# Privacidad, seguridad y anonimato

Miguel García Martín

Foo-Manroot

https://foo-manroot.github.io/

Foo_Manroot

# Necesidad de seguridad en los Sistemas de Información

- CIA:
  - Confidencialidad
  - Integridad
  - Disponibilidad (availability)

  } Definido en ISO 27000

- Programas de vigilancia:
  - PRISM (EE.UU.): desvelado por E. Snowden en 2013.
  - Data Retention Directive (U.E.): Los datos de telecomunicacions se deben retener de 6 a 24 meses por si se requieren, por orden judicial.
  - Facebook, Google, Microsoft, Apple… siguen las leyes de EE.UU. (al menos cuando les conviene → *PRISM* vs *San Bernardino*).

- Las empresas venden y compran información personal:
  - En los ToS se suele especificar que se permite a la empresa ceder datos a terceros “para una experiencia adecuada”
- Criminales comunes:
  - *Phising*, *malware*…
  - Ataques muy sencillos. Mayor amenaza que los agentes estatales

**Apps, websites and third-party integrations on or using our Services.**
When you use third-party apps, websites or other services that use, or are integrated with, our Services, they may receive information about what you post or share. For example, when you play a game with your Facebook friends or use the Facebook Comment or Share button on a website, the game developer or website may get information about your activities in the game or receive a comment or link that you share from their website on Facebook. In addition, when you download or use such third-party services, they can access your Public Profile, which includes your username or user ID, your age range and country/language, your list of friends, as well as any information that you share with them. Information collected by these apps, websites or integrated services is subject to their own terms and policies.

Learn more about how you can control the information about you that you or others share with these apps and websites.

**Sharing within Facebook companies.**
We share information we have about you within the family of companies that are part of Facebook. Learn more about our companies.

**New owner.**
If the ownership or control of all or part of our Services or their assets changes, we may transfer your information to the new owner.

ToS de Facebook

No existe la seguridad perfecta, pero se puede minimizar el riesgo.
Tampoco se pueden aplicar las políticas con efecto retroactivo → Tras una brecha, ya no se puede hacer nada

# Algunas definiciones necesarias

- *Software*
  - *Software* libre
- VPN
- Privacidad ≠ anonimato
- Cifrado
  - Estándar OpenPGP

# Seguridad individual

# Buenas prácticas

- El objetivo es minimizar la superficie de exposición.
- Mantener el software actualizado.
- Usar HTTPS:

  - Disponible en ~41% de las páginas
  - Garantiza confidencialidad (aunque el ISP sigue pudiendo ver el tráfico), integridad y autenticidad
  - Importante revisar el certificado (muy sencillo)
- Cifrado completo de disco:
  - Sencillo y transparente
  - Garantiza la confidencialidad si el sistema se ve comprometido físicamente (robado, requisado por orden judicial…)
  - Herramienta para cifrar el disco: VeraCrypt

- Contraseñas (sin olvidar 2FA):
  - Una diferente para cada sitio
  - Usar frases o varias palabras seguidas
  - Facilitado con un administrador de contraseñas:
    - Sólo hace falta recordar una contraseña maestra
    - Hay muchas opciones (*open-source*):
      - Keepass (muy popular, con multitud de *plugins*)
      - Gnome password manager
      - (…)
      - Incluso se puede usar un fichero cifrado con GPG (manejado con cuidado)
      - Es muy importante disponer del código del administrador para poder verificarlo

- Teléfonos móviles (sobre todo Android):
  - Apagar wi-fi cuando se esté fuera de rango
  - Evitar al máximo Google Apps (Gmail, Drive, Calendario…):
    - Lo mínimo necesario para mantener la funcionalidad es el núcleo (sistema base, instalador, Play Store...)
    - Es preferible usar OpenGAapps (*open-source*… más o menos):
      - Se pueden encontrar algunas partes del código original de Google en sus repositorios
      - También existe MicroG; pero puede haber problemas de seguridad (suplantación de Gapps, el pequeño *hack* usado para que funcione) o de experiencia de uso
    - Algunas alternativas *open-source* se pueden encontrar en F-Droid + Yalp (interfaz con Google Play)
  - Desactivar GPS (la mayor parte del tiempo no es necesario)
  - Controlar permisos:
    - Granularidad de permisos (globales, por aplicación…)
    - Si una aplicación pide muchos permisos, sospechar...
    - Si una aplicación pide permisos que no parecen necesarios, sospechar…
  - Hay que recordar que Android está desarrollado por Google
    - S.O. alternativo (si está disponible): LineageOS → *Software* libre

- Cuidar imagen:
  - Perfiles en Twitter, Instagram, Facebook...
    - OSINT *(Open Source INTelligence):*
      - Si un perfil es público, millones de personas (y *bots*) pueden acceder a la información (descargar fotos, controlar actividad…)
    - Hacer las cuentas privadas
    - Controlar la información que se proporciona (por ejemplo, no mostrar las llaves en una foto)
    - *Si un producto es gratis, el producto eres tú*:
      - Las empresas venden los datos (hábitos de uso, perfil demográfico…) y relacionan cuentas de diferentes servicios (Facebook y Whatsapp, por ejemplo)
      - Se pueden usar servicios como 10minutemail para ayudar a evitar esto
  - Bloquear cámaras cuando no se usen

- Usar *software* libre:
  - Se puede verificar que se respeta el derecho a la privacidad
  - Mozilla Firefox:
    - Funcionalidades y rendimiento similares a Google Chrome (desarrollado por Google), con un largo historial de lucha por un internet libre.
      - Curiosidad: en Firefox para Android, se puede apagar la pantalla mientras se ve un vídeo en YouTube (Chrome no lo adopta porque son productos de Google).
  - GNU/Linux:

    - Distribuciones amigables (Ubuntu, Fedora, Mint…)
    - Mayor control sobre el equipo
    - No es necesaria experiencia en administración de sistemas (*la terminal*).
  - Mensajería: Signal, Keybase, Protonmail...
  - En su defecto, *software* que exprese el respeto de la privacidad:
    - Buscadores: DuckDuckGo o Ixquick (el recomendado por la UE)
    - No hay otra alternativa más que confiar en estos servicios

# Modo paranoia (justificada)

- Al navegar por internet:
  - Activar protección contra rastreo
  - Desactivar JavaScript
  - No usar tecnologías antiguas (Flash, applets de Java…) → HTML5 resolvió las necesidades de aplicaciones interactivas hace mucho tiempo
  - Rechazar cookies. Se usa más JS para el rastreo y las analíticas. Las cookies que se usan suelen ser por seguridad (CSRF) o autentificación

- Mensajería instantánea (ampliado más adelante):
  - Problemas de Whatsapp:
    - Propiedad de Facebook → Cruza los metadatos con Facebook para sugerir relaciones (“gente que quizá conozcas”).
    - Código cerrado → No se puede verificar la correcta implementación del cifrado extremo a extremo.
    - Las conversaciones se guardan en claro en */data/data/com.whatsapp/databases* → Si se compromete el terminal, se tiene acceso a todas las conversaciones
  - Problemas de Telegram:
    - Por defecto las conversaciones no están cifradas de extremo a extremo → La compañía puede ver el contenido de los mensajes
      - Sólo están cifradas de extremo a extremo las conversaciones secretas → Usa un protocolo propio, que no ha sido probado
    - Igual que Facebook vende los datos a otras compañías y gobiernos (EE.UU. y aliados), Telegram lo hace (presumiblemente) con compañías rusas y gobiernos afines a Rusia
    - Telegram proclama que es seguro, pero no aporta medios suficientes y pone restricciones anormales para comprobarlo (límites de fechas, escenarios reducidos a casos muy concretos) → Estrategia propagandística

- Uso de VPNs:
  - Permiten enmascarar la dirección IP al servidor final:
  - El proveedor de VPN controla todo el tráfico:
    - Se traslada la confianza de un proveedor (ISP) a otro (VPN)
    - El problema (evitar que el tráfico pueda ser monitorizado) permanece
  - Normalmente son de pago. Si alguna no lo es, seguramente venda los datos (o algo peor...)
  - ToR / I2P / etc.:
    - *Software* libre
    - Se impide que los nodos intermedios puedan ver la información y que el nodo de salida sepa de dónde vienen los datos
      - Pretenden conseguir el anonimato en la red
      - El nodo de salida sigue pudiendo ver los datos (no se garantiza la privacidad)
    - Las identidades se descubren por errores humanos:
      - Habilitar JavaScript, Flash…
      - Descargar y ejecutar documentos u otros archivos
      - Usar cuentas personales (Gmail, YouTube, Facebook…) → Silk Road (Ross Ulbricht)

- Cifrar y firmar mensajes de manera habitual:
  - Cifrar y firmar tanto texto del mensaje como archivos adjuntos
  - PGP (GPG, Keybase..)
  - Garantiza confidencialidad, integridad y autenticidad

# Modo “paranoia total”

- Técnicas muy usadas en las grandes empresas, sobre todo en los niveles más altos

- Aislar componentes electrónicos:
  - Desactivar redes (modo avión)
  - Quitar fuente de alimentación (batería, enchufe…)
    - Con esto suele bastar
      - Si se hubiera introducido un elemento de escucha que siguiera funcionando sin esta alimentación principal, seguramente se notarían desperfectos en la carcasa.
    - Si no → Jaula de Faraday (caja con papel albal, microondas…)
  - En algunos casos, los fabricantes introducen accesos directos que pueden ser explotados:
    - Intel IME

- Cifrado de archivos (aparte del cifrado de disco):
  - Copias de seguridad
  - USB
  - Carpetas en un terminal compartido
- Borrado efectivo de archivos: shred
- Desbloqueo del terminal con USB o similares (2FA)

# Seguridad en grupos

# Comunicaciones

- Mensajería instantánea:
  - Necesidades:
    - Confidencialidad
    - Integridad
    - Autentificación
    - Repudio
    - Acceso al código
    - En algunos casos, destrucción de mensajes
  - Es recomendable usar diferentes métodos, según las necesidades:
    - Se evita que toda la información se encuentre en el mismo sitio → Relacionar el uso de los diferentes métodos es más complicado

| | Whatsapp | Telegram | Signal | Facebook Messenger | Wickr |
|---|---|---|---|---|---|
| Confidencialidad, integridad y autentificación | Protocolo Signal. Sin revisiones independientes | Sin cifrar (salvo chat secretos) | Protocolo Signal. Público y revisado | Sin cifrar (salvo conversa-ciones secretas) | Protocolo Wickr. Público y revisado |
| Accceso al código | No | Sólo los clientes | | No | Sí (con licencia privativa) |
| Destrucción de mensajes | No | Se pueden eliminar (a mano) | Mensajes con autodes-trucción | No | Mensajes con autodestrucción |
| Comentarios | Propiedad de Facebook | | Protocolo revisado de manera indepen-diente | Propiedad de Facebook | • Protocolo revisado de manera independiente<br>• P2P |

Se han omitido otras opciones para mantener la comparativa manejable.
El resto de aplicaciones (de las más usadas) tienen características similares a Whatsapp o Telegram

- Mensajería instantánea:
  - Las mejores opciones parecen Signal y Wickr
  - Se pueden usar las dos:
    - Signal para uso principal
    - Wickr para complementar (conversaciones adicionales, como debates que no deban ir en el grupo principal)
    - (o viceversa)
  - Poca adopción de Signal y Wickr en España:
    - Whatsapp sigue dominando el mercado

- Otra opción es usar redes descentralizadas:
  - XMPP:
    - Estándar de comunicación
      - Múltiples opciones de aplicaciones que implementan este estándar → Mayor flexibilidad
  - Matrix:
    - Más moderno que XMPP
    - Cuenta con “puentes” para otros protocolos (IRC, XMPP...)
  - Si se cuenta con los recursos, se puede montar un servidor propio → No se depende de terceras partes

- Correo electrónico:
  - Mismas necesidades que en la mensajería instantánea
  - La solución más sencilla es usar PGP para cifrar y firmar todos los correos (incluyendo los archivos adjuntos)
    - Existen muchas implementaciones de uso sencillo:
      - Keybase
      - GPG
      - OpenKeychain
    - Algunos clientes (como K-9 mail) facilitan la integración para cifrar y firmar los mensajes

# Redes sociales

- Alternativas a las redes tradicionales que respetan la privacidad:
  - Facebook → Diaspora
  - Twitter → Mastodon
- Redes descentralizadas y *open-source*
- Problema: poca adopción por el público

mastodon

diaspora*

# Miscelánea

- Al distribuir imágenes:
  - Comprobar metadatos
  - Si se quiere ocultar información, no pixelar (se puede recuperar información), sino pintar encima
- Si se cifran los correos con PGP, distribuir correctamente las claves:
  - Algunas implementaciones (como Keybase) facilitan esta tarea
  - Comprobar las claves en persona
- Usar *software* libre:
  - Buscar alternativas a los servicios tradicionales (Google, Microsoft, etc.):
    - Correo
    - Edición colaborativa de documentos
    - Almacenamiento en la nube

# Conclusiones

- Repaso de herramientas propuestas (también se pueden encontrar otras opciones y recomendaciones en internet):
  - Administrador de contraseñas:
    - Keepass
  - Mensajería instantánea:
    - Signal $\bigvee$ Wickr $\bigvee$ XMPP
  - Correo
    - Proveedor:
      - ProtonMail $\bigvee$ OpenMailBox $\bigvee$ Tutanota
    - Cliente:
      - K-9 mail (móvil)
      - Thunderbird (ordenador)
    - Cifrar con PGP (existen plugins para facilitar la tarea)
  - PGP:
    - Keybase $\veebar$ GPG (para manejar las claves)

- Repaso de herramientas propuestas (cont.):
  - GNU/Linux:
    - Distribuciones amigables y estables:
      - Ubuntu
      - Fedora
      - Mint
    - Cifrar disco (con las herramientas del S.O., o con otras externas como VeraCrypt)
    - Cifrar carpeta personal
  - Firefox:
    - Revisar plugins y extensiones:
      - Desactivar Flash, Java, JavaScript…
      - Controlar HTTPs
      - Extensiones para PGP y Keepass
    - Proteger contra rastreo y rechazar cookies
    - Usar DuckDuckGo $\bigvee$ Ixquick
  - VPN (de pago) $\veebar$ ToR / I2P / Freenet (tráfico lento)

- Para evitar paranoias injustificadas:
  - Revisar el código (aprender es muy sencillo)
  - Monitorizar tráfico
  - Consultar a gente experta en el sector

- Distribuir la información:
  - Limita el impacto al comprometerse un sistema
  - Aumenta la superficie de exposición
- Controlar información pública
  - Saber (o deducir) dónde puede estar la información

<u>No existe la seguridad perfecta</u>

Hay que estar siempre alerta

Demo time!