PROTEGE.LA

protege.la

SOCIALTIC

socialtic.org

CHECKLIST DE
SEGURIDAD DIGITAL
SYS ADMIN

Para equipos, redes, cuentas en línea y sitios web

PROTEGE.LA

Notas:

CONTENIDOS:
Haydeé Quijano | Paul Aguilar | Sergio Araiza | Juan Manuel Casanueva

DISEÑO EDITORIAL Y GRÁFICO:
Sandra Ordóñez | Mirelle Mora

Notas:

¡Te damos la bienvenida a tu checklist de privacidad y seguridad digital para **Sys Admin!**

Esta checklist está creada para las personas que dan mantenimiento y administran sistemas en una organización, grupo o colectivo. Con ella podrás saber qué mejorar y por dónde comenzar hábitos de seguridad digital que cuiden la información y equipos administrados. También te puede ser útil como documento de guía y revisión periódica de tus actividades como Sys Admin.

El propósito entonces es que:

A nivel personal cuentes con un listado de las actividades periódicas y claves en relación a: equipos, redes, cuentas en línea y sitios web.

A nivel colectivo, en tu equipo, grupo u organización, puedes partir de esta checklist para establecer bases y hábitos de seguridad y privacidad; y usarla en casos como el compartir o delegar la administración de equipos.

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; recuerda que las medidas y consejos de seguridad que hoy funcionan y se ajustan a tus necesidades, en otro grupo o situación pueden cambiar. Por esto es necesario seguir probando y 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 primer paso de esta checklist de **seguridad y privacidad digital** es revisar las actividades necesarias para contar con equipos y sistemas seguros y sanos; para esto encontrarás una lista de preguntas divididas en cuatro categorías:

- **Equipos**
- **Redes**
- **Sitios web y hosting**
- **Cuentas en línea**

Los **consejos** se enfocan en recomendaciones básicas para mejorar hábitos de seguridad y privacidad digital en las cuatro 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 herramientas que protegen tu seguridad y privacidad.

Consideraciones:

Partimos de que en las organizaciones y grupos existe diversidad de dispositivos y sistemas operativos (SO).

También sugerimos aplicar todos los consejos y recomendaciones sin importar el sistema operativo que uses; ya que todos son vulnerables a software malicioso.

Cualquier actividad que consideres necesaria y no se encuentre en esta checklist, puedes agregarla a este documento para contar con una versión adaptada a tu ambiente y contexto.

EQUIPOS

Limpieza y actualizaciones
Configuración
Archivos
Navegación
Comunicación

REDES

Administración

CUENTAS EN LÍNEA

Privacidad
Seguridad

SITIOS WEB Y HOSTING

Administración

Notas:

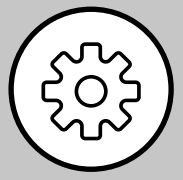
Notas:

EQUIPOS

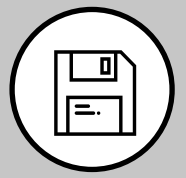
Aquí vamos a revisar las actividades periódicas relacionadas a configuración y actualización de equipos, así como hábitos de manejo de archivos, y de prevención ante posibles riesgos de seguridad y privacidad.

Los aspectos que vamos a revisar son:

LIMPIEZA Y ACTUALIZACIONES



CONFIGURACIÓN



ARCHIVOS

NAVEGACIÓN

COMUNICACIÓN

En esta sección, los consejos están enfocados a las computadoras que usen en tu organización o equipo; por esto recomendamos que junto a tus compañerxs **revisen también la Checklist de seguridad digital para usuarixs en línea (https://protege.la/checklists/)** y esta versión para imprimir, esto ayudará a que todas las personas cuenten con las bases para tener equipos más saludables y seguros.

Herramientas: Todas las herramientas recomendadas de esta sección las puedes encontrar en: **https://protege.la/herramientas**

CHECKLIST

de seguridad y privacidad digital:
EQUIPOS

LIMPIEZA Y ACTUALIZACIONES

1. ¿Has revisado que el sistema operativo de los equipos sean compatibles con las características de las máquinas? Por ejemplo Windows (de 32 bits) para equipos con modelos viejitos:

☐ **Sí** ☐ **No**

2. ¿Mantienes actualizado el sistema operativo (SO) y aplicaciones de los equipos? Ej. Windows o Mac

☐ **Sí** ☐ **No**

3. ¿Los equipos usan SO y programas originales? (es decir, no usan programas piratas o "crackeados")

☐ **Sí** ☐ **No**

4. Entre todos los equipos de tu grupo/organización ¿utilizan la misma versión de SO o compatibles?

☐ **Sí** ☐ **No**

5. ¿Has formateado los equipos hace menos de un año?

☐ **Sí** ☐ **No**

CONFIGURACIÓN

6. ¿Tienen un antivirus instalado y configurado?

☐ **Sí** ☐ **No**

7. ¿Tienen un antimalware instalado y configurado?

☐ **Sí** ☐ **No**

8. ¿Tienen un monitor de USB instalado y configurado?

☐ **Sí** ☐ **No**

9. ¿Tienen un firewall instalado y configurado?

☐ **Sí** ☐ **No**

10. ¿Mantienes la gestión y los permisos de las cuentas actualizadas y de acuerdo a tareas? Es decir: cuentas de usuarias con contraseña, separadas por accesos correspondientes.

☐ **Sí** ☐ **No**

Ya vimos los cuidados técnicos, vemos ahora los cuidados éticos para interacciones seguras y positivas con personas y máquinas.
Algunos consejos:

PARTIR DEL **RESPETO** A LA DIVERSIDAD; EVITAR QUERER **~~"CONVERTIR"~~** A UNA HERRAMIENTA O SISTEMA OPERATIVO FAVORITO.

TOMAR CONCIENCIA DEL DAÑO QUE PUEDEN REPRESENTAR LO QUE HAGO (FÍSICO Y DIGITAL)

HACERSE CARGO, **TOMAR RESPONSABILIDAD** DE LO QUE HAGO Y DIGO

RESPETAR LOS LÍMITES DE OTRAS PERSONAS, **INTIMIDAD Y PRIVACIDAD EN SU INFORMACIÓN, PERTENENCIAS, ESPACIO, MAQUINAS, CUERPOS.**

DOCUMENTAR, COMPARTIR Y PONER INFORMACIÓN ÚTIL A **DISPOSICIÓN DE OTRAS PERSONAS**

EVITAR USAR Y PERMITIR EL USO DE SOFTWARE PIRATA.

COMO SYSADMIN SE TIENE ACCESO A CUENTAS DE CORREO, MENSAJES, ARCHIVOS Y BASES DE DATOS. NO USAR Y ABUSAR DE ESTE ACCESO **PARA BENEFICIO PROPIO, EN PERJUICIO DE OTRAS PERSONAS, O PARA "CURIOSEAR".**

Referencias:

https://socialtic.org/codigo/
https://github.com/linuxitux/La-Biblia-del-SysAdmin/blob/master/README.md
https://sindominio.net/biblioweb/telematica/hacker-como.html
https://criticalengineering.org/es
https://blog.bastelfreak.de/2015/09/sysadmin-manifesto/

¡Hasta aquí tu chequeo de seguridad y privacidad digital para SysAdmin!

Te invitamos a revisar periódicamente tus hábitos para cuidar tu información y contar con dispositivos sanos.

Esperamos que esto también te sirva para tener una vida apacible como sys admin y dormir tranquilamente por las noches :)

Recuerda compartirlo con tu equipo, organización, colectivo. Antes de cualquier tecnología, estamos juntxs para cuidarnos y compartir este proceso de aprendizaje.

11. En equipos y carpetas ¿está configurada la opción de visibilidad y acceso en red?

☐ **Sí** ☐ **No**

12. ¿Los equipos tienen desactivada la opción de ubicación?

☐ **Sí** ☐ **No**

13. ¿Los equipos tienen bloqueadas las cámaras y micrófonos?

☐ **Sí** ☐ **No**

14. ¿Los equipos tienen activada contraseña de bloqueo?

☐ **Sí** ☐ **No**

15. ¿Los equipos cuentan con el bloqueo automático cuando no están en uso?

☐ **Sí** ☐ **No**

ARCHIVOS

16. ¿Programas respaldos de la información de manera periódica?

☐ **Sí** ☐ **No**

17. ¿Usas alguna herramienta para hacer respaldos automáticos?

☐ **Sí** ☐ **No**

18. ¿Guardas los respaldos en algún lugar externo? (como un disco duro o en “la nube”)

☐ **Sí** ☐ **No**

19. ¿Has activado en los equipos un sistema de cifrado de archivos?

☐ **Sí** ☐ **No**

20. ¿Los equipos cuentan con un orden o estructura para nombrar carpetas y archivos?

☐ **Sí** ☐ **No**

NAVEGACIÓN

21. ¿Has instalado en los equipos un navegador web actualizado y seguro?

☐ **Sí** ☐ **No**

22. ¿Los equipos tienen instalados y configurados complementos (plugins o add-on) en el navegador que protegen la privacidad y seguridad de usuarixs?

☐ **Sí** ☐ **No**

23. ¿Los navegadores están configurados para que se limpien de manera automática? (es decir, que no guarden historial, ni archivos temporales)

☐ **Sí** ☐ **No**

24. ¿Has configurado un buscador alternativo a Google para tu grupo / organización?

☐ **Sí** ☐ **No**

25. ¿Has configurado una VPN (Virtual Private Network, en español Red Privada Virtual)?

☐ **Sí** ☐ **No**

COMUNICACIÓN

26. ¿Usan canales seguros (con cifrado de extremo a extremo) de chats, llamadas y videollamadas?

☐ **Sí** ☐ **No**

27. Quienes tienen cuenta de correo y manejan información privada y sensible ¿Usan correo electrónico cifrado?

☐ **Sí** ☐ **No**

CONSEJOS PARA PROTEGER:

Equipos

LIMPIEZA Y ACTUALIZACIONES

1. Compatibilidad de sistema operativo y equipos

- Revisa que los sistemas operativos y las características de los equipos sean compatibles; esto significa que los elementos y programas "hablen el mismo idioma" y las partes puedan convivir; con esto se aprovecharán mejor los recursos físicos del equipo, rendimiento y velocidad.

- Considera que los equipos nuevos que vienen de fábrica, generalmente ya cuentan con un procesador y sistema operativo compatibles.

- Apliquen HTTPS al sitio y su contenido

- Bloqueen intentos de sesión sucesivos desde un mismo origen

4. Gestión de contraseñas

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

5. Gestión de credenciales: usuarios y contraseñas

Recuerda que otras personas necesitan acceder a los servicios. Por lo que te sugerimos gestionar estos accesos. La administración de credenciales puede contener:

- Dominios

- Servidores/Hosting

- Correos

- Usuarios de equipos

Apóyate en un gestor de contraseñas, como KeePassXC que contenga un registro de accesos para otros usuarios. Por ejemplo: crea un llavero por área, para que las personas que trabajan en ellas puedan acceder a la información.

6. Respaldo

La creación y respaldo de copias actualizadas del sistema es una tarea importante. De esta manera garantizas que el trabajo de todas las personas, incluyendo el de sitios web, no se perderá y podrá recuperarse.

7. 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.

Recuerda que las opciones de herramientas para tus cuentas las puedes encontrar en: **https://protege.la/herramientas/**

CONSEJOS PARA PROTEGER:

SITIOS WEB Y HOSTING

1. Pagos actualizados
Recuerda mantener al día los pagos de tu alojamiento y servicios web, mantén notificado a quien corresponda para evitar suspensiones de servicio. La falta de pagos provoca contratiempos o pérdidas de información.

2. Revisar el tráfico de red para identificar actividad sospechosa
Los servicios web son susceptibles a recibir ataques automatizados, como: cambios en contenidos, tráfico malicioso o ataques de denegación de servicios (DDoS) por lo que revisar el tráfico de red e identificar actividad sospechosa de manera regular es clave para prevenir incidentes.

3. Cambiar configuraciones preestablecidas
Las configuraciones por default o preestablecidas de la mayoría de servicios o tecnologías son fáciles de encontrar en los manuales de usuario, por eso es recomendable cambiarlas.

Si administras servidores:

- Mantenlos actualizados, tanto en hardware como en software.
- Configura conexiones seguras a tu servidor como HTTPS, SSH o SFTP.
- Mantén limpios tus archivos eliminando todo aquello que ya no sea requerido en el servidor.

Si administras plataformas CMS como WordPress, Joomla, Drupal, etc:

- Mantén el software actualizado
- No instales complementos de fuentes no oficiales o complementos desactualizados.
- Utiliza complementos que incrementen la seguridad, por ejemplo:
  - Plugins para ocultar las urls de inicio de sesión
  - Forzar conexiones seguras

Cuando lxs usuarixs cambian el sistema operativo por alguna razón, éste puede ser de 32 o 64 bits. Para revisar cuál es tu caso:

- En Windows: ve al menú de inicio y escribe Acerca de tu PC, revisa el tipo de sistema y si es compatible con el procesador.
- En GNU/Linux: ve a configuración de sistema, y a Detalles

En definitiva ¿de qué depende que tenga 32 o 64 bits? depende qué tan viejito sea tu equipo.

2. Sistema Operativo
Actualiza la versión más reciente de los programas y sistemas operativos que usen los equipos. Puedes activar la actualización automática o descargarlas manualmente. Ten en cuenta que estar al día con las actualizaciones protege los equipos y la información.

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

4. Compatibilidad entre equipos
Contar todxs con el mismo sistema operativo en los equipos te facilitará el día a día de actualizaciones y fallas recurrentes.

La forma en que administras los dispositivos puede ser diversa y ajustarse a equipos y sistemas operativos mixtos; para estos casos recomendamos evaluar procesos de mantenimiento y revisar colectivamente prácticas de seguridad.

5. Formatear equipos
Formatear equipos al menos una vez al año mejora el rendimiento y reduce la posibilidad de robo de información. Mantén respaldos actualizados de la información.

CONFIGURACIÓN

6. Antivirus
Instalar antivirus evita daños a los equipos y archivos. Es recomendable hacer un análisis completo cada dos semanas, así como un análisis automático de archivos recién descargados.

7. Antimalware
Al igual que un antivirus, el anti malware evita infecciones en los equipos y archivos, para su configuración te aconsejamos incluir análisis automáticos de archivos recién descargados y de memorias USB, así como un análisis completo cada dos semanas.

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

9. Firewall
Un firewall analiza la información que entra y sale de los equipos, detecta y bloquea tráfico malicioso que busque infectar los equipos de la organización o grupo.

10. Gestión de cuentas y accesos
Para la gestión de accesos al sistema, es importante que como organización consideren acuerdos y políticas de accesos y permisos a personas y grupos de acuerdo a sus necesidades.

Por ejemplo, para algunas tareas de mantenimiento no es necesario llegar a todos los rincones del sistema. Para mitigar riesgos y accesos no previstos:

•Asigna accesos a quienes realmente lo necesiten para sus tareas. Por ejemplo:

"Administración", para quien realiza mantenimiento o cambios en el sistema.
"Estándar", para quien utiliza el equipo de forma regular.
"Invitada", una opción para personas que usan algún equipo de forma ocasional.

•Documenta y actualiza los accesos personales - grupales y sus necesidades.

•Monitorea las notificaciones de solicitudes de accesos.

•Contempla un plan para eliminar accesos y cuentas. (Por ejemplo: cuando una persona ya no forma parte de la organización).

11. Uso y visibilidad en red
Revisa la configuración de red y asigna permisos a carpetas y equipos de acuerdo a tareas; esto previene accesos no previstos, fuga de información, ejecución remota de programas e infecciones con softwares maliciosos.

12. Ubicación de equipos
De preferencia mantén desactivadas la localización de equipos, activa la ubicación sólo para las aplicaciones y momentos que sean necesarios; esto evita que los datos de ubicación se almacenen sin el consentimiento de las personas.

13. Cámara y micrófono
Si las computadoras cuentan con cámara y micrófono integrado, un tip es 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.

CHECKLIST

de seguridad y privacidad digital:
SITIOS WEB Y HOSTING

ADMINISTRACIÓN

1. ¿Mantienes al día el pago de los servicios?

☐ **Sí** ☐ **No**

2. ¿Monitoreas regularmente el tráfico de red o uso de ancho de banda de los sitios web?

☐ **Sí** ☐ **No**

3. ¿Cambias las configuraciones que vienen preestablecidas de los servicios que administras, como servidores y CMS? Por ejemplo: contraseñas, usuarios, permisos de archivos, etc.

☐ **Sí** ☐ **No**

4. ¿Utilizas un llavero digital para guardar y administrar contraseñas de tus sitios web y hosting?

☐ **Sí** ☐ **No**

5. ¿Cuentas con un registro o archivo de credenciales y configuraciones organizadas y accesibles para la administración de la organización?

☐ **Sí** ☐ **No**

6. ¿Cuentas con respaldos actualizados de la información y contenidos de tu sitio web?

☐ **Sí** ☐ **No**

7. ¿Guardas los respaldos de información en algún lugar externo? (como un disco duro o en "la nube")

☐ **Sí** ☐ **No**

SITIOS WEB Y HOSTING

En esta última sección: sitios web y hosting, vamos a repasar las tareas relacionadas a la administración de sitios web, servidores web, gestores de contenido (CMS) y alojamiento.

Los aspectos que vamos a revisar son:

ADMINISTRACIÓN

Herramientas: Todas las herramientas recomendadas de esta sección las puedes encontrar en: **https://protege.la/herramientas**

14. Contraseña de bloqueo
Establezcan contraseñas de acceso a las computadoras. Con esto, además de evitar accesos no deseados, podrán tener al margen actualizaciones que para ejecutarse requieren contraseña.

15. Bloqueo automático por inactividad
Protejan los equipos activando el bloqueo automático y solicitud de contraseña.

ARCHIVOS

16. Plan de respaldos
Respaldar es una de las tareas que no pueden faltar a la hora de administrar redes y sistemas.

El mejor consejo: sistematiza la creación de copias actualizadas de información, servidores, dispositivos de redes y aplicaciones de seguridad.

Al planear tu respaldo, ten en cuenta:

•Cada cuándo: depende de la actividad de tu organización, elige si semanal o mensual.

•Cuánto espacio ocupa: verifica espacio libre en discos duros y guárdalos en lugares seguros contra daño y robo.

•Elige programas que hagan copias verificadas y automáticas. ¡Prueba que los respaldos sirvan!

•Automatiza los respaldos: esto facilita copias actualizadas y hace más rápido y ligero el proceso.

•Haz respaldos por equipo y de tipo incremental.

17. Respaldos automáticos
Los respaldos automáticos facilitan copias actualizadas de tu información sin problemas o pérdidas, además de hacer más rápido y ligero el proceso. En **https://protege.la/herramientas/#respaldos-equipos-de-computo** usa los filtros para conocer opciones de Linux, Windows, Mac y multiplataforma.

18. 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. Si eliges guardar archivos en la nube, **usa los filtros en https://protege.la/herramientas/#respaldos-servicios-en-linea** para conocer herramientas.

19. Cifrado de archivos
Cifra archivos, medios extraíbles como USBs y equipos que tú y tu equipo lleven a viajes, salgan del lugar de trabajo, o estén en riesgo de pérdida o robo.

En casos de información delicada, además del respaldo, también es aconsejable cifrar; ya que el cifrado protege contenido y equipos con contraseña.

20. Organización de carpetas y archivos
Mantén un orden o "estructura de carpetas y archivos" de manera que quienes administran y usan reconozcan y mantengan actualizado; esto mejora el manejo de la información en el equipo (por ejemplo, tus respaldos ordenados).

NAVEGACIÓN

21. Navegador actualizado y seguro
No todos los navegadores web protegen lo que hacemos y compartimos en línea. Consulta la lista de navegadores recomendados en la sección de herramientas. **https://protege.la/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.

22. Complementos para navegadores (plugins o add-ons)
Para navegar de forma segura en Internet, instala complementos o extensiones que tengan un enfoque de privacidad y seguridad en los navegadores de equipos; en **https://protege.la/herramientas** 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.

23. Limpieza de navegadores
Revisa la configuración de tu navegador y elimina de forma periódica los datos de tu navegación, esto evita dejar rastro de las actividades en línea. Elige:

•Cerrar sesiones de manera automática.

•No guardar historial por más de una semana.

•No almacenar cookies ni archivos temporales más de una semana.

24. Buscadores alternativos a Google
Google mantiene un historial completo de tu actividad, por lo que al buscar información por la

4. Gestión 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.

5. Verificación de dos pasos
Para proteger la información y cuentas en línea, activa la verificación de 2 pasos (o de 2 factores, 2FA). Con la verificación de 2 pasos tienes doble capa de seguridad (contraseña + código).

Cada vez más sitios y plataformas tienen esta opción, te recomendamos activarla en tantas plataformas 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, entre otros. Activa la doble verificación en los servicios que administras dentro de la organización, y promueve que tu equipo también la activen en los servicios que usan en la organización y de forma personal.

6. Accesos en redes sociales
Mantén la gestión y los permisos actualizados de las cuentas que administran: revisa quiénes tienen acceso a las cuentas y elimina las cuentas que no sean relevantes.

7. Alertas de inicio de sesión
Las alertas son actualizaciones sobre la actividad de tus cuentas. Desde las opciones de configuración controla qué tipo de alertas quieres recibir (por SMS, correo electrónico o notificación en tu dispositivo). Te aconsejamos que actives las alertas de inicio de sesión en otros dispositivos

9. Configuración de panel de control
Al gestionar un producto o servicio tienes acceso a una consola o panel de administración, procura sacarle el mayor provecho revisando y configurando adecuadamente las opciones que ésta tiene.
Cada servicio tiene funcionalidades útiles como la gestión de contraseñas, notificaciones sobre actualizaciones y uso del servicio, opciones de perfiles o accesos.
Lo importante es que conozcas tus paneles de administración y les saques provecho.

Revisa estos consejos relacionados a cuentas en línea con tus compañerxs y hazlos parte de un plan o protocolo de seguridad de la organización.

CONSEJOS PARA PROTEGER:

Cuentas en línea

PRIVACIDAD

1. Configuración de privacidad
Promueve que todas las personas del equipo revisen la sección de privacidad y seguridad de sus aplicaciones y cuentas en línea. También el hábito de cerrar sesiones al finalizar. Para las personas que gestionan redes sociales de la organización o grupo y tienen vinculadas sus cuentas personales con las de la organización es importante revisar la configuración de cada plataforma.

2. Registro de actividad
Empresas como Facebook, Google, Microsoft, Apple registran constantemente nuestra actividad, desde ubicación, fotografías, mensajes, búsquedas que hacemos y aplicaciones que usamos.
Para tomar mayor control de nuestros datos y actividad, promueve en tu equipo los siguientes hábitos:

•Borrar el registro de actividad que tengas hasta la fecha.

•Configurar las opciones de privacidad de cada plataforma para desactivar el registro de actividad

•Usar aplicaciones y programas alternativos que protegen la privacidad.

•Antes de instalar una aplicación, revisar los accesos y permisos que pide.

SEGURIDAD

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

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. En **https://protege.la/herramientas** encuentra alternativas.

25. 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

26. Canales de comunicación cifrados
Desde los equipos nos comunicamos a través de mensajería web, correo, llamadas y videollamadas; para que la información que comparten sea transmitida de forma segura, es importante que elijan canales cifrados de extremo a extremo (E2EE).

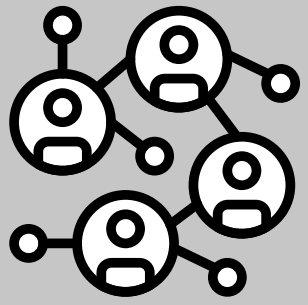
Cifrado de extremo a extremo significa que solo tú y la persona con la que te estás comunicando pueden acceder a tus mensajes o archivos, lo que garantiza que nadie de por medio (ni el propio proveedor de servicios) accedan a los mismos.

Para navegadores y escritorio utiliza aplicaciones con cifrado auditado y que sean transparentes en su funcionamiento.

27. Correo cifrado
Como parte de los acuerdos con las personas de tu equipo, cuiden 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 necesitan, elijan canales con cifrado de extremo a extremo, o usen cuentas de terceros como Gmail por ejemplo con mensajes cifrados. Para cifrar correos pueden utilizar PGP directamente o apoyarse en herramientas gráficas de terceros que hacen su uso más sencillo.

Como mencionamos al inicio, revisa estos consejos relacionados a equipos con tus compañerxs y hazlos parte de tu plan o protocolo de seguridad de la organización :)
Recuerda que las opciones de herramientas para dispositivos están en: **https://protege.la/herramientas/#equipos-de-computo**

REDES



Aquí vamos a revisar las actividades periódicas relacionadas a administración de redes alámbricas e inalámbricas.

En esta sección, los consejos están enfocados a: routers y módem, puntos de conexión a wi-fi y equipos conectados en red.

ADMINISTRACIÓN

Herramientas: Todas las herramientas recomendadas de esta sección las puedes encontrar en: **https://protege.la/herramientas**

CHECKLIST

de seguridad y privacidad digital:
CUENTAS EN LÍNEA

PRIVACIDAD

1. Quienes tienen cuentas en línea ¿Tienen configuradas las opciones de privacidad en sus redes sociales?

☐ **Sí** ☐ **No**

2. ¿Tienen desactivado el registro de actividad que hacen plataformas como Google, Facebook, Apple, Microsoft?

☐ **Sí** ☐ **No**

SEGURIDAD

3. Quienes tienen cuentas en línea ¿Cuentan con contraseñas seguras?

☐ **Sí** ☐ **No**

4. ¿Utilizas un llavero digital para guardar y administrar contraseñas de cuentas en línea?

☐ **Sí** ☐ **No**

5. Quienes tienen cuentas en línea ¿Tienen activada la verificación de dos pasos en las cuentas de correo y redes sociales de la organización?

☐ **Sí** ☐ **No**

6. ¿Mantienes actualizada la gestión y los permisos de las cuentas que tienen acceso a redes sociales? Es decir: revisar quiénes tienen acceso y desvincular las cuentas que no sean necesarias.

☐ **Sí** ☐ **No**

7. ¿Tienes activada las alertas de inicios de sesión o actividad inusual?

☐ **Sí** ☐ **No**

9. ¿Has explorado y probado las herramientas de configuración del panel de control y la consola de servicios (por ejemplo el panel de Google y el de tu hosting)?

☐ **Sí** ☐ **No**

CUENTAS EN LÍNEA

LLegaste a la sección para revisar la administración y configuración de permisos en cuentas en línea. Esto incluye redes sociales, servidores de correo, bases de datos y otros servicios.

Los aspectos que vamos a revisar son:

PRIVACIDAD

SEGURIDAD

Herramientas: Todas las herramientas recomendadas de esta sección las puedes encontrar en: **https://protege.la/herramientas**

CHECKLIST

de seguridad y privacidad digital:
REDES

ADMINISTRACIÓN

1. ¿Has cambiado los valores de fábrica del módem? Por ejemplo el nombre de la red, clave de WiFi, frecuencia en la que trabaja, etc.

☐ **Sí** ☐ **No**

2. ¿Está activada una red de invitadxs a parte de la red que usan personas de la organización o colectivo?

☐ **Sí** ☐ **No**

3. ¿Cambias las contraseñas de red periódicamente? Por ejemplo cada 3 o 6 meses.

☐ **Sí** ☐ **No**

4. ¿Se encuentra desactivado el uso compartido de archivos y dispositivos?

☐ **Sí** ☐ **No**

5. Para impresoras en equipos de trabajo ¿Cualquiera puede acceder al equipo destinado para impresión en red?

☐ **Sí** ☐ **No**

6. Para impresoras en las que se imprime información sensible, ¿el acceso está configurado para las personas que manejen la información?

☐ **Sí** ☐ **No**

7. ¿Utilizas redes alámbricas (es decir cableadas) para los equipos de cómputo?

☐ **Sí** ☐ **No**

8. ¿Cuentas con un diagrama de red actualizado? (Que indique qué equipos se encuentren conectados)

☐ **Sí** ☐ **No**

9. ¿Mantienes un monitoreo del uso de red y del tráfico de información con el fin de observar patrones inusuales?

☐ **Sí** ☐ **No**

10. ¿Se utilizan firewall y elementos de seguridad físicos? Por ejemplo una VPN portátil o una Yubikee (llave de seguridad)

☐ **Sí** ☐ **No**

CONSEJOS PARA PROTEGER

Redes

1. Configuración del módem
Para proteger la redes a las que se conectan, cambia los valores de fábrica de tu router; a menudo los routers vienen configurados de fábrica con información que puede ser encontrada en Internet; por lo que es recomendable cambiar el nombre y contraseña que viene de fábrica, por otra combinación fuerte y única.

2. Red WiFi para invitadxs
Mantén una red WiFi para invitadxs separada de la red principal de trabajo de la organización. Una red WiFi para invitadxs (con su propia contraseña) servirá como puerta para entrar en Internet, pero no para ver archivos compartidos ni acceder a recursos locales; incluso si algún dispositivo invitado tiene un virus, este no se propagara por toda nuestra red.

3. Contraseña de la red
En Internet hay varios manuales que explican cómo robar contraseñas WiFi; para proteger tu red (y ponérselas difícil) cambia la contraseña del router cada 3 o 6 meses.

4. Uso compartido
Desactiva el uso compartido de archivos y dispositivos para evitar filtraciones de datos o que los equipos se encuentren expuestos a ser vistos o analizados en la red.

5. Impresoras en red
Los procesos de impresión también son un aspecto de seguridad a tener en cuenta, por ejemplo, si las impresoras dependen de un equipo de cómputo para imprimir, esto implica tener acceso al equipo y a la información. O si las impresoras están visibles en la red, pueden ser una puerta para posibles ataques.

Para mejorar la seguridad con respecto a las impresoras:

•Revisa su configuración y a qué equipos y redes tienen acceso,

•Cambia la contraseña que viene de serie o fábrica

•Mantén al día las actualizaciones y los servicios que se ejecutan a partir de las impresoras.

6. Impresoras e información sensible
La seguridad además de estar en la red también está en la información. Para proteger la información confidencial o sensible en impresoras compartidas:

•Revisa los accesos

•Revisa la configuración de impresión, por ejemplo la opción manual, donde se imprime el documento cuando se solicita físicamente. Otra opción es un sistema de autenticación donde las personas deben autenticar para liberar la impresión.

•Lleva un control de documentos después de imprimirlos.

•Otra opción es el uso de marcas de agua en documentos, y en el caso de archivos, archivos cifrados.

7. Redes alámbricas
La red alámbrica usa cables que conectan computadoras y otros dispositivos para formar las redes. La instalación y los cables físicos aseguran que solo los equipos deseados se conecten a la red, compartan recursos, se comuniquen entre sí y tengan mayor velocidad.

8. Diagrama de red
Un mapa o diagrama de red es una representación gráfica que te permite conocer qué equipos están conectados y cómo se conectan, incluidos routers, dispositivos, hubs, firewall, etc. El diagrama de red te permite planificar mantenimientos y realizar cambios cuando sea necesario.

9. Monitoreo de red
Monitorear la red ayuda a conocer el rendimiento de la red para detectar y corregir problemas. Esta revisión facilita información sobre el tráfico que fluye a través de la red y los dispositivos, así como cambios sospechosos en velocidad y la conexión de dispositivos no autorizados.
Ten en cuenta:
•Realizar el monitoreo de forma regular y ante cualquier actividad inusual

•Recuerda siempre avisar cuando realices este tipo de actividad en tu organización

•Involucrar a tu equipo para proteger juntxs la red, compartan sobre prácticas de seguridad, privacidad y accesos.

10. Elementos físicos con VPN
Integra a la red elementos de seguridad físicos como: hardware con Firewall, VPN, Yubikey, esto protege equipos e información.