

CAI3. CONSULTA SOBRE LA CONFIDENCIALIDAD DE LA INFORMACIÓN EN UNA ENTIDAD HOSPITALARIA



 Escuela Técnica Superior de
Ingeniería Informática

Índice

| | |
|--|----|
| Alcance y Objetivos de la Consultoría..... | 3 |
| Recursos de la Consultoría..... | 3 |
| Recursos Humanos..... | 3 |
| Recursos Tecnológicos..... | 3 |
| OpenSSL..... | 3 |
| BitLocker..... | 3 |
| Thunderbird..... | 4 |
| Aplicaciones de Mensajería Instantánea..... | 4 |
| Estudio Inicial..... | 4 |
| Actividades de la Consultoría..... | 4 |
| Tratamiento de las Imágenes..... | 4 |
| Proceso de Encriptación..... | 4 |
| Proceso de Desencriptación..... | 4 |
| Rastreo de Huellas..... | 5 |
| Análisis de la Posible Sustracción de Información..... | 5 |
| Análisis de la Salvaguarda de la Confidencialidad de Soportes Físicos..... | 5 |
| Creación de un Manual de Configuración de Thunderbird con PGP..... | 5 |
| Pruebas del Entorno Configurado..... | 6 |
| Análisis de las Aplicaciones de Mensajería Instantánea..... | 8 |
| Informe Final..... | 9 |
| Anexo I: Script de Cifrado..... | 11 |
| Anexo II: Script de Descifrado..... | 12 |
| Anexo III: Script de Rastreo de Huellas..... | 13 |
| Anexo IV: Configuración y Uso de Bitlocker..... | 14 |
| Anexo V: Manual de Configuración de Thunderbird con PGP..... | 15 |

Alcance y Objetivos de la Consultoría

Desde una entidad hospitalaria, se nos han hecho una serie de consultas sobre la Integridad y la confidencialidad de los datos que tratan, ya que actualmente incumplen 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. Por tanto, el principal objetivo de esta consultoría será resolver estos problemas, haciendo que los datos sean ininteligible por terceros, para ello se analizarán distintas formas de cifrado.

Además, se nos ha hecho una consulta, sobre si un contenido robado puede haberse visto comprometido, esto se verá más tarde cuando hablemos de los tipos de cifrado, ya que el cifrado de imágenes pude dejar rastros que no deseamos.

Y finalmente, analizaremos distintas formas de comunicación que no pongan en compromiso la Política de Correo Segura de la entidad hospitalaria, para ello hemos asumido que esta entidad usa la versión actual del sistema operativo Windows 10.

Recursos de la Consultoría

Para esta auditoría se harán uso de los siguientes recursos.

Recursos Humanos

El equipo de seguridad para esta asignatura se compone de los siguientes miembros:

- Barragán Candel, Marina - estudiante de Ing. Informática – Tecnología Informática, en la mención de Tecnologías de la información
- Calcedo Vázquez, Ignacio - estudiante de Ing. Informática – Tecnología Informática, en la mención de Sistemas de Información
- Polo Domínguez, Jorge - estudiante de Ing. Informática – Ingeniería de Computadores
- Sala Mascort, Jaime Emilio - estudiante de Ing. Informática – Tecnología Informática, en la mención de Computación

Recursos Tecnológicos

El equipo ha reunido un conjunto de herramientas con el objetivo de realizar la consultoría.

OpenSSL

OpenSSL se trata de un conjunto de herramientas, destinado principalmente para TLS y SSL, además de una librería general de criptografía que nos permitirá gestionar el cifrado y descifrado de la información fácilmente.

BitLocker

BitLocker es una aplicación de cifrado que nos permite proteger nuestro disco duro de un posible robo de información, para ello cifra volúmenes enteros, utilizando un algoritmo de cifrado AES en modo CBC con una clave de 128 bits.

Thunderbird es un cliente de correo, calendario, noticias y chat opensource muy popular, resultando una de las alternativas más comunes a clientes de pago como Outlook. Actualmente se encuentra en la versión 78.5.

Aplicaciones de Mensajería Instantánea

En el ultimo apartado de esta consultoría se analizarán distintas aplicaciones de mensajería con el objetivo de analizar los niveles de seguridad de cada una. Estas aplicaciones serán Telegram, WhatsApp y Signal, que usan principalmente cifrado end-to-end, E2EE.

Estudio Inicial

En primer lugar, nos debemos plantear que es el cifrado de información y cuales son algunos tipos de cifrado. El cifrado es un procedimiento que utiliza un algoritmo de cifrado para transformar un mensaje de tal forma que sea incomprendible para aquellos que no conozcan la clave del cifrado. Existen varios tipos de cifrado, pero en esta consultoría se va a atender a un solo tipo de cifrado, el cifrado con clave simétrica, donde la clave de cifrado y descifrado son la misma.

Dentro de los cifrados simétricos, encontramos distintos algoritmos de cifrado como AES o Rijndael, Aria o Camellia. Estos tres descritos son distintas implementaciones de un cifrado en bloques de 128 bits, con distintos tamaños de claves, en nuestro caso escogeremos una clave de 256 bits para asegurar una mayor seguridad. Además, tenemos que tener en cuenta que seguramente los archivos cifrados serán mayores que el tamaño de bloque, pudiendo dejar patrones dentro del archivo, por eso se consideran distintos modos de operación, que influencian los siguientes bloques.

En segundo lugar, tenemos que considerar la Política de Correo Segura, que nos indica que 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. Para ello se hará uso del gestor de correos como Thunderbird y un protocolo como PGP para la confidencialidad y autenticidad de la información que explicaremos más adelante.

Actividades de la Consultoría

Para poder realizar esta consultoría se han llevado a cabo las siguientes actividades

Tratamiento de las Imágenes

Para poder trabajar fácilmente con las imágenes sin tener que cifrarlas una a una, se han desarrollado pequeños scripts que ayudan en estas tareas.

Proceso de Encriptación

Para poder realizar la encriptación de las radiografías, se ha realizado un pequeño script que nos permite escoger la carpeta contenedora de imágenes y el tipo de cifrado que queremos, en nuestro caso, hemos elegido AES-256-CBC, Camellia-256-CBC y Aria-256-CBC. Este script se encuentra descrito en el [Anexo I: Script de Encriptación](#).

Proceso de Desencriptación

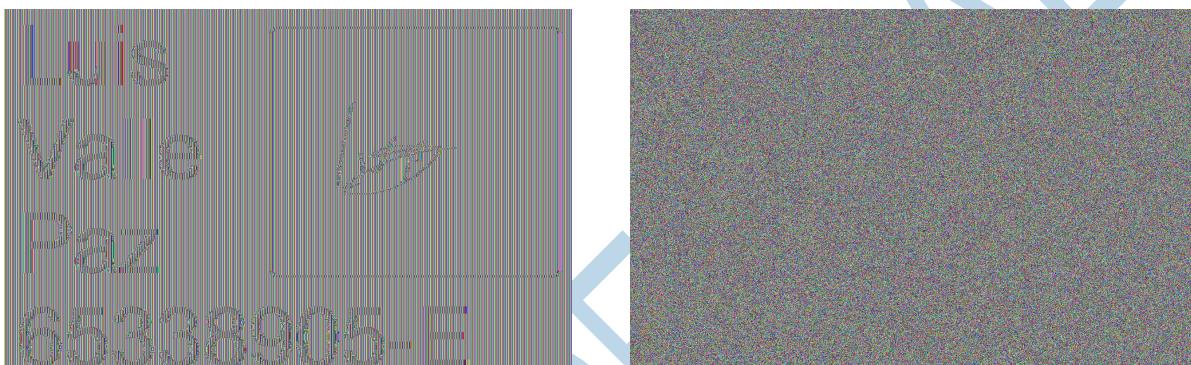
Al igual que en el proceso anterior, se ha usado un pequeño script que recibe las imágenes cifradas y el tipo de cifrado y nos devuelve las imágenes originales, en principio. Este script se encuentra descrito en el [Anexo II: Script de Desencriptación](#).

Este script adicional se ha realizado con el objetivo de restaurar las cabeceras de las imágenes en formato bmp de forma sencilla, también se puede consultar en el Anexo III: Script de Rastreo de Huellas.

Este script nos ayudará en el siguiente apartado para saber si la información filtrada puede ser comprometida.

Análisis de la Posible Sustracción de Información

La entidad sanitaria nos ha comunicado que se ha sustraído un ordenador que contenía imágenes con las firmas y DNI de tres médicos, dos de ellas no estaban cifradas, pero una tercera sí. Sin embargo, el modo de operación en el cifrado de los bloques podemos asumir que se trata de ECB, ya que restaurando la cabecera, hemos podido ver patrones que nos desvelan la información cifrada, como se observa en la imagen de la izquierda.



Si se hubiese estudiado cuáles son los casos de uso de este modo de operación no habría problemas, sin embargo para el cifrado de imágenes se hace patente que no es un buen modo de operación, siendo mejores CBC o CFB ya que se retroalimentan de los bloques anteriormente cifrados para generar más diversidad, dando como resultado una imagen como la derecha.

Análisis de la Salvaguarda de la Confidencialidad de Soportes Físicos

A parte de la información que un usuario medio puede considerar confidencial, existen muchos más datos guardados en todo los sistemas informáticos, y no siempre se encuentra en un estado de cifrado, por tanto hay que considerar medidas aún más drásticas como el cifrado de volúmenes de disco, donde se cifran sectores de los discos duros, haciendo que dado el caso de que haya una sustracción de los soportes físicos sea temporalmente imposible acceder a la información que contienen. Para dar solución a este problema en Windows, podemos hacer uso de una herramienta del sistema llamada BitLocker.

Bitlocker se trata de una aplicación de cifrado de volúmenes incluida en la Windows Suite desde la versión Windows Vista en 2007. Esta usa un algoritmo AES de cifrado en modo CBC con claves de 128 y 256 bits. Su uso es relativamente sencillo, sin embargo hay que activarlo mediante opciones más avanzadas para un usuario medio, por tanto se ha realizado una pequeña guía en el Anexo IV: Configuración y Uso de Bitlocker.

Creación de un Manual de Configuración de Thunderbird con PGP

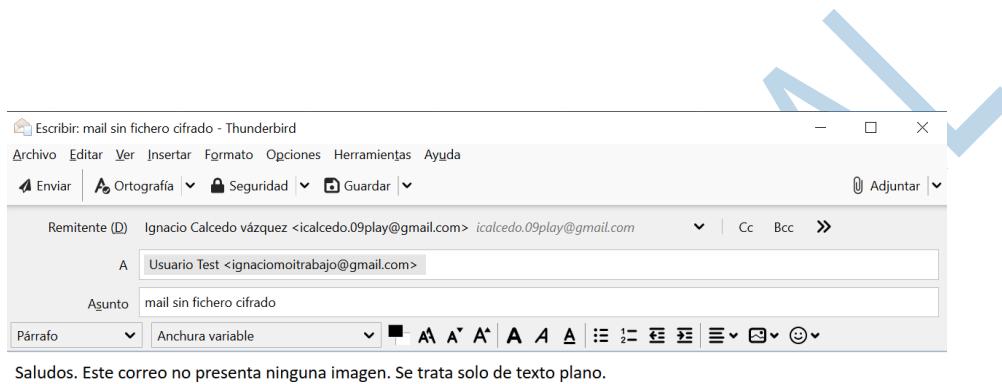
Para poder cumplir la Política de Correo Segura de la entidad hospitalaria, que indica que:

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.

Hemos elaborado un manual de configuración de un gestor de correo electrónico como es Thunderbird, donde a través de OpenPGP hemos configurado una clave pública que certificará la autenticidad del remitente. Este manual se encuentra en el [Anexo IV: Manual de Configuración de Thunderbird con OpenPGP](#).

Pruebas del Entorno Configurado

Para dejar constancia de que la comunicación PGP que se ha configurado es segura, el cliente ha solicitado que se realicen pruebas que corroboren un funcionamiento correcto de la implementación. Para ello, debemos asegurar la confidencialidad de la información enviada, para ello se han realizado dos envíos, uno que contenga solo texto y otro que contenga al menos una imagen adjunta.



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam non lacinia nulla. Nulla sem ex, fringilla vitae quam a, auctor elementum lacus. Mauris magna justo, fringilla tempus mollis a, vulputate ac magna. Aenean et nisi quis erat facilisis interdum. Morbi et pulvinar ante. Mauris placerat massa sem, ac lobortis turpis vulputate sed. Praesent eu metus quis nulla vehicula porta. Interdum et malesuada fames ac ante ipsum primis in faucibus. Vivamus sit amet commodo purus. Sed nulla mi, pellentesque sed lacinia non, hendrerit at nunc. Nunc posuere efficitur libero in posuere. Proin egestas arcu id quam tempus maximus.

Mauris semper nunc eget orci consectetur sollicitudin. In sodales lectus dolor, ac sagittis elit iaculis non. Proin sed mattis nisl, sed vulputate quam. Ut dictum lectus at risus commodo, quis sodales ligula commodo. Vestibulum euismod urna scelerisque odio ultrices maximus. Nam ultricies est vitae imperdiet efficitur. Suspendisse hendrerit sollicitudin ligula, non varius mauris blandit nec. Curabitur ac magna efficitur, iaculis ex sit amet, pharetra ipsum. Praesent faucibus velit ac velit euismod tempus eu sit amet eros. Integer id magna augue. Nam in tortor eget orci finibus vulputate. Nunc lacinia elit tristique lorem pretium, non fringilla odio egestas. Phasellus tempor diam sit amet tellus rhoncus, in ullamcorper turpis hendrerit.



Saludos. Este correo adjunta una imagen. Se trata de texto plano y una radiografía

Etiam non lacinia nulla. Nulla sem ex, fringilla vitae quam a, auctor elementum lacus. Mauris magna justo, fringilla tempus mollis a, vulputate ac magna. Aenean et nisi quis erat facilisis interdum. Morbi et pulvinar ante. Mauris placerat massa sem, ac lobortis turpis vulputate sed. Praesent eu metus quis nulla vehicula porta. Interdum et malesuada fames ac ante ipsum primis in faucibus. Vivamus sit amet commodo purus. Sed nulla mi, pellentesque sed lacinia non, hendrerit at nunc. Nunc posuere efficitur libero in posuere. Proin egestas arcu id quam tempus maximus.

Mauris semper nunc eget orci consectetur sollicitudin. In sodales lectus dolor, ac sagittis elit iaculis non. Proin sed mattis nisl, sed vulputate quam. Ut dictum lectus at risus commodo, quis sodales ligula commodo. Vestibulum euismod urna scelerisque odio ultrices maximus. Nam ultricies est vitae imperdierit efficitur. Suspendisse hendrerit sollicitudin ligula, non varius mauris blandit nec. Curabitur ac magna efficitur, iaculis ex sit amet, pharetra ipsum. Praesent faucibus velit ac velit euismod tempus eu sit amet eros. Integer id magna augue. Nam in tortor eget orci finibus vulputate. Nunc lacinia elit tristique lorem pretium, non fringilla odio egestas. Phasellus tempor diam sit amet tellus rhoncus, in ullamcorper turpis hendrerit.

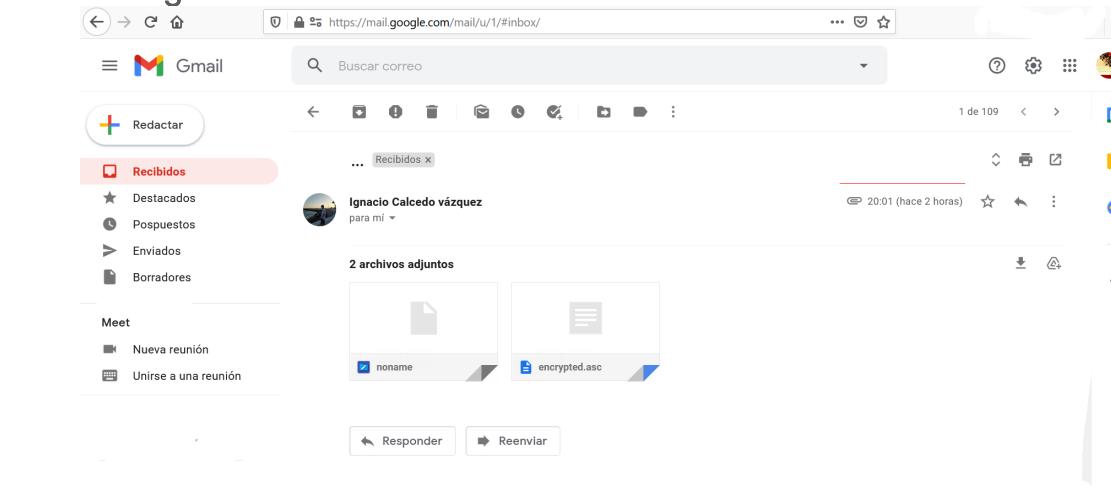
OpenPGP

Una manera sencilla de comprobar que el correo se ha enviado y cifrado correctamente utilizando PGP es intentar abrir el correo en cuestión, a través de otro cliente de correo, ya sea Gmail, Outlook... Si accedemos a este cliente y revisamos el correo, podemos comprobar como se demuestra en la imagen inferior, que el correo es completamente ilegible. Otra forma sería eliminar los certificados de Thunderbird y nos daría el mismo resultado.

En las siguientes capturas de pantalla se puede observar que ambos mensajes no tienen ningún parecido con lo enviado anteriormente.

The screenshot shows a Gmail inbox with the following details:

- Header:** https://mail.google.com/mail/u/1/#inbox/
- Toolbar:** Back, Forward, Home, Search (Buscar correo), More options, Settings, Grid icon.
- Left Sidebar:** Redactar, Recibidos (highlighted in red), Destacados, Pospuestos, Enviados, Borradores, Meet, Nueva reunión, Unirse a una reunión.
- Message Preview:** From Ignacio Calcedo Vázquez (profile picture), sent at 18:44 (hace 3 horas). The message body says "para mí".
- Attachments:** 2 archivos adjuntos: noname (document icon) and encrypted.asc (file icon).
- Bottom Buttons:** Responder (Reply), Reenviar (Forward).



Análisis de las Aplicaciones de Mensajería Instantánea

Signal App es una aplicación de mensajería instantánea similar a las conocidas Whatsapp y Telegram, cuya diferencia radica en un mayor nivel seguridad, y menor almacenamiento de información del usuario en la aplicación.

Respecto a la seguridad, la aplicación utiliza un protocolo de cifrado extremo a extremo, también adoptado por Whatsapp, por lo que si estos mensajes se interceptan por el camino, no será posible leer su contenido, por otra parte Telegram solo aplica este tipo de cifrado en conversaciones privadas.

Al hacer uso por primera vez de la aplicación, nos requerirá la creación de un PIN de seguridad, con esto nuestra cuenta quedará cifrada en los servidores de la propia aplicación, y podremos acceder a ella aunque cambiemos de dispositivo. Al ser un PIN personalizado, nadie tendrá acceso a la cuenta si se escoge una PIN con responsabilidad.

Comparte algunas características con Telegram, al ser ambas de código abierto y poder usar mensajes que con un tiempo de visualización limitado. A diferencia de las otras, Signal no te permite tomar capturas de pantalla mientras se usa la aplicación, para así mantener la confidencialidad de las conversaciones. Además se puede especificar un tamaño máximo de longitud para las conversaciones, y lo que es más importante, los datos guardados en la aplicación corresponden exclusivamente al número de teléfono del usuario, y el día de su última conexión. Mientras que Telegram y Whatsapp almacenan el número, la última conexión, la lista de contactos del usuario, el nombre y el estado o biografía. De esta forma, la retención de información que pudiera ser comprometedora por parte de Signal, es mínima. El resto de utilidades de la aplicación son las mismas que las dos mencionadas, permitiendo enviar mensajes, llamadas de voz, audios, fotos y todo lo usual.

Informe Final

Finalmente, se ha establecido lo siguiente, en cuanto al cifrado de las imágenes, se han analizado los tiempos de tres algoritmos distintos, AES, Aria y Camellia, donde en la tablas inferiores se muestra como AES es mejor en todos los ámbitos, tanto a la hora de cifrar como descifrar, siendo la mejor opción ya que combina la seguridad de un algoritmo robusto, una clave suficientemente grande como para hacer el descifrado por fuerza bruta difícil, además de un modo de operación que no genera patrones en imágenes, todo eso agregado al tiempo de ejecución bajo.

| Cifrado | AES-256-CBC | ARIA-256-CBC | CAMELLIA-256-CBC |
|----------|-------------|--------------|------------------|
| Tamaño | Tiempo (ms) | Tiempo (ms) | Tiempo (ms) |
| 100KBx4 | 29 | 33 | 31 |
| 500KBx4 | 37 | 62 | 43 |
| 1000KBx4 | 39 | 73 | 62 |
| 1500KBx4 | 57 | 93 | 83 |

| Descifrado | AES-256-CBC | ARIA-256-CBC | CAMELLIA-256-CBC |
|------------|-------------|--------------|------------------|
| Tamaño | Tiempo (ms) | Tiempo (ms) | Tiempo (ms) |
| 100KBx4 | 27 | 31 | 35 |
| 500KBx4 | 29 | 54 | 54 |
| 1000KBx4 | 39 | 68 | 6 |
| 1500KBx4 | 47 | 87 | 80 |

Por ello recomendamos el uso de AES con una clave de 256 bits con CBC.

Sin embargo, tras el descifrado de la información, tenemos que asegurar que sea haya ningún problema de integridad intrínseco a estos algoritmos, para ello usaremos las imágenes de prueba que se han obtenido de un Data Set de Kaggle sobre radiografías de personas que sufren la COVID-19, estas imágenes han sido tratadas y convertidas a las especificaciones que nos indica el cliente, imágenes de 100, 500, 1000 y 1500 KB en formato bmp.

Gracias a una modificación del [PAI](#), donde se ha usado el script, apicultor, en vez del servicio para comprobar que los hashes no se hayan visto modificados, hemos realizado rápidamente las comprobaciones, a continuación se ofrecen unos resultados simplificados, con ejemplos de cada tamaño usado.

| | | |
|---------|--|---|
| 100KB: | b03b465d36fc85f25398f38cb901c70fa0e49c826f67c1c4dc8246bd7352cdd4 | Ej101.bmp |
| | b03b465d36fc85f25398f38cb901c70fa0e49c826f67c1c4dc8246bd7352cdd4 | aes-256-cbc/DECRYPT/Ej101-aes-256-cbcDECRYPT-aes-256-cbc.bmp |
| 500KB: | ff0c0b6a34d630917345e1ea932ab176b4d6102b7f5d44cb0a4fc90b7e40c552 | Ej501.bmp |
| | ff0c0b6a34d630917345e1ea932ab176b4d6102b7f5d44cb0a4fc90b7e40c552 | aes-256-cbc/DECRYPT/Ej501-aes-256-cbcDECRYPT-aes-256-cbc.bmp |
| 1000KB: | 8e961f0cf31c165404134f606ce1f1ab86c5e7f878f3131f460bf282ec99a620 | Ej1001.bmp |
| | 8e961f0cf31c165404134f606ce1f1ab86c5e7f878f3131f460bf282ec99a620 | aes-256-cbc/DECRYPT/Ej1001-aes-256-cbcDECRYPT-aes-256-cbc.bmp |
| 1500KB: | 18eafa62a5e00dbfe42cf78224d5833025909b7433f9c8824114d0946fae3333 | Ej1501.bmp |
| | 18eafa62a5e00dbfe42cf78224d5833025909b7433f9c8824114d0946fae3333 | aes-256-cbc/DECRYPT/Ej1501-aes-256-cbcDECRYPT-aes-256-cbc.bmp |

A pesar de las medidas de seguridad que se pueden tomar a la hora de almacenar datos confidenciales de los usuarios del hospital, recomendamos el uso de mayores niveles de seguridad, ya que en el caso de que se efectúe una sustracción del equipo informático del hospital, no podemos garantizar que información se encontrará correctamente cifrada en el momento del robo. Por tanto recomendamos el uso de herramientas de cifrado de volúmenes como se ha expuesto en los apartados anteriores, ya que con una clave lo suficientemente robusta, hará que la información sea irrecuperable, dejándonos solo ante el problema de la seguridad física de los dispositivos.

Frente al paradigma de las comunicaciones dentro del hospital, hemos creado un manual de configuración donde se implementa en Thunderbird un protocolo PGP, cumpliendo con las expectativas del cliente. En relación a las aplicaciones de mensajería instantánea hay que distinguir los modos de uso, ya que no es lo mismo un uso a nivel de tratamiento de información de los pacientes a un uso organizativo dentro de la organización, permitiendo una comunicación rápida que podría mejorar la calidad del servicio. Por ello, debemos ser tajante con el uso de estas aplicaciones más allá del carácter organizativo.

CONFIDENCIAL

Anexo I: Script de Cifrado

Este script realizado en bash hace uso de las herramientas de OpenSSL para cifrar la información. Para hacer uso de él, simplemente recibe un directorio con las imágenes, el modo de cifrado, una clave y un vector de inicialización inicial.

```
#!/bin/bash
mkdir "$1"/"$2"
key="$3"
iv="$4"
for file in "$1"/*
do
    if [ -f "${file}" ] ; then
        nombre=$(basename "$file" .bmp)
        openssl enc $2 -e -in "${file}" -out "$1"/"$2"/"$nombre""$2".bmp -K "$key" -iv "$iv"
    fi
done
```

CONFIDENCIAL

Anexo II: Script de Descifrado

Este script realizado en bash hace uso de las herramientas de OpenSSL para descifrar la información. Para hacer uso de él, simplemente recibe un directorio con las imágenes, el modo de cifrado, la clave adecuada y su vector de inicialización inicial.

```
#!/bin/bash

mkdir "$1"/"$2"/DECRYPT/
key="$3"
iv="$4"
for file in "$1"/"$2"/*
do
    if [ -f "${file}" ] ; then
        nombre=$(basename "$file" .bmp)
        openssl enc $2 -d -in "${file}" -out "$1"/"$2"/DECRYPT/"$nombre"DECRYPT"$2".bmp -K "$key" -iv "$iv"
    fi
done
```

CONFIDENCIAL

Anexo III: Script de Rastreo de Huellas

Este script realizado en bash repara las cabeceras de las imágenes en formato bmp. Para hacer uso de este, solo tenemos que pasarle un directorio con las imágenes cifradas y una imagen bmp en buenas condiciones .

```
#!/bin/bash
mkdir "$1"/SNIFFED/
for file in "$1"/*
do
    if [ -f "${file}" ] ; then
        nombre=$(basename "$file" .bmp)

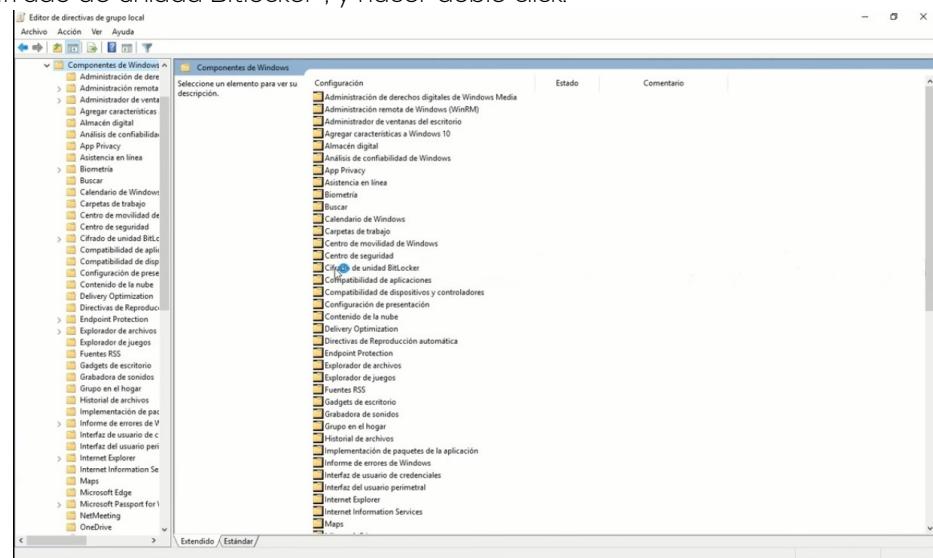
        head -c 54 $2 > header
        tail -c +55 $file > body_cbc
        cat header body_cbc > "$1"/SNIFFED/"$nombre"Sniff.bmp

        rm header
        rm body_cbc
    fi
done
```

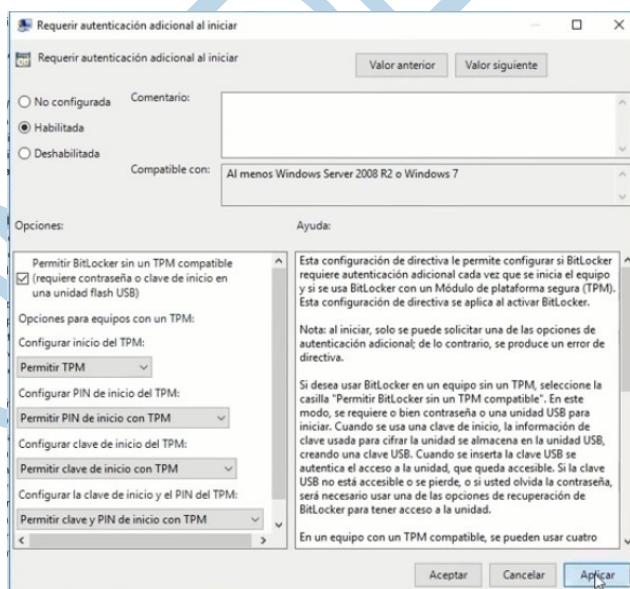
CONFIDENCIAL

Anexo IV: Configuración y Uso de Bitlocker

Antes de empezar, hay que realizar una serie de pasos previos, debemos iniciar sesión en Windows con una cuenta que tenga privilegios de administrador, y a continuación, en el cuadro de búsqueda de Windows, buscar "Editar directiva de grupo", esto nos llevará a la siguiente ventana. Aquí debemos buscar la opción de "Cifrado de unidad Bitlocker", y hacer doble click.



Esto nos abrirá un cuadro de diálogo donde tenemos que seleccionar las opciones que aparecen en la imagen inferior.

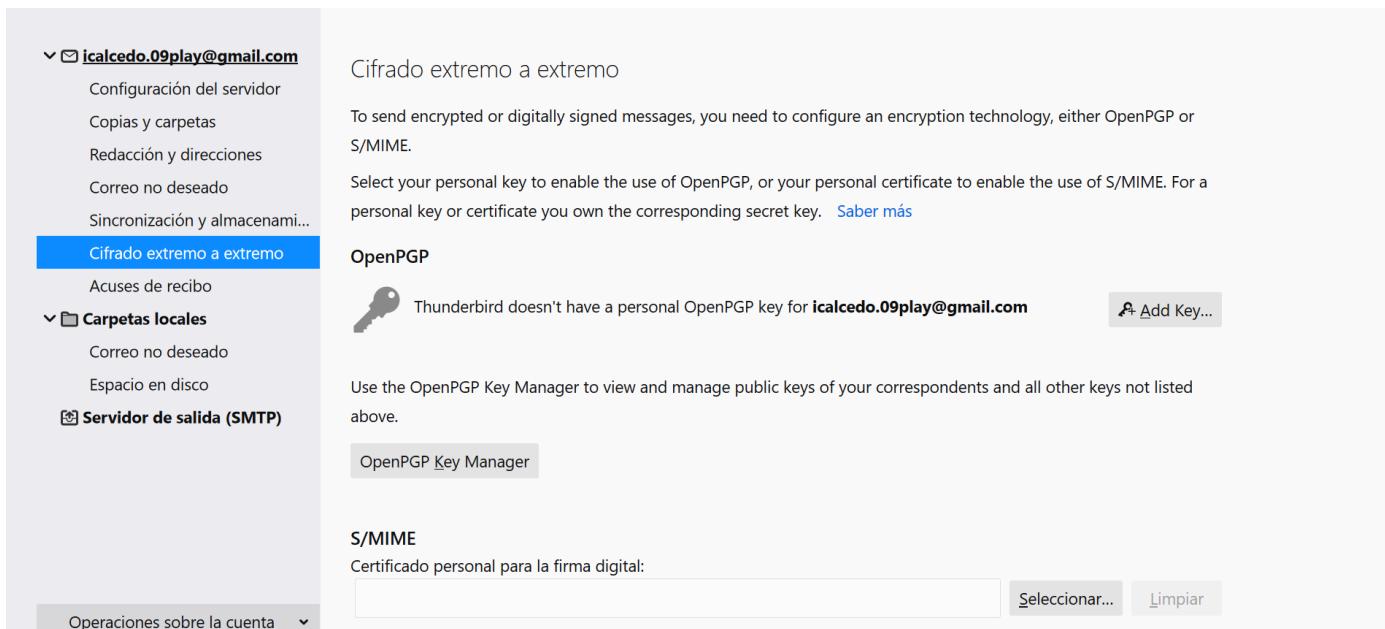


Para activar Bitlocker, en el cuadro de búsqueda de Windows, buscar "Administrar BitLocker" y a continuación se debe clickar la opción Activar BitLocker, que se encuentra junto a la unidad que se desea cifrar. Acto seguido, elegimos escribir una contraseña, recordando siempre que sea segura y elegimos nuestra opción de copia de seguridad de la clave de recuperación preferida. Tras esto reiniciamos nuestro sistema y ya tenemos nuestro volumen cifrado.

Anexo V: Manual de Configuración de Thunderbird con PGP

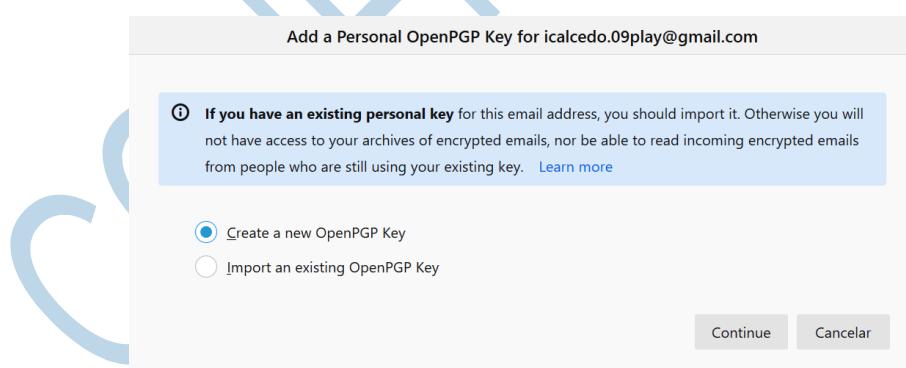
En primer lugar, abrimos Thunderbird, y posteriormente en la pestaña de inicio, buscamos el menú de acciones que se encuentra en la esquina superior derecha y abrimos la "Configuración de cuenta", sino tenemos una cuenta en el sistema, la abrimos con "Operaciones de la cuenta" y seguimos con los pasos que nos indican, si ya la tenemos configurada, nos podemos saltar este paso.

A continuación, seleccionamos Cifrado extremo a extremo, y hacemos click sobre "Add Key..." en el apartado de OpenPGP.



The screenshot shows the Thunderbird account configuration window. On the left, there's a sidebar with account names (including 'icalcedo.09play@gmail.com') and various configuration sections like 'Configuración del servidor', 'Copias y carpetas', etc. The main panel is focused on 'Cifrado extremo a extremo'. It contains text about enabling encryption using OpenPGP or S/MIME, a note that Thunderbird lacks a personal OpenPGP key for the selected account, and a 'Add Key...' button. Below this, there's a 'OpenPGP Key Manager' button. Further down, the 'S/MIME' section is shown with a 'Certificado personal para la firma digital:' input field and 'Seleccionar...' and 'Limpiar' buttons.

Una vez realizado estos pasos, se nos resaltará una pestaña que nos indica si queremos crear o importar una clave nueva, en nuestro caso, crearemos una nueva.



The screenshot shows a modal dialog titled 'Add a Personal OpenPGP Key for icalcedo.09play@gmail.com'. It includes a note about existing keys, two radio button options ('Create a new OpenPGP Key' selected, 'Import an existing OpenPGP Key' unselected), and 'Continue' and 'Cancelar' buttons at the bottom.

Tras haber realizado el último paso, aparecerá una ventana en la que configurar qué parámetros deseamos que tenga nuestra clave. Además del parámetro identidad, Thunderbird nos solicitará dos parámetros esenciales de nuestra clave. El primero es el periodo de expiración de la misma. Por defecto Thunderbird lo marca en 3 años, pero en función de las necesidades del cliente, se puede configurar para que el periodo sea menor o mayor, en nuestro caso indicaremos que el plazo sea de un año para así poder revisar la autenticidad cada año. El segundo de los parámetros a configurar es el tipo de clave que se va a utilizar en los procesos de comunicación. Por defecto, Thunderbird indica que la key será para el tipo de cifrado RSA y su tamaño será de 3072 bits, pero la configuraremos de forma que se usen 4096 bits aumentando así la seguridad de los certificados. Una vez especificados las opciones, haremos click sobre "Generate Key".

Add a Personal OpenPGP Key for icalcedo.09play@gmail.com

Generate OpenPGP Key

Identity Ignacio Calcedo vázquez <icalcedo.09play@gmail.com> - icalcedo.09play@gmail.com

Key expiry
Define the expiration time of your newly generated key. You can later control the date to extend it if necessary.

Key expires in years

Key does not expire

Advanced settings
Control the advanced settings of your OpenPGP Key.

Key type: RSA

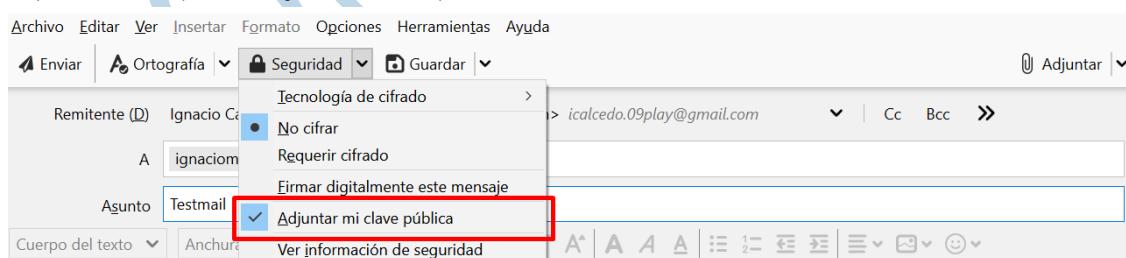
Key size: 3072

Buttons: Generate key, Cancelar, Go back

Una vez seleccionados los parámetros, aparecerá por pantalla un aviso explicando que la generación de la clave tomará varios minutos y que no se interrumpa Thunderbird durante el proceso. Confirme el aviso y espere a que finalice la generación de su clave.

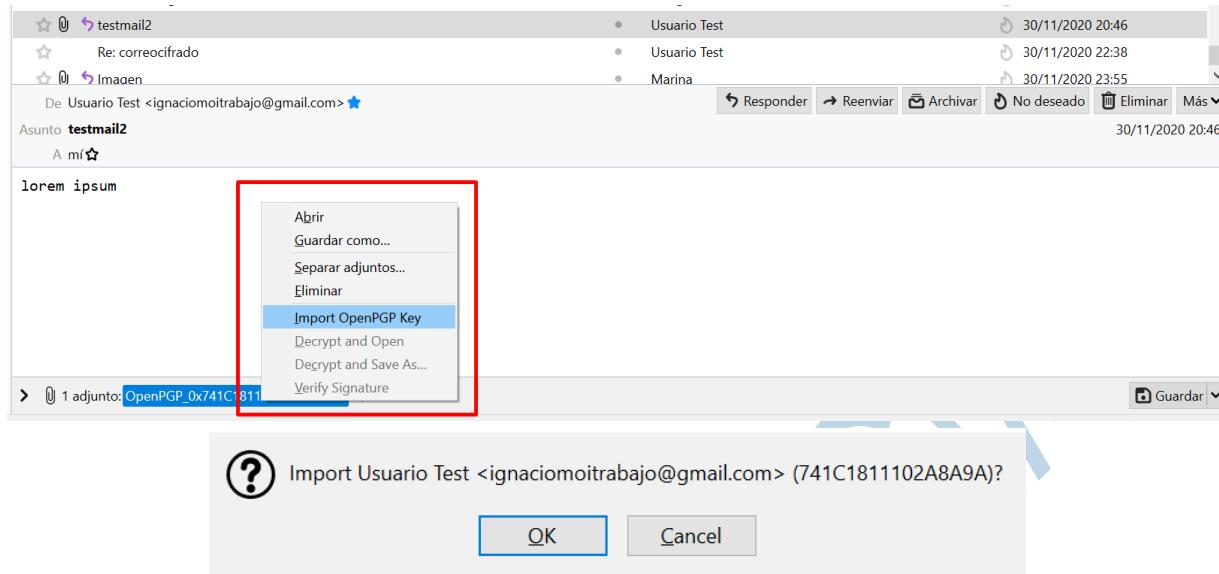
Tras la finalización de la generación de la clave por parte de Thunderbird, es necesario dar una serie de pasos adicionales para poder establecer una configuración óptima que permita la comunicación segura. Para poder establecer comunicaciones cifradas por correo es necesario conocer la clave pública del correspondiente y aceptarla. Destacamos especialmente aceptarla, ya que la política de seguridad de Thunderbird entiende que al aceptar una clave, el usuario está confiando en la identidad del poseedor de la clave. Por tanto, se recomienda encarecidamente comprobar la identidad del poseedor de la clave que se reciba en el correo.

La manera más directa de obtener la clave de un correspondiente es que se mande un correo con la clave pública adjuntada, bien directamente o de manera regular, o bien en una cabecera escondida. Para ello, seleccione la opción de redactar en su bandeja principal y cree un correo para el correspondiente al que desea transmitir información privada. Una vez redactado el correo, despliegue la pestaña de seguridad y active la opción adjuntar clave pública.



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Para importar la clave del usuario, haga click derecho en la clave pública adjuntada y seleccione Import openPGP key, donde tendrá que decidir si aceptar al usuario y su clave pública para importarlo en su sistema.



Una vez que se hayan realizado con los pasos descritos previamente descritos, la creación de los mensajes cifrados se facilita mucho. En caso de que quiera establecer una comunicación cifrada de punto a punto, redacte el correo al usuario al que desea contactar. Una vez finalizado, despliegue el menú de la herramienta de Seguridad. Ahí podrá seleccionar la opción requerir cifrado, lo que activará OpenPGP. Si quiere revisar la información de la comunicación, así como de la clave pública del usuario remitente, siempre puede hacer clic en "Ver información de seguridad", donde se le llevará a otra ventana en la que podrá gestionar las claves públicas del remitente.