SEGURIDAD MÍNIMA PARA TU CELULAR Y PC

Guía práctica 2026 para reducir riesgos sin ser especialista

12 revisiones esenciales + checklist + señales de fraude + plan de acción de 30 minutos

InterNEXOS · Tecnología que te conecta. Seguridad que te protege.

1. ¿Por qué empezar por tu celular y PC?

El celular concentra correo, WhatsApp, banca, fotografías, códigos de autenticación, archivos y acceso a sistemas de trabajo. La PC suele contener sesiones abiertas, documentos, contraseñas y datos de clientes. Perder el equipo es solo uno de los riesgos: también existen robo de cuentas, phishing, aplicaciones maliciosas, contraseñas reutilizadas y respaldos que nunca se probaron.

La idea clave es la defensa por capas: actualización + bloqueo + autenticación + respaldo + hábitos. Si una capa falla, las demás ayudan a limitar el daño.

2. Las 12 revisiones esenciales

1. Actualiza sistema y aplicaciones

Activa actualizaciones automáticas cuando sea posible. Revisa el sistema operativo, navegador, Office, aplicaciones de mensajería y cualquier programa que maneje información importante.

2. Configura un bloqueo fuerte

Usa PIN o contraseña y biometría. Evita 1234, fechas de nacimiento y patrones fáciles. Configura un tiempo de bloqueo automático razonablemente corto.

3. Activa MFA / verificación en dos pasos

Empieza por tu correo principal, banca, nube, redes sociales y cuentas de trabajo. El segundo factor reduce el impacto de una contraseña robada.

4. Deja de reutilizar contraseñas

Cada servicio importante debe tener una clave distinta. Un gestor de contraseñas facilita crear credenciales largas y únicas sin memorizarlas todas.

5. Revisa permisos de apps

Comprueba cámara, micrófono, ubicación, contactos, SMS y archivos. Una calculadora no debería necesitar tus contactos; una app que no usas no debería conservar permisos indefinidamente.

6. Instala solo desde fuentes confiables

En Android mantén Google Play Protect activo. Desconfía de APK enviados por WhatsApp, SMS o páginas que piden desactivar protecciones.

7. Comprueba antivirus y firewall

En Windows abre Seguridad de Windows. Revisa Protección contra virus y amenazas, Firewall y protección de red, y cualquier alerta que indique acciones pendientes.

8. Prepara localización y bloqueo remoto

Activa las funciones de localización/recuperación antes de perder el equipo. En Android compatible, revisa también las opciones de protección antirrobo.

9. Oculta información sensible en la pantalla bloqueada

Los mensajes pueden revelar códigos MFA, clientes, correos o conversaciones sin desbloquear el teléfono. Configura qué muestran las notificaciones.

10. Haz respaldos y prueba recuperarlos

Copia la información importante en una ubicación separada y verifica periódicamente que puedas restaurarla. Un respaldo que nunca se probó puede fallar cuando más se necesita.

11. Reconoce el phishing

Urgencia, miedo, premios, facturas inesperadas, cambios bancarios, QR desconocidos y solicitudes de instalar software son señales para detenerte y verificar por otro canal.

12. Protege la recuperación de tus cuentas

Revisa correo/teléfono de recuperación, dispositivos con sesión abierta y códigos de respaldo. Tu correo principal suele ser la llave para recuperar muchas otras cuentas.

3. Android: qué revisar

Seguridad y privacidad: Android muestra alertas, recomendaciones, estado de actualizaciones, bloqueo del dispositivo, seguridad de cuenta y permisos. En versiones recientes suele estar en Ajustes > Seguridad y privacidad.

Google Play Protect: revisa aplicaciones al instalarlas y analiza periódicamente el dispositivo en busca de comportamiento potencialmente dañino. Conviene mantenerlo activado.

Protección antirrobo: en dispositivos Android compatibles existen funciones para detectar robo y bloquear el teléfono. La disponibilidad depende de versión y modelo.

Permisos: revisa aplicaciones con acceso a cámara, micrófono, ubicación, contactos y archivos; retira permisos que ya no sean necesarios.

Consejo: no cambies configuraciones que no entiendas solo por seguir una lista. Si el teléfono es corporativo, respeta primero las políticas de la empresa.

4. Windows: qué revisar

Seguridad de Windows: abre la aplicación y comprueba que no existan advertencias que requieran acción. Revisa protección contra virus y amenazas, seguridad de cuenta, firewall y protección de red.

Firewall: Windows Firewall filtra tráfico de red y ayuda a bloquear accesos no autorizados. No lo desactives para “hacer funcionar” una aplicación sin entender antes la causa.

Actualizaciones: instala actualizaciones del sistema y aplicaciones. Reiniciar cuando corresponde también forma parte del proceso de actualización.

Cuenta: activa MFA en la cuenta de correo o Microsoft que uses para recuperar accesos y evita trabajar habitualmente con privilegios administrativos si no son necesarios.

Respaldos: identifica qué carpetas contienen información realmente crítica y comprueba que estén respaldadas fuera del equipo.

5. Phishing y fraude: cinco señales para detenerte

Si aparece cualquiera de estas señales, no respondas desde el mismo mensaje. Busca el teléfono o sitio oficial por tu cuenta y verifica. Nunca compartas un código MFA con alguien que te llame o escriba.

Una regla especialmente útil para empresas: cualquier cambio de cuenta bancaria de un proveedor debe confirmarse por un segundo canal conocido antes de pagar.

6. Checklist de 30 minutos

Tiempo	Área	Acción
Min 0-5	Actualizaciones	Revisa actualizaciones del celular, PC, navegador y aplicaciones críticas.
Min 5-10	Acceso	Comprueba PIN/contraseña, biometría, bloqueo automático y MFA en el correo principal.
Min 10-15	Apps	Revisa permisos de cámara, micrófono, ubicación, contactos y archivos.
Min 15-20	Protección	Comprueba Play Protect / Seguridad de Windows y firewall.
Min 20-25	Recuperación	Revisa localización, bloqueo remoto, correo/teléfono de recuperación y sesiones abiertas.
Min 25-30	Respaldos	Confirma que tus archivos importantes tienen copia y que sabes cómo recuperarla.

7. ¿Cuándo deja de ser suficiente una guía?

En una empresa, la seguridad deja de ser solo una configuración personal cuando existen varios usuarios, correo corporativo, servidores, bases de datos, accesos remotos, información de clientes o equipos compartidos. En ese punto conviene documentar inventario, responsables, políticas, respaldos, permisos, altas/bajas de usuarios y respuesta a incidentes.

InterNEXOS puede ayudar a revisar el entorno y priorizar mejoras sin convertir la seguridad en una colección de herramientas aisladas.

Checklist imprimible

- ■ Mi sistema y aplicaciones están actualizados
- ■ Uso bloqueo fuerte y biometría
- ■ MFA está activo en correo y cuentas críticas
- ■ No reutilizo contraseñas importantes
- ■ Revisé permisos de aplicaciones
- ■ Play Protect / Seguridad de Windows no muestran alertas críticas
- ■ Firewall está activo
- ■ Localización/bloqueo remoto están configurados
- ■ Oculté notificaciones sensibles
- ■ Tengo respaldo reciente
- ■ Probé recuperar al menos un archivo
- ■ Sé reconocer solicitudes sospechosas de códigos o acceso remoto
- ■ Mis datos de recuperación están actualizados
- ■ Eliminé sesiones/dispositivos que ya no uso

¿Quieres revisar la seguridad de tu empresa?

InterNEXOS · ventas@internexos.mx
WhatsApp (477) 779.7128 · (477) 188.2468
internexos.mx/contacto/