

Kit de Respuesta ante Robo de Identidad

Pasos primeras 72 horas + burós + IRS + reportes + monitoreo continuo

Como usar: si detectas o sospechas robo de identidad, sigue los pasos en orden. Cada hora que pasa entre el descubrimiento y la accion aumenta el dano. Este kit funciona para robos de tarjeta de credito, apertura fraudulenta de cuentas, robo de identidad fiscal, y suplantacion en cuentas gubernamentales.

Fase 1 - Primeras 72 horas

Hora 0-2: (1) Congela credito en Equifax (equifax.com), Experian (experian.com) y TransUnion (transunion.com). Gratis y bloquea apertura de cuentas nuevas.

Hora 2-4: (2) Reporta a la FTC en IdentityTheft.gov. Genera un plan personalizado + una carta oficial (Identity Theft Report) que necesitaras para disputas.

Hora 4-8: (3) Contacta cada institucion financiera afectada (banco, aseguradora, corretaje). Cierra tarjetas y cuentas comprometidas.

Hora 8-24: (4) Presenta reporte policial en tu jurisdiccion local. Solicita numero de caso y copia oficial - los bancos frecuentemente lo requieren.

Hora 24-72: (5) Cambia contraseñas de correo, banca en linea y redes sociales. Activa autenticacion de dos factores en todas las cuentas.

Fase 2 - Semana 1-2

Coloca alerta de fraude en los tres buros de credito (dura 1 ano, gratis, se activa en un buro y se propaga).

Solicita reporte de credito completo de los tres buros gratis en annualcreditreport.com. Marca todas las cuentas fraudulentas.

Envia carta de disputa a cada cuenta fraudulenta con copia del Identity Theft Report de la FTC.

Si robaron identidad fiscal, presenta IRS Form 14039 (Identity Theft Affidavit).

Si robaron identidad para Seguridad Social o beneficios, contacta a la Administracion del Seguro Social (SSA) en oig.ssa.gov.

Contacta al departamento de vehiculos motorizados (DMV) si sospechas robo de identidad para licencias.

Fase 3 - Meses 1-3

Monitorea estados de cuenta bancarios semanalmente durante 3 meses.

Revisa reportes de credito mensualmente durante 3 meses.

Documenta cada llamada, correo y accion en una bitacora con fechas y nombres de agentes.

Confirma que la alerta de fraude sigue activa en los tres buros.

Verifica que la congelacion de credito sigue activa (algunos buros la levantan si no la extiendes).

Revisa cuentas gubernamentales (IRS, SSA, estatales) por actividad no autorizada.

Fase 4 - Monitoreo continuo (12 meses)

Considera suscripcion a servicio de monitoreo de credito (\$10-\$25/mes) durante 1-3 anos.

Servicios comunes: Experian IdentityWorks, Equifax Credit Watch, IdentityForce, Aura, LifeLock. Compara precios y coberturas.

Revisa reporte de credito de los tres buros al menos una vez cada 4 meses (rotando gratuitos en annualcreditreport.com).

Considera bloqueo de credito permanente (mas fuerte que congelacion, requiere PIN para levantar).

Mantenerte alerta a phishing por correo, telefono y mensaje - los ladrones frecuentemente reincidan.

Contactos y numeros clave

FTC IdentityTheft.gov - reporte y plan personalizado

Equifax: (888) 378-4329

Experian: (888) 397-3742

TransUnion: (833) 395-6938

IRS Identity Protection Specialized Unit: (800) 908-4490

SSA Office of Inspector General: (800) 269-0271

National Do Not Call Registry: (888) 382-1222

Prevencion a futuro

[] Congelacion de credito activa permanentemente en los tres buros (levantar solo cuando necesites credito nuevo).

[] Autenticacion de dos factores activada en correo, banca y todas las cuentas criticas.

[] Contraseñas unicas por cuenta usando administrador de contraseñas (1Password, Bitwarden, LastPass).

[] Triturador de papel para documentos con informacion personal antes de tirar.

[] Buzon de correo cerrado con llave o P.O. Box para correspondencia sensible.

[] No compartir nunca numero de Seguro Social por telefono a menos que TU hayas iniciado la llamada.

[] Revisar reporte de credito de los tres buros al menos una vez al ano.

[] No usar la misma contrasena en dos sitios.

El robo de identidad no siempre se resuelve rapido. Casos simples se cierran en 3-6 meses. Casos complejos (identidad fiscal, apertura fraudulenta de multiples cuentas, uso de identidad para crimen) pueden tomar 12-24 meses de seguimiento activo. Mantener la documentacion es critico: sin bitacora ordenada, cada llamada empieza desde cero. La respuesta rapida en las primeras 72 horas reduce el dano tipico en un 80-90%.