Bogotá, NOVIEMBRE 3 de 2022

INFORME FINAL

"AUDITORÍA GESTIÓN DE INCIDENTES Y EVENTOS DE SEGURIDAD DE LA INFORMACIÓN"

TABLA DE CONTENIDO

1. Objetivo

Evaluar la calidad de los controles establecidos en el proceso telemática para establecer la gestión del riesgo y la efectividad de los controles aplicados, si es el caso, realizar recomendaciones encaminadas a coadyuvar al logro de los resultados.

2. Contenido del informe.

2.1. Alcance.

La auditoría se realizará entre el 1 de enero de 2021 y el 31 de Agosto de 2022 al procedimiento "Gestión de incidentes de seguridad de la información", P-3-2-03V2.

2.2. Justificación.

La Oficina de Control Interno, en ejercicio de su función de evaluador independiente, en desarrollo del plan de auditoría 2022, aprobado por Comité de Coordinación de Control Interno, incluyó la auditoría al procedimiento Gestión de incidentes de seguridad de la información

2.3. Criterios.

- P-3-2-03V2, "Gestión de incidentes de seguridad de la información",
- Seguridad y Privacidad de la Información 2022
- Matrices del proceso
- Manuales, Instructivos y demás documentos relacionados con el procedimiento
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías de la Información y las Comunicaciones
- ISO 27001:2013

2.4. Desarrollo de la auditoría.

De acuerdo a lo establecido en la guía de auditorías del DAFP, se realizó la apertura de la auditoría con el coordinador del proceso y con los profesionales que actúan dentro del mismo, se dieron a conocer el plan de auditorías y se solicitó la información que el grupo de auditores requería para adelantar los procedimientos de verificación. Una vez analizada la información se dio inició a la prueba de recorrido, interactuando con los funcionarios que ejecutan las actividades del procedimiento, con la información y el conocimiento adquirido se procedió a elaborar el programa de auditoría.

Con fundamento en la información sobre los activos de información se procedió a realizar un muestreo para aplicar pruebas. Los estimadores estadísticos utilizados para definir el tamaño de muestra fueron:

- Nivel de confiabilidad del 95%,
- Margen de error del 10%,
- Probabilidad del 50%

- Mediante correo electrónico se realizó la solicitud escrita de la información requerida para verificar el cumplimiento del procedimiento:

2.5. Análisis del control

N/A

3. Hallazgos

3.1. Hallazgo Número 1

En el análisis de la Políticas del Sistema de Gestión de Seguridad de la Información se encuentra que contiene la política general, las políticas específicas y los objetivos de la información; sin embargo, no se evidencian soportes para argumentar que la misma es liderada desde la Alta Dirección y obedece a la misionalidad de la entidad; además que está asegurando la integración de los procesos de la organización.

La Norma Técnica Colombiana, NTC-ISO-IEC 27001, en el numeral 5.1, Liderazgo y Compromiso, establece que "La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información".

La situación anterior presenta un riesgo para la certificación del proceso, ya que el incumplimiento de este numeral se considera una conformidad mayor.

3.2. Hallazgo Número 2

Para analizar el tratamiento de los incidentes de seguridad se solicitó el reporte de los tares en donde se informa de los eventos de seguridad de la información durante el período de alcance, se reportaron 1.858 casos. Con un margen de error del 5% y un nivel de confianza del 95% se tomó una muestra de 318 casos, evaluada la información los resultados son los siguientes:

Tabla 1. Análisis de Muestra por Categoría de TAR

Solicitud Nro.	Categoría	Número de veces
11378	Cupo de impresión y copias	97
11380	Privilegios	18
11393	Acceso no autorizado	1
11395	Perfil de usuario	7
11410	Office	6
11411	Fallas	17
11412	Fallas en la generación de bck up	1
11421	Acceso	13
11425	Préstamo sala	42
11442	Orfeo	8
11447	Comunicaciones	11
11450	Control de acceso	9
11453	Equipo de cómputo	27
11468	Infraestructura de red	10
11508	Adulteración de la información	1
11556	Pin de liberación	3

11632	Mouse	6
11682	Cargue de papel	4
11785	Rigthnow	2
11818	Configuración impresora	6
11893	CCTV	1
12129	Modulo	6
12173	Aplicaciones	7
12320	Digiturno	2
12386	Responsabilidades	2
12415	Otros programas	3
12424	Otro	1
12480	Sistema operativo	3
12522	Portátil	2
12695	Teclados	1
12985	Carpeta escáner	1
Total		**318**

Analizando la información solo se presenta una solicitud por acceso no autorizado; al buscar la descripción se encuentra que lo que se requiere es "me brinden los privilegios para el acceso a la carpeta compartida…"; es decir el TAR no corresponde a un caso de seguridad en la información.

Tabla 2: Análisis de Muestra de TAR por tipo de Servicio

Solicitud Nro.	Servicio	Categoría	Descripción
11393	SEGURIDAD DE LA INFORMACIÓN	ACCESO NO AUTORIZADO	Buen día de manera atenta me permito solicitar me brinden los privilegios para el acceso a la carpeta compartida del Grupo COVIN con el fin de realizar consulta para la conciliación de los convenios interadministrativos muchas gracias por su colaboración
11412	SEGURIDAD DE LA INFORMACIÓN	FALLAS EN LA GENERACION DE BCK UP	Buenas tardes, De manera atenta me permito solicitar backup de la información del computador N° 2049500030013 para pasarla al computador N° 2061800010015 el cual se asignó a la funcionaria Erika Limas Herreño. De igual manera hacer traslado del equipo en mención.
11508	SEGURIDAD DE LA INFORMACIÓN	ADULTERACION DE LA INFORMACIÓN	Buenas tardes, De manera atenta me permito solicitar su apoyo, lo anterior teniendo encuentra que intento ingresar a la plataforma de SIIF Nación y cuando doy clic para la firma del token no conecta y salen los mensajes que aparecen en los adjuntos. Agradezco su amable colaboración.

12424	SEGURIDAD DE LA INFORMACIÓN	OTRO	buena tarde solicito comedidamente sea habilitado un puerto USB del computador del usuario Claudia Romero dicha solicitud se realiza por qué se debe descargar la grabación de una audiencia para respuesta a juzgado de manera urgente. agradecemos su colaboración

De acuerdo a la información reportada, en la muestra evaluada se presentaron 4 casos por seguridad de la información; al evaluar la descripción encontramos que ninguno de los casos reportados hace referencia a seguridad de la información.

Con fundamento en lo anterior queda claro que en la entidad, durante el período de alcance de la auditoría no se presentó ningún caso de seguridad de la información; sin embargo es claro que se evidencia un desconocimiento de los usuarios en el Fondo Rotatorio de la Policía de que es un riesgo de seguridad de la información.

3.3. Hallazgo Número 3

En lo que hace referencia a los roles y responsabilidades para la seguridad de la información, la política tiene establecido claramente los actores y niveles de atención para cada caso; no obstante, al verificar la funcionalidad se encuentra que en la práctica no existe segregación de funciones, puesto que el funcionario que realiza las funciones de administrador de la base datos es el mismo que efectúa la evaluación a la modificación de las bases de datos, ingreso de súper usuarios, soporte a las bases de datos y quien ejecuta los log de auditoria.

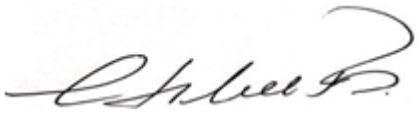
3.4. Hallazgo Número 4

En lo que hace referencia a la continuidad del negocio, la entidad tiene registrado dos causas como posibles generadores del regiego, en el período de tiempo objeto de evaluación se han presentado dos eventos en donde la entidad se ha quedado aislada por impedimentos para acceso a la red de datos, esta situación impide el uso de las plataformas institucionales y del correo electrónico.

4. Conclusión

Una vez aplicada las pruebas de auditoría al procedimiento incidentes y eventos de seguridad de la información encontramos que la entidad técnicamente tiene los controles indicados para realizar la gestión del riesgo del proceso; los controles tecnológicos y el apoyo del CSIR de Policía Nacional corrigen oportunamente las vulnerabilidades que se puedan generar por ataques externos.

No obstante lo anterior; es preciso indicar que la política de seguridad de la información y la gestión misma del proceso se realizan desde la Coordinación responsable del procedimiento; sin evidenciar que esta hace parte de los lineamientos de la Alta Dirección.

Elaboró:	Revisó:	Aprobó:
 **Adm. Emp Carol Liliana Reina Diaz** **Profesionales Oficina Control Interno**  **Apoyo:** **Adm. Emp Vilma Rincón Cepeda** **Técnico para Apoyo Seguridad y Defensa**	 **Economista Omar Antonio Pereira Góez** **Jefe Oficina de Control Interno**	 **Economista Omar Antonio Pereira Góez** **Jefe Oficina de Control Interno**