PROTEGE.LA

protege.la

SOCIALTIC

socialtic.org

CHECKLIST DE SEGURIDAD DIGITAL

para tu computadora, celular y cuentas en línea

PROTEGE.LA

CONTENIDOS: Haydeé Quijano
Paul Aguilar
Sergio Araiza
Juan Manuel Casanueva

DISEÑO EDITORIAL Y GRÁFICO: Sandra Ordóñez

NOTAS:

¡Te damos la bienvenida a tu checklist de privacidad y seguridad digital!

Con esta Checklist tú misma(o) y con tu equipo podrás identificar qué mejorar y por dónde comenzar a cambiar tus hábitos de seguridad digital para cuidar tu información y tener dispositivos sanos.

Nos gusta verlo como un acto de amor propio: cuidar tus archivos, cuentas, comunicaciones y los dispositivos que siempre llevas cerca de ti <3 Porque en la medida en que cuidamos nuestra información, cuentas y perfiles también cuidamos a nuestras redes, contactos, familia y amigxs.

El propósito entonces es que:

- A nivel personal sepas qué puedes mejorar y por dónde empezar a cuidar y proteger tus dispositivos, así como la información y equipos que usas.
- A nivel colectivo, en tu equipo, grupo u organización todas las personas tengan las mismas bases para generar conciencia sobre la seguridad y privacidad; y puedan usar esta checklist para verificar juntas qué prácticas y hábitos mejorar para proteger la información y equipos que comparten.
- Si facilitas espacios para aprender sobre seguridad digital, puedas tomar esta checklist y sus recomendaciones como una referencia de aspectos a revisar y valorar al momento de compartir consejos y recomendaciones.

Esta checklist y sus secciones son un proceso continuo y vivo, seguiremos actualizando las herramientas y recomendaciones. Si deseas colaborar, comentar, aportar a esta checklist, puedes enviar un correo a seguridad@socialtic.org
:) nos encantará saber tus comentarios y aportaciones.

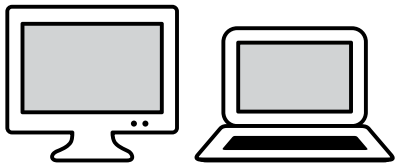
El punto de partida de esta **checklist** de seguridad y privacidad digital es revisar qué tan sanos están nuestros equipos y dispositivos, para esto encontrarás tres categorías:

◆ Computadoras ◆ Celular y tablets ◆ Cuentas en línea

Los **consejos** son recomendaciones básicas para mejorar tus hábitos de seguridad y privacidad digital en las tres categorías.

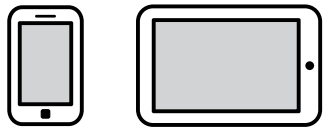
La sección en línea de **herramientas** en https://protege.la/herramientas tiene opciones que hemos probado y tomado de otros recursos de confianza para apoyarte a elegir servicios y herramientas que protegen tu seguridad y privacidad.

COMPUTADORAS



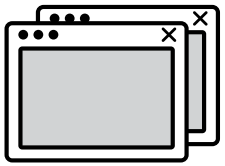
HERRAMIENTAS
https://protege.la/herramientas/#equipos-de-computo

CELULAR Y TABLETS



HERRAMIENTAS
https://protege.la/herramientas/#moviles

CUENTAS EN LÍNEA



HERRAMIENTAS
https://protege.la/herramientas/#servicios-en-linea

NOTAS:

4. Verificación de dos pasos
Para proteger tu información y cuentas en línea, activa la verificación de 2 pasos (o de 2 factores o 2FA). así tienes doble capa de seguridad (contraseña + código).
Cada vez más sitios y plataformas tienen esta opción, te recomendamos activarla en tantas páginas como puedas.
Hay distintas formas de verificación de 2 pasos, puede ser una llave física, un código que llegue a tu celular, un código aleatorio que recibas a través de una app como Google authenticator.

5. Caducidad de tus contraseñas
Cambia tus contraseñas por lo menos cada 6 meses, con esto evitas que se vean comprometidas, ya sea porque alguien las miró en alguna indiscreción, porque fuimos víctimas de hackeo, porque hubo una filtración de datos o un hueco de seguridad en aplicaciones y programas.

6. Gestor de contraseñas
El uso de un llavero digital agiliza la administración de contraseñas y credenciales, pudiendo así compartirlas en grupos de confianza, prevenir problemas de olvido, permite actualizar los datos de manera uniforme y saber concretamente a qué servicios pertenecen.

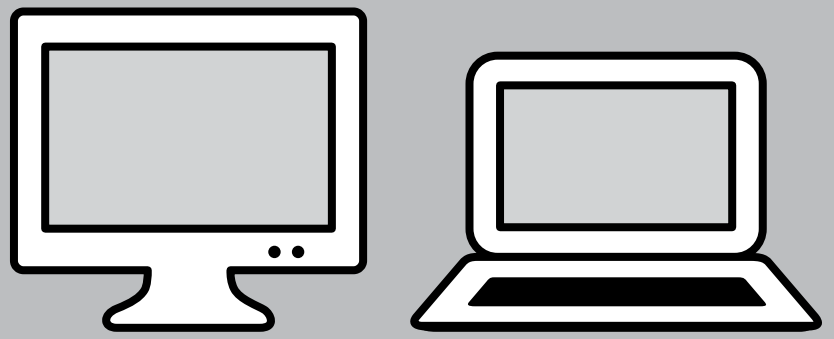
Recuerda que las opciones de herramientas para tus cuentas las puedes encontrar en: https://protege.la/herramientas/#servicios-en-linea

Hasta aquí tu chequeo de seguridad y privacidad digital :)

Te invitamos a revisar seguido tus hábitos para cuidar tu información y contar con dispositivos sanos; además de hacerlo con tu equipo, organización, colectivo.

Antes de cualquier tecnología, estamos juntxs para cuidarnos y compartir este proceso de aprendizaje.

COMPUTADORAS



Aquí revisaremos qué puedes hacer para que tu computadora se encuentre sana, actualizada y configurada; que identifiques hábitos de cuidado y manejo de archivos, y que puedas elegir qué herramientas protegen tu comunicación y navegación en Internet.

Los aspectos que vamos a revisar son:

Limpieza y actualizaciones

Configuración

Archivos

Navegación

Comunicación

Todas las herramientas recomendadas en esta sección las puedes encontrar en este enlace: https://protege.la/herramientas/#equipos-de-computo

CHECKLIST
de seguridad y privacidad digital:

Limpieza y actualizaciones

1. ¿Mantienes actualizado tu sistema operativo? Ej. Windows o Mac
   O Sí O No

2. ¿Usas programas originales (no piratas o "crackeados")?
   O Sí O No

3. ¿Formateaste tu equipo hace menos de un año?
   O Sí O No

Configuración

4. ¿Tienes un antivirus instalado y configurado?
   O Sí O No

5. ¿Tienes un antimalware instalado y configurado?
   O Sí O No

6. ¿Tienes un monitor de USB instalado y configurado?
   O Sí O No

7. ¿Tienes un firewall instalado y configurado?
   O Sí O No

8. ¿Tienes activada contraseña de bloqueo?
   O Sí O No

9. ¿Tienes activado el bloqueo automático cuando no usas tu equipo?
   O Sí O No

10. ¿Tienes desactivado el "uso compartido" en red para carpetas y archivos?
    O Sí O No

CONSEJOS
para proteger tus cuentas en línea:

Privacidad

1. Configuración de privacidad
Entra a la sección de privacidad y seguridad de tus aplicaciones y cuentas, revisa y cambia lo que desees. También recuerda cerrar tus sesiones al finalizar.

2. Registro de actividad
Empresas como Facebook, Google, Microsoft, Apple registran constantemente tu actividad, desde tu ubicación, fotografías, mensajes, las búsquedas que haces y las aplicaciones que usas. Para tomar mayor control de tus datos y actividad:

- Borra el registro de actividad que tengas hasta la fecha
- Configura las opciones de privacidad de cada plataforma para desactivar el registro de actividad
- Usa aplicaciones y programas alternativos que protegen tu privacidad
- Antes de instalar una aplicación, revisa los accesos y permisos que te pide.

Seguridad

3. Contraseñas seguras
Una contraseña se considera segura cuando es: única, privada, larga, combina números + letras + símbolos y tienen caducidad. Evita el "12345" y repetir contraseñas.

CHECKLIST
de seguridad y privacidad digital:

Privacidad 

1. ¿Tienes configurado las opciones de privacidad en tus redes sociales?
   O Sí O No

2. ¿Tienes desactivado el registro de actividad que hacen plataformas como Google, Facebook, Apple, Microsoft?
   O Sí O No

Seguridad 

3. ¿Cuentas con contraseñas seguras en tus cuentas en línea?
   O Sí O No

4. ¿Tienes activada la verificación en dos pasos para tus cuentas de correo y redes sociales?
   O Sí O No

5. ¿Has cambiado tus contraseñas en los últimos 6 meses?
   O Sí O No

6. ¿Usas un llavero digital para guardar y administrar contraseñas?
   O Sí O No

11. ¿Tienes desactivada la ubicación de tu equipo?
    O Sí O No

12. ¿Bloqueas la cámara y el micrófono?
    O Sí O No

Archivos 

13. ¿Has hecho limpieza de archivos en el último año?
    O Sí O No

14. ¿Has hecho respaldo de tu información más importante recientemente?
    O Sí O No

15. ¿Usas herramientas para hacer respaldos automáticos?
    O Sí O No

16. ¿Guardas tus respaldos en algún lugar externo o en “la nube”?
    O Sí O No

17. ¿Tienes activado un sistema de cifrado de archivos?
    O Sí O No

18. ¿Tienes definido un orden o estructura para nombrar tus carpetas y archivos?
    O Sí O No

Navegación 

19. ¿Tienes instalado un navegador web actualizado y seguro?
    O Sí O No

20. ¿Tienes instalados y configurados complementos (plugins o add-on) en tu navegador que protegen tu privacidad y seguridad?
    O Sí O No

21. ¿Usas diferentes navegadores o diferentes perfiles en tu navegador para tu actividad en línea?
    O Sí O No

22. ¿Utilizas la navegación de incógnito en equipos que no son tuyos?

O Sí O No

23. ¿Utilizas un buscador alternativo a Google?

O Sí O No

24. ¿Utilizas una VPN (Virtual Private Network, en español Red Privada Virtual)?

O Sí O No

Comunicación

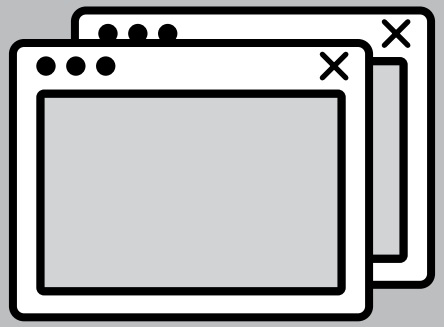
25. ¿Usas canales seguros (con cifrado de extremo a extremo) de mensajería Instantánea, llamadas y video llamadas?

O Sí O No

26. ¿Usas correo electrónico cifrado?

O Sí O No

CUENTAS EN LÍNEA



Llegamos a la última categoría dedicada a tus cuentas en línea. Esto incluye cuentas de redes sociales y de servicios como tu correo electrónico.

Los aspectos que vamos a revisar son:

Privacidad

Seguridad

Todas las herramientas recomendadas en esta sección las puedes encontrar en este enlace: https://protege.la/herramientas/#servicios-en-linea

Comunicación

15. Canales cifrados
Desde tu celular y tablet te comunicas a través de aplicaciones de mensajería, correo, llamadas y videollamadas; para que tu información sea transmitida de forma segura, es importante que tus comunicaciones las hagas en la medida de lo posible con cifrado de extremo a extremo (E2EE).

Para tus dispositivos móviles utiliza aplicaciones con cifrado auditado y que sean transparentes en su funcionamiento.
Ve la lista de herramientas recomendadas para mensajería, llamadas y video llamadas.

16. Cuentas de correo electrónico
Utiliza distintas cuentas de correo para tus actividades, así puedes mantener tus comunicaciones personales y de trabajo separadas. También te recomendamos utilizar correos "desechabes" para las herramientas o plataformas que quieres probar y que te piden un registro con correo electrónico.
Algunos son:

- 10minutemail.com
- anonbox.net
- dispostable.com

17. Correo cifrado
Intenta no comunicar información delicada o sensible a través de emails (esto incluye no solo el cuerpo del correo, si no también "el asunto"). Si lo necesitas, hazlo a través de canales con cifrado de extremo a extremo, o usa cuentas de terceros como Gmail por ejemplo, pero con mensajes cifrados. Esto evitará que alguien más pueda leer tus mensajes, excepto la persona destinataria.

Para cifrar correos desde tu celular puedes usar aplicaciones que implementen el cifrado PGP.

Recuerda que las opciones de herramientas para tus dispositivos las puedes encontrar en: https://protege.la/herramientas/#moviles

CONSEJOS
para proteger tus computadoras:

Limpieza y actualizaciones

1. Sistema Operativo
Actualiza la versión más reciente de los programas y sistemas operativos que uses. Pon atención a los avisos de "actualizaciones" para estar al día con las mejoras de seguridad, éstas corrigen fallas. Puedes activar la actualización automática o descargarlas manualmente. Teniendo todo actualizado proteges tus equipos e información.

2. Programas
Al instalar programas asegúrate hacerlo desde sitios oficiales para evitar software malicioso. También puedes optar por herramientas libres y que cuenten con soporte.

3. Formatear equipos
Formatear tus equipos al menos una vez al año mejora su rendimiento y reduce la posibilidad de robo de información. Mantén respaldos actualizados de tu información (hablamos de esto más adelante) y busca apoyo técnico de confianza.

Configuración

4. Antivirus
Instalar antivirus evita daños a tu equipo y a tus archivos. Es recomendable hacer un análisis completo cada dos semanas, así como un análisis automático de archivos recién descargados.

5. Antimalware
Al igual que un antivirus, el anti malware te evita infecciones en tu equipo y archivos, su configuración debe incluir análisis automático de archivos recién descargados y de memorias USB, así como un análisis completo cada dos semanas.

6. Monitor de USB
Esta herramienta además de analizar las memorias USB al conectarse al equipo, impiden la ejecución automática de software malicioso.

7. Firewall
Un firewall analiza la información que entra y sale de tu equipo, pudiendo detectar y bloquear tráfico malicioso y que busque infectar tu computadora.

8. Bloqueo de dispositivos
Establece una contraseña de acceso a tu computadora. Con esta medida, además de evitar accesos no deseados, podrás tener al margen actualizaciones que para ejecutarse también requieren contraseña.

9. Bloqueo automático por inactividad
Protege tus equipos activando el bloqueo automático de tu computadora después de no usarla durante unos minutos.

10. Uso compartido
Revisa tu configuración de red y desactiva el “uso compartido” y funciones similares, esto evita que tu equipo y carpetas sean visibles a las redes que te conectas.

11. Ubicación
De preferencia mantén desactivadas la localización de tus equipos, activa la ubicación sólo para las aplicaciones que desees, esto evita que los datos de tu ubicación se reporten a algún lugar de Internet sin tu consentimiento.

12. Cámara y micrófono
Si tu computadora cuenta con cámara y micrófono integrado, prueba cubrir la cámara con un sticker o cinta y utilizar un “micrófono tonto”, es decir un conector de micrófono externo que simula un micrófono conectado, desactivando así el micrófono interno. La solución que no asegura un fallo es desconectando el micrófono físicamente.

10. Identificación de número de contacto.
Si decides separar usos por tu actividad, por ejemplo tener un celular para tu trabajo o activismo y otro para uso personal, puedes ocultar tu número de contacto para evitar que guarden tus datos. Recuerda que tu número de teléfono suele ser un punto de entrada hacia otra información que te identifica.

11. Permisos y accesos de tus aplicaciones
Antes de instalar una aplicación revisa los accesos y permisos que te pide. En las aplicaciones ya instaladas, revisa los permisos y retira el acceso a contactos, geolocalización, cámara, y lo que no consideres necesario para que funcione la app. Haz esta revisión seguido para tener control de los permisos que tienen tus aplicaciones.

Archivos

12. Respaldos
Haz copias actualizadas de tu información en tus dispositivos de manera regular (elige si semanal o mensualmente), como por ejemplo contactos y archivos multimedia y guárdalas en lugares seguros contra daño y robo.

Navegación

13. VPN
Es más probable que desde tu celular busques conectarte a redes gratuitas (como en parques, cafés y aeropuertos); si te urge conectarte a WiFi gratis, descarga una VPN (Virtual Private Network o Red Privada Virtual) y actívala para proteger tu información. Con una VPN agregas una capa extra de seguridad, ya que tu info viaja por un túnel cifrado.

14. Navegador actualizado y seguro
Tu celular y tablet deben contar con navegadores predeterminados, como por ejemplo en el caso de Android, el navegador que ya viene instalado en tu celular desde fábrica es Chrome o alguno genérico. Valora elegir navegadores que protegen tu privacidad, como Firefox Focus. Encuentra más opciones en la sección de herramientas.

5. Bloqueo de dispositivos
Establece una contraseña, PIN o patrón de acceso a tu celular y tablet. Con esta medida podrás evitar accesos no deseados. Desde los ajustes de privacidad, algunas aplicaciones también ofrecen bloqueos de pantalla para evitar el acceso.

6. Ubicar, bloquear o borrar archivos de forma remota
Para casos de robo o pérdida, desde las opciones de seguridad configura la opción de encontrar, bloquear o borrar la información de tu celular o tablet de manera remota.

7. Cifrado
Para proteger los datos de tu teléfono o tablet, activa el cifrado de tu equipo.

- En Android: Abre Configuraciones > Seguridad > Encriptar teléfono.
- En iOS: Se activa de manera automática al establecer una contraseña o Touch ID.

Recuerda que el cifrado es una capa de seguridad que evita el acceso si no se cuenta con la contraseña correcta.
Para iniciar el proceso de cifrado, el teléfono debe estar cargado y conectado a energía.

8. Ubicación y envío de datos
Tus equipos constantemente transmiten información, como por ejemplo: tu ubicación. Para evitar que tu teléfono transmita tu ubicación de forma predeterminada, así como otros datos no deseados:

- Desconecta la señal de Bluetooth y GPS cuando no las uses
- Desconecta la señal WiFi cuando no la uses y borra seguido la lista de redes a las que te has conectado últimamente.
- Desactiva tus datos móviles cuando no los ocupes.

Tú eliges cuándo activar y desactivar estas funciones.

9. Limpieza de registros de llamadas y mensajes
Identifica qué información sobre ti, lo que haces y con quién te comunicas puede estar expuesta. En el caso de las llamadas y mensajes revelan quiénes son nuestros contactos más cercanos. Borra el historial de comunicaciones (llamadas y mensajes) que no sea necesario guardar.

Archivos

13. Limpieza de archivos y formateo de equipos
Elimina los archivos y programas que no necesitas, recuerda vaciar la papelera de reciclaje, también es recomendable formatear los discos duros y memorias de tus equipos. Ten presente hacer esta limpieza cada año, aumentando su frecuencia entre cada 6 o 3 meses.

14. Respaldos
Haz copias actualizadas de tu información de manera regular (elige si semanal o mensualmente) y guárdalas en lugares seguros contra daño y robo.

15. Respaldos automáticos
Los respaldos automáticos facilitan copias actualizadas de tu información sin problemas o pérdidas, además de hacer más rápido y ligero el proceso.

16. Respaldos en lugares seguros
Guarda tus respaldos en un disco duro externo o en un servicio confiable en la nube; para disminuir la posibilidad de pérdida o daño de tus archivos, prueba la combinación de ambos (disco duro externo y nube) Si usas un disco duro externo, guárdalo en un lugar seguro, donde no esté expuesto a robo o daño físico. En el caso de la nube, consulta la lista de herramientas.

17. Cifrado de equipos y archivos
Cifra los archivos, medios extraíbles como USBs y equipos que llevas a tus viajes, que salen de la organización, o que estén en riesgo de pérdida o robo. El cifrado evita el acceso a tu contenido sin una contraseña.

18. Organización de carpetas y archivos
Mantén un orden o “Estructura de carpetas y archivos” de manera que lo reconozcas y mantengas actualizado, esto mejora el manejo de la información en el equipo (por ejemplo, tus respaldos ordenados).

Navegación

19. Navegador seguro
No todos los navegadores web tienen la tecnología necesaria para proteger lo que haces y compartes en línea. Consulta la lista de navegadores recomendados en la sección de herramientas.

Las pruebas de seguridad en navegadores no califican como seguros a Internet Explorer y Microsoft Edge por lo que te recomendamos evitar su uso.

Si los sitios que frecuentas te obligan a utilizar exclusivamente un navegador en especifico, no te quedes calladx y alza la voz, ¡exige una versión para tu navegador de preferencia!

20. Complementos para tu navegador (plugins o add-ons)
Para navegar de forma segura en Internet, instala complementos o extensiones que tengan un enfoque de privacidad y seguridad en tu navegador, en las recomendaciones encuentra herramientas que bloquean el rastreo de tu actividad en línea, el spam, engaños digitales como el phishing, y otras que aseguran que tu información viaje de forma más segura y cifrada.

21. Perfiles de navegación
Utiliza distintos navegadores o distintos perfiles para tu actividad en línea, así puedes mantener tus actividades personales y de trabajo separadas.

22. Navegar como incógnito
La función “ventana de incógnito” o “navegación de incógnito” te permite utilizar el navegador sin que se guarde el historial o contraseñas en el equipo, esto no es una navegación anónima, solamente no guarda datos en el equipo. Úsala cuando no estés navegando en tu computadora, inicias sesión en algún sitio o no quieres dejar registro de tu navegación.

CONSEJOS
para proteger tu celular y tablets:

Limpieza y actualizaciones

1. Aplicaciones y sistema operativo
Procura descargar aplicaciones de los sitios oficiales. Antes de descargarla pon atención a los comentarios, a sus cuentas de soporte y a las búsquedas en Internet; esto te ayudará a detectar aplicaciones falsas y dañinas. También asegúrate de actualizar las aplicaciones así como el sistema operativo de tu celular y tablet.

2. Limpieza de archivos
Elimina archivos que ya no usas de tu celular como imágenes, videos y documentos descargados. Esta limpieza te facilitará espacio en tu celular, te permitirá tener mayor control de tu información y que tu celular esté en mejor estado.

3. Formatear equipos
Restaura tu celular a su estado de fábrica por lo menos una vez al año, así le das una limpieza completa que lo mantiene en buen estado. Para esto, ve a la sección de configuración de tu celular, buscar “Acerca de éste dispositivo” y “Restaurar a fábrica”. Antes, asegúrate de contar con respaldos actualizados de tu información, una opción es mover tus datos a tu SD desde cada aplicación.

Configuración

4. Bloqueo automático por inactividad
Activa el bloqueo automático después de ciertos segundo de inactividad para evitar que alguien más lo use o vea desde tu pantalla lo que haces.

9. ¿Tienes activada la opción para ocultar tu número de contacto al hacer llamadas?

O Sí O No

10. ¿Revisas los acceso de las aplicaciones que usas?

O Sí O No

Archivos

11. ¿Has hecho respaldo de tu información más importante recientemente?

O Sí O No

Navegación

12. ¿Usas una VPN (Virtual Private Network, Red Privada Virtual)?

O Sí O No

13. ¿Tienes instalado un navegador actualizado y seguro?

O Sí O No

Comunicación

14. ¿Utilizas aplicaciones seguras de mensajería Instantánea, llamadas y video llamadas?

O Sí O No

14. ¿Usas diferentes cuentas de correo electrónico? Por ejemplo uno para tu trabajo, otra cuenta personal.

O Sí O No

15. ¿Usas aplicaciones de correo electrónico cifrado?

O Sí O No

23. Buscadores alternativos a Google

Google mantiene un historial completo de tus acciones, por lo que al buscar información por la web vamos dejando rastros sobre lo que hacemos y cómo lo hacemos; una alternativa para buscar información sin comprometernos es utilizando buscadores que cuiden tu privacidad.

24. VPN

Las redes privadas virtuales (VPN) permiten que tu ubicación geográfica no quede expuesta de manera directa y permite que tu información viaje de manera cifrada.

Comunicación

25. Canales cifrados

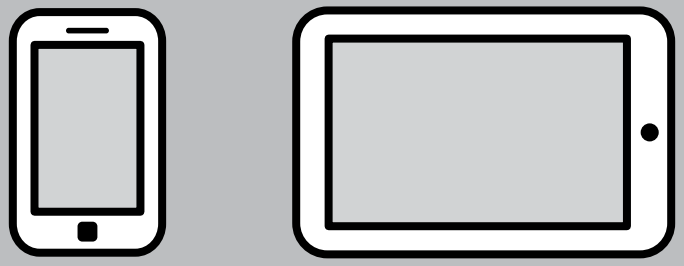
Desde tu computadora te comunicas a través de mensajería web, correo, llamadas y videollamadas; para que tu información sea transmitida de forma segura, es importante que tus comunicaciones las hagas siempre en la medida de lo posible con cifrado de extremo a extremo (E2EE). Para tu navegador y escritorio utiliza aplicaciones con cifrado auditado y que sean transparentes en su funcionamiento.

26. Correo cifrado

Intenta no comunicar información delicada o sensible a través de emails (esto incluye no solo el cuerpo del correo, si no también “el asunto”). Si lo necesitas, hazlo a través de canales con cifrado de extremo a extremo, o usa cuentas de terceros como Gmail por ejemplo, pero con mensajes cifrados. Para cifrar correos puedes utilizar PGP directamente o apoyarte en herramientas gráficas de terceros que hacen su uso más sencillo.

Recuerda que las opciones de herramientas para tu computadora las puedes encontrar en: https://protege.la/herramientas/#equipos-de-computo

CELULAR Y TABLETS



Es el turno de tus dispositivos móviles. Aquí nos enfocamos en tus celulares y tablets, refiriéndonos a ellos como “dispositivos”.

Revisaremos qué puedes tener en cuenta para contar con dispositivos sanos, actualizados y configurados; tus hábitos de cuidado para el manejo de archivos y aplicaciones, y herramientas que protejan tu comunicación y navegación en Internet.

Los aspectos que vamos a revisar son:

Limpieza y actualizaciones

Configuración

Archivos

Navegación

Comunicación

En esta sección queremos también recomendarte tomar a consideración usar diferentes teléfonos para tu trabajo, activismo o uso personal.

Todas las herramientas recomendadas las puedes encontrar en: https://protege.la/herramientas/#moviles

CHECKLIST
de seguridad y privacidad digital:

Limpieza y actualizaciones

1. ¿Todas tus aplicaciones en el celular y tablet son descargadas de sitios oficiales y de confianza?
   O Sí O No

2. ¿Borras constantemente archivos que ya no usas de tus dispositivos?
   O Sí O No

3. ¿Formateaste tus dispositivos hace menos de un año?
   O Sí O No

Configuración

4. ¿Tienes activado el bloqueo de pantalla?
   O Sí O No

5. ¿Tienes configurados tus dispositivos de tal manera que si se pierden puedan ser rastreados o borrados remotamente?
   O Sí O No

6. ¿Tienes cifrados tus dispositivos?
   O Sí O No

7. ¿Tienes desactivada la opción de compartir información de la red celular, como datos y ubicación?
   O Sí O No

8. ¿Eliminas los registros e historial de mensajes y llamadas de manera periódica?
   O Sí O No