Cuenta comprometida

Versión 1.0 · Revisado el 11 oct 2026 · TLP:CLEAR · Para: Cualquier persona y los responsables de TI de una organización.

Qué hacer cuando alguien toma control de una cuenta de correo, redes sociales, WhatsApp o un sistema interno. El objetivo es recuperar el control, sacar al intruso y evitar que use la cuenta para engañar a otros.

Señales de que está ocurriendo

- No puedes iniciar sesión aunque la contraseña sea correcta.
- Avisos de inicio de sesión desde un dispositivo o lugar que no reconoces.
- Mensajes enviados desde tu cuenta que tú no escribiste.
- Cambios en el correo o teléfono de recuperación.
- Contactos que te avisan que “tú” les pediste dinero o un código.

Qué tan grave es

Alta	Cuenta de administrador, de finanzas o de un directivo; cuenta oficial de la organización.
Media	Cuenta de un usuario con acceso a información interna.
Baja	Cuenta personal sin acceso a sistemas de la organización.

Primera hora

- [ ] **1.** Si aún tienes acceso, cambia la contraseña desde un dispositivo que sepas limpio.
- [ ] **2.** Cierra todas las sesiones abiertas y desvincula los dispositivos que no reconozcas.
- [ ] **3.** Activa la verificación en dos pasos, de preferencia con aplicación y no con SMS.
- [ ] **4.** Revisa y corrige el correo y el teléfono de recuperación.
- [ ] **5.** WhatsApp: reinstala la aplicación y registra de nuevo tu número con el código SMS.
- [ ] **6.** Avisa a tus contactos por otro medio que ignoren mensajes sospechosos.

Preparación (antes del incidente)

- Usa una contraseña distinta en cada servicio, con un gestor de contraseñas.
- Activa verificación en dos pasos en todas las cuentas importantes.
- En WhatsApp, activa el PIN de verificación en dos pasos.
- Nunca compartas un código que te llegue por SMS, ni con conocidos.
- Guarda los códigos de recuperación en un lugar seguro.

Detección y análisis

- Revisa el historial de inicios de sesión: fecha, dispositivo y ubicación.
- Identifica cómo entraron: phishing, contraseña reutilizada, código compartido o malware.
- Revisa qué hizo el intruso: mensajes enviados, archivos descargados, cambios de configuración.
- Comprueba si la misma contraseña se usaba en otros servicios.

Contención

- Si perdiste el acceso, usa el proceso oficial de recuperación de la plataforma.
- Revoca los permisos de aplicaciones de terceros que no reconozcas.
- Elimina reglas de reenvío, filtros y respuestas automáticas que no creaste.
- Cambia la contraseña en todo servicio donde la hayas reutilizado.

Erradicación

- Analiza tus dispositivos con antivirus; si hay malware, la contraseña nueva también se filtrará.
- Borra los mensajes fraudulentos enviados desde la cuenta, después de guardarlos como evidencia.
- Reporta a la plataforma las cuentas falsas que te suplanten.

Recuperación

- Confirma que sólo tus dispositivos tienen sesión activa.
- Avisa a tus contactos que ya recuperaste la cuenta.
- Revisa la actividad de la cuenta cada semana durante un mes.

Lecciones aprendidas

- Identifica el hábito que permitió el acceso y corrígelo en todas tus cuentas.
- En una organización, revisa si otras cuentas comparten la misma debilidad.
- Comparte el caso con tu equipo o familia para que reconozcan el engaño.

Evidencia que debes conservar

- Capturas de los avisos de inicio de sesión y de los cambios de configuración.
- Mensajes enviados por el intruso.
- El correo o mensaje con el que te engañaron, si lo hubo.
- Números de teléfono o cuentas a los que se pidió enviar dinero.

Qué no hacer

- Cambiar la contraseña desde un dispositivo que puede estar infectado.
- Pagar a quien ofrece “recuperar” la cuenta por redes sociales: es otra estafa.
- Compartir códigos de verificación con alguien que dice ser soporte técnico.
- Crear una cuenta nueva y abandonar la anterior en manos del intruso.

A quién avisar

- Tus contactos, por un medio distinto a la cuenta afectada.
- El área de TI, si es una cuenta de trabajo.
- Tu banco, si la cuenta daba acceso a servicios financieros.
- Ministerio Público, si hubo estafa o extorsión a terceros.
- cert.gt, en cert.gt/reportar, para recibir orientación.

Cuándo dar por cerrado el incidente

- Tienes el control de la cuenta y de sus medios de recuperación.
- La verificación en dos pasos está activa.
- No quedan sesiones, aplicaciones ni reglas ajenas.
- Tus contactos fueron avisados.

cert.gt es una iniciativa privada y comunitaria de Devel Group.

cert.gt · devel.group · Reporta un incidente en cert.gt/reportar o a incidentes@cert.gt

Guía general de buenas prácticas; no sustituye asesoría legal ni técnica especializada para tu caso. No es un documento de una entidad gubernamental. Puedes copiarla y adaptarla citando la fuente (CC BY 4.0).