VIGILANCIA DIGITAL

CÓMO PROTEGERTE DEL *CIBERPATRULLAJE*

AMNISTÍA INTERNACIONAL

PROTECCIÓN DE DISPOSITIVOS Y DATOS

USUARIOS/AS EN GENERAL

SI ESTÁS EN PELIGRO DE SUFRIR VIGILANCIA DIGITAL, PODÉS ACTIVAR Y UTILIZAR HERRAMIENTAS Y FUNCIONES ESPECÍFICAS DE TU TELÉFONO Y TUS CUENTAS PARA MEJORAR LA PROTECCIÓN DE TUS DISPOSITIVOS Y TUS DATOS.

¿TE PROTEGE FRENTE A TODO? NO, PERO AYUDA!

ARRANQUEMOS POR LO BÁSICO

PROTOCOLO DEL DEFENSOR – SEGURIDAD DIGITAL

1

Si tienes que compartir información confidencial con quienes trabajan con vos, **hacelo personalmente o mediante herramientas de comunicación que permitan el cifrado de extremo a extremo y la desaparición de los mensajes.**

2

Asegurate de que cualquier computadora o dispositivo móvil que utilices:

a. No permita el acceso físico de personas no autorizadas.

b. Necesite una contraseña o un código de acceso (passcode) para desbloquearse.

c. Esté ejecutando las últimas versiones del sistema operativo y de todas las aplicaciones y el software que tenga instalado.

d. Tenga habilitado el cifrado de disco completo, si es legal en su país (lo es en Argentina).

e. Tenga instalado un antivirus y un cortafuegos que estén actualizados y bien configurados.

f. No esté rooteado ni manipulado y no tenga instalado ningún software pirateado.

g. **Se quede apagado y desconectado siempre que sea posible, no sólo en estado de suspensión o hibernación.**

3

Asegurate de que cualquier servicio online que utilices:

a. Requiera una contraseña compleja y única para acceder.

b. Tenga habilitada la **autenticación de dos factores** (2FA/2SV), si dispone de ella.

4

Utiliza una **VPN centrada en la privacidad** si accedes a Internet a través de una red pública o no fiable.

5

Elimina de forma segura cualquier información confidencial en todas sus formas y variaciones en cuanto ya no sea necesaria, y asegúrate de que no es recuperable.

USUARIOS/AS DE ALTO RIESGO

DETERMINADOS USUARIOS/AS PODRÍAN CORRER MAYOR PELIGRO DE SUFRIR VIGILANCIA DIGITAL DEBIDO A SU PERFIL O SU ACTIVIDAD. LOS IPHONES, LOS DISPOSITIVOS ANDROID Y LOS SERVICIOS ONLINE DISPONEN DE HERRAMIENTAS Y FUNCIONES DE PROTECCIÓN PARA USUARIOS/AS DE ALTO RIESGO.

TENÉ EN CUENTA QUE ESTA LISTA NO PRETENDE SUSTITUIR A LA EVALUACIÓN Y FORMACIÓN FORMALES EN MATERIA DE RIESGOS PARA LA SEGURIDAD DIGITAL Y DE LA INFORMACIÓN.

COMPRUEBA CON FRECUENCIA EL INFORME DE PRIVACIDAD DE LAS APLICACIONES

El Informe de privacidad de las aplicaciones muestra las aplicaciones que recopilan datos confidenciales. Desactiva o elimina las aplicaciones que ya no utilizas.
Las empresas de vigilancia compran datos de ubicación a empresas de publicidad para poder llevar a cabo una vigilancia selectiva.

⚙ **Ajustes > Privacidad y seguridad > Informe de privacidad de las apps**

ACTIVA EL MODO DE AISLAMIENTO

El **modo de aislamiento** es una función de protección reforzada que Apple introdujo a raíz de las revelaciones del **Proyecto Pegasus en 2021** (el Laboratorio sobre Seguridad de Amnistía Internacional colaboró técnicamente en esta investigación). Evita muchas formas de ataques avanzados y debe estar activado en los iPhones y dispositivos Apple que pertenezcan a usuarios/as en situación de riesgo.

⚙ **Ajustes > Privacidad y seguridad > Modo de aislamiento (abajo) > Activar**

DESACTIVA LA FUNCIÓN DE LOCALIZACIÓN Y ELIMINA LAS UBICACIONES SIGNIFICATIVAS

La **función de localización** permite a las aplicaciones y sitios web usar información de diversos tipos de redes para determinar tu ubicación aproximada o exacta. Si eres un usuario/a de alto riesgo, puedes desactivar la función de localización en tus dispositivos y eliminar tus ubicaciones significativas.

⚙ **Función de localización: Ajustes > Privacidad y seguridad > Localización > Desactiva la función de compartir la ubicación**

⚙ **Ubicaciones significativas: Ajustes > Privacidad y seguridad > Localización > Servicios del sistema > Ubicaciones significativas > Borrar historial**

ACTIVA LA PROTECCIÓN EN CASO DE ROBO

La **protección en caso de robo del dispositivo** añade una capa de seguridad cuando tu iPhone no está en un lugar conocido, como tu casa o el trabajo, y ayuda a proteger tus cuentas y tu información personal si te lo roban, pues evita que se lleven a cabo operaciones críticas.

⚙ **Ajustes > Face ID y código > Protección en caso de robo del dispositivo***

*Para utilizar la protección en caso de robo del dispositivo, debes utilizar autenticación de doble factor (2FA) para tu ID de Apple, configurar un código de dispositivo, autenticación de Face ID o Touch ID y activar Ubicaciones significativas y Buscar (Find My).

DESACTIVA LA INSTALACIÓN DE APLICACIONES DE ORIGEN DESCONOCIDO

La mayoría de los programas espía para Android se implantan mediante aplicaciones maliciosas que se instalan fuera de Play Store. Al desactivar esta función se evita la instalación de aplicaciones externas.

Ajustes > Seguridad > desmarca la opción "Aplicaciones de origen desconocido"

ACTIVA LA NAVEGACIÓN SEGURA MEJORADA

Google Chrome ofrece la función opcional **Navegación segura mejorada** para rastrear los enlaces y el historial del navegador en busca de *phishing*, software malicioso y ataques selectivos avanzados. Esto supone enviar a Google información adicional sobre tu actividad de navegación en Internet, pero puede ayudar a proteger tu dispositivo frente a nuevas amenazas.

Chrome > Más (puntos de la esquina superior derecha) > Configuración > Privacidad y seguridad > Seguridad > Navegación segura > "Protección mejorada"

ACTIVA USAR SIEMPRE CONEXIONES SEGURAS

Algunos ataques avanzados pueden desencadenarse al navegar por una página web no encriptada. Este riesgo puede reducirse activando la opción **Usar siempre conexiones seguras** en Chrome.

Chrome > Más (puntos de la esquina superior derecha) > Configuración > Privacidad y seguridad > Seguridad > "Usar siempre conexiones seguras"

EJECUTA UNA COMPROBACIÓN DE SEGURIDAD EN TU DISPOSITIVO ANDROID

Google Chrome en Android ofrece una **función de comprobación de seguridad** que confirma que tu navegador y tus cuentas están a salvo de amenazas comunes (incluidas contraseñas vulneradas), que tu estado de navegación segura y si hay disponibles actualizaciones de Chrome.

Chrome > Más (puntos de la esquina superior derecha) > Configuración > Comprobación de seguridad > "Comprobar ahora"

SERVICIOS ONLINE

ACTIVA LA AUTENTICACIÓN DE DOS FACTORES (2FA) EN LAS CUENTAS ONLINE

Activa la autenticación de dos factores (2FA) en todas las cuentas y servicios online que lo permitan (ver directorio 2fa.). Es más seguro utilizar una aplicación 2FA (como Microsoft Authenticator, Aegis, Authy) o una llave de seguridad física (por ejemplo, Yubikey) que un SMS.

Asegúrate de comprobar con frecuencia tus direcciones o números de teléfono de recuperación de correo electrónico, pues también podrían utilizarse maliciosamente.

REVISA LA CONFIGURACIÓN DE PRIVACIDAD DE TUS CUENTAS DE REDES SOCIALES

Los perfiles y las conexiones de las redes sociales pueden ser aprovechados para llevar a cabo actividades maliciosas, como vigilancia virtual y física, revelación de datos personales (***doxing***), recopilación de datos, hackeo y difamación. Reduce al mínimo los datos personales que compartes en las redes sociales, mantén privadas tus cuentas siempre que sea posible y desactiva la visibilidad de cuentas a través de motores de búsqueda.

ACTIVA LA AUTENTICACIÓN DE DOS FACTORES (2FA) EN LAS APLICACIONES DE MENSAJERÍA Y UTILIZA LA DESAPARICIÓN DE MENSAJES

Las aplicaciones de mensajería, como **WhatsApp y Signal** son fundamentales para comunicarnos. Ambas ofrecen cifrado de extremo a extremo y una función de autenticación de dos factores (2FA) o bloqueo de registro para evitar que un atacante con acceso a tus mensajes secuestre tus cuentas y suplante tu personalidad.

Algunas aplicaciones ofrecen como función opcional la desaparición de mensajes para mayor privacidad, que garantiza que tu mensaje desaparece tras un tiempo determinado, salvo que se guarde.

USA UN ADMINISTRADOR DE CONTRASEÑAS

La reutilización de contraseñas es la manera más sencilla en que un atacante puede poner en peligro una cuenta personal o de una organización. Miles de millones de combinaciones de correos electrónicos y contraseñas se han filtrado públicamente, y probablemente tu contraseña favorita ya está publicada (véase **Have I Been Pwned?**).

Usa un administrador de contraseñas, que crea una contraseña específica para cada cuenta: KeepassXC, 1Password o BitWarden son buenas opciones.

CHECK-LIST

¿QUÉ TAN SEGURO ESTÁS EN LA WEB?

1 USO CONTRASEÑAS ÚNICAS PARA CADA UNA DE MIS CUENTAS

☐

⟶ Usar contraseñas únicas y difíciles (con una mezcla de letras, números y símbolos) para cada cuenta es esencial para evitar que un atacante acceda a múltiples cuentas si una se ve comprometida. Te recomendamos usar un administrador de contraseñas que guarde todas tus contraseñas en un lugar seguro y te ayude a crear una contraseña diferente y fuerte para cada cuenta.

2 TENGO ACTIVADA LA AUTENTICACIÓN EN DOS PASOS (2FA)

☐

⟶ La autenticación en dos pasos nos pide identificarnos dos veces de manera distintas por lo que añade una capa adicional de seguridad.

3 VERIFICO Y LIMITO LA INFORMACIÓN DE CARÁCTER PERSONAL QUE COMPARTO EN REDES SOCIALES

☐

⟶ Compartir demasiada información personal en redes sociales puede exponerte a riesgos como el doxing (revelación de información privada) y la vigilancia.

4 ELIMINO Y DESINSTALO LAS APPS QUE NO USO

☐

⟶ Las aplicaciones que no usas pueden seguir accediendo a tus datos personales o ejecutándose en segundo plano sin que te des cuenta.

5 TENGO MI DISPOSITIVO ACTUALIZADO CON LAS ÚLTIMAS VERSIONES DE SOFTWARE

☐

⟶ Mantener tu dispositivo y aplicaciones actualizados es clave para protegerte contra vulnerabilidades que los atacantes podrían explotar. Los desarrolladores de software trabajan constantemente para detectar y neutralizar amenazas de seguridad.

6 SIEMPRE APAGO MI COMPUTADORA CUANDO NO LA ESTOY USANDO, EN LUGAR DE SOLO DEJARLA EN SUSPENSIÓN

☐

⟶ Cuando un dispositivo está completamente apagado, es mucho más difícil para cualquier atacante remoto acceder a él: a sus datos, cámaras y micrófonos.

CHECK-LIST ¿QUÉ TAN SEGURO ESTÁS EN LA WEB?

7 ☐ **MONITOREO EL USO DE LA LOCALIZACIÓN POR PARTE DE MIS DISPOSITIVOS**

→ Tener activada la localización permite a las apps y sitios web usen información de distintos tipos de redes para determinar tu ubicación aproximada o exacta. Solo activá el servicio de localización cuando realmente lo necesites. Esto evita que las aplicaciones y servicios rastreen tu ubicación de forma continua.

→ Por otro lado, verifica qué aplicaciones tienen acceso a tu ubicación y ajusta sus permisos. Solo concede acceso a las aplicaciones que realmente necesitan saber dónde estás.

8 ☐ **USO UNA VPN CUANDO ME CONECTO A REDES PÚBLICAS O NO CONFIABLES**

→ Una VPN (Red Privada Virtual) cifra tu conexión a Internet, protegiendo tus datos cuando te conectas a redes públicas o no confiables, como las de cafeterías o aeropuertos.

9 ☐ **LEO Y ENTIENDO LOS PERMISOS QUE OTORGAN LAS APLICACIONES ANTES DE INSTALARLAS**

→ Algunas aplicaciones solicitan permisos que pueden acceder a información sensible o innecesaria. Es fundamental revisar estos permisos para proteger tu privacidad.

10 ☐ **REVISO PERIÓDICAMENTE MI CONFIGURACIÓN DE PRIVACIDAD EN REDES SOCIALES Y APLICACIONES**

SI DISTE CHECK EN ENTRE 7 Y 10 AFIRMACIONES: ¡Excelente! Tenes un fuerte control sobre tu seguridad en la web y tomas medidas proactivas para proteger tu información. Convertite en promotor/a de la seguridad online y acompañá a otras personas a que puedan completar esta lista.

SI MARCASTE ENTRE 4 Y 7: Estás en buen camino, pero hay áreas donde podes mejorar para aumentar tu seguridad. ¡Vamos por más!

SI MARCASTE ENTRE 1 Y 4: No te amargues, todos/as pasamos por esto alguna vez. Considerá revisar y mejorar tus hábitos de seguridad en la web para protegerte mejor.

AMNISTÍA
INTERNACIONAL