CAI-2. INTEGRIDAD EN EL PROCESAMIENTO DE UNA EMPRESA INTERNACIONAL DE LOGÍSTICA

CONFIDENCIAL

En esta sesión de trabajo una empresa de logística mundial que dispone para el transporte terrestre de una cantidad de 12.736 vehículos (camiones y furgonetas) pertenecientes a 5 sedes en diferentes continentes nos presenta 3 consultas relacionadas con la **integridad de la información durante el procesamiento.**

Consulta 1. INTEGRIDAD EN EL PROCESAMIENTO DE LOS KILOMETROS RECORRIDOS USANDO UN SERVIDOR TCP/IP

Contexto: Para recoger los kilómetros recorridos por cada vehículo disponen de un **servidor TCP/IP** que tienen instalado en su sede de Ginebra (Suiza) donde los conductores de los vehículos acceden al fin de su jornada laboral través de una app. y donde en un cuadro de texto van introduciendo los kilómetros recorridos cada día, la aplicación servidora va contabilizando todos estos datos para obtener al final del mes el número total de kilómetros recorridos por todos los vehículos. La empresa ha detectado que dichos **datos no se corresponden con los gastos de combustible que tiene la empresa** (hay menos kms recorridos que los que realmente deberían haber), **por lo que consideran que podrían tener problemas de integridad en el procesamiento de la información en dicho servidor**. Previamente a esta consultoría ya se ha desarrollado una consultoría previa por **INSEGUS donde se ha informado que con respecto a la integridad de la información en el almacenamiento ni en la transmisión no existe problema alguno.**

Consulta: La empresa cliente nos solicita a INSEGUS como empresa consultora lo siguiente:

- **El código fuente comentado convenientemente de un servidor TCP/IP nuevo** para que puedan recoger los Kms. recorridos y que no haya problema alguno relacionado con la integridad en el procesamiento de los kms. recorridos por los vehículos. Se debe justificar las decisiones de diseño llevadas a cabo para seleccionar tal servidor TCP/IP.
- Especificación de **los límites de procesamiento de la información que tiene dicho servidor TCP/IP, el cliente agradece si aportan pruebas experimentales de dichos límites.**
- **Especificación de las requisitos que debe cumplir el entorno para el despliegue de dicho servidor TCP/IP y qué pasos debe seguir el cliente para desplegar dicho socket en el entorno.**

Consulta 2. INTEGRIDAD EN EL PROCESAMIENTO DE AYUDA AL CONDUCTOR USANDO WEBSOCKETS o WEBHOOKS

Contexto: **A**nte los múltiples cortes de carretera con que se encuentran los conductores en sus rutas diarias a lo largo de los diferentes continentes, la empresa desea de disponer de un Websocket o un Webhook donde a través de una app. puedan introducir los conductores la ruta diaria y que puedan recibir mensajes en tiempo real sobre los cortes de carretera y recomendaciones de rutas más óptimas para evitarlos (no desean acudir a aplicaciones servidoras de terceros para ello).

Consulta: El cliente nos solicita

- **Justificación técnica de la elección de un websocket o webhook para este caso concreto.**
- **El Código fuente comentado convenientemente del websocket o webhook que se recomienda.**
- **Especificación de los requisitos del entorno para el despliegue de dicho websocket o webhook y qué pasos debe seguir el cliente puede desplegar dicho websocket o webhook en dicho entorno.**

Consulta 3. INTEGRIDAD EN EL ALMACENAMIENTO Y PROCESAMIENTO EN SISTEMAS DE FICHEROS DESCENTRALIZADOS

Contexto: Finalmente dicha empresa esta valorando la posibilidad de implantar para su gestión anual de presupuestos mundial **un sistema de almacenamiento y procesamiento descentralizado, como alternativa a un almacenamiento cloud. Los datos son almacenados en diferentes nodos, como se observa en la figura de abajo, con el objetivo que los empleados accedan de forma eficiente y segura a dicha información en los 5 continentes.**

En el ejemplo siguiente, un empleado de América propone incrementar la partida presupuestaria B en 3 y a la misma vez una empleado de Suráfrica quiere decrementar la partida presupuestaria B en 2. Los resultados al realizarse de forma concurrente, podría dejar a B con 13 (el nodo de África propaga su resultado al resto de los nodos, obviando lo que ha realizado el nodo de América con B) o con 18 (el nodo de América propaga su resultado sin tener en cuenta lo que ha realizado el nodo de África con B) cuando el resultado esperado después de las dos modificaciones debería ser 16.

Consulta: El cliente conoce que una de las propuesta para descentralizar la información sería usar la tecnología blockchain pero la han descartado pues la consideran muy compleja y costosa para el problema que tienen.También conocen las estructuras de los Merkletree y Merkledag y que están relacionadas con la verificación eficiente y segura de la integridad en este tipo de sistemas, pero desconocen si técnicamente sería razonable su aplicación para este caso particular.

Por ello nos solicita información sobre **las correspondientes propuestas tecnológicas o protocolos para el aseguramiento de la integridad en el almacenamiento y procesamiento de la información en el sistema de gestión descentralizada de** las diferentes partidas presupuestarias para mitigar los riesgos relacionados con ello:

- **Especificación de una propuesta tecnológica para mitigar los riesgos relacionados con la pérdida de la integridad de la información en el almacenamiento** que son la no inmutabilidad y la no consistencia de los datos almacenados.
    - Respecto a l**a inmutabilidad de los datos** presupuestarios almacenados en los 5 diferentes nodos de la red descentralizada, el cliente nos requiere que por ejemplo la liberación de gastos llevadas a cabo en el tiempo no pueda ser modificada una vez realizada.
    - **Respecto a la consistencia de los datos** presupuestarios almacenados, el cliente nos indica que sean los mismos en los 5 diferentes nodos en los mayores espacios de tiempo posible.
- **Especificación de una propuesta tecnológica para mitigar los riesgos relacionados con la pérdida de la integridad de la información en el procesamiento** tales como: **No exclusión mutua en procesamiento descentralizado, el Sybil attack y el Eclipse attack.**

El cliente valora MUY POSITIVAMENTE que se justifiquen las decisiones técnicas que aparecen en las anteriores especificaciones.

Durante las reuniones de briefing con el cliente, nos ha comentado que estaban barajando en su empresa un conjunto de tecnologías tales como los algoritmos de DHT, tales como Kademlia, Chord y Pastry, algoritmos de exclusión mutua distribuida tales como el de Ricart and Agrawala y el algoritmo de Maekawa, y los sistemas de ficheros decentralizados: InterPlanetary File System (IPFS) y Bit Torren File System (BTFS), pero no tienen claro si todo ello responde adecuadamente a los anteriores problemas o existen mejores alternativas tecnológicas, por esto han acudido a INSEGUS.

Recomendaciones INSEGUS para elaborar el informe de las consultorías

- **Realizar una presentación esmerada del informe con el logo de INSEGUS, la fecha, la marca de agua o etiqueta que indica que el informe es confidencial, los márgenes justificados a ambos lados, resaltar la letra de las frases más relevantes y una fidelización del cliente. El informe de consultorías no es un trabajo académico sino empresarial.**
- **Revisar el Tema 2** (integridad en el almacenamiento y procesamiento), los temas consultados por el cliente pueden ser resueltos con dichos contenidos.
- Revisar la **Guía de elaboración y evaluación de los CAI**.
- No copiar **contenido de forma íntegra fuentes bibliográficas o Web de otros autores, sin citarlos, ni usar herramientas de IA generativa, sin citarla.**
- Tener en cuenta en todos las propuestas que se hagan que no se producen condiciones de carrera, no hay pérdida de datos por las diferentes velocidades de producción y consumo de datos de clientes y servidores y si las configuraciones de los firewalls de red que existen en la empresa permiten la comunicación entre sistemas informáticos.