ANALISIS Y RECOMENDACIONES ANTE LA FALLA DEL SERVIDOR PATHFINDER

El GIT de Control Interno en su función de analizar y evaluar, en coordinación con las dependencias de la entidad, los criterios, métodos, procedimientos, indicadores de eficiencia, eficacia y economía, para evaluar la gestión y promover adopción de los correctivos correspondientes, considera pertinente pronunciarse en relación al manejo de archivos en el servidor Pathfinder de la Contaduría General de la Nación, administrado por el GIT de Apoyo Informático.

Este informe pretende analizar los aspectos más relevantes y la gestión de la problemática por perdida de información y fallo en el servidor Pathfinder que presta el servicio de almacenamiento de archivos en las diferentes estructuras de la Contaduría. De igual manera realizar las respectivas recomendaciones en pro de la mejora continua y la satisfacción del cliente.

A continuación se presentan los aspectos que informa el GIT de apoyo Informático en relación al servidor Pathfinder en su manejo de archivos:

1. INFORMACION TÉCNICA DEL MANEJO DEL SERVIDOR PATHFINDER

A. Problemas en PATHFINDER:

1. Debido a que en el momento que se realizaba el BACK UP diario del servidor hubo un fallo por falta de espacio en los discos donde se guarda el respaldo y que también contiene información, debido a esto la máquina virtual fallo y se perdió parte del backup que se realiza diariamente.
2. Por falta de espacio se realiza un back up diario y al siguiente día se sobrescribe la información, además se tiene unos Snapshot Automáticos en el sistema (restauración del sistema en un punto determinado) pero debido al fallo solo se pudo restaurar hasta la fecha de Marzo.

B. Alternativa de solución:

3. Se viene adelantando tareas con el administrador del servidor Samuel Valero junto con un técnico experto representante del proveedor de servicios de mantenimiento del Blade, realizando operaciones de recuperación de la última configuración e información del servidor virtual PATHFINDER disponible.
4. Recomendaciones para uso de Pathfinder

Recomendaciones para uso de PATHFINDER

Juan David Gómez Botero <jdgomez@contaduria.gov.co> 13 de mayo de 2014, 16:25
Para: Contaduría General de la Nación <todoscgn@contaduria.gov.co>

Cordial Saludo

Funcionarios y Colaboradores

Quiero informar algunas recomendaciones para el uso de la herramienta PATHFINDER con el fin optimizar el rendimiento de los equipos y salvaguardar la información de importancia para el desempeño de sus funciones.

Para el almacenamiento de PATHFINDER, los grupos internos de trabajo o líneas deben realizar un Backups de información semanal mensual o diario si es necesario. Cada funcionario y colaborador es responsable de su información, por tal razón se debe tener una copia de respaldo en el momento en que el sistema falle, para que las labores continúen normalmente.

Alternativa de copia de respaldo local

Las copias deben traer otros beneficios, los grupos deben realizar mensualmente depuración de sus carpetas en PATHFINDER, existe información que se ha remplazado o no es funcional y puede ser eliminada, dando así mas espacio para el almacenamiento de nuevos archivos.

Por otra parte, el PATHFINDER se usa solo para información de la Contaduría General de la Nación, solo se almacenan archivos que tengan que ver con la labor, este almacenamiento debe ser solo para los archivos importantes, de manejo compartido ,y terminados o en firme, ya que los espacios de los discos están cumpliendo con su capacidad de almacenamiento.

Alternativa Google Drive

Para realizar Backups en los en quipos si es el método que quieren usar los grupos, se adjunta protocolo para realizar la copia y si desean otros métodos como Google Drive de Backups el GIT de informática los guiara y capacitara si es necesario. **Mesa de Servicio Ext. 633**

Cordialmente.

Juan David Gómez Botero
Coordinador
GIT de Apoyo Informático
jdgomez@contaduria.gov.co
Calle 95 No 15 - 56, Código Postal: 110221
PBX 492 6400 EXT. 115

C. Aspectos relevantes:

5. El proceso de backup de los equipos está basado en la política de copias de respaldo de calidad que se encuentran en el archivo GTI03-POL01 de SIGI.
6. Debido a la división del centro de cómputo en dos (Calle 74 y Calle 95), se viene realizando un plan de mejoramiento interno con una modificación del mismo ya que la política actual no es posible implementarla en el centro de datos de la entidad (Calle 95) por falta de una librería de cintas operativa que permita grabar los backups a cintas.
7. Actualmente se tiene una librería de backup en la calle 74 que respalda toda la información misional de la entidad, y se realiza diariamente.
8. Debido a la obsolescencia de los equipos que soportan este repositorio de datos se informó por correo electrónico el día 13 de Mayo de este año el uso de PATHFINDER (Adjunto archivo con la información) que la información que reposa es responsabilidad de cada funcionario por lo tanto se deben realizar backups diariamente, también se adjuntó un manual con la explicación para realizar dichas copias

D. Política de seguridad informática

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA CGN

La Contaduría General de la Nación busca preservar la confidencialidad, disponibilidad e integridad de su información, protegiéndola contra amenazas internas, externas, accidentales o deliberadas, mediante la implementación de buenas prácticas tendientes a reducir los riesgos identificados. Así mismo, busca garantizar que todos los requerimientos normativos y legales aplicables a la información se cumplan; que existan mecanismos de concientización en temas de seguridad para los usuarios; que los incidentes de seguridad sean reportados e investigados; y que se propenda por la continuidad del funcionamiento de la Contaduría General de la Nación.

5.1.9 Soporte primario para la Seguridad de Información

El GIT de Apoyo Informático debe facilitar la administración y desarrollo de iniciativas sobre seguridad de información. El GIT de Apoyo Informático deberá proveer dirección y experiencia técnica para asegurar que la información de la Contaduría General de la Nación se encuentre protegida apropiadamente. Esto incluye considerar la confidencialidad, la integridad y la disponibilidad de la información y de los recursos informáticos que la soportan.

Los usuarios son responsables de familiarizarse, observar y cumplir las políticas de seguridad de información, las dudas que puedan surgir alrededor de éstas deben ser consultadas al GIT de Apoyo Informático de la entidad.

5.1.10 Revisiones de seguridad en sistemas de Información

Al menos una vez al año la Contaduría General de la Nación debe efectuar las pruebas necesarias para evaluar el cumplimiento de las diferentes políticas de seguridad, lo mismo que para verificar el cumplimiento de los estándares de configuración en las diferentes plataformas técnicas e instalaciones de tecnología de información. Anualmente se realizará la revisión y actualización de las políticas establecidas, con el fin de asegurar la suficiencia, conveniencia y eficacia.

6.9 Reportes de incidentes de seguridad de información POLITICA DE SEGURIDAD

Se entiende por incidente en la plataforma informática, cualquier evento que ponga en riesgo la integridad, disponibilidad, confiabilidad, veracidad y consistencia de la información de la CGN.

Todo el personal de la Contaduría General de la Nación debe estar vigilante respecto a los incidentes o debilidades de seguridad (incluyendo fallas en el sistema, pérdida del servicio, errores resultado de datos del negocio incompletos o inadecuados, rompimiento de la confidencialidad). Si se detectan estos incidentes o debilidades de seguridad, deben ser reportados en forma inmediata al encargado de la seguridad

6.11 Respaldo de datos

a) Los servidores públicos, contratistas y terceras partes que trabajan para la Contaduría General de la Nación deben establecer con el GIT de Apoyo Informático los lineamientos para el respaldo, almacenamiento y destrucción de la información sensible, valiosa o crítica de la entidad, minimizando el riesgo de pérdidas de información o el mal uso de ésta.

b) Los procedimientos de almacenamiento en medios magnéticos y ópticos (dispositivos de almacenamiento USB, CD, cintas magnéticas, etc.), deben asegurar que la información sensible, crítica o valiosa almacenada por periodos prolongados de tiempo, no se pierda por deterioro. Por ejemplo, el GIT de apoyo informático debe efectuar copias de los datos en medios de almacenamiento diferentes, si el medio de almacenamiento original muestra señas de deterioro.

c) Si se otorga a los usuarios finales la capacidad de restaurar sus archivos propios, no deben tener los privilegios para restaurar los archivos de otros usuarios o examinar qué archivos han sido respaldados por otros usuarios.

d) Toda la información sensible, valiosa o crítica residente en los sistemas de cómputo de la Contaduría General de la Nación debe respaldarse periódicamente.

E. Políticas de copias de respaldo

El documento de políticas Incluye ítems de ubicación, almacenamiento, esquema, periodicidad, vida útil de los medios de respaldo los cuales se pueden observar en el documento y se hace referencia a la Generalidad en la que dice:
“Hacer copia de respaldo, se refiere a guardar información en un dispositivo de almacenamiento de tal forma que este pueda restaurar un sistema o grupo de archivos después de una pérdida o daño de información.

La copia de seguridad es útil por varias razones:

1. Para restaurar un ordenador a un estado operacional después de un desastre (copias de seguridad del sistema)
2. Para restaurar un pequeño número de archivos después de que hayan sido borrados o dañados accidentalmente (copias de seguridad de datos)”

F. Matriz de riesgos

La matriz muestra varios riesgos que evidencian causas y efectos de perdida de información **con causas** como la falta de estimación de recursos, aparición de imprevistos frente a nuevas necesidades, no disponibilidad de recursos técnicos, falta de mantenimiento con regularidad, mantenimientos inapropiados e inoportunos, obsolescencia en Hardware y Software, desbordamiento de la capacidad de los

recursos, falta de aplicación del seguimiento y control, falta de cultura en seguridad de la información, falta de plan de implementación de los controles y procedimientos de revisión periódicos, falta de capacitación y sensibilización a todo el personal con efectos de falla en la prestación de soporte a nivel de software y hardware, problemas en la disponibilidad de los servicios, plataforma tecnológica desactualizada, sobrecostos por efectos secundarios, usuarios insatisfechos por la prestación de los servicios, perdida de información, mal funcionamiento de hardware, malas proyecciones de capacidad y uso de los recursos

2. ANALISIS

Estudiada la información anterior dada por el GIT de Apoyo Informático de la problemática presentada desde el 22 de Julio de 2014 y que venía de tiempo atrás (aproximadamente en el mes de Mayo de 2014), en relación a las fallas en el servidor Pathfinder (que contiene almacenado archivos de las diferentes dependencias de la Contaduría), las diferentes políticas y riesgos relacionados con el manejo de la información y el manejo que se le ha dado al mismo, se observan las siguientes deficiencias susceptibles de mejora:

- Fallo por falta de espacio en los discos
- Falla en la máquina virtual
- Sobrescribir información de backup por falta de espacio
- Snapshot automáticos con fallas
- Requerimiento de apoyo técnico experto por el tipo de falla
- Alternativa de backup locales y google drive sin espacio suficiente
- Responsabilidad delegada y distribuida
- Backup basado en políticas de copias de respaldo que no se cumplen
- Falta de librería de cintas operativa en la sede de la Calle 95
- Obsolescencia de los equipos
- La información que reposa es responsabilidad de cada funcionario
- Políticas de seguridad aprobadas con textos como:
    - “Implementación de buenas prácticas tendientes a reducir los riesgos identificados”
    - “Incidentes de seguridad reportados e investigados”
    - “El GIT de Apoyo Informático deberá proveer dirección y experiencia técnica para asegurar que la información de la Contaduría General de la Nación se encuentre protegida apropiadamente. Esto incluye considerar la confidencialidad, la integridad y la disponibilidad de la información y de los recursos informáticos que la soportan “
    - “Al menos una vez al año la Contaduría General de la Nación debe efectuar las pruebas necesarias para evaluar el cumplimiento de las diferentes políticas de seguridad”

- “Anualmente se realizará la revisión y actualización de las políticas establecidas”
- “Se entiende por incidente en la plataforma informática, cualquier evento que ponga en riesgo la integridad, disponibilidad, confiabilidad, veracidad y consistencia de la información de la CGN”
- “Todo el personal de la Contaduría General de la Nación debe estar vigilante respecto a los incidentes o debilidades de seguridad (incluyendo fallas en el sistema, pérdida del servicio, errores resultado de datos del negocio incompletos o inadecuados, rompimiento de la confidencialidad). Si se detectan estos incidentes o debilidades de seguridad, deben ser reportados en forma inmediata al encargado de la seguridad”

- Los servidores públicos, contratistas y terceras partes que trabajan para la Contaduría General de la Nación deben establecer con el GIT de Apoyo Informático los lineamientos para el respaldo, almacenamiento y destrucción de la información sensible, valiosa o crítica de la entidad, minimizando el riesgo de pérdidas de información o el mal uso de ésta.
- Los procedimientos de almacenamiento en medios magnéticos. Por ejemplo, el GIT de apoyo informático debe efectuar copias de los datos en medios de almacenamiento diferentes, si el medio de almacenamiento original muestra señas de deterioro.
- Si se otorga a los usuarios finales la capacidad de restaurar sus archivos propios, no deben tener los privilegios para restaurar los archivos de otros usuarios
- En la política de copias de respaldo se resalta que la copia de seguridad es útil por varias razones:
  - Para restaurar un ordenador a un estado operacional después de un desastre (copias de seguridad del sistema)
  - Para restaurar un pequeño número de archivos después de que hayan sido borrados o dañados accidentalmente (copias de seguridad de datos)”
- La matriz de riesgos, muestra varios riesgos que evidencian causas y efectos de perdida de información
- El hecho de estar en los equipos locales también trae diferentes riesgos como son: la pérdida de información, daño en los discos duros, personal que se va de la entidad y elimina archivos o no los comparte, la no realización de copias de respaldo por parte de los usuarios por olvido.

3. RECOMENDACIONES

Los aspectos anteriormente destacados muestran falencias relacionadas con la problemática dada por el GIT de Apoyo informático y se refleja en los diferentes grupos de trabajo de la Entidad, en cumplimiento de la norma NTC-ISO 27001 de seguridad de la información y la información y comunicación requerida en el modelo técnico MECI 2014, donde el eje transversal busca satisfacer la calidad y seguridad de la información

y optimizar el uso de los recursos disponibles incluyendo aplicaciones, información e infraestructura que permita una medición objetiva de la información y la comunicación utilizada por los diferentes procesos, este GIT hace las siguientes recomendaciones:

a. Evaluar la renovación tecnológica teniendo en cuenta los incidentes y fallas de la plataforma
b. Proyectar la adquisición de la plataforma tecnológica en relación a:
    - Crecimiento de información de la CGN a mediano y largo plazo
    - Incluir todos los componentes necesarios para su completa aplicación y respaldo (ej.: falta de librería para backup).
    - Tener en cuenta la renovación tecnológica para evitar los niveles de obsolescencia de los equipos.
c. Planear los mantenimientos técnicos (preventivo y correctivo) con la periodicidad que permitan mantener los componentes tecnológicos en buen estado para mantener la operación permanentemente.
d. Implementar planes de contingencia que permitan minimizar los incidentes de pérdida de información de la CGN.
e. Seleccionar alternativas de solución probadas y con responsabilidades individuales y no colectivas que amplían la probabilidad de materializar el riesgo.
f. Aplicación estricta de las políticas de copias de respaldo realizando seguimiento, control y monitoreo, contando con los elementos para aplicarlas.
g. Aplicación de las políticas de seguridad teniendo en cuenta amenazas, riesgos, controles, incidentes, fallas, buenas prácticas.
h. Asegurar como GIT de apoyo Informático la confidencialidad, integridad y disponibilidad de la información como lo especifican en las políticas de seguridad informática.
i. Sensibilizar a los usuarios de manera más eficaz, asegurándose de su retroalimentación en relación a las políticas de seguridad de la información y su manejo, en directrices del uso de los componentes tecnológicos de la Entidad y todo lo que esto involucra, con el fin de concientizar al usuario en la importancia del buen uso y manejo de la información.
j. Ejecutar periódicamente las revisiones de seguridad de la información.
k. Analizar en trabajo de campo las necesidades de almacenamiento, conservación y uso de la información que manejan los diferentes grupos de la Entidad en relación a su importancia, criticidad, valor, manejo y seguridad.
l. Documentar los incidentes de seguridad para no repetir el error o la falla y así tomar las acciones para controlarlos.
m. La pérdida de servicio tecnológico ocasiona malestar en los usuarios, quienes deben tener un alto nivel de satisfacción en los servicios que se prestan.
n. Conservar los lineamientos de respaldo, almacenamiento y destrucción de la información para minimizar el riesgo de pérdidas o mal uso de la misma.

o. Evitar mediante el control y monitoreo el deterioro de los medios de almacenamiento.
p. Analizar la matriz de riesgos realizando seguimiento permanente, con el objetivo de aplicar los controles existentes y actualizarla periódicamente de acuerdo a su evaluación y riesgos nuevos que se detecten.
q. Teniendo en cuenta que la información de apoyo para soportar auditorías internas de calidad, auditorias de gestión, auditorías externas, solución de consultas, gestión misional y administrativa, conceptos y doctrina contable entre otras, se encuentra actualmente en el servidor Pathfinder, es importante evaluar la posibilidad de contar con una herramienta más segura y robusta para el manejo de esta información institucional.
r. Existen herramientas como repositorios u otras que permiten unidad, centralización, control, preservación a largo plazo, organización, estándar, búsqueda ágil, visibilidad, versionamientos, control de cambios, interoperabilidad, seguridad, comunicación e intercambio de información, entre otros beneficios a tener en cuenta.

   Las posibles mejoras de implementar una herramienta segura y robusta para el manejo centralizado de la información institucional redundarán en imagen, organización, centralización, seguridad y otros beneficios para la Entidad y los funcionarios que laboran en ella.

Para concluir, se entiende que aunque no es una tarea fácil, es mejor empezar ahora que continuar con un problema que se va convirtiendo en una bola de nieve en el tiempo.

Es importante resaltar que la administración segura del manejo de la información institucional con responsabilidad centralizada en el GIT de Apoyo Informático redundará en eliminar problemáticas para ellos mismos y brindar un servicio satisfactorio para los usuarios de la entidad en el manejo de la información.

Cabe aclarar que la intención del GIT de Control Interno con este informe no es otra que plantear alternativas de mejora para que sean evaluadas por el GIT de Apoyo Informático y tomar las medidas pertinente para optimizar y hacer más eficiente la gestión de sus operaciones al interior de este GIT, que se refleje en la prestación y seguridad de la información, que maneja cada uno de los procesos en sus diferentes archivos, teniendo en cuenta que es una información institucional que guarda la historia y trazabilidad del funcionamiento de la Entidad.