INFORME DE SEGUIMIENTO MAPAS DE RIESGOS SEGURIDAD DIGITAL

II CUATRIMESTRE 2022

OFICINA DE CONTROL INTERNO

SEPTIEMBRE 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 mayo y agosto 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:

- 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 II 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. Controles Existentes

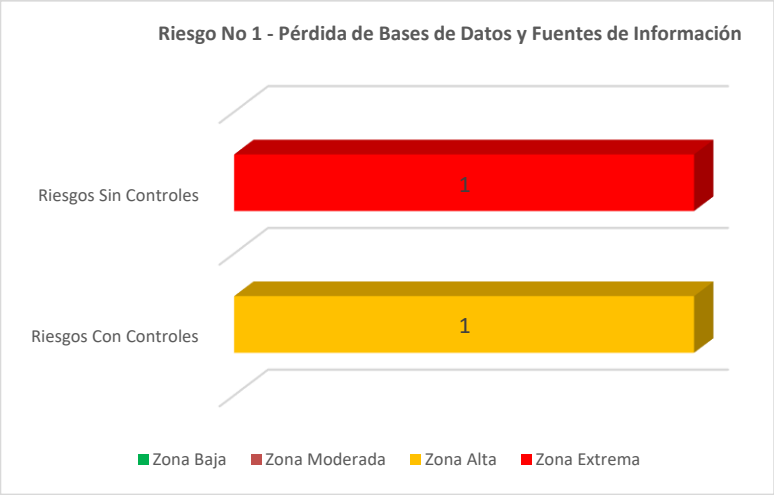
No.	CONTROLES ESTABLECIDOS
1	Copias de seguridad alojadas en Drive
2	Capacitaciones realizadas en las herramientas disponibles DE GOOGLE en la FND
3	Claves únicas para trabajadores. Manejo de información por áreas o procesos.
4	Actualizaciones y cambios periódicos de contraseñas
5	Cambios periódicos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

Gráfico No 1. “Pérdida de bases de datos y fuentes de información”

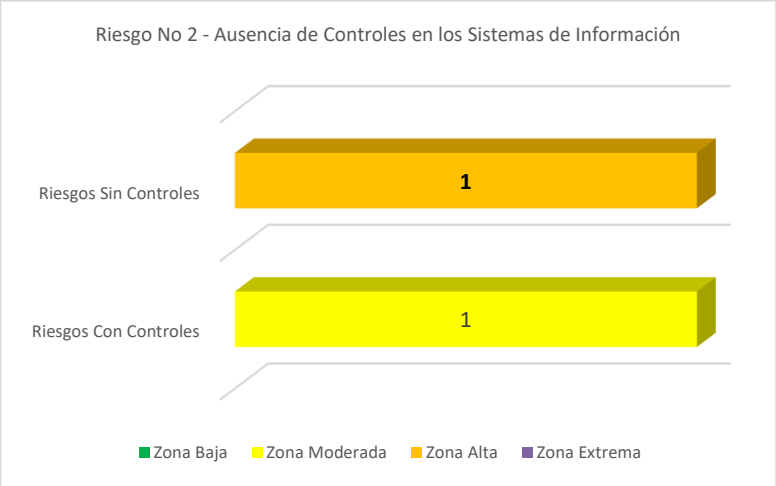
Observaciones Control Interno: *Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que el riesgo residual sigue siendo ALTO.*



Fuente: Matriz de Riesgos de Seguridad Digital

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

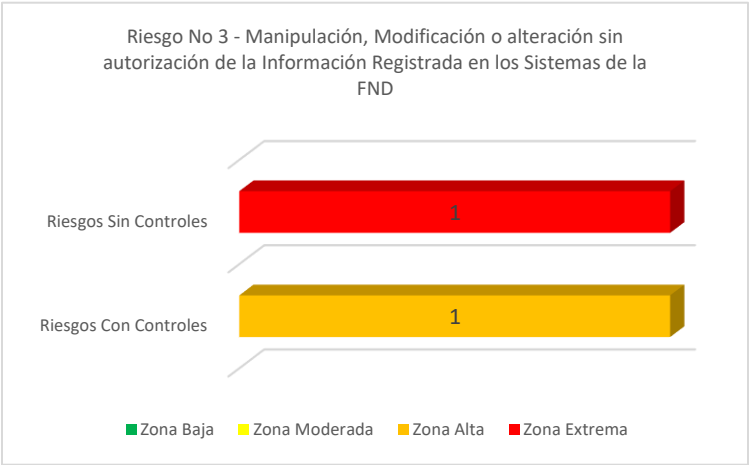
Observaciones Control Interno: *1. Los controles propuestos para bajar la valoración del riesgo residual son los mismos del riesgo inherente, es decir que sin controles la valoración del riesgo es Alta, y con los mismos controles la valoración es moderada (riesgo residual). 2. Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos.*



Fuente: Matriz de Riesgos de Seguridad Digital

Gráfico No. 3 “Manipulación, Modificación o alteración sin autorización de la Información Registrada en los Sistemas de la FND”

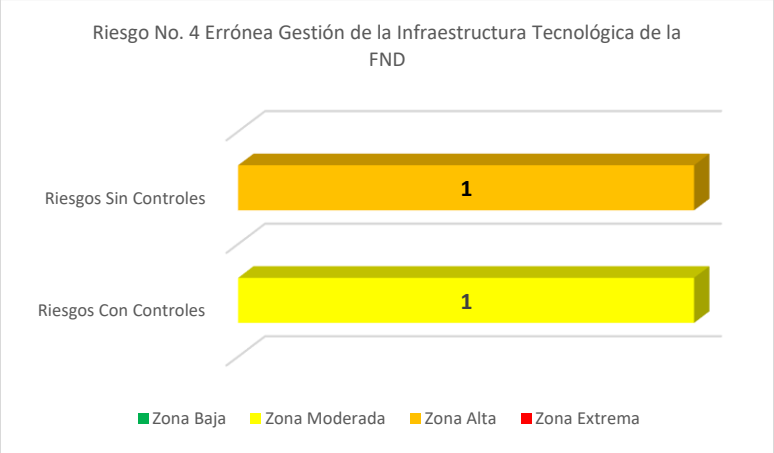
Observaciones Control Interno: *1. Los controles propuestos para bajar la valoración del riesgo residual son los mismos del riesgo inherente, es decir que sin controles la valoración del riesgo es Extrema, y con los mismos controles la valoración es Alta (riesgo residual). 2. Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos.*



Fuente: Matriz de Riesgos de Seguridad Digital

Gráfico No. 4 “Errónea Gestión de la Infraestructura Tecnológica de la FND”

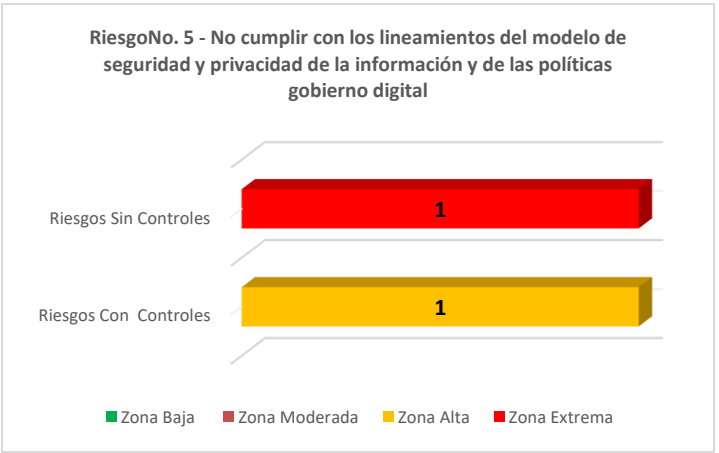
***Observaciones Control Interno**: 1. Los controles propuestos para bajar la valoración del riesgo residual son los mismos del riesgo inherente, es decir que sin controles la valoración del riesgo es Alta, y con los mismos controles la valoración es moderada (riesgo residual). 2. Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos,*



Fuente: Matriz de Riesgos de Seguridad Digital

Grafica No 5“No cumplir con los lineamientos del modelo de seguridad y privacidad de la información y de las políticas gobierno digital”

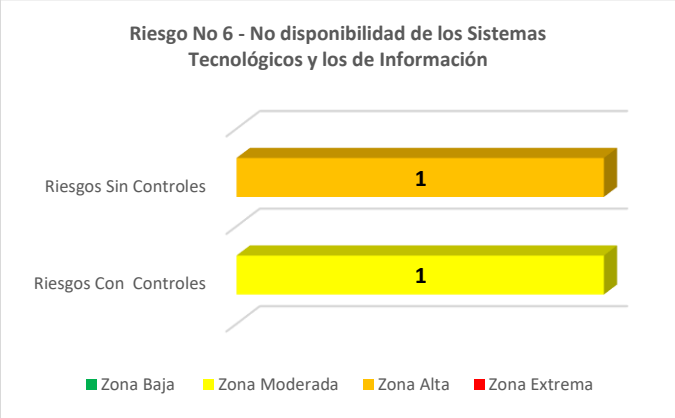
***Observaciones Control Interno:** 1.Los controles propuestos para bajar la valoración del riesgo residual son los mismos del riesgo inherente, es decir que sin controles la valoración del riesgo es Extrema, y con los mismos controles la valoración es Alta(riesgo residual).2. Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos*



Fuente: Matriz de Riesgos de Seguridad Digital

Grafica No.6 “No disponibilidad de los Sistemas Tecnológicos y los de Información”

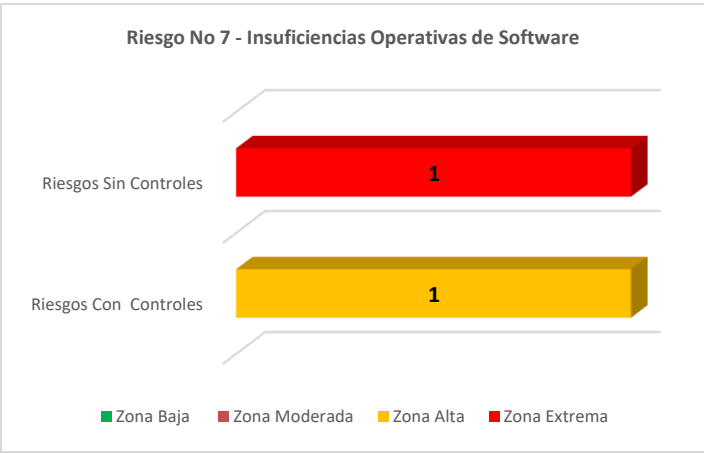
Observaciones Control Interno: *1. Los controles propuestos para bajar la valoración del riesgo residual son los mismos del riesgo inherente, es decir que sin controles la valoración del riesgo es Alta, y con los mismos controles la valoración es moderada (riesgo residual). 2. Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos.*



Fuente: Matriz de Riesgos de Seguridad Digital

Gráfico No.7 “Insuficiencias Operativas de Software”

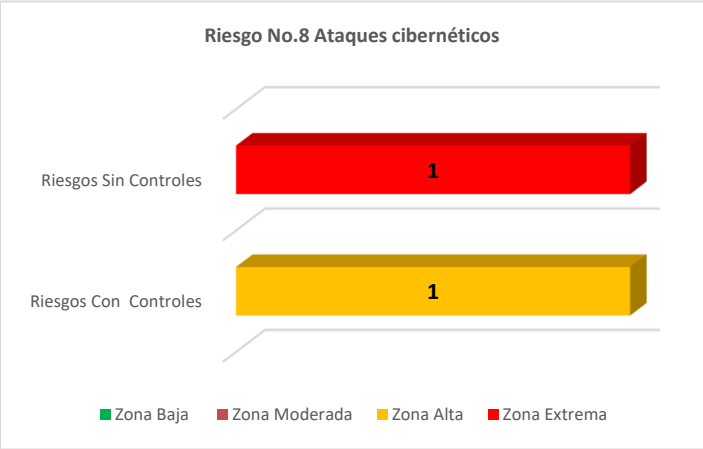
Observaciones Control Interno: *1. Los controles propuestos para bajar la valoración del riesgo residual son los mismos del riesgo inherente, es decir que sin controles la valoración del riesgo es Extrema, y con los mismos controles la valoración es Alta(riesgo residual).2. Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos.*



Fuente: Matriz de Riesgos de Seguridad Digital

Gráfico No.8 “Ataques cibernéticos”

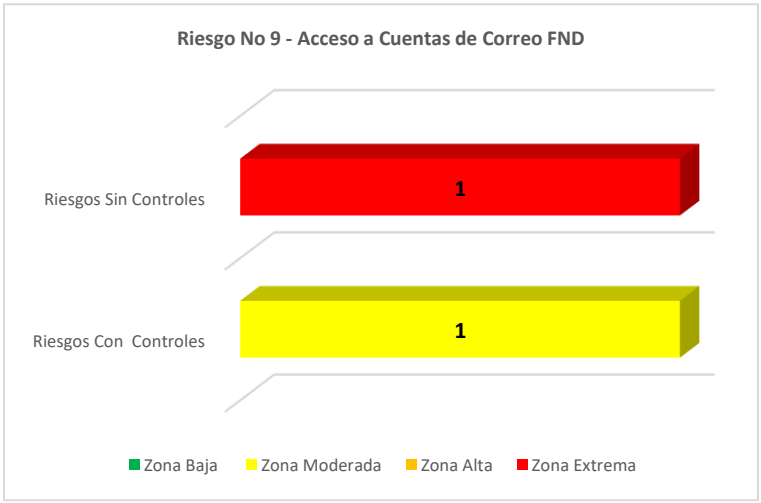
Observaciones Control Interno: *1. Los controles propuestos para bajar la valoración del riesgo residual son los mismos del riesgo inherente, es decir que sin controles la valoración del riesgo es Extrema, y con los mismos controles la valoración es Alta(riesgo residual). 2. Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos.*



Fuente: Matriz de Riesgos de Seguridad Digital

Gráfico No 9 “Acceso a Cuentas de Correo FND”

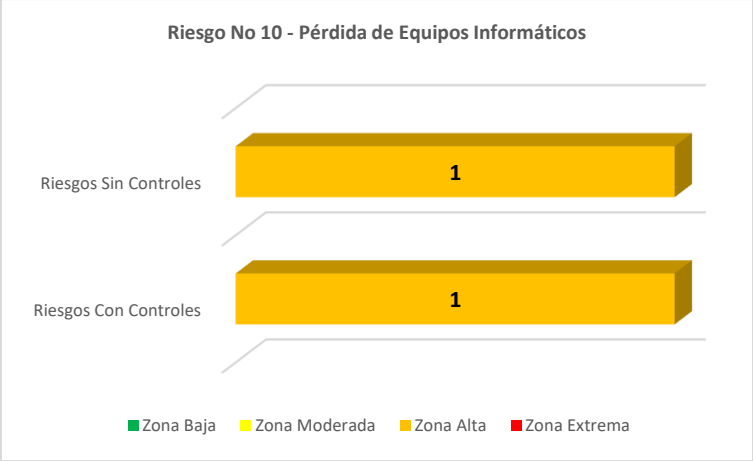
Observaciones Control Interno: *1. No fueron efectivos los controles ya que el riesgo se materializó. 2. Los controles son los mismos en el riego inherente y residual, y sin embargo no son efectivos, 3. Revisar los controles e implementar un plan de choque con el fin de mitigar el riesgo materializado.*



Fuente: Matriz de Riesgos de Seguridad Digital

Riesgo No 10 “Pérdida de equipos informáticos”

Observaciones Control Interno: *Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que el riesgo residual sigue siendo ALTO.*

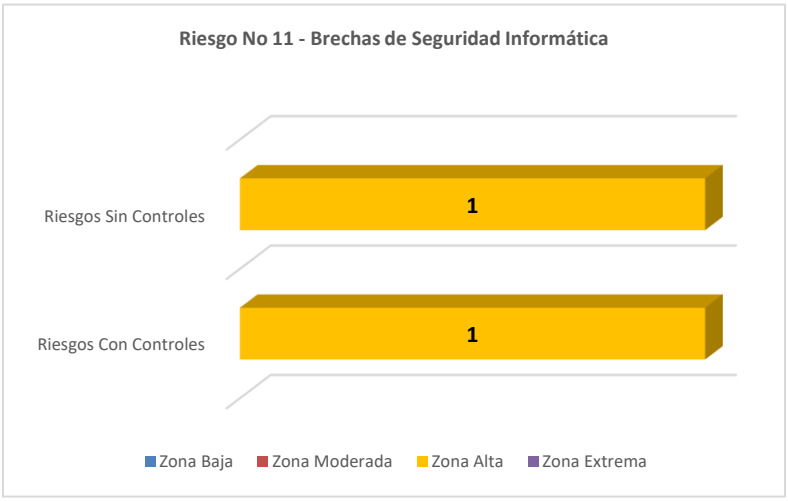


Fuente: Matriz de Riesgos de Seguridad Digital

Riesgo No 11. Brechas de seguridad informática

Observaciones Control Interno: *Revisar los controles existentes, medirlos, controlarlos y crear planes de acción que ayuden a evitarlos o mitigarlos, ya que el riesgo residual sigue siendo ALTO.*

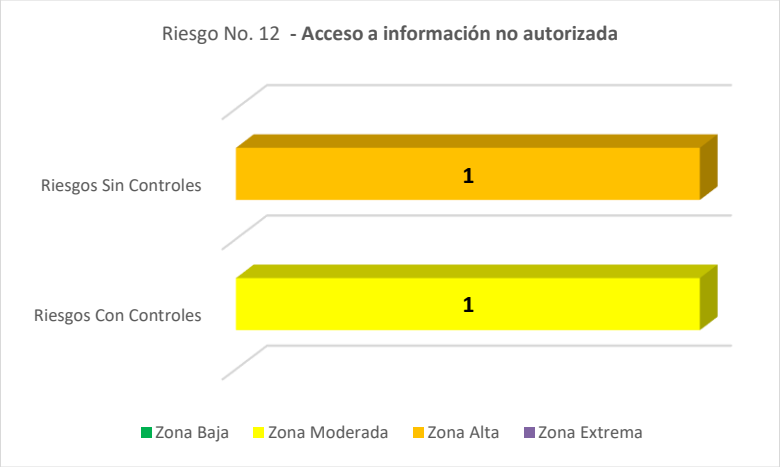
.



Fuente: Matriz de Riesgos de Seguridad Digital

Gráfico No 12. Acceso a Información no Autorizada

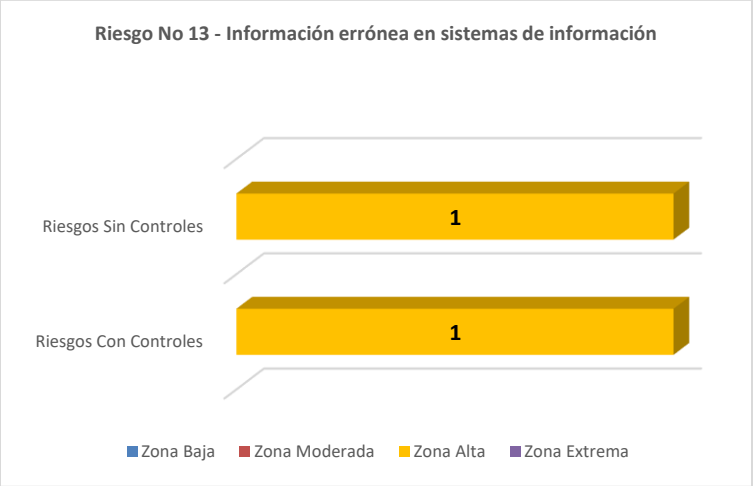
***Observaciones Control Interno**: 1. No fueron efectivos los controles ya que el riesgo se materializó. 2. Los controles son los mismos en el riego inherente y residual, y sin embargo no son efectivos. 3. Revisar los controles e implementar un plan de choque con el fin de mitigar el riesgo materializado.*



Fuente: Matriz de Riesgos de Seguridad Digital

Gráfico No 13. Información errónea en sistemas de información

***Observaciones Control Interno:** 1. No fueron efectivos los controles ya que el riesgo se materializó. 2. Los controles son los mismos en el riego inherente y residual, y sin embargo no son efectivos, 3. Revisar los controles e implementar un plan de choque con el fin de mitigar el riesgo materializado.*



Fuente: Matriz de Riesgos de Seguridad Digital

11. RECOMENDACIONES

1. 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).

2. Analizar y dar tratamiento a las causas que conllevaron al incumplimiento de las actividades de control o acciones preventivas, a fin de que sean superadas para el seguimiento del próximo cuatrimestre.

3. Establecer e implementar acciones de seguimiento por parte de GTE ante la materialización de riesgos, trabajando conjuntamente con la Oficina de Planeación, con el fin de identificar las causas raíz que dieron origen a los mismos; así como de un plan de tratamiento de riesgos con el fin de mitigar y/o disminuir su ocurrencia.

12. CONCLUSION

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 II cuatrimestre del 2022, se materializaron 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 mitigar los riesgos generados en el entorno digital, que se encuentran en **nivel de riesgo alto y extremo y aquellos que se materializaron.**

No Riesgo	Riesgos Materializados
9	Acceso a cuentas de correo FND
12	Acceso a información no autorizada
13	Información errónea en sistemas de información

NOTA: *La dependencia auditada levantará un Plan de Mejoramiento; con base en el presente informe que contiene las recomendaciones y observaciones planteadas por esta oficina, el mismo debe ser remitido según el formato establecido GIO-PD-04-FT-01, dentro de los cinco (5) días siguientes al recibo del presente informe.*

Atentamente

CLARA CONSUELO OVALLE JIMÉNEZ
Jefe Oficina Control Interno

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