ADENDA — CIBERSEGURANÇA RESIDENCIAL

Wi-Fi Seguro numa casa com Dispositivos IoT

Guia prático para residências com televisões inteligentes, câmeras, assistentes de voz, termostatos e outros dispositivos ligados. Como isolar, proteger e monitorizar sem ser especialista de IT.

Complemento ao Guia Principal ·

CONTEXTO

Em 2025, uma residência portuguesa tem em média 12 dispositivos ligados a internet.

Em 2028 esse número deve ultrapassar os 20. Cada dispositivo e um ponto de entrada potencial.

Este guia e um complemento ao artigo principal e foca-se exclusivamente nas ameaças e soluções especificas para ambientes IoT residenciais.

1. O Que e um Dispositivo IoT — e Porque e Diferente do Seu Computador

IoT (Internet of Things) significa, literalmente, Internet das Coisas. São todos os dispositivos que ligam a internet mas que não são computadores tradicionais, por exemplo: televisões inteligentes, cameras de vigilância, assistentes de voz, fechaduras smart, termostatos, balanças, robots aspiradores e muito mais.

A diferença critica de segurança é esta: o seu computador recebe atualizações de segurança regulares, tem um antivírus, e o utilizador (você) interage com ele todos os dias. Um dispositivo IoT pode estar ligado a internet durante anos sem receber uma única atualização e provavelmente nem pensa nele.

Categoria	Exemplos de dispositivos	Risco base
Entretenimento	TV, streaming box, consola de jogos, coluna Bluetooth	**Médio**
Segurança	Câmera IP, campainha inteligente, fechadura smart	**Alto**
Casa inteligente	Termostato, persiana, tomada, interruptor smart	**Médio**
Voz & IA	Assistente de voz (Echo, Google Home, Siri)	**Alto**
Rede & Internet	Repetidores Wi-Fi, powerline adapters, NAS	**Crítico**
Wearables & Saúde	Smartwatch, balança, monitor de sono, glucómetro	**Baixo**

O PROBLEMA CENTRAL DOS DISPOSITIVOS IOT

São concebidos para ser baratos e fáceis de instalar — a segurança e uma prioridade secundaria.

Muitos usam sistemas operativos Linux antigos sem suporte oficial continuado.

Fabricantes abandonam produtos passados 2-3 anos sem lançar mais atualizações.

As passwords de fábrica são iguais para todos os dispositivos do mesmo modelo — e são publicas.

2. Ameaças Especificas em Redes com Dispositivos IoT

Alem das ameaças já cobertas no guia principal, uma rede com dispositivos IoT esta exposta a riscos adicionais e específicos.

Botnets IoT — O Seu Frigorifico a Atacar Bancos

Este e provavelmente o cenário mais comum e menos visível. Em 2016, a botnet Mirai comprometeu milhões de camaras e routers domésticos para lançar o maior ataque DDoS da história, derrubando grandes sites como Twitter e Netflix.

Como funciona: um software malicioso infeta o seu dispositivo IoT (que raramente tem antivírus). O dispositivo continua a funcionar normalmente para si, mas em segundo plano executa ataques a terceiros. O seu consumo de dados aumenta ligeiramente — e praticamente impossível de detectar sem ferramentas especializadas.

Espiões em Casa — Cameras e Microfones Comprometidos

Cameras IP de baixo custo (marcas como Tenda, Hikvision em versões antigas, ou marcas brancas de sites de comercio eletrónico) são frequentemente comercializadas com backdoors, isto é, acessos secretos que permitem ao fabricante (ou a quem os descobrir) visualizar o feed em tempo real.

Em 2023, o portal Shodan (um motor de busca para dispositivos ligados a internet) listava mais de 800.000 cameras acessíveis publicamente na internet — sem password, ou com a password de fabrica. Muitas em residências europeias.

> **COMO VERIFICAR SE A SUA CAMERA ESTA EXPOSTA**
>
> 1. Aceda a shodan.io e pesquise pelo modelo da sua camera.
> 2. Verifique se a interface de configuração esta acessível a partir da internet (WAN access).
> 3. Se estiver, desative imediatamente o acesso remoto nas configurações da camera.
> 4. Coloque a camera numa VLAN/rede IoT isolada (ver Seccao 3).

Assistentes de Voz — Privacidade e Seguranca

Dispositivos como Amazon Echo, Google Nest ou Apple HomePod estao sempre em escuta ativa. Investigadores de segurança demonstraram que é possível ativar estes dispositivos remotamente através de comandos de voz inaudíveis para humanos (ultrassons), enviados por alto-falantes à distancia ou mesmo por vídeo no YouTube.

Alem disso, as conversas são processadas em servidores externos. Em caso de comprometimento da sua conta na Amazon, Google ou Apple, um atacante pode aceder ao histórico de conversas.

Lateral Movement — O Dispositivo como Trampolim

Este é o cenário mais perigoso para redes domesticas não segmentadas. Um atacante compromete um dispositivo IoT de baixa segurança (por exemplo, uma tomada inteligente de 15 euros). A partir dai, analisa a rede interna e identifica dispositivos mais valiosos: o NAS com as fotos e documentos da família, o computador com as passwords guardadas no browser, o router.

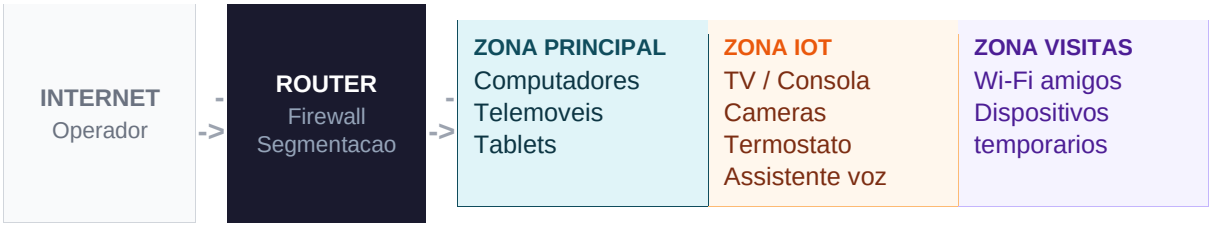
Sem segmentação de rede, o caminho e direto. Com segmentação, o atacante fica confinado a zona IoT e não consegue aceder ao resto da rede.

3. A Solução Fundamental: Segmentação da Rede

A segmentação de rede e o principio mais importante para proteger uma casa com dispositivos IoT. A ideia é simples: separar os dispositivos em grupos, de forma a que um dispositivo comprometido num grupo não consiga comunicar com os dispositivos nos outros grupos.

Pense numa vivenda com vários apartamentos: cada apartamento tem a sua própria fechadura. Se um ladrão entrar num apartamento, não tem automaticamente acesso aos outros.

Arquitectura Recomendada



Esta separação e conseguida de duas formas, dependendo do equipamento disponível:

- **Rede de convidados do router:** a solução mais simples. A maioria dos routers modernos permite criar uma rede Wi-Fi separada (normalmente chamada 'Guest Network'). Todos os dispositivos IoT devem ser ligados a esta rede. O custo: zero.
- **VLANs (Virtual LANs):** solução mais avançada, disponível em routers de gama media/alta (ASUS, TP-Link, Ubiquiti). Permite criar redes logicamente separadas com regras de comunicação especificas. Recomendado para quem tem muitos dispositivos IoT ou necessidades de segurança mais elevadas.

PASSO A PASSO: CRIAR A REDE IOT NO SEU ROUTER

1. Entre no painel do router (192.168.1.1 ou 192.168.0.1).
2. Procure 'Rede de Convidados', 'Guest Network' ou 'Wi-Fi secundário'.
3. Ative a rede com um nome neutro (ex: 'Rede2' ou 'IoT-Casa').
4. Defina uma password forte e diferente da rede principal.
5. Certifique-se que a opção 'Isolamento de clientes' ou 'Client Isolation' esta ATIVA.
6. Ligue todos os dispositivos IoT a esta nova rede — não a principal.

4. Checklist de Seguranca para Cada Dispositivo IoT

Aplique estes passos a cada dispositivo IoT que instalar em casa. O ideal e faze-lo no momento da instalacao.

1 **Mude imediatamente as credenciais do dispositivo** Crítico

A maioria dos dispositivos IoT vem com utilizador e password predefinidos — publicados online pelo fabricante. Altere-os assim que instalar o aparelho. Se o dispositivo não permitir alterar a password, considere substituí-lo.

2 **Ligue o IoT exclusivamente na rede de visitas/IoT** Crítico

Nunca coloque câmeras, TVs ou assistentes de voz na mesma rede dos seus computadores e telemóveis. Se o dispositivo for comprometido, o atacante fica isolado na rede IoT e não consegue aceder ao resto.

3 **Ative as atualizações automáticas** Alto

Dispositivos IoT são conhecidos por não receber atualizações durante anos. Verifique se há atualizações de firmware disponíveis e ative a atualização automática sempre que possível. Se o fabricante já não dá suporte ao dispositivo, é hora de o substituir.

4 **Desative funcionalidades não usadas** Alto

Bluetooth, Z-Wave, Zigbee, ligação remota, microfone — se não usa, desative. Cada funcionalidade ativa é uma porta adicional que pode ser explorada. Câmeras de segurança com acesso remoto ativo que "nunca são usadas" são um risco frequente.

5 **Verifique as permissões das apps de controlo** Médio

As aplicações dos fabricantes (para controlar a câmera, o termostato, etc.) pedem frequentemente permissões excessivas: acesso à localização, contactos, microfone. Reveja e recuse tudo o que não for estritamente necessário.

6 **Isole câmeras e microfones fisicamente quando possível** Médio

Assistentes de voz ouvem constantemente. Câmeras gravam. Para divisões privadas, considere desligar o dispositivo quando não é usado, ou usar um interruptor físico na ficha. Alguns dispositivos têm botões de mute do microfone — use-os.

5. Passwords e Gestores de Passwords

Uma das vulnerabilidades mais exploradas em dispositivos IoT sao as passwords fracas ou as passwords padrão de fábrica. A tabela abaixo mostra exemplos práticos de como a forca de uma password afeta dramaticamente o tempo necessário para a quebrar.

Exemplo	Forca	Tempo a quebrar	Observacao
`casa123`	**Muito fraca**	< 1 seg	Palavra comum + número simples
`CasaAzul2024`	**Fraca**	dias	Previsível, dicionário expandido
`C@s4Az!2024`	**Moderada**	meses	Substituições obvias
`Gato!Telhado#Rio`	**Forte**	seculos	3 palavras aleatórias + símbolos
`Xk9#mP2$vL8@nQ`	**Excelente**	milénios	Gerada por gestor de passwords

A Solução Pratica: Use um Gestor de Passwords

Memorizar dezenas de passwords fortes e impossível. A solução profissional — e a que qualquer especialista de segurança usa pessoalmente — e um gestor de passwords.

- **Bitwarden:** gratuito, open-source, disponível em todos os dispositivos. Recomendado para utilizadores domestico.
- **1Password:** pago, excelente interface, muito usado em empresas.
- **KeePass:** gratuito, os dados ficam no seu dispositivo (não na cloud). Para quem prefere controlo total.

Um gestor de passwords gera passwords únicas e complexas para cada dispositivo ou serviço, e recorda-as por si. A única password que tem de memorizar e a password mestra do gestor.

6. Como Monitorizar a Sua Rede Regularmente

Segurança não é um evento único é um processo continuo. Estabeleça uma rotina de verificação com base na tabela abaixo.

DIÁRIO

- ☐ Verificar se o router esta acessivel
- ☐ Rever alertas do ISP ou app do router

SEMANAL

- ☐ Verificar lista de dispositivos ligados
- ☐ Rever logs de atividade (se disponivel)
- ☐ Confirmar que firmware esta atualizado

MENSAL

- ☐ Mudar password Wi-Fi (rede de visitas)
- ☐ Revogar acessos de dispositivos nao usados
- ☐ Verificar apps de IoT e permissões

SEMESTRAL

- ☐ Atualizar firmware do router
- ☐ Rever toda a configuração de segurança
- ☐ Avaliar se dispositivos mais antigos devem ser substituídos

Ferramentas Gratuitas para Monitorizar a Rede

- **App do router:** a maioria dos routers modernos tem uma app oficial (ASUS Router, TP-Link Tether, NETGEAR Orbi) que mostra dispositivos ligados e alertas de segurança em tempo real.
- **Fing:** app gratuita (iOS e Android) que lista todos os dispositivos na rede, identifica o fabricante de cada um e deteta intrusos.
- **Home Assistant:** plataforma open-source para gestão de casa inteligente que inclui monitorização avançada de rede. Para utilizadores mais técnicos.
- **Router com suporte a DNS filtering (ex: Pi-hole ou NextDNS):** bloqueia automaticamente domínios maliciosos conhecidos, incluindo servidores de comando e controlo de malware IoT.

7. O Que Fazer se Suspeitar que a Rede Foi Comprometida

Sinais de alerta: consumo de dados anormalmente elevado, dispositivos IoT a funcionar de forma errática, ligamentos desconhecidos no painel do router, redução na velocidade de internet sem razão aparente.

1. **Desconecte imediatamente da internet** o dispositivo suspeito (desligue o cabo de rede ou remova da rede Wi-Fi).
2. **Reinicie o router** para forcar a desconexão de qualquer sessão ativa.
3. **Altere todas as passwords** — router, Wi-Fi principal, Wi-Fi IoT.
4. **Faca um reset de fábrica** ao dispositivo IoT suspeito e reconfigure-o de raiz.
5. **Verifique outros dispositivos** na mesma rede em busca de comportamentos anómalos.
6. **Contacte o seu ISP** se suspeitar que a ligação foi usada para actividades ilegais — e importante ter um registo.

AVISO IMPORTANTE

Se tiver cameras de segurança comprometidas ou suspeitar de vigilância ilegal, contacte as autoridades (GNR / PSP) antes de fazer qualquer alteração aos dispositivos.

A preservação de evidencias pode ser importante para uma eventual investigação.

A Casa Inteligente Precisa de um Dono Atento

Cada novo dispositivo IoT que entra em casa aumenta a superfície de ataque da sua rede. A boa noticia: com segmentação correcta, passwords fortes e atualizações regulares, a maioria dos riscos e eliminada antes de se tornarem problemas.

Regra de ouro: trate cada dispositivo IoT como se fosse de um estranho. Isole-o, limite o que pode fazer, e vigie-o regularmente.