CASO 39

Una alumna se queja de que ha notado algún movimiento raro en su cuenta, como mensajes marcados como leídos a pesar de no recordar haberlos abierto siquiera. Sospecha de una compañera que se sentaba a su lado en informática y que ahora lleva unos días enferma en casa.

SOLUCIÓN. Auditoría de Inicio de sesión

PROCEDIMIENTO 39. Registro de Auditoría de Inicio de sesión

Iniciar sesión en la Consola de administración de Google. Entre en la página de Informes. En el marco izquierdo hemos de seleccionar la opción *Inicio de sesión* del menú *Auditorías*.

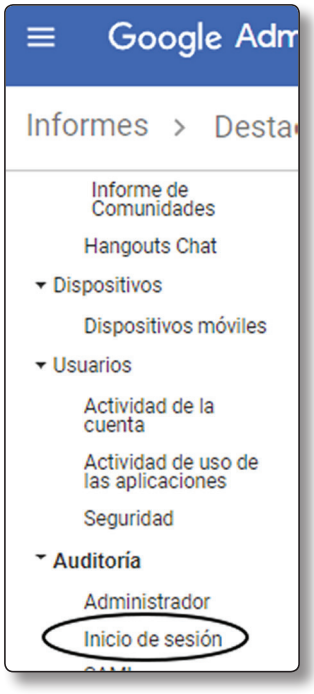

Figura 13.10. Situación del link Auditoría de Inicio de sesión

Si miramos la página sin aplicar filtros, tenemos en el marco derecho un registro de los inicios de sesión realizados en navegadores web, comenzando por el

más reciente. Estos eventos van acompañados de fecha y hora, la cuenta que lo ha realizado y la IP desde la que se han producido. En el listado se clasifican los eventos en varias categorías:

- Verificación de la identidad para el inicio de sesión
- Inicio de sesión correcto
- Error al iniciar sesión
- Inicio de sesión sospechoso; será marcado con un icono de advertencia rojo. El criterio de sospecha puede ser que abra la sesión desde una IP no habitual. El IP es un número de identificación de un equipo al conectarse mediante el protocolo de Internet.
- Cerrar sesión

En el caso 39, si no hay actividad sospechosa, podría encontrar inicios de sesión desde tres tipos de IP: móvil, casa y escuela. Si como sospecha la alumna, hay una persona que entra en su cuenta, encontraremos algún IP de más.

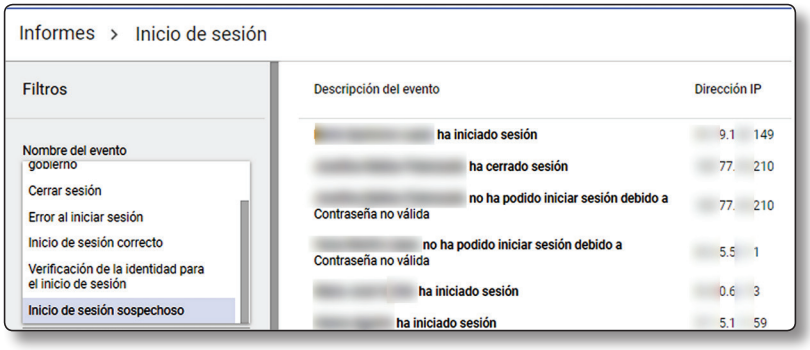

Figura 13.11. Diferentes eventos en la auditoría de inicio de sesión

Aunque en la auditoría no nos adviertan de inicios de sesión sospechosos, podemos realizar una nueva búsqueda usando esas IP. Pueden pasar varias cosas:

- Vemos que la IP la utilizan todos los usuarios. Se trata de la IP externa del centro educativo.
- Vemos que la IP solo la utiliza una cuenta.

- Vemos que la IP la usan dos cuentas. Podrían ser usuarios que comparten dispositivo o, como en el caso 39, que se trate de un suplantador que está usando la cuenta propia y la robada desde su casa.

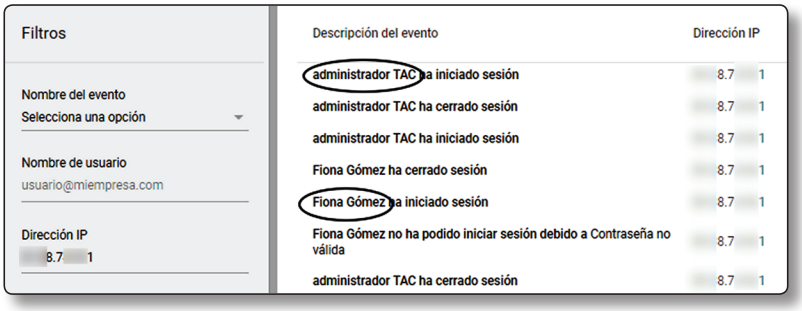

Figura 13.12. Búsqueda por IP

> **NOTA**
> Una página gratuita bastante correcta para localizar IPs que además muestra el Proveedor de Servicio de Internet o compañía que proporciona acceso a Internet (ISP) se encuentra en *goo.gl/vEp3t9*.

CASO 40

Algunos compañeros se quejan de recibir avisos sobre cambios en la política de gestión de móvil y para usar Gmail en el dispositivo Android necesitan instalar la aplicación Google Apps Device Policy. Sois dos los superadministradores y varios administradores en la dirección.

SOLUCIÓN. Auditoría de Administración

PROCEDIMIENTO 40. Registro de Auditoría de la Consola de Administración

Iniciar sesión en la Consola de administración de Google. Entre en la página de Informes. En el marco izquierdo hemos de seleccionar la opción *Administrador* del menú *Auditorías*.