GENOMA DEL ROBO

**ENFOQUE DEL RIESGO**

# Datos delincuenciales
# Análisis de comportamiento

Autor: José Miguel, Ángel Olleros.
Febrero 2021

**Datos delincuenciales.**

En primer lugar, es relevante conocer que no existe una única fuente oficial y completa de datos para el robo en viviendas. Tampoco se conocen con exactitud los criterios que utilizan las diferentes administraciones para clasificar las tipologías penales actuales que ofrece el balance de criminalidad del Ministerio de I nterior en su web: http://www.interior.gob.es/prensa/balances-e-informes/2019

Además del mencionado balance de criminalidad, es posible obtener otros datos de informes técnicos que realizan entidades privadas como: Estamos Seguros, UNESPA, ICEA y acceder de forma privada a estadísticas de empresas y asociaciones en el ámbito de la seguridad privada.

Sea como fuere, sería aventurado establecer de forma categórica una probabilidad de robo según donde se resida, pero sí que los siguientes datos permiten obtener una perspectiva de la situación actual.

**Balance de criminalidad del Ministerio de Interior 2019.** Se han seleccionado solamente las tipologías penales que pueden conformar un patrón delincuencial en la zona y que son de utilidad para este estudio.

| **Balance de criminalidad 2019 Ministerio de Interior.** | **España 2019** | **Hechos por día** | **Tasa hechos esclarecidos** |
|---|---|---|---|
| Item 6. Robos con violencia en intimidación | 66.209 | 181 | 33,6% |
| Item 7. - Robos con fuerza en domicilios, establecimientos y otras instalaciones. | 142.780 | 391 | 18,5% |
| Item 7.1 - Robos con fuerza en domicilios. | 98.520 | 270 | 15,6% |
| Item 8. Hurtos. | 700.477 | 1.919 | 18,7 |
| Item 9. Sustracciones de vehículos. | 35.248 | 97 | 28% |
| Item 10. Tráfico de drogas. | 16.268 | 44,6 | 93,2% |
| **Infracciones penales.** | **2.201.859** | **6.032** | **36,1%** |
| Porcentaje que representa los ciberataques | 10% | | |

Figura 1. Balance de criminalidad Ministerio del Interior. Año 2019. Robos.

Es importante indicar que los datos ofrecidos por el Ministerio de Interior son solo de poblaciones superiores a 30.000 habitantes, es decir, considera 250 municipios españoles de los 8.115 que existen en total. Por otro lado, se sabe, aunque sin datos concretos, que no todas las intrusiones, con o sin robo, son denunciados.

La primera reflexión es que, a nivel nacional, se denuncian 6.032 delitos al día, de los cuales, entre 270 y 391 están específicamente clasificados como robo con fuerza en domicilios. Nótese que un porcentaje no determinado, de hurtos y sustracciones de vehículos, estaría también relacionado con las viviendas y particulares.

Se incluyen los delitos de tráfico de drogas a modo de perspectiva delincuencial en la zona puesto que se sabe que el tráfico de drogas genera otras acciones delictivas en las que se encuentran los robos.

En una segunda reflexión, se evidencia el bajo porcentaje de hechos esclarecidos relacionados con el robo en domicilios (entre el 15% y 19%). Son realmente bajos y significantes si se comparan con delitos de tráfico de drogas, homicidios, lesiones y delitos contra la libertad sexual, donde todos ellos muestran una tasa de esclarecimiento superior al 80%.

Este dato pone el foco en que los sistemas de seguridad actuales no sirven como evidencia de un delito a las Fuerzas y Cuerpos de Seguridad, y puede ser un agravante, el hecho de que los recursos policiales destinados al esclarecimiento de estos delitos, sean insuficientes.

El informe elaborado por *"Estamos Seguros"* gracias a la colaboración de las entidades aseguradoras asociadas a UNESPA, indica que durante el año 2018 atendieron 27.089 daños por robos (1 cada 19 minutos y 24 segundos).

Si se analizara el impacto que supone el robo o daños por robo para las compañías aseguradoras, de sus respectivos informes se desprende que no es un daño relevante para ellas, aunque si para sus asegurados.

De forma genérica, se desprende que los robos o daños por robos, son solo el 5,73% de los siniestros totales declarados y supone el 14,14% del importe siniestral (importe de los siniestros pagados en el ejercicio anual). La frecuencia siniestral es de apenas el 2,73%, mientras que la suma de daños por agua, cristales y servicios de asistencia suponen el 34,56%

Con estos datos, se podría decir que el robo domiciliario no supone un problema para las aseguradoras y, por lo tanto, se comprende que no vean necesario activar estrategias de prevención antes de contratar pólizas, como por ejemplo sería que un perito en seguridad realizara una inspección de la vivienda antes de contratar la póliza, y deriven las decisiones de restauración de la seguridad, a empresas multiservicios poco o nada especializadas en la seguridad privada residencial.

**Periodos de robos según diferentes estadísticas.**

- Meses del año con más robos: agosto y enero.
- Días de la semana con más robos: martes y sábados.
- Periodo del robo: durante el día.
- Horas del robo: entre 12,00h y 17,00h / 21,00h y 02,00h.

**Edad de los delincuentes en el residencial.** Los delitos son cometidos por varones (85%), entre 18 y 35 años (59%), españoles (62%).

**Regiones de España con mayor atractividad.** Cataluña, Andalucía, C. Valenciana, C. Madrid y País Vasco, las regiones más atractivas para el robo y donde más probabilidad de robo existe. Pero en general, todo el litoral mediterráneo y Andalucía son las zonas más calientes junto con la Comunidad de Madrid.

**Impacto económico del robo.** Cataluña es la comunidad que mayor impacto tienen sus robos, es decir, que los delincuentes se toman su tiempo para desvalijar la vivienda. Seguida de Murcia y la Comunidad Valenciana.

**Datos de sistemas de seguridad.** No existe una estadística fiable, ni siquiera una estadística, que vincule los datos de robos denunciados, con los sistemas de seguridad que disponían estas viviendas. No obstante, algunos datos aportados por compañías de seguros y otros obtenidos de empresas del sector, muestran un notorio desequilibrio en la seguridad global de las viviendas.

1.282.500. Sistemas de alarma UNE 50131 grado 2, conectados a servicio C.R.A.
60%-70%. Con Puertas Blindadas y bombillos de seguridad UNE 1303 grado 6/2.
30%. Con rejas de seguridad sin ninguna certificación
13%-15%. Con ventanas de seguridad.
9%-10%. Con caja fuerte.
8%-11%. Con seguridad privada 24 horas.

(Datos extraídos sin fuente concreta, fruto del cruce de datos de diferentes informantes).

Según el último estudio de DBK, referido a Centrales Receptoras de Alarmas, de febrero 2020, en España existen 1,3 millones de contratos de conexión permanente de sistemas de alarma a centrales receptoras (C.R.A) para viviendas. Por otro lado, se estima que solo el 20% de estos sistemas residenciales, disponen de doble línea de comunicación supervisada. Estas conexiones contratadas por los propietarios de viviendas, para supervisar los sistemas de alarma instalados, generan una facturación anual mínima de 400 millones de euros. Estas cifras solo reflejan el coste económico en conexiones de sistemas, sin considerar el coste de instalación, equipos y mantenimiento.

**Segmentación de robos con fuerza**. En la siguiente tabla se combina el volumen de robos denunciados por año, día y horas, así como su impacto. La media nacional presenta datos nada desdeñables puesto que evidencia cifras de negocio bastante considerables y que pudieran estar detrás de la proliferación de “empresarios” del robo.

| Robos con fuerza en domicilios, establecimientos y otras instalaciones. (Item 7) | 2019 | Robos día | Robos por hora | Coste robo (unidad) | Coste robo (zona) |
|---|---|---|---|---|---|
| Andalucía | 22.455 | 62 | 3 | 1.141 € | 25.621.155 € |
| Aragón | 2.348 | 6,5 | 0,27 | 755 € | 1.772.740 € |
| Asturias | 1.563 | 4,3 | 0,18 | 556 € | 869.028 € |
| Baleares | 3.571 | 10 | 0,42 | 1.360 € | 4.856.560 € |
| Canarias | 4.310 | 12 | 0,50 | 882 € | 3.801.420 € |
| Cantabria | 1.628 | 4,5 | 0,20 | 1.089 € | 1.772.892 € |
| Castilla León | 4.765 | 13 | 0,50 | 822 € | 3.916.830 € |
| Castilla La Mancha | 6.525 | 18 | 0,75 | 1.330 € | 8.678.250 € |
| Cataluña | 33.993 | 93 | 4 | 2.741 €. | 93.174.813 € |
| Comunidad Valenciana | 19.823 | 54 | 2,3 | 1.336 € | 26.483.528 € |
| Extremadura | 1.661 | 4,6 | 0,2 | 557 € | 925.177 € |
| Galicia | 5.291 | 14,5 | 0,6 | 718 € | 3.798.938 € |
| Comunidad de Madrid | 18.255 | 50 | 2 | 1.765 € | 32.220.075 € |
| Comunidad Murciana | 6.184 | 17 | 0,7 | 1.506 € | 9.313.104 € |
| Comunidad Navarra | 1.514 | 4 | 0,2 | 557 € | 469.716 € |
| País Vasco | 8.162 | 22,3 | 1 | 725 € | 5.917.450 € |
| La Rioja | 552 | 1,5 | | 619 € | 341.688 € |
| **Media España** | **142.780** | **391** | **16,3** | **1.494 €** | **213.313.320 €** |
| | | **213 millones euros anuales (declarados)** | | | |

Figura 2. Segmentación de robos por coste y zona realizada para este trabajo. Fuentes de datos: Estamos Seguros, UNESPA, Ministerio del Interior.

**¿Dónde son más dañinos los delincuentes?** Otra forma de ver los datos sería establecer las zonas donde el impacto del robo es más dañino para los propietarios.

La siguiente tabla es más específica de la provincia. Considera el volumen de robos, el coste medio y el impacto de este robo con respecto a la media española. Se podría establecer que esta selección de provincias es donde los propietarios deberían ser más precavidos porque la delincuencia es especialmente activa, a la vez que dañina contra el patrimonio.

| Provincias | 2019 | Robos día | Robos por hora | Coste robo | Impacto del robo con respecto a la media española |
|---|---|---|---|---|---|
| Barcelona | 23.544 | 64,5 | 2,7 | 2.910 € | +129% |
| Gerona | 4.879 | 13,4 | 0,5 | 2.602 € | +148% |
| Tarragona | 4.436 | 12 | 0,5 | 2.045 € | +82% |
| Guadalajara | 845 | 2,3 | 0,1 | 1.823 € | -10% |
| Toledo | 3.345 | 9,1 | 0,4 | 1.802 € | +8,22% |
| Madrid | 8.797 | 24 | 1 | 1.765 € | -13% |
| Salamanca | 477 | 1,3 | 0,7 | 1.538 € | +59% |
| Sevilla | 6.422 | 17,6 | 0,7 | 1.510 € | -1,24% |
| Valencia | 9.089 | 25 | 1 | 1.509 € | +6,29% |
| Murcia | 1.920 | 5,3 | 0,22 | 1.506 € | +29% |

Figura 3. Segmentación de robos por impacto. Fuentes de datos: Estamos Seguros, UNESPA, Ministerio del Interior.

Sorprende el coste de robo de provincias como Tarragona, Guadalajara, Toledo, Salamanca y Murcia. La provincia de Gerona y Tarragona muestran porcentajes muy elevados de impacto con respecto a la media española, lo cual indica que los propietarios de estas zonas son más vulnerables.

**El Big Data como aliado del ciudadano.** Que fácil sería cruzar todos estos datos y disponer anualmente de la ratio de vulnerabilidad por zonas, caracterizando población vulnerable y población de riesgo e incluso saber el *modus operandi* para mejorar sistemas de defensa en previsión de un más que posible dinamismo del riesgo. Sería una forma de prevenir, sencilla, actualizada y económica, utilizando el conocimiento de una realidad.

**Conclusiones de los datos delincuenciales.** Los datos muestran claramente que el robo no tiene clases ni zonas y que afecta a todos por igual, sin embargo, parece que la delincuencia tiene especial fijación en Cataluña, el litoral mediterráneo y la Comunidad de Madrid.

Aunque el coste medio de robo declarado no parece elevado (1.494€), se constata que hay muchas zonas donde el impacto es muy superior (>3.000€). Y en este sentido sorprenden robos puntuales en poblaciones no significativas por su atractividad expositiva, lo cual, hace sospechar que existe información y planificación previa al acto delictivo con lo que se desmonta la creencia de que el perfil delincuencial es solo un oportunista que aprovecha “descuidos”.

A la vista de los datos, no cabe ninguna duda de que la sociedad está desprotegida, quizás por una falta de información o por pura imprudencia al tener la sensación de que el robo no les acecha.

Ha de considerarse que España es el país europeo con mayor número de sistemas de alarma residenciales conectados a una central receptora de alarmas (actualmente 1,3 millones de conexiones en un mercado que crece a un 12% anual).

Con estas cifras y considerando según el INE (Instituto Nacional de Estadística), que la unidad familiar es de 2,49 personas, en 10 años habrá entre 2,5 y 3,6 millones de personas nuevas afectadas. Habrán perdido en robos, otros 2.130 millones de euros en patrimonio, habiendo invertido un mínimo de 5.000 millones de euros solo en cuotas de sistemas de alarmas (sin contabilizar inversiones en la compra inicial, mantenimientos, ni en sistemas de seguridad física).

Sea como fuere, los datos indican que la actividad del robo es altamente atractiva para vendedores y delincuentes. Para el delincuente, no requiere de grandes esfuerzos, gracias a las insuficientes defensas y el exceso de confianza de los propietarios, la expectativa de botín es adecuada y en algunos casos sobresaliente. Y en el aspecto punitivo de la acción, el robo no tiene especial castigo, además de como indica el Balance del Ministerio del Interior, tiene una probabilidad de esclarecimiento muy baja (del 15%-19%).

Y efectivamente es una actividad atractiva y lucrativa que bien podría ser objeto de estudio como un nuevo sector de actividad profesional y modelo de negocio de una sociedad donde la brecha de desigualdades sociales irá en aumento.

**Detalle de localidades y barrios más perjudicados por el robo:**

Tarragona: Olesa de Bonesvalls, Lluçà (Barcelona) y Bellbei (30.000€ a 60.000€). Barrios de Barcelona: Horta-Guinardó El Guinardó; El Carmel y la Font d'en Fargues (9.958€). Sant Martí El Parc i La Llacuna del Pobleneu y el Clot (9.735€). Les Corts La Maternitat i Sant Ramón; Les Corts y Sants-Badal (7.694€). Comunidad de Madrid: Chapinería (22.400€), Algete (17.000€), Cenicientos (12.000€) y Torrejón de Velasco (11.000€). Barrios de Madrid: Latina y Carabanchel, Las Águilas y Buenavista (7.125€). Chamberí, Ríos Rosas y Vallehermoso (6.028€). Vicálvaro y Casco Histórico de Vicálvaro (5.958€). País Vasco: Artea (5.138€), Mundaka (3.759€) y Gamiz-Fika (3.577€). Un dato interesante es que Vizcaya tiene un 14% más de probabilidad de robo que la media del País Vasco. Andalucía: Almensilla (26.350€). Burguillos (18.319€). Bormujos (17.942€). Albaida del Aljarafe (13.409€). Aragón: Pradilla de Ebro (13.791€), Burjaraloz (5.407€) y Villamayor de Gállego (5.015€).

Fuentes de datos: Estamos Seguros, UNESPA,

**Datos de falsas alarmas.**

Es ciertamente complejo obtener datos del coste que las falsas alamas suponen a las empresas centrales receptoras de alarmas y a las FCSE. No existe una base de datos oficial unificada, ni siquiera una estadística de las propias empresas C.R.A de la que pudiéramos extraer conclusiones.

No obstante, se disponen de datos aislados de diferentes fuentes que indican que el porcentaje de falsas alarmas recibidas en las C.R.A. es muy elevado, aunque sus porcentajes de filtrado también lo sean, en torno al 99%. Pero ese 1% de las alarmas en las que las C.R.A. no consiguen verificar su falsedad y comunican a FCSE, supone cuantitativamente un número muy elevado de comprobaciones policiales. Y el crecimiento del parque de clientes conectados aumenta cada año (se estima en un 12%).

El Ministerio del Interior publica unos anuarios con información sobre el número de alarmas y avisos recibidos. Si bien el último publicado es de 2018, el último en el que dieron mayor detalle sobre los avisos alarma y los comunicados a cuerpo policial es de 2016. En dicho informe reflejaron que los 1,67 millones de conexiones de aquel momento, produjeron más de 73 millones de saltos de alarma. De estos, las C.R.A. les comunicaron 153.079 avisos (0,2% de los saltos), de los cuales, a su vez, fueron incidentes reales 32.656 (el 0,044% de los saltos y el 21% de las comunicaciones recibidas). Por tanto, ese año, más de 120.000 veces hubo desplazamientos innecesarios de todos los cuerpos policiales, generando un desconocido, pero previsiblemente, importante coste de dinero al erario público.

Al cierre de 2019 se alcanzó la cifra global de 2,25 millones de alarmas conectadas a C.R.A. (el 57% de viviendas), lo que supuso un crecimiento cercano al 10% respecto al año anterior y un aumento del 22% en comparación con la cifra registrada en el año 2017.

Considerando este ritmo de crecimiento y volúmenes de sistemas conectados, que a su vez generan varios millones de señales técnicas, de control y alarma a gestionar en el día a día, cualquier medida que reduzca las actuales ratios de falsas alarmas serán altamente bien recibida por todas las partes.

Según algunas fuentes, incluidas algunas policiales, al menos el 50% de estas falsas alarmas son generadas por los usuarios, cometiendo errores de conexión-desconexión del sistema, por dejadez en atender las llamadas desde la C.R.A para verificar la situación de alarma u otras circunstancias. Otras fuentes, como la empresa GRUPO ON SEGURIDAD, aumenta al 70% esta ratio de falsas alarmas generadas por circunstancias relacionadas por errores o responsabilidad de usuarios. La diferencia de porcentajes puede estribar en diversas causas; como la calidad del filtrado que realiza cada C.R.A. para intentar no comunicar a FCSE falsas alarmas, el tipo de actividad de sus clientes conectados o la complejidad de los sistemas gestionados, puesto que, a mayor sofisticación del sistema de detección con diferentes escenarios de uso, con usuarios no formados adecuadamente, etc., mayor probabilidad de falsas alarmas.

**Ejemplo estadística C.R.A GRUPO ON SEGURIDAD /** Fuente GRUPO ON SEGURIDAD.
Especializada en clientes de distinta tipología (comercial, industrial, residencial, etc.). Los clientes de residencial se caracterizan por ser muchos de ellos sistemas de alta sofisticación para gestión de escenarios y detección, tanto en interiores como en entornos de exterior.

Tipo de empresa: PYME / Gestionada por pequeñas empresas de seguridad instaladoras de sistemas.
Conexiones totales: 16.500 (a octubre 2020).
Señales mensuales recibidas (se incluyen los controles técnicos): 4,6 millones.
Alarmas mensuales gestionadas: 125.000.
Porcentaje de errores reconocidos por los usuarios:70%.
Porcentaje de filtrado en el proceso de calidad: 99,70%.
Media de comunicadas a FCSE al mes: 381 alarmas.
Media de alarmas reales al mes confirmadas en el desplazamiento de FCSE: 20,4 intrusiones.
Porcentaje de filtrado alarmas reales versus comunicadas a FCSE: 5,4%.

| Avisos a FCSE (a octubre 2020) | Avisos | Falsa alarma | Alarma real | Ratio Alarma real |
|---|---|---|---|---|
| GUARDIA CIVIL | 1.705 | 1.597 | 108 | 6,3% |
| POLICIA NACIONAL | 1.443 | 1.389 | 53 | 3,7% |
| MOSSOS D´ ESCUADRA | 380 | 355 | 25 | 6,6% |
| ERTZAINTZA | 282 | 264 | 18 | 6,4% |
| **TOTALES** | **3.810** | **3.606** | **204** | **5,4%** |

Figura 4. Alarmas comunicadas a FCSE durante 2020 por GRUPO ON SEGURIDAD.
Fuente GRUPO ON SEGURIDAD.

Ahondando en el objetivo de identificar los generadores de falsas alarmas para poder reducir sus costes asociados a todas las partes, se confirma la gran influencia de errores de usuarios cuando se comparan datos de falsas alarmas recibidas durante la primera fase de confinamiento COVID-19 y en los meses siguientes de verano.

Según un estudio realizado por MOSSOS D´ ESCUADRA, indican que, durante los meses de marzo a mayo 2020, las comunicaciones de alarmas se redujeron entre un 35% y 42%, llegando a la conclusión de que el movimiento de población, con el consiguiente aumento del número de entradas y salidas a viviendas y locales, genera normalmente una mayor activación indebida de los sistemas conectados, de los que una parte acaba siendo comunicada a las FCSE. Según la fuente GRUPO ON SEGURIDAD, confirman que, durante el confinamiento, también redujeron prácticamente a la mitad, el porcentaje de alarmas reales respecto a las comunicadas a FCSE.

En conclusión, sobre este importante aspecto de la gestión y aprovechamiento de recursos, varios expertos consultados, indican que una mayor concienciación de los usuarios, supondría una drástica reducción de las falsas alarmas recibidas en C.R.A y comunicadas a FCSE. En este sentido, cobra fuerza el enfoque de que una mejora en la información y formación de los usuarios, redundaría en beneficio de todas las partes. Se estima que las empresas de seguridad deberían realizar un proceso más pausado con los propietarios durante la fase de selección del sistema y en la posterior puesta en servicio donde el tiempo de formación de uso no debería ser inferior a 2 horas.

**Grupos vulnerables y grupos de riesgo.**

Hace décadas se pensaba que existía el concepto de “grupos vulnerables” bien por su condición social y entorno o por cuestiones de agrupación. Hoy en día, se ha verificado que clasificar por grupos vulnerables de ser víctimas es indefinido, y parece más adecuado diferenciar entre lo que sería un grupo vulnerable y un grupo de riesgo.

Un grupo vulnerable es aquel que siendo afectado por la acción (real o hipotética), tiene una capacidad de recuperación económica y emocional, limitada, normalmente en rangos bajos, mientras que un grupo de riesgo, es aquel que técnicamente evidencia una llamada a la acción delincuencial.

Un grupo vulnerable se establece considerando su CRITICIDAD, es decir, el impacto y su capacidad de recuperación, mientras que un grupo con factor de riesgo se establece considerando su POSIBILIDAD con sus variables técnicas de Oportunidad, Atractividad y Vulnerabilidad.

Ninguno de ellos tiene salvaguardas de status social o de entorno privilegiado, puesto que las evidencias de robo, acontecidas en la última década, demuestran, primero que la delincuencia es itinerante, y segundo, que la intrusión se produce, tanto en viviendas humildes en barrios desprotegidos, como en viviendas premium de urbanizaciones vigiladas, estableciendo la máxima de que la intrusión residencial no tiene “clases” ni “espacios” predeterminados.

La práctica demuestra que la peor situación se da cuando coinciden ambos, es decir, personas que pertenecen al grupo vulnerable y que además son grupo de riesgo. Y en su otro extremo estarían las personas que, aun siendo un grupo de riesgo, no se pueden considerar grupo vulnerable porque su tolerancia al riesgo y capacidad de recuperación es elevada.

Un problema latente es determinar cuanta población es un grupo vulnerable que además está en una situación de riesgo sin saberlo.

Este es uno de los grandes retos de todos los interlocutores pero que tiene difícil éxito debido a la desinformación “nativa”; fruto de las decisiones de cada persona como consumidores, y a la desinformación “dirigida” desde las administraciones, asociaciones y empresas que no se esfuerzan lo suficiente en aumentar el nivel de transparencia.

**Perfiles delincuenciales.**

En la investigación sobre perfiles delincuenciales, éstos, aparecen clasificados bien por lugar de procedencia, familiar y especialidad, o se pueden encontrar por una pseudo agrupación que los identifica como oportunistas, profesionales, clanes familiares, bandas organizadas, bandas criminales, etcétera.

Este trabajo propone otra forma de agrupar, enfocada a la amenaza en lugar de a la persona, diferenciando el agente agresor en base a su posibilidad técnica de preparación de la acción, considerando así, su contundencia y disposición al riesgo; a saber, el perfil de Oportunidad y el perfil Planificado.

**Oportunidad.** Es el perfil más habitual, un 90% según algunas fuentes policiales. Considera la oportunidad en base a la desocupación de la vivienda y a las debilidades de los sistemas o a la baja disposición de los usuarios para seguir protocolos seguros. También suelen aprovechar oportunidades en viviendas de grandes dimensiones y poco ocupadas, puesto que permiten accesos por zonas no ocupadas y lejanas sin que sus moradores se enteren.

**Planificado.** Considerado en un 10% según las mismas fuentes, aunque se sospecha que este porcentaje ha crecido sustancialmente en los últimos años. Sea como fuere, existen diversos niveles de planificación. Son profesionales que obtienen información previa de la vivienda, actividad, entorno, expectativa de botín, sistemas de seguridad, proveedores y rutinas.

Lógicamente la efectividad del perfil planificado es mayor que el perfil de oportunidad, tienen mayor motivación y, por lo tanto, los diseños de las defensas deben considerar esta particularidad.

Es aquí donde aparece una pregunta clave en el proceso de evaluación por parte del diseñador o de la diseñadora de las defensas puesto que debe preguntar al cliente ¿Para qué perfil delincuencial desea protegerse? Y lógicamente, los receptores de la pregunta solo podrán responder con criterio, si han recibido la información suficiente para comprender la importancia de su respuesta.

### 1.1.1 Tipologías de ataques | Dinamismo del riesgo.

Es ciertamente difícil conocer cuál de todos los perfiles delincuenciales acecha y atacará e igualmente difícil es establecer su capacidad de ataque en base a sus habilidades. Por lo tanto, no es posible establecer un tratamiento en base a un supuesto aún desconocido.

Sin embargo, si es posible diseñar medidas una vez que se clasifica según la posibilidad de ataque. En este campo se ha avanzado considerablemente al poder identificar las vulnerabilidades de los sistemas y procesos. Es decir, **no se puede conocer quien atacará, pero si se pueden establecer los "gap" susceptibles de ser atacados.**

En concordancia con esta reflexión, el trabajo realizado se ha orientado fundamentalmente no tanto al agresor sino a las vías que utilizará este agresor para el ataque, concretizando que, si estas vías son reducidas o evitadas, el agresor no tendrá oportunidad para la acción o su oportunidad se verá drásticamente reducida, con lo que a su vez aumentará su nivel racional de disuasión ante el aumento del riesgo percibido para acometer la acción.

Añadido a los ataques técnicos, la clasificación de ataques llamados "estratégicos", se ha contextualizado por oportunidad y por planificación. Se parte de la base de que cualquier sistema es susceptible de ser vulnerado, si el agresor dispone de suficiente tiempo, habilidades y motivación, pero son precisamente estos parámetros los que también juegan a favor del prescriptor para diseñar el espacio seguro o espacio libre de ataques.

En el campo de la investigación de sistemas, cabe destacar que hay indicios de que no existe una falta de tecnología para contrarrestar al agresor, sino que subyace una carencia de conocimiento y metodología en los actores implicados en esta defensa (tanto consumidores como profesionales de la seguridad).

Estos indicios, se convierten en evidencias cuando se conocen robos sin que las medidas de seguridad hayan avisado. Defensas que ni siquiera funcionaron porque el agresor pudo evitarlas o porque no estaban operativas, dicho de otro modo, que no ha existido la oportunidad de enfrentar las características técnicas del sistema a las habilidades del delincuente y, por lo tanto, si no existe enfrentamiento tampoco existe la posibilidad de perder.

Este ha sido un gran "descubrimiento martillo", una clave que ha permitido poner el énfasis en los métodos de los profesionales y en los hábitos de los usuarios más que en los productos. Y este -giro de foco- ofrece a los diseñadores de defensas, nuevas oportunidades que hacen que los agresores, afincados en su zona de confort de "no enfrentamiento", tengan que volver a reconstruir su plan de acción.

**Ataques técnicos.** Son todos los referidos al enfrentamiento del agresor contra las funcionalidades técnicas del sistema (sabotajes, rotura, inhibición, …).

**Ataques de oportunidad o selectivos.** Se engloban todos los técnicos y se añaden los referidos a la oportunidad que ofrecen sistemas, diseños y entorno para ser evitados. Se trata de ataques donde el delincuente aprovechará descuidos, dejadez de usuarios y operadores, franjas horarias propicias por falta de ocupación o por deslumbramiento de cámaras que vigilan, sobre todo al amanecer y atardecer, días de tormenta, los ya consabidos fallos técnicos de los sistemas por su nivel de entropía[1], y el aprovechamiento de los corredores de paso y ángulos ciegos que dejan los actuales diseños de seguridad.

Así se han identificado las siguientes especificidades:

Por franjas horarias.
Climatología.
Falta de hábitos.
Fallas del sistema.
Huecos del diseño.

[1] Entropía. Tendencia al caos y el desorden de un sistema, bien sea por su diseño, uso continuado y/o falta de mantenimiento.

**Ataques por planificación.** Son los referidos a una acción anticipada, preparatoria e inteligente por parte de los agresores. Naturalmente en esta familia se engloban todos los ataques de oportunidad anteriores y se añaden nuevos grupos de ataques, que previsiblemente serán altamente efectivos.

Inseguridad en el proveedor del sistema.
Inseguridad en el vecino colindante.
Desanonimización (propia o por personal interno).
En destino (segundas residencias en periodo de ocupación).
En remoto (facilitado por la automatización de la vivienda).
Amenaza directa (arma, intimidación, etc).

Estas tipologías de ataque por planificación son aún residuales en el conjunto de la sociedad, pero es indudable, que ya han sido identificadas y, por lo tanto, han pasado a formar parte del catálogo de amenazas en la seguridad residencial, de manera que es solo una cuestión de tiempo el que la delincuencia comience a democratizar su uso.

Es interesante enumerar los posibles esfuerzos que requieren estos ataques planificados, para darse cuenta de que no requieren de una especialización mayor a la que ya tienen los delincuentes para acometerlos, sino que basta con un simple -cambio de foco- en los agresores. Y esto les convierte en letales, porque volverán a romper el anillo de protección diseñado desde el enfoque técnico de pensamiento único[2], y con ello, todas las inversiones realizadas por los consumidores.

**Ataques en remoto (predelito).** Es una de las tipologías de ataque que se estima crecerán exponencialmente y merece una consideración aparte en este trabajo.

La llave que abre la puerta a los ataques en remoto es la automatización de las viviendas mediante centralitas domóticas y mediante los puertos y protocolos no seguros de routers comerciales y dispositivos IoT (Internet de las cosas), que se instalan en las viviendas, por instaladoras no especializadas en seguridad privada residencial.

De momento, la desinformación generalizada ha generado una perversa confusión con imprevisibles consecuencias para los propietarios. Se confunde, automatización del confort con automatización de los escenarios de seguridad.

Otra consecuencia aún no bien medida es que esta nueva consideración de ataque, se asienta sobre el concepto del pre-delito, es decir, permite planificar un delito sin exposición para el delincuente. Además, evita y desconecta, “sin romper”, todas aquellas defensas físicas o electrónicas que estén “conectadas” a la operativa domótica.

Y por último, se desconoce la respuesta del atestado policial y coberturas de las pólizas de seguros, debido a que serán intrusiones técnica y legalmente “sin rotura”, y por lo tanto, sin evidencias, lo cual, complicará aún más los esclarecimientos e indemnizaciones futuras.

En breves palabras, el impulso digital está aumentando la atractividad para el robo a espaldas de sus propietarios. Lo hace camuflado con un nuevo *lifestyle* de viviendas modernas, pero altamente costosas, inseguras e insostenibles.

[2] Enfoque técnico de pensamiento único. Su objeto es de validar certezas propias de los desarrolladores en lugar de exponerlas a confrontación. Concepto que se atribuye a fabricantes de productos, administraciones y grupos sectoriales que buscan refutar sus hipótesis buscando “cisnes blancos” en lugar de “cisnes negros”. Genera endogamia técnica y una protección de consumo en lugar de una protección de consistencia.

**Más detalles de las tipologías de ataque, fallas y errores.**

Aunque destacan los robos por la escalada, rotura de puertas y fractura del bombillo, se identifican hasta 30 tipologías de ataque a sistemas físicos. La deficiente instalación de los productos es un problema creciente puesto que está facilitando la efectividad del ataque.

| Tipologías de ataque a sistemas físicos | Soluciones |
|---|---|
| Apalancamientos (cerrojos, bisagras y estructuras). | Requiere refuerzos tipo BR13 o cambio de puertas a UNE 85160 grado 4C1A2A con detección anticipada del ataque. |
| Habilidad (ganzuado, impressioning, bumping). | Aplicar norma UNE 1303:2015 grado 6D con protección antibumping. |
| Rotura del bombillo. | Aplicar norma UNE 1303:2015 grado 6D, en unión de un escudo acorazado con placa base abocardada y 3-4 fijaciones tipo aeroflexi. |
| Apertura mediante lámina al resbalón. | Requiere cerrar la puerta siempre con cerrojos. |
| Ataque técnico al mecanismo de cerradura. | Requiere placa adicional de acero manganeso para proteger mecanismos. Y cerradura con re-bloqueos contra apalancamiento de cerrojos y extracción del bombillo. |
| Ocupación de la vivienda | Requiere escudo acorazado por el exterior e interior de la vivienda (ambos) para evitar desmontaje del bombillo. |
| Robo de llaves originales por empleado desleal y error humano en copia de llaves. | Procedimientos de control y custodia de llaves, claves y acceso a máquinas copia-llaves. Auditoria de custodia y producción de llaves. El establecimiento debe disponer de sistema de intrusión con videograbación, puerta de seguridad certificada y caja fuerte debidamente anclada. |
| 6 Tipos de ataques a escudos acorazados. | 1. Cizallamiento de fijaciones del escudo \| 2. Extracción del núcleo del escudo y del rotor del cilindro \| 3. Decapado del cuerpo del escudo \| 4. Arrancado completo del cuerpo del escudo \| 5. Ataque lateral al envolvente del escudo \| 6. Taladro y fresado del escudo. |
| Rotura de muros. | Combinar cerámica con entramados y placas de aceros. |
| Rotura de cristales. | Aplicar norma UNE 356 P5A a P8B y Láminas UNE 12600 1B1. |
| Apertura ventanas. | Estructuras EN 1627 RC3 y bloqueadores del giro de manetas. |
| Rotura y arrancado de cajas fuertes. | Aplicar norma UNE 1143-1 grado II-IV con anclaje UNE 108136. |

Figura 5. Tipologías de ataque a sistemas físicos. Fuentes: Estudio de Posibilidad del Robo en el Residencial 2018. Think Tank Genoma del Robo 2020.

Se identifican hasta 41 diferentes tipologías de ataque, fallas y errores en los sistemas de alarmas y de videovigilancia. Al igual que en los sistemas físicos, la inadecuada selección del sistema y su instalación, facilitan la efectividad del ataque.

| Tipologías de ataque a sistemas electrónicos | Soluciones |
|---|---|
| Corredores de paso sin cubrir y zonas de sombra. | Requiere profesionalidad en la fase de diseño y adecuado rigor del usuario para no tapar los detectores a futuro con nuevos objetos, cortinas o vegetación. |
| Avance de reptil / Ángulo 0. | Requiere detectores ángulo 0% y adecuada ubicación en altura e inclinación. |
| Sabotaje a cámaras. | Requiere asociar cámaras con detectores que se cubran mutuamente y detectores con su detección segmentada en zonas. |
| Sabotaje a comunicaciones. | Doble vía de comunicación supervisada cada 10-15 minutos (cable físico + comunicación inalámbrica). Cortatuegos físico para router. |
| Enmascaramiento detectores | Requiere de detectores con protección antimasking. Requiere doble tecnología con programación en “OR”. |
| Forzar saltos reiteradamente. | Sin solución técnica. Servicios premium de inteligencia. |
| Anticamuflaje. | Requiere de detectores con protección específica anticamuflaje. |
| Varias tipologías a la vez. | Sistema integral de altas prestaciones con gestión de escenarios y zonas. |
| Intrusión habitual sin salto de alarma. | Corregir el inadecuado diseño de ubicación de detectores con regulaciones precisas en giros, alturas y umbrales de detección (los sistemas de kit comerciales, orientados a evitar falsas alarmas, con doble tecnología, no suelen detectar bien las intrusiones). |
| Cortes de energía. | Para sistema de detección requiere centralita con fuente de alimentación bien dimensionada (mínimo 17Amperios). Automatismo de rearmado en el cuadro eléctrico. Para sistemas CCTV requiere SAI dimensionado al consumo del sistema. |

Figura 6. Tipologías de ataque a sistemas electrónicos de intrusión. Fuentes: Estudio de Posibilidad del Robo en el Residencial 2018. Think Tank Genoma del Robo 2020.

Independientemente de la habilidad de los atacantes, se identifican fallas y errores que son generados por la falta de conocimiento y dedicación de instaladores, usuarios y operadores.

**Fallos habituales generados por el instalador:**

1. No ajustar bien los tiempos de entrada para el desarmado (excesivamente largos).
2. No cambiar los códigos de fábrica.
3. No cambiar las configuraciones de fábrica en detectores.
4. No utilizar el tamper de la centralita como detector de intrusión.
5. Falta de tiempo dedicado al proyecto (diseño de ubicaciones y pruebas).
6. Falta de tiempo dedicado a la instalación generado por el bajo precio contratado.
7. Falta de tiempo dedicado al ajuste de detectores.
8. Desconocimiento especializado del producto que instalan.
9. Imprecisiones en la documentación de ubicaciones de detectores entregada a la CRA.
10. Inadecuada custodia de la información en la empresa (planos, claves, plantillas de programación, códigos de ingeniero).
11. Compartir canalización con sistema eléctrico general de la vivienda.
12. Mala ubicación de la centralita (por comodidad).
13. No fijación permanente de la centralita a la pared.
14. Priorización de las peticiones del cliente sobre las recomendables por seguridad.
15. Falta de asignación de la cámara con su detector correspondiente.
16. Sistemas de videovigilancia con videograbadores sin pasarela directa a su C.R.A.
17. Sin SAI para alimentación del sistema de videovigilancia.

**Baja consciencia e implicación del usuario:**

18. Despreocupación de los códigos de alarma que se informan a terceras personas.
19. Excesiva generación de falsas alarmas que obliga a las empresas a curarse mucho en salud ante posibles molestias y sanciones de la administración.
20. No conectar el sistema. Apagar regleta alimentación router.
21. Modificaciones de obra que no comunican y alteran las condiciones iniciales.
22. No aceptar las recomendaciones de mejora (sistemas obsoletos).
23. No comunicar un error de conexión-desconexión que genera una alarma.

**Fallos del servicio C.R.A:**

24. Cantidad, capacitación y motivación de operadores.
25. Ratio de equilibrio entre conexiones y operadores en servicio.
26. Sincronizaciones con hardware del sistema intrusión y vídeo de cada fabricante.
27. Criterios empresariales prevalecen sobre criterios del servicio óptimo a clientes.
28. Prioridades de los diferentes perfiles de aviso en C.R.A.

**7 grandes generadores de errores provocados por diferentes causas como:**

29. La baja calidad del hardware y software del sistema. Enfoque “fast security”.
30. No supervisión permanente de líneas.
31. Bajo reciclado de operadores CRA.
32. Fuentes de alimentación de insuficiente potencia para gestión de escenarios.
33. Sin automatismo de rearmado del sistema eléctrico.
34. Uso de protocolos de comunicación P2P en video vigilancia.
35. Utilizaciones de direcciones IP dinámicas sin ajustes.

Figura 7. Fallas y errores en la instalación y gestión de sistemas electrónicos de intrusión. Fuentes: Estudio de Posibilidad del Robo en el Residencial 2018. Think Tank Genoma del Robo 2020.