sepian

Seguridad Digital
de Andalucía

Charla virtual

# Protección de datos y cifrado de unidades

Fecha de celebración: 27 de noviembre del 2020

Junta de Andalucía

# Introducción a la protección de datos

- Es un derecho fundamental protegido por el artículo 18.4 de la Constitución Española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno.

- En un primer momento no se considera como un derecho independiente, sino que se encuentra vinculado al derecho a la intimidad, al honor personal y familiar y al pleno ejercicio de sus derechos.

# Introducción a la protección de datos

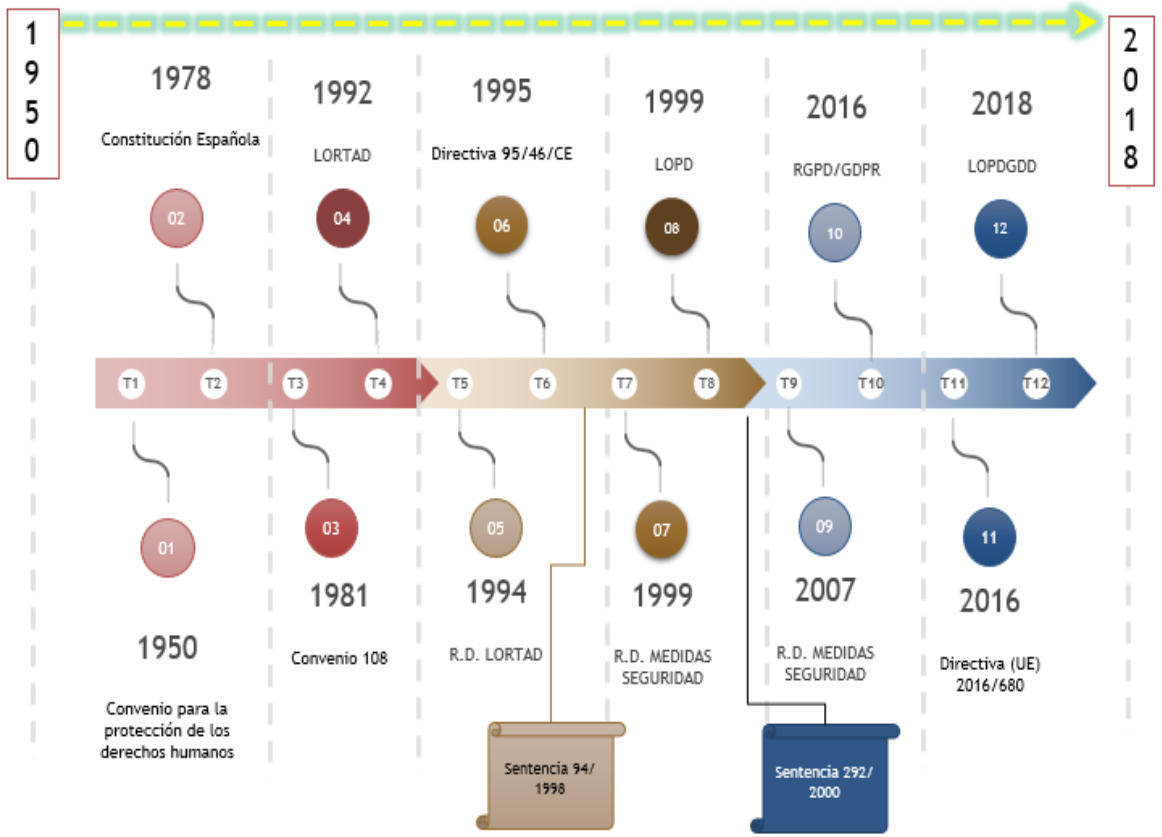
La Constitución Española de 1978 nos dice en su artículo 18 en la Sección 1. ª De los derechos fundamentales y de las libertades públicas:

> *Artículo 18*
> *1. Se garantiza el **derecho al honor, a la intimidad personal** y familiar y a la propia imagen.*
> *2. El **domicilio es inviolable. Ninguna entrada o registro** podrá hacerse en él **sin consentimiento del titular o resolución judicia**l, salvo en caso de flagrante delito.*
> *3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
> *4. La ley **limitará el uso de la informática para garantizar el honor y la intimidad** personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

# Introducción a la protección de datos

En el año 2000 con las Sentencias del Tribunal Constitucional es cuando se reconocía que se trataba de regular un Derecho Fundamental. A partir de entonces es cuando se empezaría a hablar de Autodeterminación Informativa, Habeas Data o Derecho de Protección de Datos como un Derecho Fundamental y Autónomo, cuyo contenido está integrado por los principios y derechos que se contemplan en la Ley Orgánica 15/1999.


# Introducción a la protección de datos



# Introducción a la protección de datos

El Comité Europeo de Protección de Datos considera el cifrado como un elemento de vital importancia para garantizar la privacidad de las comunicaciones y defiende la necesidad de implementar sistemas de cifrado robustos, eficientes y estandarizados para la protección de la privacidad de los ciudadanos europeos.

El Comité establece el cifrado como un elemento necesario e irremplazable para garantizar la privacidad de la comunicación en Internet y que dicha protección ha de implementarse de extremo a extremo, es decir, directamente entre los usuarios finales sin elementos intermedios que tengan acceso a la información.


# Introducción a la protección de datos

El Reglamento (UE) 2016/679, General de Protección de Datos (en adelante, RGPD), en su artículo 25 y bajo el epígrafe 'Protección de datos desde el diseño y por defecto', incorpora a la normativa de protección de datos la práctica de considerar los requisitos de privacidad desde las primeras etapas del diseño de productos y servicios.

El RGPD le otorga la categoría de requisito legal al "principio de integrar las garantías para la protección de los derechos y libertados de los ciudadanos con relación a sus datos personales desde las primeras etapas del desarrollo de sistemas y productos".

# Introducción a la protección de datos

Para integrar la privacidad a lo largo de todas las etapas del tratamiento de datos, se deben analizar detenidamente las distintas operaciones implicadas (recogida, registro, clasificación, conservación, consulta, difusión, limitación, supresión...) e implementar, en cada una de ellas, las medidas más adecuadas para proteger la información y entre lasque cabe considerar:

- La seudonimización temprana o técnicas de anonimización como la k-anonimización.
- Clasificación y organización de los datos y operaciones de tratamiento en base a perfiles de acceso.
- El cifrado por defecto de modo que el estado “natural” de los datos en caso de pérdida o robo sea “ilegible”.
- La destrucción segura y garantizada de la información al final de su ciclo de vida

# Clasificación de la información

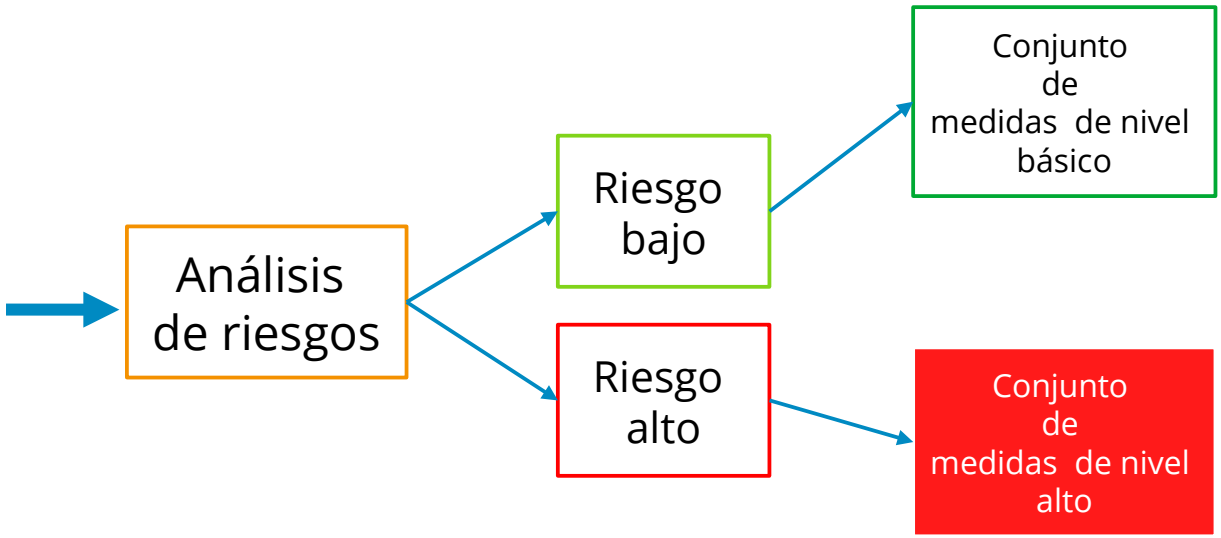
**Clasificar la información** es una medida para garantizar una gestión de seguridad adecuada. Para clasificar la información debemos tener en cuenta algunos criterios como la confidencialidad, la disponibilidad, la integridad, etc.

En la mayoría de las ocasiones ayuda y complementa esta labor valorar la información. Este proceso determina los niveles de seguridad que se deben de aplicar, con los que se establecen unos requisitos básicos.

El **RGPD** establece categorías para su clasificación en la gestión de riesgos.

# Clasificación de la información

**RGPD**
Establecer categorías y asignarlas a los datos para su clasificación.



# Clasificación de la información

**ENS**

La clasificación de la información permite determinar el grado de acceso de los usuarios a la información.

Los niveles de seguridad permiten valorar la información a partir de criterios derivados tanto de requisitos legales, como de aquellos que puede adoptar la organización, para cumplir con los objetivos en relación con la protección de la información.

# Clasificación de la información

**Otras normas**

**ISO 27001:2013** → A.8.2 Clasificación de la información

**Nist 800** → S.PR.AM-5 Clasificación, etiquetado y tratamiento de la información según su nivel de clasificación (valor, sensibilidad y criticidad)

# Clasificación de la información

**Ejemplos**

**Clasificación**

- Pública y Clasificada.
- Interna y Confidencial.
- Sensible y Reservada.
- ...

**Valoración**

- Alta, media y baja
- Crítica, alta, media y baja.
- Grado 0, 1, 2, 3, 4, 5.
- ...

# Gestión de riesgos. El cifrado

Es un elemento básico de **seguridad en la política de seguridad** de la información y, en particular, es una de las garantías adicionales que se pueden emplear para reducir el riesgo en el tratamiento de datos de carácter personal.

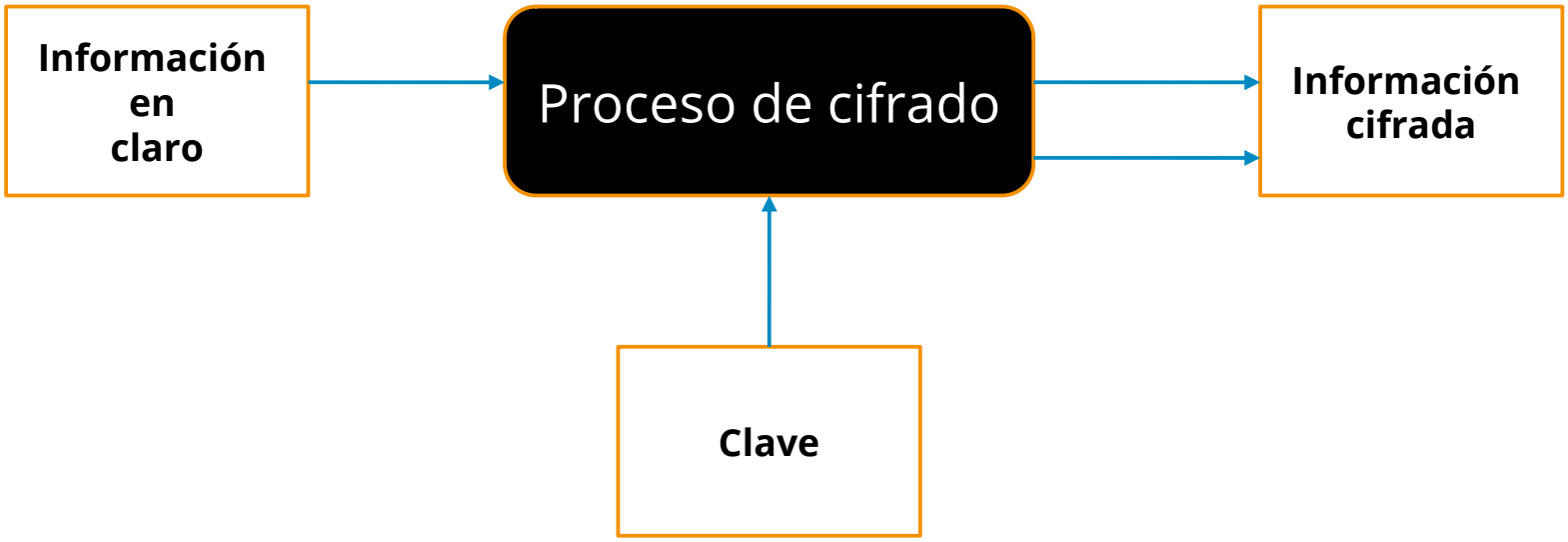
Como un elemento básico para **garantizar la privacidad** de la comunicación ha de implementarse de extremo a extremo, es decir, directamente entre los usuarios finales sin elementos intermedios que tengan acceso a la información.

# Gestión de riesgos. El cifrado

Es un proceso que utiliza un algoritmo con una clave que transforma un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave del algoritmo.

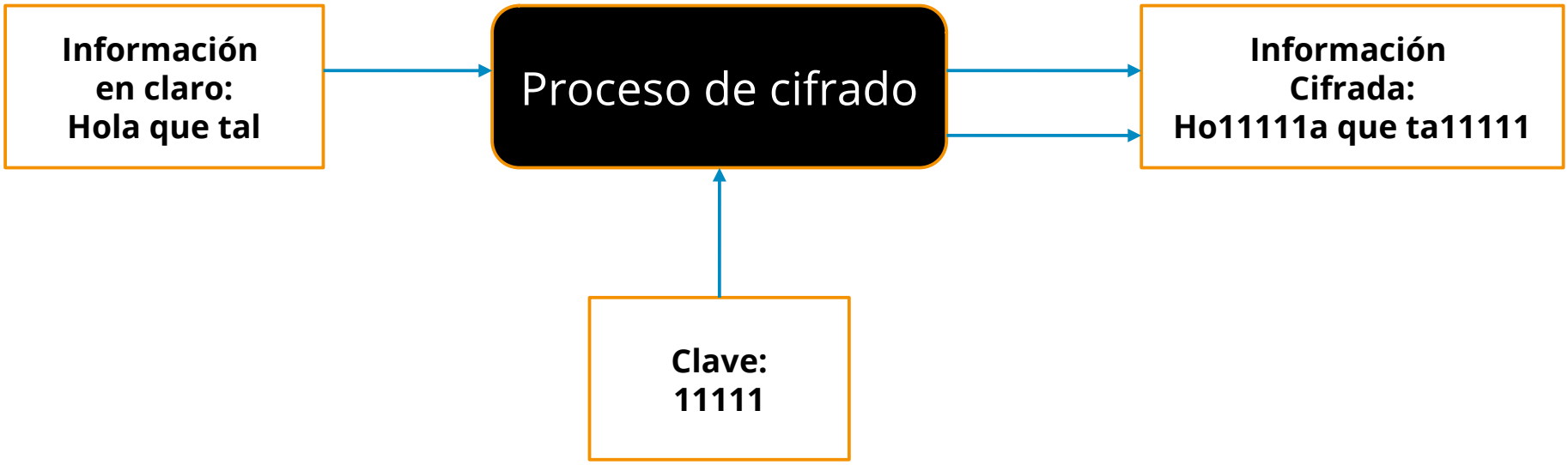
Cifrar una información consiste en transformarla de modo que pase a ser ininteligible para todos salvo para las entidades autorizadas a acceder a dicha información. En general, el acceso a la información original a partir desu versión cifrada se lleva a cabo mediante el uso de claves y algoritmos.

# Gestión de riesgos. El cifrado




*Esquema Básico del proceso de cifrado*

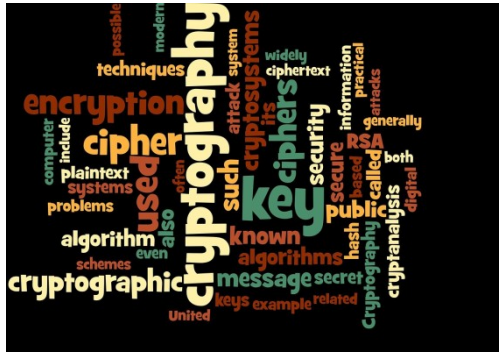
# Gestión de riesgos. El cifrado




*Esquema Básico del proceso de cifrado*

# Introducción a criptografía/ cifrado/ encriptado/ seudonimización/ anonimización

La **criptografía** es la “ciencia“ que se encarga de estudiar las distintas técnicas empleadas para transformar (“encriptar“ o “Cifrar“) la información o hacerla irreconocible a todos aquellos usuarios no autorizados de un sistema de información, de modo que solo el personal autorizado pueda “tratar“ la información.



# Introducción a criptografía/ cifrado/ encriptado/ seudonimización/ anonimización

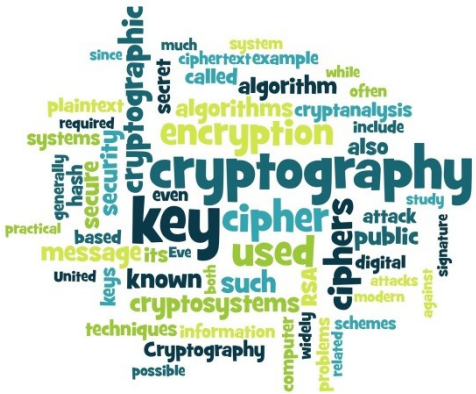
Mediante la criptografía es posible mitigar los riesgos referentes a la confidencialidad, la integridad y la autenticidad de la información.

- **Confidencialidad**: es una de la dimensiones de la seguridad, que se refiere a que la información llegue solamente a las personas autorizadas.
- **Integridad**: es una de las dimensiones de seguridad, que se refiere a que la información mantenga las características de completitud y corrección de los datos. Sin la integridad la información puede aparecer manipulada, corrupta o incompleta.
- **Autenticidad**: es una de las dimensiones derivadas o característica que consiste en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

# Introducción a criptografía/ cifrado/ encriptado/ seudonimización/ anonimización

**Cifrado y Encriptado**: Algunos autores consideran más correcto el término cifrar en lugar de encriptar, si bien en la práctica es habitual encontrar cualquiera de los dos términos en los libros y artículos sobre criptografía.

Referencia: https://dle.rae.es/encriptar



# Introducción a criptografía/ cifrado/ encriptado/ seudonimización/ anonimización

**Seudonimización**: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

**En resumen: cifrado reversible.**

# Introducción a criptografía/ cifrado/ encriptado/ seudonimización/ anonimización

**Anonimización:** proceso al que se somete a los datos personales para eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de los mismos, es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleva una distorsión de los datos reales.

**En resumen: cifrado no reversible en la medida de lo posible.**

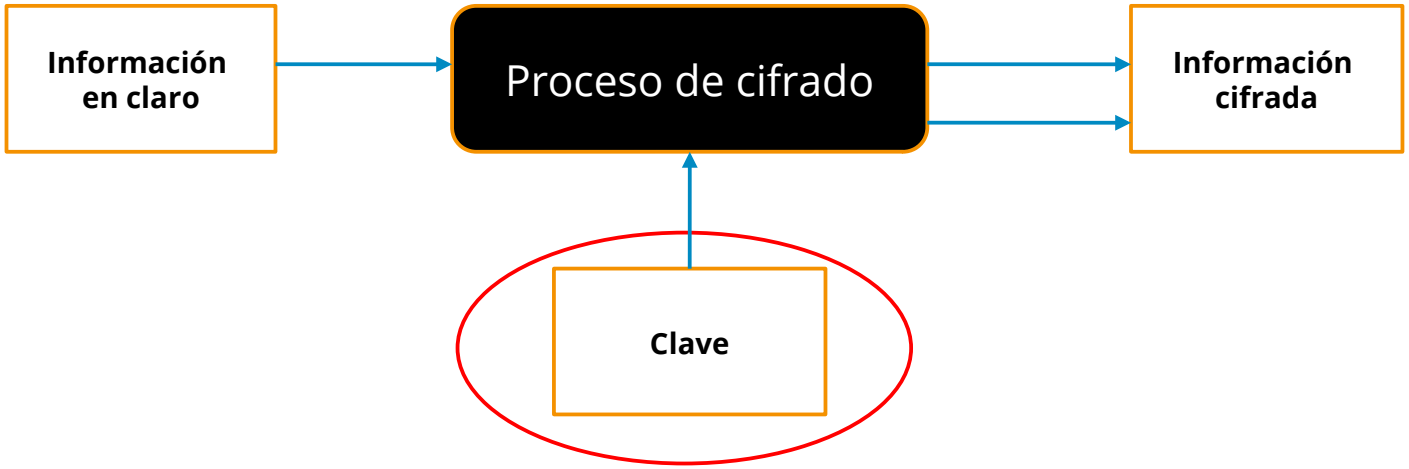
# Introducción a criptografía/ cifrado/ encriptado/ seudonimización/ anonimización

**K-Anonimización:** es una propiedad de los datos anonimizados que permite cuantificar hasta qué punto se preserva la anonimización de los sujetos presentes en un conjunto de datos en el que se han eliminado los identificadores. Dicho de otro modo, es una medida del riesgo de que agentes externos puedan obtener información de carácter personal a partir de datos anonimizados.

**Función HASH:** un proceso que transforma cualquier conjunto arbitrario de datos en una nueva serie de caracteres con una longitud fija, independientemente del tamaño de los datos de entrada.

# Sistemas criptográficos

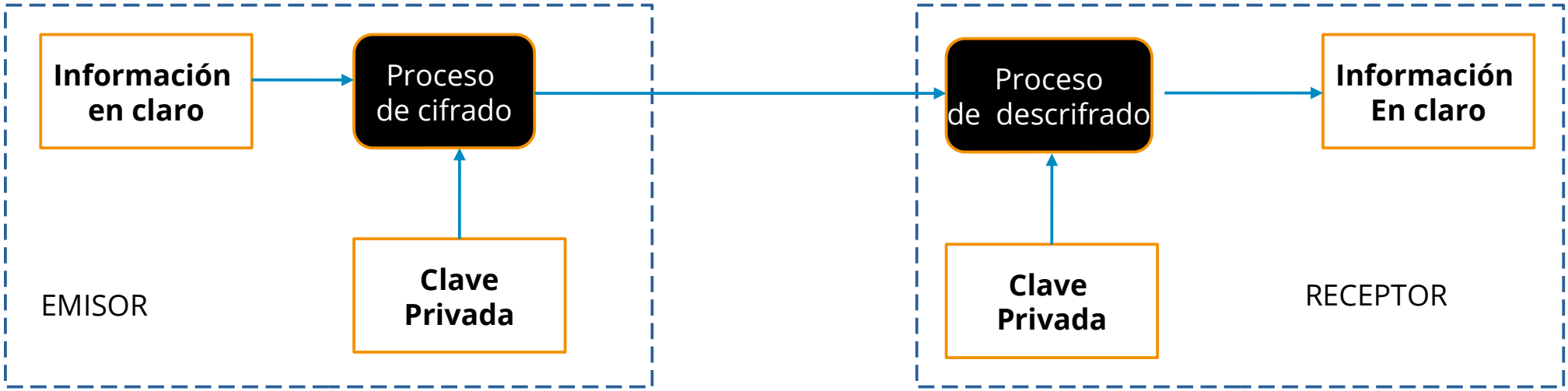
Hemos visto en el esquema fundamental del proceso de cifrado que intervienen la información, el proceso de cifrado, una clave y el mensaje cifrado.  A continuación veremos como en base a esa clave existen dos tipos de sistemas criptográficos Simétricos y Asimétricos.




*Esquema Básico del proceso de cifrado*

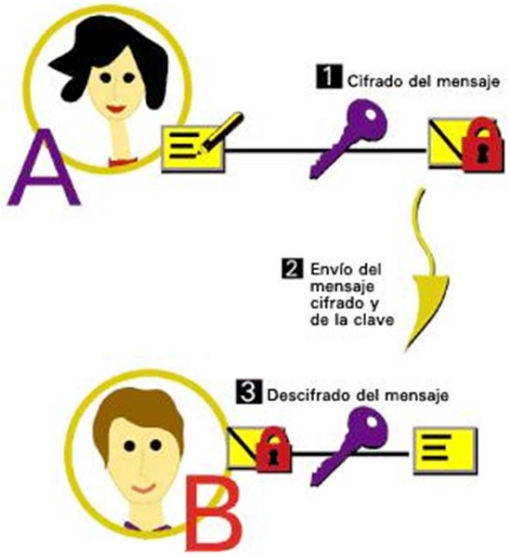
# Sistemas criptográficos simétricos

En los sistemas de cifrado simétrico la clave utilizada es la misma tanto para cifrar como para descifrar. En este caso la clave se denomina **clave privada**.



# Sistemas criptográficos simétricos

Cuando el emisor y el receptor son distintos, deben llegar a un acuerdo para compartir la clave. Una recomendación es que si deben compartir la clave, no sea por el mismo medio, ni en el mismo momento.



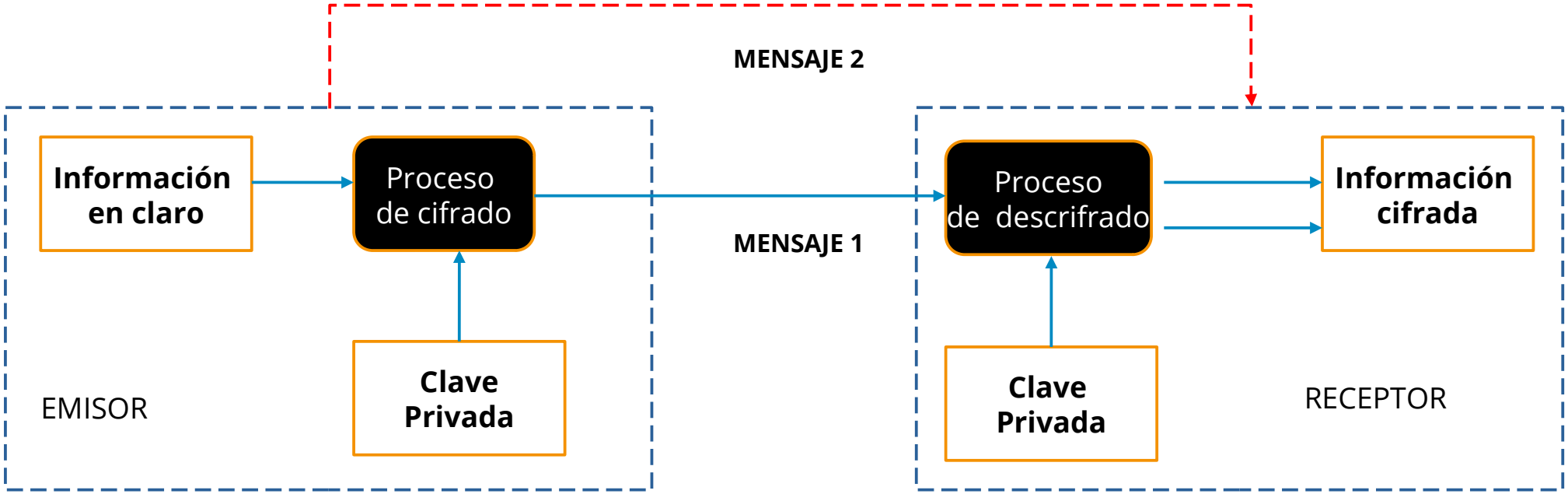

*Ejemplo*:

*Si envío información cifrada mediante correo electrónico, y el receptor no conoce la clave privada, se puede contactar vía telefónica para facilitarle la clave, pudiendo verificar la identidad del receptor y confirmar la recepción del mensaje.*

Si no podemos utilizar un segundo medio, enviar la clave en un segundo mensaje.

**¿De qué serviría enviar un fichero de cifrado si lo acompaño con la clave para descifrarlo?**

# Sistemas criptográficos simétricos



# Sistemas criptográficos simétricos

Entre los algoritmos simétricos más utilizados hoy en día podemos encontrar:

- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- RC2, RC4, RC5...
- BlowFish.
- SKIPJACK
- CAST
- GOST
- AES (Advanced Encryption Standard)

# Sistemas criptográficos simétricos

El cifrado simétrico es muy usado por los sistemas para tareas como cifrar archivos, particiones, cifrar completamente dispositivos (USB´S), ordenadores usando el cifrado de disco completo, bases de datos como las de administradores de contraseñas. Para descifrar esta información cifrada simétricamente, a menudo se pide una contraseña para poder descifrarlo.


# Sistemas criptográficos simétricos

El **cifrado simétrico** esconde **un problema** que reside sobre todo en **el intercambio de las claves:** como el destinatario debe conocer la clave, cuantos más participantes en la comunicación compartan una clave, más inseguro y vulnerable se vuelve el intercambio.

**Es decir, mayor riesgo.**


**El cifrado asimétrico** es una alternativa muy práctica a este método, ya que cada **usuario tiene su propio par de claves** La clave pública (que conocen todos los usuarios) y su clave privada (que solo conoce el usuario que descifra) .

# Sistemas criptográficos asimétricos

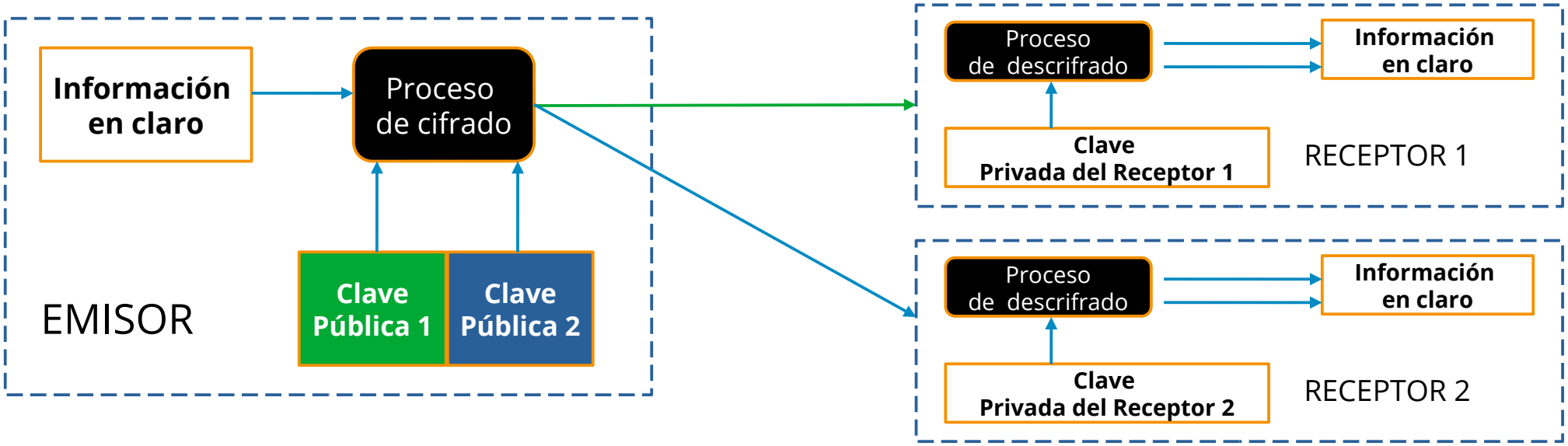
En los sistemas de cifrado Asimétrico se generan **dos claves que se encuentran relacionadas** por un algoritmo. Este algoritmo, por lo general suele ser un proceso donde están involucrados un conjunto de complejas operaciones matemáticas.

Una de estas claves se denomina **clave pública**, que tiene por objeto ser la clave que utilicen los usuarios del sistema **para cifrar la información.**

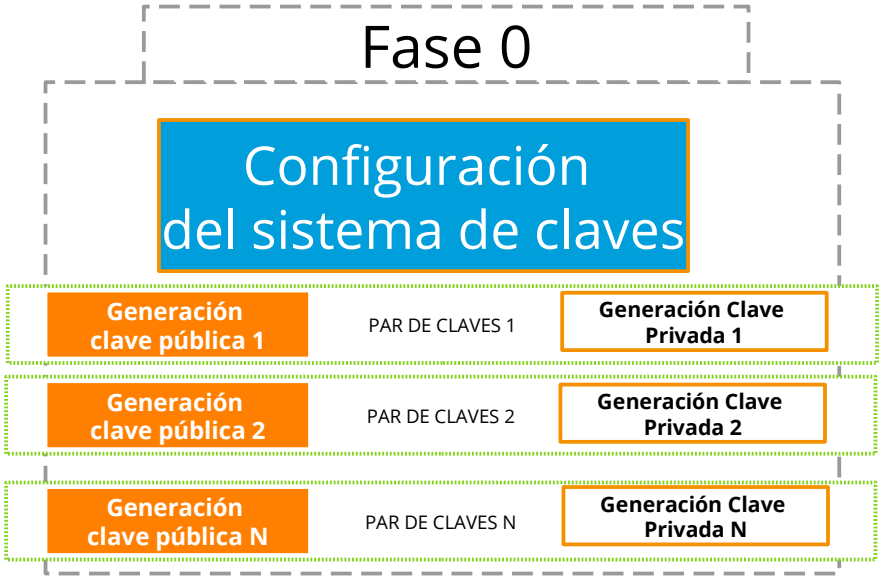
La segunda clave se denomina **clave privada**, cada usuario tiene una clave privada **para descifrar el mensaje.**

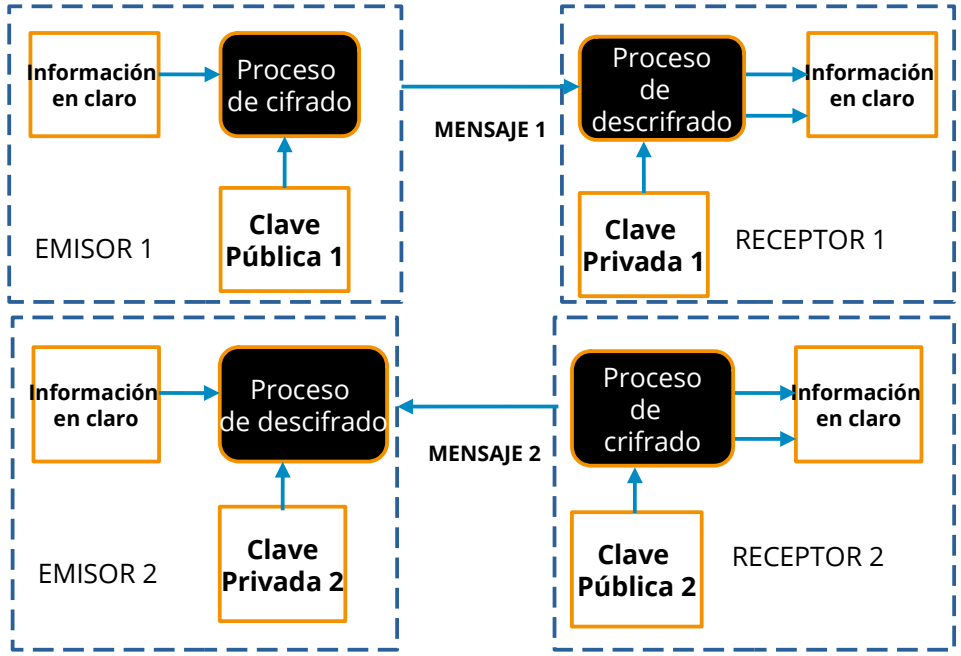
# Sistemas criptográficos asimétricos

En los sistemas de cifrado Asimétrico la clave utilizada es distinta para cifrar y  para descifrar. En este caso existe la clave **pública** y la clave **privada**.

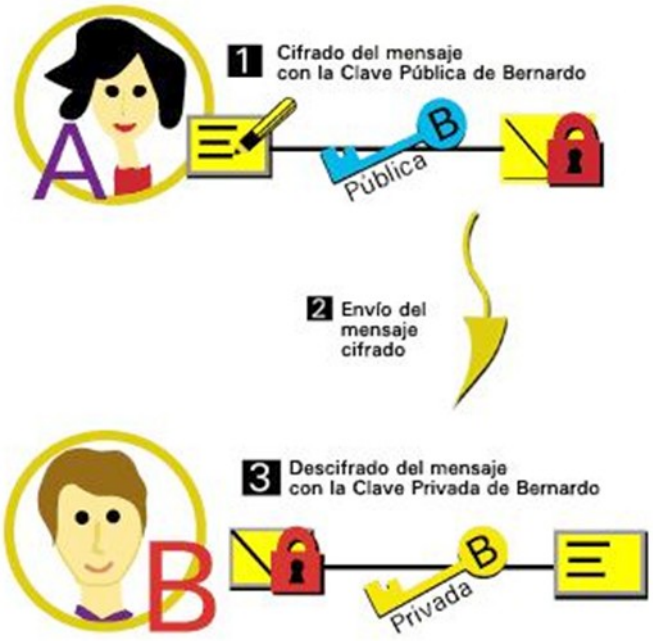


# Sistemas criptográficos asimétricos



# Sistemas criptográficos asimétricos


**Cada usuario tendrá un par de claves (**clave pública y clave privada).
No sólo protegemos la **confidencialidad** del mensaje, también su **autenticidad**, siempre sabremos que el mensaje proviene de la persona que tenía que enviarlo

# Sistemas criptográficos asimétricos

1. Diffie-Hellman
2. ElGamal
3. RSA (Rivest- Shamir-Adleman)
4. DSA (Digital Signature Algorithm)
5. Funciones Hash
6. Curvas Elípticas
7. Criptografía Cuántica

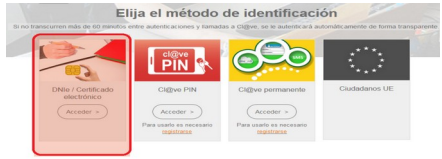
# Sistemas criptográficos asimétricos

El cifrado asimétrico es muy usado para los certificados digitales (usan una clave pública y una clave privada, fueron diseñados para poder intercambiar información de manera segura sin necesidad de haber acordado previamente una clave secreta de cifrado. En efecto todo mensaje cifrado con la clave pública de un usuario sólo puede ser descifrado con la clave privada que el usuario mantiene segura).

**Cifrar comunicaciones.**


**Firmar mensajes y documentos.**

**Identificación ante un sistema o autenticación de usuarios.**



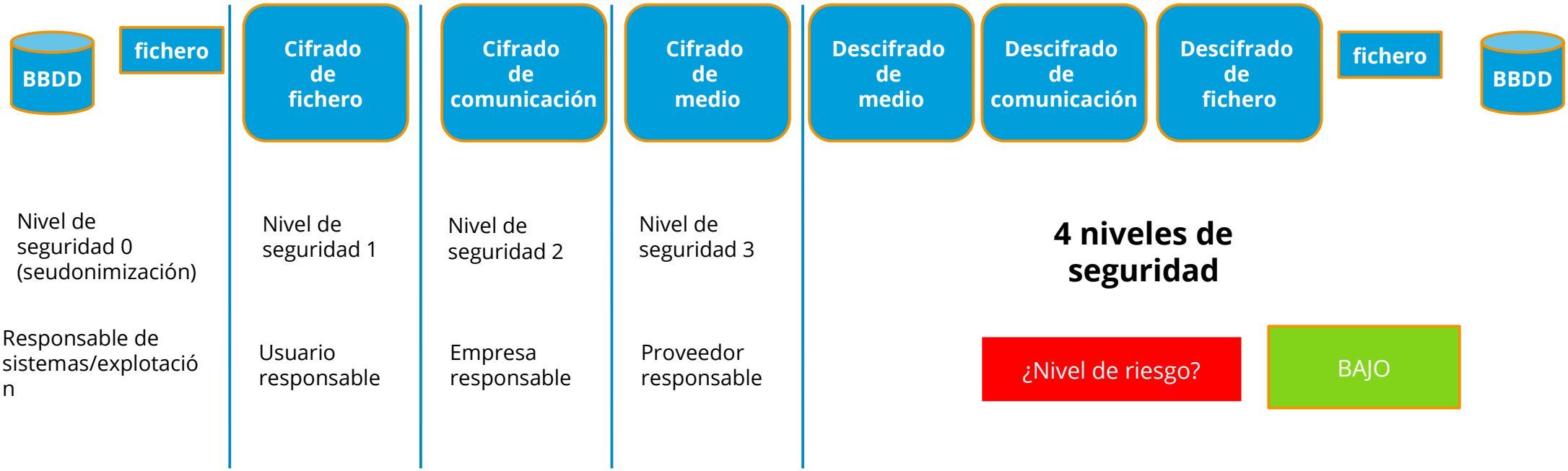
# Sistemas criptográficos vs

| Cifrado simétrico | Cifrado asimétrico |
|---|---|
| Rápido | Lento |
| No requiere una PC poderosa | Requiere una gran capacidad de cómputo |
| Útil para cifrar mensajes grandes y pequeños | Útil para mensajes pequeños |
| Requiere que se comparta la llave para el cifrado y descifrado | No es necesario compartir la clave de descifrado, sólo se comparte la "clave pública" para el cifrado. |
| **No se puede usar para verificar identidades (autenticación)** | **Puede ser usado para la verificación de identidad (autenticación)** |

# Responsabilidad de cifrar

| | |
|---|---|
| La entidad A (Emisor) | Debe implementar protocolos como el https o el ftps, que cifra la información en el canal. |
| La entidad B (Receptor) | Al responder debe continuar con los protocolos de seguridad y exigirlos al emisor. |
| El usuario A (Emisor) | Cifrado de ficheros, el usuario debe saber cifrar su información (cifrar pdf´s, ficheros, el disco externo, incluso el propio disco duro, etc). |
| El usuario B (Receptor) | Cifrado de ficheros, el usuario debe saber cifrar su información y aceptar que este cifrada. (cifrar pdf´s, ficheros, el disco externo, incluso el propio disco duro, etc. Y exigirlo al emisor.) |
| La empresa que facilitan las comunicaciones | Se debe exigir la posibilidad de conexiones/medios cifrados (medio de transmisión) |

# Responsabilidad de cifrar



# Responsabilidad de cifrar

- **SIMÉTRICO**
  - BITLOCKER
  - ZIP/WINZIP
  - VERACRYT
- **ASIMÉTRICO**
  - PRETTY GOOD PRIVACY, PGP (CORREOS ELECTRÓNICOS)
  - SSL/TLS*
  - HTTPS

# Responsabilidad de cifrar


**SIMÉTRICO**
**BITLOCKER**

Permite mantener a salvo todo, desde documentos hasta contraseñas, ya que cifra toda la unidad en la que Windows y sus datos residen (todo el disco duro). Una vez que se activa BitLocker, se cifran automáticamente todos los archivos almacenados en la unidad.

El mejor tipo de medidas de seguridad son transparentes para el usuario durante su implementación y uso. Cada vez que haya un posible retraso o dificultad debido a una característica de seguridad, hay una alta probabilidad de que los usuarios intenten omitir la seguridad. Esta situación es especialmente cierta en el caso de la protección de datos y es un escenario que las organizaciones deben evitar. Ya sea que desee cifrar volúmenes completos, dispositivos extraibles o archivos individuales

# Responsabilidad de cifrar

**SIMÉTRICO**

**ZIP (windows)** 

El sistema operativo de Windows 10 (Microsoft Windows 10 Pro, Education y Enterprise, aunque no con Microsoft Windows 10 Home) integra una función para cifrar archivos y carpetas de archivos. Es decir, sin que sea necesario recurrir a software de terceros es posible asignar una contraseña a un archivo ZIP para impedir el acceso no autorizado.

**WINZIP (terceros)** 


Es ideal para comprimir archivos y carpetas, pero también es un medio excelente para cifrar datos confidenciales. Es una herramienta de seguridad muy útil para el usuario no técnico que necesita enviar datos confidenciales por correo electrónico a través de Internet.

# Responsabilidad de cifrar

**SIMÉTRICO**

**VERACRYPT**

Es una herramienta de código abierto, por lo que no tendremos que pagar ninguna licencia para poder utilizarla y además es multiplataforma, lo que significa que podremos utilizarla en sistemas operativos “Windows, Linux o Mac“

# Responsabilidad de cifrar

**ASIMÉTRICO**

**Pretty Good Privacy, PGP (Correos electrónicos)**

Es una herramienta que ayuda a proteger nuestra privacidad, que las comunicaciones estén seguras, garantiza la autenticidad de los mensajes electrónicos que enviamos. Podemos cifrar cualquier tipo de información personal (emails, archivos o el disco duro entero), siendo difícil para un atacante, intentar leer información. También proporciona la opción de “firma digital” para enviar mensajes que serán verificados por el destinatario.

La clave pública puede ser exportada a un fichero o cargada en un servidor de claves para poderla compartir con otras personas.

# Responsabilidad de cifrar

**ASIMÉTRICO**


**HTTPS**

El protocolo HTTPS (Hyper Text Transfer Protocol Secure). En sí mismo HTTPS es el protocolo HTTP sobre SSL/TLS. Como se encuentra sobre SSL/TLS, que funciona en la capa más baja de comunicación, **se cifran todos los datos de HTTP.** No sólo la página web sino también **la dirección web completa, los parámetros enviados, las cookies...** Lo único que se queda al descubierto son los datos del paquete TCP (el servidor y el puerto al que se conecta).

HTTPS impide que alguien vea las páginas web que estamos visitando, impide que puedan conocer las direcciones web por las que nos movemos, los parámetros que enviamos al servidor (por ejemplo, los usuarios y contraseñas se envían como parámetros POST normalmente) o las cookies que enviamos y recibimos (alguien con acceso a estas cookies podría robar nuestra sesión, como demostraba la herramienta Firesheep).

# Responsabilidad de cifrar

**ASIMÉTRICO**


**SSL/TLS**

Combina los métodos asimétrico y simétrico. La clave pública está firmada por un organismo de certificación, y el certificado resultante, a su vez, está encriptado. El certificado solo puede abrirse utilizando la clave pública del organismo de certificación. Para este fin, el servidor web envía, por ejemplo, su clave pública certificada al navegador, que verifica el certificado. Si este es válido, el navegador genera una clave simétrica y la envía al servidor web. Ambos ahora utilizarán esta clave común durante el resto de la sesión SSL/TLS para cifrar simétricamente su tráfico de datos.

# Responsabilidad de cifrar

**ASIMÉTRICO**


**SSL/TLS**

Combina los métodos asimétrico y simétrico. La clave pública está firmada por un organismo de certificación, y el certificado resultante, a su vez, está encriptado. El certificado solo puede abrirse utilizando la clave pública del organismo de certificación. Para este fin, el servidor web envía, por ejemplo, su clave pública certificada al navegador, que verifica el certificado. Si este es válido, el navegador genera una clave simétrica y la envía al servidor web. Ambos ahora utilizarán esta clave común durante el resto de la sesión SSL/TLS para cifrar simétricamente su tráfico de datos.

sedian Seguridad Digital de Andalucía