Agencia Nacional de Infraestructura

Rad No. 20241020096113
Fecha: 2024-06-06->102
FRANCISCO OSPINA RAMIREZ PRESIDENTE
Vicepresidencia de Planeacion Riesgos y Entorno
Anexos: 1 informe en PDF
https://www.ani.gov.co

Agencia Nacional de Infraestructura

MEMORANDO

Bogotá D.C.

PARA: **FRANCISCO OSPINA RAMÍREZ**
Presidente

MIGUEL CARO VARGAS
Vicepresidente de Planeación, Riesgos y Entrono

DE: **LINA LEIDY LEAL DÍAZ**
Jefe Oficina de Control Interno (e)

ASUNTO: Informe de seguimiento especial por incidente de tecnología, presentado en abril de 2024.

Respetados Doctores,

La Oficina de Control Interno, en el mes de mayo de 2024, realizó seguimiento especial por incidente de tecnología, presentado en abril de 2024.

Las conclusiones se describen en el capítulo 6 del informe que se anexa a la presente comunicación, con el fin de coordinar las acciones tendientes a la atención de las recomendaciones realizadas.

Atentamente,

LINA LEIDY LEAL DÍAZ
Jefe Oficina de Control Interno (E)

Anexos: CCDESC_ANEXOS

Proyectó:
VoBo: CCF_DOCTO1
Nro Rad Padre: CCRAD_E
Nro Borrador: CCNRO_BORR 2024-102-0033196
GADF-F-010

COLOMBIA POTENCIA DE LA VIDA

ANI Agencia Nacional de Infraestructura

INFORME DE SEGUIMIENTO ESPECIAL

Por incidente de tecnología, presentado en abril de 2024

OFICINA DE CONTROL INTERNO

2024 JUNIO

CONTENIDO

1. OBJETIVO. 3
2. ALCANCE. 3
3. METODOLOGÍA. 3
4. ASPECTOS RELEVANTES DEL SEGUIMIENTO ESPECIAL 4
5. DESARROLLO DEL INFORME. 4
5.1. Hechos 4
5.2. Gestión 6
a. Primera posible causa identificada 10
b. Segunda posible causa identificada 10
5.3. Estado actual 14
5.4. Otros aspectos relevantes 16
c. Tercera posible causa identificada 21
6. CONCLUSIONES 21
6.1 Resumen del Incidente 21
7. RECOMENDACIONES 24
7.1. Recomendaciones para el proceso de Gestión tecnológica 24
7.2. Recomendaciones para el proceso estratégico (Sistema Estratégico de Planeación y Gestión) 25

1. OBJETIVO.

Evaluar y verificar por parte de la Oficina de Control Interno – OCI el incidente de tecnología del 6 de abril de 2024 identificando las posibles causas, el impacto y demás datos relevantes de acuerdo con la información obtenida y su correspondiente análisis para finalmente emitir las conclusiones y las recomendaciones a que haya lugar con enfoque en riesgos y a la aplicación de controles por parte de los responsables.

2. ALCANCE.

El seguimiento se circunscribe al análisis de la documentación, a las gestiones previas, concomitantes y posteriores a la presentación de la falla del 6 de abril de 2024 y hasta el 30 de mayo de 2024, realizadas por el GIT de Tecnologías de la Información y las Comunicaciones, de acuerdo con los lineamientos establecidos en la Guía de Auditoría basada en riesgos emitida por el Departamento Administrativo de la Función Pública.

3. METODOLOGÍA.

La metodología empleada por la Oficina de Control Interno fue la usualmente aceptada para la elaboración de este tipo de informes de acuerdo con las normas de auditoría, para lo cual se hizo necesario efectuar una planeación y ejecución de trabajo, donde se tuvieron en cuenta los siguientes aspectos:

- **Etapa de Planeación:** Consecuente con la mesa de trabajo realizada con la jefatura de la Oficina de Control Interno, realizada el 15 de abril de 2024, se definieron los objetivos y el alcance del seguimiento y la lista de documentos iniciales a solicitar para llevar a cabo el seguimiento.

- **Solicitud de información**: El día 18 de abril de 2024, mediante correo electrónico se solicitó al GIT de Tecnología la siguiente información:

  - Plan de Contingencia de TI
  - Formato diligenciado de reporte de incidentes CSIRT
  - Documentos relacionados con las gestiones realizadas para la recuperación del sistema
  - Documentos de antecedentes de las gestiones preventivas realizadas
  - Plan de recuperación de TI
  - Los demás documentos que considere relevantes en relación con el tema

- **Entrevista:** El día 22 de abril de 2024, se llevó a cabo reunión virtual a través de la plataforma Teams, con el fin de conocer los detalles del incidente y recabar la información relevante para el cumplimiento del objetivo del seguimiento.

- **Desarrollo del seguimiento:** A partir de la información recibida y la obtenida adicionalmente, se efectuó el análisis correspondiente que permitiera determinar la gestión realizada por el GIT de Tecnología, la gestión del riesgo, el estado actual de la infraestructura y el cumplimiento de la información de los pilares de seguridad (confidencialidad, integridad y disponibilidad).

4. ASPECTOS RELEVANTES DEL SEGUIMIENTO ESPECIAL

El incidente objeto del seguimiento especial por parte de la Oficina de Control Interno se realiza bajo el esquema de líneas de defensa del Modelo Integrado de Planeación y Gestión – MIPG, desarrollado a través del Modelo Estándar de Control Interno – MECI, dentro del cual la OCI desempeña el rol de seguimiento como tercera línea de defensa[1], precisando que le corresponde a la primera línea de defensa (Coordinadores de GIT y Gerentes) la identificación de los riesgos y el establecimiento de los controles necesarios para mitigarlos y a la segunda línea de defensa (Directores de Planeación- Media y Alta Gerencia) Asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces.

5. DESARROLLO DEL INFORME.

5.1. Hechos

De acuerdo con la información obtenida a través de la entrevista y de la documentación recolectada, del incidente tecnológico se tuvo conocimiento por parte de TI* el domingo 7 de abril de 2024 a las 10:00 a.m., a partir de la llamada de un usuario* del Sistema de Gestión Documental Orfeo, quien informa la imposibilidad de ingresar al aplicativo generando aviso de no conexión a la base de datos. En virtud de lo anterior, se le informa al administrador del sistema*.

[1] La función de la auditoría interna, a través de un enfoque basado en el riesgo, proporcionará aseguramiento objetivo e independiente sobre la eficacia de gobierno, gestión de riesgos y Control Interno a la alta dirección de la entidad, incluidas las maneras en que funciona la primera y segunda línea de defensa.

(*) Se omiten nombres por protección de datos personales.

El administrador del sistema hacia las 12:00 p.m., y de manera remota, realiza las primeras acciones de revisión sin encontrar respuesta de ninguno de los sistemas a los que se intentó conectar, evidenciando de manera inmediata una falla general en todos los servicios digitales de la Entidad.

El equipo de TI, desde la mañana del lunes 8 de abril de 2024, realiza inspección física de la infraestructura tecnológica incluyendo los servidores, los servicios electrónicos y las conexiones y realiza las pruebas correspondientes de acceso y operación sin obtener respuestas positivas y como diagnóstico inicial se evidencia una falla en el Volume Group (VG)[2], que dicho en términos prácticos es un servidor de almacenamiento, en el cual tienen su operación las máquinas virtuales (VM)[3] configuradas en la Entidad.

A partir de las variadas pruebas determinan que el primer diagnóstico concentra la falla general en un componente físico de la infraestructura de TI (discos duros Hitachi) que impide el acceso y funcionamiento de los aplicativos locales ORFEO y SINFAD (aplicativos cuyo funcionamiento requieren de servicios locales, tales como, motores de base de datos y código instalados en maquinas locales).

En virtud de lo anterior, se desconectan los 54 servidores (VM) con que cuenta la ANI y se evidencia que los aplicativos que cuentan con servicios en la nube, tales como, ANISCOPIO, Correo electrónico y demás herramientas de Microsoft, funcionan correctamente. De igual manera se determinó que el aplicativo Orfeo no funcionaba desde las 18:30 horas del sábado 6 de abril de 2024.

En conclusión, la falla del sistema se presenta en el servidor de almacenamiento (VG) por falla en alguno o algunos discos duros físicos Hitachi, que como se explicó anteriormente contienen varios discos duros virtuales. Lo anterior fue corroborado a partir del informe técnico de Hitachi.

[2] El VG (Volume Group) permite contar con un número de discos duros virtuales a partir de uno o varios discos duros físicos o particiones, funcionando como una estructura única que permite combinar las capacidades de los discos duros físicos que lo conforman y optimizando el almacenamiento de información.

[3] Una máquina virtual (VM) es un entorno virtual que funciona como sistema informático virtual con su propia CPU, memoria, interfaz de red y almacenamiento, pero se crea en un sistema de hardware físico, ya sea en las instalaciones o no.

5.2. Gestión

De acuerdo con la entrevista al GIT de Tecnología realizada el 22 de abril de 2024 (grabación incluida en los papeles de trabajo y que puede ser consultada) y consecuente con los hechos, el GIT de TI elabora a partir del diagnóstico primigenio un plan de contingencia o estrategia de restablecimiento de los servicios, denominado ***"Plan A"*** discriminado en acciones de tipo físico (hardware) y actividades de tipo lógico (software) lideradas por dos equipos de trabajo.

De acuerdo con el procedimiento GTEC-P-002 "Gestión de incidentes y requerimientos de TI", el GIT de TI debía gestionar el incidente a través de la herramienta para registro de incidentes y requerimientos de TI (GLPI), sin embargo, no se evidencian los soportes que den cuenta de la aplicación rigurosa del procedimiento, para determinar el nivel de criticidad del incidente, ni se advierte el reporte del caso en la herramienta GLPI, lo cual impide validar la trazabilidad.

Ahora bien, en aplicación de la actividad No. 11 del citado procedimiento "Documentar acciones realizadas y solicitar aprobación para escalar a tercer nivel la solución (apoyo a proveedor externo)", se realizó la siguiente acción:

La acción de tipo físico acompañada por el primer equipo de trabajo consistió en contactar al fabricante de los discos duros Hitachi solicitando presencia urgente de un ingeniero de la marca que determinara la gravedad del daño y las actividades resultantes en cuanto a reparación, reemplazo de componentes materiales, recuperación de la información y servicios contenidos en estos discos duros.

El fabricante hace presencia el mismo lunes 8 de abril de 2024 con el objetivo de "*realizar diagnóstico acerca de incidencia presentada sobre la plataforma Hitachi, la cual, el usuario percibe degradación de servicio e indisponibilidad del almacenamiento presentado a un ambiente HyperV*[4]*"* (Informe diagnóstico Hitachi Vantara LLC - abril 2024 - disponible para consulta en los papeles de trabajo).

El ingeniero de la marca emite diagnóstico para los discos duros de referencia VSP G350 y HUS 130 y la HNAS, cuyos apartes más relevantes se copian a continuación, para finalmente concluir de manera sucinta y precisa:

[4] Hyper-V permite crear unidades de disco duro virtuales, conmutadores virtuales y otros dispositivos virtuales, y todos ellos pueden agregarse a máquinas virtuales.

"Inicialmente como resumen de los equipos involucrados en la incidencia, se tiene que los almacenamientos no cuentan con contrato de soporte activo y tanto el almacenamiento VSP G350 como la HNAS que de allí consume capacidad, ambos están con niveles de firmware por debajo de las versiones recomendadas y soportadas por fábrica".

- VSP G350
  - Entitlement expired 12/31/2023
  - No hardware errors
  - Microcode MGA
  - Space 69,73%
- HNAS
  - Entitlement expired 12/31/2023
  - No hardware errors
  - Microcode MGA
  - Space 99,95%
- HUS 130
  - Entitlement expired 12/31/2018
  - End of service life 6/30/2021
  - Unknown hardware errors
  - Unknow Microcode version

"En las revisiones realizadas sobre el equipo VSP G350, se encuentra que existen alertas de External VOL Read Error, lo cual indica que existen inconvenientes sobre el equipo virtualizado".

```
<ht_mail_id_2024040716354379.15430> Error information follows:
_System Type: VSP Gx00v2
_Site ID: 0434213 (HRO), 434213 (Salesforce)
_Unit Name: SAN-VSP-G350
_Location: ANI-P2
_IP Address: 10.1.1.235
_System S/N: 453980
_Microcode: DKCMAIN = 88-08-11-20/00
The following Hitachi VSP G350 errors have been transferred from this site by Hitachi Remote Ops (Hi-Track):
------- SIM 01 Follows: ------------------------------------
SIM:
Type: Device
Reference Code: ff5004
Severity: Moderate
Section: External device error
Location: LDEV =00:00:04
Detail: External VOL Read Error
SIM Timestamp: 2024/04/07 14:53:12
SIM ID: 16208
Action Codes:
Code: 58000000, Parts: TROUBLESHOOT SECTION, Location: SEE MANUAL
Related error ID: 16209
_Error Detail: Time: 2024/04/07 14:53:12; Code: ff5004; Description: External VOL Read Error;
_ErrorSummary: ff5004[1]
SITE_ID: 434213
```

Resumen de errores: ff5004: Pin no leído se produce cuando ya no hay redundancia en un grupo RAID (ejemplo: falla de un solo disco en un grupo RAID RAID5 o falla de doble disco en un grupo RAID6 RAID) y durante la copia de corrección (reconstrucción de paridad) allí es un área en otro disco del grupo RAID que no se puede leer y no existe en paridad. Es pérdida de datos. El pin no leído solo se puede borrar sobrescribiéndolo, una vez que se haya reemplazado todo el hardware marginal. (texto original en inglés extraído del Informe diagnóstico Hitachi Vantara LLC - abril 2024 - disponible para consulta en los papeles de trabajo).

Por su parte, el almacenamiento HUS 130 cuenta con múltiples discos en falla, no cuenta con discos de spare y las paridades dentro de los RAID Groups están siendo afectadas adicionalmente este equipo está en "End of Service Life". Desde julio de 2021 el fabricante no provee servicio de soporte para este producto.

"Teniendo en cuenta esto, se encuentra que el pool 5, donde pertenecen los volúmenes presentados al VSP G350, tiene tres discos en falla, los cuales dos de ellos hacen parte del RAID Group 64 y el tercero al RAID Group 68. De esta manera, el pool está en un estado de "regression" por reconstrucción de sus datos debido a la falla de estos discos, el cual por protección no permite escribir o leer." Es necesario reemplazar el dispositivo.

De acuerdo con el informe en comento el ingeniero realizó las siguientes actividades:

"Actividades realizadas

• Se evaluó en detalle el almacenamiento HUS 130 con el fin de tener alternativas de repuestos para reemplazar las posiciones en falla, sin embargo, el pool al estar formado por discos de 4TB NLSAS, el sistema no cuenta con más discos de repuesto disponibles con las mismas características.

Nota 1: El sistema tiene 6 discos de 4TB en falla. (HUS 4TB SAS 7.2K RPM HDD LFF for CBSL/DBL-Base / Product Code: DF-F850-4TNLC.P)

Nota 2: El sistema tiene 12 discos SAS en falla. (HUS 300GB SAS 15K RPM HDD SFF for CBSS/DBS-Base / Product Code: DF-F850-3HGSSH.P

• Se evaluó la alternativa de suministrar más capacidad desde el sistema HUS 130 en sus pools sin afectación al equipo VSP G350, con el fin de crear un nuevo pool y realizar posteriormente el proceso de volume migration. Sin embargo, el sistema VSP G350 no está permitiendo realizar tareas administrativas que cambien la configuración ya que arroja un error de inconsistencia de Share Memory o de sistema bloqueado".

Finalmente, en el informe el ingeniero de la marca emite sus recomendaciones, transcritas a continuación:

"(…)

- *Se recomienda adquirir los discos fallidos con un tercero. (Este ítem sale del alcance o acompañamiento de parte de fabrica ya que la maquina HUS 130 se encuentra EOSL (End of Service Life) por lo cual no se pueden ofrecer este tipo de componentes).*

- *Realizar el reemplazo de todos los discos que están fallando en el HU130. Esta solicitud tiene como objetivo evitar que, durante cualquier acción, otros discos del HUS130 presenten fallas y vuelvan a poner el ambiente en un estado crítico durante la actividad. (Este ítem sale del alcance o acompañamiento de parte de fabrica ya que la maquina HUS 130 se encuentra EOSL (End of Service Life) por lo cual no se pueden ofrecer este tipo de componentes).*

Nota 1: Como medida proactiva, Hitachi, incluso sin un contrato de mantenimiento para este equipo, buscó en su inventario si hay piezas (discos) para apoyar a ANI en la estabilización del HUS130. Desafortunadamente, no identificamos componentes para este equipo HUS130 que fue descontinuado hace más de 3 años.

Nota 2: El cambio de estos discos no garantiza que el "Pin Slot / Pin track" se remueva y que la data comprometida no se pierda". (Subrayas fuera de texto)

a. Primera posible causa identificada

De acuerdo con lo expuesto en párrafos anteriores, el informe de diagnóstico de la marca permite concluir que el daño, efectivamente, se produjo en tres discos duros de la HUS 130 (Hitachi Unified Storage) y por ello la controladora de discos VSP G350, cuya función principal es coordinar los accesos de lecto-escritura en los discos duros, en su intento por recuperar los discos, generó un bloqueo por protección. Lo anterior permite identificar la primera posible causa identificada, siendo esta, desgaste de materiales por obsolescencia.

b. Segunda posible causa identificada

No se evidencia un profesional a cargo de la infraestructura que tenga dentro de sus funciones el monitoreo de los equipos, al igual que la coordinación de las labores de mantenimiento, actualizaciones y/o reemplazos de los componentes de hardware y software que conforman la infraestructura tecnológica de la Entidad. Lo anterior permite identificar una segunda posible causa, falta de recurso humano.

Continuando con el plan de recuperación, las acciones de tipo lógico realizadas por el segundo equipo de trabajo se enfocaron principalmente en la inspección de los logs[5] de los servidores DELL revisando los registros en búsqueda del detalle de los mensajes de error, corroborando la desconexión de todos los servicios digitales de la Entidad.

Las fallas en los discos duros impactan directamente las 54 máquinas virtuales configuradas en la entidad impidiendo el acceso a los aplicativos tanto locales (ORFEO, SINFAD) como en la nube (ANISCOPIO, MICROSOFT) y la utilización de los servicios al Directorio Activo (validación de usuarios y accesos de red), la conectividad de red (DNS, WIFI).

El equipo de trabajo realiza actividades tendientes a desvincular los volúmenes virtualizados de los discos duros de la HUS 130 permitiendo así el acceso a la información almacenada en las maquinas virtuales, dada la imposibilidad de reemplazar de manera inmediata los discos duros dañados, ya por que no se encuentran en el mercado componentes iguales, así como por que no

[5] Es el registro de las acciones y de los acontecimientos que ocurren en un sistema computacional cuando un usuario o proceso está activo y sucede un evento que está configurado para reportar. Rastro de lo que se está ejecutando sobre la plataforma tecnológica.

se contaba con el tiempo ni el recurso de manera inmediata, se aprovisionó almacenamiento en discos virtuales sin fallas del mismo HUS 130 y allí se migraron las maquinas virtuales para dar inicio a la recuperación de los servicios.

> Aquí resulta relevante aclarar un aspecto técnico importante y es que todos los aplicativos se componen de dos atributos, la plataforma sobre la cual se instala (sistema operativo) y la información (data) que almacena y gestiona de acuerdo con su funcionamiento. Cuando el aplicativo utiliza bases de datos, es necesario contar con motores de bases de datos que permiten realizar las consultas de la data, estos motores u otros requerimientos particulares deben ser instalados en la plataforma para permitir su funcionamiento.
>
> En cadena de lo anterior, es importante precisar que ni la plataforma, ni los sistemas operativos, ni los requerimientos particulares de funcionamiento de cada aplicativo, ni los parámetros de instalación ni funcionamiento se respaldan en backup, en ninguna circunstancia, porque deja de ser eficiente, en virtud a que no es información que cambie constantemente y si representa grandes volúmenes que ocupan el espacio de la información relevante; lo que si debe respaldar con la periodicidad que se considere es la data (información gestionada por los aplicativos).

Dicho esto, es importante destacar que toda la data se encuentra respaldada en la nube de Microsoft y por ello cuenta con toda la seguridad en cumplimiento de los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad.

La importancia de lo anterior radica en el hecho de que, si bien la información se encuentra respaldada, es necesario realizar la reinstalación de los aplicativos en los nuevos discos duros, lo cual conlleva, en algunos casos, a dificultades en la instalación y/o parametrización necesaria para su correcto funcionamiento y es precisamente ahí donde se tomó la mayor parte del tiempo de restauración para la solución del incidente.

Una vez aprovisionados los espacios en los discos duros sin fallas, el equipo de trabajo inició la segunda fase del plan de restablecimiento denominado ***"Plan B"*** consistente en la reinstalación de los servicios de conectividad y Directorio activo, lo cual se realizó con éxito el mismo lunes 8 de abril de 2024, asimismo, reestableció los aplicativos en la nube ANISCOPIO Y OFFICE 365. Sin embargo, la instalación de los sistemas de información On Premise (ORFEO y SINFAD) resultó más complejo, no por la data, que se encontraba respaldada en la nube, sino por las dificultades para la instalación desde ceros tanto del sistema operativo sobre el cual funcionan, como de la parametrización e instalación de los motores de bases de datos.

Enfocados en lo anterior y al no contar en la entidad con especialistas en la instalación y parametrización de los sistemas operativos de Linux y Windows Server, el equipo de trabajo gestionó el acompañamiento de expertos, incluido un ingeniero del Ministerio de Transporte que fue pieza clave en el restablecimiento de los sistemas.

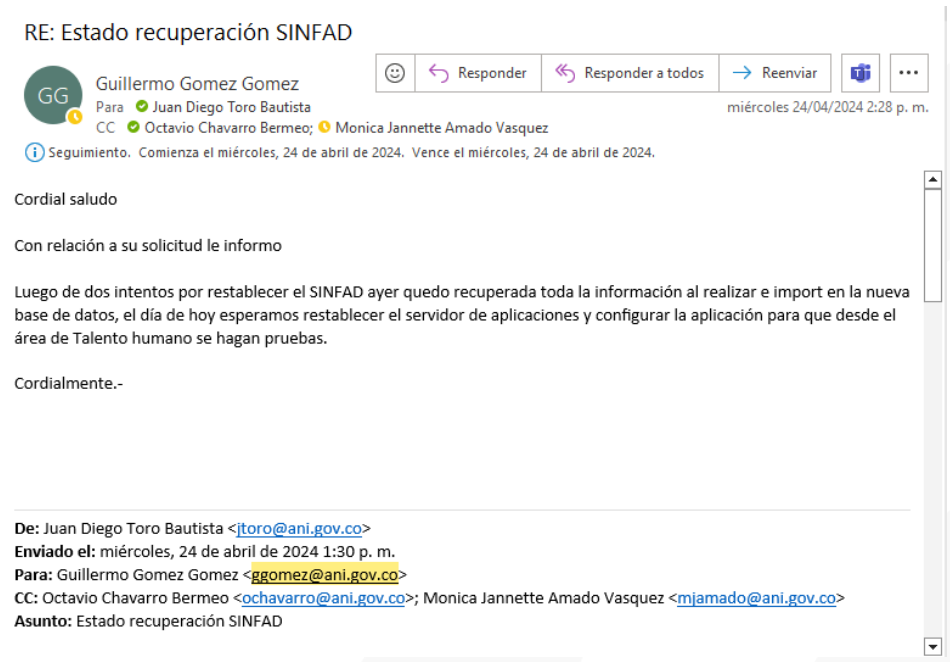
A partir del martes 9 de abril de 2024 y en los días subsiguientes se dedicaron los esfuerzos a la instalación y puesta a punto de los servidores, al igual que los motores de bases de datos, en cumplimiento de la fase 3 del plan de restablecimiento del servicio denominado ***"Plan C"***, cuyas actividades rindieron resultados positivos en la madrugada del jueves 18 de abril de 2024 y ya con el servidor de Oracle (Motor de base de datos utilizado por ORFEO) se procedió a la recuperación del backup desde la nube al nuevo servidor, se realizaron las pruebas correspondientes y la verificación de la información descargada de la nube garantizando el 100% de la data recuperada.

Como resultado de lo anterior el jueves 18 de abril de 2024 a las 6:00 p.m., el sistema de Gestión Documental Orfeo se restableció su funcionamiento y servicio de manera normal y la información se recuperó completamente hasta el sábado 6 de abril de 2024, fecha del último backup realizado[6].

En virtud de, la limitante de personal y a que el mayor impacto en la entidad se generaba por el no funcionamiento del Sistema de Gestión Documental Orfeo, todos los esfuerzos se volcaron a la recuperación de este aplicativo, por lo cual, una vez liberado Orfeo se iniciaron las actividades propias para la recuperación del SINFAD. Que vale la pena resaltar que el respaldo de la copia de seguridad se había revisado y la data incluía el 100% hasta la misma fecha de 6 de abril de 2024.

En entrevista de seguimiento se solicitó al Coordinador del GIT de TI la fecha tentativa para la puesta en funcionamiento del aplicativo SINFAD, frente a lo cual manifestó que lo más probable era el mismo lunes 22 de abril de 2024, sin embargo, al no obtener confirmación, desde este ejercicio se requirió, vía correo electrónico de fecha 24 de abril de 2024, el reporte de la situación. Como respuesta, el mismo 24 de abril se obtuvo:

[6] Backup tipo incremental en la nube de Microsoft, con periodicidad diaria y corte 12:00 a.m.



RE: Estado recuperación SINFAD

Responder | Responder a todos | Reenviar

GG Guillermo Gomez Gomez

Para Juan Diego Toro Bautista

CC Octavio Chavarro Bermeo; Monica Jannette Amado Vasquez

miércoles 24/04/2024 2:28 p. m.

Seguimiento. Comienza el miércoles, 24 de abril de 2024. Vence el miércoles, 24 de abril de 2024.

Cordial saludo

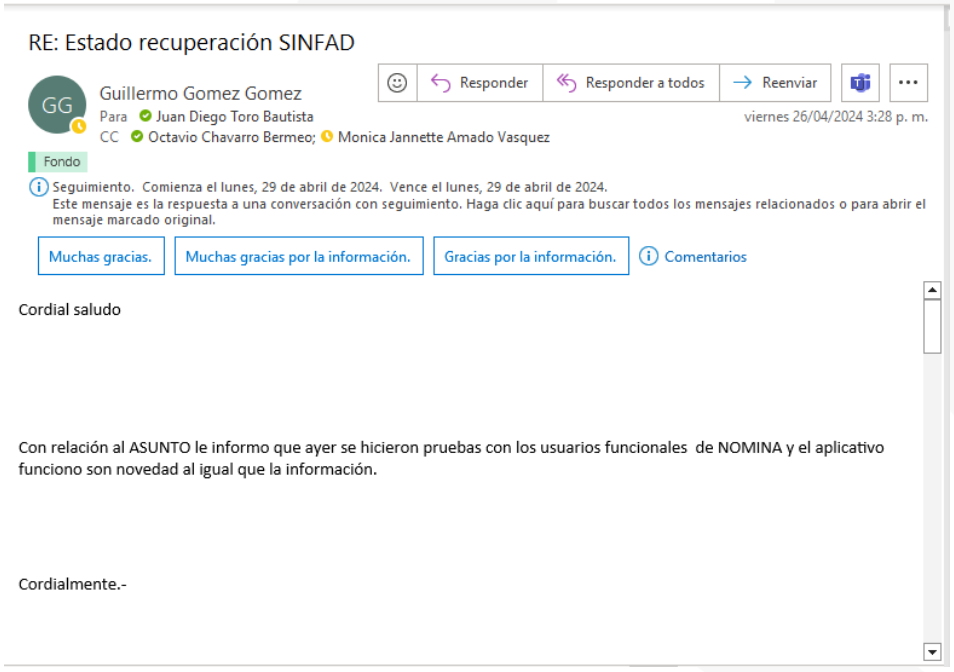
Con relación a su solicitud le informo

Luego de dos intentos por restablecer el SINFAD ayer quedo recuperada toda la información al realizar e import en la nueva base de datos, el día de hoy esperamos restablecer el servidor de aplicaciones y configurar la aplicación para que desde el área de Talento humano se hagan pruebas.

Cordialmente.-

De: Juan Diego Toro Bautista <jtoro@ani.gov.co>
Enviado el: miércoles, 24 de abril de 2024 1:30 p. m.
Para: Guillermo Gomez Gomez <ggomez@ani.gov.co>
CC: Octavio Chavarro Bermeo <ochavarro@ani.gov.co>; Monica Jannette Amado Vasquez <mjamado@ani.gov.co>
Asunto: Estado recuperación SINFAD

Finalmente, el 26 de abril de 2024, nos fue informado el funcionamiento sin novedad y la recuperación del 100% de la información, a través del siguiente correo:



RE: Estado recuperación SINFAD

Responder | Responder a todos | Reenviar

GG Guillermo Gomez Gomez

Para Juan Diego Toro Bautista

CC Octavio Chavarro Bermeo; Monica Jannette Amado Vasquez

viernes 26/04/2024 3:28 p. m.

Fondo

Seguimiento. Comienza el lunes, 29 de abril de 2024. Vence el lunes, 29 de abril de 2024.
Este mensaje es la respuesta a una conversación con seguimiento. Haga clic aquí para buscar todos los mensajes relacionados o para abrir el mensaje marcado original.

Muchas gracias. | Muchas gracias por la información. | Gracias por la información. | Comentarios

Cordial saludo

Con relación al ASUNTO le informo que ayer se hicieron pruebas con los usuarios funcionales de NOMINA y el aplicativo funciono son novedad al igual que la información.

Cordialmente.-

5.3. Estado actual

En este seguimiento especial y desde el rol de usuario final se realizaron, desde el 19 de abril y hasta el 26 de abril de 2024, pruebas de acceso, funcionamiento general y consulta de información de diferentes vigencias corroborando el cumplimiento de los tres pilares de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad.

Ahora bien, teniendo en cuenta que entre el 8 de abril y el 18 de abril de 2024, no se gestionó información a través del Sistema de Gestión Documental Orfeo, se implementó un plan de contingencia por parte de la VGCorp, comunicado a la entidad mediante Circular de fecha 10 de abril de 2024, impartiendo las directrices para la radicación de documentos en atención a la contingencia.

A partir de esta Circular contentiva de los lineamientos para los radicados de entrada (internos y externos), los radicados de salida y memorandos, Resoluciones y Autos, se fueron generando radicados consecutivos temporales como medida de control para que una vez recuperado el sistema se ingresaran en Orfeo.

En consecuencia, una vez reestablecido el Orfeo se solicitó mediante correo electrónico de fecha 24 de abril de 2024 a la Coordinación de Archivo y Correspondencia informar el estado actual de la incorporación en Orfeo de las comunicaciones tramitadas en el periodo de la contingencia (8 al 18 de abril de 2024), adicional se preguntó por las eventuales problemáticas presentadas en materia de respuestas con términos perentorios u otros aspectos detectados en el trámite, obteniendo la siguiente respuesta:

"Al jueves18 de abril se tenía esta cantidad por radicar:

FECHA	INGRESADOS	REENVIADOS	PERSONAS TRABAJANDO	OBSERVACIONES
8/04/2024	288	2	3	FALLA DE ORFEO, NO SE GESTIONO
9/04/2024	402	188	3	SE EMPEZARON HACER REENVIOS
10/04/2024	765	72	3	INSTALACION PARA NUEVOS ID, IMPLEMENTACION NUEVOS FORMATOS - ESTEFANY
11/04/2024	574	56	2	TRABAJO DESDE CASA - DIA SIN AGUA
12/04/2024	535	45	3	CAPACITACION DE 9:00 A.M A 1:00 P.M
13/04/2024	38		0	SABADO
14/04/2024	19		0	DOMINGO
15/04/2024	520	102	3	CAPACITACION ALEXANDRA Y VIVIANA SIN EQUIPO
16/04/2024	589	188	5	
17/04/2024	736	187	5	
18/04/2024	379	193	6	YEIMI DESDE 12:00 P.M
TOTAL	4845	1033		

El viernes 19 de abril se comenzó a radicar así:

1. *Tres personas comenzaron a radicar lo que estaba llegando desde el 18 de abril para evitar acumular pendientes por radicar.*
2. *Un grupo de 4 personas para radicar lo que estaba en la base de datos y una persona para los que estaban pendientes desde el 4 de abril.*
   El resultado en radicación fue 1.165 radicados realizados.

El sábado 20 de abril se adelanto (sic) en media jornada con el mismo personal del viernes y se radicó 508 ya en las horas de mañana hubo una hora sin base de datos en Orfeo.

El lunes 22 de abril se realizó así:

- *Radicación de oficios de salida 1 persona realizó 22 radicados.*
- *Radicación de oficios de entrada desde el 8 de abril ventanilla física 4 personas realizaron 195 radicados, sin imagen, pues el digitalizador de Orfeo no estaba permitiendo imprimir los stiker con los radicados.*
- *Radicación de correos de contactenos@ani.gov.co 11 personas realizaron 880 radicados. Hubo dificultades, dos personas no tenían computador y no pudieron radicar.*

El martes 23 de abril se realizó así:

- *Radicación de oficios de salida 2 personas se realizó 69 radicados.*
- *Radicación de oficios de entrada desde el 8 de abril ventanilla física 3 personas realizaron 125 radicados, se comenzó a digitalizar con stikers*
- *Radicación de memorandos internos 2 personas, se realizó 42 radicados*
- *Radicación de correos de contactenos@ani.gov.co 14 personas 777 radicados, una contratista no tuvo computador, se dio capacitación sobre radicación".*

Con el reporte anterior y con fecha de corte 24 de abril de 2024, se validó por consulta en Orfeo el registro de la información de correspondencia que ingresó a la entidad entre el 8 y 18 de abril de 2024 de acuerdo con el plan de contingencia, establecido por la Entidad, obteniendo los siguientes resultados:

Día	Entradas	Ingresados a Orfeo*	Verificado en Orfeo**
8 al 18 abril	4845		
18-abr		1033	50
19-abr		1165	750
20-abr		508	557
22-abr		1097	750
23-abr		1013	750

Día	Entradas	Ingresados a Orfeo*	Verificado en Orfeo**
TOTAL	4845	4816	2857

De acuerdo con los 2857 radicados se tomó una muestra aleatoria de 250 radicados (ID del 1 al 2000) distribuidos en los 5 días, encontrándose radicación de los 250 revisados. Sin embargo, dado que con corte 24 de abril de 2024 no se evidencian en Orfeo el cargue de los 4816 radicados informados por archivo y correspondencia se hace necesario realizar una nueva verificación.

Por otra parte, en entrevista del 30 de abril de 2024 con el funcionario de nómina se corroboró el correcto funcionamiento del aplicativo SINFAD, sin embargo, manifestó la dificultad para la expedición de los desprendibles de nómina del mes de abril, los cuales tuvieron que ser generados a través de Excel, ya que requería un reproceso en la información y no contaba con el tiempo suficiente desde el 26 de abril de 2024, fecha en la que se restableció el SINFAD.

De acuerdo con esta información y con el fin de validar los avances respectivos, se realizará seguimiento al funcionamiento de los aplicativos ORFEO y SINFAD, así como al registro de las comunicaciones suscitadas en el interregno del 8 al 18 de abril de 2024 ampliando la muestra al 30% y al registro de las novedades de nómina del mes de mayo de 2024. A partir de este seguimiento se generarán correos con el correspondiente reporte, fechas de revisión 14 de junio de 2024 y reporte 18 de junio de 2024 y en caso de ser necesario una segunda fecha de corte 28 de junio y reporte el 3 de julio de 2024.

5.4. Otros aspectos relevantes

Desde el 2022, el GIT de TI ha contemplado en sus iniciativas contenidas en el Plan Estratégico de Tecnologías de la Información – PETI, la actualización de la infraestructura tecnológica de la Entidad.

A finales de 2023 a partir de la obtención de recursos adicionales trasladados de la Vicepresidencia de estructuración por valor de $21 mil millones de pesos se estructuró y suscribió (propuesta para el fortalecimiento de la infraestructura de TI de la Agencia Nacional de Infraestructura de dic de 2023), el 30 de diciembre de 2023, el Convenio Marco Interadministrativo No. 939 de 2023 entre el Ministerio de Transporte, la Agencia Nacional de Infraestructura – ANI y la Corporación Agencia Nacional de Gobierno Digital – AND cuyo objeto y alcance son los siguientes:

CLÁUSULA PRIMERA. - OBJETO: Aunar esfuerzos para desarrollar actividades de transformación digital y ascenso tecnológico que propendan por la interoperabilidad, integración, administración, gestión, actualización y evolución de servicios e infraestructura de tecnologías de la información y comunicaciones – TIC, para el cumplimiento de los objetivos misionales en ejecución de políticas, planes, programas y proyectos de las PARTES; con la asesoría, gestión y apoyo de la Corporación Agencia Nacional de Gobierno Digital- AND.

CLÁUSULA SEGUNDA. – ALCANCE DEL OBJETO: La ejecución del objeto de este convenio incluye todos los aspectos consignados en los anexos derivados que se suscriban para la ejecución del convenio y que se deriven del mismo, y en especial lo relacionado con la infraestructura tecnológica, interoperabilidad, asistencia técnica, integración, administración, gestión, actualización y evolución de servicios de tecnologías de la información y comunicaciones – TIC, con un enfoque sectorial que busque el provecho, optimización y el fortalecimiento de la función administrativa y consecución de los fines estatales en todo el sector; mejorando la eficiencia, la productividad y la calidad de los servicios al ciudadano. Los Anexos Derivados contendrán las especificaciones, alcance, plazo, análisis de riesgo, garantías, valor y soportes requeridos para su suscripción, como lo son estudios previos, análisis del sector y de mercado para su suscripción.

Ahora bien, a partir del convenio derivado No. 02 del Convenio Marco Interadministrativo No. 939 del 2023 celebrado entre la Agencia Nacional de Infraestructura y la Corporación Agencia Nacional de Gobierno Digital – Numeración ANI CI-015-2023 (Publicado en Secop II link: https://community.secop.gov.co/Public/Tendering/ContractNoticeManagement/Index?currentLanguage=es-CO&Page=login&Country=CO&SkinName=CCE), se precisan el objeto y alcance del Convenio así:

CLÁUSULA PRIMERA. OBJETO DEL CONVENIO.
AUNAR ESFUERZOS TÉCNICOS, ADMINISTRATIVOS, TECNOLÓGICOS, OPERATIVOS FINANCIEROS Y JURÍDICOS ENTRE LA AGENCIA NACIONAL DE INFRAESTRUCTURA Y LA AGENCIA NACIONAL DIGITAL PARA EL FORTALECIMIENTO INTEGRAL DE LA CAPACIDAD DE CÓMPUTO, SEGURIDAD DE LA INFORMACIÓN, ALMACENAMIENTO, REDES, VIRTUALIZACIÓN Y CONEXOS DE LA INFRAESTRUCTURA TECNOLÓGICA, PARA PARA SOPORTAR LOS SERVICIOS Y PROCESOS TI DE LA AGENCIA NACIONAL DE INFRAESTRUCTURA EN VIRTUD DEL CONVENIO MARCO 939 – 2023

CLÁUSULA SEGUNDA. ALCANCE DEL PROYECTO
Para cumplir con este propósito la entidad requiere mantener y optimizar todos los activos como los servicios de TI, a través de la renovación, adopción, implementación, actualización, mantenimiento y puesta a punto de la infraestructura tecnológica y sistemas de información, considerando la rápida depreciación y obsolescencia de estos activos tecnológicos, garantizando de esta forma, una línea permanente de eficiencia administrativa y optimización de recursos. Se

han identificado los puntos de atención prioritarios agrupados en los siguientes componentes con su alcance general:

Componente 1: Hiperconvergencia, Almacenamiento y Backup: Suministro, implementación, configuración, prueba, puesta en funcionamiento, de una solución integral de cómputo, almacenamiento, redes y virtualización de la Infraestructura Tecnológica, para la Agencia Nacional de Infraestructura.

Componente 2: Dispositivos de red: Suministro, implementación, configuración, prueba, puesta en funcionamiento, de los dispositivos de red de la Infraestructura Tecnológica, para la Agencia Nacional de Infraestructura.

Componente 3: Seguridad y Gestión de tráfico: Suministro, implementación, configuración, prueba, puesta en funcionamiento, de una solución de seguridad y gestión de tráfico de la Infraestructura Tecnológica, para la Agencia Nacional de Infraestructura.

Componente 4: Acondicionamiento del centro de datos y centro de cableado: Suministro, implementación, configuración, prueba y puesta en funcionamiento, del acondicionamiento centro de datos y centros de cableado y servicio de collocation para la Agencia Nacional de Infraestructura.

(Subrayas fuera de texto)

Aunado a lo anterior, conforme el anexo técnico especificado por la ANI y que forma parte integral del convenio y que se encuentra publicado en SECOP II, se advierte en el numeral 3. Alcance Específico lo siguiente:

- Realizar el suministro de equipos, elementos y/o accesorios que hacen parte de bienes que conforman la solución, no remanufacturados o reparados, en perfectas condiciones y en empaque original de fábrica y con el licenciamiento requerido.Los bienes que hacen parte de la solución no deben aparecer en listas end-of-life ó end-off-sale o end- off-support del fabricante.
- Realizar el suministró de todos los elementos y/o accesorios de interfaz y software opcionales necesarios para la instalación de cada uno de los componentes y de todas las soluciones a adquirir.

(Subrayas fuera de texto)

Aunado a lo anterior, en el numeral 4. Características técnicas de los bienes a suministrar y actividades por ejecutar para cubrir el alcance, del mismo anexo técnico se advierten las diferentes etapas:

4.1. ETAPA 1: Planeación

A los tres (3) días siguientes a la firma del acta de inicio, se deberá hacer entrega y presentación del plan de trabajo en relación con el suministro de los bienes y la implementación de la solución. Plan que como mínimo debe contemplar las actividades por ejecutar contemplando los requerimientos que se plantean en este documento e identificando para cada una de ellas: Fecha de inicio y terminación, responsables, Resultado esperado, aspectos a tener en cuenta, recomendaciones.

Las observaciones y/o recomendaciones que realice la entidad en relación con el plan presentado debe ser atendidas en un término de dos (2) días hábiles, de tal manera que a más tardar trascurridos cinco (5) días hábiles de la firma del acta de inicio, se cuente con el plan de trabajo aprobado.

4.2. ETAPA 2: Suministro de bienes

El suministro de los bienes se debe realizar en un plazo no mayor a cuarenta y cinco (45) días calendario, contados a partir de la suscripción del acta de inicio, dando cumplimiento a las condiciones comerciales/impositivas, normativas y procedimentales que implican la adquisición para la entidad.

4.3. ETAPA 3: Verificación de Características Técnicas

Se verificará que los bienes cumplan con las siguientes características técnicas mínimas requeridas

Pese a lo anterior y como se puede corroborar en correos y solicitudes desde el GIT de TI de la ANI, verbigracia, memorando No. 20246070068011 del 27 de febrero de 2024 dirigido a la Directora de la Corporación AND, donde se solicita el plan de gestión y otros requerimientos en el cual en uno de sus apartes se advierte lo siguiente:

"Es de anotar que se han sostenido dos reuniones de seguimiento en las instalaciones de la ANI en los días 17 de enero y 13 de febrero de 2024 donde por parte la ANI se sugirió un cronograma base el cual a la fecha no ha tenido observaciones, ni a sido complementado y que fue presentado ante el comité técnico de seguimiento el día 25 de enero de 2024 en las instalaciones de la Secretaria General del Ministerio de Transporte.*

Igualmente se requiere que mediante comunicación oficial informe a la supervisión del convenio derivado cual es el equipo idóneo asignado para el desarrollo del proyecto, de acuerdo con la cláusula 5.1.1. y respecto a la cláusula 5.1.11. que dice Designar los representantes de la AND,

quienes harán parte del "comité técnico operativo de ejecución" del convenio que se encargará del seguimiento técnico, administrativo, financiero, contable y jurídico de las actividades del convenio, de acompañar el proceso, y de las gestiones necesarias para alcanzar el éxito del presente convenio.

Por otra parte, la Oficina de proyectos de la ANI solicita le haga llegar la EDT y el Project chárter o acta de constitución del proyecto.

Es muy importante que estos documentos se presenten en los términos previstos para el efecto. Finalmente, esta Coordinación Técnica a cargo de la supervisión del convenio derivado queda a disposición para cualquier asunto relacionado con el tema". (* SIC) (Subrayas fuera de texto)

Comunicación que adicional fue enviada vía correo electrónico el mismo 27 de febrero de 2024.

Sumado a lo anterior, en reunión del 15 de marzo de 2024 en las instalaciones del Ministerio de transporte cuyo objetivo fue: Reunión de supervisión Convenio Marco Interadministrativo 939 de 2023 MT/AND/ANI para realizar seguimiento, vigilancia y control al cumplimiento de los compromisos de las partes del Convenio, que de acuerdo con el acta suscrita en el numeral 3 de compromisos en relación con el Convenio No. 2 se registró lo siguiente:

"Se requiere por parte del ingeniero Guillermo Gómez -supervisor convenio derivado 02/ 2023 infraestructura TI, por favor se brinde respuesta al oficio radicado ANI No.: 20246070068011 de fecha 26 de febrero 2024: se definan los equipos, plan de gestión de acuerdo a prioridades, acta de constitución del proyecto y demás aspectos que permitan garantizar la cabal ejecución del convenio, lo anterior sin perjuicio que se hagan las mesas de trabajo".

Amparado en el Convenio referenciado, el 15 de abril de 2024 el GIT de TI, en aras de la solución del incidente, remite correo a la Corporación AND solicitando:

"(…) En atención a lo anterior y a las necesidades que tiene la Agencia Nacional de Infraestructura de contar con la renovación de soporte de los equipos Hitachi que actualmente hacen parte del inventario de infraestructura tecnológica de la entidad, requerimiento que está plasmado en las fichas técnicas del convenio interadministrativo CI-015-2023, específicamente en la sección de, Renovación numeral 4.3.1.2. relacionado con el almacenamiento. La Agencia nacional de infraestructura se dirige a usted para se (sic) priorice la renovación de soporte y se contrate de manera inmediata.

Los equipos que requieren la renovación de soporte son los siguiente:

Modelo	*Serial*
HNAS 4060	*M4SJKW1545131*
VSP 350	*453980*

Por otra parte se requiere la contratación URGENTE de una empresa que nos proporcione horas de soporte técnico Linux de un ´paquete básico de horas se servicios de infraestructura tecnológica, con la cual podamos apoyarnos en temas de gestión.

Coloco a su evaluación esta propuesta la cual ´puede ser prestada por cualquiera, consistente en 40 horas de diferentes actividades de infraestructura que podríamos requerir para superar esta contingencia.

Bolsa de créditos de servicios = 40 (BICs)".

Frente a estos requerimientos la Corporación AND remite respuesta el 16 de abril de 2024, en el marco del Convenio CI-015-2023, oferta comercial para contratar el soporte técnico y las horas de experto solicitadas para la solución de la contingencia.

c. Tercera posible causa identificada

En el marco del Convenio Marco Interadministrativo 939 de 2023 y Convenio Derivado No. 2, suscrito en diciembre de 2023, cuyo objeto es AUNAR ESFUERZOS TÉCNICOS, ADMINISTRATIVOS, TECNOLÓGICOS, OPERATIVOS FINANCIEROS Y JURÍDICOS ENTRE LA AGENCIA NACIONAL DE INFRAESTRUCTURA Y LA AGENCIA NACIONAL DIGITAL PARA EL FORTALECIMIENTO INTEGRAL DE LA CAPACIDAD DE CÓMPUTO, SEGURIDAD DE LA INFORMACIÓN, ALMACENAMIENTO, REDES, VIRTUALIZACIÓN Y CONEXOS DE LA INFRAESTRUCTURA TECNOLÓGICA, PARA PARA SOPORTAR LOS SERVICIOS Y PROCESOS TI DE LA AGENCIA NACIONAL DE INFRAESTRUCTURA EN VIRTUD DEL CONVENIO MARCO 939 – 2023, a la fecha no se ha superado la etapa No. 1 de planeación por parte de la Corporación AND lo cual resulta en una posible causa de Retraso en la puesta en marcha del Convenio por parte de la Corporación Agencia Nacional de Gobierno Digital – AND.

6. CONCLUSIONES

6.1 Resumen del Incidente

A manera de referencia se resumen los aspectos más relevantes del incidente:

Incidente	Indisponibilidad de la información de los aplicativos ORFEO y SINFAD
Fecha y hora del incidente	6 de abril de 2024 6:00 p.m.
Fecha y hora de inicio	8 de abril de 2024 7:00 a.m.
Fecha y hora de finalización	18 de abril de 2024 6:00 p.m.
Duración	10 días (tomados hasta la recuperación de ORFEO)
Clasificación del incidente	Falla de Hardware y Software
Servicios afectados	- Almacenamiento - Disponibilidad de la información
Procesos afectados	Todos los procesos de la Entidad
Impacto	Alto (Económico y Reputacional)
Riesgos materializados	- Posibilidad de pérdida de la credibilidad y/o recursos de la entidad por interrupción o falla en la continuidad de la prestación de los servicios de T.I. debido a fallas en equipos físicos, ataques o configuraciones que afecten la disponibilidad. -Posibilidad de pérdida de la credibilidad y confianza de los grupos de interés, por afectación a la disponibilidad de la información dispuesta en la plataforma tecnológica para la toma de decisiones, debido a incumplimiento en los acuerdos de niveles de servicios tecnológicos que impidan el acceso y/o utilización de la información
Pérdidas materiales	Discos duros
Pérdidas económicas	Sin determinar
Causas probables	- Desgaste de materiales por obsolescencia - Falta de recurso humano - Retraso en la puesta en marcha del Convenio por parte de la Corporación Agencia Nacional de Gobierno Digital – AND
Solución	- Recuperación de las máquinas virtuales - Aprovisionamiento de espacio en discos duros sin falla - Reinstalación de servidores, servicios, aplicativos - Recuperación de la información respaldada en la nube - Restablecimiento de la funcionalidad total
Tipo de solución	Temporal

Solución definitiva	- Reemplazo físico de los discos duros con falla y los obsoletos - Migración de los servicios y aplicativos a los nuevos espacios de almacenamiento en los discos duros nuevos - Incorporación y revisión del 100% de la información tramitada entre el 8 y 18 de abril de 2024.
Estado actual	Caso Abierto - Aplicativos funcionando sin novedad. - 100% de la Información disponible. - Corroborar la incorporación y trámite de las comunicaciones en el Orfeo recibidas por la Entidad en el periodo de la falla (8 al 18 de abril de 2024)

6.2. Conclusiones generales

- A partir de la falla en el componente de hardware que ocasionó el incidente, las gestiones realizadas por el GIT de TI fueron diligentes y mostraron eficiencia en el uso de los recursos disponibles dado que al final permitió la solución del incidente, sin embargo, no se aplicaron los procedimientos definidos por el GIT lo cual impidió revisar la trazabilidad de las gestiones.

- La revisión de los Logs de auditoría de los servidores permitió determinar que la falla se presentó en el componente físico y a través del informe de la marca Hitachi se corroboró que el daño no estaba relacionado con un ataque de ciberseguridad o la identificación de actos malintencionados o accidentales por parte de terceros internos o externos.

- La información (data) que gestionan los aplicativos de la Entidad se encuentra respaldada en su totalidad en la nube de Microsoft, lo cual representa seguridad y brinda tranquilidad al interior de la Organización. Estas copias de seguridad se hacen de manera incremental y con una periodicidad diaria con corte 12:00 m.

- En el proceso de reinstalación de los servidores y en la migración de la información respaldada en la nube a los nuevos espacios, surtido con el acompañamiento de ingenieros expertos y externos siempre estuvo a cargo y con supervisión permanente de los ingenieros de la ANI a través de “manos remotas”. Lo anterior permite garantizar que la información en ningún momento estuvo expuesta a manipulaciones externas.

- En el periodo en el cual se encontraban fuera de servicio los aplicativos On Premise (ORFEO, SINFAD), la información no estuvo disponible lo cual tuvo como consecuencia la materialización de los riesgos relacionados con la disponibilidad de la información al incumplir el pilar de la disponibilidad de la información de los tres que conforman la triple de seguridad de la información (disponibilidad, Integridad y confidencialidad), sin embargo, la data al estar respaldada en la nube, nunca estuvo en riesgo de pérdida de información o de incumplir los dos pilares restantes de integridad y confidencialidad.

7. RECOMENDACIONES

7.1. Recomendaciones para el proceso de Gestión tecnológica

- Gestionar el reemplazo inmediato y definitivo de los discos duros y realizar el alistamiento, la preparación, instalación de los requerimientos necesarios para finalmente migrar la data a los nuevos dispositivos. El proceso de migración debe ser en paralelo y garantizando la disponibilidad de la información.

- Revisar el procedimiento GTEC-P-002 Gestión de incidentes y requerimientos de TI, categorizando los incidentes ya que a en la revisión del procedimiento, este, está enfocado en incidentes comunes de bajo impacto y no contempla incidentes de alto impacto. A la muestra que el incidente no se gestionó a través de la herramienta para Registro de Incidentes y Requerimientos de TI (GLPI) como lo describe el procedimiento en una de sus actividades.

- Revisar el instructivo GTEC-I-004 Tratamiento de incidentes de seguridad de la información, incorporando un formato para el reporte de incidentes de alto impacto, ya que el instructivo en el numeral 4.2. Reporte del incidente, manifiesta que se genera a partir de un correo electrónico dirigido al buzón de mesa de servicios de la ANI soporte@ani.gov.co. Sin embargo, este correo no se advierte para el incidente objeto de seguimiento.

- Documentar el incidente mediante la elaboración de lecciones aprendidas que permitan actualizar, a partir de la identificación y su tratamiento, incluir novedades en los procedimientos e instructivos con que cuenta el proceso. En revisión del instructivo se advierte que la última actualización data del 30 de julio de 2020 y el procedimiento con fecha del 26 de octubre de 2022.

- Revisar la Política de Seguridad y Privacidad de la Información GTEC-PT-001 incorporando las lecciones aprendidas del incidente y actualizar la versión que data del 28 de mayo de 2020.

- Implementar procedimientos relacionados con:
  - Planes de contingencia y restablecimiento ante daños.
  - Recuperación de la información ante daños.
  - Instalación y parametrización de sistemas operativos y aplicativos.

- Respaldar las llaves de acceso en servidores externos a la Entidad o en la nube en servicios independientes que permitan la recuperación inmediata de las copias de seguridad y no comprometer su utilización cuando solamente se encontraban incluidas en el almacenamiento que falló.

- Implementar almacenamiento redundante (discos espejo) que permitan reducir los tiempos de recuperación ante daños.

7.2. Recomendaciones para el proceso estratégico (Sistema Estratégico de Planeación y Gestión)

- Gestionar con carácter prioritario la contratación de los profesionales y expertos requeridos que permitan cumplir con las necesidades del proceso en materia de infraestructura que cumpla funciones de monitoreo y reportes preventivos que permitan anticiparse a eventuales fallas en los sistemas.

- Con base en el rol de segunda línea de defensa, es necesario revisar la materialización de los riesgos y los controles:

  - Posibilidad de pérdida de la credibilidad y/o recursos de la entidad por interrupción o falla en la continuidad de la prestación de los servicios de T.I. debido a fallas en equipos físicos, ataques o configuraciones que afecten la disponibilidad.

  -Posibilidad de pérdida de la credibilidad y confianza de los grupos de interés, por afectación a la disponibilidad de la información dispuesta en la plataforma tecnológica para la toma de decisiones, debido a incumplimiento en los acuerdos de niveles de servicios tecnológicos que impidan el acceso y/o utilización de la información.

  Con lo anterior determinar la identificación de nuevos riesgos o el robustecimiento de los controles existentes que prevengan la ocurrencia o mitiguen el impacto.

- Escalar a nivel directivo en concurso con la Vicepresidencia Jurídica para forzar a la Corporación Agencia Nacional de Gobierno Digital – AND al cumplimiento del alcance del

Convenio Marco Interadministrativo No. 939 de 2023 y su Convenio Derivado No. 02, el cual reviste gran importancia en estos momentos para materializar la renovación tecnológica que requiere la Entidad.

Realizó verificación y elaboró informe:

Juan Diego Toro Bautista
Auditor Oficina de Control Interno

Revisó y aprobó informe:

Lina Leidy leal Díaz
Jefe de Oficina de Control Interno (e)

(versión original firmada)