

# Configuración segura de dispositivos ANDROID



Fije un código robusto de acceso al dispositivo (al menos 8 caracteres).



Establezca el bloqueo automático de la pantalla, evitando utilizar el Smart Lock.



Mantenga el dispositivo y las apps actualizadas.



Desinstale las apps que no se estén utilizando.



Desactive las interfaces de Wi-Fi y Bluetooth si no se están empleando.



Evite la conexión a redes Wi-Fi abiertas.



Limite los permisos otorgados a las aplicaciones (localización, micrófono, contactos, etc.), prestando especial atención al permiso especial "administrador de dispositivo".



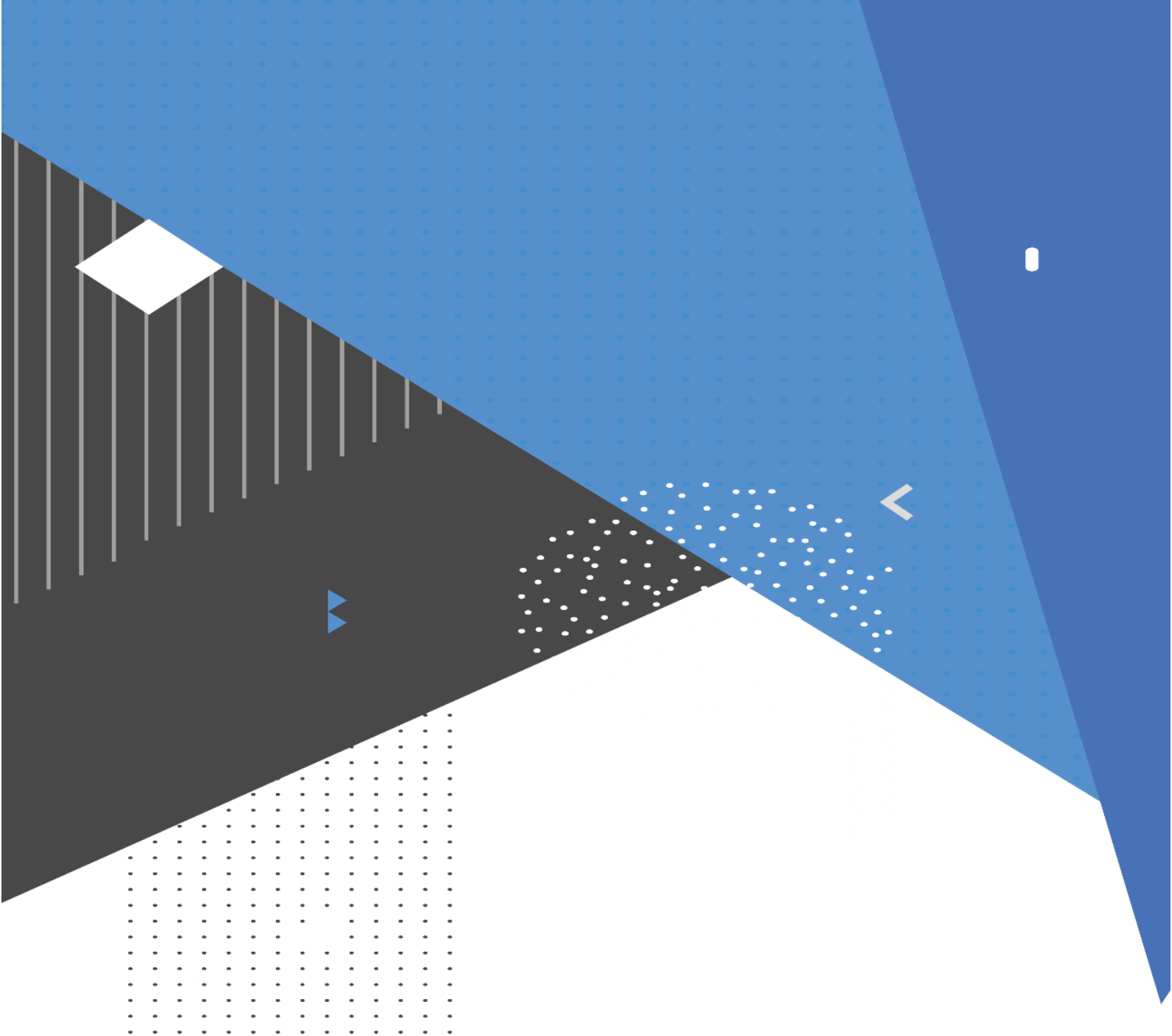
Bloquee la instalación de aplicaciones desconocidas.



Limite el acceso a la información en la pantalla de bloqueo, desactive el asistente de voz, elimine los ajustes rápidos sensibles y oculte las notificaciones.



Proteja la cuenta de usuario de Google con contraseña robusta y exclusiva y habilite el segundo factor de autenticación.



centro criptológico nacional