Algunos ataques vienen precedidos por amenazas, y otros no. Sin embargo, a menudo los individuos que planean un ataque violento denotan sus intenciones en su conducta, puesto que necesitan averiguar el mejor momento para atacar, planear cómo alcanzar el blanco, y cómo escapar.

La amenaza de un ataque puede disminuir si.
surgen cambios en la capacidad potencial del atacante para organizar un ataque,
si cambia su actitud de cara a lo aceptable que es un ataque, o si aumentan las probabilidades que tiene de ser capturado/a y castigado/a.

Por lo tanto es fundamental detectar y analizar cualquier señal que indique un posible ataque. Esto requiere:

- Determinar la posibilidad de que se lleve a cabo una amenaza (véase capítulo 3);
- Identificar y analizar los incidentes de seguridad (véase capítulo 4).

Los incidentes de seguridad que denotan la vigilancia de los defensores o de su lugar de trabajo están dirigidos a obtener información. Esta información no siempre se recoge con la intención de ser utilizada en un ataque, pero es importante determinar esto (véase Capítulo 4).
El objetivo de vigilar a los trabajadores o las oficinas es el de obtener información que pueda destinarse a varios fines como:

- Establecer qué actividades se están llevando a cabo, cuándo y con/por quien;
- Utilizar esa información más adelante para atacar a personas u organizaciones;
- Obtener la información necesaria para llevar a cabo un ataque;
- Recopilar información para hacer una acusación legal u otro tipo de coacción (sin violencia directa);
- Intimidarnos o intimidar a colaboradores o a otras personas con las que trabajemos, o presionarnos para que dejemos de ver a esas personas o de hacer algo ("vigilancia demostrativa").

Es importante recordar que la vigilancia suele ser necesaria para poder llevar a cabo un ataque, pero que no constituye por sí misma un ataque. Además, no todas las vigilancias implican un ataque posterior. Sin embargo, por otra parte, en algunas ocasiones un individuo puede improvisar un ataque cuando de repente ve una oportunidad para ello, aunque incluso en estos casos suele haber un mínimo de preparación previa.
No hay mucha información disponible que pueda ayudarte a reconocer la fase de preparación de un ataque. La ausencia de estudios sobre este tema contrasta enormemente con el gran número de ataques contra defensores. Sin embargo, los estudios existentes aportan interesantes revelaciones[1].

[1] Claudia Samayoa y Jose Cruz (Guatemala) y Jaime Prieto (Colombia) han realizado unos interesantes estudios sobre ataques contra defensores de los derechos humanos. Mahony y Eguren (1997) también realizaron un análisis de dichos ataques.

- Atacar a un defensor no es fácil y requiere disponer de recursos. La vigilancia es necesaria a la hora de establecer los movimientos de un individuo y el mejor momento para atacar. Dar en el blanco y escapar de forma efectiva y rápida es también primordial (sin embargo, si el entorno es altamente favorable para el atacante le resultará más sencillo llevar a cabo los ataques).

- Quien ataca a los defensores suele mostrar cierto grado de consistencia. La mayoría de los ataques van dirigidos a defensores muy implicados en temas que afectan a los atacantes. Es decir, los ataques no suelen ser casuales o sin objetivo, sino que responden a los intereses de los atacantes.

- Los factores geográficos son importantes. Por lo general, los ataques a defensores en zonas rurales no se divulgan tanto y en consecuencia provocan menos reacciones en la aplicación de la ley y a nivel político que los de las zonas urbanas. Los ataques en zonas urbanas contra oficinas de ONGs o contra organizaciones destacadas generan una reacción mucho mayor.

- Antes de atacar se deben tomar ciertas decisiones y optar por diferentes posibilidades. Los individuos que pretenden atacar a una organización de defensores deben decidir si atacar a los líderes o a los miembros de la base, o escoger entre un único golpe (contra una persona clave e importante lo que a su vez genera un mayor coste político) o una serie de ataques (que afecten a los miembros de la organización). Los pocos estudios realizados al respecto sugieren que suelen aplicarse ambas estrategias.

Establecer la probabilidad de un ataque

Para poder averiguar la probabilidad de que un ataque se lleve a cabo debemos analizar los factores relevantes. Para poder determinar cuáles son estos factores, debemos distinguir los diferentes tipos de ataques, es decir, los ataques directos (targeting), la delincuencia común y los ataques indirectos (estar en el lugar equivocado en el momento equivocado), haciendo uso de los tres cuadros de las páginas siguientes.[2]

[2] Esta clasificación de ataques incluye las mismas categorías que en las amenazas: Véase el capítulo sobre amenazas para una aclaración.

Cuando se es objeto de una amenaza y se quiere reducir el riesgo asociado a ésta, es importante actuar – no sólo contra la propia amenaza, sino que también sobre las **vulnerabilidades** y **capacidades** más **cercanamente vinculadas** a la amenaza. Cuando estamos sometidos a grandes presiones y queremos actuar con la mayor rapidez, a menudo actuamos sobre las vulnerabilidades de fácil solución o las más accesibles, en vez de hacerlo sobre las más relevantes para la amenaza en cuestión.

Ten cuidado: Si el riesgo de ataque es elevado (es decir, si la amenaza es inminente, y tienes varias vulnerabilidades y pocas capacidades), no tiene sentido centrarse en las vulnerabilidades o capacidades para reducir el riesgo, porque cambiarlas requiere tiempo. Si el riesgo es muy elevado (cuando un ataque directo y severo es inminente) tan sólo es posible evitarlo de tres modos:

a ◆ Confrontando la amenaza con inmediatez y efectividad, si se sabe que puedes lograr un resultado inmediato y específico que prevendrá el ataque. (Normalmente es muy difícil estar seguro de que se obtendrá un resultado inmediato y efectivo, porque las reacciones requieren su tiempo, y el tiempo es muy valioso en estos casos).

b ◆ Procurar no exponerse en absoluto (por ejemplo, escondiéndose o abandonando la zona temporalmente[4]).

c ◆ Otra opción sería la de solicitar una protección armada, asumiendo que haya una disponible (inmediata), y que esto podría disuadir al presunto atacante y no incrementa la situación de peligro del defensor a medio o largo plazo (en la práctica, es muy difícil que se cumplan estos tres requerimientos en la protección armada). En ocasiones, tras una presión nacional o internacional, el Gobierno decide ofrecer escoltas armados al defensor; en estos casos, el aceptar o rechazar la escolta podría determinar el grado de responsabilidad estatal en la seguridad de los defensores, pero aunque el defensor no acepte los escoltas armados un Gobierno no puede bajo ningún concepto declararse exento de sus obligaciones. Las empresas privadas de seguridad pueden representar un mayor riesgo si están vinculadas informalmente a las fuerzas de Estado (véase Capítulo 9). En lo referente a la posesión de armas por parte de los defensores debemos señalar que éstas suelen resultar inefectivas en un ataque organizado, y además pueden colocar a los defensores en una situación de vulnerabilidad puesto que el Gobierno podría utilizarlo como justificación para atacarles bajo pretexto de lucha antiterrorista o insurgencia.

Resulta mucho más fácil manejar las situaciones de amenaza que pueden conducir a un ataque cuando otros actores relevantes se implican y trabajan conjuntamente, por ejemplo, con un sistema judicial operativo; redes de apoyo (nacionales e internacionales) que puedan presionar a las autoridades responsables; redes sociales (dentro de las organizaciones o entre ellas), redes personales y familiares, ONU/fuerzas internacionales de pacificación, etc.

Vigilancia y contra-vigilancia

La contra-vigilancia puede ayudarte a determinar si estás sometido a vigilancia. Es difícil descubrir si tus sistemas de comunicación han sido interceptados, y por esta razón deberías presumir siempre que sí lo están[5]. Sin embargo, es posible determinar si alguien vigila tus oficinas y tus movimientos.

[4] Si bien hay situaciones en las que viajar representa una situación de riesgo mayor.
[5] Para más información sobre cómo asegurar las comunicaciones véase el Capítulo 13

¿Quién podría estar vigilándote?

Personas que suelen estar ubicadas en tu zona, como conserjes o porteros de edificios, vendedores que trabajan cerca de la entrada del edificio, gente en vehículos cercanos, visitas, etc., podrían estar vigilando tus movimientos. Hay personas que espían por dinero, o porque les presionan para que lo hagan; por sus inclinaciones, o debido a la combinación de estos factores. Los responsables de la vigilancia pueden también colocar colaboradores miembros de su organización en tu zona.

También puedes ser vigilado desde una cierta distancia. Normalmente son miembros de una organización que suelen practicar la táctica de intentar vigilar sin ser vistos. Esto requiere mantener una cierta distancia, alternarse con otras personas por turnos y observarte desde diferentes lugares, utilizando diferentes vehículos, etc.

Cómo averiguar si estás bajo vigilancia

Puedes averiguar si estás bajo vigilancia observando a aquéllos que podrían estar vigilándote, y adoptando las siguientes normas (sin, evidentemente, caer en la paranoia):

- Si sospechas que alguien podría estar vigilándote, deberías prestar atención a la actividad de la gente de tu zona y a los cambios en su conducta como, por ejemplo, alguien que empieza a hacer preguntas sobre tus actividades. Recuerda que pueden ser tanto hombres como mujeres, al igual que ancianos o gente muy joven.

- Si sospechas que te están siguiendo, podrías poner en marcha una medida de contra-vigilancia que implique a una tercera persona de confianza, desconocida para aquéllos que podrían estar vigilándote. La tercera persona podría observar, por adelantado y desde una buena distancia, los movimientos que se producen cuando llegas, te vas o te diriges a algún lugar. La persona que te esté vigilando probablemente lo realice desde un lugar desde donde te pueda localizar fácilmente, incluyendo tu casa, la oficina y los lugares donde sueles trabajar.

Por ejemplo

Antes de llegar a casa podrías pedirle a un miembro de tu familia o a un vecino de confianza que tome una posición cercana (por ej. cambiando una rueda del coche), para comprobar si alguien está a la espera de tu llegada. Podrías hacer lo mismo cuando salgas de la oficina a pie. Si utilizas un vehículo privado, deberás dejar que salga otro coche después del tuyo para darle tiempo al presunto observador a que se aproxime.

La ventaja de la contra-vigilancia es que, al menos inicialmente, la persona que te observa no es consciente de que está siendo vigilada. Por lo tanto deberías dejar claro a toda persona implicada en la contravigilancia que no es recomendable enfrentarse a la persona que te está observando. De esta forma sabrían que eres consciente de sus actividades, y esto podría desencadenar una reacción violenta. Es importante ser extremadamente precavido y mantener una distancia cuando sospeches que alguien te está vigilando. Una vez detectada la vigilancia, puedes poner en marcha la acción recomendada en este manual (véase Capítulo 9).

La mayoría de nuestros consejos sobre la contra-vigilancia hacen referencia de forma casi exclusiva a las zonas urbanas y semi-urbanas. En las zonas rurales la situación es muy diferente, porque los defensores y las comunidades que viven en estas zonas están más acostumbrados a detectar la presencia de extraños. Por lo tanto la persona que quiera vigilarte en una zona rural tendrá más dificultades para aproximarse a los habitantes - a no ser que la población local sea muy hostil a tu labor.

Nota: Existen situaciones en las que podría resultarte ventajoso relacionarte con las fuerzas de seguridad que te controlan – a veces la vigilancia no es tan secreta, y se exterioriza con el objetivo de intimidar. En algunas ocasiones los defensores establecen relaciones con personas de las fuerzas de seguridad para que les avisen cuando se planee vigilarles o incluso llevar a cabo una acción contra ellos.

Cuándo comprobar si estás siendo vigilado.

Es recomendable comprobar si estás sometido a vigilancia cuando tengas alguna razón para sospecharlo – por ejemplo, por incidentes de seguridad que podrían estar relacionados con la vigilancia. Si tu labor de derechos humanos conlleva un cierto riesgo, es aconsejable organizar de vez en cuando una simple acción de contra-vigilancia, por si acaso.

También debes pensar en el riesgo que representas para los demás cuando estás siendo vigilado – puede suponer un mayor riesgo para un testigo o un familiar de una víctima que visites que para ti mismo. Piensa sobre dónde sería más seguro verles. Tal vez necesites avisarles de que tus movimientos están siendo vigilados.

Reaccionar a los ataques

No existe una única norma aplicable a todos los ataques contra defensores. Los ataques también son incidentes de seguridad, y encontrarás las pautas de cómo reaccionar a los incidentes de seguridad en el Capítulo 4.

En todo tipo de ataque hay dos puntos primordiales a recordar:

- Piensa siempre en la seguridad – tanto **durante** el ataque como **después**. (Si estás siendo atacado y tienes dos posibles alternativas, ¡opta por la más segura!)

- Tras un ataque, deberás recuperarte física y psicológicamente, actuar para solventar la situación, e intentar restaurar un entorno de trabajo seguro para ti y tu organización. Es importante que retengas la mayor información posible sobre el ataque: Qué ocurrió, quién/cuántas personas estaban implicadas, número de matrícula de los vehículos, descripciones, etc. Todo esto podría resultar útil para documentar el caso, y debería ser anotado cuanto antes. Conserva copias de todos los documentos que presentes a las autoridades para documentar el caso.