GOBERNACIÓN DE ANTIOQUIA República de Colombia	**ACTA DE REUNIÓN**	**Código:** FO-M1-P5-005
		Versión: 02
		Fecha de aprobación: 25/06/2018

Tipo de reunión: Presencial		**Fecha de reunión:** 17 de febrero de 2025
Organismo, Dependencia o Proceso: Dirección de Proyectos e Inversión Pública		**Fecha de elaboración:** 28 de febrero de 2025
Asistentes, Organismo: Por parte de la Dirección de Proyectos e Inversión Pública: Daniel Alberto Arbeláez Echeverri – Director Gema Adelaida Marulanda Gutiérrez – Supervisora Contrato 4600017809 Por parte del Área Tecnologías de Información TI: Alexander Ocampo Benjumea Fabio Andrés Márquez Zapata (virtual) Carlos Antonio Serna Cortés (virtual) Por parte de M.R Asesores y Consultores S.A.S.: Mauricio Andrés Ramírez Espitia Wendy Yojana Cárdenas Archila Jonnathan Marentes Párraga	**Ausentes, Organismo:** Por parte del Área Tecnologías de Información TI: Sergio Andrés Cadavid Echeverry	

Orden del Día:

1. Lectura del acta anterior
2. Revisión compromisos anteriores
3. Temas tratados
4. Proposiciones y varios
5. Compromisos pactados

Desarrollo de la Reunión:

1. Lectura del acta anterior: N/A

2. Revisión de compromisos anteriores: N/A

No.	Compromisos Anteriores	Responsable	Fecha de Logro	Estado del Compromiso

3. Temas tratados:

El día lunes 17 de febrero de 2025, se llevó a cabo una mesa de trabajo entre la Dirección de Proyectos e Inversión Pública, el área de Tecnologías de Información TI y la firma contratista M.R ASESORES Y CONSULTORES S.A.S. Dicha mesa de trabajo, tuvo por objeto dar alcance a la solicitud realizada el día martes 04 de febrero de 2025, por parte del funcionario del área de TI, Alexander Ocampo Benjumea, donde se precisó la existencia de brechas de seguridad críticas en el sistema de información SIFFMA, según lo informado por el Grupo de Especialistas en Seguridad Informática de la Gobernación de Antioquia, y para las cuales se requería acción inmediata.

Con el fin de brindar una oportuna solución, efectuar la corrección de dichas vulnerabilidades y evitar posibles riesgos a la seguridad de la información, se llevó a cabo en el despacho de la Dirección, la mesa de trabajo solicitada con el acompañamiento de la supervisora del contrato 4600017809, Gema Adelaida Marulanda Gutiérrez, donde se plantearon las siguientes consideraciones:

1. Por parte de la firma contratista, el ingeniero Jonnathan Marentes Párraga, señaló que se analizaron las vulnerabilidades descritas y se identificó que todas las brechas de seguridad reportadas de carácter crítico, alto y medio están ligadas al uso de la versión Apache Tomcat 8.5.35 que está instalado en el servidor 10.62.1.36 del ambiente de producción para la ejecución del frontend del sistema de información SIFFMA y que es suministrado por el área de TI de la Gobernación de Antioquia, por lo que esta actualización no se realiza directamente por M.R ASESORES Y CONSULTORES S.A.S., dado que no posee los permisos ni la autorización para realizar modificaciones en los servidores de la entidad.

2. Se reitera por parte de la firma contratista que el día 06 de febrero de 2025, vía correo electrónico se informó que la actualización del Tomcat debía ser realizada por el área de TI tal como se ha efectuado hasta el momento, esto teniendo en consideración que, dicha base de herramientas, la Gobernación de Antioquia la entrega al contratista para que sobre ellas realice las tareas a cargo. Sin embargo, con el objeto de la reunión se daba a entender que es la firma M.R ASESORES Y CONSULTORES S.A.S. quien debe realizar dicha actualización y que en caso de ser así, se solicitó dar claridad respecto a si se entregarían los respectivos permisos y si la versión a instalar la proveería la Gobernación.

3. El ingeniero Fabio Andrés Márquez en conjunto con el Ingeniero Carlos Serna, indicaron en la reunión, que el área de infraestructura de TI proporciona únicamente lo concerniente a instalación de servidores y que todas las herramientas que estén instaladas dentro de dicho servidor, son total potestad del contratista, en este caso M.R ASESORES Y CONSULTORES S.A.S., por lo que el área de infraestructura no se encargaría de la actualización de la versión de Apache Tomcat.

4. El Ing. Jonnathan Marentes Párraga, indicó que siempre se había tenido la directriz, que el área de infraestructura se encargaba de la administración de los servidores y sus respectivos componentes, no obstante, siendo así el proceso explicado por parte de los ingenieros Fabio Márquez y Carlos Serna, el Ing. Jonnathan Marentes Párraga preguntó el por qué no se contaba con el acceso a dichos servidores si su administración era potestad del contratista, adicionalmente el ingeniero puso en contexto que existen servidores que son compartidos como son los de base de datos que le parecía delicado administrar las herramientas de dichos servidores.

5. El Ing. Fabio Márquez, indicó que ese tipo de recursos compartidos ocurrían únicamente en los servidores de base de datos por temas de economía en recursos y que sobre estos se tenía el 100% de administración por parte de TI, pero en el caso de los servidores de aplicaciones SIFFMA tanto para QA como para producción, estos están de forma independiente como era de conocimiento general y que dichos servidores donde están alojados los servicios de sistemas como SIFFMA, si debían ser gestionados por el contratista.

6. El funcionario Alexander Ocampo Benjumea, confirmó que cada vez que se requiere una ventana de mantenimiento para hacer un despliegue o actualización del sistema, debe efectuarse en una instancia controlada, por lo cual desde el área de TI se solicita un plan de cambios, el cual contenga fechas, horas, detalle de las actividades a realizar, persona(s) responsable(s) y demás información requerida, con el fin que el personal de infraestructura pueda generar la ventana de mantenimiento

que permite el acceso a cualquier sistema de información que tenga la Gobernación de Antioquia contratado, que para este caso corresponde a SIFFMA.

7. Aclarado el punto de que es la firma contratista quien debe efectuar las actualizaciones a los productos dentro del servidor de aplicaciones de SIFFMA, el Ing. Jonnathan Marentes Párraga, planteó las siguientes alternativas, precisando que en cualquiera de los casos se debían efectuar las pruebas de rigor:

   - Realizar actualización del Tomcat del servidor del ambiente de producción
   - Sacar el sistema de información SIFFMA de Apache Tomcat y ponerlo bajo el esquema REDHAT
   - Usar un servidor de aplicaciones como JBoss tanto en ambiente QA como en ambiente de producción

   Sin embargo, indicó que a futuro podrían presentarse nuevos inconvenientes tanto en el uso de un servidor de aplicaciones como JBoss como en una versión posterior de Apache Tomcat, debido a posibles desactualizaciones en las versiones de alguna de dichas herramientas. Por lo tanto, conforme al análisis realizado en la mesa de trabajo, se decidió de manera conjunta que la mejor opción es tomar SIFFMA y bajarlo del servidor Apache Tomcat y colocarlo directamente como servicio en el servidor de aplicaciones REDHAT.

8. Adicionalmente a la solución planteada, para poder dar correcto trámite a dicha solución que tiene por objetivo extinguir las brechas de seguridad, se estableció utilizar el servidor QA de SIFFMA ANTLAP150 para el uso bajo HTTPS, por lo que fue necesario establecer el siguiente plan de actividades:

   - Realizar la solicitud y gestión del dominio para el ambiente QA
   - Gestionar el certificado de seguridad SSL con base en el subdominio de QA (Alias del certificado)
   - Efectuar la respectiva instalación en SIFFMA ambiente QA
   - Verificar el correcto funcionamiento en el servidor, es decir, que este ejecute según el dominio asignado
   - Solicitar análisis de vulnerabilidades al Grupo de Especialistas en Seguridad Informática de la Gobernación de Antioquia

9. El Ing. Jonnathan Marentes Párraga, preguntó si el ambiente QA estaba expuesto en internet dado que no conocía dicho detalle y el Ing. Fabio Márquez indicó que el ambiente QA está en la zona DMZ y que se accede bajo IP pública http://181.233.159.52:8090, con lo que se comprobó y efectivamente se generó dicho acceso sin estar dentro de la red de la Gobernación.

10. Acorde a lo anterior, el Ing. Jonnathan Marentes Párraga indicó que para el proceso normal de operación no era necesario que el ambiente QA de SIFFMA estuviera en la zona desmilitarizada, pero que para efectos de la prueba de ejecución de SIFFMA QA bajo HTTPS, si era necesario que se conservara en el DMZ para garantizar las pruebas en condiciones similares a producción.

11. Desde el área de TI se planteó la posibilidad de efectuar el formateo de la máquina que tiene configurada para el ambiente QA de SIFFMA ANTLAP150, teniendo en cuenta que se espera realizar la actualización del REDHAT (versión 9).

12. Sin embargo, debido a la programación de capacitaciones que realizará la Dirección de Proyectos e Inversión Pública a las entidades territoriales del Departamento de Antioquia, respecto a la

transmisión en el sistema de información SIFFMA, para efectos de medición de cumplimiento del indicador de Ley 617 de 2000, las cuales se llevarán a cabo durante la semana del 24 al 28 de febrero, se propuso realizar dicho proceso la semana siguiente, es decir, del 03 al 07 de marzo, con el fin de no afectar las sesiones de capacitación.

13. Finalmente, la firma contratista realizará el envío de la documentación técnica actualizada a la fecha correspondiente a manuales de procesos, arquitectura del sistema, microservicios, bases, y la respectiva documentación referente a cómo bajar y subir los servicios una vez culmine el proceso de pruebas de ejecución de SIFFMA bajo HTTPS sin servidor Apache Tomcat.

4. Proposiciones y varios

5. Compromisos pactados

No.	Compromiso	Responsable	Fecha de Logro	Resultado Esperado
1	Gestionar la asignación de dominio para SIFFMA QA	Área de Tecnologías de Información TI	Fecha pendiente de definir acorde con la culminación de la fase de capacitación	Asignación de dominio para el ingreso al sistema de información SIFFMA QA
2	Generar keystore.jks y archivo .csr con el alias basado en el subdominio de SIFFMA QA y enviarlo al funcionario Alexander Ocampo Benjumea, con copia al Director Daniel Alberto Arbeláez Echeverri, Carlos Antonio Serna Cortés, y Mauricio Andrés Ramírez Espitia, para que se efectúe le respectiva gestión por parte del Área de TI	M.R. Asesores y Consultores S.A.S.	Fecha pendiente de definir acorde con la culminación de la fase de capacitación	Entrega de archivos keystore.jks y archivo .csr para la gestión del certificado
3	Gestionar certificado de seguridad SSL con base en los archivos keystore.jks y archivo .csr	Área de Tecnologías de Información TI	Fecha pendiente de definir acorde con la culminación de la fase de capacitación	Generación de certificado de seguridad SSL para instalar en el cliente SIFFMA QA
4	Efectuar el formateo del servidor de aplicaciones SIFFMA ambiente QA ANTLAP150, teniendo en cuenta que se espera realizar la actualización del redHat (versión 9).	Área de Tecnologías de Información TI	Fecha pendiente de definir acorde con la culminación de la fase de capacitación	Servidor con sistema operativo actualizado a la versión más reciente posible

5	Generar la instalación de los servicios y los componentes necesarios para la ejecución de SIFFMA QA en el servidor ANTLAP150 incluyendo el certificado generado, para pruebas de accesibilidad mediante HTTPS.	M.R. Asesores y Consultores S.A.S.	Fecha pendiente de definir acorde con la culminación de la fase de capacitación	Garantizar que el sistema de información SIFFMA se ejecute directamente sobre el REDHAT mediante el uso del certificado SSL para ejecución sobre HTTPS
6	Solicitar análisis de vulnerabilidades al Grupo de Especialistas en Seguridad Informática de la Gobernación de Antioquia	Área de Tecnologías de Información TI	Fecha pendiente de definir acorde con la culminación de las actividades propuestas	Identificar si existen vulnerabilidades adicionales a las brechas de seguridad inicialmente relacionadas.
7	Envío de documentación técnica actualizada referente a manuales de procesos, arquitectura del sistema, microservicios, bases, y la respectiva documentación referente a cómo bajar y subir los servicios una vez culmine el proceso de pruebas de ejecución de SIFFMA bajo HTTPS sin servidor Apache Tomcat	M.R. Asesores y Consultores S.A.S.	Fecha pendiente de definir acorde con la culminación de las actividades propuestas	Entrega de documentación técnica actualizada

Firma de quien elabora

Firma de quien revisa y aprueba

Firma de quien elabora

Firma de quien elabora

Mauricio A. Ramírez C.
Wendy Yojana Cárdenas
Nombres de quienes elaboran

Sandra Marcela Lopez S.

Gema Adelaida Honolanda G.
Nombre de quien revisa y aprueba