

# Seguridad en el Correo Electrónico

Alberto Gregorio Gómez

Jaime Egido Miguélez (Caja Duero)

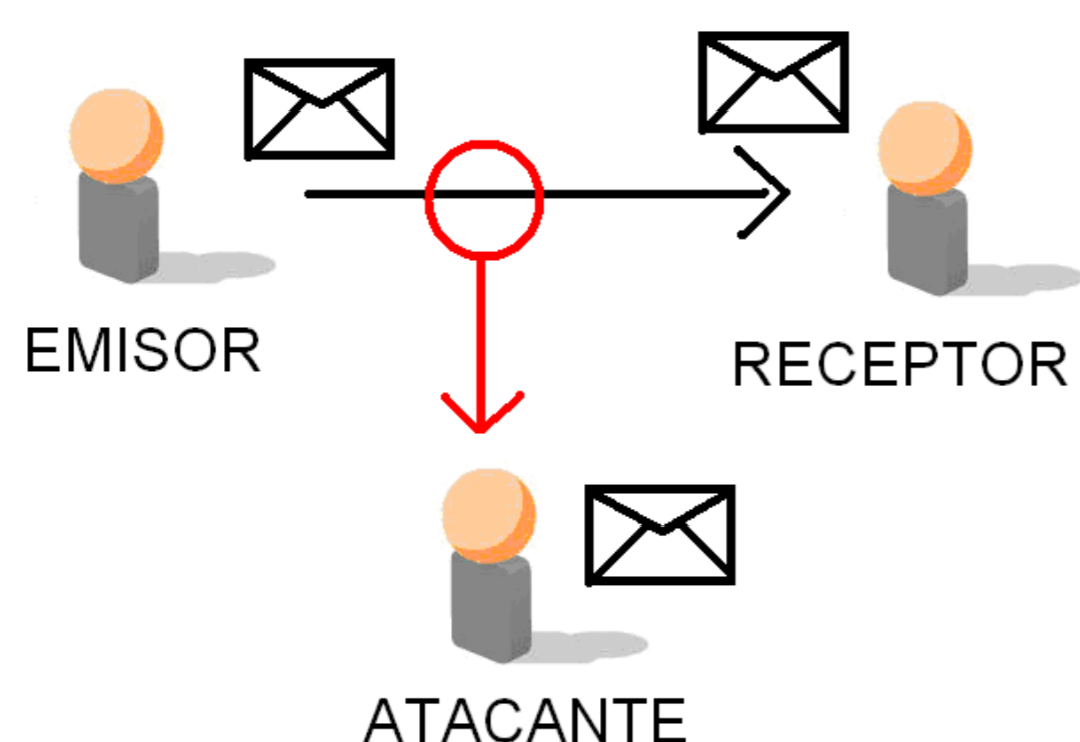
Montserrat Mateos Sánchez (Directora)

(Proyecto en colaboración con Informática Caja Duero)

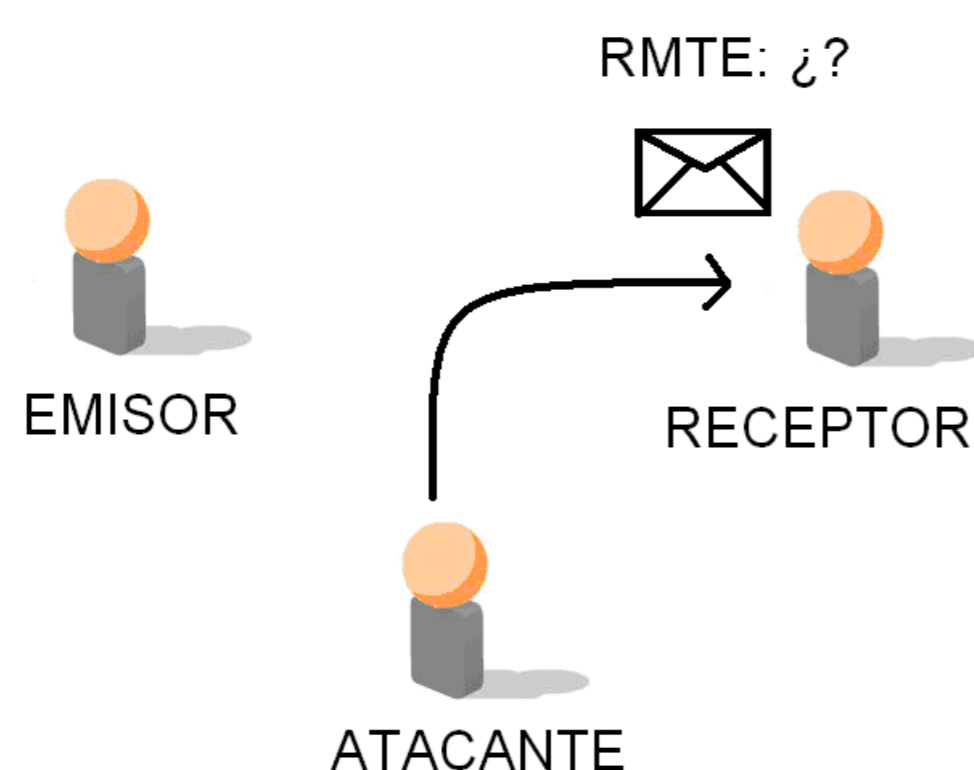


## 1. Descripción General del Proyecto

- Existen diversos **problemas** que afectan a la **seguridad del correo electrónico**.
  - ✓ La **intercepción de los mensajes** permite a un atacante obtener los datos privados de una comunicación.



- ✓ La **falta de autenticación** impide que el receptor de una información pueda verificar la identidad del emisor de la misma.



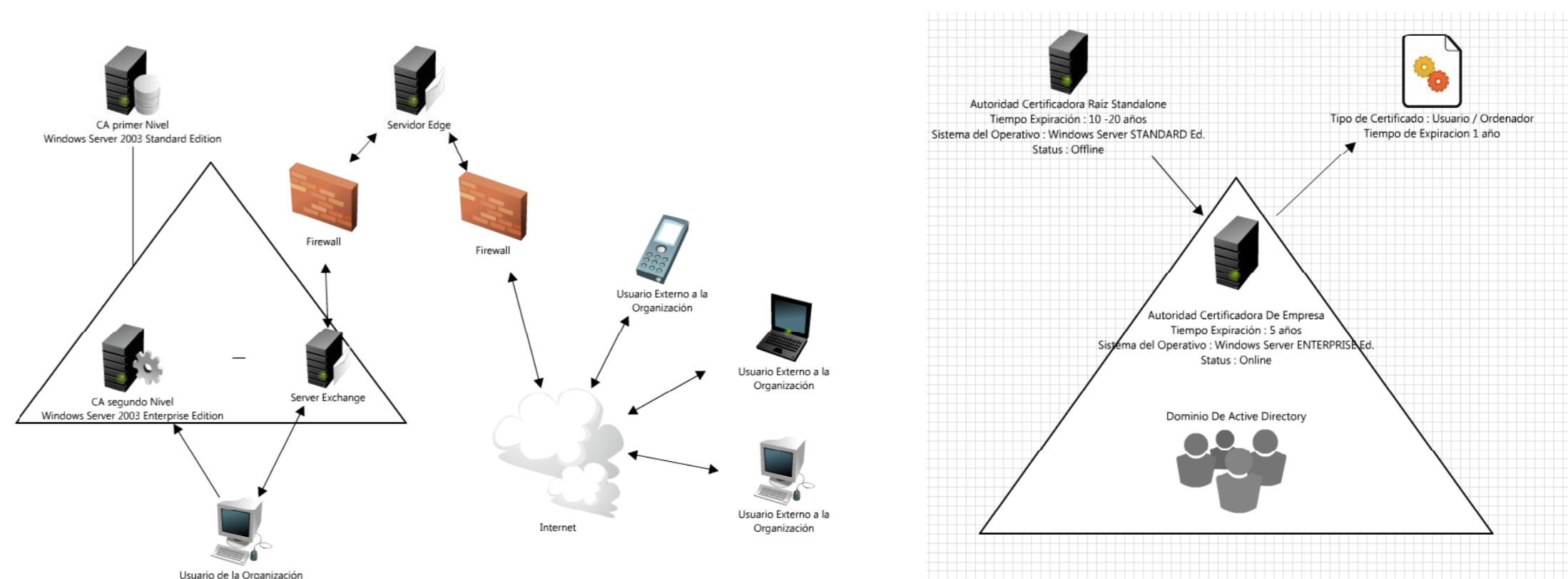
- Sin unas medidas de seguridad** que aseguren nuestra privacidad y la seguridad en la información **somos vulnerables a las amenazas** presentadas.
- La solución pasa por **firmar y cifrar** la información.
- La forma más completa y segura de conseguir el uso de la firma y cifrado actualmente es el uso de una **Infraestructura de Clave Pública**.

## 2. Objetivos

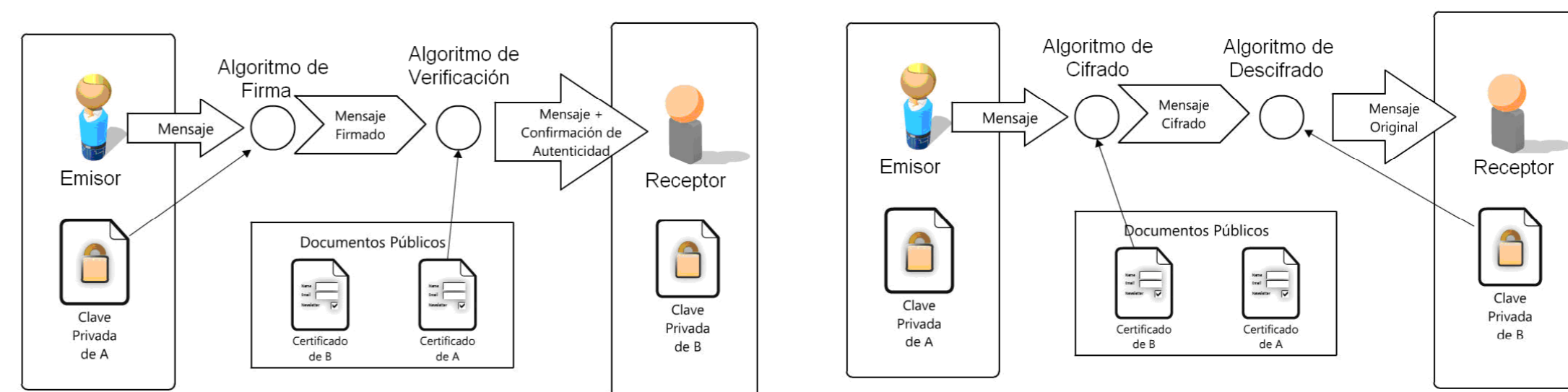
- Estudio de las posibilidades disponibles para asegurar la **seguridad y privacidad** de la información
- Realización de un **proyecto piloto** en el que probar las soluciones en un entorno de trabajo real y similar al que encontramos en la **Universidad Pontificia de Salamanca (UPSA) y Caja Duero**
- Extracción de conclusiones acerca del correcto uso del correo electrónico, asegurando la confidencialidad e integridad y su adaptación al día a día de los usuarios

## 3. Resultados Obtenidos

- Comparativa de soluciones:
  - **Outsourcing**, consistente en contratar los servicios de una empresa dedicada a la seguridad (Verisign) ofreciendo mayor seguridad con un coste superior.
  - **Solución propia**. Desarrollo de un **piloto**.
- Proyecto Piloto**
  - Implementación de una **Infraestructura de Clave Pública (PKI)** para la generación de *certificados digitales*
  - Adaptado a las necesidades **Caja Duero-UPSA**
  - Se basa en el software proporcionado por Microsoft.
  - Se organiza en dos niveles de una jerarquía, ya que es suficiente para aumentar la seguridad sin perjudicar el rendimiento.



- Se ha configurado el escenario con tres máquinas virtuales, simulando una **Autoridad de Certificación** que proporciona seguridad adicional, un **Servidor de Buzones** (autoridad de segundo nivel que genera los certificados) y un cliente que dispone de un navegador y un sistema de correo (**Outlook**)
- Con los **certificados digitales**:
  - Los usuarios pueden **utilizar la firma digital** en sus mensajes asegurando **autenticación e integridad**.
  - Se posibilita el **uso de encriptación** asegurando la **privacidad de los datos**.



- Las **Conclusiones** extraídas del estudio realizado son:
  - El correo electrónico es un **medio inseguro**, necesita de la firma digital y la encriptación para garantizar la **confidencialidad, la integridad** y el **no repudio** en las comunicaciones.
  - Los **certificados digitales** son necesarios para permitir a los usuarios el uso de las técnicas anteriormente citadas.
  - La utilización de estas técnicas ha de ser lo más **sencilla e intuitiva** posible de cara a los usuarios finales del sistema, que deben poder usarlo de manera natural.