CAI-3 - CONSULTORÍA SOBRE LA CONFIDENCIALIDAD EN EL ALMACENAMIENTO DE PRUEBAS DE DIAGNÓSTICO POR LA IMAGEN DE UNA GRAN ENTIDAD HOSPITALARIA

CONFIDENCIAL

En esta sesión de trabajo el cliente es una gran entidad hospitalaria que dispone de **un centro de diagnóstico por la imagen (**incluye radiología digital, gammagrafía, tomografía por emisión de positrones PET , Tomografías computarizadas, pruebas de medicina nuclear, Resonancia magnética, Ecografías**)** donde los resultados de todas las pruebas realizadas a los pacientes se **almacenan digitalmente en un sistema de almacenamiento tipo NAS (Network Attached Storage)** y situado físicamente en una sala de un edificio del complejo hospitalario (las transmisiones entre los dispositivo de diagnóstico y el servidor de almacenamiento las han asegurado por el protocolo TLS versión 1.3). En los dispositivos no queda información alguna de las imágenes que generan pues se envían inmediatamente al servidor de almacenamiento. Todos los equipos están conectados a la VLAN donde tqmbién se encuentra dicho NAS. También disponen en dicha VLAN de un NAS más que almacena las copias de seguridad de cada día de trabajo.
Los archivos de imágenes médicas de los pacientes son archivos del estándar DICOM (Digital Imaging and Communications in Medicine) que contienenDICOM contienen no solo la imagen en sí, sino también información relevante sobre la paciente (nombre, fecha de nacimiento, género,...), información del estudio (tipo de estudio, fecha y hora del estudio, descripción del estudio,...) y los parámetros de la imagen (configuración del equipo de adquisición, resolución, espaciado entre pixeles,...) y también archivos de imágenes en formatos estándares.
Actualmente se realiza el NAS sin cifrado alguno y se han producido ya fuga de esta información por **no estar cifrada por lo que es un sistema no confiable** (***untrustworthy***).
Las preocupaciones (**riesgos en ciberseguridad**) de la entidad hospitalaria son las siguientes:

- **Fuga de datos de datos que deben ser especialmente protegidos (datos de salud)** y que puede producir la pérdida de reputación de la entidad y sanciones en la Unión Europea que pueden ser de millones de euros por incumplimiento del Reglamento General de Protección de Datos (RGPD).
- **Posibles ataques de Ransomware**: Estos ataques **podrían cifrar indebidamente las imágenes, los almacenes de claves o ambos** y se tendrían que pagar cantidades millonarias para conocer la clave para descifrarlas.

Las consultas que nos presenta esta gran entidad hospitalaria son las siguientes:

Consulta 1. GESTIÓN Y ALMACENAMIENTO SEGURO DE LAS CLAVES Y DEMÁS ELEMENTOS PARA CIFRAR/DESCIFRAR LOS ARCHIVOS DICOM y DE IMÁGENES

Contexto: La entidad desea que el médico que solicita la prueba diagnóstica sea la única persona que tenga acceso a dicha prueba, para ello tienen implementado un riguroso control de acceso a la imágenes de diagnóstico. Pero al encontrarse cifrada en el sistema de almacenamiento solamente se podrá acceder a dicha información si se conocen las claves y demás elementos necesarios para el descifrado. En la entidad están pensando en **cifrar/descifrar bien con criptografía de clave simétrica como criptografía de clave asimétrica.**

Consulta: El cliente nos solicita:

- Especificación del proceso para gestionar las claves para que los médicos que solicitan las pruebas diagnósticas, puedan visualizar las imágenes que están cifradas en la entidad hospitalaria mediante el correspondiente descifrado. Tenga en cuenta que el gestor de claves podría estar en el puesto de trabajo del médico, en el propio NAS, en una nube pública.
- Mostrar al cliente de forma práctica **cómo se pueden almacenar las claves y cómo se puede recuperar las claves en un sistema concreto de almacenamiento seguro de las claves** y demás elementos que se necesitan para cifrar/descifrar los archivos de imágenes, justifcando los criterios que ha decidido el Security Team para tomar tal decisión.

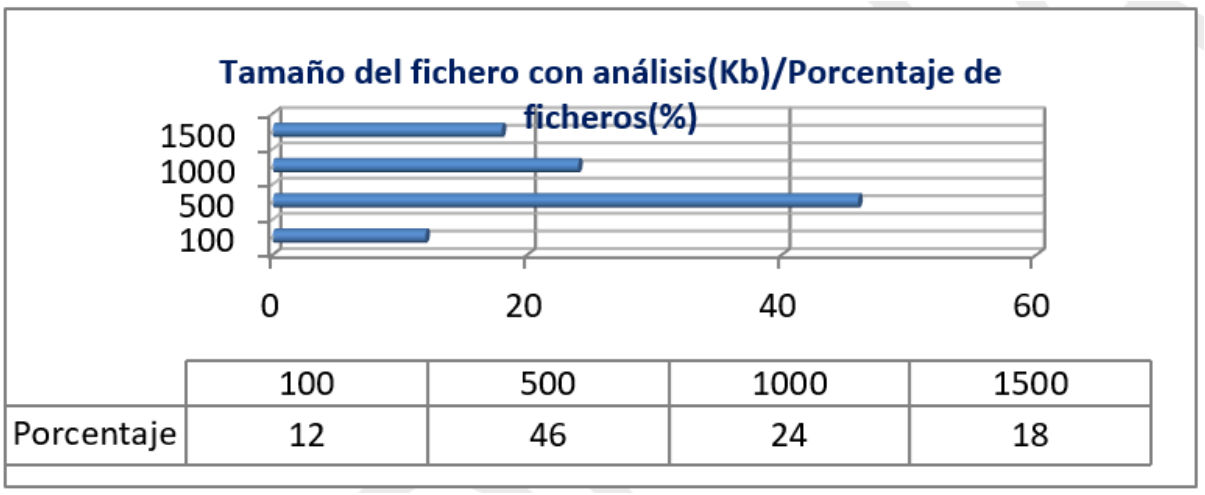
Lo que espera de nosotros el cliente son **propuestas concretas de INSEGUS para solucionar estos dos problemas relacionados con la confidencialidad de la información.**

Consulta 2. ELECCIÓN DEL ALGORITIMO DE CIFRADO/DESCIFRADO PARA APLICAR A LOS ARCHIVOS DICOM Y DE IMÁGENES

Contexto: También, la gran entidad hospitalaria nos indica que para el cifrado/descifrado le ha recomendado otra consultora de ciberseguridad que el algoritmo adecuado para ello podría ser AES-128-CBC. No obstante, dudan de ello pues creen que este algoritmo no responde a los criterios técnicos sobre un **algoritmo de cifrado/descifrado eficiente y seguro (debe incluirse el tamaño de la clave y los modos de cifrado) para** el sistema de almacenamiento y que han establecido los siguientes por orden de mayor a menor preferencia:

- **Alta Garantía que la información cifrada no sea inteligible por terceros**
- **Alto mantenimiento de la integridad de la información al aplicar los algoritmos de cifrado/descifrado considerados (**al respecto nos indican que la integridad de la información **es fuertemente preferida** a los tiempos de procesamiento del cifrado y descifrado)
- **Bajos tiempos medio de procesamiento del cifrado en los algoritmos considerados (**al respecto nos indican que los tiempos de cifrado son **moderadamente preferidos** con respecto a los tiempos de descifrado), puesto que hay muchos TeraBytes que cifrar y descifran al cabo del día y el procesamiento debería ser ágil.
- **Bajos tiempos medio de procesamiento del descifrado en los algoritmos considerado**

Para el cálculo de los tiempos medios puede tener en cuenta que los ficheros que se almacenan en la entidad hospitalaria actualmente tienen un tamaño aproximado de 100, 500, 1000 y 1500 Kb, con los porcentajes que aparecen en la figura 1.



	100	500	1000	1500
Porcentaje	12	46	24	18

Fig. 1. Porcentajes de ficheros (eje X) frente al tamaño (en Kb) aproximado de las pruebas digitales (eje Y).

Consulta: La entidad hospitalaria nos solicita que se escojan de los siguientes algoritmos de cifrado simétrico y asimétricos (pero están abierto a propuestas más eficientes/seguras de INSEGUS) para mejorar el algoritmo propuesto por los expertos en ciberseguridad:

chacha20, salsa20, blowfish, aes-128-cfb, aes-128-ecb, aes-128-ofb, aes-192-cbc, aes-192-cfb, aes-192-ecb, aes-192-ofb, aes-256-cbc, aes-256-cfb, aes-256-ecb, aes-256-ofb, camellia-128-cbc, camellia-128-cfb, camellia-128-ecb, camellia-128-ofb, camellia-192-cbc, camellia-192-cfb, camellia-192-ecb, camellia-192-ofb, camellia-256-cbc, camellia-256-cfb, camellia-256-ecb, camellia-256-ofb, cast5-cbc, cast5-cfb, cast5-ecb, cast5-ofb, serpent-128-ecb, serpent-128-cbc, serpent-128-cfb, serpent-128-ofb, rsa-2048-cbc,…

Lo que espera el cliente de INSEGUS son:

- **Los datos experimentales obtenidos, tales como los tiempos de cifrado/descifrado y si se mantiene íntegra la información enviada (muy recomendable presentar toda esta información en una tabla) de tres algoritmos de cifrado/discifrado diferentes, para justificar el más adecuado según sus criterios.**
- **Producto software con el algoritmo de cifrado/descifrado que escogido de los tres anteriores para cifrar/descifrar de acuerdo a las pruebas experimentales llevadas a cabo.** Nos indica que dicho producto se pueda usar pasándole como parámetros el archivo de imágenes y la clave para cifrar e igualmente para descifrar

Consulta 3. ELECCIÓN DEL SISTEMA DE COPIAS DE SEGURIDAD/RESPALDO PARA EVITAR LOS ATAQUES DE RANSOMWARE SOBRE LOS ARCHIVOS DE IMÁGENES ALMACENADAS.

Contexto: La preocupación de la entidad es mitigar los riesgos que podría producir el malware que cifra los archivos (RANSOMWARE) DICOM Y DE IMÁGENES en el NAS (**el cliente estima que la cantidad de datos total de los archivos que gestionan al día es de unos 4.5 TB**) para posteriormente solicitar un rescate, generalmente en forma de criptomonedas, a cambio de proporcionar la clave de descifrado o restaurar el acceso a los archivos. Dada las graves consencuencias que puede producir ello por la pérdida de la información de los pacientes, la entidad nos ha solicitado nuestra ayuda tecnológica, ya que se está planteando bien realizar:

- Copias de seguridad de dichos archivos de imágenes cifradas del NAS, bien en el otro NAS o en una nube pública convenientemente securizado para evitar el ransomware.
- Usar una nube pública para almacenar las copias de seguridad y cuyo precio durante un año para los archivos que dispone que no sea superior a 4.500 euros.

Consulta: El cliente nos solicita:

- **Especificar la gestión del ciclo de vida de los datos (DLM) de imágenes que propone para la entidad hospitalaria**. DLM es un enfoque para gestionar los datos en su ciclo de vida, desde la entrada hasta la destrucción de los datos del cliente. Esto permitirá comprender cómo piensa el consultor sobre las transformaciones y cambios de posición que van sufriendo las imágenes desde que el especialista médico pide la prueba de diagnóstico hasta que la recibe y posteriormente se destruye cuando no haya impedimiento legal que lo prohiba.
- J**ustificar las razones de la elección de una de las dos soluciones tecnológica anteriores para las copias de seguridad** (bien otro NAS en la propia empresa o en una nube pública) y que no sobrepase el presupuesto económico (4.500€/año). Tenga en cuenta los tipos de operaciones de respaldo. Los diferentes tipos de *backup* más corrientes son el respaldo completo, el incremental y el diferencial, o la copia en espejo, Tenga en cuenta que dada las características de esta entidad hospitalaria se necesita que el tipo de copia elegido

se puedan restaurar los datos en un tiempo mínimo, por tanto que tengan mínimos tiempo de recuperación (RTO). Debe especificar detalladamente en qué se basa la seguridad de dichas copias de seguridad frente al ransomware.

Consejos:

- **Revisar el** Tema 3 (confidencialidad en el almacenamiento), se tratan todos los temas relacionados con las consultas del cliente.
- Revisar la Guía de elaboración y evaluación de los CAI.
- Tener en cuenta **los check del ciclo de mejora continua que se han publicado para los anteriores CAI**
- No copiar contenido de **esta especificación en el informe solo apoyar la respuesta con el contenido del mismo.**
- No copiar contenido de herramientas de consulta o de IA generativa en el informe,
- En el caso que la **herramienta anti-plagio encuentre un grado mayor del 30% con respecto al texto ya publicado por otras personas o artefactos de IA generativa, se valorará toda el CAI con grado de satisfacción nulo.**