

TUS CONTRASEÑAS DEBEN SER:

- **ROBUSTAS**

COMPUESTA POR NÚMEROS, SÍMBOLOS Y UNA COMBINACIÓN DE LETRAS MAYÚSCULAS Y MINÚSCULAS.



Y SE DEBEN:

- **CAMBIAR PERIODICAMENTE**

- **NO COMPARTIRLAS**

Usar contraseñas diferentes para cada billetera virtual o aplicación y activar el doble factor de autenticación para iniciar sesiones.



EN CUANTO A LAS REDES:

- NO ACEPTES LA SUGERENCIA DE GUARDAR LA CONTRASEÑA EN EL NAVEGADOR.

- EVITA REDES DE USO PÚBLICO, DESACTIVA EL BLUETOOTH O NFC.

- VERIFICA QUE LOS REMITENTES DE LOS CORREOS ELECTRÓNICOS RECIBIDOS COINCIDAN CON EL DOMINIO DE LAS ENTIDADES O EMPRESAS.

CON TUS DISPOSITIVOS TOMA LOS SIGUIENTES RECAUDOS

DESACTIVA LA UBICACIÓN,
LA CÁMARA Y EL
MICRÓFONO CUANDO NO
SEAN NECESARIOS.

USA ANTIVIRUS Y ANTIMALWARE.

MANTEN ACTUALIZADO EL
SISTEMA OPERATIVO, EL
NAVEGADOR Y LAS
APLICACIONES.



EN CASO DE FRAUDE PODES:

COMUNICARTE CON LA UNIDAD
FISCAL ESPECIALIZADA EN
CIBERDELINCUENCIA (UFECI).
DIRECCIÓN: SARMIENTO 663, 6°
PISO, CABA
TELÉFONO: (+54 11) 5071-0040 /
0041
CORREO ELECTRÓNICO:
DENUNCIASUFECI@MPF.GOV.AR
SI RECIBÍS INFORMACIÓN O
MENSAJES QUE SIMULAN SER DEL
BANCO CENTRAL PODÉS
REENVIARLOS A AYUDA EN LÍNEA
(AYUDAENLINEA@BCRA.GOB.AR).

CUIDADO

EN EL MOMENTO MENOS
PENSADO PODES SER
VICTIMA DE UNA
ESTAFA.



AQUI UNOS
CONSEJOS, PARA
QUE NO TE
SORPRENDAN