesgos por GTE

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

Fuente: Oficina Control Interno

Nota: Continuar con el inventario de activos de información, continuar con los repositorios de copias de seguridad y el Backups de Orfeo

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).

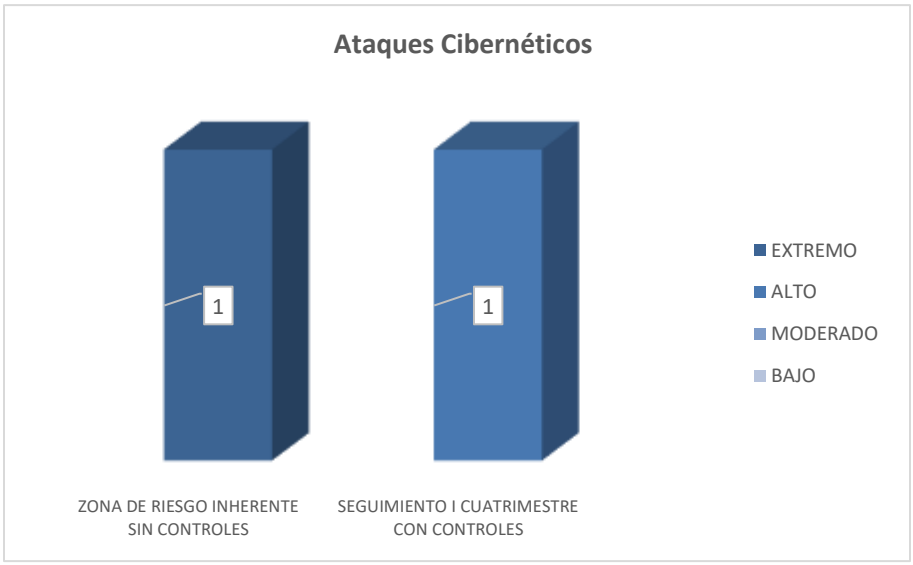
Riesgo No.7 “Insuficiencias Operativas de Software”

Fuente: Oficina Control Interno

Nota: Continuar robusteciendo los sistemas de información y las alertas de vencimiento de licencias

Continuar con la bitácora para el almacenamiento de datos en el cual se puede ver registro de evento en el sistema

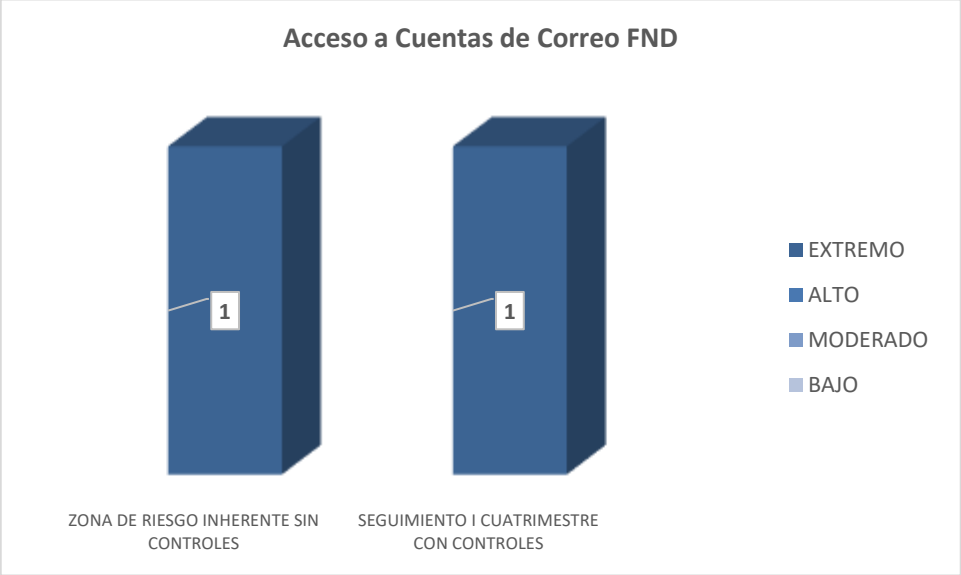
Riesgo No.8 “Ataques cibernéticos”



Fuente: Oficina Control Interno

Nota: Continuar con la implementación de una política y medidas de seguridad de soporte, para proteger, salvaguardar la información a la que se tiene acceso
Nota. Mantener el Antivirus actualizado y vigente
Nota: Continuar la centralización de los equipos informativos la cual debe ser lo suficientemente flexible para adaptarse a las necesidades de la entidad.

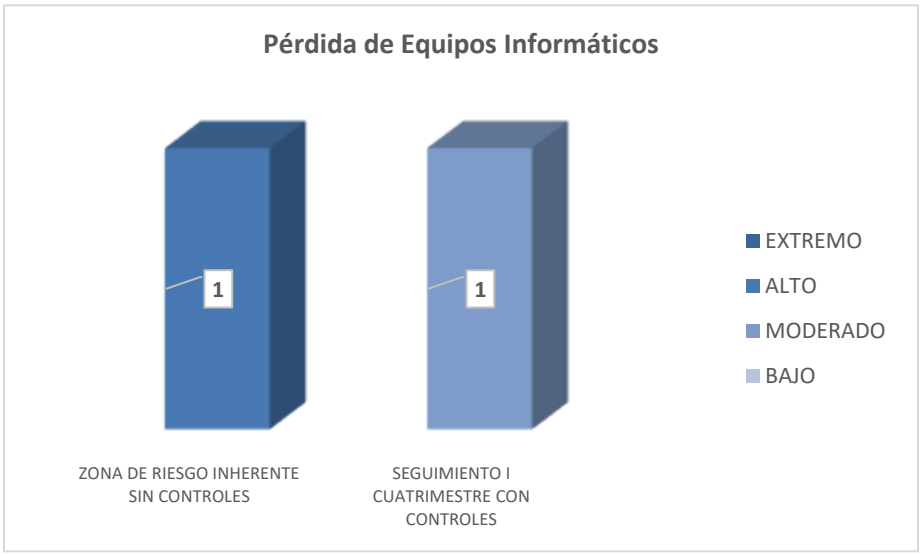
Riesgo No 9 "Acceso a Cuentas de Correo FND"



Fuente: Oficina Control Interno

Nota: Continuar con la implementación 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 que por una u otra razón ya no le prestan ningún servicio a la FND.
Continuar con las copias de respaldo por parte de la GTE periódicamente a los equipos de la FND

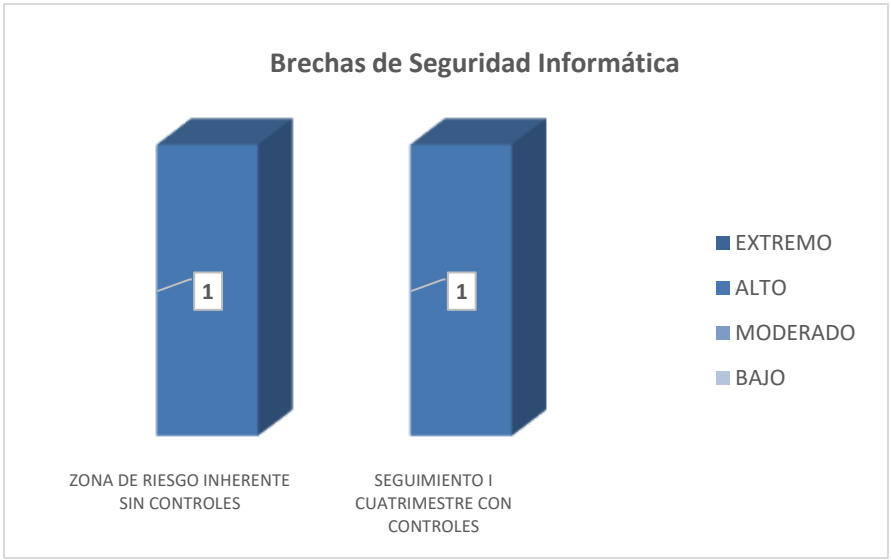
Riesgo No 10 “Pérdida de equipos informáticos”



Fuente: Oficina Control Interno

Nota: Continuar con el inventario de activos de información. Tendrán los activos de información que representan algún valor para la FND y que quedan dentro del alcance del SGSI.

Riesgo No 11. Brechas de seguridad informática



Fuente: Oficina Control Interno

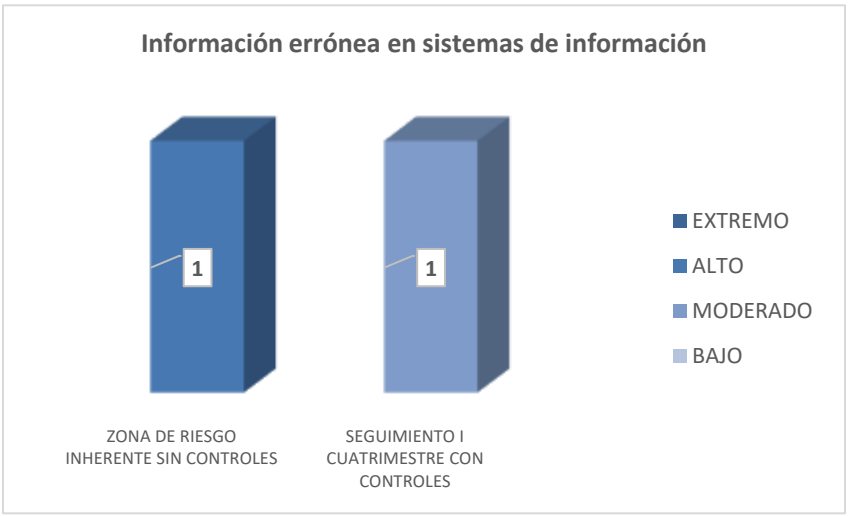
Nota: Continuar con la aplicabilidad de la política de seguridad y privacidad de la información que se tienen en la FND, para preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

Riesgos No 12. Acceso a información no autorizada

Fuente: Oficina Control Interno

Nota: Continuar con las pautas a través de capacitaciones o Tips a los usuarios para la creación y establecimiento de contraseñas seguras en los equipos de la FND
Dar continuidad a las capacitaciones de seguridad de la información en coordinación con la SGH, con el fin de que los colaboradores conozcan las políticas de seguridad de la información

Riesgo No 13. Información errónea en sistemas de información



Fuente: Oficina Control Interno

Nota: Dar aplicabilidad a las políticas de seguridad de la información que se tienen en la FND, para preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

Nota: Aplicar las políticas de administración de riesgos y los lineamientos establecidos por el Mintic sobre el mismo.

11. OBSERVACIONES

1. El área de tecnología está dando cumplimiento a la implementación del modelo de seguridad digital y privacidad de la información, para preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

2. El PETI, (plan estratégico de tecnología de la información) se encuentra pendiente de revisión por el Comité de Gestión y Desempeño, debido a la falta de aprobación por parte de los actores del proceso (Subdirectora Administrativa y Financiera y GTE)

3. Los controles establecidos son efectivos en el objetivo de disminuir el nivel de riesgo identificado en el proceso; sin embargo, los riesgos tecnológicos siempre van a estar en zona alta de materialización de estos, por lo que se debe implementar controles aún más robustos y de esta manera blindar a la organización.

4. En la Matriz, los controles establecidos no permiten disminuir el nivel de riesgo identificados en el proceso, ya que, la mayoría de los 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	0	1
Pérdida de equipos informáticos	0	1	0	0
Brechas de seguridad informática	0	0	1	0
Acceso a información no autorizada	0	0	1	0
Información errónea en sistemas de información	0	0	1	0
TOTAL	**0**	**1**	**11**	**1**

Fuente: Matriz de Riesgos. GTE

12. RECOMENDACIONES

1. Realizar campañas de concientización y socialización en temas de seguridad de la información, donde se dé a conocer la responsabilidad en la gestión de la seguridad digital en la FND, por parte de GTE.

2. 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).

3. 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.

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

5. verificar las cuentas de correo de personas que ya no laboran en la entidad y que aún están activas.

6. Remitir por parte de la GTE, las políticas de seguridad de la información y datos personales, así como el PETI, a la subdirección administrativa y financiera, para su revisión y aprobación previas a llevarse a comité de gestión y desempeño.

13. CONCLUSIONES

En cumplimiento de los roles y responsabilidades de la tercera línea de defensa, la Oficina de Control Interno realizó seguimiento al mapa de riesgos de seguridad digital de la entidad, donde se evidencia que en el I cuatrimestre del 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**.

El MRSD cuenta con 13 riesgos identificados, de los cuales se concluye que, once (11) se encuentran en de Zona Alta, Uno (1) Zona extrema y uno (1) Zona moderada, generando una alta probabilidad de ocurrencia de situaciones que pueden afectar el normal funcionamiento de la dependencia y por ende a toda la FND.

RIESGOS SEGURIDAD DIGITAL

NIVEL DE RIESGO INHERENTE	CANTIDAD	%
EXTREMO	6	46%
ALTO	7	54%
MODERADO	0	0%
BAJO	0	0%
TOTAL	13	100%

Perfil de Riesgos
Antes de Controles

NIVEL DE RIESGO RESIDUAL	CANTIDAD	%
EXTREMO	1	8%
ALTO	11	84%
MODERADO	1	8%
BAJO	0	0%
TOTAL	13	100%

Perfil de Riesgos
Después de Controles

Atentamente

CLARA CONSUELO OVALLE JIMÉNEZ
Jefe Oficina Control Interno

Preparó:	Revisó:	Aprobó
Carolina Navarrete/Clara Ovalle	Clara Ovalle Jiménez	Clara Ovalle Jiménez
Fecha: Mayo 2022	Fecha: Mayo 2022	Fecha: Mayo 2022