9 mar 2026

Revisión GLPI

Invitados Jaime Alexander Méndez Pulecio Dario Orlando Becerra Erazo Faver Perez Guiterrez Daniel Enrique Bernal Contreras

Archivos adjuntos Revisión GLPI

Registros de la reunión Transcripción Grabación

Resumen

Discusión sobre el estancamiento de GLPI, el equipo identificó serios problemas de seguridad y coordinó un plan de acción para mitigar riesgos.

Progreso y Requisitos de GLPI
El proyecto GLPI está estancado con la fecha límite acercándose y solo se entregó la máquina virtual. Se identificó la necesidad de conectar GLPI al Directorio Activo, configurar el correo electrónico y definir el árbol jerárquico de enrutamiento de casos.

Seguridad Crítica y Mitigación
Se detectaron graves problemas de seguridad, incluyendo un 'rootkit' en un servidor de acceso remoto e intentos de conexión anómalos a la base de datos. La decisión fue informar inmediatamente a la gerencia, solicitar una reunión con seguridad el miércoles y proponer la 'dockerización' de servicios misionales como medida de choque.

Configuración Final de GLPI
Se decidió crear un buzón de prueba y usar el usuario de lectura del Directorio Activo para configurar la nueva instancia de GLPI. Se definió la estructura de soporte de GLPI para incluir un grupo de desarrollo con una estrategia de enrutamiento de solicitudes de desarrollo.

Detalles

- **Discusión sobre el progreso de GLPI**: Faver Perez Gutierrez informó sobre una conversación con el ingeniero Óscar, quien inquirió sobre el estado del proyecto GLPI, señalando que la fecha límite se estaba acercando (00:00:00). Jaime Alexander Méndez Pulecio había indicado previamente que la fecha límite era a finales de marzo, y Faver Perez Gutierrez comunicó la necesidad de acelerar el proceso. Se confirmó que solo se había entregado la máquina virtual y que no se había avanzado más debido a que el equipo había estado ocupado en otras tareas y "apagando incendios" (00:01:05).
- **Requisitos técnicos y procedimentales para GLPI**: Dario Orlando Becerra Erazo describió las tareas técnicas pendientes, que incluyen conectar el GLPI al directorio activo para la fuente de usuarios, conectarlo a la bandeja de entrada para descargar casos, y al relé de correo para enviar notificaciones. También mencionó la necesidad de definir los procedimientos internos, los cuales declaró desconocer (00:02:05).
- **Participación del ingeniero Daniel Enrique Bernal Contreras**: Se mencionó que el ingeniero Daniel Enrique Bernal Contreras fue invitado a la reunión porque previamente había compartido su conocimiento sobre el tema GLPI. Esto se presentó como una oportunidad para obtener una nueva perspectiva sobre el proyecto (00:02:05).
- **Estructura jerárquica y enrutamiento de casos en GLPI**: Jaime Alexander Méndez Pulecio enfatizó la necesidad de definir el árbol de jerarquías para el GLPI y cómo se estructuraría el enrutamiento de casos (00:02:05). Dario Orlando Becerra Erazo cuestionó si el software enrutaba los casos automáticamente o si requeriría enrutamiento manual. Faver Perez Gutierrez sugirió que lo ideal sería la automatización, pero Jaime Alexander Méndez Pulecio y Faver Perez Gutierrez expresaron dudas sobre hasta qué punto esto podría automatizarse, describiéndolo como un desafío (00:03:36).
- **Historial de configuración de enrutamiento de GLPI**: Daniel Enrique Bernal Contreras recordó que en una instalación anterior de GLPI, se utilizaba un filtro en la bandeja de entrada para redirigir correos a un buzón que el GLPI leía (00:03:36). Una regla dentro del GLPI distribuía las solicitudes según etiquetas que definían el flujo de trabajo (00:04:39).
- **Uso del plugin OCS Inventory para GLPI**: Dario Orlando Becerra Erazo consultó si se incluiría el plugin OCS Inventory para el inventario (00:04:39). Jaime Alexander Méndez Pulecio y Faver Perez Gutierrez confirmaron que la idea es usarlo para inventariar software y hardware. Dario Orlando Becerra Erazo mencionó que OCS Inventory es una herramienta gratuita que puede

tener la capacidad de ejecutar comandos para la instalación de software (00:06:18).

- **Acceso a la configuración del GLPI anterior**: Dario Orlando Becerra Erazo preguntó sobre la posibilidad de acceder al GLPI anterior para obtener los datos de las conexiones y configuraciones. Faver Perez Gutierrez señaló que han existido dos versiones de GLPI en la entidad y que la que "medio funcionó" fue la primera instalada alrededor de 2016-2017 (00:07:06). Se determinó que era necesario acceder a la configuración del sistema anterior para obtener las cadenas de conexión (00:08:07).
- **Dificultades para definir el árbol de jerarquías**: Jaime Alexander Méndez Pulecio intentó encontrar la estructura del árbol de jerarquías en la interfaz del GLPI en funcionamiento, pero no logró encontrar la división clara de soportes como "soporte técnico" o "sistemas misionales" (00:08:07). La discusión se centró en la pestaña de "entidades" como la ubicación potencial de esta jerarquía (00:09:22).
- **Problemas de acceso a la base de datos de GLPI**: Los participantes exploraron varias opciones para acceder a la configuración del GLPI, incluyendo la posibilidad de que el usuario principal fuera "GLPI" (00:14:15). La incapacidad de acceder a la base de datos (MariaDB) con la contraseña existente se convirtió en un obstáculo, lo cual detuvo el intento de acceder a la información de conexión (00:19:48).
- **Propuesta para la configuración inicial de GLPI**: Dado el problema de acceso, Faver Perez Gutierrez preguntó si se podía intentar ingresar a la interfaz normal, mientras que Dario Orlando Becerra Erazo sugirió la opción de generar un buzón de pruebas y usar el usuario de lectura del Directorio Activo (el cual ya se tiene) para configurar la nueva instancia de GLPI (00:22:39) (00:27:25). Jaime Alexander Méndez Pulecio se dedicó a crear el árbol de jerarquías del nuevo GLPI con tres niveles: Secretaría Jurídica como entidad principal y luego sistemas misionales y administrativos (00:15:24) (00:28:19).
- **Identificación de serios problemas de seguridad**: Dario Orlando Becerra Erazo alertó sobre un grave problema de seguridad en la entidad, ya que encontró un archivo que identificó como un "rootkit, malware" en un servidor (193) que provee acceso remoto, espionaje y registro de pulsaciones de teclas (key logger) (00:34:18). También se identificó que desde otra IP (219) se estaban intentando conectar a la base de datos, lo cual podría ser Legal Box (00:30:29).
- **Propuestas para mitigar los riesgos de seguridad**: Daniel Enrique Bernal Contreras propuso una estrategia de choque para mitigar el riesgo de

seguridad, sugiriendo la "dockerización" de los servicios y sistemas misionales en un servidor de producción para eliminar el servidor comprometido (193) (00:44:09). La solución de dockerizar podría tardar dos semanas para los cuatro sistemas misionales (00:49:03).

- **Compromiso y plan de acción sobre seguridad**: El equipo acordó que los problemas de seguridad eran muy preocupantes y debían ser comunicados de inmediato al superior (00:41:10). Se decidió informar al jefe y solicitar una reunión con el equipo de seguridad para el miércoles, ya que la agenda del día siguiente era complicada (00:43:16) (00:48:01). Se mencionó la necesidad de restringir la salida a Internet de los servidores como una medida rápida para mitigar el riesgo (00:37:34) (00:41:10).
- **Preparación para la nueva configuración de GLPI**: Faver Perez Gutierrez verificó que el usuario "GLPI jurídica" existía en el Directorio Activo. Se le pidió que restableciera la contraseña de ese usuario y la colocara en la descripción para que Dario Orlando Becerra Erazo pudiera proceder con la conexión del nuevo GLPI (00:55:40).
- **Discusión sobre la instalación de Keycloak**: Daniel Enrique Bernal Contreras mencionó la necesidad de enviar un correo electrónico relacionado con la instalación de Keycloak (un sistema de inicio de sesión único) para la granja de microservicios, sugiriendo que se instalara en una máquina virtual. Dario Orlando Becerra Erazo confirmó que la instalación se realizaría en un entorno virtual, ya que no se tienen máquinas físicas (00:52:47).
- **Definición de Categorías y Niveles en GLPI**: El equipo ha estado ajustando los niveles de soporte y las categorías para el sistema GLPI, donde se requiere cambiar los niveles de "Sistemas Operativos" a dos (00:57:04). Se sugirió incluir una parte para el grupo de desarrollo dentro de las categorías de soporte, con el fin de facilitar la gestión de casos y la descarga de informes para la cuenta de cobro de Faver Perez Gutierrez (00:59:02). Se acordó que el primer nivel de desarrollo debe ser la definición y la historia de usuario, a cargo de Liliana y Solange, y que el equipo de desarrollo actuaría como un disparador o un segundo nivel tras la definición (01:01:44).
- **Estrategia para Solicitudes de Desarrollo**: Se definió que la solicitud de desarrollo es un disparador, llegando primero a Jaime Alexander Méndez Pulecio, quien la define como una solicitud de desarrollo antes de que las "chicas" (Liliana y Solange) evalúen si es una implementación, una mejora o un desarrollo nuevo (01:01:44). Se señaló la necesidad de incluir al grupo de desarrollo dentro de esta estructura, asegurando que las primeras en evaluar sean las personas mencionadas (01:02:51).

- **Incorporación de Servicios Misionales Legales en GLPI**: Se planteó la necesidad de incluir nuevos servicios misionales, como "legal IBC," dentro de la estructura de GLPI, ya que se implementarán módulos que requerirán soporte. La solución propuesta es ajustar el formato de las categorías, utilizando "LB guión el módulo" para permitir que la estructura siga creciendo y funcione como un todo (01:04:08).
- **Discusión sobre Redirección y Reputación de Alcaldía Bogotá**: Dario Orlando Becerra Erazo preguntó si era posible eliminar la redirección del PMU (Plan de Movilidad Urbana) que entra a los sistemas misionales desde la Secretaría General (01:05:44). Se explicó que la permanencia de la URL de Alcaldía Bogotá en la búsqueda se debe a que aparece de primera por temas de reputación, lo cual se considera un "hit" o visita a pesar de que el tráfico no sea directo, aunque esto causa problemas técnicos, como el hecho de que el navegador pida escanear la red local (01:07:46).
- **Análisis de Consultas Anómalas y Esfuerzos de Seguridad**: Daniel Enrique Bernal Contreras compartió datos sobre consultas inusuales a normas viejas en la base de datos, lo que sugiere posibles vulnerabilidades o ataques de fuerza bruta (01:08:50). Se concluyó que la modernización de los sistemas, incluyendo la "containerización," puede ser una victoria temprana para mitigar vulnerabilidades y mejorar la seguridad general de los sistemas (01:09:54).
- **Plan de Mitigación y Coordinación de Acciones de Seguridad**: Jaime Alexander Méndez Pulecio anunció que, dada la identificación de inconvenientes y brechas de seguridad, hablará con el jefe y se reunirá con el jefe de seguridad (Diego Ferney) para pedir una sesión de mitigación a más tardar el jueves. La estrategia incluye trabajar con administradores técnicos de las plataformas para crear sesiones conjuntas y solicitar planes de mitigación a cada uno, empezando por los sistemas misionales (01:11:27).
- **Uso del Equipo de Respuesta a Incidentes de Seguridad (CSIRT) en la Estrategia**: Se mencionó que para abordar las vulnerabilidades, como la necesidad de actualizar Java y las dificultades de reprogramación, se debe seguir el lineamiento de seguridad y solicitar el apoyo del CSIRT para revisar y ayudar a configurar las protecciones, como el WAF. Se determinó que el WAF debería bloquear casi todo el tráfico, pero no lo está haciendo, y el enlace con el CSIRT debe ser gestionado por el personal de seguridad (01:13:21).
- **Configuración del Buzón de Correo para GLPI**: Dario Orlando Becerra Erazo confirmó que Faver Perez Gutierrez le había enviado los accesos necesarios (LDAP y el buzón) para configurar GLPI, el cual debe recibir correos, y el sistema borra el correo del buzón después de jalarlo. Por ello, se concluyó

que es necesario utilizar un buzón con licencia para el soporte y obtener uno adicional para las pruebas (01:14:20).

- **Instrucciones para Microservicio de Correo Electrónico**: Daniel Enrique Bernal Contreras solicitó a Dario Orlando Becerra Erazo las instrucciones para utilizar un microservicio genérico de envío de correo electrónico para notificaciones y la capacidad de adjuntar archivos (01:15:41). Dario Orlando Becerra Erazo proporcionó los detalles del servidor SMTP sin autenticación, que es la dirección 10.54.80.102 por el puerto 25 (01:16:44).
- **Sospechas de Ataques de Fuerza Bruta en GLPI**: Se especuló que la base de datos de GLPI podría haberse dañado debido a ataques de fuerza bruta, ya que se estaban realizando consultas fallidas de forma masiva desde una máquina (01:17:38). Jaime Alexander Méndez Pulecio concluyó que las actividades observadas son consistentes con minería de datos o intentos de colapsar los servicios a través de la fuerza bruta (01:18:37).

Pasos siguientes recomendados

- [ ] Jaime Alexander Méndez Pulecio y Faver Perez Gutierrez enviarán los datos de la cuenta GLPI y la cuenta del directorio activo a Dario Orlando Becerra Erazo para que pueda configurar el GLPI que instalaron.
- [ ] Faver Perez Gutierrez restablecerá la contraseña del usuario GLPI del directorio activo y la pegará en la descripción del usuario.
- [ ] Dario Orlando Becerra Erazo se pondrá a revisar qué más inconvenientes de seguridad encuentra y configurará el buzón de correo con licencia para pruebas en GLPI una vez que Faver Perez Gutierrez se lo envíe.
- [ ] Jaime Alexander Méndez Pulecio hablará con el jefe y con Diego Ferney, jefe de seguridad, para solicitar una sesión el miércoles o jueves y exponer los inconvenientes y brechas de seguridad identificadas.

Revisa las notas de Gemini para asegurarte de que sean correctas. Obtén consejos y descubre cómo toma notas Gemini

Danos tu opinión sobre el uso de Gemini para tomar notas en una breve encuesta.