GENOMA DEL ROBO
by MCS

Estudio

Posibilidad del robo en el residencial

Estudio de la posibilidad del robo en función de la oportunidad, atractividad y vulnerabilidad que ofrecen los sistemas de seguridad instalados en diferentes tipologías de viviendas.

Este estudio ha sido elaborado por:

Iván Ballesteros Ballesteros.
Ingeniero consultor en medidas electrónicas y gestión del riesgo.

José Miguel, Ángel Olleros.
Consultor prevención del delito CPTED y seguridad por diseño.

Madrid, Noviembre 2018.

GENOMA DEL ROBO
by MCS

Estudio

Posibilidad del robo en el residencial

Estudio de la posibilidad del robo en función de la oportunidad, atractividad y vulnerabilidad que ofrecen los sistemas de seguridad instalados en diferentes tipologías de viviendas.

Se parte de la base de que la delincuencia es una característica inevitable de la civilización. El delito es algo normal porque una sociedad exenta del mismo es totalmente imposible. Erradicarlo completamente no es viable, pero como legítimos propietarios, podemos reducir, tanto su POSIBILIDAD como su IMPACTO.

Estudio y su motivación social

- ***Consejo de la Unión Europea (Bruselas, 24 de marzo de 2011, conclusión del Consejo 8094/11). El Consejo de la UE considera que:***

  "- En relación a la prevención del miedo al delito, se establece que el miedo al delito debería considerarse y tratarse como un problema social por derecho propio. El delito es perjudicial para una entidad, ciudad o país, en costes económicos y en costes sociales en cuanto a la percepción ciudadana de la inseguridad ; - (...);

  "- hay una serie de obstáculos que se han identificado en relación con el desarrollo de CPTED (Críme prevención trough environmental design), como la falta de conocimiento, la resistencia al cambio, la percepción de la panacea, el costo, la falta de apoyo legislativo y práctico, las influencias económicas; - (...);

Costes para la víctima

Económicos: Se identifican los costes tangibles que están relacionados con la pérdida económica del robo, de menor o mayor cuantía, dependiendo de la actividad generada en la vivienda y con menor o mayor capacidad para reponerse del daño, en función de los ingresos anuales de cada unidad familiar.

Emocionales: El impacto emocional se identifica como un daño de mayor calado, persistente en el tiempo y de mayor dificultad para superarlo. Está relacionado con sentimientos de inseguridad, miedo, paranoia, estrés, rabia e impotencia, que generan una bioquímica negativa en las personas que lo sufren. Daño que se traslada a la actividad de la persona en su día a día.

Objetivo SOCIAL del estudio

A través de una mejor información, aumentar la probabilidad de éxito en las decisiones de compra relacionadas con los sistemas de seguridad que son responsables de la protección de nuestro estilo de vida, mejorando nuestra bioquímica y nuestro doble derecho, como ciudadanos libres, de; **SENTIRNOS SEGUROS Y ESTAR SEGUROS.**

Objetivos TÉCNICOS del estudio

01

Medir la efectividad de los sistemas de seguridad instalados en viviendas.

02

Investigar el factor de riesgo que determina la posibilidad de ser víctima de un robo.

03

Desarrollar un modelo que ayude a tomar las mejores decisiones de compra.

Metodologías

Para desarrollar las formulaciones y métricas de este estudio, se han considerado además, las metodologías:

ISO EN 31000 / EN 31010
Análisis y gestión del riesgo.

Guía NodumLAPS®
Seguridad por diseño.

CPTED
Prevención del delito a través del entorno construido.

EASY
Estimate of adversary sequence interruption.

CONCLUSIONES GENERALES
DEL ESTUDIO

41
Tipologías de ataque, fallas y errores en sistemas de alarmas y videovigilancia.

30
Tipologías de ataque, fallas y errores en seguridad física (puertas, llaves y ventanas).

18,9%
Efectividad (ponderada) de los sistemas de seguridad residencial.

1) **Rupturas en la cadena de decisión.** Durante las fases de evaluación, comparación y adjudicación, del proceso de decisión de la compra, se identifican tres grandes problemas, aún no resueltos por las empresas del sector, que provocan elevados niveles de desorientación y desinformación en el comprador:

   a) **¿Cómo sé, si necesito mayor protección?**
   b) **¿Cómo comparo entre las opciones?**
   c) **¿A quién me dirijo?**

2) **Hasta 71 problemas a solventar.** Se han identificado hasta 71 posibles fallos de los sistemas de seguridad entre ataques, fallas y errores, que afectan a la efectividad de los sistemas (41 en sistemas de intrusión y 30 en sistemas de seguridad física). Al no aplicarse la auditoría externa de puesta en marcha de los sistemas instalados por las empresas contratadas (commissioning), los usuarios no tienen forma de verificar si estos posibles fallos, están cubiertos y de que forma.

3) **Evaluación antes que diagnóstico y antes que recomendación del sistema**. Un sistema de seguridad *"per se"* nunca alcanza una efectividad mínimamente adecuada. Durante todo este estudio, se evidencia que el método de evaluación y diagnóstico previo, junto con el proceso de ejecución, son más determinantes que las propias características técnicas de los sistemas.

4) **Efectividad (ponderada) se tasa en un 18,9% sobre 100%**. Las recomendaciones realizadas sin ninguna metodología de análisis, no supera el 18,9% de efectividad. Se advierte el hecho de que existe un elevado porcentaje de gusto por el autodiagnóstico[1], no se realizan mantenimientos adecuados y que la gran mayoria de los comerciales, dependientes y asesores de seguridad residencial, carecen de alguna titulación de especialización en seguridad.

5) **La resistencia física junto con la pronta detección son claves en la defensa.** La resistencia física de muros, puertas y huecos de ventanas retienen al agresor, mientras que la pronta detección reduce su ventana de tiempo, y al mismo tiempo, aumenta la ventana de las fuerzas de intervención (propiedad, vigilantes, fuerzas y cuerpos de seguridad del Estado). La línea de tiempo determina el éxito o fracaso de la defensa en profundidad. Cuanto antes se anticipe la detección, mayor será la probabilidad de interrumpir la acción del agresor.

6) **La defensa en profundidad reduce drásticamente la posibilidad de robo.** El modelo evidencia que una única medida de defensa es insuficiente. La defensa mejora drásticamente cuando se aplican capas de dificultad que combinan resistencia, detección y control (llamada seguridad transversal o defensa en profundidad).

Este estudio concluye que los sistemas de seguridad instalados son inadecuados e inefectivos debido al proceso de evaluación y diagnóstico realizados por asesores no cualificados en seguridad y a la falta de método en el proceso.

Los ratios de este estudio podrían explicar - *el por qué* – los sistemas de seguridad instalados, en las viviendas robadas, no fueron efectivos.

---

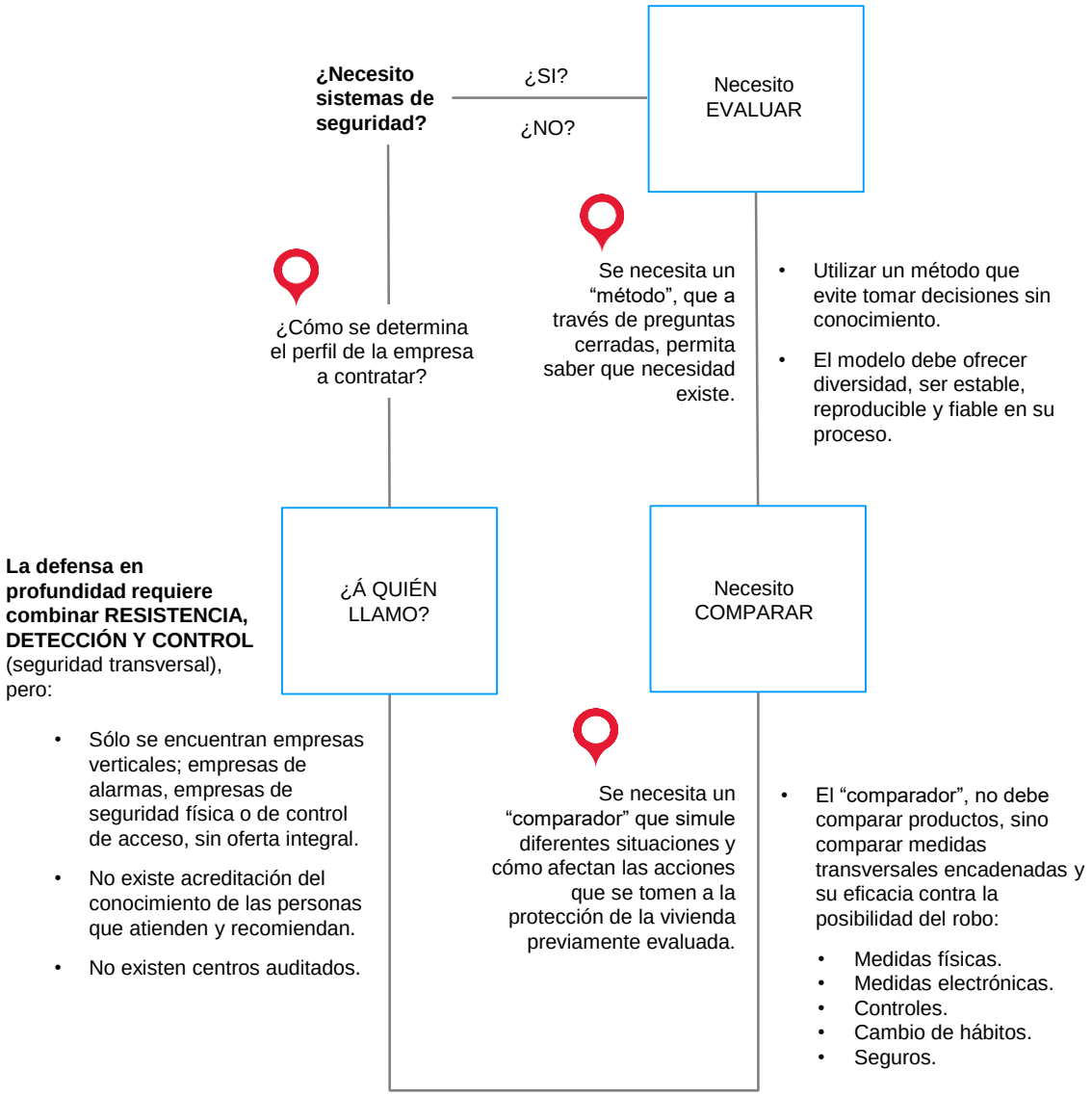
autodiagnóstico[1] : Toma de decisiones basadas únicamente en experiencias aleatorias, el precio, creencias, catálogos comerciales, charlas, internet, junto con la ausencia de un método de diagnóstico y la insuficiente capacitación en seguridad integral, son el principal problema a resolver ante la ineficacia de los sistemas de seguridad residencial.

RUPTURAS EN LA CADENA DE DECISIÓN
DEL COMPRADOR

Para tomar una decisión de compra**, el comprador necesita poder evaluar, comparar y saber a quién dirigirse** para adquirir los sistemas y ejecutar la solución. Al tratarse de una compra de importante impacto económico y emocional, el cliente, necesita tener la confianza en que su decisión sea la más acertada.

EVIDENCIA 1.

Realizando diferentes acciones en empresas y análizando los foros de Internet, no se ha podido dar continuidad a nuestro "proceso de decisión acertada".



DIFICULTADES DEL COMPRADOR
PARA PODER MEJORAR SU SITUACIÓN

En la medida que aumenta la consciencia de los usuarios, mejoran las decisiones, y por ende, aumenta la probabilidad de efectividad de los sistemas de defensa. Sin embargo, se detectan fuertes barreras (dificultades) para que el comprador pueda completar su cadena de decisión sin ruptura.

La información debe servir para mejorar el conocimiento actual del comprador con el fin último de aumentar la probabilidad de éxito en sus decisiones de compra.

Barrera 1. Económica.

Los propietarios heredan, sin ser conscientes de ello, un nivel ínfimo de defensa cuando adquieren la vivienda en origen. Esto supone que la inversión posterior sea mas elevada de lo esperado y que muchas familias tengan que vivir con mayor inseguridad de la aconsejable, al no disponer de nuevos recursos económicos.

Barrera 2. Compañías de seguros.

Ante un siniestro de robo, solo reponen productos, sin evaluación de riesgo, ni diagnóstico, ni mejora. En la práctica, el seguro repone la misma inseguridad que se tenía previamente al robo.

Barrera 3. Legislativa.

Ni el Código Técnico de Edificación, ni el Reglamento de Seguridad Privada español, recogen las recomendaciones del consejo UE sobre la reducción de miedo al delito, ni el derecho a la reducción del sentimiento de inseguridad de sus ciudadanos. No consideran la seguridad residencial dentro de sus responsabilidades.

Barrera 4. El sector.

La comunicación ha sido invadida por productos “fast security”. La mayoría de fabricantes e intermediarios solo invierten en producto estandarizado y paquetizado. Los programas de televisión solo están interesados en el sensacionalismo de las técnicas de ataque. El resultado es que las propuestas más técnicas y de mayor calidad, no tienen hueco para su comunicación y el cliente tiene más difícil poder conocerlas y encontrar puntos de venta.

Barrera 5. Influenciadores de ventas.

Entidades financieras y empresas de seguros, han comenzado a recomendar sistemas “fast security”, como modelo de negocio. El cliente inexperto lo adquiere confiando en su entidad y asume el coste de la recomendación realizada sin diagnóstico previo, emitida por un vendedor no acreditado en seguridad. Son ofertas con financiación, que en su mayoria, obligan a una cautividad durante 24-36 meses.

Barrera 6. Estudios de arquitectura, promotores inmobiliarios y administraciones locales.

No se realiza ningún informe de impacto sobre el nivel de seguridad o inseguridad, que genera un inadecuado diseño arquitectónico, infraestructuras, pre-canalizaciones, calidades de puertas, perfilerías, cristales, vegetación e iluminación de zonas comunes y zonas privadas.

Barrera 7. Planes formativos.

No existen planes de formación presencial especializados en seguridad residencial. Esto genera que prácticamente no exista la profesión de asesor de seguridad residencial.

Barrera 8. La sobreinformación.

El consumidor no tiene fuentes fidedignas de comparación. En su lugar se le inunda con un maremágnum de información comercial, camuflada como artículos técnicos. Desinformación.

NORMATIVAS EN VIGOR
PARA SEGURIDAD RESIDENCIAL

>30
Normativas.

El conocimiento y uso de las normativas en vigor, permite desarrollar soluciones con mayor rigor en términos de idoneidad, calidad, compatibilidad, funcionalidades y fiabilidad.

Los asesores de seguridad deben manejar estas normativas para emitir sus recomendaciones con criterio y rigor.

Norma	Scope
UNE-1143-1:2012	Cajas fuertes, cajeros automáticos, puertas y cámaras acorazadas.
UNE-1300:2014	Clasificación de cerraduras de alta seguridad.
UNE-108136:2010	Procedimientos de anclaje para cajas fuertes.
UNE-14450:2007	Cajas de seguridad.
UNE-1047	Armarios y cámaras ignífugos.
UNE-108142:1988	Rejas fijas. Características y ensayos de calificación.
UNE-1125:2009	Dispositivos antipánico para salidas de emergencia (barra horizontal).
UNE-179:2009	Dispositivos emergencia para evacuación (accionados manilla o pulsador).
UNE-13637:2016	Control electrónico de rutas de evacuación.
UNE-12209:2017	Cerraduras y cerraderos mecánicos.
UNE-12600:2003	Vidrio plano. Ensayo pendular. Método de ensayo al impacto.
UNE-356:2001	Vidrio de seguridad antimotín. Resistencia al ataque manual.
UNE-1063	Cristales antibalas.
UNE-1303:2016	Cilindros para cerraduras.
UNE-14351-1:2006	Puertas y ventanas exteriores peatonales (sin características de humo).
UNE-85160:2017	Puertas de seguridad. Selección, aplicación e instalación.
UNE-1627:2011	Puertas, ventanas, rejas y persianas. Resistencia a la efracción.
UNE-1630:2011	Puertas, ventanas, rejas, … Resistencia a la efracción (ataques manuales).
UNE-1906:2015	Manillas y pomos de puertas. Requisitos y métodos de ensayo.
UNE-EN 50131-1	Sistemas de alarma contra intrusión y atraco. Requisitos del sistema.
UNE-50131-7:2005	Sistemas de alarma de intrusión. Parte 7. Guía de aplicación.
UNE-50132-7	Sistemas de vigilancia CCTV. Guía de aplicación.
UNE-50133-7	Sistemas de alarma. Sistemas de control de accesos-Guía de aplicación.
UNE-50518	C.R.A Centros de supervisión y recepción de alarmas.
UNE-62676	Sistemas de Vídeo Vigilancia.
UNE-50131-8:2009	Sistemas de alarma-Niebla de seguridad.
UNE-14383 (1 a 8)	Planificación urbana y diseño de edificios.
UNE-31000-31010	Gestión del riesgo. | UNE-ISO GUÍA 73 Gestión del riesgo – Vocabulario.
DA DB-SI | DB-SUA	Seguridad en caso de incendio | Seguridad de utilización y accesibilidad.

SEGURIDAD FÍSICA Y LLAVES
FALLAS EN SISTEMAS

30
Fallas.

Puertas, cierres, escudos acorazados, persianas, bombillos, cristales, ventanas, perfilerías, etcétera, son adquiridas sin considerar las diferentes tipologías de ataques que existen y que son utilizadas de forma habitual por el agresor. Otro aspecto que no se valora lo suficiente es la instalación, la cual, genera el 40% de la efectividad del producto.

Tipologías de ataque	Soluciones
Apalancamientos; cerrojos, bisagras y estructuras.	Aunque se puede realizar un reforzamiento de puertas existentes, la solución más efectiva y duradera es el cambio de cierres y puertas.
Habilidad; ganzuado, impressioning, bumping.	Requiere cambio de bombillo. Adquirir bombillos contra estas tipologías de ataque, con protecciones específicas de alto nivel.
Rotura del bombillo.	Aunque existen refuerzos interiores, la rotura solo se evita con la protección mediante un escudo acorazado exterior (con 3-4 fijaciones tipo aeroflexi).
Apertura mediante lámina al resbalón.	Requiere cerrar la puerta siempre con cerrojos (2 vueltas de llave).
Ataque técnico al mecanismo de cerradura.	Requiere placa adicional de acero manganeso para proteger mecanismos. Requiere cerradura con re-bloqueos de cerrojos y extracción del bombillo.
Ocupación de la vivienda	Requiere escudo acorazado por el exterior e interior de la vivienda (ambos).
Robo de llaves originales por empleado desleal y error humano en copia de llaves.	Deben establecerse procedimientos de control y custodia de llaves, claves y acceso a máquinas copia-llaves. Debe realizarse una auditoria de custodia y producción de llaves. Auditoria externa del cumplimiento de procesos y procedimientos asegurados al cliente. **Los bombillos electrónicos con acceso mediante smartphone no requieren control físico de llaves.**
Robo en el establecimiento, de llave, claves y/o dirección de cliente.	El establecimiento debe disponer de sistema de intrusión con videograbación, puerta de seguridad certificada y caja fuerte debidamente anclada.
Copia técnica de llaves (mecánicas y electrónicas).	La llave debe disponer de restricciones técnicas para evitar la copia técnica no autorizada, por medio de máquinas mecánicas y electrónicas.
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.

La deficiente instalación de los productos es un problema creciente en la seguridad física.

- ❑ Los compradores se fijan en las características técnicas del producto pero no así en las capacitación técnica de la persona que lo tiene que instalar.
- ❑ La venta por Internet (no asistida), con instalación por los mismos compradores, es otro aspecto que ha incrementado las fallas y la menor efectividad del producto contra ataques muy básicos.

SEGURIDAD ELECTRÓNICA DE DETECCIÓN
FALLAS EN SISTEMAS

41
Fallas.

Se identifican diferentes tipologías de ataque, fallas y errores en los sistemas de alarmas y de videovigilancia, que en su mayoría, son generadas por la inadecuada selección del sistema y la falta de tiempo en el diseño e instalación. Al ser defectos en diseño, instalación, comunicación y programación, el cliente no es consciente de estas fallas hasta que, tiempo después, es víctima de una intrusión en su vivienda y el sistema no ha sido efectivo.

Tipologías de ataque	Soluciones
Rapidez.	No importa el sistema puesto que el tiempo de comunicación + el tiempo de intervención siempre es superior al tiempo de llegada de la policía.
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.
Sabotaje a comunicaciones.	Doble vía de comunicación supervisada permanentemente (cable físico + comunicación inalámbrica).
Enmascaramiento detectores	Requiere de detectores con protección antimasking. Requiere doble tecnología con programación en “OR”.
Forzar saltos reiteradamente.	Sin solución técnica.
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 el 100% de las intrusiones.
Cortes de energía.	Requiere fuente de alimentación bien dimensionada con apoyo de SAI. Automatismo de rearmado y doble vía de comunicación supervisada.

> ***El régimen de sanciones del Reglamento de Seguridad Privada, está generando que fabricantes e instaladores se preocupen más de evitar falsas alarmas, en lugar de enfocarse al objetivo del sistema, que no es otro que la detección de una intrusión y la gestión de escenarios de defensa.***

El usuario deber ser testigo del siguiente protocolo de pruebas finales:

1. Comprobación con disparo alarma de todas las zonas y escenarios programados.
2. Enumerar y comprobar los detectores que están tanto en modo disparo instantáneo como en modo retardado para evitar errores de instalación.
3. Asegurarse de que el retardo coincide con el tiempo mínimo imprescindible de entrada para no regalar tiempo al agresor.
4. Que los volumétricos y cámaras cubren exactamente el rango de cobertura y distancias.
5. Listar los volumétricos y cámaras con funcionalidades extras de detección (anti camuflaje, etc.).
6. Comprobar los volumétricos doble tecnología en modo activación "OR".
7. Comprobar que recibe alarma por ambas vías y que estas están supervisadas (ambas vías).
8. Desconectar una línea y comprobar que transmite por la otra línea (llamada de CRA al usuario).

El caballo de Troya de los sistemas de intrusión (alarmas y cámaras), es conseguir comunicaciones estables y disponer de infraestructuras adecuadas.

Seguridad por diseño.
*Una parte importante de los fallos más habituales, solo pueden solventarse si en el proyecto inicial o aprovechando la reforma de la vivienda**, se consideran ubicaciones y canalizaciones de seguridad.***

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.

Fallos del usuario:

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

Fallos del servicio C.R.A:

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

7 Grandes generadores de errores provocados por diferentes causas como:

La baja calidad del hardware y software del sistema *"fast security",* no supervisión permanente de líneas, bajo reciclado de operadores CRA, fuentes de alimentación de insuficiente potencia para gestión de escenarios, sin automatismo de rearmado, uso de protocolos de comunicación P2P en video vigilancia y utilizaciones de direcciones IP dinámicas sin ajustes.

¿CÓMO MEDIR LA EFECTIVIDAD DE LOS SISTEMAS?
DE SEGURIDAD RESIDENCIAL

18,9%

Efectividad (ponderada) de los sistemas de seguridad residencial.

Nuestro modelo cuantifica la efectividad del sistema (no sus fallos), en función de las probabilidades de decisiones acertadas, así como la oportunidad de que decisiones erróneas puedan ser corregidas en fases siguientes, si se contratan profesionales con conocimientos adecuados en seguridad transversal. **Por consiguiente, si la probabilidad de tomar decisiones acertadas en el proceso es baja, el sistema será poco efectivo.**

¿Cuál es la probabilidad de que no se cometan errores en la decisión inicial (P_{de})?

%Tenemos una necesidad / % no tenemos una necesidad / % en realidad no la necesitamos / % en realidad si la necesitamos / % decidimos mejorar la detección / % decidimos mejorar la protección física / % decidimos reducir el impacto / % son suficientes / % son insuficientes.

EVIDENCIA 2. **Probabilidad de éxito en la decisión inicial**. La falta de consultor acreditado con titulación de especialización y la falta de una metodología de evaluación, obligan al comprador a tomar decisiones de probabilidad que el modelo sitúa en un 25,5% máximo sobre su 99% posible.

Posteriormente, se establece que la efectividad de cualquier sistema se ve afectada por la probabilidad de éxito individual, en cada una de las cuatro fases de un proyecto, **siendo la decisión inicial (P_{de}), la más relevante, por ser la primera y ser condicionante del resto.**

P_{de}

Decisiones iniciales

% Probabilidad de que las decisiones iniciales sean las acertadas.

P_{di}

El diseño

% Probabilidad de que el diseño de protección sea el adecuado.

P_{eje}

La ejecución

% Probabilidad de que la ejecución sea la adecuada.

P_{ma}

El mantenimiento

% Probabilidad de que el mantenimiento sea el adecuado.

El modelo permite establecer además un porcentaje de probabilidad de corrección de errores **(P_{ce})** por los profesionales de la siguiente fase, siempre y cuando, estos estén capacitados.

Tabla base	**Probabilidad Decisión inicial**	**Probabilidad Diseño**	**Probabilidad Ejecución**	**Probabilidad Mantenimiento**
Responsable	***Consultor***	***Consultor/ Productos***	***Instalador***	***Mantenedor***
Aplica | 20%	*Acreditado.*	*Producto certificado.*	*Acreditado.*	*Acreditado.*
Aplica | 30%	*Titulación de especialidad.*	*Titulación de especialidad.*	*Método de instalación.*	*Conocedor del modelo aplicado.*
Aplica | 49%	*Utilización de un modelo de evaluación.*	*Aplicación de defensa en profundidad (capas).*	*Commissioning y documentación final.*	*Periodicidad adecuada.*
Total	***99%***	***99%***	***99%***	***99%***

EVIDENCIA 3. **Efectividad de la solución basada en la probabilidad de errores.** En la medida que el comprador se auto diagnóstica en Internet o recurre a establecimientos no cualificados en seguridad residencial, productos no certificados e instaladores y mantenimiento no cualificados, aumenta la probabilidad de errores y disminuye la efectividad de la solución.

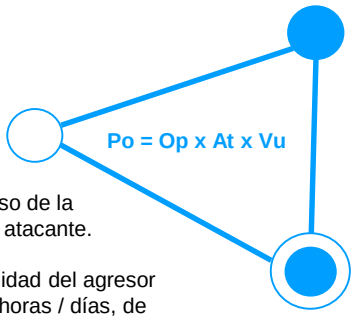
¿Quién toma la decisión inicial, qué método de evaluación se utiliza, qué producto se pone, quién y cómo lo instala, y quién y cómo se mantiene en el tiempo?

Tabla EFECTIVIDAD de los sistemas.

(Pce: Probabilidad corrección de errores).	Pde	Pdi	Pej	Pma	Pce	Total
Mejor situación posible (método y profesionales acreditados en seguridad transversal).	*95%*	*95%*	*80%*	*90%*	*90%*	*88,6%*
Auto diagnóstico + (profesionales especializados solo en su producto).	25,5%	*95%*	*80%*	*90%*	10%	*25,6%*
***Media ponderada del sector** (valores subjetivos de diferentes profesionales).*	**25,5%**	***75%***	***70%***	***70%***	**0%**	***18,9%***
El cliente decide todo (autodiagnóstico, compra internet no asistida, sin método, sin mantenimiento).	**25,5%**	**25,5%**	**25,5%**	**25,5%**	**0%**	*15,2%*

¿CUÁL ES EL MÉTODO DE ANÁLISIS QUE DETERMINA LA POSIBILIDAD DE SER VÍCTIMA DE UN ROBO?

El modelo analiza la **POSIBILIDAD** objetiva de ser víctima de un robo, analizando 19 elementos básicos que se computan dentro de tres variables: **Oportunidad** (Op), **Atractividad** (At) y **Vulnerabilidad** (Vu).



Atractividad

Atractivo de la vivienda para el ataque.

Guarda relación con el tipo de vivienda, su actividad y la recompensa estimada. Se ve afectada por el ratio general de vulnerabilidad.

Oportunidad

Facilidad que el uso de la vivienda aporta al atacante.

Analiza la oportunidad del agresor en función de las horas / días, de desocupación de la vivienda y personas con capacidad de defensa y disuasión.

Considera la actividad de la vivienda; morada, desocupada, segunda residencia, trabajo en casa y empresarial de riesgo.

Vulnerabilidad

La dificulta o facilidad que las infraestructuras y medidas de defensa de la vivienda generan al atacante.

Considera el tiempo de ataque con el tiempo de detección y resistencia. Se aplica a la envolvente de la vivienda y a su entorno próximo. Considera el diseño de defensa en profundidad y la obsolescencia de las medidas.

EVIDENCIA 4.

No se debe realizar una aplicación sin un tratamiento concreto. Un tratamiento concreto solo es efectivo cuando ha existido un diagnóstico previo. El diagnóstico solo es efectivo cuando se ha realizado una evaluación previa (análisis de riesgos). **La evaluación solo es rigurosa cuando se aplica bajo un método de análisis.**

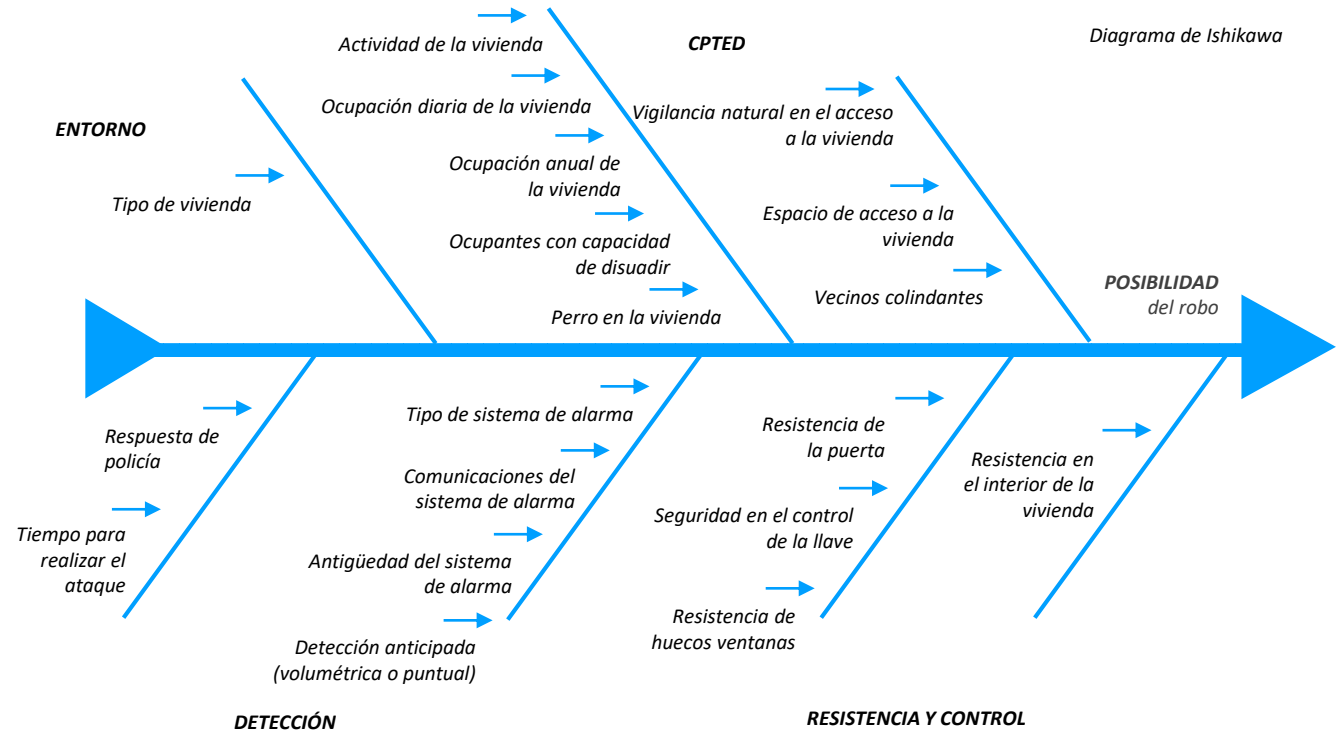
Sin haber realizado todo el proceso, una recomendación es inefectiva y falta de rigor.

MODELO CÁLCULO DE POSIBILIDAD DEL ROBO
PARA TOMAR MEJORES DECISIONES DE COMPRA

139
Millones de posibilidades.

El modelo identifica 19 elementos básicos y formula 17 preguntas para determinar la posibilidad del robo. Cada una de las 17 preguntas dispone de una lista de comprobación para obtener una respuesta cerrada (determinista). A su vez, algunas de las respuestas condicionan alguna de las preguntas y respuestas siguientes. En conclusión, cada vivienda se caracteriza por el cálculo ponderado del total de las 17 preguntas.

Todo el desarrollo de cálculo, ha permito caracterizar la posibilidad de robo de la vivienda entre **139.276.800 posibilidades**.



El modelo utiliza la técnica de *árbol de fallos* como herramienta para determinar la posibilidad del robo a partir de los 19 elementos básicos. En su desarrollo se han utilizado las siguientes técnicas:

- ❑ Enfoque *CPTED* en la seguridad de las viviendas.
- ❑ Métodos *NodumLAPS*® y *Genoma del Robo*®.
- ❑ El proceso de análisis jerárquico *AHP*. Arbol de fallos (FTA: Faul tree analysis).
- ❑ *Easy* (Estimate of adversary sequence interruption).
- ❑ Matrices discretas para aplicar las constantes a utilizar como función de los elementos básicos.
- ❑ Análisis por escenarios para probar el árbol de fallos (se han probado >500 escenarios).
- ❑ Análisis de valor.

El modelo considera la estrategia de defensa en profundidad que se aplica tanto en las normativas **ISO EN 31000 / EN 31010** como en otras normas-guías referidas a buenas prácticas en el análisis de riesgos malintencionados**.**

El modelo permite visibilizar y resolver de forma estratégica, las principales preocupaciones en la seguridad residencial:

Viviendas con 5 capas:

1) **DISEÑO.**
2) **RESISTENCIA.**
3) **DETECCIÓN.**
4) **PROTECCIÓN INTERIOR.**
5) **CONTROL.**

a) ¿Cuál es la probabilidad de detección en las diferentes fases del avance del agresor.

b) Cuál es la probabilidad de detección en la vivienda en función de las condiciones naturales de la vivienda y su entorno (CPTED).

c) ¿Cómo afectan las medidas técnicas (características e instalación) de puertas, cerraduras, llaves, alarmas, cámaras y comunicaciones para interrumpir el intento de robo.

01	02	03	04	05
Probabilidad de detección en la vecindad.	Probabilidad de detección en la proximidad.	Probabilidad de detección antes de la envolvente.	Retardos en la envolvente e interior de la vivienda.	Probabilidad de detectar el ataque en el interior de la vivienda.

EVIDENCIA 5.

El modelo demuestra que la mayor efectividad se consigue concatenando diferentes medidas técnicas y distribuyéndolas en capas de defensa en profundidad: perímetro de la parcela, perímetro de la vivienda (envolvente) e interior de la vivienda.

a. Se ha considerado la efectividad de intervención de las Fuerzas y Cuerpos de Seguridad del Estado (estimada en tiempo de asistencia).

b. Se ha considerado la habilidad y conocimiento requerido del agresor para vulnerar las defensas (estimada en tiempo de ataque).

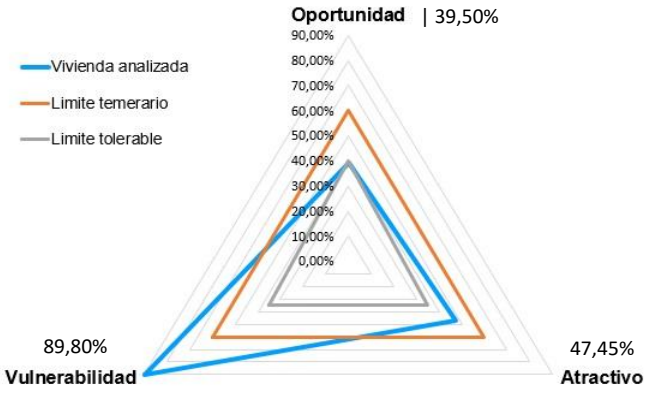
Combinaciones de éxito por orden de efectividad:

1) Vigilancia natural - pronta detección – resistencia física – detección interior – protección interior – control de llaves – mantenimiento actualizado.
2) Pronta detección – resistencia física – detección interior – protección interior – control de llaves – mantenimiento actualizado.
3) Resistencia física – detección interior – protección interior – control de llaves – mantenimiento actualizado.
4) Resistencia física - detección interior – control de llaves – mantenimiento actualizado.
5) Resistencia física – mantenimiento actualizado.
6) Detección interior – mantenimiento actualizado.

EJEMPLO DE DESARROLLO GRÁFICO DEL MODELO POSIBILIDAD DEL ROBO.
Se considera un unifamiliar adosado, de nueva construcción, en una zona residencial, no vallada, que permite vigilancia natural, para una familia de 2 miembros adultos y cuya actividad laboral es por cuenta ajena. La vivienda es residencia habitual, sin actividad empresarial (solo morada). **La vivienda dispone de;** puerta acorazada UNE 1627:2011 grado 3 con bombillo y llave de seguridad con tarjeta de propiedad. El perimetral de la vivienda tiene persianas de aluminio y cristal templado 4+4 (sin rejas, sin persianas autoblocantes).

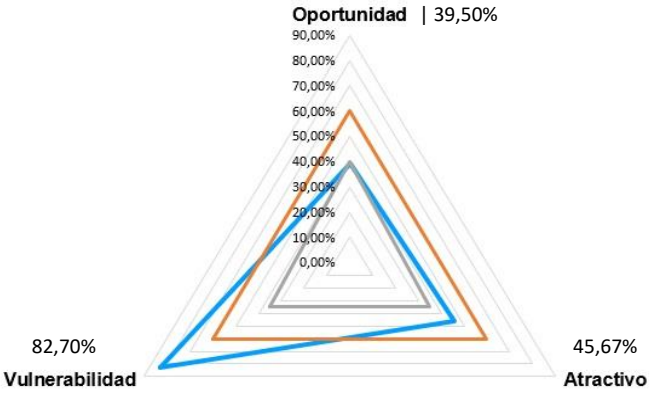
1 CAPA
clase 1A1

Evaluación básica
Posibilidad de robo 8 (sobre 12)



2 CAPAS
clase 2A1

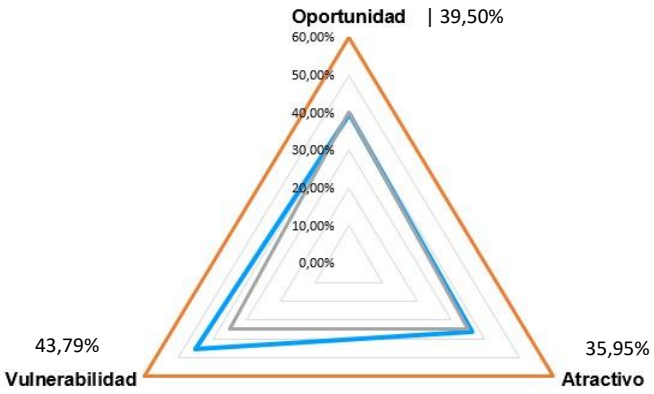
Evaluación básica + alarma inalámbrica interior.
Posibilidad de robo 7 (sobre 12)



1 CAPA
clase 1B2

Puerta seguridad UNE 85160 grado 4C | Rejas o persianas autoblocantes | Control suministro llave | Sin alarma.

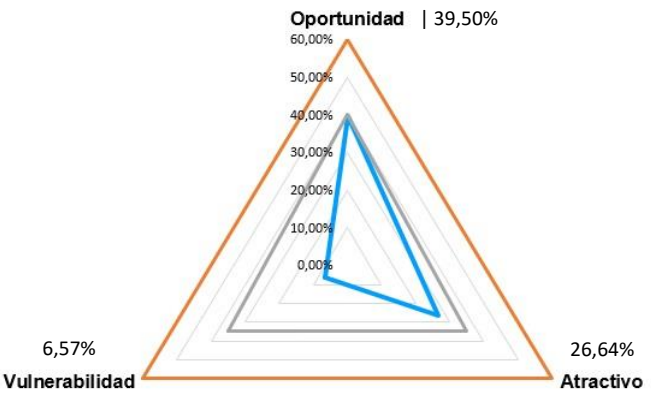
Posibilidad de robo 5 (sobre 12)



3 CAPAS
clase 3B2

Puerta seguridad UNE 85160 grado 4C | Rejas o persianas autoblocantes | Alarma cableada con doble vía | detección anticipada en puertas y ventanas | Control y proveedor acreditado.

Posibilidad de robo 2 (sobre 12)



EVIDENCIA 6. SOLO LA DEFENSA EN PROFUNDIDAD REDUCE ADECUADAMENTE LA POSIBILIDAD.
Aunque la vivienda se entrega con puerta acorazada (nivel medio), la vulnerabilidad es muy alta puesto que es fácilmente accesible por el perímetro de jardín y ventanas (clase 1A1). Al incluir sistema de alarma inalámbrico, los ratios mejoran muy poco porque el sistema no resuelve la debilidad del perímetro (el delincuente accede y escapa fácilmente - gráfico 2A1). En el gráfico 1B2, el ratio de vulnerabilidad mejora sustancialmente porque se aumenta la resistencia perimetral y mejora el control de suministro de llave (aún a pesar de no tener sistema de alarma). El gráfico 3B2 evidencia que la concatenación de medidas ordenadas en profundidad, son la única solución para reducir drásticamente la posibilidad del robo. Si sobre el gráfico 3B2, se activara la capa de protección interior (habitación refugio), el ratio de vulnerabilidad se reduciría a 1,57% con posibilidad de 1.

EVIDENCIA 7 | EL ENTORNO, DISEÑO ARQUITECTÓNICO Y LA VIGILANCIA NATURAL CONDICIONAN LA EFECTIVIDAD DE LAS MEDIDAS TÉCNICAS DE DEFENSA

En las siguientes tablas se evidencia que la misma medida tiene dispar efectividad dependiendo del tipo de vivienda y entorno. Por lo tanto, es necesaria una evaluación previa para diagnosticar diferenciadas medidas de defensa y conseguir la mayor efectividad posible, adaptada a cada tipología de vivienda y situación.

Medidas de defensa tipo **2A1 | Vivienda con 2 capas** (Seguridad física puntual + alarma interior inalámbrica).

Vivienda	Entorno	Op	At	Vu	POS (sobre 12)	Posibilidad
Piso en altura	Casco urbano / Urb Cerrada	39,50%	24,31%	***54,49%***	4	Baja +
Piso bajo jardín	Casco urbano / Urb Cerrada	39,50%	34,80%	***72,25%***	*6*	Media +
Piso ático	Casco urbano / Urb Cerrada	39,50%	34,80%	***72,25%***	*6*	Media +
Adosado	Zona residencial	39,50%	45,22%	***80,88%***	*7*	Alta -
Adosado	Zona aislada	39,50%	46,19%	***84,74%***	*8*	Alta +
Chalet independiente	Zona residencial	39,50%	57,73%	***86,33%***	*8*	Alta +
Chalet independiente	Zona aislada	39,50%	57,86%	***93,14%***	*9*	Muy alta +

Medidas de defensa tipo **1B2 | Vivienda con 1 capa integral** (Seguridad física perimetral / sin alarma).

Vivienda	Entorno	Op	At	Vu	POS (sobre 12)	Posibilidad
Piso en altura	Casco urbano / Urb Cerrada	39,50%	20,35%	***22,77%***	3	Baja -
Piso bajo jardín	Casco urbano / Urb Cerrada	39,50%	26,16%	***26,19%***	3	Baja -
Piso ático	Casco urbano / Urb Cerrada	39,50%	26,16%	***26,19%***	3	Baja -
Adosado	Zona residencial	39,50%	35,95%	***43,79%***	*5*	Media -
Adosado	Zona aislada	39,50%	43,16%	***72,63%***	*7*	Alta -
Chalet independiente	Zona residencial	39,50%	44,73%	***51,12%***	*6*	Media +
Chalet independiente	Zona aislada	39,50%	56,95%	***90,22%***	*9*	Muy alta +

Medidas de defensa tipo **3B2 | Vivienda con 3 capas integrales** (Seguridad física + Detección ant. + Control proveedor).

Vivienda	Entorno	Op	At	Vu	POS (sobre 12)	Posibilidad
Piso en altura	Casco urbano / Urb Cerrada	39,50%	17,90%	*--*	Medidas sobre dimensionadas	
Piso bajo jardín	Casco urbano / Urb Cerrada	39,50%	21,94%	***3,66%***	*1*	Muy baja -
Piso ático	Casco urbano / Urb Cerrada	39,50%	21,94%	***3,66%***	*1*	Muy baja -
Adosado	Zona residencial	39,50%	26,64%	***6,57%***	*2*	Muy baja +
Adosado	Zona aislada	39,50%	27,60%	***10,41%***	*2*	Muy baja +
Chalet independiente	Zona residencial	39,50%	31,03%	***7,29%***	*2*	Muy baja +
Chalet independiente	Zona aislada	39,50%	32,80%	***12,97%***	*3*	Baja -

Agradecemos especialmente la aportación de los sponsors que han apoyado y contribuido de manera desinteresada en este estudio de investigación y divulgación de datos para la mejora de las decisiones de compra de la ciudadanía en sistemas de seguridad residencial.

inn. SOLUTIONS

Maldonado smart

SUKOT

DISEC

FERRIMAX

WINK HAUS

grupo on seguridad S.L.

MOS MAPS OF SECURITY

Tecnoalarm

Ingeniería Blue Black

PREVENT

Madrid Noviembre 2018

Madrid Noviembre 2018