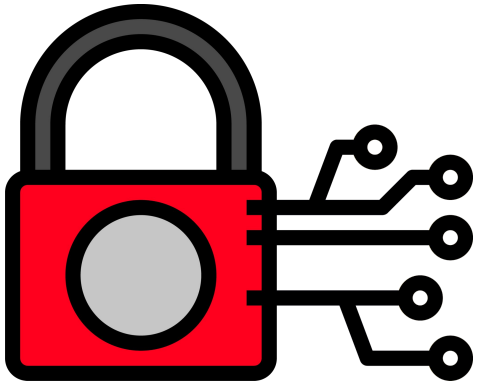
# Usar la criptografía como mecanismo de autenticación

DigitalHouse >
Coding School

Certified Tech Developer
The Ultimate Degree

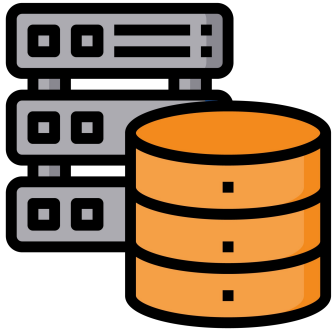
# Usar criptografía simétrica y/o HMAC

Cuando usamos criptografía simétrica para proteger una comunicación o un mecanismo como HMAC para proteger la integridad de los datos estamos utilizando una clave criptográfica que es secreta y solo conocida por las partes involucradas. De este modo, podemos decir que al utilizar comunicaciones encriptadas de forma simétrica (**confidencialidad**), con una clave que es solo conocida por los receptores y emisores (**autenticación**) y sobre la que se monta HMAC (**integridad**) estamos cumpliendo con el principio de seguridad CIA (asegurar la confidencialidad, verificar la integridad y autenticar a las partes).



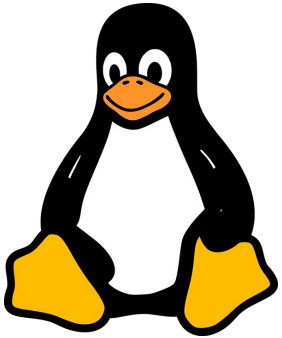
# Usar certificados SSL

Como ya hemos observado, es posible que organizaciones deseen o deban proteger las comunicaciones contra sus sitios (recuerden el ejemplo de un banco y su plataforma de Home Banking). Sabemos que para lograrlo, las compañías deben hacer uso de la criptografía asimétrica, y el mecanismo de distribución para la clave pública son los ya conocidos certificados. Para que los mismos para que sean confiables, deben ser emitidos por una entidad certificante conocida por nuestras computadoras. Caso contrario, nuestros navegadores indican que las claves siendo utilizadas por el sitio del banco no fueron generadas por una entidad confiable. Y para que una entidad confiable genere un certificado en nombre de una compañía, esta debe poder verificar su identidad. De este modo, y por carácter transitivo, podemos decir que los certificados SSL sirven para verificar la identidad de una compañía y así cumplir con el principio de CIA.



# Usar pares de claves asimétricas

En los sistemas **Linux** la manera tradicional de conectarnos de forma remota es utilizando el comando y protocolo SSH (Secure Shell). El administrador debe ingresar el comando `ssh usuario@servidor` en una consola para conectarse a otro servidor. A continuación, se procederá a pedir al usuario que ingrese su contraseña.
Esto quiere decir que en cada servidor al que nos vayamos a conectar tenemos que tener un conjunto de usuario y password. ¿Qué pasa si administramos una cantidad significativa de servidores?
Indefectiblemente vamos a tener que recordar combinaciones de usuario y password por cada uno de ellos.
Linux provee una alternativa: utilizar **claves criptográficas asimétricas** para **autenticarnos**.



# ¿Cómo utilizar pares de claves asimétricas?

| Paso 1: Generación de claves | Paso 2: Distribución de clave pública | Paso 3: Acceder a los servidores |
| --- | --- | --- |
| Un administrador de sistemas utiliza los comandos `ssh-keygen` o `openssl`, esto producirá un par de claves (pública y privada). La clave privada debe ser mantenida en secreto y no debe compartirse con nadie. | El administrador luego distribuye la clave pública a aquellos servidores a los que quiera conectarse utilizando este método. | Una vez distribuida la clave, el administrador solo deberá ejecutar desde la computadora en la que tenemos la clave privada `ssh usuario@servidor` para conectarse sin la necesidad de proveer ningún dato adicional. |


DigitalHouse>
Coding School