Departamento de Lenguajes y Sistemas Informáticos
E.T.S. Ingeniería Informática. Universidad de Sevilla

Avda Reina Mercedes s/n. 41012 Sevilla
Tlf/Fax 954 557 139 **E-mail** lsi@lsi.us.es **Web** www.lsi.us.es

E.T.S. ingeniería informática

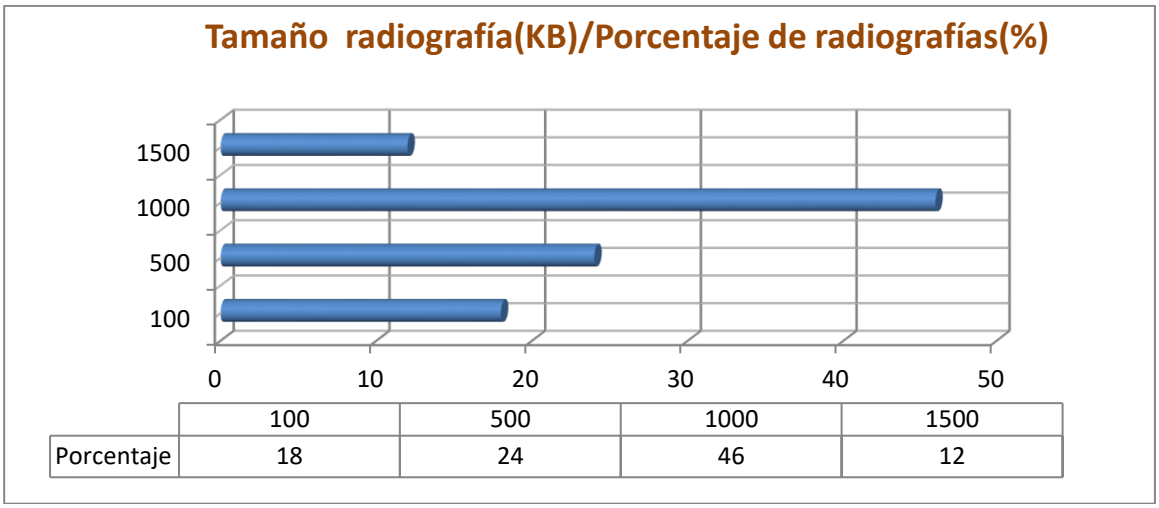
SEGURIDAD EN SISTEMAS INFORMÁTICOS Y EN INTERNET

CSI 3. CONSULTA SOBRE LA CONFIDENCIALIDAD DE LA INFORMACIÓN EN UNA ENTIDAD HOSPITALARIA

Un área hospitalaria, que cuenta con múltiples edificios, dispone de un sistema de realización de radiografías donde los resultados de estas se almacenan digitalmente en ficheros que no están cifrados y que son usados por el personal sanitario en toda la entidad, sin estar cifradas dichas radiografías en su transporte entre los edificios. Por tanto, se incumple claramente el art. 101.2 del RD 1720/2007 que aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y que indica que para datos de nivel alto "***La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte"***.

El Gerente de la entidad hospitalaria nos comunica que desea cifrar todas las radiografías que tiene almacenadas en dicho sistema para su posterior transmisión por las instalaciones hospitalarias a través de soportes y de las redes internas. Además, nos indica que los criterios tecnológicos que se deben tener en cuenta en la decisión final son los siguientes por orden de prioridad:

1. **<u>Garantía</u> de que la información cifrada no sea inteligible por terceros.**
2. **<u>Mínima Complejidad</u> temporal (tiempo de ejecución para cifrado/descifrado) y espacial (diferencia entre el tamaño del fichero cifrado y sin cifrar) de los algoritmos.**



	100	500	1000	1500
Porcentaje	18	24	46	12

La gráfica anterior representa los porcentajes de radiografías (eje X) frente al tamaño aproximado de los ficheros digitales (eje Y) que contienen las radiografías. (1 KB = 1024 bytes)

De acuerdo con ello, se pide:

a) **Establecer un ranking de preferencias sobre al menos tres algoritmos diferentes de cifrado** de acuerdo con los criterios especificados arriba por el cliente. Para ello se diseñarán experimentos que podrían servir para construir u**na tabla para el cifrado y otra tabla para el descifrado donde aparezcan** los valores con la media de 3 pruebas realizadas para cada casilla. Recuerde, por favor, que el cliente necesita conocer las pautas sobre qué algoritmo usar dependiendo del tamaño de los ficheros a cifrar/descifrar. **Indicar los modos de cifrado de bloque, padding y tamaño de clave que se han considerado más adecuados, y los criterios que se han tenido en cuenta para seleccionar el modo y el tamaño de la clave**. Se puede realizar una aplicación en un lenguaje concreto, o utilizar alguna herramienta de código abierto. Si utiliza el cifrado de una herramienta de compresión (7Zip por ejemplo) para hacer las pruebas active la opción de no comprimir. **Justifique con pruebas empíricas los aspectos enteriores**. Entregue el código utilizado o los pasos seguidos en el caso de uso de alguna herramienta. **(Valoración 20%)**

Cifrado/Descifrado Tamaño	Alg1 (ms)	Alg1 (MB)	Alg2 (ms)	Alg2 (MB)	Alg3 (ms)	Alg3 (MB)
Tamaño1						
Tamaño2						
Tamaño3						
Tamaño4						

b) **Especificar y realizar las pruebas que permitan comprobar la integridad tras el proceso cifrado/descifrado** de todas las radiografías que han sido tratadas. Informe sobre cómo lo ha realizado tecnológicamente. **(Valoración 10%)**

c) **Realizar un informe en el que se analice la salvaguarda de la confidencialidad de la información en carpetas o volúmenes de soportes físicos (discos duros), bien con herramientas del Sistema Operativo o herramientas de terceros**. El informe se centrará en un SO concreto (ejemplos: LUKS (Linux), BitLocker (Windows), FileVault (Mac) …), o en alguna herramienta multiplataforma (Veracrypt o similar). Debe contener información sobre los algoritmos de cifrado disponibles en cada caso y una justificación sobre que algoritmos y opciones se deben utilizar (si la herramienta lo permite). **(Valoración 15%).**

d) **También nos consulta sobre la posible pérdida de información en uno de los ordenadores que ha sido sustraído del Hospital.** Para la firma automatizada de documentos internos, se tenían almacenadas en dicho ordenador imágenes de tipo BMP, que contienen las firmas escaneadas de los médicos, su nombre y NIF. Dichas imágenes están cifradas con el algoritmo AES mediante una aplicación que utiliza una clave de 32 dígitos/letras/símbolos totalmente aleatorios, y las claves no estaban almacenadas en el ordenador. En el momento de la sustracción sólo dos ficheros estaban descifrados y el resto estaban cifrados. Se adjunta los dos ficheros descifrados y uno cifrado. Nos consultan si podemos estar tranquilos que la información almacenada en las imágenes cifradas no será accesible por nadie dadas las medidas de seguridad tomadas. ¿Se pueden tomar más medidas para proteger mejor la información guardada en las imágenes cifradas? La empresa valorará la justificación de la respuesta. **(Valoración 15%).**

Continuando con el **Plan Director de la Seguridad de la Información**, se pretende abordar en esta consultoría la **"Política de Correo Segura en la Entidad Hospitalaria"** que indica que se debería cumplir lo siguiente:

Todos los correos institucionales del personal médico y de enfermería en los que se contengan datos personales de salud deberán ir cifrados y firmados por la persona que los envía.

Una de las posibles soluciones para enviar correo seguro y firmado sería ***la instalación de PGP en un cliente de correo como por ejemplo Thunderbird*****,** aunque el Equipo Consultor podría escoger cualquier otra opción pues el cliente no requiere un sistema concreto. **PGP** junto con **S/MIME** son los protocolos más utilizados para conseguir privacidad y autenticación en los mensajes de correo electrónico. A ello ha contribuido su distribución como herramientas gratuitas, así como su puesta al día en sucesivas versiones mejorando sus capacidades. PGP se puede encontrar como plug-in para la mayoría de clientes de correo electrónico, incluyendo Exchange y Outlook de Microsoft, Eudora o Pine, Thunderbird, etc.

PGP nos permite:

- Cifrar mensajes y archivos para que no resulten legibles sin nuestra autorización (Confidencialidad).
- Firmarlos digitalmente para asegurarnos que no son modificados sin nuestro consentimiento (Integridad y autenticación).

Por otra parte, el Hospital tiene indicios de que se están utilizando Apps de mensajería entre los empleados. En concreto la aplicación Signal es la app de mensajería más utilizada.

Se pide en el informe de consultoría:

e) **Descripción detallada sobre cómo deben configurar los clientes de correo** el personal sanitario con el correspondiente plug-in en su cliente de correo (tutorial con capturas de pantalla). **(Valoración 20%)**

f) **Describir y presentar todas las pruebas que ha realizado para comprobar el correcto funcionamiento de las herramientas instaladas y configuradas**, mediante las correspondientes pruebas para 2 mensajes diferentes uno con fichero y otro sin fichero adjunto (desde cuentas de correo de los consultores). **(Valoración 10%)**

g) **Realizar un informe sobre la Seguridad en general en la App Signal.** Compare dicha App con otras de mensajería (por ejemplo Telegram) desde el punto de vista de la seguridad, ¿es la más segura?. Por otra parte el Hospital nos consulta si se debe prohibir el uso de dichas aplicaciones para el envío de mensajes que puedan contener información del Hospital. **(Valoración 10%)**

Normas del entregable

- El plazo de entrega de esta consultoría finalizará el próximo **día 2 de diciembre a las 8.30 horas.**
- Debe entregar el informe EquipoXCAI3.pdf que contenga todos los detalles que responden a los puntos de la consultoría y un zip con el proyecto (se debe indicar expresamente los alumnos del equipo que han participado en el trabajo).