REFERENCIA	NOMBRE DE AUDITORIA	FECHA DE REALIZACIÓN		FECHA DEL INFORME
		INICIO	CIERRE	
AE-P-GI-01-19	Auditoria especial revisión incidente lentitud Sistema e-KOGUI	01/08/2019	11/09/2019	11/09/2019

PROCESO /AREA AUDITADA	AUDITOR LIDER / AUDITOR
Gestión de Información de Defensa Jurídica- Gestión de Tecnología de la Información	Adriana María Ocampo Loaiza
EQUIPO DE AUDITORES	**AUDITORES ACOMPAÑANTES**
----------	

1. OBJETIVO:

- Revisar incidente de lentitud del sistema misional e-KOGUI.

2. ALCANCE:

Evaluar los procesos de Gestión de Información de Defensa Jurídica y Gestión de Tecnología de la Información frente a los componentes Software y Hardware del sistema e-kogui antes y durante el incidente registrado en el periodo comprendido entre el 11 al 23 de julio de 2019.

3. CRITERIOS:

- Marco de mejores prácticas en Tecnología alineados con COBIT 5, ITIL V3 2011-
- TOGAF (o marco de trabajo) de Arquitectura Empresarial.
- GTI-P-02 Gestión de Cambios de TI.
- GTI-F-010 Solicitud de Cambios RFC.
- Documentos internos.

4. LIMITACIONES PARA EL DESARROLLO DE LA AUDITORIA:

Ninguna

5. DOCUMENTOS EXAMINADOS:

- Herramienta de Enterprise Architect, herramienta Jenkins y GitLab.
- Herramientas de monitoreo Jira software - Tableros Scrum.
- Pruebas de despliegue realizadas.
- Instructivo para la realización de despliegues.
- Solicitud de cambios RFC 14/07/2019

6. PLAN DE MUESTREO

- No aplica

7. INFORME

7.1 FORTALEZAS

No aplica

7.2 CUMPLIMIENTO DE PRINCIPIOS

Principio de disponibilidad: el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos. La información deberá permanecer accesible a elementos autorizados.

Principio de celeridad: Impulsar oficiosamente los procesos, e incentivar el uso de las tecnologías de la información y las comunicaciones.

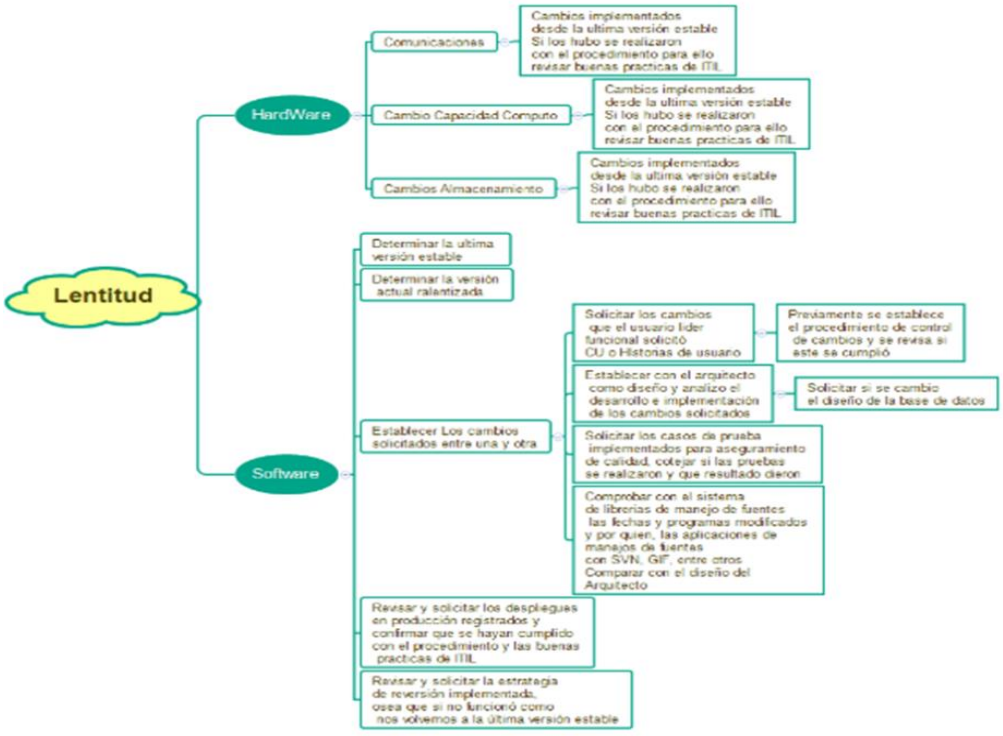
7.3 CONTENIDO

7.3.1 Descripción de la revisión

Para realizar la verificación se llevó a cabo el siguiente procedimiento:

- Recolección de información: Se solicitó la información mediante correo electrónico del día 09/08/2019 dirigido a los responsables de los procesos Gestión de Información de Defensa Jurídica y Gestión de Tecnología de la Información para verificar los componentes de hardware y software que pueden ser potenciales fuentes de riesgo como lo muestra el siguiente esquema:

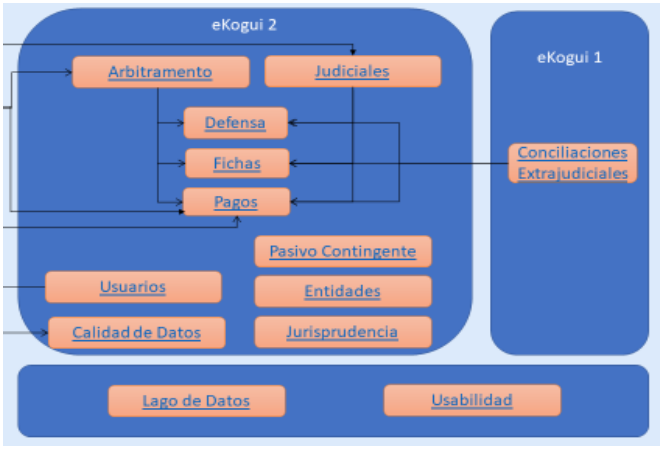
Gráfica 1: Diagrama de verificación de lentitud



- Comprobación general de la configuración básica del sistema:

En este ítem se realizó la verificación de la configuración del sistema e-kogui, como está constituida su arquitectura para comprender su funcionamiento. La arquitectura de bases de datos se compone así:

Gráfica 2: Arquitectura Sistema de Información Ekogui



Fuente: Módulos y Arquitectura General de Ekogui

En reunión del día 14/08/2019 con la Directora y el experto del proceso de Gestión de la Información de Defensa Jurídica, la coordinadora del proyecto, el arquitecto de e-kogui, se llevó a cabo la revisión del diseño de bases de datos en la herramienta Enterprise Architect, la herramienta Jira para evidenciar la trazabilidad de los incidentes, para los despliegues en la herramienta Jenkins y el código fuente GitLab que permite la trazabilidad del versionamiento de la aplicación.

También se verificaron los despliegues del día 08/07/2019 en los ambientes de producción y soporte y su correspondiente rollback que para esta ocasión no fue requerido, como lo evidencia la siguiente imagen:

Gráfica 3: Plan de despliegue

FECHA: 8 de julio de 2019

Tipo de Actividad	Actividad	Responsable	Cantidad (Horas)	Estado	Hora Inicio	Hora Fin
DESPLIEGUE EN PRODUCCIÓN						
Despliegue	Bajar Servicios Ekogui2	Diego Forero	5	OK	7:00 PM	7:05 PM
Despliegue	Despliegue Monolítico	Diego Forero	15	OK	7:22 PM	7:38PM
Despliegue	Despliegue Transversales	Diego Forero	15	OK	7:50 PM	7:55 PM
Despliegue	Despliegue Gateway	Diego Forero	15	OK	4:22 AM	4:47 AM
Despliegue	Subir Ekogui2	Diego Forero	10	OK	7:55 PM	8:00 PM
Despliegue	Verificar Ekogui1 Autenticación	Rosse -Adriana	5	OK	8:00 PM	8:05 PM
Despliegue	Verificar Ekogui2 Autenticación	Rosse -Adriana	5	OK	8:05 PM	8:10 PM
Despliegue	Verificar Opciones de Menú	Rosse -Adriana	20	OK	8:10 PM	8:30 PM
DESPLIEGUE EN SOPORTE						
Despliegue	Bajar Servicios Ekogui2	Diego Forero	5	OK	6:30 PM	6:35 PM
Despliegue	Despliegue Monolítico	Diego Forero	15	OK	6:44 PM	7:13 PM
Despliegue	Despliegue Transversales	Diego Forero	15	OK	6:45 PM	6:54 PM

Despliegue	Despliegue Gateway	Diego Forero	15	OK	6:36 AM	7:03 AM
Despliegue	Subir Ekogui2	Diego Forero	10	OK	6:55 PM	7:00 PM
Despliegue	Verificar Ekogui1 Autenticación	Rosse -Adriana	5	OK	7:00 PM	7:05 PM
Despliegue	Verificar Ekogui2 Autenticación	Rosse -Adriana	5	OK	7:05 PM	7:10 PM
Despliegue	Verificar Opciones de Menú	Rosse -Adriana	30	OK	7:10 PM	7:40 PM
ROLLBACK						
Rollback	1. Realizar Restore de Backup de la base de datos generados	Fredy Niño		No fue Requerido	N/A	N/A
Rollback	2. Reemplazar los WAR existentes por cada microservicio o monolítico desplegado, por el backup tomado antes del despliegue	Diego Forero	10	No fue Requerido	N/A	N/A
Rollback	3. Reiniciar el microservicio correspondiente	Diego Forero	10	No fue Requerido	N/A	N/A

Fuente: Gestión de Información de Defensa Jurídica

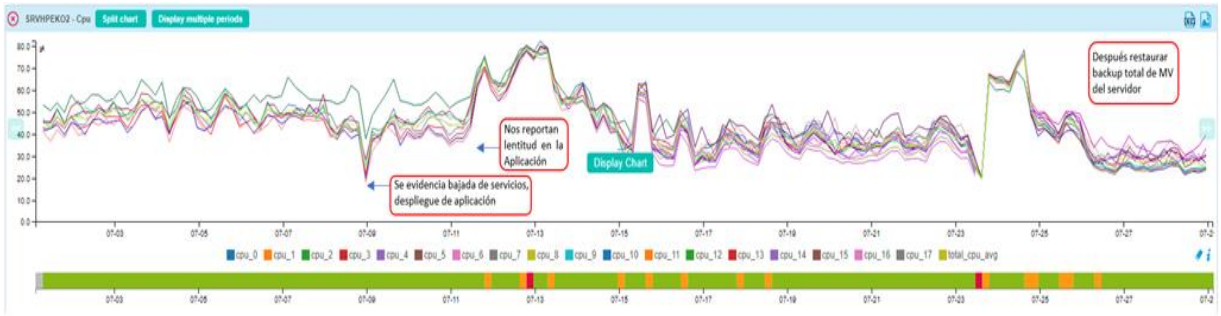
Antes del incidente este fue el despliegue de gran magnitud que se verificó, con el fin de establecer la funcionalidad y desempeño del aplicativo después de pasar a producción; comportamiento que no generó impacto adverso en los días siguientes, en cuanto a disponibilidad o lentitud.

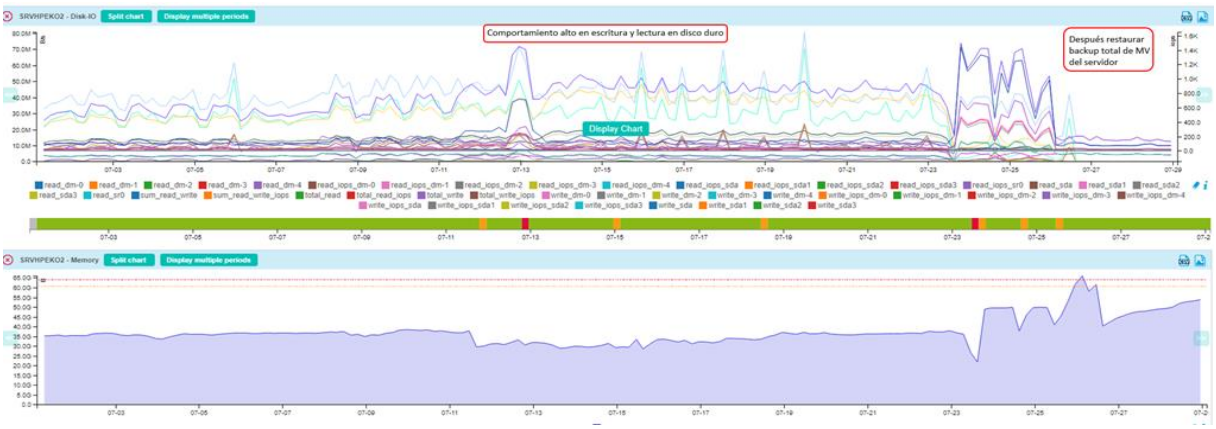
- <u>Identificación y análisis de posibles problemas:</u>

Para el informe final se tuvieron en cuenta las reunión de mesa de trabajo informe preliminar realizada el 30/08/2019 y se analizó la información suministrada por el proceso de Gestión de Información de Defensa Jurídica y Gestión de Tecnología de la Información en los archivos de respuesta al informe preliminar emitido el 28 de agosto de 2019 en los archivos: Histórico de Uso de Recursos Computacionales (1).docx y Reportes Herramienta de Monitoreo TI; frente a las siguientes imágenes que generan las herramientas de monitoreo en un periodo más largo de tiempo antes y después del incidente, evidenciando los siguientes comportamientos:

Servidor de Aplicaciones, Rango de tiempo (03/07/2019 - 29/07/2019)

Grafica No 4: Monitoreo CPU, Disco I/O, memoria

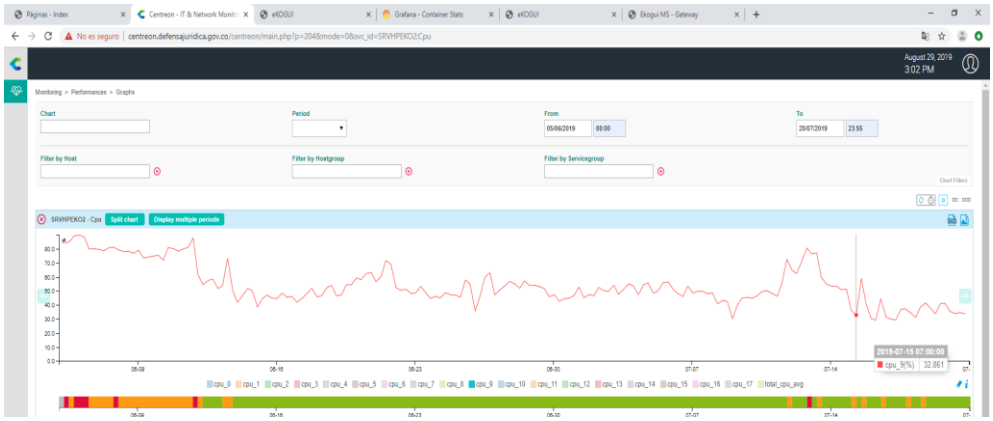




Fuente: Proceso Gestión de Tecnología de la Información

Periodo: 1 al 21 de julio de 2019

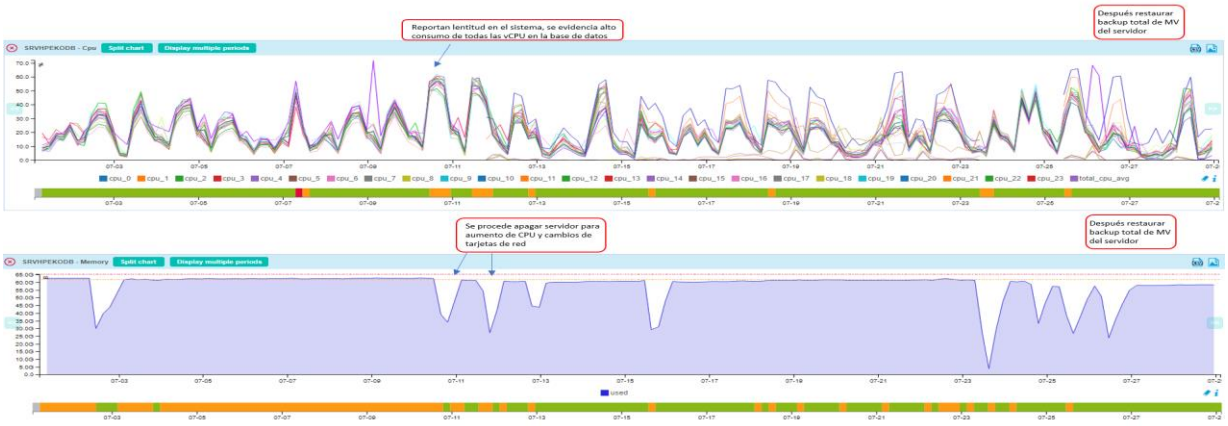
Gráfica No 5 Uso de Procesamiento (CPU_9) del servidor de contenedores Web de Producción



Fuente: Gestión de Información de Defensa Jurídica

Periodo (03/07/2019 - 29/07/2019)

Gráfica No 6 Servidor de base de datos



Fuente: Proceso Gestión de Tecnología de la Información

Analizando las imágenes que muestran las herramientas de monitoreo y las hipótesis y probabilidades que argumentan los dos procesos revisados sobre las posibles causas que dieron origen al incidente, no son evidencias contundentes que permitan que esta auditoría determinar la causa raíz. Por lo tanto, a continuación, se evalúa el evento de riesgo materializado

- Riesgos

Teniendo en cuenta la verificación de los riesgos asociados a los procesos revisados, se encontró, que la materialización del evento de riesgo corresponde a: "PERDIDA DE IMAGEN DE LA AGENCIA ANTE LAS ENTIDADES USUARIAS DEL SISTEMA", por causa de: Limitaciones, defectos y bajo desempeño del sistema.

Grafica No 7: Evaluación de riesgos

RIESGO	CAUSA	IMPACTO	EVENTO MATERIALIZADO	CONTROLES	EVALUACIÓN ZONA DE RIESGO RESIDUAL	EVALUACIÓN EFECTIVIDAD DE CONTROLES	OBSERVACIÓN
PERDIDA DE IMAGEN DE LA AGENCIA ANTE LAS ENTIDADES USUARIAS DEL SISTEMA.	Limitaciones, defectos y bajo desempeño del sistema.	No cumplir con las expectativas de las entidades frente a la labor de la Agencia en cuanto a la solución de necesidades funcionales y capacitación sobre el sistema.	Inoportunidad en el tiempo de respuesta de las funcinalidades del sistema e-kogui	Procedimiento gestionar requerimientos y organizar el proyecto del sistema único de información litigiosa del estado GIP06 Usuario Customer Management Services control de trafico telefonico Procedimiento brindar soporte al sistema único de gestión e información litigiosa del estado GIP07 Procedimiento realizar mantenimiento al sistema único de información litigiosa del estado GIP10.	4 Zona de Riesgo ALTA	No efectivos	Teniendo en cuenta la materialización de un evento de riesgo, la Ofcina de Control Interno considera que aún cuando se aplican los 4 controles establecidos no hay uno que ataque directamente la causa de este evento materializado, razón por la cual se deben implementar controles más fuertes que ayuden a bajar la valoración y zona en la que se encuentra este riesgo residual.

Se requiere revisar los controles asociados para mitigar el riesgo, en atención a la materialización del mismo, por causa del incidente de bajo desempeño del sistema. Teniendo en cuenta que los controles son en su gran mayoría son procedimientos, que, si bien se aplican, no son controles. Por lo tanto, la auditoría solicita plantear acciones puntuales que ataquen todas las causas identificadas.

Para este incidente puntual, la valoración de no efectividad de los controles radica en que no hay un control que este orientado a mitigar directamente la causa.

Adicional, con controles más fuertes permitiría bajar la zona de riesgo residual ALTA en la que se encuentra, en atención a que se trata de un sistema de apoyo misional de la Entidad.

- Conclusiones

Con referencia a la información suministrada por los procesos Gestión de Información de Defensa Jurídica- Gestión de Tecnología de la Información, se precisa:

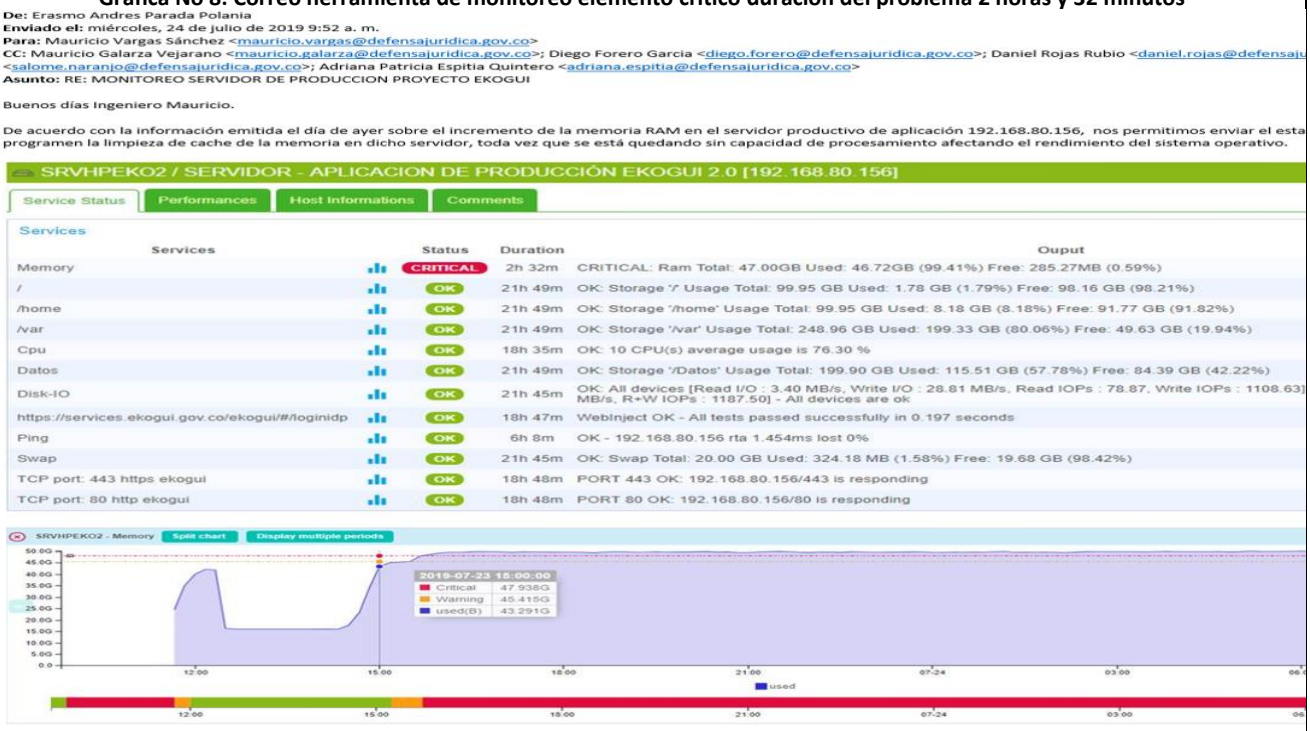
- Existen procedimientos documentados para despliegue, herramientas de monitoreo que permiten advertir comportamiento del sistema a nivel de hardware.
- En cuanto al control y administración de cambios, al igual que el manejo de incidentes, no se observa una actividad articulada entre los dos procesos (Gestión de Información de Defensa Jurídica- Gestión de Tecnología de la Información), razón por la cual el incidente duró en restablecerse durante (13 días).
- Con la información remitida por los procesos y la verificación frente a las herramientas revisadas

no es posible identificar la causa raíz, pero en concordancia con lo anterior, esta auditoria permite plantear el siguiente camino para aplicar en los despliegues que gran complejidad:

1. Establecer cambios en la tabla de parámetros del sistema antes de los eventos de memoria, CPU y disco.
2. Realizar pruebas asociadas a trazabilidad de instrucciones ejecutadas.
3. Realizar pruebas a los caminos alternativos de manera intensiva, principalmente a funcionalidades que no se usan frecuentemente.

Finalmente, se observa que los eventos que se han presentado a nivel de memoria, CPU y disco tienen una detección oportuna por parte de las herramientas de monitoreo de la infraestructura del sistema, pero, la respuesta a estos incidentes es tardía, como se observa en la siguiente gráfica de acuerdo con el estado de servicios se incurre en un uso del 99.41 ***crítico*** (como lo indica la herramienta de monitoreo) duración del problema 2 horas y 32 minutos, sin respuesta para corregir este incidente.

Gráfica No 8: Correo herramienta de monitoreo elemento crítico duración del problema 2 horas y 32 minutos



De: Erasmo Andres Parada Polania
Enviado el: miércoles, 24 de julio de 2019 9:52 a. m.
Para: Mauricio Vargas Sánchez <mauricio.vargas@defensajuridica.gov.co>
CC: Mauricio Galarza Vejarano <mauricio.galarza@defensajuridica.gov.co>; Diego Forero Garcia <diego.forero@defensajuridica.gov.co>; Daniel Rojas Rubio <daniel.rojas@defensaju
<salome.naranjo@defensajuridica.gov.co>; Adriana Patricia Espitia Quintero <adriana.espitia@defensajuridica.gov.co>
Asunto: RE: MONITOREO SERVIDOR DE PRODUCCION PROYECTO EKOGUI

Buenos días Ingeniero Mauricio.

De acuerdo con la información emitida el día de ayer sobre el incremento de la memoria RAM en el servidor productivo de aplicación 192.168.80.156, nos permitimos enviar el esta
programen la limpieza de cache de la memoria en dicho servidor, toda vez que se está quedando sin capacidad de procesamiento afectando el rendimiento del sistema operativo.

SRVHPEKO2 / SERVIDOR - APLICACION DE PRODUCCIÓN EKOGUI 2.0 [192.168.80.156]

Service Status | Performances | Host Informations | Comments

Services

Services	Status	Duration	Ouput
Memory	CRITICAL	2h 32m	CRITICAL: Ram Total: 47.00GB Used: 46.72GB (99.41%) Free: 285.27MB (0.59%)
/	OK	21h 49m	OK: Storage '/' Usage Total: 99.95 GB Used: 1.78 GB (1.79%) Free: 98.16 GB (98.21%)
/home	OK	21h 49m	OK: Storage '/home' Usage Total: 99.95 GB Used: 8.18 GB (8.18%) Free: 91.77 GB (91.82%)
/var	OK	21h 49m	OK: Storage '/var' Usage Total: 248.96 GB Used: 199.33 GB (80.06%) Free: 49.63 GB (19.94%)
Cpu	OK	18h 35m	OK: 10 CPU(s) average usage is 76.30 %
Datos	OK	21h 49m	OK: Storage '/Datos' Usage Total: 199.90 GB Used: 115.51 GB (57.78%) Free: 84.39 GB (42.22%)
Disk-IO	OK	21h 45m	OK: All devices [Read I/O : 3.40 MB/s, Write I/O : 28.81 MB/s, Read IOPs : 78.87, Write IOPs : 1108.63] MB/s, R+W IOPs : 1187.50] - All devices are ok
https://services.ekogui.gov.co/ekogui/#/loginidp	OK	18h 47m	WebInject OK - All tests passed successfully in 0.197 seconds
Ping	OK	6h 8m	OK - 192.168.80.156 rta 1.454ms lost 0%
Swap	OK	21h 45m	OK: Swap Total: 20.00 GB Used: 324.18 MB (1.58%) Free: 19.68 GB (98.42%)
TCP port: 443 https ekogui	OK	18h 48m	PORT 443 OK: 192.168.80.156/443 is responding
TCP port: 80 http ekogui	OK	18h 48m	PORT 80 OK: 192.168.80.156/80 is responding

SRVHPEKO2 - Memory | Split chart | Display multiple periods

2019-07-23 15:00:00
Critical 47.936G
Warning 45.415G
used(B) 43.291G

used

Fuente: Proceso Gestión de Tecnología de la Información

- <u>Recomendaciones</u>:

✓ Establecer un comité de análisis de incidentes entre los dos procesos (Gestión de Información de Defensa Jurídica- Gestión de Tecnología de la Información) para revisar las posibles causas ante un evento materializado, en el cual toda decisión sea de conocimiento y consentimiento por las dos partes.

✓ Frente a las alertas presentadas por las herramientas de monitoreo, se debe mejorar los tiempos de reacción o atención de los mismos, lo anterior, en concordancia con la gráfica No 8. “duración del problema 2 horas y 32 minutos”.

- ✓ Teniendo en cuenta que no se logró identificar una causa raíz del incidente del sistema e-kogui, como consecuencia, no está controlado el problema, el riesgo persiste. Por lo anterior, esta Oficina conmina a llevar a cabo las acciones planteadas por la auditoria. (ver conclusiones).

- ✓ Como parte de la solución para identificar la causa raíz del problema, esta oficina considera pertinente gestionar y obtener el diagnóstico de un experto.

- ✓ Reportar el incidente como evento de riesgo materializado al proceso de mejora continua para su correspondiente tratamiento.

- ✓ Revisar los controles asociados al riesgo PERDIDA DE IMAGEN DE LA AGENCIA ANTE LAS ENTIDADES USUARIAS DEL SISTEMA del proceso de Gestión de Información de Defensa Jurídica, teniendo en cuenta que no son efectivos y no mitigan el impacto del riesgo.

Firma Auditor Designado y Equipo Auditor	Firma Jefe de Control Interno ANDJE
Informe realizado por: Adriana María Ocampo Loaiza Contratista Oficina de Control Interno No. Radicado. 20191020009373	Firmado Electrónicamente por: Luis E. Hernandez León Jefe Oficina de Control Interno No. Radicado. 20191020009373