INFORME DE SEGUIMIENTO MAPAS DE RIESGOS
SEGURIDAD DIGITAL

II CUATRIMESTRE 2021

OFICINA DE CONTROL INTERNO

BOGOTA, SEPTIEMBRE 2021

TABLA DE CONTENIDO

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 los mismos 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 – 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 mayo y el 30 agosto de 2021.

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

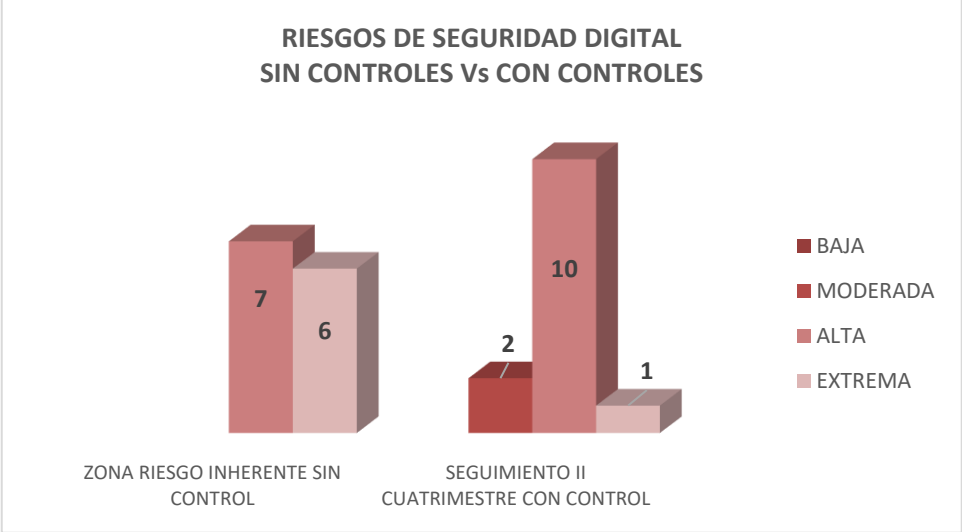
No se presentaron limitaciones para la realización del presente informe

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 2021 y remitida por la Oficina Asesora de Planeación pudiendo establecer:
- 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 (30) controles como se relacionan a continuación:



Fuente: Oficina Control Interno

Cuadro No 1. Controles establecidos -GTE_

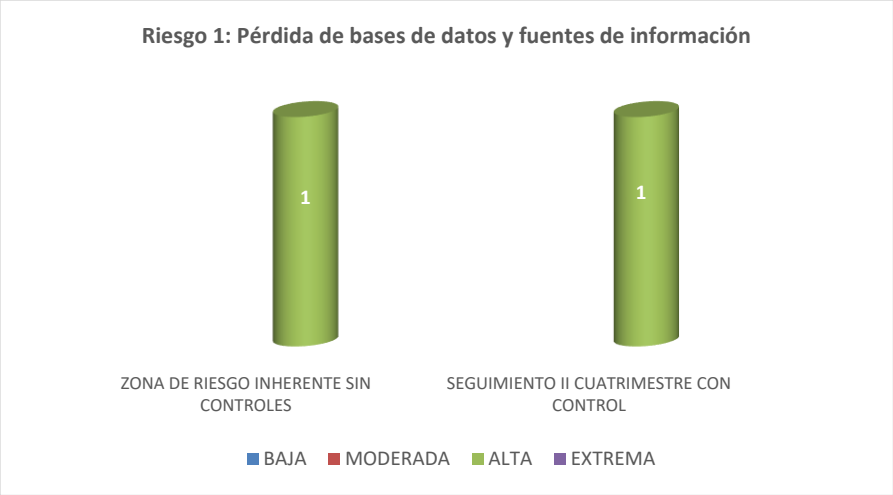
No.	CONTROLES
1	Copias de seguridad alojadas en Drive
2	Capacitaciones realizadas en las herramientas disponibles DE GOOGLE en la FND
3	Claves únicas para trabajadores. Manejo de información por áreas o procesos.
4	Actualizaciones y cambios periódicos de contraseñas
5	Cambios periódicos de contraseñas
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	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.
20	Copias de seguridad alojadas en Drive
21	Equipos protegidos a partir de Antivirus
22	Eliminación de cuentas de correos electrónicos.
23	Backups de cuentas de correos electrónicos.
24	Listado de activos físicos de tecnología
25	Correos de asignación de equipos
26	Implementar políticas de seguridad de la información que aseguren la integridad de los sistemas de información de la FND
27	Cambios periódicos de contraseñas
28	Capacitar a los funcionarios para la solicitud de requerimientos
29	Acceso a funcionarios a sistemas de información mínimos necesarios.
30	Backups de información para poder restaurar datos en caso de materialización del riesgo

Cuadro No 2. Riesgos de s seguridad digital con controles

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	1	0	0
TOTAL	**0**	**2**	**10**	**1**

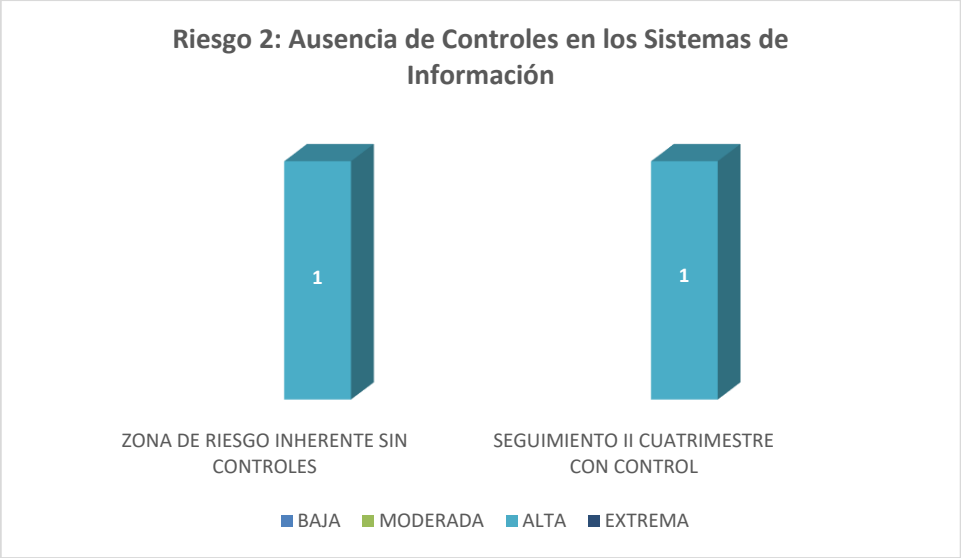
Fuente: Matriz riesgos seguridad digital -GTE-

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



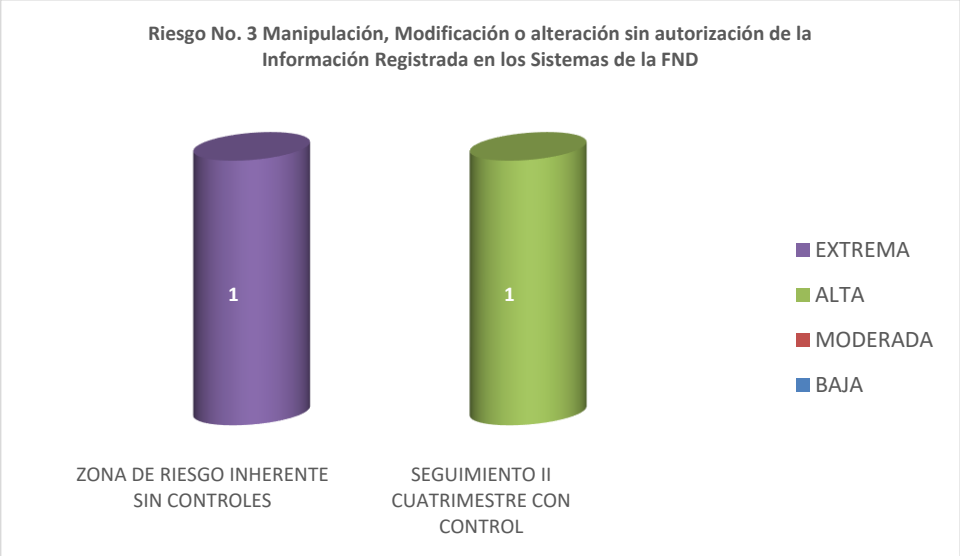
No.	CONTROLES	Recomendaciones Oficina de Control Interno
1	Copias de seguridad alojadas en Drive	Revisar las copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada por el proceso
2	Capacitaciones realizadas en las herramientas disponibles DE GOOGLE en 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 que les pueda ayudar abordar las amenazas de seguridad e implementar estrategias para mitigar las vulnerabilidades de seguridad de IT, así como definir cómo recuperarse cuando se produce un incidente. Además, las capacitaciones proporcionan pautas sobre qué hacer y qué no hacer

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



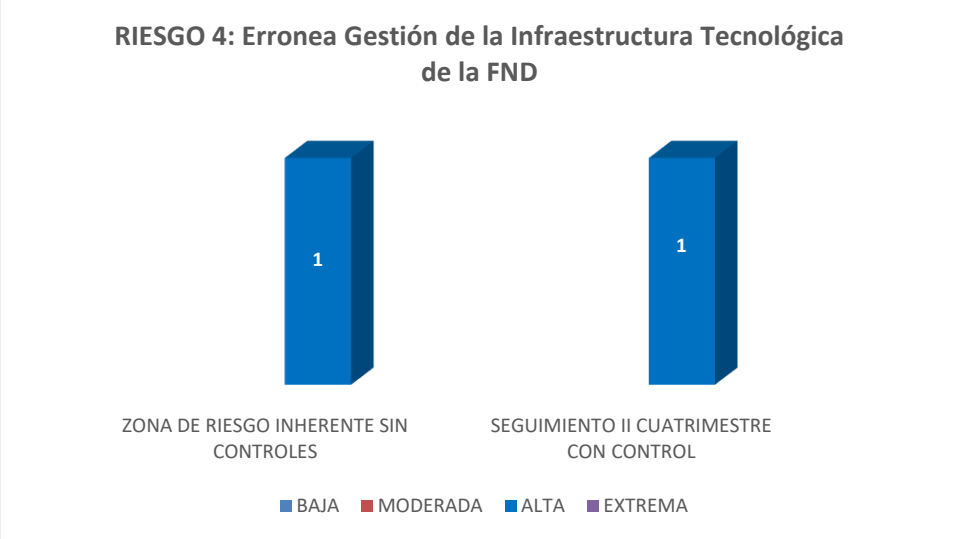
No.	CONTROLES	Recomendaciones Oficina de Control Interno
1	Claves únicas para trabajadores. Manejo de información por áreas o procesos.	Continuar con los controles existentes y evidenciar que estas actualizaciones y cambios periódicos en las contraseñas se realicen; es pertinente, que el mismo sistema arroje mensaje de alerta para que la tarea de actualización y cambio de contraseña se ejecute. Claves únicas de autenticación.
2	Actualizaciones y cambios periódicos de las contraseñas.	Dar pautas a través de capacitaciones o Tips a los usuarios para la creación y establecimiento de contraseñas seguras en los equipos de la FND, con el fin de evitar la suplantación de identidad y del usuario y que se corra el riesgo que un extraño a la FND pueda sustraer todo tipo de información del trabajador y/o de la empresa, o bien utilizar esta entrada para modificar o incluso eliminar archivos, con las consecuencias que esto podría acarrear para la Institución.

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



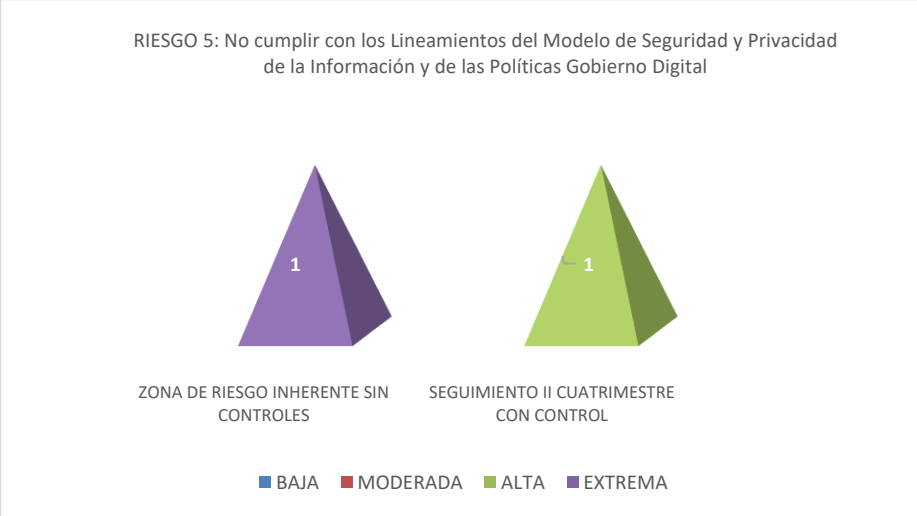
No.	CONTROLES	Recomendaciones Oficina de Control Interno
1	Capacitar a los colaboradores para la solicitud de requerimientos	Continuar con capacitaciones por parte de la GTE, en relación con la seguridad en los sistemas de información y darles a conocer a todos los colaboradores los procedimientos, protocolos, políticas, manuales implementados por el área de tecnología, para el desarrollo de las actividades.
2	Actualizaciones y cambios periódicos de las contraseñas.	Dar pautas a través de capacitaciones o Tips a los usuarios para la creación y establecimiento de contraseñas seguras en los equipos de la FND, con el fin de evitar la suplantación de identidad y del usuario y que se corra el riesgo que un extraño a la FND pueda sustraer todo tipo de información del trabajador y/o de la empresa, o bien utilizar esta entrada para modificar o incluso eliminar archivos, con las consecuencias que esto podría acarrear para la Institución. es pertinente, que el mismo sistema arroje mensaje de alerta para que la tarea de actualización y cambio de contraseña se ejecute.

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



No.	CONTROLES	Recomendaciones Oficina de Control Interno
1	Actualización y mantenimiento de herramienta	1.Vigilar el estado de actualización de todos nuestros dispositivos y aplicaciones. 2. Elegir la opción de actualizaciones automáticas siempre que esté disponible. 3. Instalar las actualizaciones tan pronto como se publiquen, especialmente las de los sistemas operativos, navegadores y programas antivirus. 4. Ser cuidadosos con las aplicaciones que instalamos, huyendo de fuentes no confiables y vigilando los privilegios que les concedemos. 5. Evitar hacer uso de aplicaciones y sistemas operativos antiguos que ya no dispongan de actualizaciones de seguridad.
2	Mantenimiento de los activos de la FND y los proveedores	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"



No.	CONTROLES	Recomendaciones Oficina de Control Interno
1	Ejecución al plan de trabajo de la Política digital	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.
2	Entrega de informes y porcentaje de avances	Remitir los informes solicitados a la GTE en forma oportuna a los diferentes órganos de control o procesos que así los requieran.
3	Creación del PETI	Llevar a Comité de Gestión y desempeño el PETI, para su aprobación y posterior ejecución por parte de la GTE.
4	Plan de tratamiento de riesgos de seguridad digital	Dar aplicabilidad y ejecutar el plan de tratamiento de riesgos por GTE

Observaciones:

- La GTE, 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.

- El PETI, no se ha actualizado debido a las demoras que ha presentado por parte de la Oficina de Planeación y aprobado por el Comité de Gestión y Desempeño, debido a:

  La planeación estratégica de tecnologías de la información PETI, tiene como objetivo asegurar que las metas y objetivos de TI estén vinculados y alineados con las metas y objetivos de la Entidad, es decir con el Plan estratégico, el cual no se encuentra a disposición del área de tecnología, con el fin de alinear el PETI y el PE, de la FND, se ha solicitado en dos oportunidades a Planeación el documento sin que a la fecha de este informe se conozca por parte de GTE y, esto ha retrasado la construcción y ejecución del mismo (PETI).

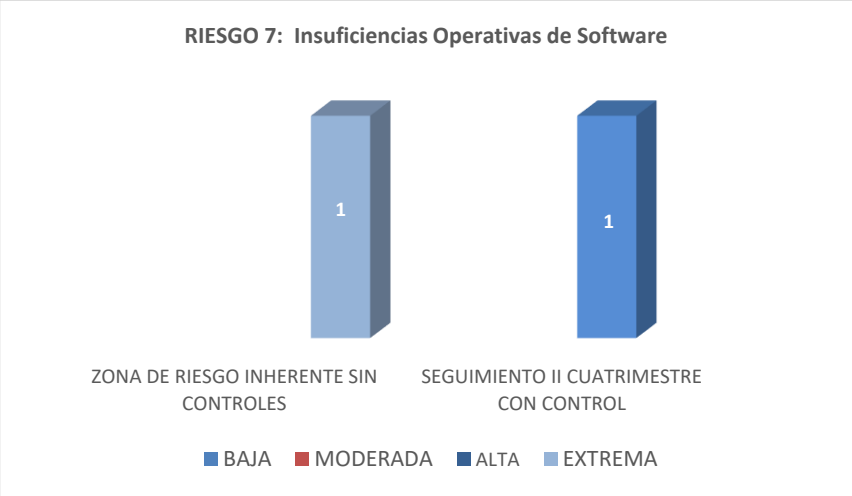
- La FND viene construyendo un plan de tratamiento de riesgos de seguridad digital, orientado a gestionar los riesgos de seguridad digital asociados a los servicios de tecnologías de información y comunicaciones, que apoyan el desarrollo de las diferentes actividades asociadas al modelo de operación por procesos adoptados en la entidad, sin embargo, hace falta la revisión por parte de la Oficina de planeación y posterior aprobación del comité de gestión y desempeño. El documento se realizó con el acompañamiento de la Subdirección Administrativa y Financiera (ingeniero Asesor), teniendo en cuenta los lineamientos establecidos por el Mintic, para el uso de tratamiento de información y estrategias aplicadas al

mismo; sin embargo, estos documentos deben tener el acompañamiento de la Oficina de Planeación, para su revisión y análisis.

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

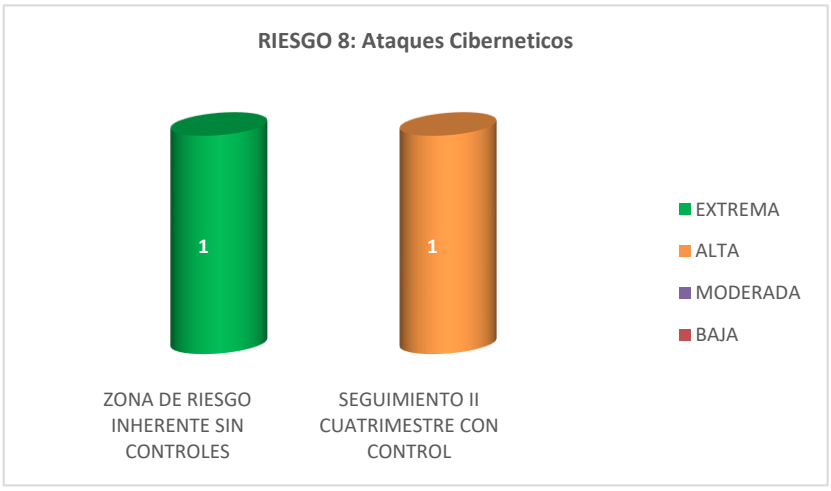
No.	CONTROLES	Recomendaciones Oficina de Control Interno
1	Listado de activos físicos de tecnología	llevar a cabo un inventario de activos de información. Tendrán los activos de información que **representan algún valor para la FND** y que quedan dentro del alcance del SGSI.
2	Listado de inventario intangible (Sistemas de información)	Llevar a cabo un inventario de los sistemas de información intangibles. como patentes y marcas, que no se concretan en bienes materiales, pero tienen un valor liquidativo Los intangibles son activos que existen y que tienen su valor, pero al no ser activos físicos ni existir la capacidad de convertirlos fácilmente en dinero, calcular su valor real se convierte en un desafío, para la organización
3	Controles de fechas de terminación de contratos y+AA31cuerdos de Niveles de Servicios (ANS).	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).
4	Aplicación de los Acuerdos de Niveles de Servicios (ANS)	
5	Copias de seguridad alojadas en Drive	

Riesgo No.7 "**Insuficiencias Operativas de Software**"



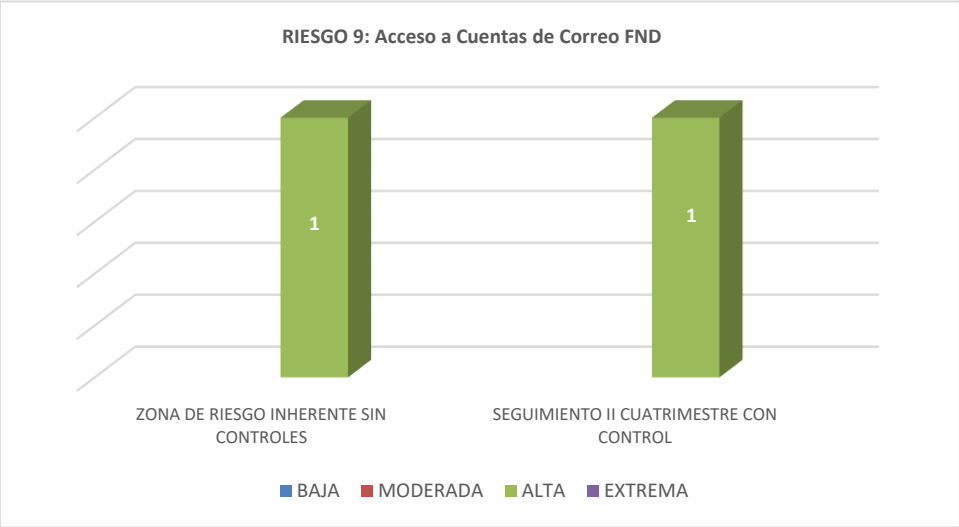
No.	CONTROLES	Recomendaciones Oficina de Control Interno
1	Programación de actividades de renovación con sistema de alarmas+AA31.	1. Un sistema de seguridad es un conjunto de medios y métodos para mantener los sistemas de información de la FND seguros y, prevenir, detectar y eliminar amenazas contra la información de la Institución. 2. Continuar robusteciendo los sistemas de información
2	Bitácora de sistemas de información de la FND con sus respectivos tiempos de vigencias.	Una bitácora es un almacén de datos en el cual se puede ver registro de evento en el sistema. con la finalidad de: 3. Aumentar la eficiencia y eficacia de los procesos, 4. Automatizar el flujo de forma rápida y simple. 5. Reducir ciclos de integración. 6. Brindar a los usuarios una idea de cómo funciona el proceso. 7. Romper la barrera de comunicación entre el área de sistema y el resto de los usuarios. 8. Mantener patrones de procesos. 9. Identificar y corregir más rápido los problemas asociados. 10. Manejo de excepciones. 11. Modelar por partes. 12. Transparencia de procesos. 13. Responsable de cada proceso.

Riesgo No.8 "**Ataques cibernéticos**"



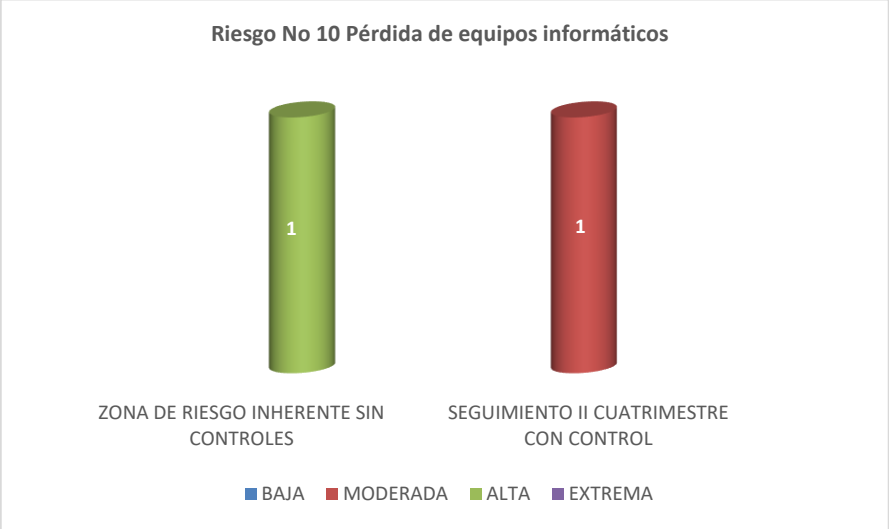
No.	CONTROLES	Recomendaciones Oficina de Control Interno
1	Constituir nuevas políticas de trabajo y políticas de seguridad digital (incluyendo modalidad de trabajo en casa).	Estudiar por parte del proceso GTE, la implementación de una política y medidas de seguridad de soporte, para proteger, salvaguardar 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.
2 3	Control centralizado de equipos informáticos. Equipos protegidos con antivirus	1. Le permitirá optimizar 'sus recursos". 2. Mejorar la productividad. 3. Más seguridad. Al quedar centralizado, el sistema establece unos sistemas de control y acceso a la información claros y contundentes lo que impide la pérdida por error o por el acceso indeseado de elementos externos o que no disponen de la autorización pertinente para acceder al sistema. 4. Competitividad. Cifrada, fundamentalmente, en dos aspectos muy importantes. 5. Una buena centralización debe facilitar en todo momento la implantación rápida de nuevos sistemas operativos, ya sean estos físicos o virtuales. Vinculada a esta primera característica, una buena centralización debe ser lo suficientemente flexible para adaptarse a las necesidades de la entidad.

Riesgo No 9 “**Acceso a Cuentas de Correo FND**”



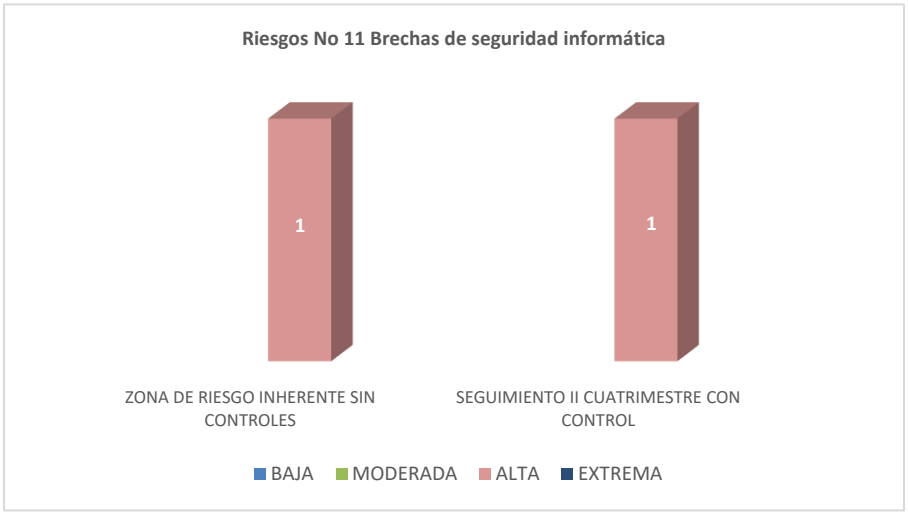
No.	CONTROLES	Recomendaciones Oficina de Control Interno
1	eliminación de cuentas de correos electrónicos.	1. Estudiar por parte del proceso GTE implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza el trabajo en casa, por parte de los colaboradores que por una u otra razón ya no le prestan ningún servicio a la FND. 2. 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).
2	Backups de cuentas de correos electrónicos.	Realizar copias de respaldo por parte de la GTE periódicamente a los equipos de la FND, con el fin de poder volver a disponer de su información en caso de que alguna eventualidad, accidente o desastre ocurra y ocasione su pérdida del sistema.

Riesgo No 10 “**Pérdida de equipos informáticos”**



No.	CONTROLES	Recomendaciones Oficina de Control Interno
1	Listado de activos físicos de tecnología	llevar a cabo un 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.
2	Correos de asignación de equipos	1. Levantar un inventario de los correos asignados a los colaboradores 2. 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 11. **Brechas de seguridad informática**

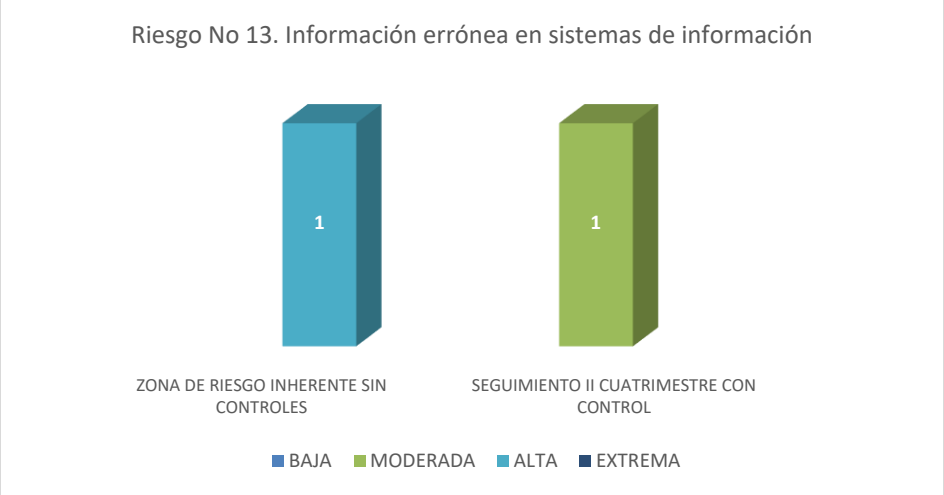


No.	CONTROLES	Recomendaciones Oficina de Control Interno
1	políticas de seguridad de la información que aseguren la integridad de los sistemas de información de la FND	Dar aplicabilidad a las políticas de seguridad de la información que se tienen en la FND, para preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

Riesgos No 12. **Acceso a información no autorizada**

No.	CONTROLES	Recomendaciones Oficina de Control Interno
1	Actualizaciones y cambios periódicos de contraseñas	Dar pautas a través de capacitaciones o Tips a los usuarios para la creación y establecimiento de contraseñas seguras en los equipos de la FND, con el fin de evitar la suplantación de identidad y del usuario y que se corra el riesgo que un extraño a la FND pueda sustraer todo tipo de información del trabajador y/o de la empresa, o bien utilizar esta entrada para modificar o incluso eliminar archivos, con las consecuencias que esto podría acarrear para la Institución. es pertinente, que el mismo sistema arroje mensaje de alerta para que la tarea de actualización y cambio de contraseña se ejecute.
2	Capacitar a los colaboradores para la solicitud de requerimientos.	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 que les pueda ayudar abordar las amenazas de seguridad e implementar estrategias para mitigar las vulnerabilidades de seguridad de IT, así como definir cómo recuperarse cuando se produce un incidente. Además, las capacitaciones proporcionan pautas sobre qué hacer y qué no hacer

Riesgo No 13**. Información errónea en sistemas de información**



No.	CONTROLES	Recomendaciones Oficina de Control Interno
1	Acceso a funcionarios a sistemas de información mínimos necesarios.	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.
2	Backups de información para poder restaurar datos en caso de materialización del riesgo.	1. Aplicar las políticas de administración de riesgos y los lineamientos establecidos por el Mintic sobre el mismo. 2. debe tener en cuenta la Guía para la administración del riesgo y el diseño de controles en entidades públicas- Versión 5 de diciembre 2020,

11. OBSERVACIONES

1. La GTE, 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, no se ha actualizado debido a las demoras que ha presentado por parte de la Oficina de Planeación y aprobado por el Comité de Gestión y Desempeño, debido a:

   La planeación estratégica de tecnologías de la información PETI, tiene como objetivo asegurar que las metas y objetivos de TI estén vinculados y alineados con las metas y objetivos de la Entidad, es decir con el Plan estratégico, el cual no se encuentra a disposición del área de tecnología, con el fin de alinear el PETI y el PE, de la FND, se ha solicitado en dos oportunidades a Planeación el documento sin que a la fecha de este informe se conozca por parte de GTE y, esto ha retrasado la construcción y ejecución del mismo (PETI).

3. 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, sin embargo, hace falta la revisión por parte de la Oficina de planeación y posterior aprobación del comité de gestión y desempeño.

4. El documento se realizó con el acompañamiento de la Subdirección Administrativa y Financiera (Asesor), teniendo en cuenta los lineamientos establecidos por el Mintic, para el uso de tratamiento de información y estrategias aplicadas al mismo; sin embargo, estos documentos deben tener el acompañamiento de la Oficina de Planeación, para su revisión y análisis.

5. Los controles establecidos son efectivos en el objetivo de disminuir el nivel de riesgo identificado en el proceso, más 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

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	1	0	0
TOTAL	**0**	**2**	**10**	**1**

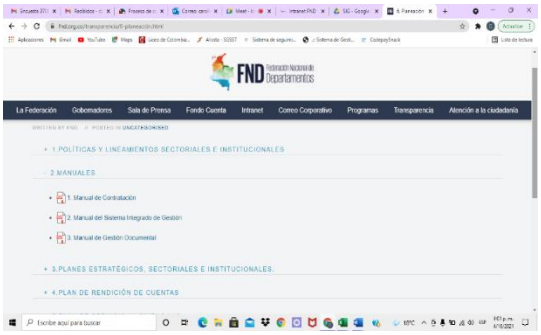
Fuente: Matriz de Riesgos. GTE

1. El enlace de Transparencia de la Página Web se encuentra con algunas secciones desactualizadas, corriéndose el riesgo de posibles llamados de atención por parte de la PGN, por no dar cumplimiento a lo establecido en la Ley No. 1712/2014, artículo 9 Artículo 9°." Información mínima obligatoria respecto a la estructura del sujeto obligado". Todo sujeto obligado deberá publicar la siguiente información mínima obligatoria de manera proactiva en los sistemas de información del Estado o herramientas que lo sustituyan https://www.fnd.org.co/# ,
2. planeación: https://fnd.org.co/transparencia/6-planeaci%C3%B3n.html.
3. https://fnd.org.co/transparencia/2-informaci%C3%B3n-de-inter%C3%A9s.html.
4. https://fnd.org.co/federacion/calidad.html
5. https://fnd.org.co/federacion/estructura-administrativa.html

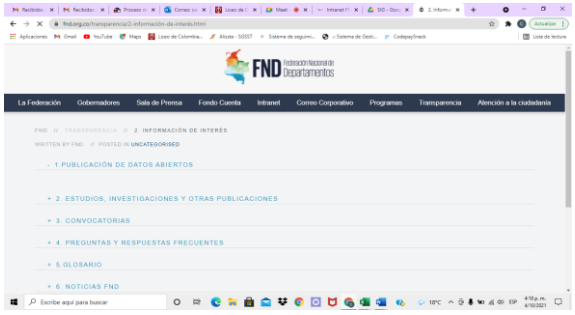
Parágrafo: Los sujetos obligados deberán actualizar la Información a la que se refiere el artículo 9°, mínimo cada mes. (el subrayado es mío).

6. Documentos desactualizados enlace de transparencia por dependencia (planeación y comunicaciones)

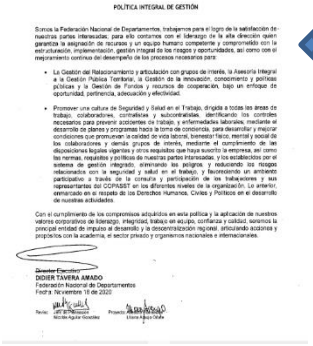
Manual de funciones



Datos abiertos



7. Documentos desactualizados página web (Oficina de Planeación y comunicaciones)


POLITICA INTEGRAL DE GESTIÓN

Somos la Federación Nacional de Departamentos, trabajamos para el logro de la satisfacción de nuestras partes interesadas, para ello contamos con el liderazgo de la alta dirección quien garantiza la asignación de recursos y un equipo humano competente y comprometido con la estructuración, implementación, gestión integral de los riesgos y oportunidades, así como con el mejoramiento continuo del desempeño de los procesos necesarios para:

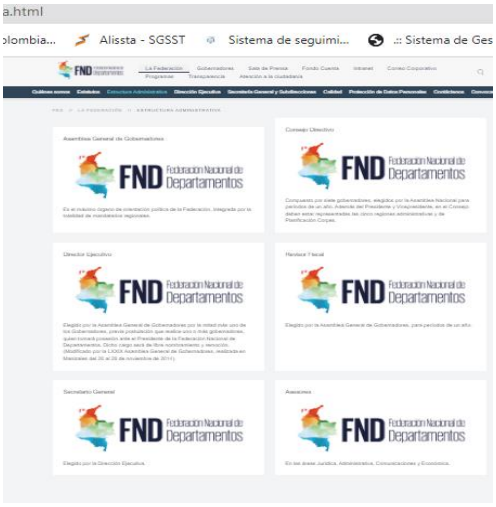
- La Gestión del Relacionamiento y articulación con grupos de interés, la Asesoría Integral a la Gestión Pública Territorial, la Gestión de la innovación, conocimiento y políticas públicas y la Gestión de Fondos y recursos de cooperación, bajo un enfoque de oportunidad, pertinencia, adecuación y efectividad.
- Promover una cultura de Seguridad y Salud en el Trabajo, dirigida a todas las áreas de trabajo, colaboradores, contratistas y subcontratistas, identificando los controles necesarios para prevenir accidentes de trabajo, y enfermedades laborales, mediante el desarrollo de planes y programas hacia la toma de conciencia, para desarrollar y mejorar condiciones que promuevan la calidad de vida laboral, bienestar físico, mental y social de los colaboradores y demás grupos de interés, mediante el cumplimiento de las disposiciones legales vigentes y otros requisitos que haya suscrito la empresa, así como las normas, requisitos y políticas de nuestras partes interesadas, y los establecidos por el sistema de gestión integrado, eliminando los peligros, y reduciendo los riesgos relacionados con la seguridad y salud en el trabajo, y fomentando un ambiente participativo a través de la consulta y participación de los trabajadores y sus representantes del COPASST en los diferentes niveles de la organización. Lo anterior, enmarcado en el respeto de los Derechos Humanos, Civiles y Políticos en el desarrollo de nuestras actividades.

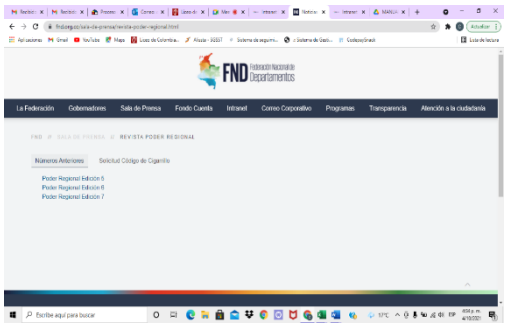
Con el cumplimiento de los compromisos adquiridos en esta política y la aplicación de nuestros valores corporativos de liderazgo, integridad, trabajo en equipo, confianza y calidad, somos la principal entidad de impulso al desarrollo y la descentralización regional, articulando acciones y propósitos con la academia, el sector privado y organismos nacionales e internacionales.

Director Ejecutivo
DIDIER TAVERA AMADO
Federación Nacional de Departamentos
Fecha: Noviembre 16 de 2020

Política integral de gestión

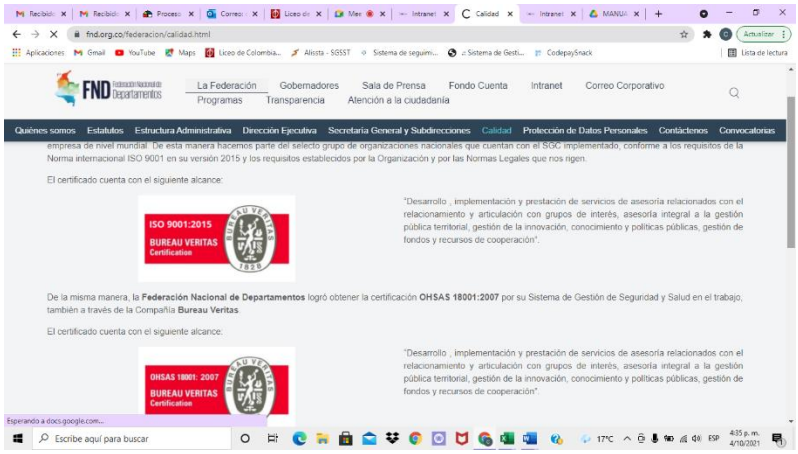
Estructura administrativa





Revista poder: no se evidencian las ediciones Nos. 1,2 y 3

Calidad : Desactualizada la norma, no se observa la certificación en **ISO 45001:2018. Oficina de Planeación.**



12. RECOMENDACIONES

- ✓ Revisar por parte de la Oficina de planeación 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.

- ✓ Convocar por parte de la Oficina de Planeación a Comité de Gestión y Desempeño, y llevar las políticas de seguridad de la información, política de tratamiento de datos, el PETI 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, si los hay, 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.

- ✓ Actualizar por parte de la Oficina de planeación, la Información mínimo cada mes tal como se refiere el artículo 9° “de la ley No. 1712/2014, **Ley de Transparencia y acceso a la información pública.**

- ✓ Implementar por parte de la GTE, formato de ingreso de equipos que no pertenecen a la FND, con el fin de tener un control de entradas y salidas de insumos tecnológicos ajenos a la FND, y con esto estudiar la creación de la política de control de acceso, con el fin de dar cumplimiento a las normas técnicas ISO 37001:2017 e ISO 27001:2015.

13. CONCLUSIONES

Del seguimiento efectuado al mapa de riesgos de seguridad digital de la entidad, se concluye que en el periodo de mayo -agosto se incluyeron tres (3) riesgos, 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 minimizar 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 el apoyo del ingeniero asesor de la SAF 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 estos.

El MRSD cuenta con 13 riesgos identificados, de los cuales se concluye que, diez (10) se encuentran en de Zona Alta, Uno (1) Zona extrema y dos (2) Zona moderada, generando una alta probabilidad de ocurrencia de situaciones que pueden afectar el normal funcionamiento de la dependencia y por ende al resto de la entidad.

Las dependencias involucradas deben levantar un plan de mejoramiento producto de las observaciones y recomendaciones y remitirlo a esta Oficina, dentro de los cinco (5) días siguientes al recibo de este informe

	Riesgo Inherente (Sin Control)	*Zona Riesgo*	*Riesgo Residual (Con Control)*
EXTREMA	6	EXTREMA	1
ALTA	7	ALTA	10
MODERADA		MODERADA	2
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: septiembre 2021	Fecha: septiembre 2021	Fecha: septiembre 2021