Aplicación para el envió de información cifrada por medio de dirección MAC
Trabajo Terminal No 2021-B076

Alumnos: Cabrera Salinas U riel, García Dolores Fernando.
Directores: M. en C. Mendez Segundo Laura, M. en C. Hernández Avilés Fernando Dante.
Turno de Presentación del TT: MATUTINO
E-mail: cabrera.cs.personal@outlook.com, fernandogarciadolores@gmail.com .

Resumen - El envío de archivos por medios digitales constituye una necesidad de primer orden en la sostenibilidad de los sistemas de información. Dado que los servicios de mensajería y almacenamiento no son capaces de cumplir con las exigencias de privacidad requeridas por ciertos usuarios, el presente trabajo tiene como propósito el desarrollo de una aplicación movil que permite cifrar documentación e imágenes de uso cotidiano por medio de un cifrado simétrico haciendo usando del algoritmo AES en el cual la llave será generada a partir de la dirección MAC del dispositivo con lo que se reduce el riesgo de acceso a la información ya que, el uso de la dirección MAC constituye una alternativa válida contra vulnerabilidades a la confidencialidad al ser única para cada dispositivo móvil. Cabe destacar, que para acceder a esta aplicación se creara un registro del dispositivo en el sistema, una vez registrado se podrán mandar solicitudes para que los usuarios puedan aceptar o declinar si desean ser el remitente de un archivo cifrado.
Palabras clave - Criptografía, Ingeniería de Software, Seguridad Web.

1. Introducción

En la actualidad, una gran parte de la población envía todo tipo de información a través de la red, es común que gran parte de esta información compartida sea de carácter sensible, es decir, el remitente desea que solo ciertas personas puedan ver esta información, sin embargo, en ocasiones estos datos se ven comprometidos ya que, terceras personas pueden tener acceso a ellos. Por lo cual, existen algoritmos de cifrado que ofrecen mayor seguridad a dicha información a través de un cambio en su estructura que garantiza la disponibilidad para quien el autor requiera. Dichos algoritmos hacen uso de llaves para proteger dicha información, sin embargo, estas pueden verse expuestas,comprometiendo la seguridad y confidencialidad de estos datos. Para un mayor entendimiento, se hace referencia a dos métodos de cifrado utilizados en diversos sistemas de intercambio de datos:

- Cifrado simétrico: Los sistemas de cifrado de clave privada o simétrico utilizan una sola clave que comparten el remitente y el destinatario. Ambos deben poseer la clave; el remitente cifra el mensaje mediante la clave y el destinatario descifra el mensaje con la misma clave. Para poder establecer una comunicación privada, tanto el remitente como el destinatario deben mantener la clave en secreto. [1]
- Cifrado asimétrico: El cifrado de clave pública o asimétrico utiliza un par de claves relacionadas matemáticamente. Un mensaje cifrado con la primera clave debe descifrarse con la segunda clave y un mensaje cifrado con la segunda clave debe descifrarse con la primera clave. Cada participante en un sistema de claves públicas dispone de un par de claves. Una clave se designa como clave privada y se mantiene secreta. La otra clave se distribuye a quien lo desee; esta clave es la clave pública.[1]

Entendiendo las implicaciones de estos métodos, es indispensable encontrar algún dato único que los teléfonos inteligentes provean, pues a partir de este, se puede construir una llave de cifrado. En

la actualidad, la mayoría de los teléfonos inteligentes cuentan con una tarjeta de red la cual permite conectarse a internet y cada tarjeta dispone de una dirección MAC la cual garantiza una clave única por dispositivo. Es por lo anterior que, en el presente trabajo se considera a la dirección MAC como un potencial candidato para servir como llave al momento de cifrar archivos.

Para extender el marco teórico necesario, se describen a continuación algunos de los sistemas para el cifrado y protección de archivos existentes, con base en el requerimiento presentando en este documento.

Software	Características	Precio
Cryptomator	Permite cifrar una carpeta entera a través de criptografía simétrica mediante el algoritmo AES. Disponible para Windows, MacOS, Linux, IOS y Android.	Gratuito
Bitlocker	Permite cifrar cualquier tipo de archivo o contenido: del disco duro interno, de discos de arranque y USB utilizando AES de 128 bits. Disponible para Windows.	Gratuito.
AES Crypt	El software es capaz de integrarse directamente con el menu, es decir, una vez descargado, basta con pulsar el botón derecho sobre un archivo para desplegar el menú de opciones el cual contará con la opción de cifrar. Como su nombre lo indica usa el algoritmo AES para cifrar los archivos. Disponible para Windows, Android, macOS y IOS.	Gratuito.
Private Photo Video Locker	Simula ser una calculadora común y corriente, sin embargo, dentro de la aplicación se encuentra una galería que oculta fotos y vídeos, para mostrar dicho contenido es necesario ingresar la contraseña previamente definida. Disponible para Android.	Gratuito
File Locker	Permite proteger con contraseña diferentes tipos de archivos, creando una ubicación segura donde se almacenan y protegen dichos archivo. Disponible para Android.	Gratuito.

Figura 1: Tabla 1. Resumen de sistemas Relacionados.

2. Objetivo

Crear una aplicación móvil, que permita cifrar archivos por medio de una llave simétrica generada a partir de la dirección MAC del dispositivo remitente usando el algoritmo AES y generar un contenedor que permita visualizar dicha información dentro del sistema, lo cual ofrecerá al usuario seguridad al compartir sus archivos.

2.1. Objetivos específicos

- Desarrollar un módulo de cifrado en el cual se genere una llave tomando como base la dirección MAC.
- Desarrollar un módulo de seguridad para la generación de la llave simétrica.
- Aplicar el cifrado para archivos con extensión: *.jpg*, *.png*,*.pdf*.

- Desarrollar instancias de envió generadas por solicitud de usuario para garantizar la comunicación y confidencialidad de la información en la aplicación por medio de un sistema de cifrado asimétrico de clave pública y privada.
- Integrar los medios de visualización necesarios para el despliegue de los archivos en la aplicación.

3. Justificación

Como parte de una respuesta integral a las necesidades de confidencialidad y comunicación directa es necesario comprender que algunos usuarios requieren que su información se vea encapsulada por diversos medios de seguridad. Una de las alternativas para esta problemática es el uso de servicios de almacenamiento en la nube, los cuales permiten reservar un espacio controlable donde el cliente pueda resguardar sus archivos y dar acceso únicamente a quienes lo requieran o bien se opta por el traspaso de información a través de medios de comunicación más convencionales como los servicios de mensajería integrados para la disponibilidad de todos, sin embargo, estos se ven gravemente afectados por diversas vulnerabilidades y son susceptibles a traspaso no autorizado por su jerarquía de permisos que no bloquea directamente la posibilidad de compartir dichos espacios con alguien no autorizado por el propietario.

A raíz de esto, un rediseño de estos servicios que sea capaz de proveer algún modulo que pueda mitigar los riesgos antes mencionados, tiene una alta demanda en un entorno donde necesitamos mantener nuestra confidencialidad. Por lo anterior, la elaboración de este trabajo pretende implementar un modelo de cifrado y descifrado que nos permita reducir considerablemente la perdida de información sensible y los problemas que esto puede causar.

Para esto, se toma como base la dirección MAC del dispositivo remitente para cifrar con el algoritmo AES. Dado que la dirección MAC se encuentra presente en cualquier dispositivo móvil inteligente y funge a su vez como un identificador para dicho dispositivo, puede ser reformulada atraves de la combinancion de su flujo de caracteres para conseguir un nuevo flujo pseudoaleatorio que pueda servir como llave para el algoritmo AES.

Anudado a lo anterior, es importante aclarar que para llegar a un grupo más amplio de usuarios se debe realizar la implementación de dicho modelo en una aplicación móvil, a bien de que este servicio pueda ser aprovechado aun por quienes no tienen la confidencialidad como una necesidad de primer orden.

4. Productos o Resultados esperados

Con la elaboración de este proyecto, se pretende conformar una aplicación móvil para dispositivos con sistema operativo Android. En dicha aplicación se permitirá cifrar y descifrar los archivos, usando como base la dirección MAC obtenida del dispositivo.

Para la evaluación del TT-1, se prevé tener listo un prototipo de generación de la llave de cifrado para el algoritmo AES, integrando un módulo donde quienes comparten la información puedan disponer de la llave con la que se cifrará. Además, al finalizar la constitución de estas funcionalidades, se conformará la documentación correspondiente.

En la evaluación de TT-2, se pretende tener los prototipos del sistema completados y en funcionamiento, el reporte de cumplimiento del proyecto y los correspondientes manuales técnicos y de usuario.

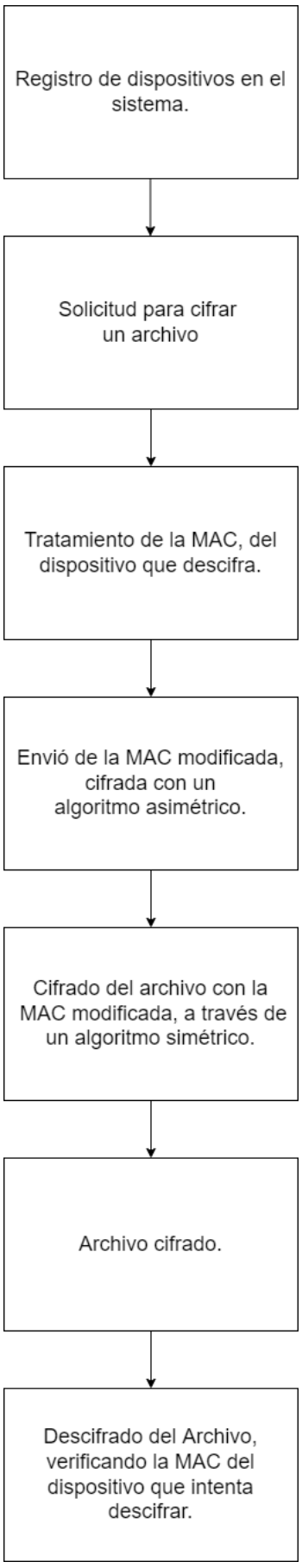

Figura 2: Diagrama de sistema

5. Metodología

Acorde a las exigencias de un correcto desarrollo de proyectos es necesario establecer las normativas y metodologías de desarrollo necesarios para garantizar la organización, cumplimiento y enfoque direccionado de nuestro producto final. Como parte de una planeación que nos permita cumplir activamente con los diversos módulos que integran la aplicación, se ha convenido en usar un Modelo basado en prototipos comenzando con la definición de los objetivos globales e identificación de requerimientos y posterior desarrollo por áreas de esquema a bien de conseguir vistas preliminares del software, una integración controlada y fase de pruebas ágil.

Este modelo de desarrollo evolutivo nos permitida realizar una constante identificación del cumplimiento a los requisitos iniciales y un replanteamiento del esquema de trabajo acorde a las exigencias del proyecto en tiempo real. Dicho modelo de avance será asimilado y aplicado bajo sus etapas principales que nos aseguran un cumplimiento integral y oportuno de los objetivos planteados, estas etapas a seguir son:

- Recolección de requisitos.
- Modelado del sistema.
- Construcción del prototipo.
- Desarrollo y pruebas.
- Refinamiento del producto.
- Evaluación de avance e integración modular.

Los prototipos considerados para el desarrollo del producto final son:

1. Módulo de regristro de usuarios.
2. Manejo de solicitudes de conexion de envio.
3. Módulo obtencion y modificación de Direccion MAC.
4. Modelo de intercambio de llaves de cifrado.
5. Modelo de almacenamiento de llaves de cifrado.
6. Módulo de cifrado de archivos jpg y png.
7. Módulo de cifrado de archivos pdf.
8. Módulo de decifrado de archivos jpg y png.
9. Módulo de decifrado de archivos pdf.
10. Módulo de Visualización de archivos jpg y png.
11. Módulo de Visualización de archivos pdf.

Para garantizar un óptimo desarrollo y posterior satisfacción de los usuarios, el proyecto se apoyara enteramente en la normativa *ISO 27001*. La aplicación de dicho estándar nos permitirá establecer los requisitos necesarios para mantener y mejorar un sistema de gestión de la seguridad de la información.

A bien de cumplir con la estructura del estándar antes mencionado es necesario establecer los puntos clave para el desarrollo del producto final:

- Evaluación de riesgos: Para garantizar la usabilidad de nuestro producto final se deberá constituir un análisis de los potenciales problemas que podrían afectar a nuestro modelo de manejo de información.

- Implementación de medidas para el manejo de riesgos: Una vez identificada la localización y repercusiones de los potenciales problemas será propuesto un modelo sistémico que responda activamente a dichos riesgos.
- Constitución de políticas y procedimientos: Con base en la implementación técnica para el manejo de errores, serán definidas y acotadas las normativas que posteriormente servirán de base para detallar el correspondiente SGSI.

6. Cronogramas

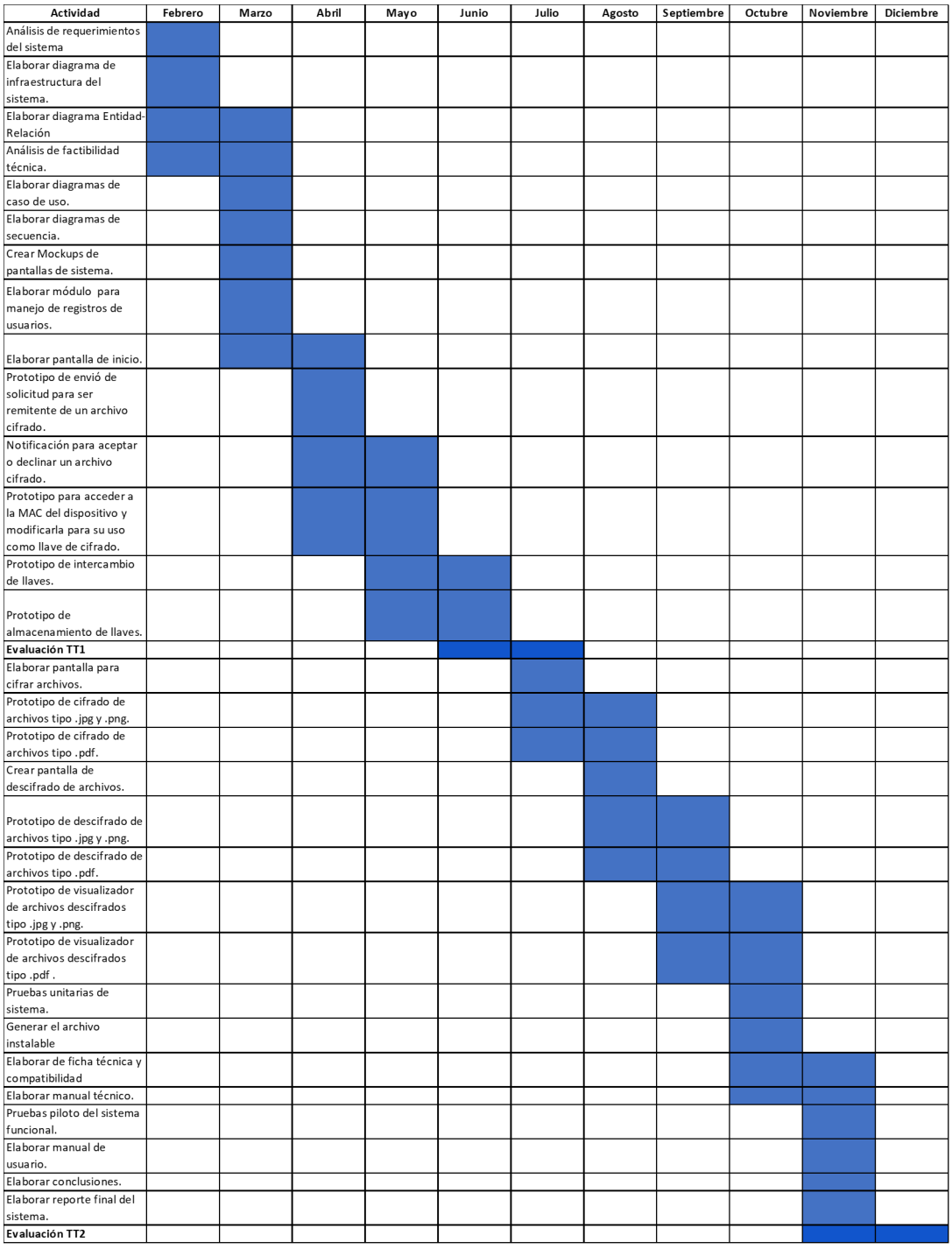

Figura 3: Cronograma General

Actividad	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Análisis de requerimientos del sistema											
Elaborar diagrama Entidad-Relación											
Elaborar diagramas de caso de uso.											
Crear Mockups de pantallas de sistema.											
Elaborar pantalla de inicio.											
Notificación para aceptar o declinar un archivo cifrado.											
Prototipo de intercambio de llaves.											
Evaluación TT1											
Elaborar pantalla para cifrar archivos.											
Prototipo de cifrado de archivos tipo .pdf.											
Prototipo de descifrado de archivos tipo .jpg y .png.											
Prototipo de visualizador de archivos descifrados tipo .jpg y .png.											
Pruebas unitarias de sistema.											
Elaborar de ficha técnica y compatibilidad											
Pruebas piloto del sistema funcional.											
Elaborar conclusiones.											
Evaluación TT2											

Figura 4: Cronograma - Fernando García Dolores

Actividad	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Elaborar diagrama de infraestructura del sistema.											
Análisis de factibilidad técnica.											
Elaborar diagramas de secuencia.											
Elaborar módulo para manejo de registros de usuarios.											
Prototipo de envió de solicitud para ser remitente de un archivo cifrado.											
Prototipo para acceder a la MAC del dispositivo y modificarla para su uso como llave de cifrado.											
Prototipo de almacenamiento de llaves.											
Evaluación TT1											
Prototipo de cifrado de archivos tipo .jpg y .png.											
Crear pantalla de descifrado de archivos.											
Prototipo de descifrado de archivos tipo .pdf.											
Prototipo de visualizador de archivos descifrados tipo .pdf .											
Generar el archivo instalable											
Elaborar manual técnico.											
Elaborar manual de usuario.											
Elaborar conclusiones.											
Elaborar reporte final del sistema.											
Evaluación TT2											

Figura 5: Cronograma - Uriel Cabrera Salinas

7. Referencias

[1] IONOS Digitalguide, 2021. Cifrado asimétrico: transmisión segura de datos. [En línea] Disponible en: https://www.ionos.mx/digitalguide/servidores/seguridad/cifrado-asimetrico/ [Accedido el 20 de Octubre de 2021].

[2] Ibm.com, 2021. Criptografía de clave pública. [En Línea] Disponible en: https://www.ibm.com/docs/es/integration-bus/10.0?topic=ssmkhh-10-0-0-com-ibm-etools-mft-doc-ac55940–htm [Accedido el 21 de Octubre de 2021].

[3] Prieto, J., 2021. Algoritmo de generación de llaves de cifrado basado en biometría facial. [En Línea] Bogotá, Colombia: Universidad Piloto de Colombia. Disponible en: http://polux.unipiloto.edu.co:8080/00002315.pdf [Accedido el 28 Octubre de 2021].

[4] IONOS Digitalguide, 2021. Cifrado asimétrico: transmisión segura de datos. [En Línea] Disponible en: https://www.ionos.mx/digitalguide/servidores/seguridad/cifrado-asimetrico/ [Accedido el 28 de Octubre de 2021].

[5] Adeva, R., 2021. Cómo cifrar tus archivos y carpetas más importantes. [En Línea] ADSLZone. Disponible en: https://www.adslzone.net/reportajes/software/que-es-encriptar-cifrar-programas/ [Accedido el 28 de Octubre de 2021].

[6] IONOS Digitalguide, 2021. Dirección MAC (Media Access Control). [En Línea] Disponible en: https://www.ionos.mx/digitalguide/servidores/know-how/direccion-mac/ [Accedido el 28 de Octubre de 2021].

8. Alumnos y Directores

Cabrera Salinas Uriel - Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM. Especialidad: Sistemas, Boleta: 2019630214, Tel:5569133336, email: ucabrera1500@alumno.ipn.mx

Firma: _____

García Dolores Fernando - Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM. Especialidad: Sistemas, Boleta: 2019630442, Tel:5538034558, email: fernandogarciadolores@gmail.com

Firma: _____

M. en C. Laura Méndez Segundo - Profesora investigadora de la Escuela Superior de Cómputo del IPN. M. en C. en Ingeniería Eléctrica con especialidad en computación (CINVESTAV 1998), Licenciatura en Informática (Universidad Veracruzana 1991). Certificado de SCRUM Master en el 2017, Áreas de Interés: Bases de Datos, Ingeniería de Software, UML. cómputo educativo, realidad aumentada, criptografía y procesamiento de imágenes. Tel: 57-29-60-00 Ext. 52032, Email: lmendez@ipn.mx

Firma: _____

M. en C. Fernando Dante Hernández Avilés - Profesor Invitado por la Escuela Superior de Cómputo.Doctorante en el CUGS. Maesrtro en Ciencias por el CIDETEC. Ingeniero en Comunicaciones y Electrónica Especializado en comunicaciones. Coordinador Operativo del Centro Nacional de Cálculo.

Firma: _____

TURNO PARA LA PRESENTACIÓN DEL TRABAJO TERMINAL:
MATUTINO

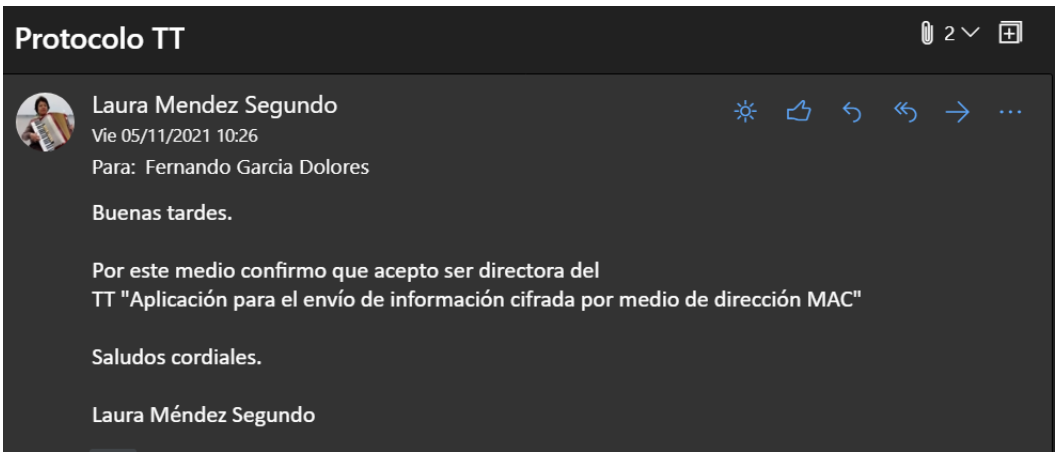

Figura 6: Aceptación del Protocolo - M. en C. Laura Méndez Segundo

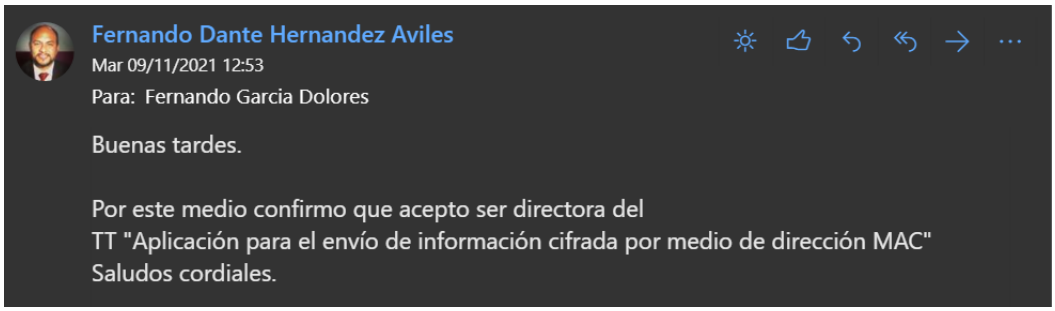

Figura 7: Aceptación del Protocolo - M. en C. Fernando Dante Hernandez Aviles

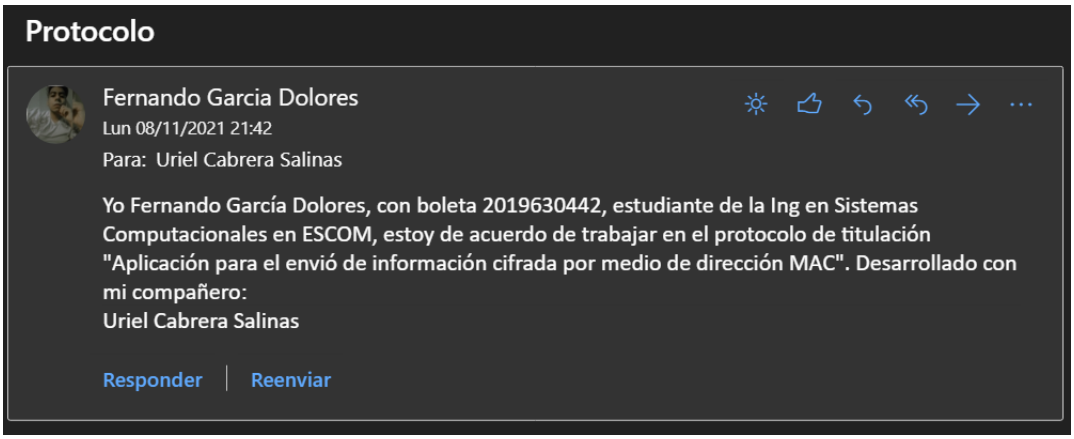

Figura 8: Aceptación del Protocolo - García Dolores Fernando

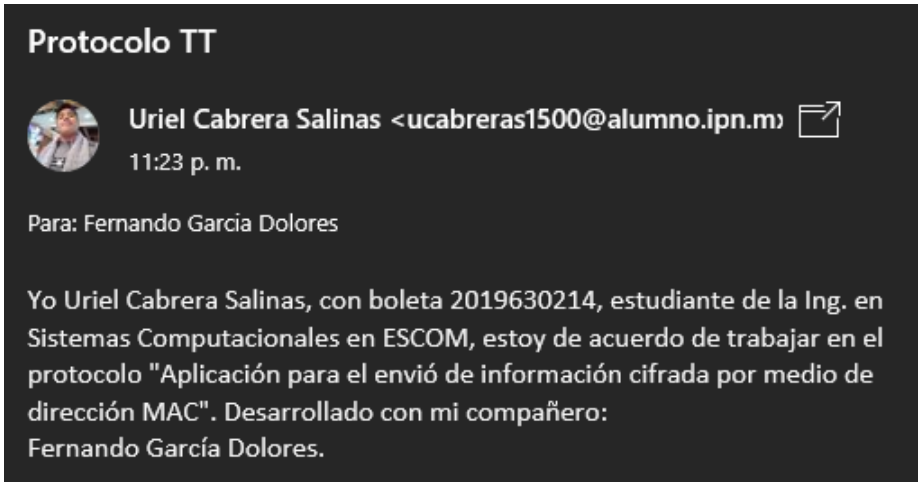

Figura 9: Aceptación del Protocolo - Cabrera Salinas Uriel