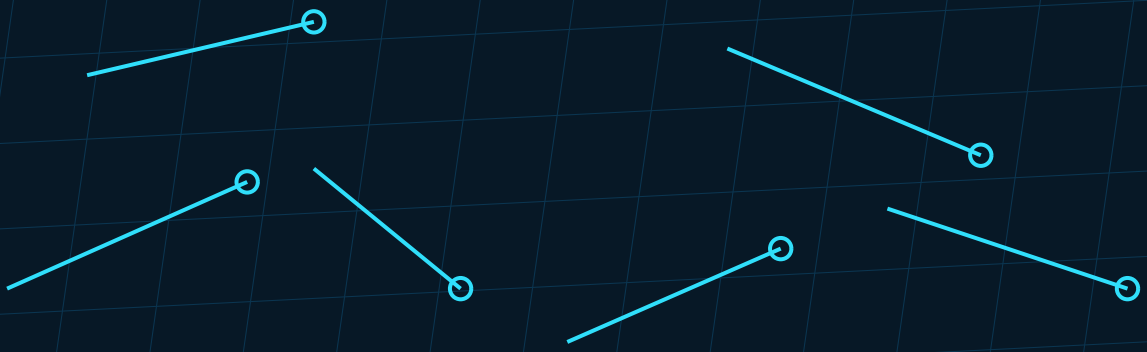

GUIA DEFINITIVA DE ACTUACION ANTE UN HACKEO ROBO DE CUENTA O COMPROMISO

Manual profesional de respuesta, recuperacion y prevencion

Creado por COTNAS

Empresa especializada en ciberseguridad y respuesta ante incidentes

Protocolos paso a paso para cuentas de correo, redes sociales, videojuegos, bancos, criptomonedas y dispositivos.
Incluye arboles de decision, evidencias, denuncias y checklists imprimibles.

Version de trabajo: 02/06/2026

OBJETIVO: recuperar el control sin empeorar el incidente

No compartas codigos, no pagues a falsos soportes, conserva evidencias y usa canales oficiales.

Indice general

Indice ampliado por bloques, sin repetir dentro de cada plataforma apartados como "donde entrar" o "procedimiento paso a paso". Haz clic en cualquier punto para saltar a su pagina.

Indice por tipo de ataque o problema

Usa esta pagina cuando ya sabes que te ha pasado, pero no sabes a que apartado ir.
Los nombres indican el tipo de incidente, no repiten los pasos internos de cada cuenta.

Creditos de la guia

Esta guia ha sido creada por COTNAS como material profesional de divulgacion, formacion y

Entidad creadora

COTNAS - Empresa especializada en ciberseguridad, respuesta ante incidentes y recuperacion de cuentas. Material orientado a la divulgacion y a las buenas practicas de proteccion digital.

El contenido esta orientado a ayudar a usuarios particulares, creadores de contenido, jugadores, pequenas empresas y cualquier persona que necesite actuar de forma ordenada cuando sufre un hackeo, robo de cuenta, phishing, malware, ransomware o compromiso de dispositivos.

Aviso: esta guia no sustituye la asistencia oficial de bancos, plataformas, INCIBE 017, profesionales forenses o Fuerzas y Cuerpos de Seguridad cuando exista fraude economico, extorsion, datos sensibles o delito.

Como usar esta guia

Este documento esta pensado para actuar bajo presion. Cuando una cuenta es robada o un dispositivo esta comprometido, el error mas comun es ir cambiando contrasenas al azar desde el mismo equipo infectado, responder al atacante o seguir enlaces enviados por correo o SMS. La guia ordena la respuesta: primero se contiene el dano, despues se recupera el acceso y finalmente se limpia la causa que permitio el compromiso.

Regla de oro

El correo principal y el telefono son la llave de casi todo. Si el atacante controla el correo de recuperacion, los SMS, la app autenticadora o las sesiones abiertas del navegador, podra volver a robar tus cuentas aunque cambies contrasenas.

El manual mezcla pasos para usuarios no tecnicos con recomendaciones avanzadas. En una emergencia, empieza por el capitulo de los primeros 15 minutos y luego salta directamente al apartado de la plataforma afectada. Si hay dinero, identidad, menores, chantaje, acceso a empresa o datos sensibles, conserva evidencias y contacta con soporte oficial, banco, INCIBE 017 y Fuerzas y Cuerpos de Seguridad.

Situacion	Primera prioridad	Despues
Aun puedo entrar a la cuenta	Cambiar contrasena desde un dispositivo limpio y cerrar sesiones.	Revisar reenvios, reglas, dispositivos, MFA y apps autorizadas.
No puedo entrar	Iniciar recuperacion oficial desde el enlace correcto.	Aportar pruebas de propiedad y evitar formularios falsos.
Hay cargos o transferencias	Bloquear tarjeta/cuenta y avisar al banco inmediatamente.	Descargar movimientos, guardar SMS/correos y denunciar.
Hay malware o keylogger	Desconectar de la red y no introducir mas contrasenas.	Analizar, reinstalar si procede y rotar credenciales desde equipo limpio.
Me robaron el movil	Bloquear SIM, activar modo perdido y cerrar sesiones.	Cambiar contrasenas y bloquear banca/cripto.

1. Como saber si te han hackeado

No todos los incidentes son iguales. Una contrasena reutilizada filtrada en Internet no se gestiona igual que un troyano activo en el ordenador. Antes de correr, identifica el tipo de compromiso. Esta clasificacion ayuda a decidir si basta con recuperar una cuenta o si hay que limpiar el dispositivo completo.

Senales habituales de compromiso

- Avisos de inicio de sesion desde paises, ciudades, dispositivos o navegadores que no reconoces.
- Correos de restablecimiento de contrasena que tu no has pedido.
- Contactos que reciben mensajes tuyos con enlaces, sorteos, inversiones o peticiones de dinero.
- Reglas de correo nuevas, reenvios automaticos, filtros que archivan o borran mensajes de seguridad.
- Publicaciones, videos, directos, anuncios o cambios de perfil que no has realizado.
- Compras, transferencias, intercambios, tradeos de skins o movimientos de criptomonedas no autorizados.
- Antivirus desactivado, extensiones raras, procesos desconocidos, ventanas de login repetidas o consumo inusual de CPU/red.
- La contrasena deja de funcionar y el correo/telefono de recuperacion ya no es el tuyo.
- Codigos 2FA que llegan sin que estes intentando entrar.
- La cuenta aparece limitada, bloqueada o usada para spam.

Diferencias rapidas

Tipo	Que significa	Riesgo principal	Accion clave
Robo de contrasena	Alguien conoce tu clave.	Entrada directa si no hay MFA.	Cambiar clave unica y cerrar sesiones.
Phishing	Metiste datos en una pagina falsa.	El atacante puede tener clave y codigo 2FA.	Cambiar clave y revisar sesiones/aplicaciones.
Robo de sesion/cookies	El atacante usa tu sesion sin saber la clave.	Cambiar clave no siempre basta si la sesion sigue activa.	Cerrar todas las sesiones y revocar tokens.
Malware/infostealer	Un programa robo claves, cookies y archivos.	Robo masivo de cuentas.	Equipo limpio, reinstalacion y cambio escalonado de claves.
SIM swapping	Duplican o portan tu numero.	Reciben SMS de bancos y cuentas.	Operador movil, bloqueo SIM y cambio de MFA a app/passkey.
Robo de identidad	Usan tus datos para altas, prestamos o fraudes.	Dano legal/economico.	Denuncia, bloqueo financiero y vigilancia de cuentas.

No confundas sintoma con causa

Si te han robado Steam, puede que el problema real sea tu correo. Si te han robado Instagram, puede que el problema sea una extension del navegador. Si te han vaciado Revolut, puede que el origen sea una llamada de soporte falso o un movil comprometido.

2. Los primeros 15 minutos

En los primeros minutos el objetivo no es dejarlo todo perfecto, sino cortar el control del atacante y evitar que escale a correo, banco, criptomonedas, redes y dispositivos. Trabaja por prioridades.

Orden de actuacion de emergencia

Minuto	Accion	Detalle practico
0-2	Respira y cambia de dispositivo	Usa otro movil/PC que sepas limpio. No metas claves en el equipo sospechoso.
2-5	Protege el correo principal	Recupera Gmail/Outlook/Yahoo/Proton, cambia contrasena y cierra sesiones.
5-8	Corta dinero y cripto	Bloquea tarjetas, avisa al banco, congela tarjetas virtuales y bloquea exchange si procede.
8-12	Cierra sesiones criticas	Redes, Discord, Steam, consola, cloud, password manager y dispositivos vinculados.
12-15	Guarda evidencias	Capturas con hora, emails, SMS, transacciones, IDs, IPs, nombres de usuario y enlaces.

Que NO hacer

- No respondas al atacante ni negocies si no hay asesoramiento y evidencia preservada.
- No pagues a personas que prometen recuperar cuentas por Telegram, Discord, Instagram o WhatsApp.
- No introduzcas codigos 2FA dictados por telefono ni compartas pantallas con desconocidos.
- No borres correos, chats, registros ni historial antes de documentar el incidente.
- No uses enlaces de un SMS o correo sospechoso; entra siempre escribiendo la web oficial o desde la app oficial.
- No cambies todas las contrasenas desde el ordenador infectado porque el atacante podria capturarlas de nuevo.

Arbol de decisiones rapido

SI todavia tengo acceso al correo principal -> cambio contrasena -> cierro sesiones -> reviso recuperacion, reenvios, filtros y MFA -> despues recupero cuentas secundarias.

SI perdi el correo principal -> uso el formulario oficial de recuperacion desde equipo limpio -> recupero telefono/SIM si hace falta -> aviso a plataformas conectadas y banco -> documento todo.

SI hay dinero o cripto en riesgo -> bloqueo de tarjeta/cuenta/exchange antes de discutir con soporte general -> guardo movimientos -> denuncia si hay cargos o transferencias no autorizadas.

SI sospecho malware -> desconecto el equipo de Internet -> cambio claves desde otro equipo -> clono o preservo evidencias si el caso es grave -> reinstalo o limpio con criterio.

SI el atacante activo esta cambiando datos -> priorizo cierre de sesiones y cambio de MFA -> contacto soporte con asunto urgente: account takeover / hacked account.

3. Protocolo universal de recuperacion

La recuperacion profesional sigue siempre el mismo patron: contener, recuperar, expulsar, revisar, limpiar y prevenir. No basta con cambiar una contrasena. Una cuenta robada suele tener puertas traseras: correo de recuperacion modificado, reglas de correo, aplicaciones OAuth, tokens, sesiones, API keys, dispositivos autorizados y metodos MFA anadidos por el atacante.

Fase 1: contencion

- Trabaja desde un equipo limpio: movil de confianza, PC recien actualizado o navegador en modo seguro sin extensiones.
- Desconecta el equipo sospechoso si hay indicios de malware o control remoto.
- Bloquea tarjetas y pagos si existe cualquier movimiento economico.
- Cambia la contrasena del correo principal antes que las demas cuentas.
- Revoca sesiones, tokens, aplicaciones conectadas y claves API.

Fase 2: recuperacion

- Usa solo formularios oficiales. Busca desde la web oficial o desde el centro de ayuda; evita anuncios patrocinados o enlaces de terceros.
- Aporta datos de propiedad: correos antiguos, facturas, ultimos cuatro digitos de tarjetas, codigos de producto, IDs de usuario, capturas y fechas aproximadas.
- No abras varios tickets contradictorios. Un ticket claro, completo y con pruebas suele funcionar mejor.
- Si el soporte pide verificacion de identidad, usa el canal oficial de la plataforma y no envies documentos por chats no verificados.

Fase 3: erradicacion y cierre de puertas traseras

Elemento a revisar	Por que importa	Ejemplos
Sesiones abiertas	Permiten seguir dentro aunque cambies clave.	Gmail dispositivos, Instagram login activity, Discord devices, Steam Guard.
Reenvios/filtros	Ocultan alertas y copian correos.	Gmail Forwarding, Outlook Rules, Yahoo filters.
Apps autorizadas	Acceso persistente por OAuth/token.	Apps de sorteos, bots Discord, extensiones, herramientas de marketing.
MFA/passkeys	El atacante puede dejar su metodo anadido.	Llaves de seguridad, authenticator, SMS, passkeys, codigos de respaldo.
API keys	Muy critico en Steam, Binance, cloud y servidores.	Steam API key, exchange API, Google Cloud, GitHub tokens.

Fase 4: vuelta a la normalidad

Cuando recuperes la cuenta, no la des por segura hasta revisar actividad y permisos. En redes sociales borra publicaciones y mensajes fraudulentos; en YouTube revisa videos, permisos y AdSense; en bancos descarga extractos; en videojuegos revisa inventario y compras; en cripto conserva TxID y direcciones. Despues avisa a contactos si pudieron recibir estafas desde tu cuenta.

4. Cuentas de correo electronico

Este bloque agrupa varias plataformas del mismo tipo para que el indice sea claro y facil de usar. Dentro se mantienen los pasos concretos por servicio, pero el indice no se llena con cada cuenta individual.

4. Gmail y cuenta Google

Prioridad

La cuenta Google suele ser la llave de Gmail, YouTube, Android, Drive, Fotos, Chrome, passkeys y recuperacion de otras plataformas.

Donde entrar

```
accounts.google.com/signin/recovery | myaccount.google.com/security |
myaccount.google.com/permissions | myaccount.google.com/device-activity
```

Procedimiento paso a paso

- Desde un dispositivo limpio entra en la recuperacion oficial de Google. Contesta con datos reales: contrasenas anteriores, dispositivo habitual, ubicacion habitual y fecha aproximada de creacion si la recuerdas.
- Si aun puedes entrar, ve a Gestionar tu cuenta de Google > Seguridad. Cambia la contrasena por una unica y fuerte.
- En Tus dispositivos, cierra todo lo que no reconozcas. Si un dispositivo no te suena, marca que no lo reconoces y sigue los pasos.
- Revisa Actividad de seguridad reciente y confirma cambios de contrasena, recuperacion, passkeys, MFA o ubicaciones raras.
- Comprueba Telefono y correo de recuperacion. Elimina datos que no sean tuyos y anade los correctos.
- Revisa Verificacion en dos pasos: app autenticadora, llaves de seguridad, passkeys y codigos de respaldo. Regenera codigos si sospechas robo.
- En Gmail revisa Configuracion > Ver todos los ajustes > Reenvio y POP/IMAP, Filtros y direcciones bloqueadas, Cuentas e importacion y Delegacion de correo.
- En Acceso de terceros elimina aplicaciones desconocidas o innecesarias. Revisa tambien Chrome Password Manager si sincronizabas contrasenas.
- Si tienes YouTube, revisa permisos del canal, videos subidos, directos, cambios de nombre, descripcion y AdSense.

Advertencia especifica

Si el atacante cambio telefono y correo de recuperacion, la recuperacion puede tardar. Google valora el dispositivo, red y ubicacion habituales. Repetir intentos desde muchos lugares puede empeorar la confianza del proceso.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

5. Outlook, Hotmail y cuenta Microsoft

Prioridad

Protege Outlook, OneDrive, Windows, Xbox, Office, Teams personal y recuperacion de muchas cuentas externas.

Donde entrar

```
account.live.com/password/reset | account.live.com/acsr | account.microsoft.com/security |
outlook.live.com
```

Procedimiento paso a paso

- Usa Restablecer contrasena si aun tienes metodos de verificacion. Si no, usa el formulario de recuperacion de cuenta Microsoft.
- Rellena el formulario desde una red y equipo usados antes con esa cuenta. Incluye asuntos de correos recientes, contactos y datos de servicios Microsoft si los recuerdas.
- Al recuperar, entra en Seguridad > Opciones avanzadas de seguridad. Cambia contrasena y actualiza informacion de seguridad.
- Cierra sesiones, revisa actividad reciente e inicios de sesion correctos/incorrectos.
- Comprueba metodos MFA: Microsoft Authenticator, SMS, correo alternativo, passkeys y codigos de recuperacion.
- En Outlook revisa Reglas, Reenvio, respuestas automaticas, direcciones conectadas y firmas. Los atacantes suelen crear reglas para ocultar avisos de seguridad.
- Si afecta a Xbox, revisa compras, suscripciones, tarjetas vinculadas y dispositivos de confianza.

Advertencia especifica

Microsoft advierte que soporte no puede enviar enlaces de reseteo ni cambiar datos por ti si no superas la recuperacion. La calidad de las respuestas del formulario es clave.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

6. Yahoo Mail

Prioridad

Aunque se use menos, Yahoo sigue siendo correo de recuperacion de cuentas antiguas, foros, tiendas, juegos y redes.

Donde entrar

```
login.yahoo.com/forgot | login.yahoo.com/account/security | help.yahoo.com
```

Procedimiento paso a paso

- Entra en el asistente de inicio de sesion de Yahoo. Usa correo alternativo o telefono de recuperacion.
- Si puedes entrar, cambia contrasena y revisa la pagina de seguridad de la cuenta.
- Revisa actividad reciente, dispositivos, metodos de recuperacion y Account Key si lo usas.
- En Yahoo Mail comprueba filtros, direccion de respuesta, firma, reenvios, respuesta de vacaciones y nombres de envio.
- Elimina sesiones y apps no reconocidas. Revisa si Yahoo se usaba como correo de recuperacion de otras cuentas y cambia esas credenciales.

Advertencia especifica

Yahoo recomienda revisar ajustes de correo porque un atacante puede cambiar filtros, firma, reply-to o reenvios para seguir recibiendo informacion.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

7. Proton Mail

Prioridad

Proton cifra datos. Recuperar acceso no siempre implica recuperar todos los mensajes si no existian metodos de recuperacion de datos.

Donde entrar

```
account.proton.me | mail.proton.me | proton.me/support/reset-password |
proton.me/support/set-account-recovery-methods
```

Procedimiento paso a paso

- Si aun tienes una sesion iniciada, usa la recuperacion desde cuenta iniciada y cambia la contrasena con cuidado.
- Si estas fuera, usa los metodos de recuperacion configurados previamente: correo, SMS, frase/archivo de recuperacion o dispositivo de confianza.
- Revisa sesiones, 2FA, llaves de seguridad, metodos de recuperacion y dispositivos de confianza.
- Si Proton bloqueo la cuenta por seguridad, sigue el desbloqueo oficial y cambia contrasena cuando lo solicite.
- Despues de resetear, verifica si tus datos cifrados necesitan recuperacion con clave antigua, frase, archivo o dispositivo de confianza.

Advertencia especifica

En servicios cifrados de extremo a extremo, perder la contrasena sin metodos de recuperacion puede impedir descifrar datos antiguos aunque recuperes la cuenta.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

5. Redes sociales y mensajeria

Este bloque agrupa varias plataformas del mismo tipo para que el indice sea claro y facil de usar. Dentro se mantienen los pasos concretos por servicio, pero el indice no se llena con cada cuenta individual.

8. Instagram

Prioridad

Los robos suelen venir por phishing, soporte falso, enlaces de verificacion, sorteos o gestores de seguidores.

Donde entrar

```
instagram.com/hacked | app Instagram > Obtener ayuda para iniciar sesion | Centro de cuentas Meta
```

Procedimiento paso a paso

- Entra en instagram.com/hacked o en la app oficial. Indica que tu cuenta ha sido hackeada.
- Usa el correo o telefono original. Si el atacante cambio el correo, busca el email de Instagram que avisa del cambio y usa la opcion para revertirlo si esta disponible.
- Completa verificacion por video selfie o datos de cuenta cuando Instagram lo pida.
- Al entrar, cambia contrasena, revisa actividad de inicio de sesion y cierra sesiones desconocidas.
- Revisa correo, telefono, cuentas vinculadas, Centro de cuentas, Facebook asociado, metodos 2FA y codigos de respaldo.
- Elimina apps conectadas, publicaciones fraudulentas, enlaces de bio y mensajes enviados.

Advertencia especifica

No confies en perfiles que dicen ser soporte de Instagram. El soporte oficial no te pedira codigos 2FA por DM.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

9. Facebook

Prioridad

Facebook puede tener paginas, anuncios, tarjetas, Business Manager, grupos y acceso a Instagram.

Donde entrar

```
facebook.com/hacked | facebook.com/login/identify | Centro de cuentas Meta
```

Procedimiento paso a paso

- Usa facebook.com/hacked para iniciar el flujo de cuenta comprometida.
- Identifica la cuenta con correo, telefono, nombre o URL del perfil.
- Cambia contrasena, elimina sesiones desconocidas y revisa seguridad e inicio de sesion.
- Revisa correos y telefonos, 2FA, cuentas vinculadas, administradores de paginas y Business Manager.
- Comprueba anuncios activos, metodos de pago, publicaciones, mensajes, Marketplace y actividad de grupos.
- Si se hicieron anuncios o cargos, descarga facturas y contacta soporte de Meta con evidencias.

Advertencia especifica

El atacante suele usar cuentas robadas para anuncios fraudulentos. Bloquea metodos de pago y revisa roles de paginas inmediatamente.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

10. TikTok

Prioridad

Riesgo de perdida de canal, directos, monetizacion, mensajes y vinculaciones a correo/telefono.

Donde entrar

```
support.tiktok.com | App TikTok > Perfil > Menu > Ajustes y privacidad > Reportar un problema
```

Procedimiento paso a paso

- Intenta restablecer contrasena con telefono o correo desde la app oficial.
- Si no puedes entrar, usa Reportar un problema o el centro de ayuda indicando cuenta hackeada.
- Al recuperar, cambia contrasena y revisa correo, telefono y cuentas vinculadas.
- En Seguridad, revisa Gestionar dispositivos y elimina dispositivos desconocidos.
- Activa verificacion en dos pasos y revisa permisos de apps o servicios de terceros.
- Borra videos, enlaces de bio o mensajes fraudulentos y avisa a tus seguidores si recibieron estafas.

Advertencia especifica

Muchos robos de TikTok empiezan con falsos patrocinios o archivos de media kit infectados. Si descargaste algo, trata el equipo como comprometido.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

11. X / Twitter

Prioridad

Puede usarse para estafas cripto, suplantacion, DM masivos, dano reputacional y recuperacion de otras cuentas.

Donde entrar

```
help.twitter.com/forms/account-access/regain-access/hacked-or-compromised | Ajustes > Seguridad y acceso a la cuenta
```

Procedimiento paso a paso

- Usa el formulario oficial para cuenta hackeada o comprometida.
- Si puedes entrar, cambia contrasena y verifica correo/telefono.
- Cierra sesiones desde Apps y sesiones. Revoca aplicaciones conectadas y permisos de API que no reconozcas.
- Activa 2FA con app autenticadora o llave de seguridad; evita depender solo del SMS.
- Borra publicaciones, anuncios, DMs o enlaces maliciosos y fija una aclaracion si hubo estafa visible.
- Revisa si el atacante cambio nombre de usuario, imagen, bio, email o reglas de acceso.

Advertencia especifica

Las estafas cripto en X se mueven muy rapido. Captura tweets, direcciones y DMs antes de borrar si hay denuncia o perdidas.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

12. Discord

Prioridad

El robo de Discord puede afectar servidores, bots, Nitro, pagos, comunidades y tokens de sesion.

Donde entrar

```
support.discord.com/hc/requests/new | Discord > User Settings > Devices / Authorized Apps / Billing
```

Procedimiento paso a paso

- Si aun puedes entrar, cambia contrasena y pulsa cerrar sesion en todos los dispositivos.
- Revisa Dispositivos, Aplicaciones autorizadas, conexiones, correo, telefono y 2FA.
- Regenera codigos de respaldo y cambia 2FA si sospechas robo.
- En servidores donde seas admin, revisa roles, webhooks, bots, permisos y canales creados.
- Revisa Billing/Nitro y elimina metodos de pago si hay cargos raros.
- Si perdiste acceso, abre ticket oficial de hacked account con correo original, usuario, fecha y pruebas.

Advertencia especifica

No ejecutes supuestos juegos, mods, cracks o verificadores enviados por DM. Muchos roban el token de Discord y evitan necesitar tu contrasena.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

13. WhatsApp

Prioridad

El atacante usa tu numero para pedir dinero a contactos, robar grupos o activar estafas por urgencia.

Donde entrar

```
App WhatsApp oficial | Ajustes > Cuenta > Verificacion en dos pasos | Ajustes > Dispositivos vinculados
```

Procedimiento paso a paso

- Reinstala o abre WhatsApp oficial y registra tu numero de nuevo. Introduce el codigo SMS o llamada solo en tu telefono.
- Si el atacante activo verificacion en dos pasos, espera el proceso de recuperacion indicado por WhatsApp y no compartas codigos.
- Entra en Dispositivos vinculados y cierra todos los que no reconozcas.
- Activa Verificacion en dos pasos con PIN y correo de recuperacion protegido.
- Avisa a contactos por llamada o canal alternativo de que ignoren peticiones de dinero o codigos.
- Si hay SIM duplicada, contacta con el operador para bloquear la SIM fraudulenta.

Advertencia especifica

WhatsApp nunca te pedira el codigo de seis digitos por chat. Si lo das, otra persona puede registrar tu numero.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

14. Telegram

Prioridad

Riesgo de acceso a chats cloud, grupos, canales, bots y mensajes de suplantacion.

Donde entrar

```
Telegram > Settings > Devices | Settings > Privacy and Security > Two-Step Verification |
telegram.org/support
```

Procedimiento paso a paso

- Si tienes acceso, ve a Dispositivos y termina sesiones desconocidas. En caso de emergencia usa Terminate all other sessions.
- Activa contrasena de verificacion en dos pasos y correo de recuperacion seguro.
- Revisa canales y grupos donde seas admin, bots conectados y permisos anadidos.
- Si no puedes entrar porque el atacante puso 2FA, conserva la SIM y sigue el proceso de recuperacion/espera de Telegram.
- Usa soporte oficial si hay bloqueo, suplantacion o perdida de canales.
- Avisa a contactos y grupos si se enviaron estafas desde tu cuenta.

Advertencia especifica

Los chats secretos no se sincronizan como los chats cloud. En un cambio de dispositivo puede perderse informacion no respaldada.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

6. Canales de creadores y plataformas de contenido

Este bloque agrupa varias plataformas del mismo tipo para que el indice sea claro y facil de usar. Dentro se mantienen los pasos concretos por servicio, pero el indice no se llena con cada cuenta individual.

15. YouTube y canales de creadores

Prioridad

Un canal robado suele implicar una cuenta Google comprometida. Puede haber videos fraudulentos, cambios de AdSense, strikes y directos de estafas.

Donde entrar

```
support.google.com/youtube/answer/76187 | studio.youtube.com | myaccount.google.com/security
```

Procedimiento paso a paso

- Primero recupera y asegura la cuenta Google vinculada al canal. Sin eso, la recuperacion de YouTube queda incompleta.
- En YouTube Studio revisa el panel de limpieza de canal si aparece, videos subidos, directos, permisos y cambios inusuales.
- Elimina videos o directos que no subiste para evitar sanciones adicionales.
- Revisa permisos del canal y Brand Account: propietarios, administradores y niveles de acceso.
- Si eres partner y ya recuperaste Google, contacta Creator Support. Si no puedes, usa @TeamYouTube en X como apoyo oficial.
- Revisa AdSense para YouTube, datos de pago, enlaces externos, descripcion del canal y cuentas conectadas.

Advertencia especifica

YouTube indica que para recuperar un canal hackeado hay que recuperar primero la cuenta Google asociada. Si el incidente ocurrio hace muchos meses, la capacidad de soporte puede estar limitada.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

7. Cuentas de videojuegos y consolas

Este bloque agrupa varias plataformas del mismo tipo para que el indice sea claro y facil de usar. Dentro se mantienen los pasos concretos por servicio, pero el indice no se llena con cada cuenta individual.

16. Steam

Prioridad

Robos de inventario, skins, Mercado, tradeos, Steam Guard y cuenta de correo asociada.

Donde entrar

```
help.steampowered.com/wizard/HelpWithAccountStolen | store.steampowered.com/twofactor/manage | steamcommunity.com/dev/apikey
```

Procedimiento paso a paso

- Antes de resetear Steam, escanea el equipo y cambia la contrasena del correo asociado desde un dispositivo limpio.
- Usa la pagina oficial de cuenta robada. Steam permite contactar soporte aunque hayan cambiado correo, telefono o contrasena.
- Aporta pruebas: recibos de compra, tarjetas regalo, ultimos cuatro digitos de tarjeta, PayPal, claves de juegos o correos de Steam antiguos.
- Activa Steam Guard Mobile Authenticator y revisa dispositivos autorizados.
- Revisa el historial de tradeos, Mercado, compras y mensajes enviados.
- Comprueba la Steam Web API Key y revocala si existe una que no has creado. Muchos robos de inventario usan API key maliciosa.
- No esperes restauracion de objetos: Steam informa que no restaura items perdidos o transferidos en muchos casos.

Advertencia especifica

Si alguien te escribe diciendo que te han reportado y debes hablar con un administrador de Steam por Discord, es una estafa clasica.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

17. Riot Games: League of Legends y Valorant

Prioridad

Puede haber cambios de region, correo, nombre, compras, baneos por uso fraudulento o perdida de acceso a LoL/Valorant.

Donde entrar

```
recovery.riotgames.com | support-leagueoflegends.riotgames.com | support-valorant.riotgames.com
```

Procedimiento paso a paso

- Usa recovery.riotgames.com para recuperar usuario/contrasena o verificar correo.
- Si no puedes, abre ticket de cuenta comprometida en soporte Riot con Riot ID, region, correo original, fecha aproximada de creacion y compras.
- Cambia contrasena del correo vinculado antes de resetear Riot.
- Revisa correo, pais/region, conexiones, metodos de pago y actividad reciente.
- Si hubo sancion mientras estaba robada, explica cronologia y aporta prueba de compromiso.
- Activa 2FA de Riot y usa contrasena unica.

Advertencia especifica

No compres cuentas ni compartas credenciales; complica la recuperacion porque soporte valida propiedad historica.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

18. Epic Games y Fortnite

Prioridad

Fortnite, compras, skins, cuentas vinculadas a consola, creador, Unreal/Epic y metodos de pago.

Donde entrar

```
epicgames.com/help | epicgames.com/account/password | epicgames.com/account/connections
```

Procedimiento paso a paso

- Restablece contrasena desde Epic si controlas el correo. Si no, usa soporte oficial de cuenta comprometida.
- Cambia antes la contrasena del correo principal.
- Revisa conexiones con PlayStation, Xbox, Nintendo, Steam, GitHub, Twitch y otras.
- Activa 2FA, revisa sesiones y elimina dispositivos no reconocidos.
- Comprueba compras, V-Bucks, regalos, cambios de nombre y tarjetas vinculadas.
- No desvincules cuentas de consola sin entender el impacto; documenta primero y consulta soporte si hay robo.

Advertencia especifica

Muchos robos de Fortnite comienzan con webs de pavos gratis, intercambio de cuentas o falsos torneos.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

19. Battle.net / Blizzard

Prioridad

Riesgo en World of Warcraft, Diablo, Overwatch, compras, saldo, personajes y sanciones.

Donde entrar

```
battle.net/support | account.battle.net/security | Battle.net Authenticator
```

Procedimiento paso a paso

- Intenta recuperar acceso desde Battle.net Support con correo, telefono o pruebas de propiedad.
- Cambia la contrasena del correo asociado antes de cambiar Battle.net.
- Activa o restablece Battle.net Authenticator y revisa SMS Protect.
- Revisa historial de compras, cambios de datos, personajes, regalos y actividad.
- Si la cuenta fue usada para trampas o spam, abre ticket explicando el compromiso.
- Elimina apps o addons sospechosos y analiza el equipo si instalaste mods no oficiales.

Advertencia especifica

Los addons y herramientas externas pueden ser vector de malware. Descarga solo desde fuentes fiables.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

20. Ubisoft

Prioridad

Afecta Ubisoft Connect, compras, juegos, Rainbow Six, conectividad de consola y metodos de pago.

Donde entrar

```
ubisoft.com/help | account.ubisoft.com | Ubisoft Account Management
```

Procedimiento paso a paso

- Restablece contrasena desde la pagina oficial o abre caso de cuenta comprometida.
- Revisa correo asociado, 2FA, dispositivos de confianza y cuentas vinculadas.
- Comprueba compras, amigos, mensajes, cambios de perfil y sanciones.
- Si perdiste el correo, prepara pruebas de propiedad: recibos, claves, usuario y fecha aproximada.
- Activa 2FA y elimina conexiones que no reconozcas.

Advertencia especifica

Evita comprar claves o cuentas en mercados dudosos; la recuperacion puede depender de pruebas de compra legitimas.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

21. EA

Prioridad

FIFA/EA SPORTS FC, Apex, The Sims, Battlefield, compras, puntos y vinculaciones a consola.

Donde entrar

```
help.ea.com | myaccount.ea.com | EA Login Verification
```

Procedimiento paso a paso

- Usa ayuda de EA para cuenta hackeada o comprometida. Cambia primero la contrasena del correo.
- Revisa correo, ID de EA, cuentas vinculadas a Xbox/PlayStation/Steam/Nintendo y metodos de pago.
- Activa Login Verification y guarda codigos de respaldo.
- Comprueba compras, transferencias de monedas/puntos y sanciones.
- Si te cambiaron correo o no recibes codigos, abre caso y aporta datos de propiedad.

Advertencia especifica

En juegos competitivos, una cuenta robada usada con trampas puede generar sanciones. La cronologia y evidencias importan.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

22. PlayStation Network

Prioridad

Protege PSN, compras, suscripciones, tarjetas, biblioteca, consola principal y acceso a juegos.

Donde entrar

```
playstation.com/support/account | playstation.com/support/store/unauthorised-payment
```

Procedimiento paso a paso

- Cambia contrasena de PSN y del correo asociado. Si no puedes entrar, usa recuperacion o soporte PlayStation.
- Cierra sesion en todos los dispositivos si la opcion esta disponible desde gestion de cuenta.
- Activa 2SV y revisa codigos de respaldo.
- Revisa metodos de pago, transacciones, suscripciones, monedero y consola principal.
- Contacta soporte si hay cargos no autorizados o cambio de ID/correo.
- No compartas cuenta ni uses webs de skins, monedas o juegos gratis.

Advertencia especifica

Si hay cargos, bloquea tambien la tarjeta en el banco. No esperes solo a la resolucion de la plataforma.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

23. Xbox y Microsoft Gaming

Prioridad

Xbox depende de la cuenta Microsoft. Protege Game Pass, compras, tarjetas y correo Outlook.

Donde entrar

```
support.xbox.com | account.microsoft.com/security | account.microsoft.com/billing
```

Procedimiento paso a paso

- Recupera la cuenta Microsoft antes de actuar sobre Xbox.
- Cambia contrasena, actualiza informacion de seguridad y revisa actividad reciente.
- En Xbox revisa suscripciones, compras, tarjetas, consola principal y dispositivos.
- Activa MFA en Microsoft y guarda recovery code en lugar seguro.
- Si hay cargos, gestiona reembolso desde Microsoft/Xbox y bloquea tarjeta si procede.
- Elimina accesos familiares o dispositivos que no reconozcas.

Advertencia especifica

Un cambio de datos de seguridad Microsoft puede tener periodos de espera. No elimines informacion valida hasta anadir y verificar la nueva.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

8. Bancos, tarjetas y pagos online

Este bloque agrupa varias plataformas del mismo tipo para que el indice sea claro y facil de usar. Dentro se mantienen los pasos concretos por servicio, pero el indice no se llena con cada cuenta individual.

24. Bancos: Santander, BBVA, CaixaBank, ING, Sabadell y Revolut

Prioridad

Si hay dinero, la prioridad es bloquear y comunicar. Despues se reclama y se denuncia.

Donde entrar

```
App oficial del banco | telefono oficial escrito por ti | banca online | oficina | canal de fraude
```

Procedimiento paso a paso

- Bloquea tarjeta desde la app o telefono oficial 24h. Si no sabes el telefono, buscalo en la tarjeta, app o web oficial escribiendo la direccion manualmente.
- Cambia claves de banca online desde dispositivo limpio y revisa dispositivos autorizados.
- Desactiva Bizum, pagos contactless, tarjetas virtuales y transferencias si sospechas control activo.
- Descarga o captura movimientos, cargos, transferencias, IBAN destino, comercio, fecha, hora y numero de operacion.
- Abre incidencia/reclamacion de operacion no autorizada en el banco. Santander permite reportar fraude en banca online; CaixaBank y Revolut incluyen gestion desde app/web; BBVA publica telefonos de atencion antifraude; Sabadell indica bloqueo inmediato por app o telefono.
- Si hay prestamo, alta de producto o suplantacion, pide bloqueo preventivo y certificado/documento de cargos para denuncia.
- Denuncia ante Policia Nacional, Guardia Civil o juzgado si existe fraude, cargos, suplantacion o extorsion.

Advertencia especifica

No devuelvas llamadas supuestamente del banco. Cuelga y llama tu al numero oficial. Nadie del banco debe pedirte claves completas, codigos OTP ni que transfieras dinero a una cuenta segura.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

9. Criptomonedas, exchanges y wallets

Este bloque agrupa varias plataformas del mismo tipo para que el indice sea claro y facil de usar. Dentro se mantienen los pasos concretos por servicio, pero el indice no se llena con cada cuenta individual.

25. Criptomonedas: Binance, Coinbase, Kraken y wallets

Prioridad

Las transferencias blockchain son normalmente irreversibles. La velocidad y las evidencias son criticas.

Donde entrar

```
App/web oficial del exchange | soporte oficial | explorador blockchain | denuncia policial
```

Procedimiento paso a paso

- Si el exchange permite bloqueo o security lock, activalo de inmediato. Coinbase permite bloquear cuenta comprometida; Kraken recomienda contactar y bloquear; Binance permite reportar scams y aportar TxID.
- Cambia contrasena del correo, exchange y 2FA desde dispositivo limpio. Si el email esta comprometido, recuperalo primero.
- Revoca API keys, direcciones de retiro guardadas, dispositivos, sesiones, passkeys y whitelist alteradas.
- Guarda TxID, direcciones origen/destino, capturas, hora, activo, red y valor aproximado.
- No transfieras fondos a una supuesta wallet segura indicada por un soporte que te llamo. Es una estafa comun.
- Si robaron una seed phrase, considera esa wallet perdida: crea wallet nueva en dispositivo limpio y mueve fondos restantes si aun existen.
- Presenta denuncia y proporciona TxID. En muchos casos el exchange necesita requerimiento policial/judicial para congelar fondos de terceros.

Advertencia especifica

Quien conoce tu seed phrase controla la wallet. Cambiar la contrasena de la app no protege una seed ya filtrada.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

10. Malware, infostealers y ransomware

Este bloque agrupa varias plataformas del mismo tipo para que el indice sea claro y facil de usar. Dentro se mantienen los pasos concretos por servicio, pero el indice no se llena con cada cuenta individual.

26. Malware, keyloggers, troyanos, RATs e infostealers

Prioridad

Si el origen es malware, cualquier recuperacion hecha en el mismo equipo puede volver a caer.

Donde entrar

```
Equipo afectado | antivirus/EDR | administrador de tareas | extensiones | programas instalados | logs
```

Procedimiento paso a paso

- Desconecta el equipo de Internet si sospechas control remoto o robo activo.
- Desde otro dispositivo cambia contrasena del correo principal, password manager, banco, cripto y cuentas criticas.
- Haz copia de documentos importantes sin ejecutar archivos sospechosos. Si el caso es grave, preserva evidencias antes de limpiar.
- Pasa analisis con Microsoft Defender/antivirus actualizado y herramientas antimalware reconocidas. Revisa extensiones de navegador, tareas programadas, inicio automatico y programas recientes.
- Elimina cracks, keygens, mods, supuestos visores de facturas, instaladores de patrocinio y extensiones desconocidas.
- En caso de infostealer confirmado, considera reinstalacion limpia del sistema y rotacion de todas las credenciales, no solo las afectadas.
- Regenera tokens: sesiones, cookies, API keys, codigos de backup, llaves SSH/Git si estaban en el equipo.

Advertencia especifica

Un infostealer puede robar cookies y entrar sin contrasena. Por eso hay que cerrar sesiones y revocar tokens.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

27. Ransomware

Prioridad

Contener expansion, preservar evidencias y recuperar desde copias limpias. No improvisar en empresas.

Donde entrar

```
Equipo/servidor afectado | copias offline | INCIBE-CERT/017 | denuncia | soporte tecnico
```

Procedimiento paso a paso

- Aisla el equipo: desconecta red cableada, Wi-Fi y unidades compartidas. No apagues si necesitas analisis forense y tienes soporte tecnico.
- No pagues precipitadamente. Pagar no garantiza recuperacion y puede financiar delincuencia.
- Fotografia la nota de rescate, extensiones de archivos, direcciones, emails, wallets y hora de deteccion.
- Identifica alcance: equipos, servidores, NAS, backups, usuarios y credenciales usadas.
- Restaura solo desde copias verificadas y en entorno limpio. No conectes backups a equipos infectados.
- Cambia credenciales administrativas, VPN, RDP, correo y servicios expuestos.
- Notifica a INCIBE-CERT/017 o proveedor de respuesta si hay empresa, datos personales o servicio critico.

Advertencia especifica

Antes de restaurar hay que cerrar la puerta de entrada. Si no, el ransomware puede repetirse.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

11. Moviles comprometidos o robados

Este bloque agrupa varias plataformas del mismo tipo para que el indice sea claro y facil de usar. Dentro se mantienen los pasos concretos por servicio, pero el indice no se llena con cada cuenta individual.

28. Android comprometido o robado

Prioridad

El movil recibe SMS, apps bancarias, autenticadores, WhatsApp y notificaciones de seguridad.

Donde entrar

```
google.com/android/find | Ajustes > Seguridad | Play Protect | operador movil
```

Procedimiento paso a paso

- Si esta robado, usa Encontrar mi dispositivo para localizar, bloquear o borrar si procede.
- Llama al operador para bloquear SIM y pedir duplicado seguro. Solicita bloqueo IMEI si corresponde.
- Desde otro dispositivo cambia contrasenas y cierra sesiones de Google, WhatsApp, banca y redes.
- Si sospechas malware, desinstala APKs fuera de Play Store, revisa accesibilidad, administradores de dispositivo, VPN/perfiles y apps con permisos raros.
- Actualiza Android y apps. Ejecuta Play Protect y antivirus si procede.
- Si el compromiso es serio, realiza copia de fotos/documentos y restablece de fabrica; reinstala apps manualmente, no todo el backup si sospechas app maliciosa.
- Activa bloqueo de pantalla fuerte, biometria, Find My Device y 2FA no basado solo en SMS.

Advertencia especifica

Una app con permiso de accesibilidad puede leer pantalla y pulsar por ti. Revisa ese apartado con especial cuidado.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

29. iPhone comprometido o robado

Prioridad

El Apple Account protege iCloud, Fotos, llavero, pagos, iMessage, App Store y localizacion.

Donde entrar

```
icloud.com/find | Ajustes > Apple Account | Find My | operador movil
```

Procedimiento paso a paso

- Si fue robado, marca el dispositivo como perdido en iCloud.com/find o Buscar. Apple recomienda hacerlo rapidamente.
- No elimines el dispositivo de tu cuenta si quieres mantener Activation Lock. Borrar remotamente no es lo mismo que eliminar de la cuenta.
- Cambia la contrasena de Apple Account y revisa dispositivos de confianza, numeros, correos y 2FA.
- Revisa compras, tarjetas de Apple Pay, perfiles VPN/MDM y apps instaladas recientemente.
- Si sospechas spyware avanzado por perfil de riesgo alto, actualiza iOS y considera Lockdown Mode con asesoramiento.
- Bloquea SIM/IMEI con operador y cambia claves de cuentas que recibian codigos en ese telefono.
- Si recuperas el movil, revisa Face ID/Touch ID, codigo, perfiles, VPN, calendario suscrito y apps desconocidas.

Advertencia especifica

No introduzcas tu Apple ID en enlaces de mensajes que dicen haber encontrado tu iPhone. Son phishing para quitar Activation Lock.

Checklist rapido

[ ] He accedido desde dispositivo limpio.

[ ] He cambiado contrasena por una unica.

[ ] He cerrado sesiones desconocidas.

[ ] He revisado correo/telefono de recuperacion.

[ ] He revisado MFA/passkeys/codigos.

[ ] He eliminado apps autorizadas sospechosas.

[ ] He guardado evidencias antes de borrar cambios del atacante.

30. Conservacion de evidencias

La evidencia sirve para recuperar cuentas, reclamar dinero, demostrar suplantacion y denunciar. Debe recogerse antes de borrar mensajes, publicaciones, reglas o transacciones. El objetivo no es hacer peritaje complejo, sino conservar datos fiables, ordenados y con fecha.

Que guardar

Evidencia	Como guardarla	Por que importa
Correos de alerta	Guardar .eml o imprimir a PDF con cabeceras si es posible.	Demuestran cambios de contrasena, correo, IP o dispositivo.
SMS/WhatsApp/DM	Captura completa con numero, usuario, fecha y enlace visible.	Prueba de phishing, extorsion o suplantacion.
Transacciones	PDF/extracto de banco, capturas, numero de operacion, comercio o IBAN.	Necesario para reclamacion y denuncia.
Cripto	TxID, red, wallet origen/destino, hora UTC, exchange y valor.	Permite rastreo y posible congelacion por autoridad.
Redes	URL del perfil/post, capturas, mensajes y cambios de nombre.	Acredita suplantacion o dano reputacional.
Dispositivo	Fotos de nota ransomware, hashes si sabes, logs, lista de programas.	Ayuda a determinar causa y alcance.

Metodo simple para organizar pruebas

Crea una carpeta con este formato: INCIDENTE_YYYY-MM-DD_NOMBRE. Dentro separa: 01_correos, 02_capturas, 03_banco, 04_plataformas, 05_dispositivo, 06_denuncia. Renombra archivos con fecha y descripcion: 2026-06-03_1015_aviso_cambio_contrasena_gmail.pdf. Apunta una linea temporal: hora de deteccion, acciones del atacante, acciones tuyas y respuestas de soporte.

Importante

No edites las capturas para que se vea mas bonito. Si necesitas tapar datos para compartir publicamente, conserva tambien el original sin editar en una carpeta privada.

31. Denuncias, INCIBE y canales oficiales en Espana

Denunciar no siempre recupera una cuenta al instante, pero es importante si hay fraude economico, suplantacion, extorsion, amenazas, difusion de datos privados, robo de identidad, cargos, prestamos o acceso a sistemas de empresa.

Cuando denunciar

- Cuando hay cargos, transferencias, prestamos, compras o robo de criptomonedas.
- Cuando alguien suplanta tu identidad para pedir dinero, extorsionar o publicar contenido.
- Cuando se han expuesto datos personales, documentos, fotos intimas o informacion de menores.
- Cuando hay ransomware, acceso a empresa, datos de clientes o continuidad de negocio afectada.
- Cuando el banco o plataforma te pide denuncia o documento oficial para tramitar reclamacion.

Canales utiles

Canal	Uso	Entrada orientativa
INCIBE 017	Ayuda gratuita y confidencial en ciberseguridad para ciudadanos, menores, empresas y profesionales.	Telefono 017, WhatsApp 900 116 117, Telegram @INCIBE017 y formulario oficial.
Policia Nacional	Denuncia de estafas, fraudes, suplantacion y ciberdelitos.	policia.es > Denuncias / comisaria.
Guardia Civil	Denuncias presenciales y algunos tramites telematicos; unidad de delitos telematicos.	web.guardiacivil.es > Denuncias / Puesto de Guardia Civil.
Banco	Bloqueo, reclamacion, certificado de cargos y expediente de fraude.	App oficial, telefono oficial o oficina.
Plataforma afectada	Recuperacion de cuenta, reversar cambios, bloquear actividad y retirar contenido.	Centro de ayuda oficial de cada servicio.

Plantilla breve para denuncia o soporte

Titulo: Cuenta comprometida / robo de cuenta / operaciones no autorizadas.

Descripcion: El dia [fecha] a las [hora] detecte [hecho]. La cuenta afectada es [usuario/correo/telefono]. No autorice [cambio/cargo/publicacion/transferencia]. Sospecho que el acceso se obtuvo mediante [phishing/malware/SIM/soporte falso/desconocido]. Acciones realizadas: [bloqueo, cambio de contrasena, cierre de sesiones]. Evidencias adjuntas: [capturas, emails, extractos, TxID, URL]. Solicito recuperacion/bloqueo/investigacion y confirmacion de pasos siguientes.

Consejo

En una denuncia por fraude bancario, la Policia Nacional indica que puede ser necesario aportar certificado de la entidad bancaria o documento con cargos fraudulentos. Pidelo al banco cuanto antes.

32. Prevencion: que dejar configurado antes del proximo incidente

La mejor recuperacion es la que no hace falta. La prevencion reduce la probabilidad de robo y, si ocurre, evita que el atacante controle todo.

Configuracion minima recomendada

Control	Nivel recomendado	Notas
Contrasenas	Unicas, largas, generadas por gestor.	Nunca reutilizar correo/banco/juegos/redes.
MFA	App autenticadora, passkey o llave fisica.	SMS solo como respaldo, no metodo principal si hay banco/cripto.
Correo principal	Recuperacion actualizada y sin reenvios raros.	Revisar filtros cada cierto tiempo.
Password manager	Clave maestra unica + MFA.	Guardar codigos de recuperacion offline.
Copias de seguridad	3-2-1: tres copias, dos medios, una offline.	Imprescindible contra ransomware.
Dispositivos	Actualizados, sin cracks, sin extensiones raras.	Separar equipo de ocio/descargas de banca/cripto.
Cripto	Seed offline, hardware wallet si hay importe alto.	Nunca fotografiar seed ni enviarla por chat.
Redes/creadores	Roles separados y minimos privilegios.	No compartir passwords; usar permisos oficiales.

Rutina mensual de 20 minutos

- Revisar dispositivos conectados en Google, Microsoft, Apple, Meta, Discord y Steam.
- Eliminar aplicaciones autorizadas que ya no usas.
- Actualizar telefono, navegador, sistema y gestor de contrasenas.
- Comprobar que el correo de recuperacion y telefono son correctos.
- Probar que puedes acceder a tus codigos de recuperacion, sin guardarlos en el mismo correo.
- Revisar movimientos bancarios, suscripciones y pagos automaticos.
- Comprobar que las copias de seguridad se pueden restaurar.

33. Checklists imprimibles

Gmail / Google

[ ] Entrar en myaccount.google.com/security

[ ] Cambiar contrasena

[ ] Cerrar dispositivos desconocidos

[ ] Revisar actividad reciente

[ ] Revisar telefono/correo de recuperacion

[ ] Revisar reenvio, filtros, POP/IMAP y delegacion

[ ] Revocar apps de terceros

[ ] Regenerar codigos de respaldo

[ ] Revisar YouTube/Drive/Chrome si aplica

Outlook / Microsoft

[ ] Cambiar contrasena

[ ] Revisar actividad de inicio de sesion

[ ] Actualizar informacion de seguridad

[ ] Revisar reglas y reenvio de Outlook

[ ] Cerrar sesiones

[ ] Activar MFA

[ ] Revisar OneDrive y Xbox

[ ] Comprobar facturacion

Instagram / Facebook

[ ] Usar instagram.com/hacked o facebook.com/hacked

[ ] Cambiar contrasena

[ ] Cerrar sesiones

[ ] Revisar correo y telefono

[ ] Revisar Centro de cuentas

[ ] Activar 2FA

[ ] Quitar apps conectadas

[ ] Revisar publicaciones/mensajes/anuncios

[ ] Avisar a contactos si hubo estafa

WhatsApp

[ ] Registrar de nuevo el numero

[ ] No compartir codigo SMS

[ ] Cerrar dispositivos vinculados

[ ] Activar PIN de verificacion en dos pasos

[ ] Anadir correo de recuperacion

[ ] Avisar contactos

[ ] Bloquear SIM si hay duplicado

Discord

[ ] Cambiar contrasena

[ ] Cerrar sesiones en Devices

[ ] Revisar Authorized Apps

[ ] Revisar Billing/Nitro

[ ] Regenerar 2FA/codigos

[ ] Revisar bots/webhooks/roles

[ ] Limpiar malware si se ejecuto archivo

Steam

[ ] Escanear equipo

[ ] Cambiar correo asociado

[ ] Recuperar Steam por soporte oficial

[ ] Activar Steam Guard

[ ] Revisar trade history

[ ] Revisar Steam API key

[ ] Revisar compras y Mercado

[ ] Reportar perfiles de estafa

Riot / Epic / Juegos

[ ] Recuperar correo primero

[ ] Usar soporte oficial

[ ] Aportar datos historicos y recibos

[ ] Revisar conexiones a consola

[ ] Activar 2FA

[ ] Revisar compras/sanciones

[ ] Cambiar contrasenas reutilizadas

Banco

[ ] Bloquear tarjeta/cuenta

[ ] Llamar a telefono oficial escrito manualmente

[ ] Cambiar claves desde dispositivo limpio

[ ] Descargar movimientos

[ ] Abrir incidencia de fraude

[ ] Pedir certificado/documento de cargos

[ ] Denunciar si procede

[ ] Vigilar nuevos cargos

Binance / Coinbase / Kraken

[ ] Bloquear cuenta si la plataforma lo permite

[ ] Cambiar email y contrasena

[ ] Restablecer 2FA

[ ] Revocar API keys

[ ] Revisar whitelist/direcciones

[ ] Guardar TxID

[ ] Reportar scam

[ ] Denunciar con datos blockchain

Android

[ ] Localizar/bloquear/borrar con Find My Device si robado

[ ] Bloquear SIM/IMEI

[ ] Revisar apps y permisos de accesibilidad

[ ] Actualizar sistema

[ ] Cambiar claves desde otro equipo

[ ] Reset fabrica si compromiso serio

[ ] Reinstalar apps manualmente

iPhone

[ ] Marcar como perdido en iCloud.com/find

[ ] No eliminar de la cuenta si esta robado

[ ] Cambiar Apple Account

[ ] Revisar dispositivos de confianza

[ ] Bloquear SIM/IMEI

[ ] Revisar Apple Pay y perfiles

[ ] Actualizar iOS

Ransomware

[ ] Aislar equipo/red

[ ] Fotografiar nota

[ ] No pagar precipitadamente

[ ] Identificar alcance

[ ] Proteger backups

[ ] Contactar soporte/INCIBE si empresa

[ ] Restaurar desde copia limpia

[ ] Cambiar credenciales

34. Plantillas listas para copiar

Mensaje a contactos tras robo de cuenta

Hola. Mi cuenta ha sido comprometida entre [hora] y [hora]. Si has recibido mensajes mios con enlaces, inversiones, sorteos, codigos o peticiones de dinero, no los abras y no envies ningun codigo. Ya estoy recuperando la cuenta. Si has hecho clic, cambia tu contrasena y revisa sesiones. Gracias.

Ticket a soporte de plataforma

Asunto: Cuenta robada / Account takeover - solicitud urgente de recuperacion.

Cuenta afectada: [usuario/correo/ID]. Correo original: [correo]. Fecha aproximada de creacion: [fecha]. Ultimo acceso legitimo: [fecha/hora]. Cambios no autorizados detectados: [correo, telefono, contrasena, publicaciones, compras]. Evidencias adjuntas: [capturas, recibos, IDs, enlaces]. Ya he asegurado mi correo y dispositivo. Solicito recuperar acceso, cerrar sesiones del atacante y revertir cambios no autorizados.

Linea temporal de incidente

Fecha/hora deteccion: [ ]. Primer sintoma: [ ]. Cuenta/dispositivo afectado: [ ]. Accion del atacante: [ ]. Acciones realizadas: [ ]. Personas/entidades avisadas: [ ]. Evidencias guardadas: [ ]. Pendiente: [ ].

Aviso a banco

He detectado operaciones no autorizadas en mi cuenta/tarjeta. Solicito bloqueo inmediato, apertura de expediente de fraude, certificado o documento de cargos no reconocidos, identificacion de operaciones afectadas y pasos para reclamacion. No reconozco ni autorizo las operaciones indicadas.

35. Fuentes oficiales consultadas

Las plataformas cambian menus y formularios con frecuencia. Por eso, ante un caso real, confirma siempre el flujo en el centro de ayuda oficial. Estas fuentes sirven como punto de partida y deben abrirse escribiendo la direccion manualmente o desde la app oficial, no desde enlaces de mensajes sospechosos.

Fuente	URL oficial	Uso
INCIBE 017	https://www.incibe.es/linea-de-ayuda-en-ciberseguridad	Ayuda gratuita y confidencial en ciberseguridad.
INCIBE reporte de fraude	https://www.incibe.es/ciudadania/ayuda/reporte-de-fraude	Reportar phishing, fraude y sitios maliciosos.
Policia Nacional denuncias	https://www.policia.es/_es/denuncias.php	Informacion para denunciar fraudes y delitos.
Guardia Civil denuncias	https://web.guardiacivil.es/es/tramites/denuncias/	Denuncias y orientacion en delitos.
Google cuenta hackeada	https://support.google.com/accounts/answer/6294825	Asegurar cuenta Google comprometida.
YouTube canal hackeado	https://support.google.com/youtube/answer/76187	Recuperacion de canales hackeados.
Microsoft cuenta hackeada/recuperacion	https://support.microsoft.com/account	Recuperacion y seguridad de cuenta Microsoft.
Apple Account comprometida	https://support.apple.com/102560	Recuperacion de Apple Account.
Android perdido o robado	https://support.google.com/android/answer/6160491	Localizar, asegurar o borrar Android.
iPhone robado	https://support.apple.com/120837	Modo perdido y proteccion ante robo.
Instagram hacked	https://www.instagram.com/hacked	Flujo de recuperacion Instagram.
Facebook hacked	https://www.facebook.com/hacked	Flujo de cuenta comprometida Facebook.
TikTok soporte	https://support.tiktok.com	Centro de ayuda TikTok.
WhatsApp FAQ	https://faq.whatsapp.com	Ayuda oficial WhatsApp.
Telegram support	https://telegram.org/support	Formulario de soporte Telegram.
Discord support	https://support.discord.com	Centro de ayuda Discord.
Steam account stolen	https://help.steampowered.com/wizard/HelpWithAccountStolen	Cuenta Steam robada.
Steam item restoration policy	https://help.steampowered.com/en/faqs/view/3B6E-B322-2400-8D24	Politica sobre items perdidos.
Riot recovery	https://recovery.riotgames.com	Recuperacion de cuenta Riot.
Epic Games help	https://www.epicgames.com/help	Soporte cuenta Epic.
Battle.net support	https://us.battle.net/support	Soporte Blizzard/Battle.net.
Ubisoft help	https://www.ubisoft.com/help	Soporte Ubisoft.
EA help	https://help.ea.com	Soporte EA.
PlayStation support	https://www.playstation.com/support/account/	Soporte cuenta PSN.

Fuente	URL oficial	Uso
Xbox support	https://support.xbox.com/help/account-profile	Soporte cuenta Xbox.
Santander reportar fraude	https://www.bancosantander.es/particulares/banca-online/seguridad-online/consejos-seguridad-internet/reporta-fraudes-online	Reporte de fraude online.
BBVA seguridad/fraude	https://www.bbva.es/finanzas-vistazo/ciberseguridad.html	Informacion de fraude y contacto.
CaixaBank operacion no autorizada	https://www.caixabank.es/particular/tarjetas/operacion-no-autorizada-faq.html	Devolucion de operacion no reconocida.
ING fraude en Internet	https://www.ing.es/seguridad-internet	Reportar fraude y consejos.
Banco Sabadell cargos no autorizados	https://www.bancsabadell.com/bsnacional/es/blog/que-hacer-si-tengo-cargos-en-cuenta-no-autorizados/	Bloqueo y actuacion.
Revolut report suspicious	https://help.revolut.com/en-ES/help/security-logging-in/how-do-i-report-a-suspicious-call-email-link-or-text/	Congelar tarjeta y reportar fraude.
Binance report scams	https://www.binance.com/en/support/faq/detail/49b6dbdd87ed4c60b527375918ab5683	Reporte de scams.
Coinbase compromised account	https://help.coinbase.com/en/coinbase/privacy-and-security/account-compromised/my-account-was-compromised	Bloquear cuenta comprometida.
Kraken compromised account	https://support.kraken.com/articles/4413167516692-my-account-is-compromised-what-should-i-do-	Cuenta comprometida Kraken.
Yahoo hacked account	https://help.yahoo.com/kb/recognize-hacked-yahoo-mail-account-sln2090.html	Senales y recuperacion Yahoo.
Proton reset/account recovery	https://proton.me/support/reset-password	Recuperacion de cuenta Proton.

Cierre: protocolo mental de 6 palabras

Contener. Recuperar. Expulsar. Revisar. Limpiar. Prevenir.

Si recuerdas solo una cosa de esta guia, recuerda que recuperar una contrasena no significa haber expulsado al atacante. La seguridad real llega cuando tambien cierras sesiones, quitas puertas traseras, revisas el correo, limpias el dispositivo, conservas evidencias y dejas configurado un metodo de acceso fuerte para el futuro.

Mensaje final

Actuar rapido no significa actuar impulsivamente. Usa canales oficiales, documenta cada paso y prioriza correo, telefono, dinero y dispositivos.