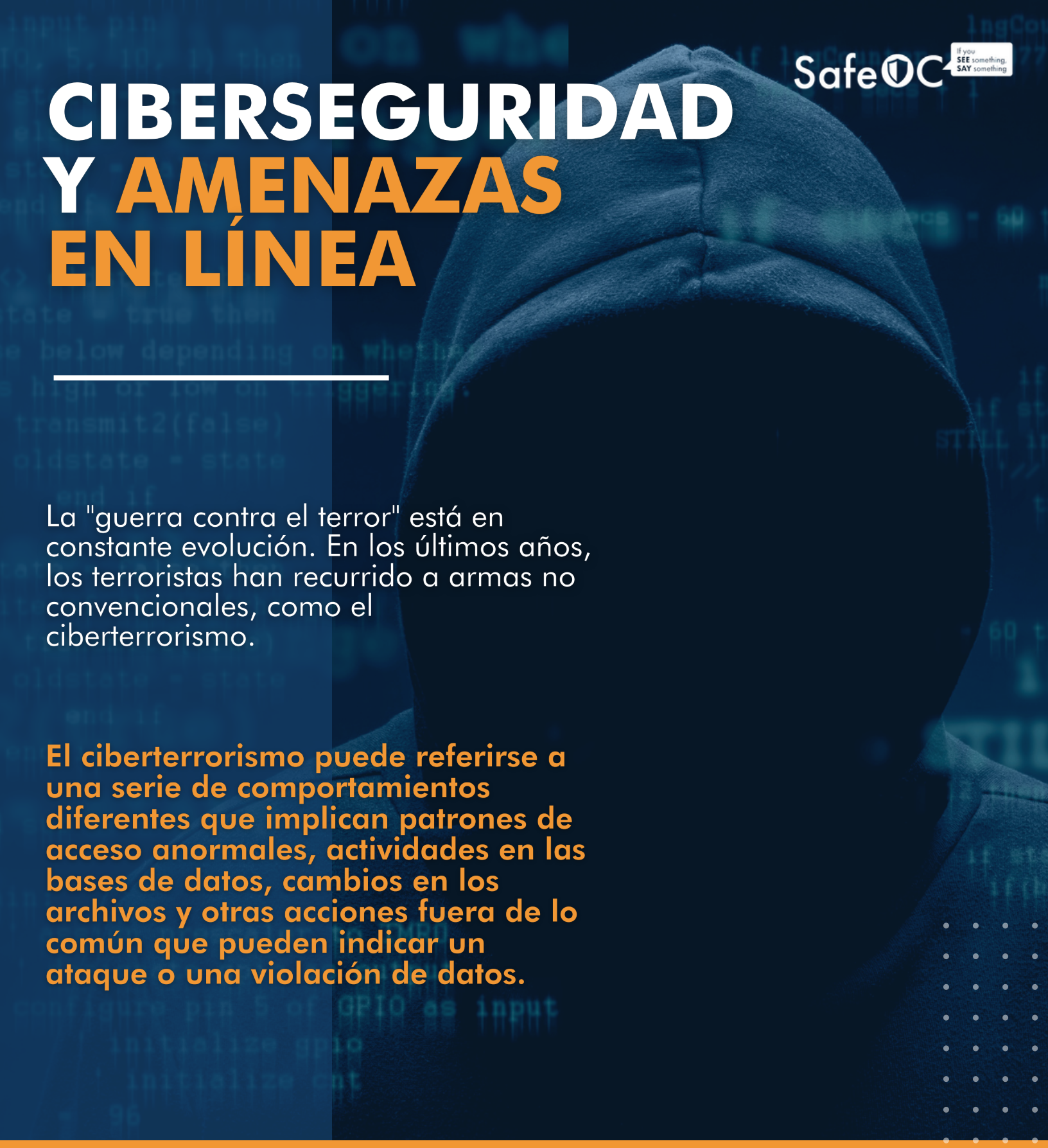
CIBERSEGURIDAD Y AMENAZAS EN LÍNEA



La "guerra contra el terror" está en constante evolución. En los últimos años, los terroristas han recurrido a armas no convencionales, como el ciberterrorismo.

El ciberterrorismo puede referirse a una serie de comportamientos diferentes que implican patrones de acceso anormales, actividades en las bases de datos, cambios en los archivos y otras acciones fuera de lo común que pueden indicar un ataque o una violación de datos.

Visite SafeOC.com para obtener más información sobre qué y cómo informar.

Síganos: @SafeOC @SafeOrangeCounty @Safe_OC

Estos son algunos de los ejemplos más comunes de actividad sospechosa:

ACTIVIDAD DE LA BASE DE DATOS:

La actividad anormal de la base de datos puede ser causada por ataques internos o externos, y los signos cruciales a los que hay que prestar atención son los cambios en los usuarios, los permisos y el crecimiento inusual del contenido de los datos.

CIBERATAQUE:

Interrumpir o comprometer los sistemas de tecnología de la información de una organización.

ABUSO DE CUENTAS:

El abuso de las cuentas privilegiadas es uno de los signos más comunes de un ataque interno, y los síntomas a los que hay que prestar atención son la modificación de los registros de auditoría, la compartición de los accesos a las cuentas y el acceso a información sensible sin necesidad.

CAMBIOS EN LOS ARCHIVOS:

Los cambios en la configuración de los archivos -incluyendo el reemplazo, las modificaciones, las adiciones de archivos y la eliminación- es una señal clásica de violación de datos, porque indica que alguien se ha infiltrado en su red y está tratando de evitar ser descubierto

Visite SafeOC.com para obtener más información sobre qué y cómo informar.

Síganos: @SafeOC @SafeOrangeCounty @Safe_OC