AGENCIA NACIONAL DE DEFENSA JURIDICA DEL ESTADO

INFORME DE AUDITORIA A LA GESTIÓN Y RESTAURACIÓN DE COPIAS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN A-P-GTI-04-2023

Diciembre 2023
Oficina de Control Interno
Elaborado Por: Andrés Mauricio Cruz Vargas
Aprobado por: Marcela Villate Tolosa

1. Introducción:

La Oficina de Control Interno de la Agencia Nacional de Defensa Jurídica del Estado, en el desarrollo de su Plan Anual de Auditorias 2022 – 2023, practicó la auditoria a la gestión y restauración de copias de seguridad de los sistemas de información de la entidad entre el periodo junio 2022 a noviembre 2023, con el objetivo de verificar la eficacia y efectividad de la gestión, ejecución y control de los respaldos de la información contenida en la infraestructura tecnológica institucional.

Dicha auditoria se efectuó del 05 al 15 de diciembre de 2023 y sus resultados se presentan a continuación.

2. Limitaciones del informe (Si aplica):

No Aplica

3. Desarrollo del informe:

El análisis realizado por parte de la Oficina de Control Interno al presente informe, se desarrolló tomando como base la Guía GTI-G-06 - Gestión de Respaldo y Restauración de Copias de Seguridad, la cual tiene como objetivo "*Garantizar la correcta gestión, ejecución, control y consideraciones de los respaldos y restauraciones de copias de seguridad para contribuir con la protección y disponibilidad de la información de la Agencia.*"

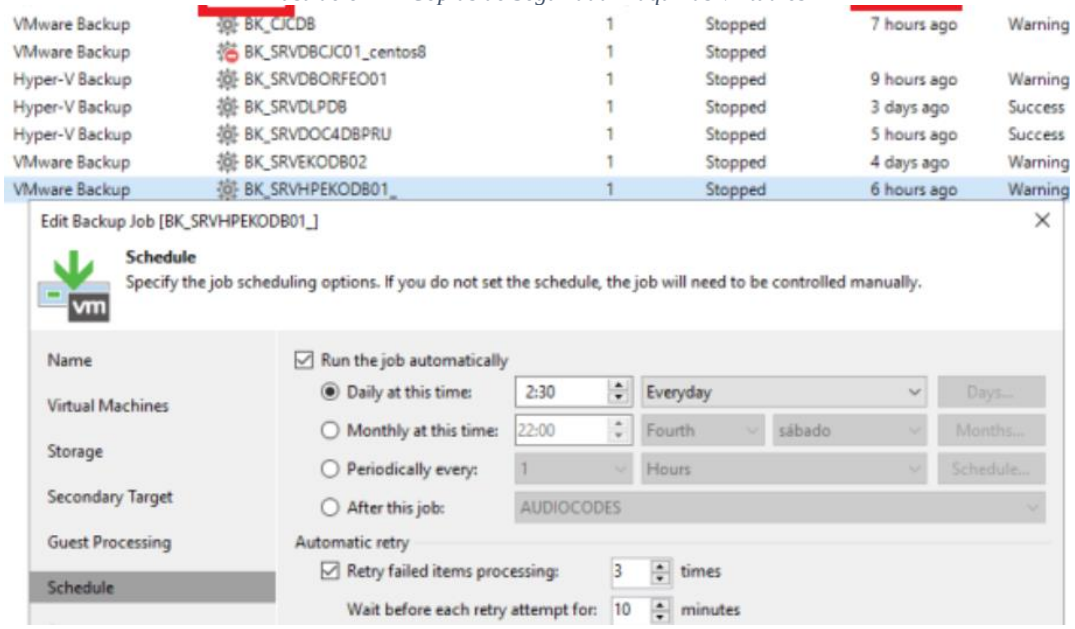
Así las cosas, en indagación preliminar con la OASTI y conforme con la "*Matriz de Activos de Información*", esta Oficina estableció una muestra a criterio del auditor los activos de información misionales con nivel de criticidad alta, obteniendo Ekogui, Orfeo y Storages.

– Copias de Seguridad de Servidores Virtuales

Conforme con lo expuesto en la guía GTI-G-06 numeral 4.2.1 BACKUP DE SERVIDORES VIRTUALES describe: "… *el respaldo de las máquinas virtuales se realiza cada mes …*", por consiguiente, esta Oficina en indagatoria con la OASTI realizó una comprobación y verificación documental que permita obtener evidencia de lo descrito. Dicho esto, esta Oficina evidenció que la OASTI administra una herramienta de copias de seguridad y restauración de datos, llamada de VEEM.

Como resultado de lo anterior, se constató que se realizan copias de seguridad incrementales para los servidores virtuales que almacenan los sistemas de información Ekogui, Orfeo y carpetas compartidas (Ilustración 1), así:

Ilustración 1 - Copias de Seguridad Máquinas Virtuales

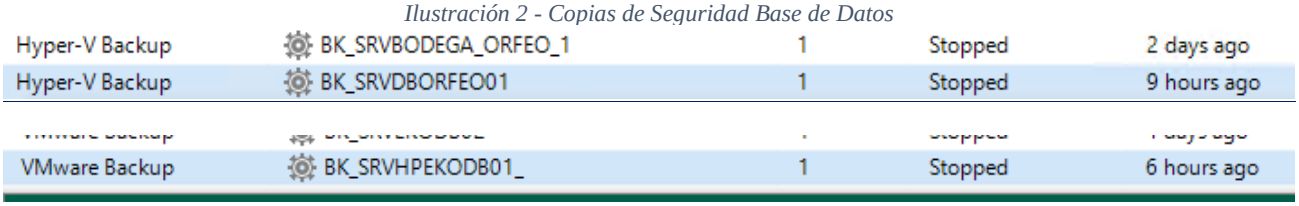


Por otra parte, de acuerdo con la guía GTI-G-06 numeral 4.2.1 BACKUP DE SERVIDORES VIRTUALES, no se identificó el tipo de esquema empleado para estas copias de seguridad. Por lo tanto, esta Oficina **recomienda** realizar la actualización documental en la que se incluya el esquema implementando para este fin.

– Copias de Seguridad de Bases de Datos

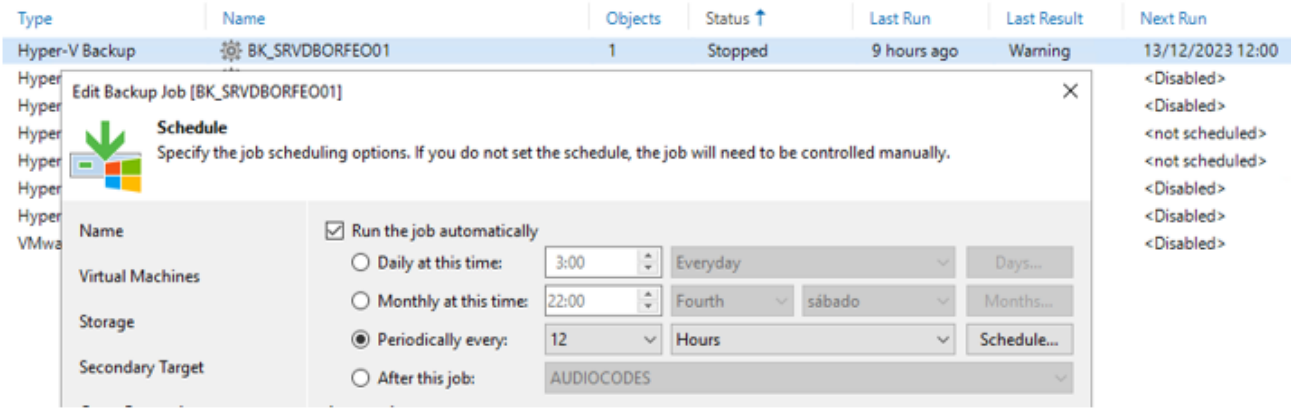
Guía GTI-G-06 numeral 4.2.2 BACKUP DE BASES DE DATOS describe: "... *respaldar las bases de datos de la ANDJE se realizan backups completos diarios* ...", por consiguiente, esta Oficina en indagatoria con la OASTI realizó una comprobación y verificación documental que permitiendo obtener evidencia de las bases de datos de eKogui y *Orfeo (Ilustración 2), obteniendo*:

Ilustración 2 - Copias de Seguridad Base de Datos



Por otra parte, conforme la información suministrada se constató que la OASTI realiza dos copias de seguridad diarias con una periodicidad de 12 horas (Ilustración 3):

Ilustración 3 - Copia de Seguridad diaria

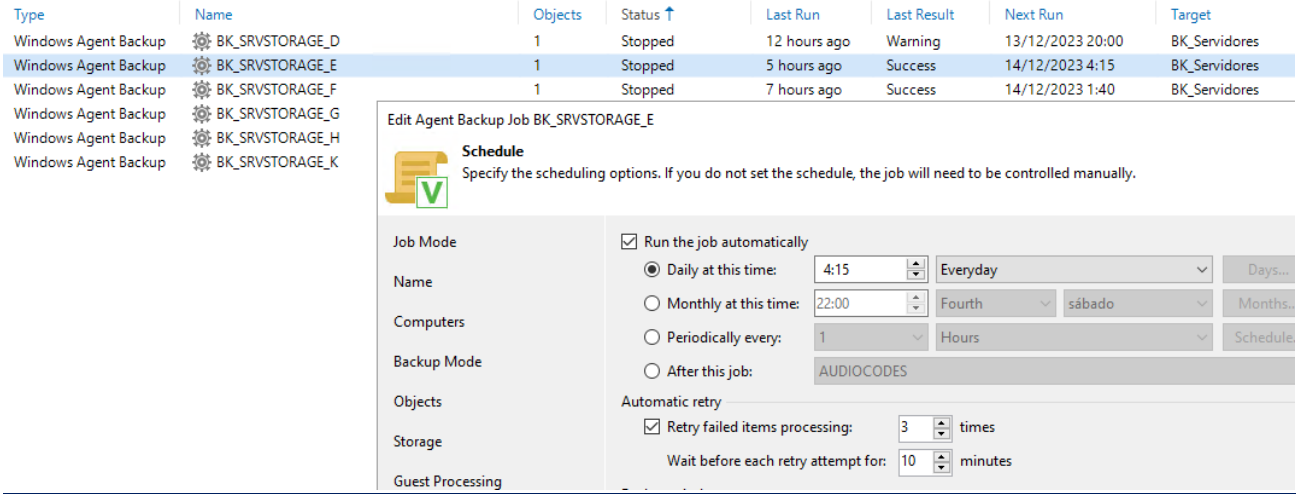


La presente configuración expresa que se realiza una copia de seguridad cada 12 horas y sobre el horario de las 12am/pm, por lo tanto, no se encuentra alineada con lo descrito en la guía GTI-G-06 numeral 4.2.2, toda vez que se indica "*copia diaria*". Así las cosas, esta Oficina **recomienda** validar la configuración descrita, toda vez que puede comprometer la operación de la herramienta, adicional, por buenas prácticas de seguridad, toda copia de seguridad se debe realizar en horarios de no concurrencia.

– Copias de Seguridad de File System

Guía GTI-G-06 numeral 4.2.3 BACKUP DE FILE SYSTEM describe: "... *backups Diferenciales los cuales se realizan de lunes a viernes y un backup completo que se realiza el fin de semana*...", por consiguiente, a esta Oficina la OASTI remitió evidencia de la configuración actual de las copias de seguridad que se tiene para los STORAGE de las carpetas compartidas (Ilustración 4):

Ilustración 4 - Copia de Seguridad File System



– Copias de Seguridad de Estaciones de Trabajo

Guía GTI-G-06 numeral 4.2.4 BACKUP DE FILE SYSTEM DE ESTACIONES DE TRABAJO (PC) describe: "*... respaldar los archivos de los usuarios de la carpeta "Mis Documentos" la ANDJE tienen configurado backups Diferenciales los cuales se realizan tres veces a la semana ....*", por consiguiente, en indagatoria con la OASTI manifestó que dicha configuración se está realizando por medio de la aplicación de OneDrive, la cual se encuentra instalada en cada máquina y los archivos se encuentran sincronizados en la nube en tiempo real.

Por lo tanto, esta Oficina **recomienda** realizar la actualización documental en la que se actualice la forma en la cual se está realizando la copia de seguridad para las estaciones de trabajo (Ilustración 5):

Ilustración 5 - Copias de Seguridad Estaciones de Trabajo (One Drive)

– Custodia de Copias de Seguridad y Periodicidad

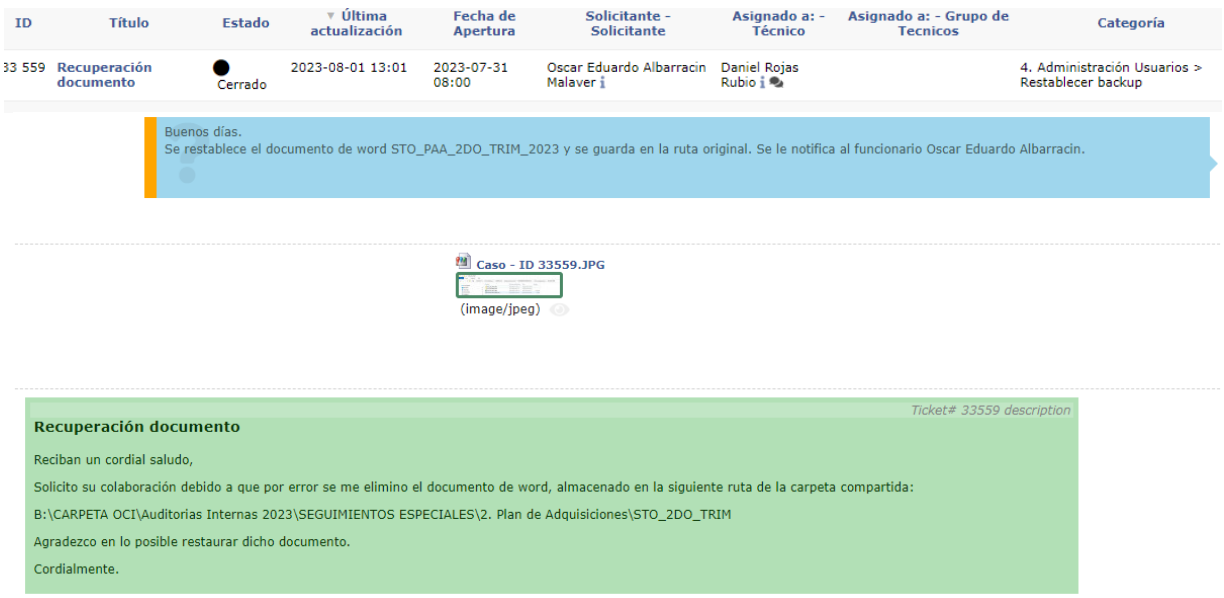
Guía GTI-G-06 numeral 4.2.5 CUSTODIA DE BACKUP Y PERIODICIDAD describe: "… *La ANDJE tiene y debe mantener un contrato activo con un tercero que se encargue de custodiar los backups fuera de las instalaciones de la agencia* …", por consiguiente, la OASTI remitió a esta Oficina el contrato que hacía parte del custodio de las copias de seguridad, el cual finalizo el pasado noviembre 07 del año en curso. Sin embargo, la OASTI ya realizó la gestión de una nueva orden de compra con otro proveedor el 28 de noviembre de 2023, razón por la cual esta Oficina no tiene observaciones a lugar.

– Pruebas de Restauración

Guía GTI-G-06 numeral 4.3.2 PRUEBAS DE RESTAURACIÓN describe que se debe realizar entre los meses de junio a noviembre mediante muestras a cada uno de los servicios: bases de datos (aleatorias), maquinas virtuales (aleatorias), File System (3 usuarios), cintas enviadas a proveedor (aleatorio). Al respecto, la OASTI remitió a esta Oficina, una serie de casos que se llevan por medio de la mesa de ayuda de la ANDJE y de la cual se obtuvo:

- ✓ Caso 33559: Conforme con la información consignada en el presente caso, esta Oficina constató la evidencia de la acción realizada (Ilustración 6):

Ilustración 6 - Caso 33559



- ✓ Caso 33677: Conforme con la información consignada en el presente caso, esta Oficina no constató la evidencia de la acción realizada dentro de la herramienta, por lo tanto, esta Oficina recomienda realizar el cargue de las tareas ejecutadas, con el fin de evidenciar la trazabilidad de las acciones realizadas (Ilustración 7):

Ilustración 7 - Caso 33677

ID	Título	Estado	Última actualización	Fecha de Apertura	Solicitante - Solicitante	Asignado a: - Técnico	Asignado a: - Grupo de Tecnicos	Categoría
33 677	Restaurar archivo en el servidor.	Cerrado	2023-08-03 13:10	2023-08-01 16:37	Jorge Mario Carrasco Ortiz	Wilson Murcia Murcia		9. Servidores Data Center > Backup Servidor

Se realiza la restauración de la carpeta solicitada y se copia la información en el disco local C del equipo del funcionario.

Ticket# 33677 description

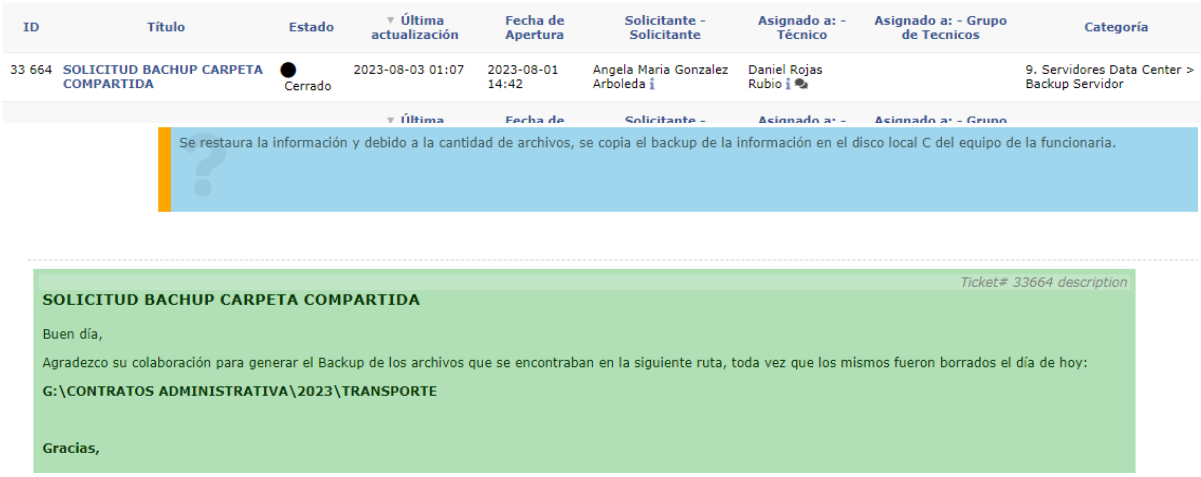
Restaurar archivo en el servidor.

Buenos días.

Se requiere la restaurar un archivo de esta carpeta **/home/notebooks/VALIDACION/21042023_identificacionesRegistraduria** la cual se borro en el servidor 192.168.90.40.

- ✓ Caso 33664: Conforme con la información consignada en el presente caso, esta Oficina no constató la evidencia de la acción realizada dentro de la herramienta, por lo tanto, esta Oficina **recomienda** realizar el cargue de las tareas ejecutadas, con el fin de evidenciar la trazabilidad de las acciones realizadas (Ilustración 8):

Ilustración 8 - Caso 33644



ID	Título	Estado	Última actualización	Fecha de Apertura	Solicitante - Solicitante	Asignado a: - Técnico	Asignado a: - Grupo de Tecnicos	Categoría
33 664	SOLICITUD BACHUP CARPETA COMPARTIDA	Cerrado	2023-08-03 01:07	2023-08-01 14:42	Angela Maria Gonzalez Arboleda	Daniel Rojas Rubio		9. Servidores Data Center > Backup Servidor

Se restaura la información y debido a la cantidad de archivos, se copia el backup de la información en el disco local C del equipo de la funcionaria.

Ticket# 33664 description

SOLICITUD BACHUP CARPETA COMPARTIDA

Buen día,

Agradezco su colaboración para generar el Backup de los archivos que se encontraban en la siguiente ruta, toda vez que los mismos fueron borrados el día de hoy:

G:\CONTRATOS ADMINISTRATIVA\2023\TRANSPORTE

Gracias,

- ✓ Caso 31740: Conforme con la información consignada en el presente caso, esta Oficina no constató la evidencia de la acción realizada dentro de la herramienta, por lo tanto, esta Oficina **recomienda** realizar el cargue de las tareas ejecutadas, con el fin de evidenciar la trazabilidad de las acciones realizadas (Ilustración 9):

Ilustración 9 - Caso 31740

ID	Título	Estado	Última actualización	Fecha de Apertura	Solicitante - Solicitante	Asignado a: - Técnico	Asignado a: - Grupo de Tecnicos	Categoría
31 740	Restablecer servidor 192.168.90.42	Cerrado	2023-05-27 23:36	2023-05-26 08:16	Jorge Mario Carrasco Ortiz	Wilson Murcia Murcia		9. Servidores Data Center > Backup Servidor

Se realiza la restauración del servidor 192.168.90.42, según los solicitado.

Ticket# 31740 description

Restablecer servidor 192.168.90.42

Hola buenos días.

Quisiera solicitar me ayuden con restablecer el backup de servidor 192.168.90.42, el backup que se necesita es el más cercano al 10 de abril que sea posterior a esa fecha.

Saludos.

JMC

Finalmente, si bien se está realizando gestión de las diferentes tareas por medio de casos en la herramienta dispuesta para tal fin, es importante anexar la evidencia del cumplimiento con lo solicitado. Por lo tanto, esta Oficina **recomienda** realizar el cargue de las tareas ejecutadas, con el fin de evidenciar la trazabilidad de las acciones realizadas.

4. Conclusiones:

La Oficina de Control Interno en cumplimiento de sus funciones de revisión y verificación, realizó la revisión de la información recibida, obteniendo como resultado que actualmente la ANDJE esta generando las copias de seguridad y restauración de las mismas conforme lo establecido en la Guía GTI-G-06 - Gestión de Respaldo y Restauración de Copias de Seguridad.

Por otra parte, esta Oficina recomienda:

- ✓ Conforme la guía GTI-G-06 numeral 4.2.1 BACKUP DE SERVIDORES VIRTUALES, se **recomienda** realizar la actualización documental en la que se incluya los esquemas implementados para las copias de seguridad.
- ✓ Conforme con la información consignada en la herramienta de gestión de casos para la mesa de ayuda, esta Oficina **recomienda** realizar el cargue de las tareas ejecutadas, con el fin de evidenciar la trazabilidad de las acciones dispuestas.

Para constancia se firma en Bogotá D.C., a los 19 días del mes de diciembre del año 2023

_____

MARCELA VILLATE TOLOSA
Jefe de la Oficina de Control Interno (E)
Nota. Los anexos al presente informe hacen parte integral.

Anexo No. 1 (si se requiere)

Informe de Auditoria a la Gestión y Restauración de Copias de Seguridad de los Sistemas De Información

Especificaciones de la auditoria Informes de ley o Seguimiento:

- **Criterios:**
  - Ley 1581 de 2012. disposiciones generales para la protección de datos personales.
  - Ley 1712 de 2014. Ley de Transparencia.
  - Ley 1955 de 2019 Plan nacional de desarrollo 2018-2022 – Art.147 Transformación digital Art. 148 Gobierno digital como política de gestión.
  - Decreto 1244 de 8 de octubre de 2021 creación de la Oficina Asesora de Sistemas y Tecnologías de la información en la Agencia
  - Decreto 1008 de 2018, el cual modificó el Decreto 1078 de 2015, en su artículo 2.2.9.1.1.3 definió la seguridad de la información como principio de la Política de Gobierno Digital.
  - Decreto 1244 de 8 de octubre de 2021 creación de la Oficina Asesora de Sistemas y Tecnologías de la información en la Agencia.
  - Manual de Gobierno Digital - MinTic
  - Guía para la administración del riesgo y el diseño de controles en entidad públicas
  - Modelo de Seguridad y Privacidad de la Información – MinTic
  - NTC ISO/IEC 27001
  - Demás normatividad interna y externa aplicable

- **Plan de muestreo:**

La muestra se determinó mediante muestreo aleatorio simple, en donde se verificó la información:

TIPO DE INFORMACION	IDENTIFICADORES
Activos de Información	➢ Matriz de Activos de Información

- **Documentos Examinados:**
  - Documentos asociados al proceso

- **Carpetas compartidas**
  - No Aplica