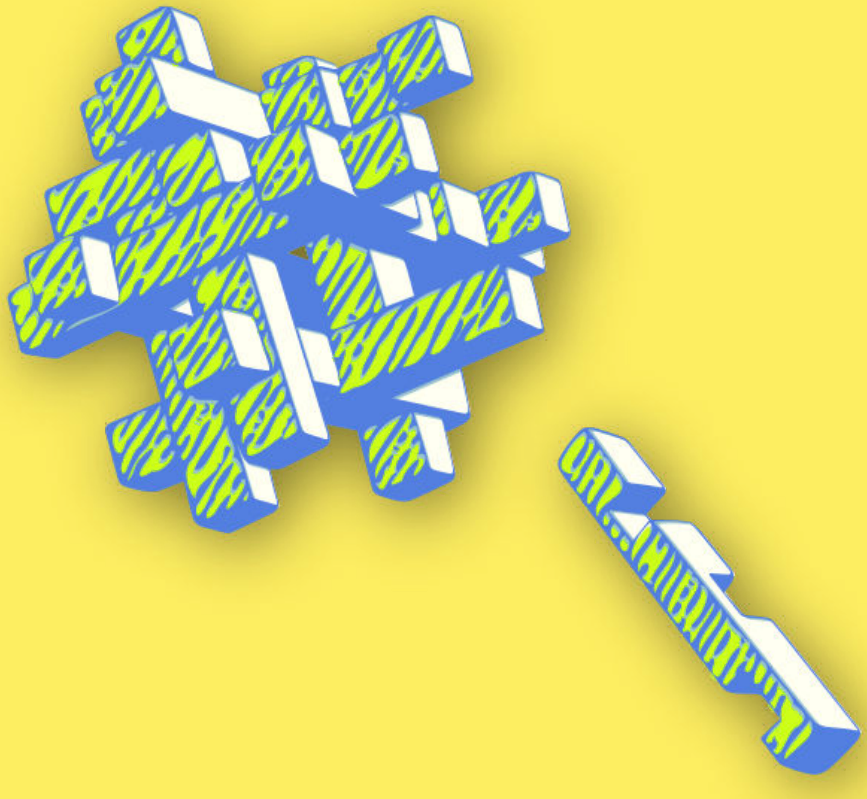
CIBERMUJERES



# Cifrado

# Cifrado




https://iwpr.net/

# Índice general

# Introducción al cifrado

- **Objetivos:** Explicar el concepto de cifrado, repaso breve de diferentes tipos de cifrado.
- **Duración:** 50 minutos
- **Formato:** Sesión
- **Habilidades:** Intermedio
- **Conocimientos requeridos:**
  - Conceptos básicos de seguridad digital y/o capacitación previa.
- **Sesiones y ejercicios relacionados:**
  - Privacidad[1]
  - Campañas online más seguras[2]
  - Comunicaciones cifradas[3]
  - Almacenamiento y cifrado[4]
- **Materiales requeridos:**
  - Diapositivas (con los puntos claves descritos a continuación)

[1] https://cyber-women.com/es/privacidad/privacidad/

[2] https://cyber-women.com/es/activismo-online-más-seguro/campañas-online-más-seguras/

[3] https://cyber-women.com/es/cifrado/comunicaciones-cifradas/

[4] https://cyber-women.com/es/principios-básicos-de-seguridad-digital-2/almacenamiento-y-cifrado/

  - Computadora y proyector configurados
- **Recomendaciones:** Este infográfico puede ser útil: https://emailselfdefense.fsf.org/es/infographic.html

# Conducir la sesión

## Parte 1 - ¿Alguna vez has cifrado?

1. Aclara que esta sesión es una introducción al cifrado, así que no van a profundizar sobre herramientas de cifrado que las participantes pueden ya haber escuchado (como GnuPG).
2. Divida las participantes en parejas y arranca la sesión mostrando algunos ejemplos de técnicas de cifrado. Prepara estos ejemplos de antemano.

#### El código BLUEPRINTS

Cada una de las letras de la palabra "blueprint" tiene un número asignado.

```
R  E  F  E  R  E  N  C  I  A
0  1  2  3  4  5  6  7  8  9
```

Aunque este ejemplo se basa en una palabra determinada, puede aplicarse a cualquier secuencia de letras y palabras. Por ejemplo, si usas el mismo sistema que el de arriba, la secuencia de números 82579 deletrea la palabra TURNS cuando se descifra.

También puedes cambiar el orden de los números, de tal manera que quedaría así:

```
R  E  F  E  R  E  N  C  I  A
9  8  7  6  5  4  3  2  1  0
```

En este ejemplo, la secuencia de números 82579 ahora deletrea ECRFR (que no es una palabra) cuando se descifra; sin embargo, podrías "descifrar"

la secuencia 903210 como RANCIA.

**Mensajería de texto a la antigua**

Utiliza una imagen de un teclado (véase abajo) para demostrar otro tipo de "cifrado" con las que se puedan familiarizar las participantes.


Old-Fashioned Text Messaging

Pregúntales cómo utilizarían ese teclado para deletrear diferentes palabras, por ej, sus nombres. El nombre Luisa se deletrearía con la secuencia 5 5 5 8 8 4 4 4 7 7 7 7

3. Pregunta si han usado otros tipos de cifrado, parecidos a los ejemplos de antes o cualquier otro tipo que se les ocurra (ej. usar conexión HTTPS).

4. Cierra la sesión planteando otra pregunta: ¿Cuáles son los elementos comunes con los que se pueden identificar a partir de estos diferentes ejemplos de cifrado?
5. Toma en cuenta que algunos servicios de correo electrónico como Gmail tienen que ser configurados para permitir el uso de Thunderbird como aplicación de terceros.

## Parte 2 - Explicar el cifrado

6. Basándote en los elementos que salieron en la parte 1, amplía sobre los principios y prácticas básicas:

   **Métodos de cifrado:** dedica tiempo a explicar cómo funciona el cifrado, refiriéndote a ejemplos de la parte 1 y mostrando capturas de pantalla sobre el aspecto que tiene un correo cifrado con GnuPG. Destaca implementaciones conocidas de cifrado, en particular, repasa con tiempo el HTTPS, el cifrado punta a punta y el cifrado GPG/PGP.

   **Llaves y pares de llaves:** explica cómo funcionan los pares de llaves y la relación algorítmica entre llaves públicas y privadas. Vuelve a repasar los ejemplos de implementaciones comentados anteriormente (HTTPS, el cifrado de punta a punta y el cifrado GPG/PGP) y explica, en cada caso, dónde se almacenan las llaves y cómo visualizarlas.

   **Prácticas de cifrado:** destaca buenas prácticas clave asociadas a las implementaciones conocidas de cifrado como el verificado de huella y la firma de llaves. A modo de demostración, pide a las participantes localizar en Signal la opción de verificado de huella de usuaria; de la misma manera, si las participantes ya tienen llaves GPG/PGP, pueden discutir las ventajas y desventajas de firmar y distribuir llaves públicas. Aprovecha para discutir la mensajería cifrada punta a punta para apps de mensajería instantánea como Signal, Telegram y Whatsapp. Aclara que el cifrado de punta a punta en algunos servicios no está habilitado por defecto.

**Respaldos cifrados:** partiendo del ejemplo de GPG/PGP de arriba, pregunta si piensan que es buena idea realizar un respaldo de su llave privada GPG y si es sí, ¿cómo lo harían?

## Referencias


- https://www.gnupg.org/gph/es/manual/book1.html

# Comunicaciones cifradas

- **Objetivos:** Partiendo de los contenidos formativos anteriores sobre cifrado, en esta sesión se transmite la importancia y utilidad de cifrar comunicaciones y se brindan herramientas relevantes.
- **Duración:** 50 minutos
- **Formato:** Sesión
- **Habilidades:** Intermedio
- **Conocimientos requeridos:**
  - Conceptos básicos de seguridad digital y/o capacitación previa.
  - Introducción al cifrado[1]
- **Sesiones y ejercicios relacionados:**
  - Introducción al cifrado[2]
  - Privacidad[3]
  - Campañas online más seguras[4]
- **Materiales requeridos:**
  - Diapositivas (con los puntos claves descritos a continuación)

[1] https://cyber-women.com/es/cifrado/introducción-al-cifrado/

[2] https://cyber-women.com/es/cifrado/introducción-al-cifrado/

[3] https://cyber-women.com/es/privacidad/privacidad/

[4] https://cyber-women.com/es/activismo-online-más-seguro/campañas-online-más-seguras/

- Computadora y proyector configurados

## Conducir la sesión

1. Comparte ejemplos relevantes de situaciones donde la comunicación cifrada es útil y dedica tiempo a explicar cómo funciona el cifrado. Muestra capturas de pantalla de correos cifrados con GPG para ilustrar por encima qué aspecto tienen los mensajes y correos cuando están cifrados. También destaca implementaciones conocidas de cifrado
    - en particular, HTTPS, cifrado de punta a punta y cifrado GPG/PGP.
2. Centra la discusión en herramientas que permiten cifrar comunicaciones. Ejemplos buenos son: Signal para llamadas y mensajes, meet.jit.si para llamadas de video, Tutanota o GPG+Thunderbird para correos.
3. Explica los beneficios a nivel de seguridad de estas herramientas, sobre todo, cómo permiten a las usuarias limitar el acceso que otras personas tienen sobre sus comunicaciones; después discute situaciones donde la seguridad de los datos de la usuaria podrían ser comprometidas, aún estando cifradas. Pregunta: ¿cómo podría comprometerse un correo cifrado con GPG a través de registradores de teclas o malware que captura la pantalla? ¿Y si un/a adversario/a consigue nuestra llave privada de GPG? ¿Cómo podrían acceder a nuestros datos?
4. Si tienen tiempo, pónganse manos a la obra con al menos dos de las herramientas comentadas en el paso 2. Aunque no tengan tiempo para repasar GPG/PGP para email, pueden optar por mostrar cómo hacer llamadas de video cifradas vía HTTPS a través de meet.jit.si o instalar Signal en los celulares para practicar enviar mensajes cifrados entre sí o realizar llamadas cifradas.

## Referencias

- https://ssd.eff.org/es/module/c%C3%B3mo-utilizar-signal-en-ios