# Usando la Criptografía para generar Confidencialidad

DigitalHouse>

Certified Tech Developer
The Ultimate Degree

# Índice

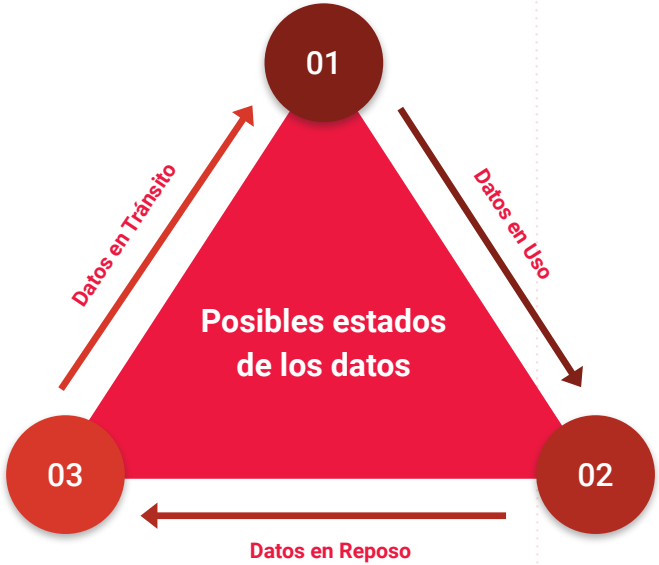
# 1 | Introducción

“Uno de los usos principales de la criptografía es habilitar la confidencialidad en otras palabras, mantener datos o información ininteligibles a ojos no autorizados.”

# Clasificación de Datos según su estado

Tal y como la materia, los datos también tienen 3 estados (bueno, si, la materia puede tener 4 estados, pero para el caso digamos que son 3). Estos no son gaseoso, líquido y sólido, sino:

- Data at **rest**: que son los datos en reposo, que no están siendo consultados por nadie ni nada (por ejemplo: un registro de una base de datos).
- Data in **transit**: que son los datos viajando de los sistemas que los albergan en reposo hacia el cliente o sistema que los haya consultado.
- Data in **use**: que son los datos siendo visualizados o procesados en el cliente o sistema que los haya consultado.



# Protección de Datos según su estado

Desde la perspectiva de la seguridad, dependiendo del estado de los datos se pueden implementar distintas técnicas o medidas para *segurizarlos*. Estos se pueden agrupar en dos grandes categorías: Seguridad **Física** y Seguridad **Lógica**.

# Algunos ejemplos

| | Seguridad Física | Seguridad Lógica |
|---|---|---|
| Data at rest | • Controles de acceso físicos<br>• Camaras de seguridad | • Implementar ACLs para reforzar el principio de 'Least Privilege'.<br>• **Implementar mecanismos de encriptación en los file systems.** |
| Data in transit | • Evitar redes wifi y priorizar redes cableadas<br>• Encriptación de dispositivos de almacenamiento removibles | • Implementar una VPN (Virtual Private Network)<br>• **Encripción de los datos en tránsito (con TLS / SSL)** |
| Data in use | • Limitar el acceso a las áreas de trabajo a sólo personal autorizado | • **Encripción de los datos en memoria.**<br>• RBAC (Role Based Access Control) en los sistemas de usuario.<br>• Un sistema de gestión de identidades robusto |

# Protegiendo los datos en tránsito

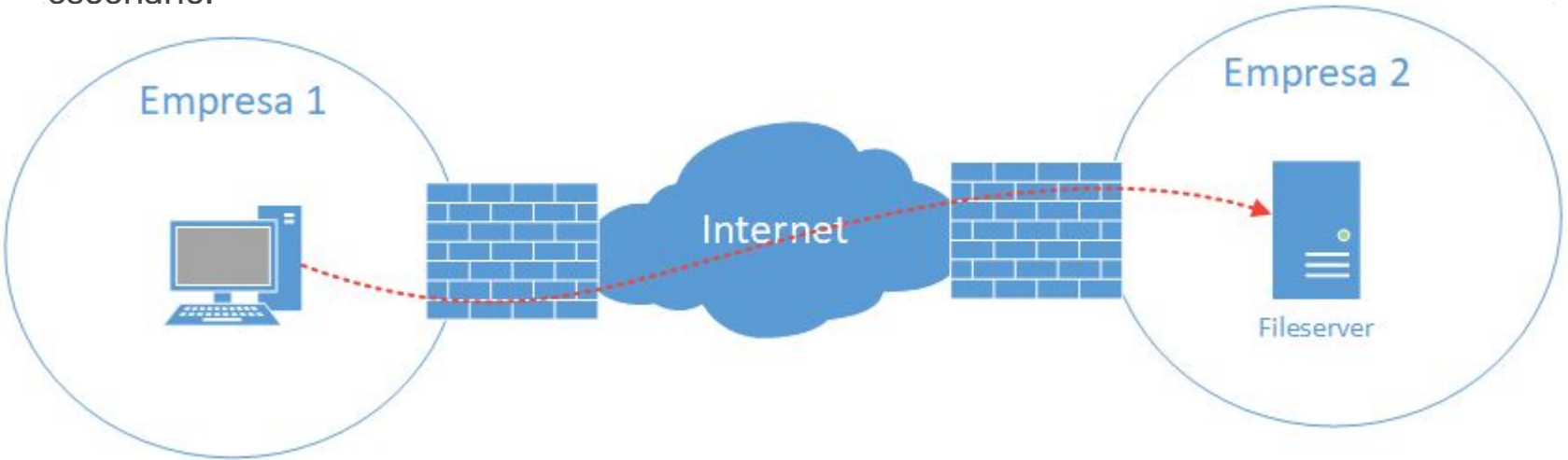
Como pudimos ver en el slide anterior, la criptografía (mencionada como encripción o encriptación) puede ser utilizada en diferentes niveles dependiendo el estado de los datos para protegerlos.

Nosotros nos vamos a enfocar en cómo podemos utilizar la criptografía para proteger los datos en tránsito.

# 2 | Datos en tránsito: Criptografía simétrica

# Criptografía simétrica

Tomemos en consideración este escenario: las empresas 1 y 2 están conectadas por medio de una VPN. Una computadora en la Empresa 1 necesita acceder a un recurso en la Empresa 2. Vamos a ver como la criptografía asimétrica nos puede ayudar en este escenario.



# Criptografía simétrica: el paso a paso

Ambas empresas se ponen de acuerdo en el algoritmo a utilizar y la clave que utilizarán.

Por cada mensaje que la Empresa 1 enviara, se produce un paquete cifrado, utilizando el algoritmo definido, la clave compartida y los datos a intercambiar.

Cuando la Empresa 2 recibe el mensaje cifrado, utiliza el mismo algoritmo y clave para realizar la operación inversa y así obtener el mensaje original.

# Desafíos de la criptografía simétrica

La mayor dificultad que tiene el uso de criptografía simétrica es que la clave a utilizar para codificar los mensajes debe ser conocidas por todas las partes involucradas en la conversación.

Esto es factible cuando conocemos a las partes que van a interactuar y en consecuencia podemos compartir con ellos la clave privada. Pero qué pasa cuando no sabemos con quienes vamos a interactuar y aun así queremos proteger las comunicaciones? Claramente no podemos distribuir la clave privada a todo el mundo, eso rompería con el principio de la confidencialidad y de autenticación...

> Un ejemplo podría ser visitar un sitio de home banking desde nuestras casas. El banco no sabe desde que computadoras o redes accederemos al sitio, y aun asi es su responsabilidad asegurar que las comunicaciones sean protegidas.

**¡Criptografía asimétrica** al rescate!

# 3 | Datos en tránsito: Criptografía Asimétrica

# Criptografía asimétrica

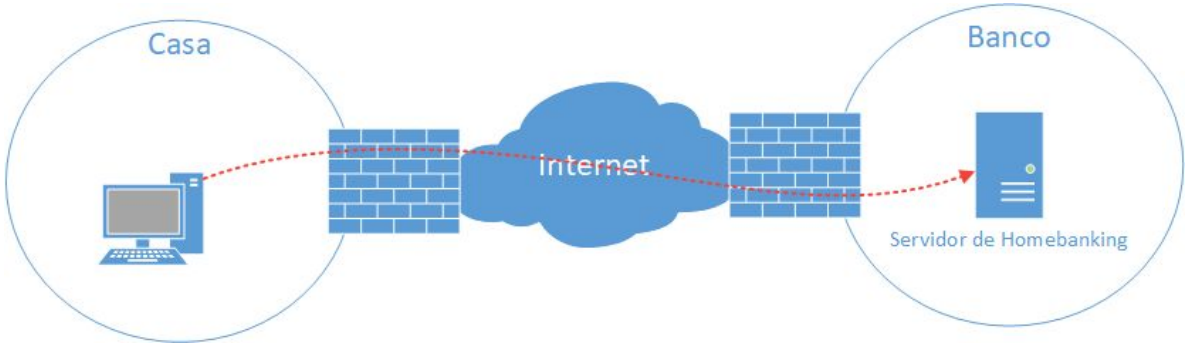
En contraste con la criptografía simétrica donde se usa una misma clave para codificar los mensajes entre todas las partes, en la criptografía asimétrica se hace uso de dos claves.

Ambas claves son generadas matemáticamente y en conjunto. De este modo, los mensajes que son codificados con la clave 1, pueden ser decodificados con la clave 2 y viceversa.

En los pares de claves, una se conoce por el nombre de clave pública mientras que la otra se conoce por el nombre de clave privada.

# Certificados

Repasemos el ejemplo anterior: Acceder a un sitio de home banking desde nuestras casas. El banco no sabe desde que computadoras o redes accederemos al sitio, y aun así es su responsabilidad asegurar que las comunicaciones sean protegidas. Para poder proteger la comunicación, el banco debe distribuir la clave pública a quien sea que visite el sitio. ¡Y esto es posible gracias a los **certificados**!



# ¿Qué tiene un certificado adentro?

Un certificado contiene los siguientes datos:

- Una forma de identificación del sitio que implementa el certificado (IP o nombre de la página)
- Las fechas entre las cuales será válido el certificado (**¡los certificados expiran!**)
- La clave pública que se usará para codificar la comunicación
- La firma de la entidad certificante que emitió el certificado
- Otros datos que hacen a la seguridad del certificado

# Entidad certificante

También conocidas como CA's o Certification Authorities. Para poder cumplir con el principio de autenticación, no cualquiera puede emitir un certificado. Sino que hay entidades conocidas como Certification Authorities (del ingles, Autoridad Certificante) que son las encargadas de verificar que quien solicita el certificado es realmente quien dice ser. En caso de que el certificado vaya a ser usado internamente en la organización, es la organización quien puede tener una CA interna y así emitir el certificado. Pero si el certificado va a ser utilizado de forma externa (como en el caso del sitio de Home Banking), entonces el certificado debe ser emitido por una organización pública que sea conocida y **confiada** por todos.

# Certificados Auto-Firmados (self-signed)

Existe la posibilidad de generar certificados auto-firmados. Es decir, generar un certificado y que seamos nosotros mismos los que lo firmamos.

**¿De qué sirve?**

No mucho más que para hacer pruebas, un certificado de este tipo no debe ser usado nunca en un ambiente de producción. Ya que de ser así, nuestro navegador nos advertirá que el certificado fue emitido por una entidad no confiada.

# Criptografía asimétrica: el paso a paso

1. El cliente ingresa a la URL de home banking.
2. El servidor envía al cliente el certificado.
3. El navegador en el cliente verifica que el certificado sea válido (firmado por una entidad confiada, que no haya expirado y que la URL que estamos visitando coincida con la especificada en el certificado) . De no cumplirse alguna de estas condiciones el navegador nos va a indicar que el certificado no es **seguro**.
4. Una vez que el navegador tiene el certificado, extrae la clave pública para poder intercambiar mensajes de manera segura con el servidor. Pero no es esta clave la que se va a usar para codificar cada mensaje enviado y decodificar cada mensaje recibido. Sino que ahora que pueden establecer una comunicación, lo que hacen es generar y negociar una 'session key'. Y es esa 'session key' la que se utilizará para cifrar el resto de la comunicación.

DigitalHouse>