Las Últimas Noticias
17/10/2024 Audiencia: 271.020 Sección: OCIO Y TIEMPO LIBRE
$3.985.937 Tirada: 91.144 Frecuencia: DIARIO
$4.399.200 Difusión: 91.144
$4.399.200 Ocupación: 90,61%

Google presenta seis nuevas funciones antirrobo: aprenda a activarlas en el teléfono

¿Usa Android? Ahora su celular se bloquea si se lo quitan de las manos

También mejora el sistema para bloquear a distancia un dispositivo que cayó en manos ajenas.

Valentina Espejo

Fotos y videos, acceso a cuentas bancarias, contraseñas, emails y mensajes de WhatsApp: esos son sólo algunos de los datos confidenciales sensibles que almacena cualquier celular. Bloquear el acceso a esa información es crucial cuando una persona sufre el robo o extravío de su dispositivo.

En un contexto de alerta mundial por el masivo robo de celulares, llegan buenas noticias: Google estrenó en Android seis nuevas funciones de protección antirrobo, las que deben ser habilitadas por el usuario en la configuración del aparato. Las primeras tres están disponibles para Android 10 y versiones posteriores; las restantes funcionan solo con Android 15, la última versión del sistema operativo.

1. Bloqueo por detección de robo: Bloquea automáticamente el teléfono si interpreta un movimiento brusco como robo. Alejandra Bonati, gerente de Comunicaciones de Google Chile, explica que el sistema usa "inteligencia artificial (IA) y sensores de movimiento para detectar cuando alguien te quita el teléfono de la mano y sale corriendo, en bici o en auto. Cuando eso ocurre, se bloqueará la pantalla para proteger su contenido". Esto ocurre tanto si el aparato está bloqueado o desbloqueado.

Rafael Cereceda, profesor de la Facultad de Ingeniería y Ciencias de la Universidad Adolfo Ibáñez (UAI), explica que "los teléfonos inteligentes contienen un sensor llamado acelerómetro que detecta cambios en la velocidad del dispositivo: este sensor puede identificar patrones de movimiento, como caminar o subir escaleras, utilizando modelos de inteligencia artificial".

Agrega que "cuando te quitan un teléfono de la mano, ocurre un movimiento desde cero a muy alta velocidad; el mismo sensor del teléfono reconoce ese patrón de movimiento y entiende que es un robo, considerando la posición y un montón de otros parámetros".

Para activar las funciones de protección antirrobo hay que ir a **Ajustes**, seleccionar **Google**, abrir **Todos los Servicios** y activar **Protección Antirrobo**.

2. Bloqueo de dispositivo sin conexión: "Poco después de que el dispositivo se queda sin conexión, esta función bloquea automáticamente la pantalla para proteger tus datos. Por ejemplo, si alguien te roba el teléfono y desactiva la conexión a internet para que no puedas encontrarlo con la función 'Encontrar mi Dispositivo' (o active el Modo Avión), el dispositivo se bloqueará después de estar sin conexión durante un breve periodo", describe Bonati. Para activar esta herramienta, en el menú Protección Antirrobo hay que activar **Bloqueo del Dispositivo sin Conexión**.

3. Bloqueo por autenticación fallida: Bloquea la pantalla del teléfono después de cinco intentos consecutivos de autenticación sin éxito al iniciar sesión en aplicaciones o funciones del sistema operativo protegidas.

4. Bloqueo remoto: Si el usuario pierde o le roban su celular Android, este sistema lo ayudará a protegerlo rápidamente. Incluso si no recuerda la contraseña de su cuenta de Google, puede usar cualquier otro dispositivo para visitar **Android.com/lock** y bloquear su teléfono solo con un número verificado. Esta herramienta protege el dispositivo mientras la persona recupera el acceso a través de Encontrar mi Dispositivo de Android, que le permite asegurar, localizar o borrarlo remotamente.

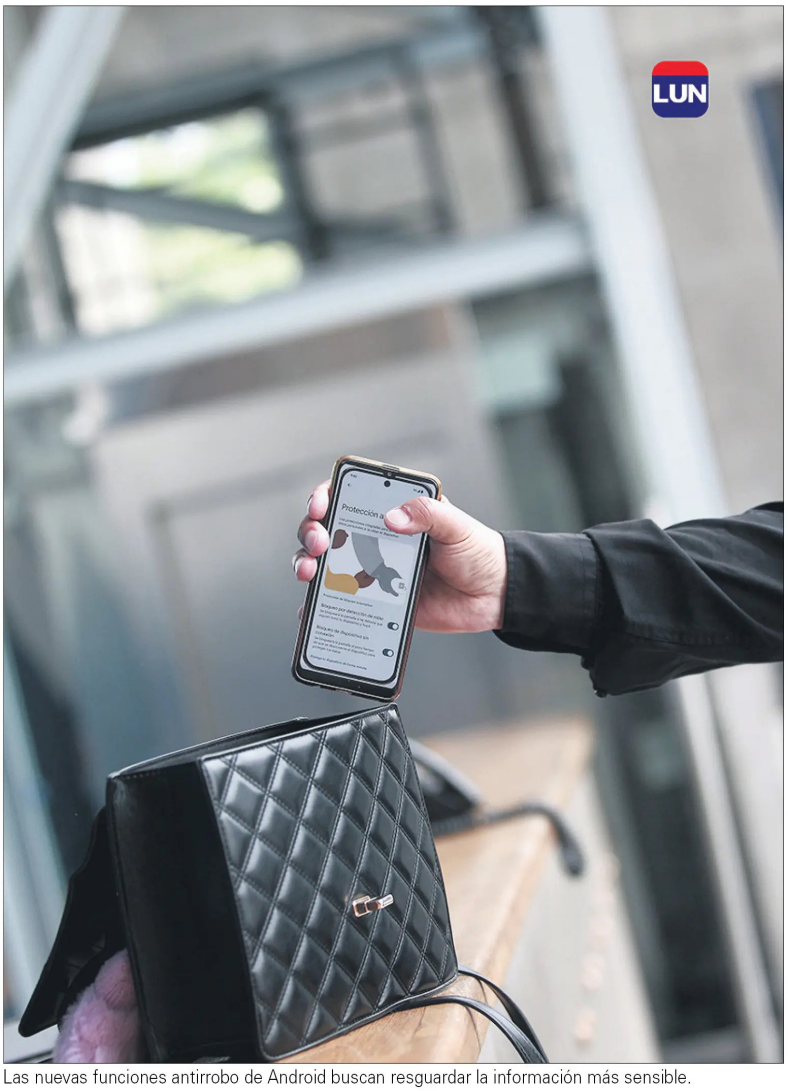
El profesor Cereceda comenta que "en la actualidad se puede bloquear e incluso resetear un teléfono Android remotamente con el famoso Find my Phone; sin embargo, está hecho en base a la cuenta de Google del dispositivo. En este caso se da un salto y se habilita, con ciertas restricciones y permisos para ser usado con el número de teléfono, dado el bloqueo por robo. Es tremendamente útil pues no todos, con el shock del robo, nos acordamos de la clave pero sí nos sabemos el número de teléfono".

5. Restablecimiento de fábrica mejorado: "La protección mejorada hace que sea aún más difícil para los ladrones restablecer el dispositivo robado sin las credenciales de la cuenta de Google del usuario, reduciendo significativamente su valor de reventa y protegiendo sus datos", destaca Bonati.

Según Cereceda, "hay que revisar bien la mejora pues muchas veces la gente se olvida de la cuenta o la clave, y con la doble autenticación en el teléfono se te pide el uso del dispositivo robado para acceder a la cuenta. Podría ser complejo cuando de verdad quieres tú mismo, el dueño del teléfono, restaurarlo de fábrica".

6. Espacio privado: El usuario puede crear un espacio aparte para organizar aplicaciones sensibles, como app sociales, de citas o bancarias. "Es como una caja fuerte digital en el teléfono. Cuando el Espacio Privado está bloqueado, las apps permanecen prácticamente invisibles para los demás y se ocultan de la lista de apps, la vista de aplicaciones recientes, las notificaciones y la configuración", puntualiza Bonati.

Para configurar el Espacio Privado hay que abrir la aplicación **Ajustes del Dispositivo**, tocar **Seguridad y Privacidad**; luego, en Privacidad, tocar **Espacio Privado**; para desbloquearlo, se debe autenticar con el método de desbloqueo de pantalla del dispositivo.



MARIOLA GUERRERO

Las nuevas funciones antirrobo de Android buscan resguardar la información más sensible.

Protección en iPhone

Los usuarios de iPhone también cuentan con herramientas de protección antirrobo, que refuerzan la seguridad cuando el teléfono está lejos de ubicaciones conocidas, como la casa o el trabajo.

-Autenticación biométrica: algunas acciones sensibles, como acceder a contraseñas y tarjetas de crédito guardadas, requieren una autenticación única con Face ID o Touch ID, sin una alternativa de código, para que solo el dueño pueda acceder a estas funciones.

-Espera de seguridad: algunas acciones, como cambiar la contraseña de la cuenta de Apple, también requieren que el usuario espere una hora y realice una segunda autenticación con Face ID o Touch ID.