Seguridad: cuatro consejos prácticos para mantener seguro el celular

20 enero, 2025

Con el objetivo de proteger a la población frente a las ciberestafas, el Ministerio de Seguridad y Justicia brinda medidas preventivas promoviendo la concientización sobre los riesgos digitales.

El Ministerio de Seguridad y Justicia continúa brindando herramientas destinadas a prevenir las ciberestafas y otras modalidades delictivas. En este sentido, especialistas de la cartera han brindado recomendaciones para garantizar la seguridad de los teléfonos celulares.

“El objetivo es concientizar a la población sobre la importancia de la seguridad digital y proporcionar las herramientas necesarias para protegerse contra las ciberestafas”, resaltaron.

Cuatro tips

Bloquear el celular: Emplear un sistema de bloqueo, mediante un PIN, una contraseña o una alternativa biométrica, como podría ser el sensor de huella dactilar o el reconocimiento facial. De esta manera, si el equipo cae en manos de terceros, no podrá ingresar. Usar todas las herramientas que el equipo permita.

Poner PIN a la SIM: Asignarle una contraseña a la SIM (*chip*) permite que, en caso de extravío o robo del equipo, esa SIM no pueda ser colocada en otro aparato y pueda ser usada. Cada vez que se inserta la tarjeta SIM en un teléfono móvil se debe ingresar el código PIN. Cada operadora cuenta con un PIN general y muy fácil de obtener para todas sus tarjetas. Sin embargo, es posible cambiar el código desde la opción de ajustes del propio teléfono. De esta manera, la próxima vez que se encienda el celular solicitará el PIN.

Verificación en dos pasos: En la *app* más usada, es necesario tener una protección que impida su clonación. Para ello, es recomendable habilitar la verificación en dos pasos, que le permitirá blindar su cuenta ante cualquier intento de clonación. Además, cuando se intente instalar esa cuenta en otro aparato, la *app* no lo permitirá porque está activada esa verificación.

Contraseña segura: No debe seguir patrones como 12345, fechas de cumpleaños ni direcciones de los domicilios, como tampoco se recomienda tener las claves de acceso preestablecidas en ningún caso.