MECANISMOS DE BLOQUEO DE UN DISPOSITIVO

CUENTAS DE USUARIO Y MEDIDAS DE PROTECCIÓN

Sistema operativo	Tipos de cuentas de usuario	Tipos de bloqueo permitidos	Características de seguridad adicionales
Windows 11	Administrador Estándar Invitado	PIN, Contraseña (*****) Huella digital (Windows Hello) Reconocimiento facial (Windows Hello)	Cifrado de datos Antivirus integrado (Windows Defender) Bloqueo remoto Soporte para 2FA
macOS Sonoma	Administrador Estándar Invitado (Solo compartir / Grupo)	Contraseña (*****) Touch ID (si el Mac o el teclado lo incorpora)	Cifrado de datos Bloqueo remoto (Find My Mac) Soporte para 2FA
iOS	Estándar	Código, Contraseña (*****) Huella dactilar (Touch ID en iPhone 8 y modelos anteriores) Reconocimiento facial (Face ID a partir de iPhone X y iPad Pro de 11 pulgadas)	Cifrado de datos Bloqueo remoto (Find My iPhone) Soporte para 2FA
Android	Usuario Invitado Perfil restringido (solo para tablets)	PIN, Contraseña (*****) Patrón Reconocimiento facial Huella dactilar (en función del fabricante del dispositivo y la versión de Android instalada, estarán disponibles unos mecanismos u otros)	Cifrado de datos Bloqueo remoto mediante (Find My Device) Soporte para 2FA

RECOMENDACIONES DE SEGURIDAD ADICIONALES AL CONFIGURAR CUENTAS DE USUARIO

Configura contraseñas fuertes y únicas.

Habilita la autenticación de dos factores (2FA) siempre que sea posible.

Selecciona adecuadamente el tipo de cuenta para cada usuario que haga uso del dispositivo.

Mantén el software y las aplicaciones actualizadas para evitar vulnerabilidades.

www.incibe.es/ciudadania

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta