

GDR | GENOMA DEL ROBO®

Sello de prevención del delito
contra la intrusión.

GDR | ET-01.2_HÁBITOS |
Generalidades de la delincuencia
y de la prevención del delito.

ET | ESPECIFICACIÓN TÉCNICA.

GDR | ET-01.2_HÁBITOS | Generalidades de la delincuencia y de la prevención del delito.

TITULO

Prevención del delito contra la intrusión.

Prevención del delito a través del diseño de las infraestructuras y de la seguridad activa positiva.

Parte 1: GDR | ET-01.2_HÁBITOS | Generalidades de la delincuencia y de la prevención del delito.

TIPO DE DOCUMENTO

Especificación técnica ET.
Technical Specification TS.

ANTECEDENTES.

Esta especificación técnica enumera los hábitos recomendados para aumentar la efectividad de medidas técnicas en la protección de las viviendas contra la intrusión. Asimismo, aporta un mayor grado de disuasión en la acción delincuencia.

CPTID. Crime Prevention Through Infrastructure Design.
CPTID. Prevención del delito a través del diseño de las infraestructuras.
CP-PAS Seguridad por Diseño Activa Positiva.

CPTID&PAS / Prevención del delito a través del diseño de las infraestructuras y de la seguridad activa positiva.
CPTID&PAS / Crime prevention through infrastructure design and positive active security.



PRÓLOGO.

Esta especificación técnica es referida a enumerar los hábitos que han sido identificados como necesarios para complementar, de forma sostenible, la protección de viviendas contra la intrusión. De forma complementaria se enumeran algunos hábitos razonables para riesgos accidentales vinculados con agua, fuego y gases.

Esta instrucción técnica elaborada en el seno del ecosistema de empresas GDR, forma parte de un completo manual técnico para la estandarización internacional de soluciones contra la delincuencia (security) y los actos accidentales (safety) y que tiene su tronco en la divulgación de información de valor para los consumidores.

Manual técnico para la estandarización internacional de soluciones contra la delincuencia y actos accidentales. Technical manual for the international standardization of solutions against crime (security) and accidental acts (safety).

GDR / CPTID&PAS / Prevención del delito a través del diseño de las infraestructuras y de la seguridad activa positiva. GDR / CPTID&PAS / Crime prevention through infrastructure design and positive active security.

- Parte 1. GDR | ET-01 | Generalidades de la delincuencia y de la prevención del delito.
- Parte 2. GDR | ET-02 | Especificación técnica de neuroseguridad.
- Parte 3. GDR | ET-03 | Especificación técnica de seguridad por diseño.
- Parte 4. GDR | ET-04 | Especificación técnica para el análisis de riesgos.
- Parte 5. GDR | ET-05 | Especificación técnica niveles de protección en viviendas unifamiliares.
- Parte 6. GDR | ET-06 | Especificación técnica niveles de protección en entornos residenciales comunitarios.
- Parte 7. GDR | ET-07 | Especificación técnica niveles de protección en tiendas y oficinas.
- Parte 8. GDR | ET-08 | Especificación técnica niveles de protección en edificios.
- Parte 9. GDR | ET-09 | Especificación técnica para la aplicación de medidas técnicas CPTID.
- Parte 10. GDR | ET-10 | Especificación técnica para el diseño ambiental CPTED.

INTRODUCCIÓN.

Los hábitos en seguridad residencial han pasado a ser considerados la primera línea de defensa. Estos hábitos no pueden ser independientes y aleatorios, sino que tienen que considerarse en su conjunto. Para aumentar la protección contra el robo, los hábitos deben estar correlacionados y formar una estructura lógica de uso.

En términos generales, un hábito hace referencia a un acto que se toma por costumbre. Es una acción que alguien realiza tantas veces que “Se vuelve un hábito para ella”. Los hábitos por lo general son movimientos sencillos de las personas para complementar su vida de momentos y funciones. Son costumbres, propias de los seres humanos que se adaptan al entorno que les rodea.

Los hábitos en seguridad son costumbres de uso, que están procedimentadas y previamente acordadas con los usuarios, que guardan relación con el entorno y los sistemas, para aumentar el rendimiento de ciertas funcionalidades de estos sistemas de protección y para generar disuasión a través del dinamismo de las acciones humanas.

Cualquier funcionalidad del sistema, sin la activación de su hábito complementario, es en sí misma, una merma de las prestaciones del sistema.

Los hábitos son considerados la primera línea de defensa en la seguridad residencial puesto que son estos hábitos acometidos por los usuarios de los inmuebles, los que suplen las labores que los vigilantes de seguridad realizarían en edificios.

- La primera línea de defensa son los hábitos y procedimientos. Y cuan de importantes son en la protección efectiva.
- La segunda línea y la más extendida entre las empresas de seguridad, es la protección por tecnología, considerando sistemas físicos, electrónicos y ciber.
- La tercera línea de defensa se considera la gestión, mantenimiento y actualización de medidas, tanto técnicas como procedimentales, debido a que las situaciones, como se refleja en el modelo de gestión del riesgo, son dinámicas y los sistemas deben ser mantenidos para reducir su tendencia al caos y desorden a los que les aboca su nivel de entropía.

Un hábito genera una protección, y un «no hábito» genera una vulnerabilidad, que es aprovechada por el delincuente. Cualquier funcionalidad del sistema de seguridad, sin la activación de su hábito complementario, es en sí mismo una merma de las prestaciones del sistema.

Todos los proyectos de seguridad residencial deben incorporar su correspondiente análisis de riesgos y los hábitos asociados a los sistemas recomendados con el propósito de protección contra la intrusión y riesgos accidentales.

CAMPO DE APLICACIÓN.

Esta especificación técnica enumera hábitos en seguridad que acompañan y complementan a las diferentes medidas técnicas que protegen viviendas. Se han clasificado según las siguientes consideraciones:

1. Generales de buenas prácticas.
2. Para sistemas de seguridad física.
3. Para sistemas de seguridad electrónica.
4. Para el control.
5. Contra ataques cibernéticos.
6. Riesgos accidentales Safety.
7. Mantenimiento.

1. GENERALES Y DE BUENAS PRÁCTICAS.

<ol style="list-style-type: none"> 1. Mantener luces exteriores encendidas en horario nocturno. 2. Mantener buzón vacío para no evidenciar ausencias largas. 3. Quitar felpudo para ausencias largas. 4. Simular presencia con luces y ligero movimiento de persianas pero sin dejar estas a media altura. 5. Ocultar leds de contadores que evidencien la ausencia de actividad en la vivienda o simular presencia que active el consumo. 6. No publicar fotos en redes sociales cuando se ausenta de la vivienda. 7. No publicar fotos del interior de la vivienda (en ningún caso). Menos aún si se observa la posición de detectores y cámaras. 8. Socializar con vecinos para poder avisar de ausencias (vigilancia natural comunitaria). 9. En caso de alta atractividad para el robo, modificar las tareas cotidianas de salida de casa, preferiblemente que sean en horarios diferentes para evitar la planificación delictiva. 10. No "abrir" sin verificar la identidad y/o necesidad de acceso de esa persona. Tanto en la propia vivienda como en accesos de la comunidad. 11. No guardar grandes cantidades de efectivo en casa. 12. No dejar en el exterior objetos que faciliten escalada. 13. Dejar las puertas de los vehículos cerradas, incluso dentro de la parcela en viviendas unifamiliares. 	<ol style="list-style-type: none"> 14. No dejar llaves del coche a distancias cortas (hall vivienda) que permitan activar el sistema de arranque por un externo. 15. No dejar nunca el mando de garaje, ni mucho menos de activación de alarma, ni llaves de la vivienda en el interior del vehículo. 16. No dejar llaves en exteriores, a modo de "de emergencia", utilizando maceteros ni otros pseudo-escondites caseros. 17. No dejar sin custodia herramientas que permitan ataques (sobre todo eléctricas). 18. Revisión de puertas y ventanas para detectar marcas delictivas. 19. Romper la rutina de aparcamiento dentro-fuera garaje para evitar planificación de ataque cuando el vehículo no está (aparcar dentro del garaje). 20. Desconectar enchufes del jardín. 21. Siempre disponer del sistema de alarma activado en las zonas donde no hay uso momentáneo durante el día/noche. 22. Nunca divulgar la ubicación del sistema de intrusión (vecinos, familiares, visitantes, ...). No presumir. 23. Esperar siempre al cierre efectivo de la puerta de vehículos de la parcela, al entrar y al salir con el coche (viviendas independientes y garajes comunitarios). 24. Revisión y actualización de pólizas de seguros, evitan el concepto de infraseguro. 25. Disponer de un listado de enseres de valor en el hogar, con nombre, foto y valor estimado (enviar a la compañía de seguros en el momento de la actualización-contratación). 26. Tener un control de páginas de navegación de menores.
--	---

2. PARA SISTEMAS DE SEGURIDAD FÍSICA.

<p>27. En caso de nueva compra o alquiler, cambiar todos los bombillos y llaves de la vivienda (parcela incluida).</p> <p>28. Mantener cerradas las puertas con vuelta de cerrojo en todo momento, durante el día, en ausencias momentáneas superiores a 15 minutos y en periodos vacacionales.</p> <p>29. Mantener ventanas cerradas de todas las dependencias, sobre todo, en las que no exista actividad momentánea.</p> <p>30. Utilizar siempre bombillos de seguridad con doble embrague y no dejar las llaves "puestas" en la puerta, ni a la vista.</p> <p>31. Mantener cerrada la puerta de la habitación refugio por la noche (si se dispone de zona refugio en planta habitaciones).</p> <p>32. Cerrar, cuando todos los vehículos estén en casa, los cerrojos manuales del portón de garaje. También en ausencias prolongadas, acordándose de abrirlos al regreso, antes de activar el mando del motor de la puerta automática (evita forzamientos y roturas).</p> <p>33. En caso de garaje con acceso directo a la vivienda, mantener cerrada con cerrojo, la puerta de interconexión.</p>	<p>34. Para cajas de seguridad o cajas fuertes, cambiar las claves de fábrica inmediatamente y suprimir el código "master" de instalador.</p> <p>35. En caso de caja fuerte profesional, conectar el retardo en la caja fuerte como mínimo 10 minutos. Se considera una caja profesional todas aquellas reguladas por la norma UNE-EN1143-1.</p> <p>36. En caso de no tener un mantenimiento contratado, realizar ciertas labores como; lubricación en elementos como bombillos de seguridad, núcleos de escudos protectores, mantener limpias las guías de las ventanas y hacer comprobaciones de elementos poco utilizados, así como los lados interiores de ciertos bombillos.</p> <p>37. En el día a día, mantener persianas de seguridad con autoblocante, prácticamente bajadas o bajadas totalmente, sobre todo en lugares donde no exista vigilancia. En ningún caso, cuando se ausentan de la vivienda, dejar las persianas a "medio bajar" para simular presencia. Las persianas no pueden ofrecer más de 20cms de abertura.</p> <p>38. Asegurarse de que las puertas comunitarias cierran correctamente.</p>
--	---

3. PARA SISTEMAS DE SEGURIDAD ELECTRÓNICA.

<p>39. Activar la alarma por zonas con la vivienda ocupada. Para ello, es necesario disponer de un sistema de intrusión segmentado en diferentes zonas que coincidan con el uso diario de esta zona y permita vivir con el sistema conectado permanentemente en las zonas no ocupadas. Así mismo es necesario que cada zona/escenario disponga de su armado personalizado e independiente.</p> <p>40. Activar la alarma "total", cuando la vivienda está desocupada (inclusive en ausencias de 15 minutos).</p> <p>41. Las desactivaciones serán realizadas únicamente mediante aplicación móvil para no disponer de retardos en la detección.</p> <p>42. Enseñar el uso de los sistemas a toda la familia y a otros usuarios que sean habituales en la casa (personal de limpieza, jardinería, mantenimiento). Siempre al nivel que les corresponda por uso y/o acceso.</p>	<p>43. No aparcar el vehículo en zonas de detección perimetral. El diseño del sistema de seguridad debe contemplar las zonas habilitadas para el aparcamiento sin oclusiones de detección.</p> <p>44. No mostrar la funcionalidad del sistema de seguridad a ninguna persona externa.</p> <p>45. Educar a los niños, que, si escuchan la sirena interior, deberán desplazarse con calma, pero sin perder el tiempo a la zona refugio.</p> <p>46. Cambiar regularmente los códigos de acceso del sistema de alarma.</p> <p>47. Instalar un magneto térmico independiente para enchufes de jardín y desconectarlos.</p> <p>48. Forzar el sistema simulando una intrusión para comprobar la efectividad de todo el sistema y comprobar la efectividad del servicio de conexión a Central Receptora de alarma. Simular detección de "reptil" y corte de línea.</p>
--	--

4. PARA EL CONTROL.

<p>49. Disponer de un documento de confidencialidad para empleados del hogar y para contratos de servicios / obras.</p> <p>50. Disponer de toda la documentación de uso de los sistemas de seguridad instalados, incluyendo planos de ubicaciones y cableados.</p> <p>51. Disponer de las declaraciones de conformidad de la correcta instalación de los sistemas, incluyendo nombre completo, DNI y firma del operario.</p> <p>52. Disponer de todos los códigos de acceso de los sistemas electrónicos, y que los operarios, requieran solicitar estos códigos para labores de mantenimiento.</p> <p>53. Disponer de las facturas de compra y mantenimientos posteriores, así como el libro de inspecciones (muy relevante para posteriores reclamaciones en caso de robo, incluso en juicios).</p> <p>54. En caso de servicios de mantenimiento de sistemas de seguridad, siempre deben ser operarios bien identificados (DNI + aviso de la empresa). Deben ser conocedores del sistema. Preferiblemente siempre los mismos.</p> <p>55. Contratar a personal de servicio que entregue certificado de penales y datos personales. Igualmente, para trabajos de conserjería comunitaria.</p> <p>56. No depositar llaves de la vivienda en custodia de conserjería, salvo que la garita del conserje disponga de seguridad física adecuada y la vivienda disponga de sistema de alarma y este esté conectado.</p> <p>57. Restringir la información al conserje, a la estrictamente necesaria para sus labores de conserjería. Más aún, a conserjes suplentes en periodos vacacionales.</p> <p>58. Disponer de un sistema de aviso automático para conocer si alguna persona ha solicitado una copia de llave/mando, o conocer si un técnico del sistema de alarma, ha cambiado alguna configuración de seguridad sin conocimiento de la propiedad.</p> <p>59. Documento firmado de empleados para garantizar el buen uso de llaves, mandos y devolución de estas cuando se les pidan por cese de la actividad profesional.</p> <p>60. No entregar llaves maestras a personas fuera del círculo de confianza.</p>	<p>61. En caso de servicios externos de mantenimiento, acompañar siempre a los operarios. En todo momento. Si deben circular por la vivienda, zona habitaciones, procurar tener las puertas cerradas de dependencias que no requieren su acceso (aumento de privacidad).</p> <p>62. Tener todas las llaves/mandos custodiados (las que están en uso y las de reserva), no dejarlas nunca a la vista de otros o de fácil acceso. Preferiblemente en caja fuerte UNE 1143 grado II o superior.</p> <p>63. Disponer de puertas con llave de servicio para restringir el uso indebido.</p> <p>64. El servicio doméstico e invitados, no deben disponer de todas las medidas de acceso a la vivienda. Restringir claves de alarma o llaves (preferiblemente restringir claves de alarma). En el caso del servicio doméstico, éste comunicará a los propietarios el fin de la jornada laboral para que estos activen la alarma en remoto de esta forma evitar la posibilidad de que los asaltantes esperen a los propietarios dentro de la vivienda.</p> <p>65. Disponer de un plan de amaestramiento jerarquizado en diferentes niveles de uso para diferentes usuarios. Este plan aporta mayor seguridad, restricciones de uso y confortabilidad.</p> <p>66. En caso de disponer de control de acceso electrónico en puertas de viviendas, asegurarse de, quienes tienen claves de acceso o llaves electrónicas, y como se formaliza la confidencialidad en el proveedor de servicios / suministro.</p> <p>67. Antes de salir de casa o a la hora de dormir, hacer una ronda de comprobación para verificar el cierre de todas las puertas, ventanas, persianas y conexión de las zonas de alarmas.</p> <p>68. Cada cierto tiempo cambio de contraseña tanto del wifi como de la alarma.</p> <p>69. Si se teletrabaja custodiar el portátil en un lugar seguro fuera del alcance de empleados.</p> <p>70. Recordar siempre tener en cuenta el protocolo de petición de llaves de la familia/empleados cuando terminan su estancia/trabajo.</p> <p>71. Todas las contraseñas deben ser alfanuméricas, con más de ocho dígitos.</p> <p>72. Las llaves de seguridad, deben cambiarse cada 5-7 años.</p>
--	--

5. CONTRA ATAQUES CIBERNÉTICOS.

<p>73. En general, hay que ser cautos con las interconexiones entre el sistema de seguridad y la domótica con o sin dispositivos IoT, ya que, en ningún momento, la domótica debe comandar el sistema de seguridad, sino todo lo contrario. El sistema de seguridad es prioritario ante cualquier función automática. En caso de vincular sistema domótico con automatismos de apertura de puertas o de activación motores de persianas, instalar un dispositivo firewall profesional para evitar sabotajes en remoto y aperturas por fallos del sistema.</p> <p>Los dispositivos electrónicos de confort y vigilancia, adquiridos en plataformas digitales y autoinstalables, en ningún caso pueden estar conectados a la misma red de comunicaciones que los sistemas de seguridad. Asimismo, se recomienda ser cautos con dispositivos robots inteligentes o cámaras IoT, que pueden servir a los delincuentes para el pre-delito (planificación de una intrusión, averiguación de rutinas, códigos, etc).</p>	<p>74. Cambiar las contraseñas del wifi regularmente.</p> <p>75. No compartir wifi principal con invitados. Disponer de otra clave de "invitados".</p> <p>76. No conectar ni permitir la conexión de ningún elemento IoT al switch del firewall (cortafuegos físico).</p> <p>77. Vincular el acceso en remoto del sistema de seguridad con una IP fija de acceso – y si posible con VPN- y no a través de IP dinámicas.</p> <p>78. No repetir contraseñas en App's ni plataformas.</p> <p>79. En caso de teletrabajo, operar siempre en la red protegida del firewall y de forma cableada.</p> <p>80. Disponer de copia de seguridad actualizada.</p>
---	---

6. CONTRA RIESGOS ACCIDENTALES (SAFETY).

<p>81. El sistema de detección de incendio debe de conectarse al sistema de alarma, y así poder aprovechar las comunicaciones y aplicaciones del sistema de seguridad. Al estar conectado a la Central Receptora de Alarmas (CRA), pueden generar un aviso a Bomberos u otras emergencias en caso de necesidad.</p> <p>82. Cerrar siempre las llaves de agua y de gas cuando nos ausentemos largas estancias.</p> <p>83. No sobrecargar enchufes eléctricos.</p> <p>84. Dejar desconectados en la manera de lo posible todos los enchufes no esenciales (electrodomésticos y mantenimiento de la vivienda) en ausencias más o menos prolongadas.</p>	<p>85. Las viviendas deben disponer de detectores de incendio, al menos dos dependiendo dimensiones; un detector térmico en la zona de la cocina y un detector de monóxido de carbono en el garaje. Igualmente, detectores de inundación (fugas de agua). Todos ellos deben estar conectados con el sistema de alarma.</p> <p>86. Disponer de manta ignífuga y extintores AFFF (útil para cocina, fuego, grasa)..</p> <p>87. Mantener un rigor en el mantenimiento preventivo del safety, por ejemplo, la caducidad de los extintores si los hubiera.</p> <p>88. En caso de viviendas con piscina, cerrar la piscina con valla perimetral.</p>
--	--

7. MANTENIMIENTO.

<p>89. Se ha recibido un plan formativo – práctico del sistema de seguridad implantado. Se conoce el protocolo de seguridad en caso de activación de alarma.</p> <p>90. Disponer de un programa de mantenimiento preventivo y mantenimiento correctivo de todos los sistemas de seguridad (intrusión y safety) y de otros que pudieran generar entropía y oclusiones (vegetación, iluminación, infraestructuras).</p> <p>91. En general, mantener el orden en todas las zonas visibles para no mostrar oportunidad al delincuente, ni mostrar dejadez.</p> <p>92. No dejar objetos en el jardín, en zonas de detección, que generen oclusiones de detectores y cámaras.</p> <p>93. Mantener la vegetación del jardín organizada y podada para evitar oclusiones en la detección.</p> <p>94. Mantener el orden en el interior (mobiliario, cortinas y plantas) para evitar oclusiones.</p> <p>95. Mantenimiento del jardín, objetos en su sitio habitual y ante cualquier cambio comunicarlo a su consultor de seguridad por si modifica algún detalle.</p>	<p>96. Comprobar de vez en cuando que los equipos de seguridad están conectados y operativos; el SAI funciona, las cámaras están bien orientadas y limpias, el video grabador se encuentra grabando y su horario es correcto.</p> <p>97. Verificar que la compañía de seguridad realiza los mantenimientos periódicos y comprobar de vez en cuando que la CRA funciona correctamente.</p> <p>98. No aparcarse el vehículo en zonas de detección perimetral, donde pueda haber oclusiones. Evitar que el vehículo, aparcado cercano a la fachada de la parcela, sirva de escalada para trepar y/o de pantalla de oclusión.</p>
--	---

8. HABITUALIDAD DE HÁBITOS APLICADOS Y VINCULADOS A LAS MEDIDAS TÉCNICAS.

Leyenda:

Habitualmente se comunican a los usuarios y estos los aplican.	
Se comunican por las empresas de seguridad, pero no son aplicados por los usuarios.	
Aún, ni siquiera se comunican a los usuarios.	

Nº	Hábito	Situación
1	Mantener luces exteriores encendidas en horario nocturno.	
2	Mantener buzón vacío para no evidenciar ausencias largas.	
3	Quitar felpudo para ausencias largas.	
4	Simular presencia con luces y ligero movimiento de persianas, pero sin dejar estas a media altura.	
5	Ocultar leds de contadores que evidencien la ausencia de actividad en la vivienda.	
6	No publicar fotos en redes sociales cuando se ausenta de la vivienda.	
7	No publicar fotos del interior de la vivienda (en ningún caso) ...	
8	Socializar con vecinos para poder avisar de ausencias (vigilancia natural comunitaria).	
9	En caso de alta atraktividad para el robo, modificar las tareas cotidianas de salida de casa ...	
10	No "abrir" sin verificar la identidad y/o necesidad de acceso de esa persona ...	
11	No guardar grandes cantidades de efectivo en casa.	
12	No dejar en el exterior objetos que faciliten escalada.	
13	Dejar las puertas de los vehículos cerradas, incluso dentro de la parcela en viviendas unifamiliares.	
14	No dejar llaves del coche a distancias cortas (hall vivienda) ...	
15	No dejar nunca el mando de garaje, ni mucho menos de activación de alarma ...	
16	No dejar llaves en exteriores, a modo de "de emergencia", utilizando maceteros ...	
17	No dejar sin custodia herramientas que permitan ataques (sobre todo eléctricas).	
18	Revisión de puertas y ventanas para detectar marcas delincuenciales.	
19	Romper la rutina de aparcamiento dentro-fuera garaje ...	
20	Desconectar enchufes del jardín.	
21	Siempre disponer del sistema de alarma activado en las zonas ...	
22	Nunca divulgar la ubicación del sistema de intrusión (vecinos, familiares, visitantes, ...). No presumir.	
23	Esperar siempre al cierre efectivo de la puerta de vehículos de la parcela, al entrar y al salir ...	
24	Revisión y actualización de pólizas de seguros, evitan el concepto de infraseguro.	
25	Disponer de un listado de enseres de valor en el hogar, con nombre, foto y valor estimado ...	
26	Tener un control de páginas de navegación de menores.	

27	En caso de nueva compra o alquiler, cambiar todos los bombillos y llaves de la vivienda ...	
28	Mantener cerradas las puertas con vuelta de cerrojo en todo momento, durante el día, ...	
29	Mantener ventanas cerradas de todas las dependencias, ...	
30	Utilizar siempre bombillos de seguridad con doble embrague y no dejar las llaves "puestas" ...	
31	Mantener cerrada la puerta de la habitación refugio por la noche ...	
32	Cerrar, cuando todos los vehículos estén en casa, los cerrojos manuales del portón de ...	
33	En caso de garaje con acceso directo a la vivienda, mantener cerrada con cerrojo, ...	
34	Para cajas de seguridad o cajas fuertes, cambiar las claves de fábrica inmediatamente ...	
35	En caso de caja fuerte profesional, conectar el retardo en la caja fuerte como mínimo 10 minutos ...	
36	En caso de no tener un mantenimiento contratado, realizar ciertas labores como; ...	
37	En el día a día, mantener persianas de seguridad con autoblocante, prácticamente bajadas, o ...	
38	Asegurarse de que las puertas comunitarias cierran correctamente.	
39	Activar la alarma por zonas con la vivienda ocupada ...	
40	Activar la alarma "total", cuando la vivienda está desocupada momentáneamente ...	
41	Las desactivaciones serán realizadas únicamente mediante aplicación móvil ...	
42	Enseñar el uso de los sistemas a toda la familia y a otros usuarios que sean habituales en la casa ...	
43	No aparcar el vehículo en zonas de detección perimetral ...	
44	No mostrar la funcionalidad del sistema de seguridad a ninguna persona externa ...	
45	Educar a los niños, que, si escuchan la sirena interior, deberán desplazarse con calma, ...	
46	Cambiar regularmente los códigos de acceso del sistema de alarma ...	
47	Instalar un magneto térmico independiente para enchufes de jardín y desconectarlos ...	
48	Forzar el sistema simulando una intrusión para comprobar la efectividad de todo el sistema ...	
49	Disponer de un documento de confidencialidad para empleados del hogar y ...	
50	Disponer de toda la documentación de uso de los sistemas de seguridad instalados, incluyendo ...	
51	Disponer de las declaraciones de conformidad de la correcta instalación de los sistemas ...	
52	Disponer de todos los códigos de acceso de los sistemas electrónicos, y que los operarios ...	
53	Disponer de las facturas de compra y mantenimientos posteriores, así como el libro de ...	
54	En caso de servicios de mantenimiento de sistemas de seguridad, siempre deben ser operarios ...	
55	Contratar a personal de servicio que entregue certificado de penales y datos personales ...	
56	No depositar llaves de la vivienda en custodia de conserjería, salvo que la garita del conserje ...	
57	Restringir la información al conserje, a la estrictamente necesaria para sus labores de conserjería ...	
58	Disponer de un sistema de aviso automático para conocer si alguna persona ha solicitado una ...	
59	Documento firmado de empleados para garantizar el buen uso de llaves, mandos y devolución ...	
60	No entregar llaves maestras a personas fuera del círculo de confianza.	

61	En caso de servicios externos de mantenimiento, acompañar siempre a los operarios ...	
62	Tener todas las llaves/mandos custodiados (las que están en uso y las de reserva), no ...	
63	Disponer de puertas con llave de servicio para restringir el uso indebido.	
64	El servicio doméstico e invitados, no deben disponer de todas las medidas de acceso ...	
65	Disponer de un plan de amaestramiento jerarquizado en diferentes niveles de uso para ...	
66	En caso de disponer de control de acceso electrónico en puertas de viviendas, asegurarse de ...	
67	Antes de salir de casa o a la hora de dormir, hacer una ronda de comprobación para verificar ...	
68	Cada cierto tiempo cambio de contraseña tanto del wifi como de la alarma.	
69	Si se teletrabaja custodiar el portátil en un lugar seguro fuera del alcance de empleados.	
70	Recordar siempre tener en cuenta el protocolo de petición de llaves de la familia/empleados ...	
71	Todas las contraseñas deben ser alfanuméricas, con más de ocho dígitos.	
72	Las llaves de seguridad, deben cambiarse cada 5-7 años.	
73	Hay que ser cautos con las interconexiones entre el sistema de seguridad y la domótica ...	
74	Cambiar las contraseñas del wifi regularmente.	
75	No compartir wifi principal con invitados. Disponer de otra clave de "invitados".	
76	No conectar ni permitir la conexión de ningún elemento IoT al switch del firewall (cortafuegos físico).	
77	Vincular el acceso en remoto del sistema de seguridad con una IP fija de acceso – y si posible ...	
78	No repetir contraseñas en App's ni plataformas.	
79	En caso de teletrabajo, operar siempre en la red protegida del firewall y de forma cableada.	
80	Disponer de copia de seguridad actualizada.	
81	El sistema de detección de incendio debe de conectarse al sistema de alarma, ...	
82	Cerrar siempre las llaves de agua y de gas cuando nos ausentemos largas estancias.	
83	No sobrecargar enchufes eléctricos.	
84	Dejar desconectados en la manera de lo posible todos los enchufes no esenciales ...	
85	Las viviendas deben disponer de detectores de incendio, al menos dos dependiendo ...	
86	Disponer de manta ignifuga y extintores.	
87	Mantener un rigor en el mantenimiento preventivo del safety, por ejemplo, ...	
88	En caso de viviendas con piscina, cerrar la piscina con valla perimetral.	
89	Se ha recibido un plan formativo – práctico del sistema de seguridad implantado ...	
90	Disponer de un programa de mantenimiento preventivo y mantenimiento correctivo de todos ...	
91	En general, mantener el orden en todas las zonas visibles para no mostrar oportunidad al ...	
92	No dejar objetos en el jardín, en zonas de detección, que generen oclusiones de detectores y ...	
93	Mantener la vegetación del jardín organizada y podada para evitar oclusiones en la detección.	
94	Mantener el orden en el interior (mobiliario, cortinas y plantas) para evitar oclusiones.	
95	Mantenimiento del jardín, objetos en su sitio habitual y ante cualquier cambio comunicarlo a ...	

96	Comprobar de vez en cuando que los equipos de seguridad están conectados y operativos; ...	
97	Verificar que la compañía de seguridad realiza los mantenimientos periódicos y comprobar ...	
98	No aparcar el vehículo en zonas de detección perimetral, donde pueda haber oclusiones ...	

Porcentaje de aplicación de los hábitos necesarios en seguridad residencial.

- a) Total, de hábitos necesarios para la seguridad residencial: 98.
- b) Hábitos que se comunican a los usuarios: 44 (supone el 45% de los necesarios).
- c) Hábitos que aplican los usuarios: 8 (supone el 8% del total y el 18% de los que son comunicados).

Existen 54 hábitos que, por diferentes razones, las empresas de sistemas de seguridad (físicos y electrónicos), aún no tienen protocolarizados en sus diseños y no son comunicados a los usuarios.