

# SEGURIDAD PARA TELÉFONO ANDROID

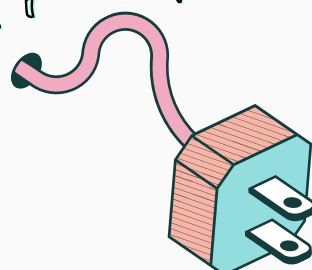


SE REFIERE A LAS MEDIDAS Y ACCIONES QUE PROTEGEN TU DISPOSITIVO Y LOS DATOS ALMACENADOS EN ÉL DE AMENAZAS EXTERNAS COMO VIRUS, MALWARE, HACKERS Y ACCESOS NO AUTORIZADOS.

## Importancia

La seguridad de tu teléfono Android es fundamental para mantener tus datos a salvo y disfrutar de una experiencia móvil segura y sin preocupaciones.

## Tips Aquí



- Mantén tu sistema operativo y aplicaciones actualizados: Las actualizaciones suelen incluir parches de seguridad que corrigen vulnerabilidades
- Utiliza contraseñas fuertes y únicas: Crea contraseñas seguras y diferentes para cada cuenta
- Instala una aplicación antivirus: Una buena aplicación antivirus puede detectar y eliminar malware de tu dispositivo.
- Habilita el bloqueo de pantalla: Utiliza un patrón, PIN o huella digital para bloquear el acceso a tu teléfono.
- Revisa los permisos de las aplicaciones: Antes de instalar una aplicación, revisa los permisos que solicita y concede solo los necesarios



## Ventajas

- Protección de datos personales: Tus fotos, mensajes, contactos y otra información sensible se mantienen a salvo de accesos no autorizados.
- Prevención de fraudes: Reduce el riesgo de que alguien utilice tu teléfono para realizar compras o transacciones bancarias sin tu consentimiento.
- Funcionamiento óptimo: Un dispositivo seguro suele funcionar de manera más fluida y sin interrupciones causadas por malware o virus.
- Tranquilidad: Saber que tus datos están protegidos te brinda una mayor sensación de seguridad y confianza.
- Cumplimiento normativo: En algunos ámbitos, la seguridad de los dispositivos móviles es un requisito legal para proteger información confidencial

## Desventajas

- Complejidad: Configurar y mantener un sistema de seguridad completo puede resultar abrumador para algunos usuarios.
- Rendimiento: Algunas medidas de seguridad, como el cifrado de datos, pueden consumir más recursos del dispositivo y afectar ligeramente su rendimiento.
- Falsos positivos: Los sistemas de seguridad pueden ocasionalmente bloquear aplicaciones o sitios web legítimos, generando falsas alarmas.
- Costo: Algunas aplicaciones de seguridad de terceros son de pago y pueden representar un gasto adicional.
- Vulnerabilidades: A pesar de las medidas de seguridad, siempre existe la posibilidad de que se descubran nuevas vulnerabilidades en el sistema operativo o en las aplicaciones.



GOBERNACIÓN DEL ESTADO BOLIVARIANO DE  
**Mérida**

**Jehyson Guzmán**  
GOBERNADOR