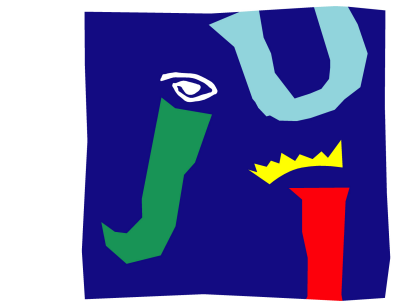


UNIVERSITAT JAUME·I

Trabajo Fin de Grado

CORREO ELECTRÓNICO Y FIRMA DIGITAL

Presentado por:

Belén Gargallo Nieto

Tutor/a:

Filiberto Pla Bañón

Grado en Criminología y Seguridad

Curso académico 2021/22

ÍNDICE

EXTENDED SUMMARY

The Internet is one of the greatest tools created by mankind. In addition, thanks to the Internet, everything has been evolving more and more, making life easier and simpler for human beings. Such is its impact on our society that it has even changed the way we communicate both personally and globally. It has made it possible to communicate with others who are miles away.

One of the greatest tools it has provided us with is e-mail, which is used daily all over the world. Such is its impact that even institutions use this means of communication in their daily operations and notifications. Just like the Internet, the number of users of this service has been increasing day by day, taking advantage of the many benefits it offers. However, there are those who are unaware of its dangerous side, vulnerabilities that many want to take advantage of.

For this reason, this work has the objective of making known what e-mail is, as well as exposing the various problems that occur or may occur when using them. Thus, the main objectives are: the study of the security and the problems of criminality that are associated to the use of the electronic mail; in the same way tools and techniques will be contributed so that we can maintain our electronic mail safe before the problems that will be exposed; and in addition the advantages that it offers to us will be exposed since it is also necessary to have it present.

All this mentioned study has been carried out by means of the method of bibliographical revision, which has consisted of the revision of scientific magazines, official webs and the utilization of the current jurisprudential resources necessary for the same one. Thus, it is possible to contrast all the information extracted and contrast it with various sources.

Before delving into the risks involved in the use of e-mail, it is first necessary to know what it is and how it works in order to have a better understanding of the problem. E-mail was born in 1971 by Ray Tomlinson as a basic project. Its initial goal was to form networks so that people could collaborate with each other. Tomlinson's program consisted of two parts: the SNDMSG (used to send messages) and READMAIL (performed the read function). Subsequently, further advances were made to implement the use of this tool, leading to what we know today as e-mail. Its importance is such that although it is an old messaging system, it is currently the most widespread. It was consolidated as a means of communication where a multitude of resources can be shared, even participating in the progress of scientific advances.

E-mail is mainly characterized by the e-mail address to be used by the user, as well as by its characteristic structure. To make use of this service an account is required, which is linked to the e-mail address and is therefore essential. This structure is divided into the recipient (to whom the message is addressed and there can be more than one), the sender (who sends the message), the subject (the title of the message) and the text of the message itself.

Even so, it is still possible to divide the mail message into two parts: the envelope which is controlled by transport agents and the actual content of the message (header and body). The function of the header is that of control, while the body contains the message to be sent, the information. At the beginning, the message text was sent in ASCII (American Standard Code for Information Interchange) format, which is composed of 7-bit characters, 96 letters in total. Later it was updated so that more characters could be sent, reaching the MIME (Multipurpose Internet Mail Extensions) standard format. Its great advantage is that it incorporated the concept of attachment since it did not belong to the mail itself.

Seen from this perspective of e-mail, its operation is not so simple since it is composed of many relevant concepts. In this process of sending and receiving messages, several fundamental elements are involved MUA (used as an interface between users and the protocol for reading or sending e-mail), MTA (has the function of receiving the message from an MUA or MTA and sending it to another MUA or an MDA depending on the situation), MDA (takes care of receiving the message sent by an MTA and stores it depending on its configuration), MAA (takes care of accessing the messages that are stored in the email) and MSA (receives the messages from an MUA and delivers it cooperating with the MTAs).

However, these concepts require the use of certain protocols for their correct operation. These protocols are the following: SMTP (Simple Mail Transfer Protocol), TCP (Transmission Control Protocol), IMAP (Internet Message Access Protocol) and POP (Post Office Protocol). Each one has a fundamental function, some are in charge of the sending functions and others of the reception of messages so that they arrive in the desired form to the corresponding servers. Even so, they also have their advantages and disadvantages to keep in mind.

On the other hand, this service is provided by e-mail providers, which are very diverse in their characteristics, given the need to cover the entire possible market. Thus, this service can be divided between personal mail (for a more informal function, among friends, family, etc.) and professional mail (of a formal nature, usually for use at work). These are used for different functions as each brings different features to the other. Some of the best known are Gmail, Outlook or Thunderbird among others.

Despite all the advantages offered by this service such as speed, low cost, access from anywhere or even a green aspect for the environment. However, there are also many drawbacks to its use. Some may be simple misinterpretations of the message received, but most involve infections in the device caused by malware, spam (all those messages that the user himself has not requested or simply does not want to have them in his inbox) or scam (use of deception and social engineering to obtain benefits, usually economic, from other users), which are used in a high percentage to commit certain computer crimes.

Within spam and scam there are other relevant subtypes. Hoax and Phishing. Hoaxes are also known as hoaxes and are quite common on the Internet. Phishing, on the other hand, is a type of computer fraud in which deception is used to obtain confidential information (bank account number, passwords, user name, etc.) from the victim. They are characterized by being chains of messages sent by means of e-mails. Thus, by knowing what they are and what their purpose is, we can find ways to prevent them, even in a specific way. Several tools will also be offered to combat these dangers in a generic way, among them the antispam filter and the use of an antivirus that must always be updated, in order to be able to prevent and solve them.

There is a drawback of equal or greater caliber than those mentioned above related to the lack of security problems they present, which jeopardize both the confidentiality and privacy of the user. This is because they do not provide end-to-end encryption to protect any message sent by this means. That is, during the process of sending the message, it can be intercepted by other people obtaining confidential information or even manipulating it. These actions cause many problems both to people in their daily lives and to the companies that use this service to carry out their actions.

This area of data protection and privacy of these users, in the EU legislation is included in the GDPR (General Data Protection Regulation). The GDPR has arisen from the need to unify all the rules and their methods of action, as well as the need to adapt to technological evolution. It has increased the protection of individuals' data, making it mandatory for companies to document all the data they obtain and its subsequent use. Some of these guarantees are: reduction of marketing and advertising or the right to be forgotten.

Spain’s legal system includes the LOPDGDD (Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales) to give more detail into what is included in the GDPR. Its objective is to protect the privacy, intimacy and integrity of individuals as well as the processes of transferring this personal data. And the Spanish Data Protection Agency is responsible for ensuring compliance with these laws in Spain. In addition, its scope of action extends to the entire Spanish territory and its headquarters are located in Madrid.

Faced with these security problems, this work provides solutions such as the use of a VPN (Virtual Private Network) that offer greater anonymity on the Internet and can even block advertising that appears on the Internet, thanks to the fact that it serves as an intermediary between the user and the Internet.

However, the most relevant aspect is the use of encryption systems to create an extra layer of security in such messages. Cryptography has been a widely used tool in our history, even the Spartans used Scythala to hide their messages from their enemies. Its evolution has never stopped until reaching to the present day and adapting to the technological level that exists nowadays.

The most commonly used cryptographic systems are the hash function (which generates digests of messages with letters and numbers), the symmetric system (which uses a private key) and the asymmetric system (which uses both a private and a public key). Therefore, there are several options, however, not everything is perfect and those systems also have certain drawbacks, so they are often used in junction to obtain the advantages of each other and thus improving its security, the so-called hybrid systems.

Currently, there is a tool which popularity has been increasing given its usefulness for the processing of legal and financial documents, the digital signature. The digital signature, which uses encryption systems attached to the message sent, guarantees the user a higher layer of security as it protects the authenticity and integrity of e-mail messages. It ensures that the message has not been tampered with by others during transport and verifies that the sender is who he or she claims to be. The main objective of the digital signature is to protect the user from being a victim of fraud or computer crime, among others. For this reason, it is considered an essential tool in many cases and is very useful for the processing of legal and financial documents.

Given the use of encryption systems that use digital signatures, this requires a public key that only belongs to the corresponding user. Thus, someone is required to verify that these public keys belong to the people they claim to be. To do this, there is a Certification Authority (CA) that is responsible for issuing, managing and revoking these certificates, which assures the receiver of the message that the key used is that of the authentic issuer and not that of another user who wants to impersonate him and commit some kind of crime.

Finally, it should be noted that this type of electronic certificates are also used in web pages as a way of authenticity concerning their users and their protection at the same time. The certificates usually issued by these CAs are SSL/TLS certificates, which allow the transport layer to use these certificates to make the Internet connection secure by encrypting the

information sent. These certificates are divided into three types (Domain validation, Organizer validation and Extended validation) depending on the level of authentication that the web certificate has, giving the user more or less security tools to use.

In reference to all that has been exposed and analyzed, several conclusions have been drawn, which are as follows: As it has been observed, the Internet has contributed to the evolution of computer technologies, having been such an important factor and also a parameter that will continue to grow constantly. The most relevant one is that e-mail is a necessary tool nowadays, due to the multiple advantages it brings us (faster, cheaper, more sustainable...).

However, we must take into account that there are also some disadvantages that we should never forget. It is due to the fact that there are people who want to benefit from these technologies and are looking for opportunities to do so. Thus, we can highlight the lack of security offered by the electronic creations, since it exposes the privacy of its users, something fundamental for any person. We must also take into account the spam and scam because they are disadvantages that can be very harmful both for our device and for the user himself. Therefore, it is necessary to equip ourselves with tools and techniques to be able to deal with these problems or at least prevent them, as is the case with digital signatures. Even so, these problems often arise due to the user's own ignorance of these dangers of what they are and how to oppose them. For that reason, it is necessary to promote this information to everybody so that we can reduce the computer crimes that happen nowadays.

RESUMEN

El propósito de este trabajo es dar a conocer más detalladamente lo que es el correo electrónico y su falta de seguridad, así como los riesgos que existen al hacer uso del mismo y dar unas soluciones a estas con el fin de evitarlas o erradicarlas.

De esta forma, en el presente documento se explicarán unos conceptos básicos referente a la estructura y al funcionamiento de dicha herramienta para tener ciertas nociones de esta. Se expondrán algunos de los clientes de correo electrónico que nos proporcionan este servicio así como sus principales características. Posteriormente se analizarán tanto las ventajas como las desventajas que existen al utilizar el correo electrónico. Este trabajo se centrará en los inconvenientes analizados dando a conocer cuales son y qué soluciones se pueden tomar para prevenirlas, así como quienes se encargan de combatir este tipo de delitos informáticos y sus regulaciones en el ordenamiento jurídico.

Así pues, se focalizará en los problemas de seguridad que presenta este servicio como es la privacidad o la autenticidad de los mensajes que son enviados. Para ello, se darán herramientas y recomendaciones para poder prevenirlos y se explicará una herramienta esencial hoy en día para solucionar este problema, que es la criptografía. También se explicará su uso en el propio funcionamiento del correo electrónico.

Una vez analizado todos estos puntos anteriores, se enfocará principalmente en la firma digital, dado su incremento de uso en los últimos años, y se informará de cómo funciona y la utilidad que tiene tanto a nivel personal como a nivel corporativo en la actualidad.

PALABRAS CLAVES

Correo electrónico, servicio, usuario, mensaje, seguridad, criptografía, firma.

ABSTRACT

The purpose of this work is to provide more detailed information about e-mail and its lack of security, as well as the risks that exist when using it and to provide solutions to these risks in order to avoid or eradicate them.

In this way, this document will explain some basic concepts referring to the structure and operation of this tool in order to have certain notions of it. Some of the e-mail clients that provide this service and their main characteristics will be presented. Subsequently, both the advantages and disadvantages of using e-mail will be analyzed. This work will focus on the

disadvantages analyzed, making known what they are and what solutions can be taken to prevent them, as well as who is in charge of combating this type of computer crimes and their regulations in the legal system.

Thus, the focus will be on the security problems that this service presents, such as privacy or the authenticity of the messages that are sent. To this end, tools and recommendations will be given to prevent them and an essential tool today to solve this problem will be explained, which is cryptography. Its use in the operation of e-mail will also be explained.

Once all these previous points have been analyzed, the main focus will be on the digital signature, given its increased use in recent years, and information will be given on how it works and how useful it is both at a personal and corporate level today.

KEYWORDS

E-mail, service, user, message, security, cryptography, signature.

1. INTRODUCCIÓN

Desde que apareció Internet, el mundo ha cambiado. Tal es el impacto que ha generado en nuestra sociedad, que este fenómeno ha pasado a ser algo cotidiano. Consiste en la conexión entre sí de varios ordenadores y otros dispositivos que se encuentran organizados en una misma red, que está formada por diferentes nodos que tienen como objetivo intercambiar información entre ellos. Gracias a este proceso, podemos acceder a los diferentes nodos desde un mismo nodo para hacer uso de sus recursos. Así pues, se considera a Internet una importante herramienta para obtener información y poder compartirla. Otra de las muchas utilidades que posee Internet es su sistema de comunicación tanto a nivel personal como mundial. Ha creado otra posibilidad de comunicarse con otras personas que están a kilómetros de distancia, cambiando así incluso nuestra forma de socializar. Por eso podemos considerarlo como uno de los mayores avances tecnológicos de la historia reciente.

El **correo electrónico** es un servicio que forma parte de las diferentes Tecnologías de Información y Comunicación (TIC) que han ido evolucionando constantemente. Y es que el correo electrónico forma parte de nuestras vidas, y más de lo que podamos imaginar. Por ejemplo, dicho servicio ha creado la necesidad de gestionar los mensajes que se reciben, responderlos… Incluso hoy en día las instituciones utilizan este medio de comunicación en sus operaciones y notificaciones diarias. El correo electrónico, o también conocido como *e-mail*, es uno de los pilares de este tipo de tecnologías, ya que cuenta con un gran número de usuarios que hacen uso de este servicio.

En 2021, son más de 4 mil millones de personas que utilizan este tipo de servicio. Y es que se prevé que en 2024 crezca aproximadamente 500 millones más. Aun así, no solo hay que tener en cuenta sus usuarios, sino también la frecuencia con la que se utiliza dicho servicio. Hoy en día es una herramienta fundamental para el uso diario, tanto de forma personal como laboral. Una prueba de ello es que en 2018 se enviaron y recibieron unos 280 mil millones de correos electrónicos cada día en todo el mundo.

A pesar de los beneficios que aporta al mundo, también posee ciertas problemáticas. En su mayoría son causadas por individuos que quieren aprovecharse de las diversas vulnerabilidades que contiene el correo electrónico. Algunos de ellos son el *spam*, la suplantación de identidad o la propagación de programas maliciosos, los cuales serán más detallados en el *apartado 2.3* de este trabajo. Sin embargo, uno de los más importantes es la falta de seguridad que ofrece este servicio del que muchas veces se sirven para realizar estas actividades. Estos problemas son más usuales de lo que podamos imaginar, uno de

sus mayores usos es para cometer delitos, y es que el delincuente que utiliza estos métodos puede acceder a nuestra información personal procedente de nuestro dispositivo e incluso utilizarlo para conseguir el dinero de nuestra cuenta bancaria entre otros. Una de las principales causas de estos hechos es su gran desconocimiento entre la población, por lo que, en su mayoría, no se sabe cómo combatirlos y sobre todo de cómo prevenirlos. Por ello, esto debería remediarse enseñando a todos cuáles son estos problemas y cómo hacerles frente.

A raíz de estos problemas han surgido varios mecanismos que actualmente sirven para frenar estos ataques. Estos serán expuestos durante el presente trabajo, sin embargo, hay que hacer alusión a uno de ellos, la **firma digital**. Gracias a esta herramienta se puede garantizar la integridad y la autenticidad de los usuarios para que no se vea afectada por otros usuarios no deseados que puedan acceder a ella durante el transporte del mensaje.

Por tanto, el objetivo de este trabajo es dar a conocer los entresijos de los correos electrónicos y exponer las diversas problemáticas que tienen al hacer uso de ellos. Así pues:

- Durante todo el trabajo se estudiará la seguridad y los problemas de criminalidad que están asociados al uso del correo electrónico.
- Se aportarán y analizarán herramientas y técnicas para mantener nuestro correo seguro ante estos problemas, ya que actualmente la delincuencia se ha ido incrementando a través de este medio.
- Se dará a conocer el correo electrónico con el fin de que los usuarios conozcan realmente como son y cómo funcionan y puedan hacer un buen uso de ello, puesto que forma parte del uso diario de muchas personas.
- Se profundizará en las ventajas e inconvenientes que nos aporta este tipo de servicio.
- Se identificarán varias amenazas que tiene el usuario de sufrir, así como métodos de prevención que el usuario puede usar y formas de combatirlas, como solución a estas. Tales métodos tienen la finalidad de proteger tanto sus datos como su privacidad para conseguir tener un correo seguro.
- Se hará alusión expresa a la firma digital, ya que es una herramienta que actualmente se está utilizando más y más como defensa de nuestro correo electrónico dada su gran utilidad, ayudar a garantizar tanto la autenticidad como la integridad de los mensajes que enviemos y suplir la falta de seguridad que posee el correo electrónico.

Para lograr estos objetivos expuestos, el método de revisión bibliográfica que se ha llevado a cabo ha consistido en la revisión de revistas científicas, webs oficiales y en los recursos jurisprudenciales actuales necesarios y útiles para ello. De esta forma se podrá extraer toda la información posible para este caso y contrastarla, con el fin de obtener las soluciones que nos plantea dicho trabajo.

2. CORREO ELECTRÓNICO

El correo electrónico surgió en 1971 de la mano de Ray Tomlinson, un ingeniero que trabajaba en la empresa BBN. La intención de Tomlinson fue crear un programa que permitiera entregar mensajes en otros ordenadores diferentes, ya que solo se podía realizar este proceso desde un mismo ordenador o una misma red en ese momento. El objetivo era formar redes de trabajo para que se pudiera colaborar entre varias personas. Sin embargo, estos mensajes eran pequeños. Por ejemplo, un programa que se solía utilizar era *Emisari*, donde se hace uso de una única red interna de comunicación.

Gracias a Tomlinson se produjo una evolución en este aspecto, permitiendo así enviar mensajes entre varios ordenadores empleando la red Arpanet[1]. Supuso un avance en el ámbito laboral, entre otros, porque ahora los grupos de trabajos que estaban separados geográficamente podían comunicarse entre ellos más fácilmente. Su programa está formado por dos partes: SNDMSG y READMAIL. La función de la primera parte era enviar los mensajes, mientras que la otra solo servía para su lectura. En su momento no existía la forma de gestionar el correo electrónico, por eso se debía combinar ambas partes. Aunque poco después se actualizó la parte READMAIL introduciendo así nuevos elementos para que dicha gestión se simplificará, como la creación de una lista que pudiera ordenar todos los mensajes por fecha y asunto. Marty Yonke, y posteriormente mejorado por John Vittal, creó BANANARD. Era una herramienta que permitía que se pudieran reenviar mensajes, agrupando así la recepción y la emisión de dichos mensajes. Así pues, el correo electrónico ha ido evolucionando constantemente hasta llegar a lo que conocemos actualmente.

En 1971 se envió el primer mensaje a través de Arpanet cuyo único fin era comprobar el funcionamiento del mismo. Un año más tarde se envió el primer mensaje público, dándose a conocer el propio sistema y su rendimiento. Posteriormente, se crea el '@' para que se pudiera diferenciar entre los destinatarios que habían y así enviar el mensaje a la persona correspondiente (Vela Delfa, Cristina, 2007).

[1] Red de ordenadores creada por el Departamento de Defensa de los EE.UU con el objetivo de reforzar las comunicaciones militares eliminando así la dependencia que había de un ordenador central.

Su éxito fue tal gracias a que este sistema ofrece una herramienta fácil de usar y a la vez rápida. Y sobre todo a su buen funcionamiento entre sus usuarios. Esto generó que, varios años después, la mayoría del tráfico que se propagaba por Arpanet perteneciera a los correos electrónicos.

A pesar de que el correo electrónico es un sistema de mensajería antiguo, es el más extendido en la actualidad. Se consolidó como un medio de comunicación dado su utilidad en las redes donde se comparten multitud de recursos, ayudando también a los avances científicos.

2.1. CARACTERÍSTICAS

El correo electrónico o email es una herramienta muy útil en Internet, un servicio de red que nos permite tanto enviar como recibir mensajes a cualquier persona del mundo, que sea usuario de este servicio. No solo permite la transferencia de mensajes de texto, sino también archivos como imágenes, sonido…

Hay muchas características a destacar de los correos electrónicos, sin embargo, las dos que más relevancia han tenido son su **rapidez** y que es la herramienta **más económica** para realizar dichas acciones. Su rapidez es debida a que el proceso es inmediato, el emisor envía el mensaje y el receptor lo recibe casi de forma instantánea. Además, si comparamos esta herramienta con otros que ofrecen servicios similares (correo postal, el teléfono…) encontramos que es el más económico entre estos. No hay que olvidar que este tipo de servicio está disponible los 365 días del año, salvo algún fallo que se produzca en la red. En referencia al aspecto ecológico, observamos que hay una ausencia de papel, por lo que este método contribuye a la sostenibilidad del medio ambiente.

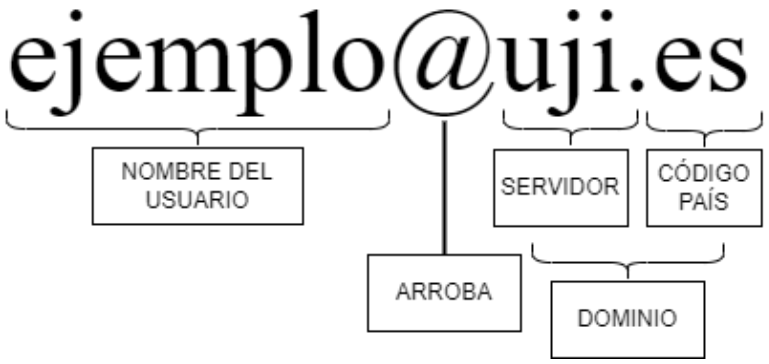


Figura 2.1: Ejemplo de una dirección de correo electrónico.

Para poder hacer uso de este tipo de herramienta de comunicación, es esencial tener una **cuenta** de este servicio de correo. Es como tener una dirección postal donde los demás usuarios envían y reciben mensajes. Así pues, esta dirección es única para cada usuario con la finalidad de poder identificarlo correctamente. Estas direcciones de correo electrónico destacan principalmente por el uso del carácter "@" (arroba) en ellos. Curiosamente, dependiendo del país este carácter se denominará de una manera diferente, por ejemplo en Italia es *chiocciola* (caracol) o en Alemania *klammeraffe* (pinza de mono). Como se observa en la figura 2.1, la dirección de correo electrónico se compone principalmente de dos elementos:

- ➔ El nombre del usuario titular. Se encuentra a la izquierda del símbolo "@". Este nombre podrá ser cualquiera que el usuario elija siempre y cuando ese nombre esté disponible, es decir, que otro usuario no lo haya elegido anteriormente en el servidor del correo electrónico utilizado. Esto se debe a que solo puede haber una dirección de correo por usuario porque si hubieran dos iguales los mensajes llegarán a los dos usuarios, entre otros problemas que surgirían.

- ➔ El nombre del dominio. Se encuentra a la derecha del símbolo "@". También es conocido como "*host*" y corresponde al servidor de correo donde se aloja. Dicho de otro modo es el sitio físico donde se colocarán los diversos mensajes que el usuario reciba.

Hay que destacar que estos servidores de correo se clasifican dependiendo de los dominios de nivel superior que asimismo conforman la dirección de correo electrónico. Algunos de los más conocidos son: *.com* (hace referencia a las entidades comerciales), *.org* (para organismos no gubernamentales), *.gov* (organismos gubernamentales), *.edu* (dirigidos a las instituciones educativas) o *.net* (exclusivos para servicios de Internet) entre muchos otros.

Finalmente, existe un elemento que sirve para asociar dicha dirección a un país. Son abreviaciones de dos letras, como por ejemplo *.es* para España o *.ar* para Argentina. En el caso de Estados Unidos, estos no utilizan este elemento porque ya se sobreentiende que esa dirección corresponde a ese país.

2.1.1. ESTRUCTURA Y FUNCIONES

La estructura que posee un mensaje es bastante simple, ya que contiene: el destinatario (a quién va dirigido el mensaje y puede haber más de uno), el remitente (quien envía dicho mensaje), el asunto (el título del mensaje) y el propio texto del mensaje. Profundizando en este aspecto, podemos dividir un mensaje de correo en dos partes: el **envoltorio**, que es

controlado por agentes de transporte; y del **contenido** del propio mensaje (cabecera y cuerpo). La **cabecera** tiene la función de controlar, por lo que cuenta con unos campos para ello. Algunos de ellos son:

- *To*: Sirve para indicar el destinatario del mensaje.
- *Cc*: Es una lista de direcciones de correo electrónico que recibirán el mensaje. Este campo está dedicado para los clientes de correo, por lo que pide al cliente que se añadan las direcciones a las que va el mensaje en el propio envoltorio, por lo que no se introducirán en la cabecera.
- *Subject*: También conocido como el asunto, que detalla el contenido de dicho mensaje.
- *Date*: En base al emisor, indica la fecha y la hora en que se envió el mensaje.
- *Reply To*: En este apartado se indica la dirección a la que el destinatario quiere que se le conteste.
- *Return path*: En caso de que el envío del mensaje fracase, este campo indica la dirección de retorno del propio mensaje.
- *From*: Indica la dirección del correo del remitente.

Recalcar que entre el campo To y Cc no hay prácticamente diferencia entre ellos y además, no es necesario que se rellenen estos porque el usuario receptor debe estar siempre especificado en el envoltorio. De esta forma, dicho mensaje llegaría al destinatario sin la necesidad de que se rellenen los campos expuestos.

En referencia al **cuerpo** del mensaje hablamos del contenido que posee. Tradicionalmente, el texto que se envía se encuentra en formato ASCII (*American Standard Code for Information Interchange*). Esta configuración se compone de caracteres de 7 bits, 96 letras en total. Esto supone que el mensaje debe ser escrito de forma bastante simple, ya que no puede contener tampoco caracteres con la letra ñ o que están acentuados. Posteriormente, se actualizó este formato, permitiendo la incorporación de caracteres de 8 bits, 256 caracteres posibles. Sin embargo, a pesar de este avance, Internet no aceptaba estos caracteres de 8 bits, sino los de 7 bits en formato ASCII. Esto hacía que el mensaje enviado con caracteres de 8 bits fuera alterado y el mensaje no llegaba como debería. Tras esta necesidad de poder enviar objetos con contenidos de información más pesados, como imágenes, se buscó otras opciones para que fuera posible convertir estos tipos de caracteres a texto. De esta forma surgieron los conversores de caracteres. Los más

conocidos fueron los métodos UUEncode, que convierte los caracteres de 8 bits a 7 bits, y UUDecode que hacia el proceso, al contrario, pasaba los caracteres de 7 bits a 8 bits. Y de esta forma se solucionaron los problemas que habían con los caracteres especiales al intercambio de archivos en formato binario (archivos de imágenes, vídeos…).

A pesar de ello, este procedimiento se requería realizar de forma manual en la generalidad de los casos, lo que suponía un problema para aquellos usuarios que no tenían mucho conocimiento sobre este tema. Finalmente, la solución que surgió fue el **estándar MIME** (*Multipurpose Internet Mail Extensions*). A parte, de que este método facilita la experiencia del usuario al realizar conversiones de forma automática, era compatible para todas las aplicaciones que hacían uso de Windows. MIME incorporó el concepto de **adjunto**, que no pertenece al propio correo. De esta modo el mensaje podía componerse no solo del texto, sino también de archivos como imágenes. Además, el receptor de dicho mensaje era informado de cómo poder acceder correctamente a ese archivo porque había que decodificarlo.

Para poder identificar los mensajes en formato MIME hay que observar la cabecera del propio mensaje (MIME-Version: 1.0). El cocreador de MIME, Nathaniel Borenstein, dijo que querían evolucionar en esta herramienta continuamente, pero esto se hizo prácticamente inviable, ya que el propio Internet no podría identificar versiones nuevas. Como solución a dicho problema, la versión 1.0 se mantuvo y se ha ido actualizando constantemente.

Si nos enfocamos más detalladamente en la estructura de la extensión MIME, se observa que es muy simple. Se divide en dos cadenas, un tipo y un subtipo, separadas de la siguiente manera: tipo/subtipo. El primero hace referencia a la categoría, que al mismo tiempo se divide en tipo discreto y en tipo multiparte. En cambio, la segunda cadena es distinta dependiendo del tipo. Resaltar que este método puede ser escrito tanto en mayúsculas como minúsculas (MDN contributors, 2020). Por un lado, los tipos discretos, como se ha comentado anteriormente, indican la categoría del propio documento. Algunos ejemplos son:

- *text*: aluden a todos los documentos que tengan texto. Como subtipos de este campo serían: *text/plain* que señala que el texto es común y no tiene formato, se utiliza para documentos de texto que no tienen especificado un subtipo. *text/html* refiere a los textos en formato HTML.

- *application*: simboliza a cualquier tipo de datos binarios. Como subtipo se encuentra: *application/pdf* se utiliza para archivos PDF, en este caso se utiliza application porque los PDF son propios de aplicaciones concretas. *application/octet-stream* es la

forma genérica para indicar un archivo binario desconocido, igual que sucede con *text/plain*, este tipo también se usa para documentos binarios que no tienen especificado el subtipo.

Por otro lado, los tipos multipartes, que también indican la categoría de un mensaje, pero en este caso se refiere a un documento que está roto en varias partes. Estas partes se componen de pequeños mensajes que tienen su cabecera y cuerpo en formato MIME. Curiosamente, estos pequeños mensajes pueden tratarse de otro tipo de multiparte, por lo que también estaría compuesto de otros pequeños mensajes. Y así se crearía una especie de árbol para un solo documento de este tipo.

El tipo de multiparte más común es el *multipart/mixed*, que representa varias partes que se encuentran aisladas entre sí. Su uso va dirigido a incorporar el concepto adjunto, ya que, por ejemplo, cuando se manda desde un correo electrónico un mensaje y al mismo tiempo adjuntamos una imagen, en este proceso se utiliza el multipart/mixed con estas dos partes (texto e imagen).

Otro subtipo también usado es el *multipart/alternative*. Se emplea en las situaciones donde un usuario crea un texto y utiliza otro formato característico de una página web, gracias al lenguaje HTML. En este caso se decide enviar este texto de forma HTML y así el receptor puede elegir el modo que quiera para poder descifrarlo. Además, todas las partes de este tipo, *multipart/alternative*, contienen la misma información.

Estos métodos son característicos de los correos electrónicos de texto sin formato. Es decir, no admite el texto en negrita, cursiva, fuentes con color o cualquier otro tipo de configuración del diseño del texto. Además, tampoco admite que dentro del mensaje se puedan visualizar imágenes. Aun así, poseen ventajas que otros tipos de correos electrónicos no tienen. Este formato puede funcionar con cualquier programa de correo electrónico. De todos modos, la forma con la que el usuario verá el mensaje depende del programa de correo electrónico que posea. Por ejemplo, si el usuario receptor tiene configurado su programa para transformar los mensajes que le lleguen, dicho mensaje que esté en formato HTML tiene la posibilidad de cambiar a un texto sin formato.

2.1.2. FUNCIONAMIENTO

Teniendo en cuenta la estructura de un mensaje de correo electrónico que se ha visto anteriormente, el proceso de envío parece que solo tarda unos segundos en ejecutarse. A pesar de ello, este proceso resulta tener cierta complejidad. Primeramente, se definirán una serie de conceptos básicos que se usarán posteriormente para la explicación de los

diferentes procesos de funcionamiento que tiene el correo electrónico (Solutions, S. A. L., 2009). Estos conceptos hacen referencia a los elementos que componen dicho funcionamiento, transmitir y administrar mensajes y son:

- MUA (*Mail User Agent*): programa que se utiliza como interfaz entre los usuarios y el protocolo de lectura o envío del correo electrónico. En caso de que se conecte a través del protocolo POP3 o IMAP, se usa para la recepción del mensaje; mientras que si se conecta a través del protocolo SMTP, se utiliza para el propio envío y en este caso debe conectarse a un MTA para que funcione. Además, proporciona la funcionalidad de leer y escribir mensajes a un usuario, personalizar los buzones del correo… Estos programas pueden tener interfaces de usuario gráficas, como en el caso del Mozilla Mail, o tener una interfaz de texto simple, como Mutt.

- MTA (*Mail Transfer Agent*): sistema que tiene la función de recibir el mensaje de un MUA o MTA y enviarlo a otro MUA o un MDA dependiendo de la situación. Su función sería como la furgoneta de Correos en la vida real. Este proceso es bastante complejo porque un mismo mensaje puede enviarse por varios MTA hasta llegar a su destino. A su vez, en este proceso, los mensajes deben ser recogidos por MTA concretas, las cuales se entregarán a la dirección indicada ya que esta elección dependerá de cómo estén configurados los MTA. Este sistema se utiliza junto al protocolo SMTP. *Postfix*, *exim* o *cyrus* son ejemplos de MTA.

- MDA (*Mail Delivery Agent*): sistema que se ocupa de la recepción del mensaje enviado por un MTA y lo guarda dependiendo de su configuración, en el disco, base de datos o incluso en programas especializados para este proceso. Aun así, los MDA no llevan los mensajes entre usuarios ni tampoco son una interfaz para el usuario final. También se utilizan para ordenar los mensajes que recibe el usuario. Su uso no es muy usual entre los usuarios, ya que realmente para enviar y recibir mensajes solo necesitas los MTA y MUA. *Procmail* o *Maildrop* son ejemplos de MDA.

- MAA (*Mail Access Agent*): programa que se ocupa del acceso a los mensajes que están almacenados en el correo electrónico, hacer que los buzones de los diferentes usuarios sean accesibles. El protocolo POP3 e IMAP son los que más utiliza este agente. *Dovecot* o *Qpopper* son ejemplos de MAA.

- MSA (*Mail Submission Agent*): programa que recibe los mensajes desde un MUA y lo entrega cooperando con los MTA. En muchas ocasiones las MTA actúan como MSA, sin la necesidad de hacer uso de estas.

Todo este proceso se visualiza con mayor facilidad en la figura 2.2 donde se ejemplifica el funcionamiento de un correo electrónico junto a las partes que lo conforman.

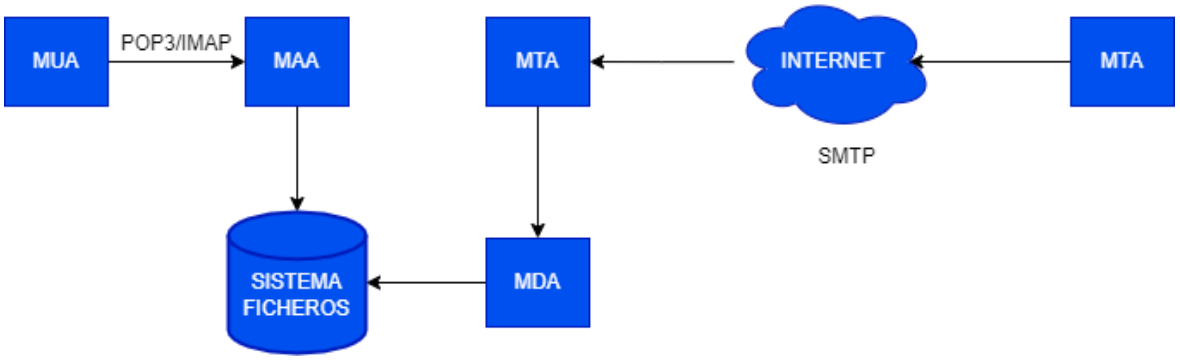


Figura 2.2: Ejemplo del funcionamiento del correo electrónico.

Cuando un usuario envía un correo haciendo uso del servicio SMTP, este se guarda en el servidor de la empresa que distribuye el correo y por medio de Internet se envía al servidor del distribuidor del destinatario. Después se utilizan los protocolos POP3 o IMAP para que este mensaje llegue al buzón del correo del receptor. Dicho de otro modo, el usuario mediante un MUA emplea a un MSA para que entregue el mensaje a un MTA. El agente MTA, como se ha comentado, puede realizar el proceso de transferencia utilizando solo un MTA o varios, por ello se usa el protocolo SMTP para coordinar este proceso. Llevado a cabo esto, el MTA requiere del DNS para averiguar la dirección y localizar a qué servidor hay que enviar dicho mensaje. Lo que realmente necesita el MTA es el registro MX, el nombre del anfitrión del dominio, que se lo facilitará el DNS. Localizado el servidor del destinatario, se le enviará el mensaje a un MDA el cual entregará dicho mensaje al correo electrónico del destinatario.

Un ejemplo de este proceso sería el siguiente:

1. El usuario Pepe quiere enviarle un mensaje a Marcos por correo electrónico. Hay que tener en cuenta que para que esto se realice ambos deben tener un correo electrónico y en este caso cada usuario tiene un correo electrónico perteneciente a servidores distintos.

2. Pepe escribe su mensaje en su correo y le da a enviar, y es cuando el propio cliente de correo que esté utilizando contacta con el servidor que esté haciendo uso Marcos para mandarle el mensaje y se lo envíe. Para ello, se utilizará el protocolo SMTP.

3. Este servidor observa que el dominio del destinatario es distinto al del remitente, pero no sabe a qué ordenador debe enviar el mensaje. Por eso, este contacta con

los servidores DNS (Sistema de Nombres de Dominio) para que le digan quien está asociado al correo con ese dominio. DNS le responderá con la información necesaria y se transferirá el mensaje, el cual se quedará guardado en dicho ordenador. Posteriormente, cuando Marcos entre en su correo electrónico, y al haber hecho uso de los protocolos POP3 o IMAP para guardar dicho correo, verá que tiene un mensaje de Pepe en su buzón.

Como se observa, durante el proceso de funcionamiento de un mensaje, no solo se requieren de los elementos detallados anteriormente. Estos elementos necesitan de unos protocolos para funcionar, por lo que son igual de importantes. Los más relevantes son los siguientes:

Protocolo SMTP

Para el funcionamiento del correo electrónico se utiliza el protocolo SMTP. El **SMTP** (*Simple Mail Transfer Protocol*) es un protocolo de red que permite intercambiar mensajes de correo de forma veraz y eficaz. Se encuentra definido en el estándar RFC[2] 5321 (Dr. John C. Klensin, 2008). Está enfocado a la conexión en base al texto, es decir, tanto el remitente como el receptor del mensaje se comunican mediante secuencias de comandos y parámetros, dando permisos y coordinando el tráfico de correos que se envían y reciben mediante el servidor SMTP. Con SMTP, el MUA debe conectarse a un MTA. Se encarga únicamente de obtener el correo electrónico que recibe mediante una conexión y enviarlo a otro sitio o entregárselo de forma local a un MDA. Durante este proceso se entregan los datos necesarios por medio de un canal de flujo de datos. Este proceso contiene transacciones SMTP que pueden ser cero o más, que al mismo tiempo, estas transacciones están formadas por tres cadenas de comando.

- MAIL: también se le conoce como *Return-Path* o remitente. Sirve para fijar la dirección de retorno.
- RCPT: sirve para establecer el destinatario del mensaje, el cual pueden ser varios, por lo que este comando se repetiría en base al número de destinatarios.
- DATA: tiene relación con el contenido del propio mensaje, ya que se encarga de enviarlo. Este comando está compuesto a su vez por varios comandos, por lo que el servidor debe responder dos veces. Una para el comando de datos (saber si se está preparado para recibir el mensaje) y otra para la secuencia final de dichos datos (aceptar o rechazar dicho mensaje).

[2] Documento numérico donde se describen los diferentes protocolos, conceptos, métodos y programas de Internet.

Protocolo TCP

El canal **TCP** (*Transmission Control Protocol*), consiste en un protocolo de red que posibilita que dos hosts se puedan conectar e intercambiar información, garantizando que los datos y paquetes lleguen al destinatario en el mismo orden en que el emisor los envió. Mejorando también estas comunicaciones con privacidad y autenticación. Además, en caso de que no llegara el mensaje al destino, se encarga de informar al emisor de dicho error. El SMTP utiliza este canal para transportar los datos por medio del puerto 25. Para garantizar la seguridad de este procedimiento, se hace servir de los **ACL** (*Access Control List*) para hacer una selección y denegar el paso de los mensajes que tengan un origen sospechoso. Así pues, este método es considerado el primer punto de control de seguridad de los diversos datos que se transportan por Internet.

No obstante, el protocolo SMTP tiene ciertas limitaciones relacionadas con la recepción de los mensajes en el servidor de destino. Como solución a este problema, se suele incorporar los protocolos POP3 o IMAP para que se encarguen de esta función, recibir los mensajes, y el protocolo SMTP se limite a las funciones de envío.

Protocolo IMAP

En referencia al protocolo **IMAP** (*Internet Message Access Protocol*), su función principal es autorizar el acceso a los mensajes que se encuentran almacenados en los servidores de Internet pudiendo acceder de forma remota. Además, permite acceder al correo electrónico para poder recuperar los mensajes del servidor a través de una conexión TCP/IP, poder leerlos y organizarlos (poner etiquetas al correo electrónico, marcar leído o no leído el mensaje, borrar mensajes...). Por ello está relacionado con el sistema MAA. La versión más actualizada de este protocolo es IMAP4ver1, que se encuentra definida en el RFC 3501 (Mark Crispin, 2003). El objetivo de su creación fue que el usuario pudiera tener una gestión completa de su buzón de correo mediante diferentes clientes de correo electrónico. El puerto que utiliza es el 143 dedicado a aplicaciones normales. El protocolo IMAP es perfecto para utilizar todos los correos electrónicos en un servidor si se va a emplear sistemas de *webmail* y más de un cliente de correo distinto. Asimismo, algunos servidores permiten que varios usuarios, empleando IMAP, puedan compartir el uso de carpetas. Gmail, Outlook o Yahoo son algunos servicios de correo que utilizan este protocolo.

Aparte de las ventajas que se han comentado, IMAP también nos ofrece otras como: avisa de que ha llegado un correo, ya que funciona en modo conexión permanente, el almacenamiento de los mensajes en modo local es opcional o que el mensaje se descarga solo cuando el usuario va a leerlo. Con todo esto, también tiene ciertas desventajas a tener

en cuenta: se necesita de conexión a Internet para ver el mensaje (a no ser que el usuario lo haya descargado previamente), se requiere de una transacción por cada mensaje que se vaya a leer, hay clientes de correo que no tienen la función de aviso de correos nuevos, ya que no son capaces de hacer uso de ella o que las carpetas, plantillas y borradores no podrán leerse mediante el protocolo POP. En la figura 2.3 se observa mejor estas características del Protocolo IMAP.

VENTAJAS	DESVENTAJAS
- Alertas de mensajes. - Conexión permanente. - Almacenamiento local - Descarga de mensajes cuando el usuario quiera.	- Requiere conexión a Internet. - Requiere transacción por cada mensaje. - Las carpetas, plantillas y borradores no se podrán leer con POP.

Figura 2.3: Algunas ventajas y desventajas del Protocolo IMAP.

Protocolo POP

En relación con el protocolo **POP** (*Post Office Protocol*), la última versión es 3 (POP3) es la más utilizada que actualmente se encuentra definido en el RFC 1939 (Myers, J., & Rose, M., 1996). Existe POP4, pero no ha tenido mucha repercusión. Se emplea en los clientes de correo locales con el fin de conseguir los mensajes que se encuentran en un servidor remoto. Está estructurado para recibir correos, pero no para que los envíe. POP3 permite la descarga y la eliminación de un buzón de correo remoto, "*maildrop*". Este proceso funciona del siguiente modo, al abrir el maildrop con POP3 los mensajes que se encuentran en el correo están fijos y son identificados mediante el número de mensaje local de dicha sesión. Destacar que este identificador es único de maildrop permitiendo que un mismo usuario pueda acceder a los mensajes en diferentes sesiones. Estos mensajes se marcan para que sean eliminados una vez se cierra la sesión. También está la opción de eliminarlos de forma remota.

Los servidores POP3 utilizan el puerto número 110 para las solicitudes de este servicio. También suelen usar el puerto 995, esto se debe a que tras iniciarse, la comunicación que está encriptada para este protocolo se solicita mediante el comando STLS que más adelante se conecta al servidor con ayuda de TLS (*Transport Layer Security*) o SSL (*Secure Sockets Layer*), que serán explicados más detalladamente en el apartado 3.2. Este proceso también es característico del protocolo IMAP, ya que también lo puede realizar. Este protocolo POP cuenta con dos extensiones a él. La primera es **STARTTLS**, la cual permite principalmente el uso de TLS y SSL. Estos dos protocolos usan funciones de encriptado con la intención de tener las comunicaciones seguras. La segunda es **SDPS**, este protocolo

otorga la posibilidad de tener múltiples cuentas por dominio. POP3 es utilizado cuando el usuario solo hace uso de un cliente correo electrónico en un mismo ordenador.

En este caso las ventajas que se encuentran son varias, como se observa en la figura 2.4, los mensajes solo se leen una vez y en caso de no tener, el propio sistema se desconecta hasta la siguiente comprobación. También potencia el uso del ancho de banda. Los mensajes se almacenan de forma local, por lo que están siempre a disposición del usuario; y al tener los mensajes descargados en nuestro ordenador, el espacio se limita por el disco de almacenamiento que se tenga y no por el propio servidor web. A pesar de ello, también posee ciertas desventajas a destacar. Al guardarse los mensajes de forma local, hace que este se pueda infectar con más facilidad. En relación, si tenemos algún fallo con el ordenador que hace que se elimine toda la información que contenga, también se perderán estos mensajes, a no ser que tengamos alguna copia de seguridad. Cuando el usuario se conecta, todos los correos nuevos que tenga se descargan sin tener en cuenta cuáles van a ser leídos y cuáles no.

VENTAJAS	DESVENTAJAS
- El sistema se desconecta hasta la próxima comprobación de mensajes. - Potencia el uso de ancho de banda. - Almacenamiento local. - El espacio se limita en base al disco duro y no al del servidor.	- Más probabilidad de que el dispositivo se infecte. - Un fallo en el dispositivo puede provocar la eliminación de todos los mensajes. - Todos los mensajes se descargan automáticamente al conectarse.

Figura 2.4: Algunas ventajas y desventajas del Protocolo POP.

2.2. CLIENTE CORREO ELECTRÓNICO

El cliente de correo electrónico, también conocido como MUA (*Mail User Agent*), comentado con anterioridad, son programas que se instalan en un dispositivo de forma local y permite que el usuario gestione su correo electrónico.

Actualmente, el uso del correo electrónico es esencial. De tal modo que le permite al usuario comunicarse con otros, registrarse en alguna página web o compartir información con los demás. Muchos son los usos a los que se le pueden dar al correo electrónico. Por ello es considerada una herramienta de trabajo fundamental para cualquier persona. Para realizar todas estas acciones comentadas es necesario que dicha persona tenga una cuenta de correo electrónico a su disposición. Estas cuentas de correo pueden ser de dos

formas, dependiendo del uso que el usuario vaya a darle le interesará más una que otra. Se distingue entre correo electrónico personal y correo electrónico corporativo o profesional.

- **Correo Electrónico Personal**: Se caracteriza por tener una función más informal. Este tipo de correo se suele utilizar para comunicarse con la familia o amigos, registrarse en páginas webs…
- **Correo Electrónico Corporativo o Profesional**: Se caracteriza por tener una función formal, ya que es comúnmente usado para el trabajo. Son las propias empresas las que proporcionan a sus trabajadores este servicio. De esta forma resulta más fácil gestionar la información.

Varias son las diferencias entre estos correos electrónicos. En referencia al acceso a este servicio, el tipo de correo electrónico personal se puede acceder desde cualquier sitio y desde cualquier dispositivo; mientras que en los correos electrónicos corporativos, normalmente solo se pueden acceder a ellos desde el trabajo, utilizando el dispositivo de la empresa. Por tanto, los de tipo personal tienen más libertad que los corporativos, ya no únicamente en su propio acceso sino también en su configuración. Los correos electrónicos corporativos, por ejemplo, el trabajador no puede cambiar ciertos elementos del propio servicio, para ello, deberá realizarlo un empleado superior de la empresa, porque sus acciones se suelen encontrar limitadas. Otro aspecto a destacar es su seguridad, la mayor diferencia es que en los correos corporativos es la propia empresa quien los suministra, por lo que todo lo que aparezca en estos correos será visto por la propia empresa. En cambio, en el tipo personal esto no sucede. Otra particularidad sería que los corporativos suelen tener contraseñas más complejas por el hecho de que la información que se maneje sea sustraída por otros. Y por último, no hay que olvidarse del precio de estos servicios. Esto dependerá del proveedor que elija el usuario o la empresa, ya que ambos tipos pueden ser de forma gratuita o de pago. Sin embargo, las empresas para la elección de sus correos electrónicos corporativos se decantarán más por los de pago que les ofrecen unas características que pueden aprovechar para tener una visión más profesional.

Por tanto, estos proveedores de correo electrónico, **ESP** (*Email Service Provider*), son las empresas que se dedican a ofrecer sus servicios tanto de envío como recepción de emails de forma automática. Son muchos los proveedores que existen para poder llegar a todos los tipos de clientes, ofreciéndoles características distintas para satisfacer sus necesidades. Las ventajas que se encuentran en la utilización de este servicio serían un aumento de la productividad, ya que los procesos se encuentran automatizados; una mayor seguridad, siguiendo los protocolos correspondientes y la legislación vigente; y un mejor análisis de los datos.

2.2.1. SERVICIOS GRATUITOS Y PREMIUM

Vistos los conceptos de cliente de correo electrónico (el software que permite gestionar los emails) y proveedor de correo electrónico (la empresa que facilita el medio para tener una cuenta de correo), destacar que ambos pueden coincidir a la hora de que el usuario haya elegido un servicio específico. Y es que estas prestaciones se pueden encontrar de manera gratuita, con la opción de conseguir ciertos privilegios añadidos si se opta por la opción de pago que ofrece este servicio. Todas estas características, tanto del Gmail, Outlook como del Thunderbird, se encuentran recogidas en la figura 2.5 para una mejor visualización.

	GMAIL	OUTLOOK	THUNDERBIRD
Creador	Google	Microsoft	Mozilla
Fecha de Lanzamiento	2004	1996	2003
Sede	Estados Unidos	Estados Unidos	Estados Unidos
Plataformas	IOS, Android y Navegador Web	IOS, Android, Windows, Navegador Web	Windows, Mac OS, Linux
Versión Gratuíta	Sí	Sí	Sí
Servicios Premium	Sí	Sí	No
Código Abierto	No	No	Sí
Almacenamiento	15Gb	15GB	Depende de la capacidad del disco del dispositivo
IMAP, SMTP y/o POP	Sí	Sí	Sí
Extras	Etiquetas, calendario, bloquear usuarios, filtros, listas de tareas	Calendario, lista de tareas, libreta de direcciones	Gran variedad de complementos, extensiones, temas

Figura 2.5: Características de: Gmail, Outlook y Thunderbird.

Gmail

Gmail es uno de los mayores servicios de correo electrónico gratuito del mundo que existen. Creado por la empresa Google y desarrollado por Paul Buchheit, fue lanzado el 1 de abril de 2004. Su característica más famosa fue la integración de un motor de búsqueda en el propio correo electrónico. Su almacenamiento fue creciendo hasta que se detuvo en los 15 GB, relacionados con el servicio de Google Drive. Ofrece este espacio

de almacenamiento de forma gratuita, pero también ofrece un aumento con la opción de pago. Una de sus principales ventajas es que permite conectarse con otros servicios de Google, así como vincularse a otras cuentas desde cualquier dispositivo, incluso permite su uso sin tener conexión a la red. Posee buenos recursos en relación con la organización del propio correo y destaca fundamentalmente por su buen filtro de spam, eliminando así los correos no deseados. Y permite enviar archivos adjuntos de hasta 25 MB. Además, Gmail es una aplicación que ya viene preinstalada en los teléfonos con Android. El principal inconveniente es su seguridad de datos, donde se observa que la privacidad de sus usuarios se encuentra desprotegida. Los términos y condiciones que posee ya permiten que se cree una divulgación de los diferentes datos de los usuarios.

Outlook

Outlook también es considerado uno de los más populares clientes de correo electrónico gratuitos del mundo. Fue creado por Microsoft y lanzado el 4 de julio de 1996. Anteriormente, era conocido como Hotmail. Igual que sucede con el servicio de Gmail, este ofrece al usuario un espacio de almacenamiento de 15 GB además de otros 5 GB más para utilizar en OneDrive. Permite enviar archivos adjuntos de hasta 20 MB. Su ventaja principal es que se sincroniza fácilmente con las diferentes aplicaciones de Microsoft y se puede utilizar desde cualquier dispositivo. Sin embargo, este servicio también tiene ciertos problemas en relación con la protección de datos, y aun así, las funciones que tiene de cifrado solo se pueden obtener si el usuario opta por la opción de pago de este servicio.

Thunderbird

Thunderbird es una de las opciones más conocidas como alternativa a las mencionadas anteriormente, tanto para uso personal como profesional. Fue creado y desarrollado por la Fundación Mozilla y lanzado en 2003. En este caso, Thunderbird es un correo electrónico multiplataforma gratuito, pudiendo así gestionar al mismo tiempo varias cuentas de correo. Se caracteriza por guardar toda la información en carpetas (perfiles) que tienen una capacidad máxima de 4 GB. Aun así, esta capacidad se puede aumentar dependiendo del espacio libre que se tenga en el disco del dispositivo que se esté utilizando. Thunderbird está formado por un proceso de código abierto, permitiendo así que se pueda proteger de mejor forma el correo. Esto sucede porque al abrir su código, muchos profesionales de la seguridad de todo el mundo se implican en buscar los fallos que pueda tener este servicio y encontrar así soluciones más rápidamente a ellos, para posteriormente actualizar este sistema. Una de sus ventajas está relacionada con la gran

capacidad de personalización, desde diversos complementos, temas o incluso extensiones. En relación con la seguridad que ofrece al usuario, se distingue por su buena privacidad, añadiendo una protección contra el rastreo de otros.

2.3. VENTAJAS E INCONVENIENTES

Considerando todos los datos que se han analizado durante el desarrollo del trabajo, se puede decir que los correos electrónicos aportan muchísimo a la vida de las personas, forman parte de ellas. Sin embargo, también existe un gran desconocimiento por parte de la población hacia ellos. Aun así, hacen la vida más fácil, ya que, en este método de comunicación, no se necesita que el emisor y el receptor estén al mismo tiempo realizando esta acción para que se puedan comunicar; se envía el mensaje y el receptor, cuando esté disponible, entrará en su correo y verá dicho mensaje. Además, todo lo que se envía por correo electrónico se almacena, por lo que se puede consultar cuando el usuario desee.

Del mismo modo, las principales ventajas que presenta este servicio es su coste, su proceso, que es prácticamente inmediato, se puede enviar cualquier tipo de información y se puede acceder a él desde cualquier lugar. Al tener un coste bastante bajo es una opción muy atractiva para el consumidor. Igualmente, al tratarse de un funcionamiento que es prácticamente instantáneo, facilita mucho la comunicación y puedes acceder a él desde cualquier lugar, ya que solo se necesita de un dispositivo para ello. La información que envía el usuario puede llegar a cualquier parte del mundo y esta, puede ser de cualquier tipo, tanto textos, imágenes o videos, entre otros.

A pesar de todas estas ventajas que ofrece, también hay que tener en cuenta sus posibles inconvenientes. Estos pueden ir desde una simple mala interpretación del correo, provocando así malentendidos entre el emisor y el receptor, hasta la posibilidad de que el equipo que se esté utilizando se infecte de algún tipo de malware, haciendo que peligre la integridad del mismo. Otro problema que está unido a este servicio es su sobrecarga de información, se debe de tener una vigilancia constante del correo, ya que en ocasiones llegan bastantes mensajes a la bandeja de entrada del correo electrónico y el usuario no es capaz de manejar tantos datos a la vez. Sin embargo, hay que hacer especial mención a los problemas más relevantes relacionados con los riesgos de seguridad que tienen los correos electrónicos. Y es que destacan por una falta de seguridad en ellos. Uno de ellos es la inundación, consiste en denegar el servicio mediante un ataque masivo de mensajes de correo electrónico. Este ataque provoca que el servidor colapse y se quede inoperativo hasta que solucionen el problema. Aun así, el riesgo más importante que debe tener en

cuenta el usuario al hacer uso de este servicio es la poca confidencialidad que nos ofrece. Se debe a que no proporcionan un cifrado de extremo a extremo para proteger cualquier mensaje que se envíe por este medio. Es decir, el mensaje que se envía, antes de llegar a su destinatario, viaja por muchos sistemas, y cada uno de estos puede ser vulnerable individualmente, y si el mensaje no está bien protegido, puede ser interceptado por otros usuarios. De esta forma, estos últimos pueden modificar o sustituir estos mensajes, perdiendo tanto la autenticidad del propio mensaje como su integridad. Una solución a dicho problema sería la encriptación de estos mensajes para que no puedan ser interceptados, sin embargo, los correos electrónicos no realizan esta función por defecto. Este problema puede no ocasionar muchos inconvenientes dependiendo de la información que se envíe, pero es algo que todos los usuarios deberían tener derecho, ya que se están exponiendo. Sin embargo, esta información puede ser fundamental, porque puede pertenecer a la confidencialidad del usuario (datos de las tarjetas de crédito, datos de alto secreto de empresas…). Como opción a los correos estándar vistos anteriormente, se encuentra el proveedor Tutanota, que proporciona una mayor seguridad al usuario. Fue lanzado en Alemania en 2011 que se caracteriza fundamentalmente por su privacidad porque, por ejemplo, envía mensajes cifrados incluso a usuarios que no pertenecen a este proveedor. Además, se encuentra respaldado por el Reglamento General de Protección de Datos de la Unión Europea. En la figura 2.6 se observan todas estas características pertenecientes al correo electrónico.

VENTAJAS	INCONVENIENTES
- No requiere que la acción sea al mismo tiempo. - Bajo coste. - Proceso inmediato. - Envío de cualquier información. - Acceso desde cualquier dispositivo.	- Interpretaciones erróneas de los mensajes. - Infección del dispositivo. - Sobrecarga de información. - Spam. - Scam. - Inundación. - Confidencialidad.

Figura 2.6: Ventajas e inconvenientes de la utilización del correo electrónico.

2.3.1. SPAM

Teniendo en cuenta todos estos inconvenientes, cabe destacar uno en particular, el cual es de los más comunes. Se trata del **spam**. Se considera spam a todos aquellos mensajes que el propio usuario no ha solicitado o que simplemente no quiere tenerlos en su bandeja de entrada, también son conocidos como correo basura. Suelen ser correos electrónicos

comerciales que en ocasiones son engañosos. A la persona que se dedica a envíar estos tipos de mensajes se le conoce como spammer, que acostumbra a conseguir estas direcciones de correo por medio de páginas webs, chats o incluso haciendo uso de determinado malware. Más allá de la incomodidad que le produce al usuario la receptación de tantos correos no deseados, también ocasionan otros a tomar en consideración. El desperdicio de recursos de red y su respectivo almacenamiento, al enviar tantos correos de este tipo las redes informáticas se colapsan, afectando así al ancho de banda, provocando daños en nuestros dispositivos e incluso se puede sopesar la pérdida de tiempo que el usuario utiliza para revisarlos o para eliminarlos de su bandeja de entrada. Este problema va aumentando año a año hasta tal punto que constituye alrededor de más del 70% del tráfico mundial que pertenece al correo electrónico. En España quien se dedica a combatir el spam es la **Agencia Española de Protección de Datos**.

Se pueden encontrar otros tipos de Spam dependiendo del medio en que se realicen estas acciones. Algunos de ellos son:

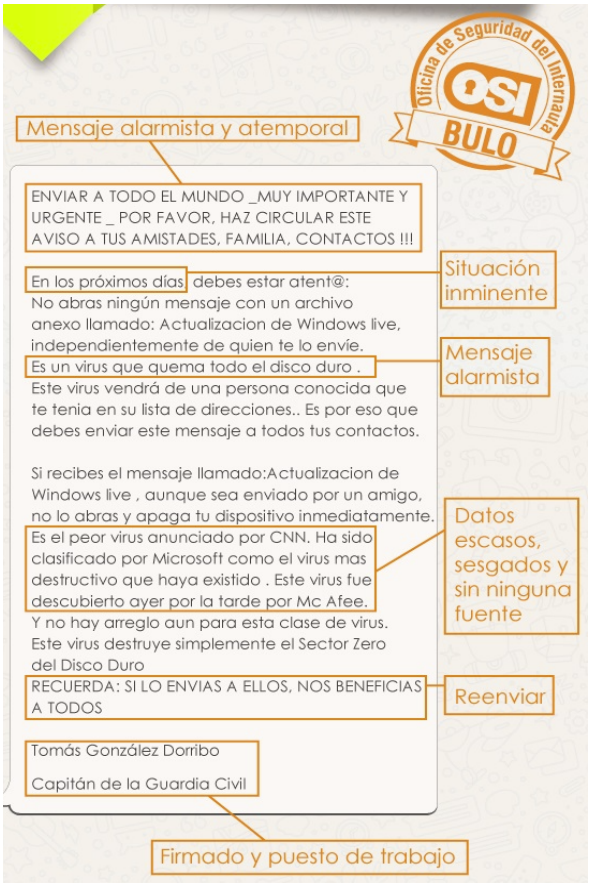
- Pop-Ups: Son ventanas emergentes que aparecen cuando se está navegando por la red. Estas aparecen encima de lo que el usuario está viendo, por lo que dificulta la visibilidad del contenido que intenta ver. Normalmente, se trata de publicidad o contenido extra de la propia página web que se visita, sin embargo, es un contenido que el usuario no ha solicitado y el cual suele resultar molesto. Su objetivo principal es captar la atención de los usuarios durante un breve periodo de tiempo y conseguir que el usuario tenga interés por el contenido de ese Pop- up.

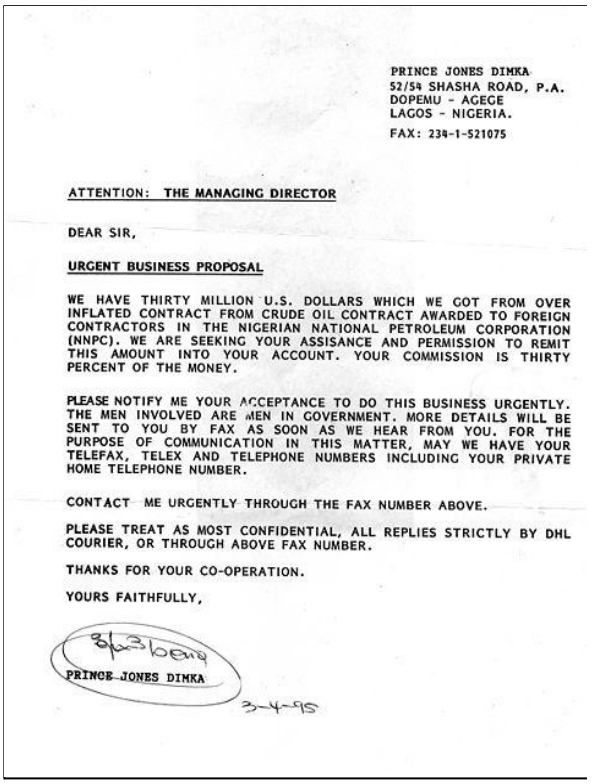
- Spam en el teléfono: en este caso se refiere a las llamadas comerciales. Estos casos son muy numerosos porque muchas compañías intentan contactar con posibles nuevos clientes. De igual forma, estas llamadas se realizan sin el consentimiento del propietario del teléfono. Se caracterizan por su malestar hacia el receptor, ya que este pierde su tiempo e incluso, en ocasiones, su dinero.

No obstante, en este trabajo, también se hará mención a las formas de spam en relación con el Hoax y al correo electrónico.

Los **Hoax**, también conocidos como bulos, son bastante frecuentes en Internet y se caracterizan por ser cadenas de mensajes que se envían por medio de correos electrónicos. Un ejemplo de este tipo de bulos se muestra en la figura 2.7. Su objetivo es generar alarma, desinformar y engañar a los usuarios que reciben estos tipos de mensajes, puesto que, conjuntamente con el contenido de estos, indican que deben de reenviarlo a todas las personas que conozcan. Y así es como intentan llegar al mayor número de personas

posibles. Se alimentan sobre todo de la ignorancia de las personas acerca de determinados temas. Tienen como costumbre hacer uso de noticias falsas sobre temas de interés social que aparentan ser reales (bulos sobre empresas relativamente conocidas, regalos gratis como cupones o si no lo reenvías puedes tener años de mala suerte).




PRINCE JONES DIMKA
52/54 SHASHA ROAD, P.A.
DOPEMU - AGEGE
LAGOS - NIGERIA.
FAX: 234-1-521075

ATTENTION: THE MANAGING DIRECTOR

DEAR SIR,

URGENT BUSINESS PROPOSAL

WE HAVE THIRTY MILLION U.S. DOLLARS WHICH WE GOT FROM OVER INFLATED CONTRACT FROM CRUDE OIL CONTRACT AWARDED TO FOREIGN CONTRACTORS IN THE NIGERIAN NATIONAL PETROLEUM CORPORATION (NNPC). WE ARE SEEKING YOUR ASSISANCE AND PERMISSION TO REMIT THIS AMOUNT INTO YOUR ACCOUNT. YOUR COMMISSION IS THIRTY PERCENT OF THE MONEY.

PLEASE NOTIFY ME YOUR ACCEPTANCE TO DO THIS BUSINESS URGENTLY. THE MEN INVOLVED ARE MEN IN GOVERNMENT. MORE DETAILS WILL BE SENT TO YOU BY FAX AS SOON AS WE HEAR FROM YOU. FOR THE PURPOSE OF COMMUNICATION IN THIS MATTER, MAY WE HAVE YOUR TELEFAX, TELEX AND TELEPHONE NUMBERS INCLUDING YOUR PRIVATE HOME TELEPHONE NUMBER.

CONTACT ME URGENTLY THROUGH THE FAX NUMBER ABOVE.

PLEASE TREAT AS MOST CONFIDENTIAL, ALL REPLIES STRICTLY BY DHL COURIER, OR THROUGH ABOVE FAX NUMBER.

THANKS FOR YOUR CO-OPERATION.

YOURS FAITHFULLY,

PRINCE JONES DIMKA

3-4-95

Figura 2.7: (a) Izquierda: Ejemplo de Hoax (INCIBE, 2017). (b) Derecha: Ejemplo de Estafa Nigeriana. (Morburre, 2010).

Para su identificación hay que tener en cuenta su objetivo, generar alarma. Por lo cual lo que indica el contenido del mensaje suele ser irreal o con pocas posibilidades de que ocurra e incitan a que la persona debe de hacer algo de forma inmediata por temor a que pueda ocurrir lo que le están diciendo. Por ello, hay que buscar la fuente del mensaje y contrastar con otras informaciones que se encuentren en Internet, en páginas de confianza. Otra opción es examinar la URL (en caso de que haya una compartida en el mensaje) y revisar que dicha página tiene un certificado digital y que empieza por “https”. Suelen contener faltas de ortografía o datos muy escasos en sus mensajes. El usuario también puede optar por contrastar este tipo de información en páginas que se dedican a desmentir estas noticias falsas, como son: Snopes, Maldito Bulo o Newtral (INCIBE, 2020).

En general son prácticamente inofensivos, ya que únicamente causan una pérdida de tiempo al usuario que es quien ve dicho mensaje o lo reenvía. Sin embargo, para aquellos que se creen estos bulos, las consecuencias pueden ser más graves. En ocasiones el mensaje puede decir que un archivo en concreto del dispositivo les está causando graves daños a este, por lo que deben eliminarlo inmediatamente, provocando que dicho dispositivo sufra algún tipo de fallo. O incluso ir más allá, hacer creer al usuario que se va a realizar un atentado cerca de donde viven, provocando que los servicios de telefónica se colapsen al recibir excesivas llamadas. En caso de recibir e identificar un hoax en el correo electrónico, lo que hay que hacer es eliminarlo y ante todo, no compartirlo con nadie para que no se propague.

El correo electrónico es una de las formas de transmisión de spam más utilizadas por los spammers. Esto se debe a que es un método rápido y fácil de usar, por lo que contribuye a que se expanda de forma más sencilla. De tal manera que los proveedores de los correos electrónicos han configurado unos **filtros antispam** para contrarrestarlos. Este método se basa en técnicas de aprendizaje automático (*Machine Learning, ML*), las cuales se dedican a aprender e identificar los correos spam que llegan a nuestro dispositivo. Esto es posible, ya que hacen uso de una amplia gama de estos mensajes para analizarlos y así poder detectarlos. En el caso de Gmail, utilizan este método, pero empleando reglas preexistentes y van actualizándose según los casos que aparecen. El modelo que emplea Google tiene una precisión del 99,9% de efectividad (Dada, E. G., Bassi, J. S., Chiroma, H., Abdulhamid, S. M., Adetunmbi, A. O., & Ajibuwa, O. E., 2019) .

El Machine Learning es una sub rama científica de la inteligencia artificial. Esta materia hace posible que tanto las computadoras como los diferentes sistemas informáticos aprendan tareas y vayan mejorando de forma progresiva. La intención es que estas máquinas desarrollen la capacidad de analizar los datos de la misma manera que lo hace el ser humano. Así pues, si estas máquinas tienen esta autonomía, pueden por ejemplo tomar decisiones bastante eficaces para sus funciones. Existen varios tipos de ML según su proceso, en el caso de los filtros de spam que utilizan los correos electrónicos, se emplea el aprendizaje supervisado. Se distingue por el proceso por el cual la máquina adquiere el conocimiento, accediendo a un grupo de datos ya existentes de los cuales aprende y se adapta a sus actualizaciones posteriores. Su objetivo es encontrar patrones del spam para así diferenciarlos y clasificarlos. De este modo, incluso es capaz de hacer predicciones en relación con los datos que aún no han sido procesados. Dentro de esta clasificación se encuentra el algoritmo **SVM** (*Support Vector Machines*) el cual es considerado una de las mejores técnicas contra el spam. Es uno de los algoritmos más potentes actualmente con una alta precisión en sus clasificaciones.

Como se ha comentado, el spam es correo no deseado por el usuario y estos pueden ser correos comerciales o bulos. Sin embargo, hay que tener en cuenta que estos correos spam también pueden ser más dañinos para nuestro dispositivo, ya que de la misma manera que contienen anuncios o bulos pueden contener algún tipo de malware en ellos. Este software malicioso puede estar en forma de archivo o directamente en un enlace que hace que el usuario al acceder a él y se descargue el malware sin darse cuenta en muchas ocasiones. Algunos tipos de malware son los troyanos, spyware o gusano, entre otros. Estos afectan el dispositivo de forma dañina, donde además, pueden combinarse para aumentar dicho mal.

2.3.2. SCAM

Por otra parte, el spam puede ser utilizado como medio para obtener beneficios, más allá de estropear nuestros equipos. En este punto se encuentra el **Scam**. Es una de las tácticas más utilizadas por los spammer donde utilizan el engaño y la ingeniería social para obtener beneficios, generalmente económicos, de otros usuarios. Se basan en la necesidad de las personas, codicia o pura ingenuidad. Este tipo de estafa se caracteriza por el cebo que les lanzan a sus destinatarios, pidiendo cierto dinero por adelantado para posteriormente la víctima obtenga un beneficio mayor, lo cual es falso. Un ejemplo muy conocido, que podemos observar en la figura 2.7, es la denominada estafa nigeriana. Los estafadores envían cientos de correos electrónicos a diversos destinatarios alegando que hay una cantidad enorme de dinero bloqueado en Nigeria y no se puede sacar si no es con una transferencia a una cuenta extranjera. De esta forma el estafador le dice que le hará la transferencia a la víctima y obtendrá un porcentaje de este a cambio de darle una cierta cantidad de dinero por adelantado. El estafado accede y envía este dinero y después ya no recibe ninguna transferencia con la supuesta cantidad de dinero ofrecida. A diferencia de este ejemplo, también existen otras formas de proceder, como cuando estos estafadores buscan muleros para blanquear dinero, lo cual es mucho más peligroso. Además, con frecuencia estas personas no saben que están siendo utilizadas.

Dentro de lo que es el scam hay varias formas más específicas de actuación, como es el caso del **phishing**. Consiste en un tipo de fraude informático en el se emplea el engaño con el fin de obtener información confidencial (número de cuenta bancaria, contraseñas, usuario…) de la víctima. Su objetivo es obtener beneficios de esta información personal adquirida. A quienes realizan estas actividades se les conoce como *phisher*. Su aparición se produjo en 1995 junto con America Online (AOL)[3]. En ese tiempo, ya existían programas que conseguían la información personal de las tarjetas de crédito de otras personas de

[3] Empresa de servicios relacionados con Internet y medios que fue absorbida por la empresa Verizon, llegando así a su desaparición.

forma automática. Posteriormente, se produjo un aumento de esta actividad sobre todo en las entidades financieras basándose en la confianza del cliente ya que los métodos de seguridad que había entonces no eran capaces de detener el phishing. Los expertos no se sorprendieron a tal impacto porque ya anunciaban que el propio correo SMTP resultaba inseguro en Windows. Además, en este incremento también contribuyó la aparición de herramientas que lo facilitaban en las que haciendo un clic podías inutilizar un correo electrónico, llegando a producirse ataques de denegación de servicio (DoS) contra las propias cuentas de correos y sus proveedores.

El phishing se puede clasificar en varios grupos, actualmente 48 grupos, dependiendo de su forma de atacar, su objetivo… Sin embargo, este fraude va evolucionando, por lo que pueden ir apareciendo más grupos añadiendo más elementos que los hagan más efectivos. La metodología que más utiliza, actualmente, es mediante el envío de correos masivos por medio del correo electrónico, para que llegue a una cantidad más grande de personas, los cuales aparentan proceder de entidades de confianza, por ejemplo un banco. En estos mensajes se le dice a la víctima que ha habido un fallo de seguridad o que se requiere que se confirmen ciertos datos de la entidad suplantada. Normalmente, estos correos llevan en sí un enlace falso donde les lleva a dicha entidad para que realicen la acción pertinente. Para que el engaño sea más creíble, los phisher utilizan URLs muy similares a las que utiliza la entidad legítima, por lo que se podría considerar un ataque contra el ojo humano (James, L., & Jevans, D., 2005).

En muchas ocasiones el usuario no se da cuenta de este error, ya que suele ser mínimo, por ejemplo: www.santtander.es. De tal forma que los estafadores imitan falsamente estas entidades también gráficamente en dicha web falsa para aparentar ser lo más veraces posibles para así ganarse la confianza de la víctima. Y así es como los usuarios pican en el anzuelo y se convierten en víctimas de estos estafadores.

Para poder identificar estos correos de phishing, lo primero que hay que ver es la URL del enlace que se encuentra en el mensaje. En muchas ocasiones, el estafador utiliza URL que no le pertenecen o la crean falseando los datos para que le sea más difícil identificarlo, ya que no dejarán rastro. También hay que examinar la dirección del remitente para comprobar si es sospechosa. Otra característica es que al ser un correo masivo no están personalizados, por lo que se puede recibir un correo de Bankia pidiendo que se cambie la contraseña y realmente este usuario no tendría ninguna cuenta en esta entidad. Por tanto, suelen ser mensajes generalizados. Para prevenir estas acciones hay que considerar varias recomendaciones: en caso de recibir dichos mensajes, primero sospechar de ellos porque no suelen ser frecuentes por parte de la entidad y acceder siempre desde el navegador web

a la página de esta identidad, nunca desde el enlace que se facilita en el correo; para saber si dicha página es segura deberá tener un certificado digital y que su URL empiece por “https://” y/o tener a nuestra disposición un antivirus actualizado como medio de protección.

Además, en 2020, el Centro de Quejas de Delitos en Internet (IC3) de Estados Unidos, recibió 241.342 quejas que supusieron unos 54 millones de dólares. En base a las estadísticas de 2020 del FBI en Estados Unidos, el phishing es uno de los 5 delitos informáticos más utilizados para cometer fraudes.

2.4. PROTECCIÓN DE DATOS Y PRIVACIDAD

Dentro de estos inconvenientes vistos se encuentra el más preocupante porque afecta a muchísimos usuarios del correo electrónico. Son los ataques a la privacidad. Hoy en día la información que se envía por correo electrónico es inmensa, tanto en el ámbito personal como profesional, donde en muchas ocasiones dicha información es privada. Entonces, ¿qué pasaría si un usuario no deseado intercepta un mensaje privado que contiene los datos bancarios de una persona o incluso imágenes personales?. Por ello, este aspecto es fundamental y hay que protegerlo para que el usuario pueda disfrutar de un correo seguro. De esta forma se da origen a leyes que sancionen estas conductas que violan la privacidad de este tipo de comunicaciones. Sin embargo, aún no se resuelve dicho problema. Hay que dotar de instrumentos científicos que hagan que se elimine la posibilidad de que suceda, o al menos, de prevenirlo, que alerte de que dicha violación de privacidad se está produciendo. Con frecuencia, los usuarios no son conscientes de que se han realizado estas acciones contra ellos o en las ocasiones donde se han dado cuenta, no disponen de las pruebas oportunas para constituirse como pruebas constituidas ante un juicio, ya que a veces es difícil de demostrar. Por ello, hay que instrumentar a los usuarios de este tipo de herramientas que les aporte la seguridad que necesitan.

Como respuesta a este problema, surgió la alternativa de utilizar **sistemas de cifrado** y descifrado para poder hacer más seguro el correo electrónico de otros. Como curiosidad, en el 2005 una sentencia de la corte de apelaciones de Minnesota determinó que el disponer de un sistema de cifrado o descifrado en un dispositivo ya se puede considerar como una evidencia de un intento de delito (McCullagh, D., 2005).

Actualmente, existen otros métodos para mantener la privacidad a salvo. Una de ellas es la **VPN** (*Virtual Private Network*). Las VPN ofrecen un mayor anonimato en Internet e incluso pueden bloquear la publicidad que surge en esta. Su función es servir de intermediario entre el usuario e Internet. Como su nombre indica, el dispositivo está conectado a una red

privada que permite que los usuarios envíen y reciban información por medio de redes virtuales. Estas conexiones se encuentran cifradas. Además, pueden realizarse desde el otro lado del mundo. Aparte de proteger la privacidad del usuario, también aporta otras ventajas como una capa extra de seguridad, acceder a contenidos censurados o bloqueados en tu país, ocultar la propia IP del dispositivo… A toda esta información solo tendrá acceso el propio servidor host de la VPN.

Como forma de **protección de datos y privacidad** dentro del ordenamiento jurídico de la UE, se encuentra el **GDPR** (*General Data Protection Regulation*). Surgió por la necesidad de unificar todas las normas sobre uso y tratamiento de datos de los diferentes países de Europa, dada también de la necesidad de actualización ante el avance de la tecnología en los últimos años. Se aplica a los 27 Estados de la UE y su entrada en vigor fue el 25 de mayo de 2016 y pasaron a ser obligatorias justo el mismo día, dos años después, en 2018. Principalmente, el GDPR ha aumentado la protección hacia los datos de los particulares, haciendo que las empresas tengan la obligación de documentar todos los datos que obtienen y su fin posterior. Algunas de las garantías más importantes que ofrece son: el derecho al olvido (el derecho del usuario a pedirle a una empresa que borre todos sus datos personales que tenga, teniendo esta 30 días para efectuarlo); disminución de marketing y publicidad (los usuarios deben de dar su consentimiento explícito y estar informados para que sus datos personales puedan ser utilizados para la comercialización, “Términos de Servicio”) y el derecho a la inocencia (seguridad extra para los jóvenes, permitiéndoles eliminar mensajes comprometedores).

Este reglamento se basó en las reglas anteriores “*Privacy Shield*” y “*Data Protection Directive*” y añadieron mayores requisitos y sanciones más duras divididas en cuatro niveles (advertencia, amonestación, suspensión del tratamiento de datos y multa económica). En caso de no cumplir este último nivel, las sanciones pueden llegar a ser de hasta 20 millones de euros o hasta el 4% de los ingresos anuales. Según el estudio realizado por el bufete DLA Piper sobre el valor total de las multas impuestas desde que este reglamento pasó a ser de obligatorio cumplimiento hasta enero del 2021, clasificaba a España en el puesto quinto del ranking (McKean, R., Kurowska-Tober, E., & Waem, H., 2021).

El GDPR se aplica en la Unión Europea, sin embargo, estos países sometidos a este reglamento también pueden tener sus propias leyes para proteger estos datos. Destacar que estas leyes no serán contrarias a lo establecido en el GDPR, simplemente podrán definir más detalladamente algunos aspectos de estos. En el caso de España, en su ordenamiento jurídico se recoge la Ley Orgánica de Protección de Datos de Carácter Personal de 1999, que fue derogada posteriormente por la Ley Orgánica de Protección de

Datos Personales y Garantía de los Derechos Digitales **(LOPDGDD)** en 2018 para así adaptarse al GDPR. Esta ley hace referencia al tratamiento de información personal que se efectúan entre usuarios y empresas (BOE, 2018). Así como a los derechos que tienen los usuarios. Su objetivo, en base al artículo 18.4 de la Constitución Española, es proteger la intimidad, la privacidad e integridad de las personas, del mismo modo que a los procesos de transferencia de estos datos personales. Creando de esta forma un marco legislativo para la protección de datos personales en Internet. Los datos personales constituyen toda la información que se encuentre tanto en texto, imagen o audio y que posibilite la identificación de la persona.

Quien se encarga de velar para que esta ley orgánica se cumpla es la **Agencia Española de Protección de Datos**. Se trata de un organismo público de control independiente creado en 1993. Su ámbito de actuación se extiende a todo el territorio español y su sede se encuentra en Madrid. Su actividad se encuentra regulada por el GDPR y la LOPDGDD. En España también existen otros organismos de carácter inferior que actúan en algunas comunidades autónomas, como es el caso de Cataluña y País Vasco. La AEPD actúa en el ámbito de Internet, las redes sociales, en la educación o en proyectos europeos como SMOOTH o TIME FOR DATA, entre otros. En 2021, recibió varios premios como: el Trofeo Extraordinario Seguridad TIC de la revista Red Seguridad y el Acto de entrega del “Premio Ciudadanía”, del Ministerio de Política Territorial y Función Pública. Sin embargo, desde 2017 ha recibido muchos más premios.

3. CRIPTOGRAFÍA

Llegados a este punto del trabajo, se ha observado que existe una problemática importante en los correos electrónicos, y es la falta de seguridad que muestran. Para subsanar estos problemas, entre otros, surgió la criptografía aplicada a la informática. La palabra Criptografía procede del griego, de “kryptos” que significa oculto y “graphia”, escritura. La RAE define este concepto como el “Arte de escribir con clave secreta o de un modo enigmático” (Asale, R., s. f.). Hace uso de cifras o códigos, mediante algoritmos matemáticos, para ocultar información a otras personas que no están autorizadas a ello. Se crean claves con las que solo puedes acceder a esa información mediante la clave correspondiente. El objetivo de esta técnica es mantener la confidencialidad de toda la información que se envíe por medio de un mensaje. Así pues, se consigue tanto la propia seguridad del usuario como la propia autenticación de él mismo, del destinatario y el mensaje (que no haya sido manipulado durante el proceso).

La criptografía consiste en el proceso de codificar algo y posteriormente se descodifica. De esta forma surgieron los primeros métodos de cifrado clásicos: cifrado de sustitución y cifrado de transposición.

- Cifrado de Sustitución: se basa en la regla de sustituir las letras del mensaje original por otras. Al mantenerse el orden de dichas letras originales, esto provocaba que fuera más fácil descodificarlos. En este grupo es muy conocido el **Cifrado César**, que consistía en sustituir cada letra del mensaje por la que se encontraba tres después en el alfabeto latino. Otros tipos de cifrado de sustitución son: sustitución Monoalfabética, la Polialfabética y la Homofónica.

- Cifrado de Transposición: se basa en la regla de desordenar las posiciones de las letras del mensaje original. Hay que tener en cuenta que de esta forma en el mensaje codificado había las mismas letras del mensaje original pero cambiadas de lugar. En este caso, la técnica más relevante fue la que utilizaban los espartanos, la **Escitala,** ya que es de los primeros en la historia. Consiste en envolver una tela con el mensaje codificado sobre una vara especial y de esta forma era la única forma de descubrir el verdadero mensaje. Otros tipos de cifrado de transposición son: transposición por grupos, por series y por filas o columnas.

3.1. TIPOS DE CIFRADOS

Posteriormente, se produjo una evolución en las tecnologías en la informática, por lo que estas máquinas criptográficas también se adaptaron a ellas, haciéndose así más seguras, consiguiendo una confidencialidad mayor. De aquí surgieron los sistemas criptográficos que conocemos hoy en día, que se basan en que un mensaje se cifra utilizando una clave específica y después se descifra con la misma clave (Gutiérrez, P., 2017). Estos tipos de sistemas de criptografía son:

- **Función Hash**: También conocido como función resumen, es un algoritmo matemático que se utiliza sobre todo para los mensajes largos. Su funcionamiento consiste en transformar un mensaje, independientemente de su tamaño de entrada, consiguiendo una cadena de longitud de salida fija, la cual siempre será del mismo tamaño. Estos resúmenes generados serán únicos para cada mensaje, ya que estás cadenas se forman con números del “0 al 9” y con letras de la “A a la F”, como se observa en la figura 3.1. En caso de que la cadena resultante coincida con otra se denomina colisión. Por tanto, esta función hash se puede considerar similar a los algoritmos de compresión de la información que utiliza la informática. De esta forma,

el usuario puede comprobar si dicho mensaje recibido utilizando este método ha sido alterado. Además, de proteger el mensaje, también se utiliza para la seguridad de contraseñas y para las firmas digitales.

Uno de estos algoritmos hash más conocidos son los **SHA-1** que utilizan 20 bytes (40 caracteres). Además es muy utilizado en la firma digital por la seguridad que aporta. A pesar de ello, actualmente se considera insegura y varias empresas han dejado de usar.

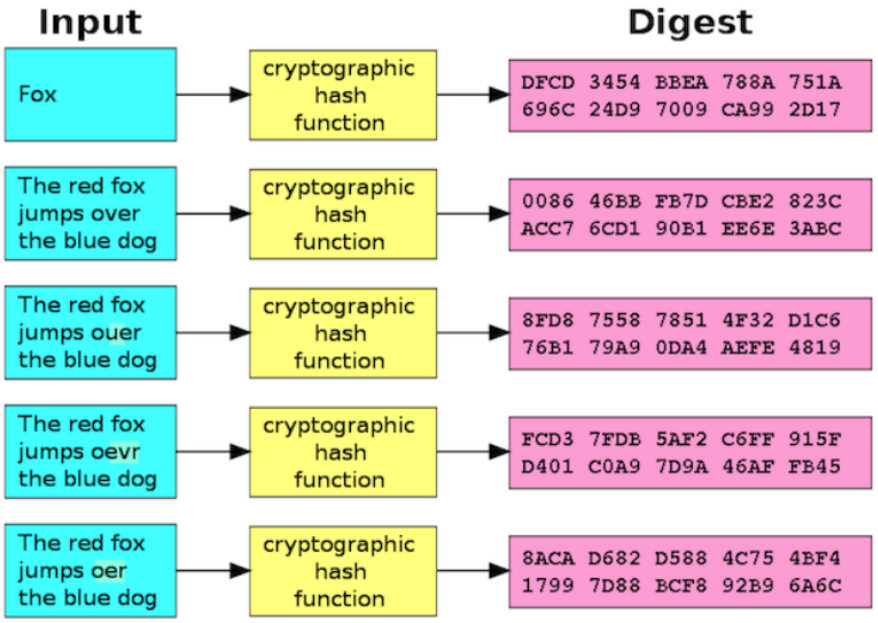


Figura 3.1: Ejemplo de función Hash (Donohue, B., 2021).

- **Sistema Simétrico**: También conocido como clave privada, se caracteriza por la utilización de la misma clave, tanto para cifrar como descifrar el mensaje, como se muestra en la figura 3.2. Este sistema genera un problema notable, su punto débil es nuestra comunicación, porque la persona que envía este mensaje como la que lo recibe tienen que tener la misma clave para poder comunicarse de esta forma. Por lo que la transmisión de dicha clave a la otra persona resulta dificultosa, ya que puede ser interceptada por otros. Su utilización principal es para proteger la privacidad y la confidencialidad.

Figura 3.2: Ejemplo gráfico del sistema Simétrico (J., s. f.-a).

Uno de estos tipos de sistema simétrico más usados actualmente es el **AES** (*Advanced Encryption Standard*) dada su alta seguridad. Existen tres tipos dependiendo de sus bits: 128 bits, 192 bits y 256 bits (el más seguro). Se caracteriza por ser de acceso público, por lo que se puede usar tanto en cualquier ámbito.

- **Sistema Asimétrico**: También conocido como clave pública, se caracteriza por la utilización de dos claves diferentes, una para cifrar y otra para descifrar. Una de estas claves será pública, mientras que la otra deberá ser privada. De esta forma se pueden producir dos casos. En el primero, si se usa la clave pública para cifrar el mensaje, solo el que posea la clave privada podrá acceder a este mensaje, asegurando así su confidencialidad. En el segundo caso, si se utiliza la clave privada para cifrar cualquiera que utilice la clave pública, podrá acceder a dicho mensaje. De este modo, se consigue la autenticidad del documento (perdiendo a su vez la confidencialidad). Estos casos se observan en la figura 3.3, donde se muestran el caso de autenticidad y el de confidencialidad. Este tipo de claves pueden llegar a tener un tamaño de 2048 bits, lo que las convierte en prácticamente imposible de descifrar.

  Dentro de este sistema se encuentra el **RSA**, uno de los más utilizados dada su sencillez de uso. Destaca porque la clave privada y pública se obtienen a través de la factorización de números primos grandes y la aritmética modular. Al crear claves con un tamaño importante se vuelven mucho más seguras. Al tener estas características permite que este algoritmo tenga otras funciones como la firma digital.

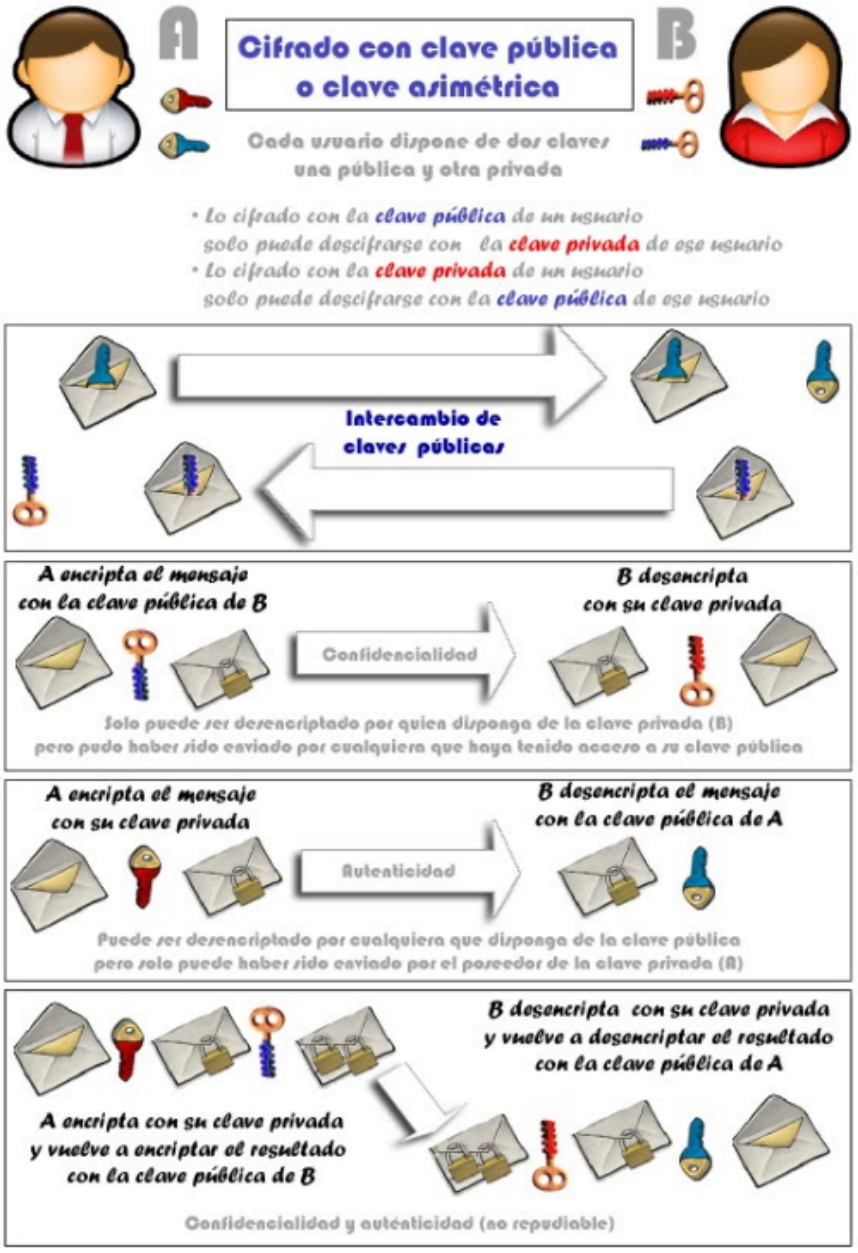


Figura 3.3: Ejemplo gráfico del sistema Asimétrico (J., s. f.-b)

En el día a día, se utiliza tanto el sistema simétrico como el asimétrico de forma complementaria para así tener mayor seguridad en los mensajes y hacer más eficientes estas operaciones. El sistema asimétrico es más costoso en sus procesos, pero más seguro, por lo que se combina con el sistema simétrico, que a su vez son más rápidos pero más inseguros. A este método se lo conoce como **Criptografía Híbrida** (se ejemplifica en el último ejemplo de la figura 3.3), la cual utiliza los dos sistemas anteriores para garantizar tanto la confidencialidad como la autenticidad de los mensajes. Un ejemplo de este proceso sería: A cifra un mensaje con la clave privada y al mismo tiempo la vuelve a cifrar con la

clave pública de B. Entonces, B lo descifrará primero con su clave privada y posteriormente con la clave pública de A.

3.2. PROTOCOLOS QUE UTILIZAN ESTE MÉTODO

Una vez visto el funcionamiento de los diferentes sistemas criptográficos, existen una serie de protocolos que hacen uso de estos métodos para garantizar la seguridad del usuario, que pueden usar los correos electrónicos para su funcionamiento de envíos de mensajes. Entre los más conocidos se encuentran el Protocolo SSL (*Secure Socket Layer*) y el Protocolo TLS (*Transport Layer Security*).

Protocolo SSL

El Protocolo SSL se empezó a utilizar en 1995 y posteriormente se actualizó a las versiones SSLv2 y SSLv3 progresivamente. Este protocolo estándar combina la criptografía simétrica y la asimétrica. Su objetivo es proteger las comunicaciones a través de Internet, garantizando al usuario que su información confidencial no sea interceptada por otros usuarios no deseados o que el mensaje no se modifique durante su transporte. Tanto el emisor como el receptor de este intercambio de información pueden ser un cliente con un servidor o incluso un servidor con otro servidor. Está formado por dos capas que dan funcionalidad a sus capas inferiores y superiores. Este protocolo pertenece a la capa de transporte que se ejecuta entre la capa dedicada al protocolo TCP/IP y el protocolo IMAP en el caso de los correos electrónicos. Además, cuenta con su propio certificado electrónico, certificado SSL, que se utiliza para asegurar la conexión de la comunicación con los sitios web (Weaver, A., 2006).

Protocolo TLS

El Protocolo TLS se ejecutó en 1999 como sustituto de la versión SSLv3. La versión más actualizada es el TLS 1.3. En muchas ocasiones tanto al TLS como al SSL se le denomina del mismo modo “SSL” o “SSL/TLS”, sin embargo, el TLS es una versión más actualizada y, por tanto, más segura, eficiente y flexible. Se considera el protocolo universal más usado sobre todo para la *World Wide Web*. Por ejemplo, Google Workspace, actualmente utiliza este protocolo para asegurar sus comunicaciones. Tiene como objetivos asegurar la autenticidad, la integridad y la confidencialidad de quienes se comunican por Internet. Se encarga de cifrar automáticamente todo el contenido que se requiera para transportar (Turner, S., 2014).

Su funcionamiento es el siguiente: Supongamos que un cliente quiere contactar con un servidor web, primero este último le enviará su certificado electrónico para que el cliente compruebe su autenticidad. Una vez hecho esto, el cliente generará una clave simétrica y la cifrará mediante la clave pública del servidor web y se la volverá a enviar, para que el propio servidor web genere una clave privada que se la enviará al cliente. De esta forma, la comunicación ya sería segura para ambas partes.

Destacar también el Protocolo **HTTP** (*Hypertext Transfer Protocol*). Se creó en la década de 1990 y pertenece a la capa de aplicación que utiliza la conexión TCP/IP o TLS como transporte. Es el que utiliza el propio navegador web para acceder a otras páginas web. Aparecerá en la dirección URL si el sitio web está protegido con un certificado SSL. El protocolo HTTP se considera inseguro, por ello, para indicar que una web es segura se coloca una “s” detrás, utilizando otro tipo de protocolo **HTTPS** (*Hypertext Transfer Protocol Secure*). De este modo, estas siglas nos indican que la web a la que accedemos es segura y está protegida garantizando la integridad y la confidencialidad de la información que se comparte. Su función es contactar con el servidor web deseado mediante un código para decirle qué página quiere ver. Es decir, realizar peticiones de datos y recursos donde las peticiones son los mensajes que envía el cliente y las respuestas hacen referencia a los mensajes enviados por el servidor. Este protocolo también es usado junto con los anteriores protocolos para los casos en que se quiere contactar con un servidor web.

4. LA FIRMA DIGITAL

Como se ha comentado anteriormente, existen muchas amenazas que pueden afectar al usuario cuando envía un mensaje por correo electrónico. Por ejemplo, los ataques phising, los cuales han ido creciendo con el paso del tiempo, incrementando así su peligrosidad porque afectan a la información confidencial de las personas. Con el uso de la criptografía, se ha encontrado una solución a este problema, las firmas digitales que van asociadas a estos mensajes. Este tipo de firmas son como una capa de seguridad que garantizan la **autenticidad e integridad del mensaje**, que no ha sido manipulado por otros durante el transporte y verifica que el emisor es quien dice ser. De esta forma permite al usuario identificar el origen del mensaje, así como la persona o empresa que lo envía y asegurarse de sí se trata de algún tipo de fraude. Por esta razón, es considerada una herramienta esencial en muchos casos, por lo que es muy útil para la tramitación de documentos legales y financieros. Consigue evitar falsificaciones con su uso o aumentar la confidencialidad en sus mensajes. Además, esta firma siempre tendrá el mismo tamaño, ya que es independiente del propio tamaño del mensaje.

La firma electrónica se encuentra regulada en el **Reglamento n.º 910/2014 del Parlamento y del Consejo**, de 23 de julio 2014, relativo a la identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior, en la Unión Europea. Mientras que en España, se regula mediante la **Ley 6/2020**, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

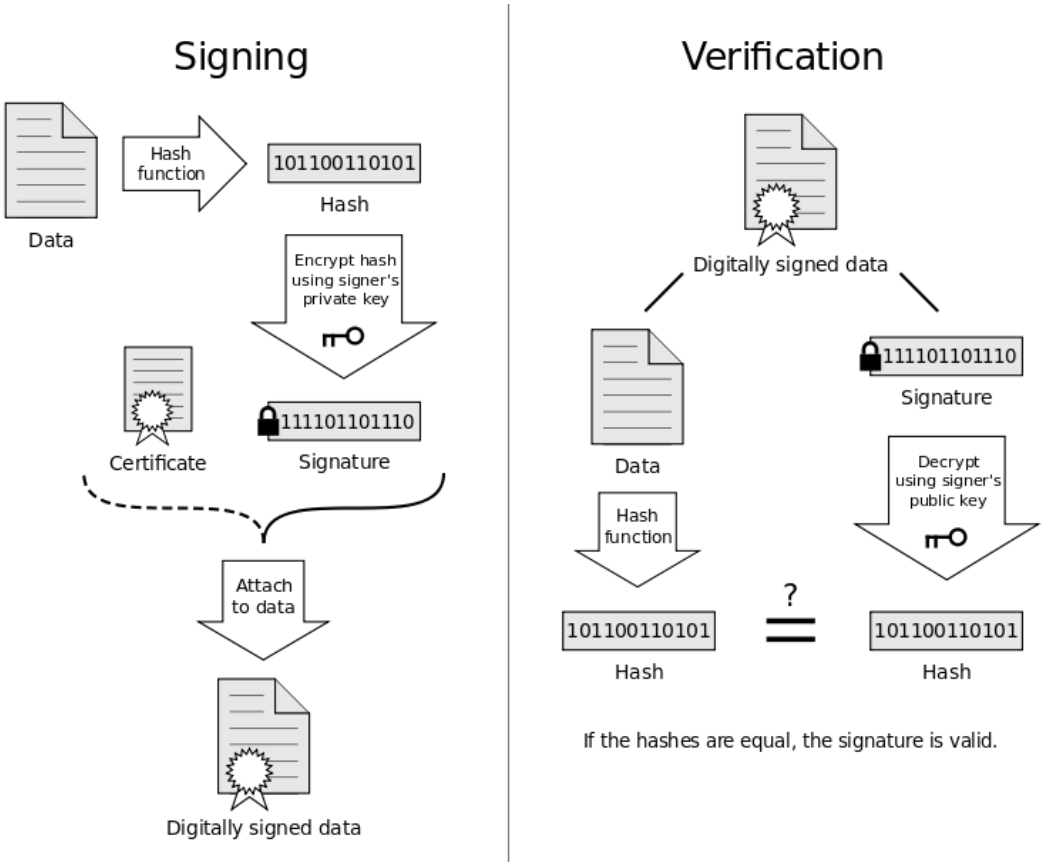


Figura 4.1: Funcionamiento y comprobación de la firma digital (A., 2010).

La creación de una firma electrónica es simple, ya que utiliza el sistema asimétrico, por lo que el emisor contará con dos claves distintas (una pública y otra privada). Estas provienen de un certificado digital expedido por una autoridad certificadora (será explicado posteriormente). Su funcionamiento es el siguiente: El documento que el emisor quiera enviar se le aplicará una función hash conocida con el fin de obtener un resumen hash del mismo para tener una huella digital del documento única. Posteriormente, se cifrará este resultado con la clave privada que tenga, obteniendo la huella digital cifrada. Después, enviará tanto el documento original, el resumen hash cifrado al receptor como la clave pública del emisor, obteniendo así el documento firmado. De esta forma se enviará un documento con la firma digital. Ahora bien, el receptor tendrá que autenticar que el emisor es quien dice ser y que el documento no ha sido manipulado por otros. Por tanto, el receptor aplicará una función hash al documento original y, mediante la clave pública del emisor,

descifrará el resumen hash cifrado recibido. Obtenido estos dos documentos de esta forma, el receptor los comparará y si coinciden significa que la transmisión del mensaje se ha realizado de forma segura y que el emisor es quien dice ser. En caso de no coincidir, significa todo lo contrario, que el mensaje ha sido alterado y que el emisor es otro al que dice ser. Este proceso lo realiza el cliente de correo electrónico siempre que se haya configurado previamente para que realice esta acción. Estas acciones se observan en la figura 4.1, mostrando tanto el funcionamiento como la comprobación de una firma digital.

En muchas ocasiones, se combina la firma digital con el cifrado de mensajes para que el proceso sea todavía más seguro. De esta forma el usuario se asegura que el mensaje no se va a poder manipular por otros (firma digital) y que no se va a poder ver su contenido durante su envío. Una solución sería utilizar el **sistema GPG** (*GNU Privacy Guard*) que permite utilizar también este cifrado de correo electrónico. Es la versión libre del sistema PGP que sirve tanto para cifrar como para firmar digitalmente un documento. Otra función que ofrece es la de repositorio de claves (anillo de claves) donde se guardan todas las claves que nuestro sistema tenga. Las claves públicas y privadas se diferencian en este repositorio con estos términos: claves públicas "*pub"*, clave privada "*sub"*. A pesar de estas facilidades, como usuarios hay que tener cuidado con la forma y a quien se le comparte una clave, ya que puede ocasionar suplantaciones de identidad, entre otros problemas (Gutiérrez, P., 2013).

Analizando toda esta información, podemos afirmar que la firma digital ofrece unas ventajas únicas al usuario como: mayor seguridad en las comunicaciones, garantiza la confidencialidad de los datos enviados e incluso se muestra como una señal de calidad por parte de las empresas.

4.1. AUTORIDAD CERTIFICADORA

Así y todo, existe un problema con estas claves generadas. ¿Cómo sabemos que son veraces? Es decir, si pertenecen a quien dicen ser. Estas claves utilizadas por un usuario para la firma digital deben de estar verificadas por un organismo oficial de certificación que asegure la asociación de estas claves con las personas correspondientes. De tal forma, mediante el certificado digital se crean las dos claves necesarias. Son las encargadas de generar dichas claves y asignarlas a quienes corresponda por medio de certificados. De esta forma el destinatario se asegura que la clave que se utiliza es la del remitente auténtico y no de otro usuario que quiera suplantarlo y cometer algún tipo de delito. Esta autoridad certificadora es la **CA** (*Certification Authority*). Se encarga de emitir, administrar y revocar certificados digitales para mantener una confianza entre los usuarios y entidades de

Internet. Su objetivo es verificar la autenticidad de una web, dominio… para que los usuarios puedan confiar en ellas. Existen muchas autoridades certificadoras, pero no todas son reconocidas. Para crear un certificado digital, esta autoridad sigue los siguientes pasos: crea un par de claves, una pública (aparece en el certificado) y una privada (se mantiene en secreto, incluso para la CA); también se genera una solicitud, por parte del solicitante, de firma de certificado (CSR) donde se incluirán los datos necesarios de forma cifrada. El CSR se enviará a la CA por parte del solicitante para su verificación. Finalmente, el CA crea el certificado y lo firma digitalmente con la clave privada y lo envía al solicitante. Este proceso en muchos casos suponen unas tasas. Destacar que la clave privada generada solo será conocida únicamente por su titular que normalmente se almacena en el disco duro o tarjeta criptográfica. En caso de que la clave de cifrado solo la tenga una persona, lo que cifre esa persona podrá ser utilizado como firma electrónica, ya que solo ella es capaz de utilizarla.

4.2. CERTIFICADO ELECTRÓNICO

Así pues, estos certificados que genera la autoridad certificadora (con algunas diferencias) también son usados para otras funciones como verificar las páginas webs y aportar una seguridad extra. Un certificado **electrónico** es un archivo que es utilizado para unir, mediante la criptografía, una entidad con una clave pública. Es como una credencial de validación que permite que la comunicación en Internet sea segura porque encripta la información. El contenido de estos certificados es muy variado, pero como norma general contiene los siguientes datos: el nombre de la entidad a la cual va asociado, clave pública, fecha de emisión del certificado, el nombre de la CA y su firma digital, entre otros. Destacar que estos certificados tienen fecha de caducidad, la cual suele ser de entre 3 y 24 meses. El formato estándar que se utiliza es el modelo x.509 del ITU-T (*International Telecommunication Union-Telecommunication Standardization Sector*) y el ISO/IEC (*International Standards Organization / International Electrotechnical Commission*).

Los certificados que suelen emitir estas CA son los **certificados SSL/TLS**. Este concepto ya se ha visto anteriormente, el cual permite que la capa de transporte utilice estos certificados para que la conexión a través de Internet sea segura, cifrando la información que se envía mediante el protocolo de transferencia de hipertexto seguro (HTTPS). El funcionamiento es el siguiente: Un navegador web inicia conexión mediante HTTPS y el certificado digital de este sitio web se envía al navegador. Y posteriormente, el navegador comprueba el certificado y lo acredita en su almacén de certificados raíz, asegurando así la conexión. El método más utilizado actualmente para cifrar es el AES junto con la función hash SHA256. Sin embargo, como la tecnología va evolucionando constantemente, este

método también va cambiando para volverse más seguro contra los ciberdelincuentes. Por tanto, estos tipos de certificados se encargan de proteger las webs, autenticar y asegurar las conexiones de forma cifrada. Un certificado SSL está compuesto por tres partes: el certificado SSL (la parte pública), la clave privada y los certificados intermedios. Los servicios de correo electrónico más utilizados soportan estos certificados, y si el cliente correo permite esta conexión, sus protocolos pasarían a llamarse IMAPS, SMTPS y POP3S. Para ello, existen los puertos de conexión más habituales para cada protocolo: 465 (SMTPS), 993 (IMAPS) y 995 (POP3S).

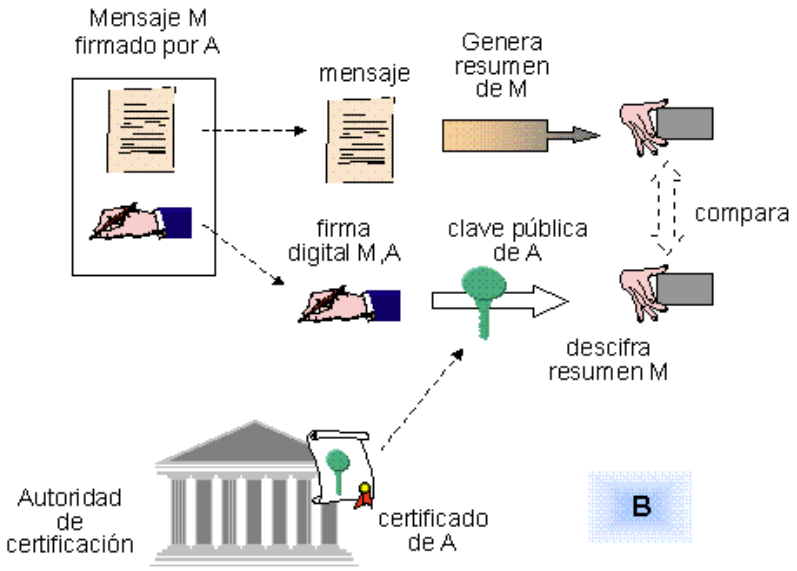


Figura 4.2: Comprobación de la firma digital junto con el certificado digital (Vázquez, E., 1999).

En muchas ocasiones, se crean páginas web fraudulentas para engañar al usuario y obtener información personal de él o conseguir sustraer dinero. Una forma es mediante el phishing, enviar un correo electrónico a alguien suplantando la identidad de algún banco, por ejemplo, y adjuntando un enlace donde remite al usuario a la supuesta página oficial de dicho banco. Gracias a la utilización de estos certificados, tanto la transmisión como la navegación en páginas se hace de forma segura, algo esencial para la propia navegación, ya que se puede comprobar dichas características como se observa en la figura 4.2. Su uso es considerado obligatorio, sobre todo para tener una compra segura por Internet. También para cualquier página u operación en la que se requiera información personal del usuario.

Hay varias formas de identificar si un sitio web está protegido con un certificado SSL. Principalmente, la dirección web de esa página empieza con “https”. También, dependiendo de su nivel de **autenticación**, puede mostrarse mediante un icono de un candado o incluso una barra de direcciones con una señal verde. Un ejemplo de ello se muestra en la figura

4.3, tanto las siglas “https” y el candado. Existen 3 grupos de niveles según su autenticación:

1. Validación de Dominios: Requieren únicamente que las webs muestran su control del nombre del dominio. Son los de nivel más básico y pueden obtenerse de forma gratuita. Sin embargo, su validación se realiza de forma superficial o incluso de forma automática, por lo que no se consideran del todo seguros.

2. Validación de Organizaciones: Requiere tanto que se demuestre la documentación de los propietarios de la web como demostrar que su compañía se encuentra registrada legalmente responsable de este. Solo pueden obtenerlo organizaciones o empresas. Estos son más seguros que los anteriores, ya que tienen más control sobre ellos.

3. Validación Extendida: Requiere de dos validaciones, de dominio y empresa, y varios documentos que verifiquen que este certificado corresponde a la empresa registrada asociada. Añade información extra al usuario en la barra de direcciones, que puede acceder a ella mediante el icono del candado. Solo lo pueden utilizar organizaciones y empresas. Este certificado es el más seguro dada la información que transmite, así como el control que se tiene de ellas.

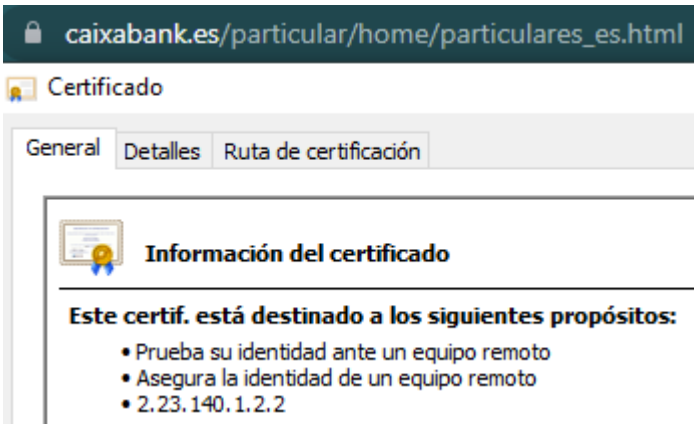


Figura 4.3: Ejemplo de certificado digital de validación extendida.

5. CONCLUSIONES

PRIMERA: Tal como se ha observado a lo largo de este trabajo, **Internet** ha ayudado a que **la evolución de las tecnologías informáticas** haya crecido (y que siga creciendo) a un ritmo cada vez más acelerado. De esta forma nos ha ofrecido herramientas para que nuestras vidas sean más cómodas, más fáciles. Y una de estas herramientas ha sido el

correo electrónico, la cual nos ha ayudado sobre todo en la comunicación de una forma tan radical que ha cambiado incluso la forma de cómo nos comunicamos socialmente.

SEGUNDA: Hay que tener presente las importantes **ventajas** que nos ofrece el correo electrónico. Facilidades que aporta en nuestras vidas y que por estas razones lo utilizamos en el día a día. Al ser una herramienta **rápida** y **económica**, atrae a qué más y más personas lo utilicen. Incluso hace una aportación importantísima a nuestro planeta, ya que se sustituye el papel de las cartas y documentos que anexamos, al simple texto que se escribe en nuestro correo electrónico y se envía de forma instantánea.

TERCERA: Como en cualquier ámbito, existen personas que quieren beneficiarse de estas tecnologías y buscan estas oportunidades para ello. Al igual que las tecnologías, los delitos también evolucionan y se adaptan al medio. Por ello, hay que destacar las **desventajas** que el correo electrónico posee al utilizarlo. Se observa que la que tiene más relevancia entre todas es **la falta de seguridad** que ofrece al usuario, una privacidad que se encuentra desprotegida. Una seguridad que garantice la confidencialidad y la autenticidad de nuestra información es esencial y que debería tener derecho cualquier usuario, aun así, en muchas ocasiones no se les ofrece porque muchos de los correos electrónicos que utilizamos no cubren estas necesidades. También encontramos el **spam** o el **scam** como inconvenientes de uso de este servicio. Y curiosamente, cada una especializada en unos fines que el delincuente puede elegir dependiendo de sus objetivos, o incluso complementarlos para tener mayor eficacia en sus planes.

CUARTA: Es verdad que existen muchas **herramientas** con las que combatir o prevenir estos problemas. Sin embargo, los problemas e inconvenientes que causa la tecnología son difíciles de combatir al tener una evolución constante. Hoy en día contamos con la **criptografía** que ayuda a que nuestros mensajes no sean captados por otros no deseados o modificados, garantizando la autenticidad y privacidad de estos. De esta forma es como ha surgido la **firma digital** que incluso muchísimas instituciones hacen uso tanto para protegerse a ellas mismas como a sus clientes. Nos aporta una seguridad extra que utilizando en el correo de forma normal no tendríamos. Además, proporciona como una prueba en caso de ir a un juicio. También encontramos instituciones que intentan combatir estos delitos como la **Agencia Española de Protección de Datos**.

QUINTA: Estos delitos informáticos han ido creciendo durante estos años y en varias ocasiones esto ocurre porque el usuario no tiene los conocimientos necesarios para hacerles frente o simplemente no son conscientes de lo que está ocurriendo. Así pues, se observa una carencia que hay que llenar. Este **desconocimiento de los peligros** a los que se someten es tal que ya no solo hay que actuar en el ámbito educativo de los más jóvenes

(algo que es importantísimo para formar unas bases), sino actuar también en el grupo de personas que son más vulnerables, que son las personas mayores. A estas personas ya de por sí les cuesta hacer uso de la tecnología actual. Por ello, son más vulnerables que otros, por ejemplo, si les llega un mensaje al correo sobre su banco que les requiere su usuario y contraseña por un problema, lo más probable es que accedan al enlace e introduzcan sus datos personales, convirtiéndose así en víctimas del delito.

6. BIBLIOGRAFÍA

- A. (2010, 13 octubre). *Digital Signature diagram*. Wikimedia Commons.
- Abbate, P. (2020). *Internet Crime Report 2020*. Internet Crime Complaint Center.
- Asale, R. (s. f.). *criptografía | Diccionario de la lengua española*. «Diccionario de la lengua española» - Edición del Tricentenario.
- Bejerano, P. G. (2014, 6 febrero). *Código Enigma, descifrado: el papel de Turing en la Segunda Guerra Mundial*. ElDiario.es.
- *BOE.es - BOE-A-2018-16673 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.* (2018, 5 diciembre). BOE.
- Dada, E. G., Bassi, J. S., Chiroma, H., Abdulhamid, S. M., Adetunmbi, A. O., & Ajibuwa, O. E. (2019). Machine learning for email spam filtering: review, approaches and open research problems. *Heliyon*, *5*(6), e01802.
- Donohue, B. (2021, 11 marzo). *¿Qué Es Un Hash Y Cómo Funciona?* Blog oficial de Kaspersky.
- Dr. John C. Klensin. (2008). Simple Mail Transfer Protocol de IETF.
- Gutiérrez, P. (2013, 15 enero). *¿Qué son y para qué sirven los hash?: funciones de resumen y firmas digitales*. Genbeta.
- Gutiérrez, P. (2017, 25 agosto). *Tipos de criptografía: simétrica, asimétrica e hibrida*. Genbeta.
- INCIBE. (2020, 23 marzo). *Ponle freno a los fraudes y bulos con buenas prácticas*. Oficina de Seguridad del Internauta.

- INCIBE. (2017, 12 julio). *WhatsApp, el compañero ideal de los bulos*. Oficina de Seguridad del Internauta.
- J. (s. f.-a). *2. Cifrado de claves simétrica - Seguridad informatica-JAVIER*. Google.
- J. (s. f.-b). *3. Cifrado de clave asimétrica - Seguridad informatica-JAVIER*. Google.
- James, L., & Jevans, D. (2005). *Phishing Exposed (English Edition)* (1.ª ed.). Syngress.
- Mark Crispin. (2003). INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1 de IETF.
- McCullagh, D. (2005, 24 mayo). *Minnesota court takes dim view of encryption*. ZDNet.
- McKean, R., Kurowska-Tober, E., & Waem, H. (2021, 19 enero). *DLA Piper GDPR fines and data breach survey: January 2021*. DLA Piper.
- MDN contributors. (2020). Tipos MIME, de Fundación Mozilla
- Morburre. (2010, 29 julio). *Estafa nigeriana* [Figura].
- Myers, J., & Rose, M. (1996). *Post office protocol-version 3*. STD 53, RFC 1939, May.
- Solutions, S. A. L. (2009, 6 abril). *¿Cómo funciona el sistema de correo?* Altenwald Blog.
- Turner, S. (2014). Transport Layer Security. *IEEE Internet Computing*, *18*(6), 60–63.
- Vázquez, E. (1999, enero). *CIPRES-UPM. Estudio de situación del comercio electrónico en España*. CIPRES-UPM.
- Vela Delfa, Cristina (2007) *El correo electrónico el nacimiento de un nuevo género.* [Tesis]
- Weaver, A. (2006). Secure Sockets Layer. *Computer*, *39*(4), 88–90.