**DECLARAÇÃO DE ATENDIMENTO AOS REQUISITOS DE SEGURANÇA CIBERNÉTICA DO LAC-BCOP-1 PARA EQUIPAMENTO CPE**

Em atendimento ao item 4.1.2 do Ato nº 77 de 2021 da Anatel, no caso de homologação de equipamentos que se enquadrarem na definição de *Customer Premise Equipment* (**CPE**), a tabela “*Anexo 1 - Tabela de Requisitos*” do documento referenciado no item 2.5 do Ato 77/21, **LAC-BCOP-1**, “*Melhores Práticas Operacionais Atuais sobre Requisitos Mínimos de Segurança para Aquisição de Equipamentos para Conexão de Assinante (CPE)*", publicado em 2019 pelo “*Grupo de Operadores de Red de América Latina y el Caribe*” (LACNOG) do Uruguai, em conjunto com “*The Messaging, Malware and Mobile Anti-Abuse Working Group*" (M3AAWG) dos Estados Unidos, deverá ser preenchida, assinada e anexada à *DECLARAÇÃO DE ATENDIMENTO AOS REQUISITOS DE SEGURANÇA CIBERNÉTICA PARA EQUIPAMENTOS PARA TELECOMUNICAÇÕES*.

Assim, a \_\_\_\_[RAZÃO SOCIAL DO REQUERENTE]\_\_\_\_\_, requerente à homologação do equipamento **CPE** de marca \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ e modelo \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ declara que o referido equipamento está em conformidade com os seguintes requisitos do documento **LAC-BCOP-1**:

|  |  |  |  |
| --- | --- | --- | --- |
| **LAC-BCOP-1 - Requisitos Gerais (GR)** | | | |
|  | **Requisito** | **M Mandatório**  **R Recomendado**  **O Opcional** | **Configuração PADRÃO** |
|  | GR-01 | M |  |
| A descrição do dispositivo DEVE incluir a identificação completa de seus componentes principais, em particular:  a. Fabricante, versões do modelo e do chipset  b. Nome, versão e data de lançamento do firmware e do sistema operacional de base | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | GR-02 | M |  |
| O fornecedor DEVE prover documentação que descreva, no mínimo:  a. Nome, versão, data de lançamento e funcionalidade do firmware ou sistema operacional  b. Nome, versão, data de lançamento e estado de inicialização de fábrica (por exemplo, ativado ou desativado por padrão) de todos os aplicativos e serviços instalados no dispositivo | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | GR-03 | M |  |
| O fornecedor DEVE prover as seguintes informações para qualquer software de código aberto utilizado:  a. Lista de todas as licenças relevantes para cada software de código aberto usado  b. nome completo e versão de cada software de código aberto incorporado ao sistema do CPE | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | GR-04 | R | Informação de contato para divulgação de vulnerabilidades disponível na interface gráfica do usuário |
| Informações de contato para divulgação de vulnerabilidades (VR-03) DEVERIAM ser incluídas em algum ponto (por exemplo, página, guia, etc.) da interface gráfica de usuário (Graphical User Interface - GUI) do CPE. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | GR-05 | R | Estado atual quanto a atualizações |
| O fornecedor DEVERIA prover informações ao usuário se o CPE está fora do período de suporte (consulte VR-01 e VR-02) e não recebe mais atualizações de firmware (por exemplo, por meio da interface gráfica de usuário). | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **LAC-BCOP-1 - Requisitos de Segurança de Software (SR)** | | | |
|  | **Requisito** | **M Mandatório**  **R Recomendado**  **O Opcional** | **Configuração PADRÃO** |
|  | SSR-01 | M |  |
| Credenciais NÃO DEVEM ser inalteráveis (hard-coded). Veja também FR-04 e FR-05. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | SSR-02 | M | Dados sensíveis protegidos |
| Os dados sensíveis de credenciais (por exemplo, senhas, chaves e tokens de segurança) armazenados no dispositivo DEVEM ser protegidos por algoritmos de hash/criptográficos apropriados. Chaves criptográficas DEVERIAM ser armazenadas em hardware seguro, se disponível. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | SSR-03 | R |  |
| Dados gerais armazenados no dispositivo DEVERIAM ser protegidos por criptografia apropriada. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | SSR-04 | M | Ferramentas de desenvolvimento de *software* e/ou *backdoors* removidos |
| Quaisquer ferramentas de software ou backdoors usados para o desenvolvimento de firmware ou sistema DEVEM ser removidos na versão de produção. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **LAC-BCOP-1 - Requisitos de Atualização e Gerenciamento (MR)** | | | |
|  | **Requisito** | **M Mandatório**  **R Recomendado**  **O Opcional** | **Configuração PADRÃO** |
|  | MR-01 | M (a) | (a) |
| O CPE DEVE implementar um mecanismo para gerenciamento remoto que contemple, no mínimo, administração remota usando um protocolo de criptografia apropriado. Verifique a tabela no Anexo I para a lista de protocolo(s) necessário(s). | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | MR-02 | M (b) | (b) |
| O CPE DEVE implementar um mecanismo para atualização remota segura. Verifique a tabela no Anexo I para obter a lista de protocolo(s) necessário(s). | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | MR-03 | a. M  b. M  c. M  d. M | (c) |
| Os mecanismos de gerenciamento e administração, e de atualização remotos DEVEM suportar:  a. Autenticação segura, e  b. Conexões criptografadas, e  c. Restrições de acesso para limitar conexões a origens específicas (por exemplo, segmentos de rede selecionados, uma URL específica etc.), e  d. A capacidade de escolher a porta de conexão (ou seja, suportar a alteração do número da porta PADRÃO/porta atribuída para o serviço [17]). | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | MR-04 | M |  |
| No caso de atualização automatizada e segura, um mecanismo DEVE ser implementado para autenticar e validar o repositório fonte. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | MR-05 | M |  |
| O CPE DEVE implementar um mecanismo para verificar – antes de prosseguir com a atualização efetiva (tipicamente na memória flash) - a integridade e a autoridade do arquivo baixado e se ele é destinado para esse dispositivo (por exemplo, se é destinado à arquitetura, modelo, versão do dispositivo, etc.) | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | MR-06 | M |  |
| O processo de atualização DEVE preservar as configurações existentes. O fornecedor PODE alterar uma configuração existente se essa alteração melhorar a segurança do dispositivo. Essa mudança DEVE ser claramente documentada. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | MR-07 | a. M  b. M  c. R |  |
| Em relação a verificações de atualizações, o CPE:  a. DEVE ter a capacidade de executar verificações periódicas para obter (pull) atualizações de forma automatizada e programada;  b. DEVE permitir que o usuário inicie a verificação de atualizações.  c. DEVERIA suportar as atualizações solicitadas pelo ISP sob demanda (push). | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | MR-08 | M |  |
| O CPE DEVE implementar mecanismos para evitar sua inutilização como resultado de falha na atualização do firmware (bricking). Os procedimentos de recuperação DEVEM ser claramente documentados e NÃO DEVEM requerer o acesso a partes internas do hardware. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **LAC-BCOP-1 - Requisitos Funcionais (FR)** | | | |
|  | **Requisito** | **M Mandatório**  **R Recomendado**  **O Opcional** | **Configuração PADRÃO** |
|  | FR-01 | M | Telnet, FTP, SOCKS, CHARGEN, SNMP desativados |
| O CPE NÃO DEVE ativar POR PADRÃO na interface WAN, serviços que permitam a divulgação de informações sensíveis ou que possam ser abusados para realizar ataques de amplificação (por exemplo, Telnet, FTP, SOCKS, CHARGEN, SNMP, etc.) | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-02 | M | (c) |
| O CPE DEVE implementar as funcionalidades de atualização remota e gerenciamento remoto, conforme descrito na sessão Requisitos de Atualização e Gerenciamento (Update and Management Requirements – MR) deste documento. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-03 | DEVE autenticar e é  RECOMENDADO  para criptografar. |  |
| Qualquer comunicação de gerenciamento do usuário final a partir da LAN/WLAN para o CPE DEVE ser autenticada6 e DEVERIA ser criptografada. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-04 | M |  |
| Qualquer informação de autenticação (por exemplo, senhas) DEVE ser alterável, incluindo a senha de administração geral (root). Os identificadores de usuários (por exemplo, nome de usuários) DEVERIAM ser alteráveis. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-05 | a. M  b. M | Senha inicial única por dispositivo |
| Em relação à senha para acessar interfaces administrativas:  a. A senha inicial DEVE ser única para cada dispositivo e NÃO DEVE ser derivada de informações que possam ser obtidas por meio da captura de pacotes ou de métodos semelhantes de observação (por exemplo, endereço MAC);  b. A qualquer momento, quando uma senha é alterada ou redefinida (reset), a senha NÃO DEVE ser nula (ou seja, vazia, em branco) nem igual ao nome de usuário, e boas práticas relevantes para complexidade da senha DEVEM ser seguidas. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-06 | M |  |
| O firmware de produção NÃO DEVE ter nenhum mecanismo não documentado para acessar o sistema ou seus dados. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-07 | M |  |
| O dispositivo NÃO DEVE ter mecanismos de comunicação não documentados para enviar dados ao fornecedor ou a terceiros. Quaisquer comunicações e dados enviados ao fornecedor ou a terceiros DEVEM ser explicitamente documentados. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-08 | a. M  b. M |  |
| Um usuário final autenticado DEVE ser capaz, por meio da interface gráfica do usuário:  a. De alterar as configurações específicas do usuário conforme apropriado (por exemplo, nome da rede WiFi, regras de firewall/encaminhamento, etc.), e  b. De desativar qualquer serviço que não seja essencial para a operação ou administração do dispositivo. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-09 | M | DNS, NTP, SSDP, UPnP não acessível a partir da WAN |
| Ao habilitar a operação de serviços para usuários na(s) interface(s) LAN/WLAN do CPE, tais serviços NÃO DEVEM ser acessíveis a partir da WAN/Internet, em particular serviços como DNS, NTP, SSDP, UPnP, ou qualquer outro protocolo que possa ser usado em ataques de amplificação. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-10 | a. M  b. M | (d) |
| Para usar um serviço/agente de monitoramento e/ou gerenciamento:  a. A configuração de um mecanismo de autenticação apropriado para definir valores e/ou para recuperar informações/dados sensíveis DEVE ser necessária;  b. O acesso a partir de interface(s) WAN DEVE usar autenticação e DEVE ser restrito a origens específicas (por exemplo, a um segmento ou endereço de rede selecionado). | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-11 | M |  |
| O dispositivo DEVE implementar métodos criptográficos baseados em padrões abertos em suas versões atuais, que permitem a seleção de parâmetros seguros em relação ao conjunto de cifras e tamanho das chaves. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-12 | M |  |
| Serviços criptográficos ou aplicações que envolvam a geração de chaves e/ou certificados digitais para autenticação de dispositivos DEVEM gerar as chaves para cada dispositivo; ou seja, uma chave privada NÃO DEVE ser compartilhada entre diferentes dispositivos. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-13 | M | Apenas cliente NTP. Nenhuma configuração inalterável (*hard-coded*). |
| O CPE DEVE suportar a sincronização de tempo por meio de um protocolo de tempo centralizado, como o Network Time Protocol (NTP). Apenas o software cliente NTP é necessário. O CPE NÃO DEVE ter uma configuração inalterável (hard-coded) para os servidores NTP e NÃO DEVE usar POR PADRÃO servidores para os quais o fornecedor não tenha permissão de uso. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-14 | R |  |
| O CPE DEVERIA suportar a RFC 6092 "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service"[6]. No caso de um conflito entre a RFC 6092 e este documento, o requisito deste documento prevalecerá. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-15 | M | Filtragem *antispoofing* ativada |
| O CPE DEVE suportar filtragem antispoofing de acordo com a BCP 38 RFC 2827 [12] para ambos os protocolos, IPv4 e IPv6. DEVE ser uma opção selecionável, ativa POR PADRÃO. Está fora do escopo deste documento determinar a técnica a ser usada para validação do endereço IP de origem. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-16 | R | Desconfigurado (e) |
| O CPE DEVERIA suportar a filtragem de pacotes para endereços IP reservados para propósito específico (Special-Purpose Address). Endereços considerados "Globally Reachable" FALSE E "Forwardable" FALSE, de acordo com a RFC 6890 [13] e RFC 8190 [14], DEVERIAM ser filtrados. Neste caso, o CPE DEVERIA ser capaz de aceitar configuração para incluir endereços IPv4 e IPv6 de acordo com os registros mantidos pela IANA (Internet Assigned Numbers Authority), como descrito em “IANA IPv4 Special-Purpose Address Registry” [15] e “IANA IPv6 Special-Purpose Address Registry” [16]. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-17 | a. M  b. R  c. R  d. M | b. Nenhuma regra de encaminhamento ativada |
| O CPE NÃO DEVE atuar como um servidor DNS recursivo aberto. Em relação a serviços DNS:  a. As consultas DNS recebidas na porta WAN e destinadas ao próprio CPE NÃO DEVEM ser permitidas ou respondidas.  b. As consultas DNS recebidas na porta WAN e destinadas a serem encaminhadas pela porta LAN PODEM ser permitidas, desde que exista uma regra explícita para isso na configuração do CPE (por exemplo, regra de encaminhamento, regra de firewall etc.).  c. Se o CPE estiver executando um servidor DNS local, ele DEVERIA marcar as consultas DNS de saída (outbound) para executar a validação DNSSEC.  d. Se o CPE não estiver executando um servidor DNS local e, em vez disso, estiver encaminhando consultas DNS para outro servidor, então ele NÃO DEVE remover marcações de validação DNSSEC das consultas DNS se elas existirem. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-18 | a. M  b. R | Criptografia apropriada ativada |
| Quando WiFi é provido, o CPE:  a. DEVE implementar mecanismos de segurança com criptografia apropriada.  b. DEVERIA suportar a versão mais recente da especificação de recursos de segurança Wi-Fi Protected Access (WPA). | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-19 | M |  |
| As senhas NÃO DEVEM ser visíveis em texto claro POR PADRÃO em nenhuma interface de gerenciamento. Senhas PODEM tornar-se visíveis quando solicitado pelo usuário. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | FR-20 | R |  |
| Um método para fazer download da configuração do dispositivo em formato de texto puro (ASCII ou UTF-8) DEVERIA existir, contanto que todas as informações sensíveis (por exemplo, senhas, strings de comunidade, etc.) sejam editadas (redacted) da saída (output). | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **LAC-BCOP-1 - Requisitos de Configuração Initial (IR)** | | | |
|  | **Requisito** | **M Mandatório**  **R Recomendado**  **O Opcional** | **Configuração PADRÃO** |
|  | IR-01 | M | SSDP, SNMP, UPnP, SOCKS, SMB, teste de largura de banda desativados |
| O CPE DEVE ser configurado de forma restritiva, ao invés de ser configurado de forma permissiva. Todos os serviços (processos do tipo servidor) que não são estritamente necessários para o processo de configuração inicial (bootstrapping) DEVEM estar desativados, especialmente (se implementado) SSDP, SNMP, UPnP, SOCKS, SMB, teste de largura de banda (ergo imbedded iperf e outros). Além disso, os serviços que estão habilitados ou podem ser ativados DEVERIAM operar em um modo padrão restritivo e/ou seguro. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | IR-02 | M | Nenhum endereço de servidor DNS predefinido e o DNS Relay desativado |
| Parâmetros relacionados a endereços de servidores DNS (resolver addresses) DEVEM estar desconfigurados e a opção de DNS Relay (se implementada) DEVE estar desativada. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | IR-03 | M | Desativadas |
| O encaminhamento de porta (port forwarding) ou a opção de host DMZ, se disponíveis, DEVEM estar desativadas POR PADRÃO. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | IR-04 | M | (f) |
| A senha inicial para acessar interfaces administrativas, tanto gráficas quanto de linha de comando, DEVE ser única para cada dispositivo e DEVE ser possível identificá-la visualmente na etiqueta do dispositivo. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | IR-05 | M | (f) |
| Quando o WiFi é provido, a(s) rede(s) WiFi DEVE(M) ter uma senha inicial única, NÃO igual ao SSID, e DEVE ser possível identificar a(s) senha(s) inicial(is) visualmente na etiqueta do dispositivo. A(s) senha(s) DEVERIA(M) ser diferente(s) da senha PADRÃO de administração. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | IR-06 | M | (g) |
| Quando o WiFi é provido, o(s) valor(es) PADRÃO do(s) Service Set Identifier(s)(SSIDs) NÃO DEVE(M) estar relacionado(s) ao nome do fornecedor nem ao modelo do produto e DEVE(M) ser customizável(eis). Verifique a tabela no Anexo I para valores PADRÃO personalizados pelo ISP. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | IR-07 | M | Nenhuma chave SSH pré-gerada |
| No caso do serviço SSH, o par de chaves do servidor NÃO DEVE ser pré-gerado na fábrica. A chave DEVE ser gerada após a primeira inicialização/boot do serviço e qualquer reinicialização (reset) de fábrica deve fazer com que uma nova chave seja gerada. O par de chaves gerado deve prover bits suficientes para ser considerado seguro no momento da implementação. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | IR-08 | M | Ativada |
| A filtragem antispoofing [FR-15] DEVE estar ativada POR PADRÃO. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | IR-09 | M | Mecanismos de transição, túneis, VPN desativados |
| Mecanismos de transição IPv6, túneis, VPNs e serviços similares DEVEM estar desativados POR PADRÃO. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **LAC-BCOP-1 - Requisitos do Fornecedor (VR)** | | | |
|  | **Requisito** | **M Mandatório**  **R Recomendado**  **O Opcional** | **Configuração PADRÃO** |
|  | VR-01 | M |  |
| DEVE ter uma política clara de suporte ao produto, especialmente em relação à disponibilidade de correções para vulnerabilidades de segurança, incluindo o período após a data de término de venda (end-of-sale date). | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | VR-02 | M |  |
| DEVE fornecer correções para vulnerabilidades de segurança no mínimo enquanto o dispositivo está à venda. O fornecedor DEVERIA continuar fornecendo correções de segurança por 3 (três) anos a partir da data de término da venda (end-of-sale date). | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | VR-03 | M |  |
| DEVE possuir uma capacidade de divulgação de vulnerabilidades de forma coordenada, incluindo um canal de comunicação/ponto de contato que permita que ISP clientes, usuários finais e terceiros (como pesquisadores) relatem vulnerabilidades de segurança descobertas no(s) produto(s). Idealmente, DEVERIA ter uma equipe de resposta a incidentes de segurança de produto (Product Security Incident Response Team - PSIRT). | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |
|  | VR-04 | M |  |
| DEVE ter um canal de suporte publicamente disponível que não exija registro prévio ou uma conta de usuário, no mínimo, por meio de um site Web em inglês para:  a. Informar sobre vulnerabilidades existentes, medidas de mitigação e correções de segurança associadas ao(s) seu(s) produto(s);  b. Prover correções de segurança e/ou novas versões de firmware ou software para seu(s) produto(s);  c. Fornecer manuais e outros materiais relacionados à configuração, atualização e segurança do dispositivo. | | |
| Justificativa: apresentar justificativa caso o requisito não seja aplicável ao produto. | | |

1. O ISP deve ter a capacidade de gerenciar os dispositivos remotamente (por exemplo, para configuração). Dependendo da tecnologia usada pelo provedor (cabo, fibra, xDSL), o correspondente segmento da indústria pode ter protocolos já especificados. Neste item, o ISP precisa escolher o(s) protocolo(s) que devem ser suportados pelo dispositivo de acordo com sua tecnologia (por exemplo, BBF TR ‑ 069 CWMP para banda larga), se ele deveria ser ativado POR PADRÃO e as configurações padrão necessárias. Se mais de um protocolo deve ser suportado, a organização precisa incluir todos eles.
2. O ISP deve ter a capacidade de atualizar o dispositivo remotamente (principalmente o *firmware*). Dependendo da tecnologia usada pelo provedor (cabo, fibra, xDSL), o correspondente segmento da indústria pode ter protocolos já especificados. Neste item, a organização precisa escolher o(s) protocolo(s) que devem ser suportados pelo dispositivo de acordo com sua tecnologia (por exemplo, BBF TR ‑ 069 CWMP para banda larga), se deveria ser ativado POR PADRÃO e as configurações padrão necessárias. Se mais de um protocolo deve ser suportado, a organização precisa incluir todos eles.
3. Não utilizar mecanismos mínimos para controle de acesso, confidencialidade e verificação de integridade nas transações entre os CPEs e o servidor de gerenciamento/atualização pode frequentemente resultar no comprometimento da infraestrutura do provedor. É altamente recomendável usar conexão criptografada (por exemplo, TLS/HTTPS) para todo o acesso; usar autenticação não baseada em um nome de usuário/senha pré-definidos para todos os dispositivos; e restringir o acesso a fontes determinadas (por exemplo, para um segmento de rede selecionado, URL específica, etc.).
4. Se o ISP quiser um serviço/agente de monitoramento e/ou gerenciamento habilitado por padrão, ele deve fornecer os parâmetros apropriados para autenticação e restrição de acesso via rede.
5. Se o ISP quiser implementar diretamente no CPE a filtragem para endereços IP reservados para propósito específico, ele poderá fornecer a lista de prefixos que podem ser filtrados POR PADRÃO. Caso contrário, a configuração PADRÃO será "desconfigurada" e o CPE não aplicará nenhum filtro para tais prefixos.
6. Se o ISP quiser personalizar como a senha inicial deve ser definida, o ISP precisa informar o fornecedor sobre o processo de seleção da senha. Caso contrário, o fornecedor pode definir valores únicos aleatórios como PADRÃO.
7. Se o ISP quiser personalizar o(s) nome(s) da(s) rede(s) WiFi, ele precisará informar como os Identificadores de WiFi (SSIDs) devem ser configurados. Caso contrário, o fornecedor pode escolher o(s) valor(es) PADRÃO(ÕES).

**Instruções de preenchimento:**

1. O requerente à homologação do equipamento CPE deve preencher a primeira coluna das tabelas desta declaração conforme a seguinte codificação:

|  |  |
| --- | --- |
| C | O equipamento apresenta conformidade ao requisito. |
| NA | O requisito não se aplica ao equipamento, devido às suas características. Justificativa deverá ser apresentada. |

Razão social:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CNPJ:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nome do representante legalmente habilitado:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Cargo:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Local e data:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Assinatura do representante legalmente habilitado