INGENIERÍA DE SEGURIDAD US
Avda. Reina Mercedes s/n. 41012 Sevilla

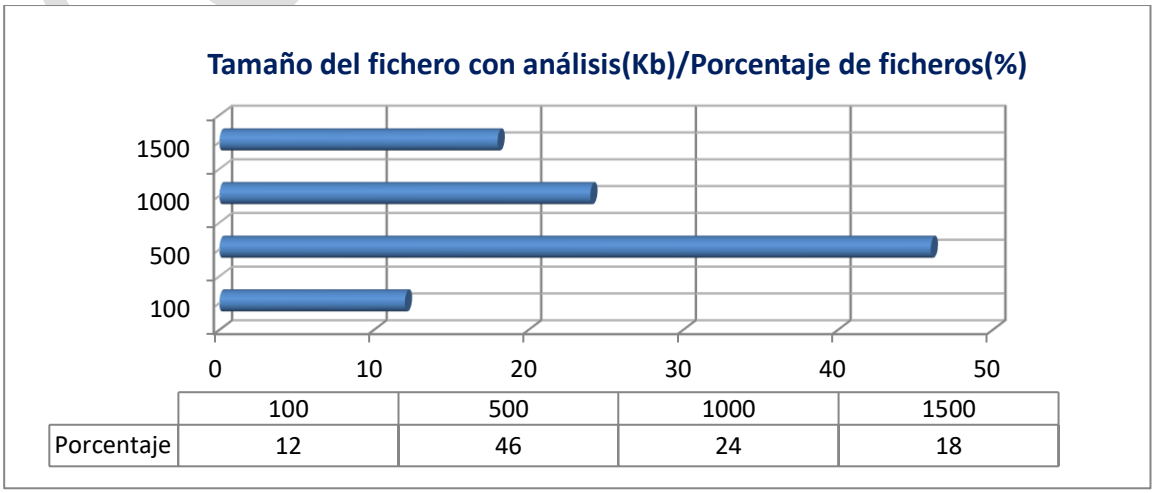
CAI 4. CONSULTA SOBRE LA CONFIDENCIALIDAD DE PRUEBAS ANALÍTICAS DE LABORATORIO DE ANÁLISIS CLÍNICOS DE UNA GRAN ENTIDAD HOSPITALARIA ALMACENADAS EN NUBE PÚBLICA

Información proporcionada por el cliente

Una gran área hospitalaria, que cuenta con múltiples edificios, dispone en uno de los edificios de **un Laboratorio de Análisis Clínicos donde los resultados realizados a los pacientes se almacenan digitalmente cada día en una nube pública** que tiene contratada dicha entidad y se realiza el almacenamiento sin cifrado alguno en origen, la confidencialidad de dichos análisis se delega a la nube pública.

Ante los múltiples problemas de confidencialidad que han ocurrido a nivel mundial en nubes públicas (y que se han expuesto en las sesiones presenciales de INSEGUS) y la necesidad de mantener estos datos especialmente protegidos, el Gerente de la entidad hospitalaria nos comunica que desea cifrar estos ficheros con los **resultados de los análisis clínicos antes de subirlos a la nube pública**. También, nos indica que los criterios técnicos a tener en cuenta en la decisión final sobre el algoritmo de cifrado, tamaños de clave y modo a usar son los siguientes:

1. **Complejidad temporal (tiempo medio de procesamiento del cifrado) en los algoritmos de cifrado (Muy Importante, equivaldría para el cliente a 7 sobre 9)**
2. **Complejidad temporal (tiempo medio de procesamiento del descifrado) en los algoritmos de descifrado (importante equivaldría para el cliente a 5 sobre 9)**
3. **Integridad de la información cifrada (Extremadamente Importante, equivaldría para el cliente a 9 sobre 9)**
4. **Garantía que la información cifrada no sea inteligible por terceros (Extremadamente importante, equivaldría para el cliente a 9 sobre 9).**



	100	500	1000	1500
Porcentaje	12	46	24	18

La gráfica de arriba representa los porcentajes de ficheros de análisis clínicos que existen en la entidad (eje X) frente al tamaño aproximado de los ficheros digitales (eje Y) que los contienen.

Consultas del cliente

De acuerdo con lo anteriormente relatado, las consultas de nuestro cliente hospitalario son las siguientes:

1. **Realizar un ranking de al menos tres algoritmos diferentes (la diferencia no se puede basar en el tamaño de la clave, pero si en el modo de cifrado) de acuerdo a criterios establecidos por el cliente para cifrar/descifrar los ficheros de análisis clínicos teniendo en cuenta los criterios técnicos de preferencia que nos han indicado arriba mediante un método de toma de decisiones multicriterio (MCDM).** Los técnicos informáticos del laboratorio de la entidad hospitalaria nos comunican también que ellos conocen los siguientes algoritmos (pero están abierto a propuestas más útiles y que respondan a los criterios establecidos arriba de la mejor manera posible):

   ChaCha20, ChaCha20-Poly1305, *aes-128-cbc, aes-128-cfb, aes-128-cfb1, aes-128-cfb8, aes-128-ecb, aes-128-ofb, aes-192-cbc, aes-192-cfb, aes-192-cfb1, aes-192-cfb8, aes-192-ecb, aes-192-ofb, aes-256-cbc, aes-256-cfb, aes-256-cfb1, aes-256-cfb8, aes-256-ecb, aes-256-ofb, aes-128-gcm, camellia-128-cbc, camellia-128-cfb, camellia-128-cfb1, camellia-128-cfb8, camellia-128-ecb, camellia-128-ofb, camellia-128-gcm, camellia-192-cbc, camellia-192-cfb, camellia-192-cfb1, camellia-192-cfb8, camellia-192-ecb, camellia-192-ofb, camellia-256-cbc, camellia-256-cfb, camellia-256-cfb1, camellia-256-cfb8, camellia-256-ecb, camellia-256-ofb, cast5-cbc, cast5-cfb, cast5-ecb, cast5-ofb, des-cbc, des-cfb, des-cfb1, des-cfb8, des-ecb, des-ede, des-ede-cbc, des-ede-cfb, des-ede-ofb, des-ede3, des-ede3-cbc, des-ede3-cfb, des-ede3-cfb1, des-ede3-cfb8, des-ede3-ofb, des-ofb, desx-cbc, rc2-40-cbc, serpent-128-ecb, serpent-128-cbc, serpent-128-cfb, serpent-128-ofb, serpent-128-gcm, rsa-2048-cbc.*
2. **Poner a disposición del laboratorio de la entidad hospitalaria el producto software que cifra/descifra un fichero de análisis clínico con el algoritmo primero del ranking resultante:** En la entidad hospitalaria necesita un programa que dado un fichero de análisis clínico cifre de forma segura y robusta dicho fichero y lo elimine el original del sistema de fichero, con la idea de mantener la confidencialidad de la información en la nube pública. También necesita otro programa para descifrar los ficheros cifrados que se descargan de la nube pública.
3. **Poner a disposición del laboratorio un sistema para la gestión segura y portable de las claves que se usarán tanto en el cifrado/descifrado (almacén de claves).** Cuando se produce el cifrado o descifrado se necesitarán claves de cifrado/descifrado, que es el elemento fundamental para el éxito de la confidencialidad de los resultados analíticos de los pacientes. Se requiere un sistema que de forma eficiente y con la seguridad adecuada evite el acceso al mismo a terceros.

El presupuesto económico para esta consultoría y que ha sido acordado con el cliente es de **1.690€+IVA**

Finalmente, nos comunica la entidad hospitalaria que se encuentra dispuesta a seguir colaborando con nuestra empresa en nuevas consultorías y proyectos sobre la Seguridad de la información en la entidad. Por ello, nos requiere la **mayor calidad posible en esta consultoría para poder abrir en breve nuevos proyectos con nuestra empresa.**

Normas del entregable

- El plazo de entrega de dicha consultoría finaliza el **día 13 de Abril a las 10:30 horas.**
- Se debe realizar la entrega al CISO de INSEGUS por parte del ingeniero ***Consultor Jefe*** a través de la Plataforma de Enseñanza Virtual de un fichero ***STnum*****CAI4.zip** que contenga el informe de la consultoría, los resultados del ***Multicriteria Decision Making (MCDM)*** llevado a cabo y el código del programa/script solicitado. **Se valorarán por el cliente las buenas prácticas en la codificación de dichos programas/scripts y la eficiencia de los mismos.**