NIST IR 8259B por

Base Principal da Capacidade de Suporte Não Técnico da IoT

Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
Rebecca Herold

Esta publicação está disponível gratuitamente em:
https://doi.org/10.6028/NIST.IR.8259B.por

National Institute of Standards and Technology
U.S. Department of Commerce

NIST IR 8259B por

Base Principal da Capacidade de Suporte Não Técnico da Internet das Coisas

Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
Divisão de Segurança Cibernética Aplicada
Laboratório de Tecnologia da Informação

Rebecca Herold
A Professora de Privacidade
Des Moines, IA

Esta publicação está disponível gratuitamente em:
https://doi.org/10.6028/NIST.IR.8259B.por

July 2021

Departamento de Comércio dos EUA
Gina M. Raimondo, Secretária

Instituto Nacional de Padrões e Tecnologia
James K. Olthoff, Desempenhando as Funções e Deveres Não Exclusivos do Subsecretário de Comércio para Padrões e Tecnologia e Diretor, Instituto Nacional de Padrões e Tecnologia

Instituto Nacional de Padrões e Tecnologia Interagência ou Relatório Interno 8259B
31 páginas (July 2021)

Esta publicação está disponível gratuitamente em:
https://doi.org/10.6028/NIST.IR.8259B.por

Comentários sobre esta publicação podem ser enviados para:

Instituto Nacional de Padrões e Tecnologia
A/C: Divisão de Segurança Cibernética Aplicada, Laboratório de Tecnologia da Informação
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
E-mail: iotsecurity@nist.gov

Todos os comentários estão sujeitos a divulgação nos termos da Lei de Liberdade de Informação (FOIA).

Traduzido por TaikaTranslations LLC sob contrato NIST [1333ND23PNB770271]. Tradução oficial do Governo dos EUA.

Translated by TaikaTranslations LLC under contract with NIST [1333ND23PNB770271]. Official U.S. Government translation.

A versão oficial em inglês desta publicação está disponível gratuitamente no National Institute of Standards and Technology (NIST): https://doi.org/10.6028/NIST.IR.8259B.

The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST): https://doi.org/10.6028/NIST.IR.8259B.

Relatórios sobre Tecnologia de Sistemas de Computação

O Laboratório de Tecnologia da Informação (ITL, pela sua sigla em inglês) do Instituto Nacional de Padrões e Tecnologia (NIST) promove a economia e o bem-estar público dos EUA, fornecendo liderança técnica para a infraestrutura de medição e padrões do país. A ITL desenvolve testes, métodos de teste, dados de referência, implementações de prova de conceito e análises técnicas para promover o desenvolvimento e o uso produtivo da tecnologia da informação. As responsabilidades da ITL incluem o desenvolvimento de padrões e diretrizes administrativas, técnicas e físicas para a segurança e privacidade econômicas de informações que não sejam relacionadas à segurança nacional em sistemas de informação federais.

Resumo

Recursos de suporte não técnicos são ações que um fabricante ou organização terceirizada executa em apoio à segurança cibernética de um dispositivo IoT. Esta publicação define a *base principal de recursos de suporte não técnico* dos fabricantes de dispositivos da Internet das Coisas (IoT), que é um conjunto de recursos de suporte não técnicos geralmente necessários de fabricantes ou outros terceiros para oferecer suporte a controles comuns de segurança cibernética que protegem os dispositivos de uma organização, bem como dados, sistemas e ecossistemas de dispositivos. O objetivo desta publicação é fornecer às organizações um ponto de partida para usar na identificação dos recursos de suporte não técnicos necessários em relação aos dispositivos IoT que elas fabricarão, integrarão ou adquirirão. Esta publicação destina-se a ser usada em conjunto com Relatório Interno do Instituto Nacional de Padrões e Tecnologia 8259 (NISTIR, pela sua sigla em inglês), *Atividades Fundamentais de Segurança Cibernética para Fabricantes de Dispositivos IoT* e NISTIR 8259A, *Base Básica de Capacidade de Segurança Cibernética de Dispositivos IoT*.

Palavras-chave

base de segurança cibernética; Internet das Coisas (IoT); dispositivos de computação seguros.

Agradecimentos

Os autores desejam agradecer a todos os colaboradores desta publicação, incluindo os participantes em workshops e outras sessões interativas; os indivíduos e organizações dos setores público e privado, incluindo fabricantes de vários setores, bem como várias organizações comerciais de fabricantes, que forneceram feedback sobre o conteúdo público preliminar e colegas do NIST que ofereceram contribuições e feedback inestimáveis. Agradecimentos especiais aos membros da equipe de Cibersegurança para IoT Brad Hoehn e David Lemire e à equipe do Projeto de Implementação do Lei de Modernização da Segurança das Informações Federais (NIST FISMA, pela sua sigla em inglês) por sua ampla ajuda.

Público

O principal público desta publicação são os fabricantes de dispositivos IoT, especialmente com o papel emergente de agentes de segurança de produtos. Esta publicação também pode ajudar os

clientes ou integradores de dispositivos IoT.

Aviso de Divulgação de Patente

AVISO: A ITL solicitou que os titulares de reivindicações de patentes cujo uso possa ser necessário para o cumprimento das orientações ou requisitos desta publicação divulguem tais reivindicações de patentes à ITL. No entanto, os titulares de patentes não são obrigados a responder aos pedidos de patentes da ITL, e a ITL não realizou uma pesquisa de patentes para identificar quais patentes, se houver, podem ser aplicadas a esta publicação.

Na data de publicação e após à(s) chamada(s) para a identificação de reivindicações de patente cujo uso pode ser necessário para conformidade com a orientação ou requisitos desta publicação, nenhuma dessas reivindicações de patente foi identificada para a ITL.

Nenhuma representação é feita ou implícita pela ITL de que as licenças não são necessárias para evitar violação de patente no uso desta publicação.

Tabela de Conteúdos

Lista de Apêndices

1 Introdução

Os dispositivos da Internet das Coisas (IoT) geralmente não possuem recursos integrados de segurança cibernética, bem como suporte não técnico relevante para a segurança cibernética. Os clientes podem usar esse tipo de informação para ajudar a mitigar os riscos de segurança cibernética relacionados aos dispositivos IoT e seu uso. A ampla gama de conectividade possível para dispositivos IoT e a capacidade desses dispositivos de interagir com o mundo físico significam que proteger esses dispositivos muitas vezes se torna uma prioridade; mas é um desafio para os clientes quando eles não são adequadamente suportados.

Esta publicação deve ser utilizada e compreendida no contexto do NISTIR 8259, *Atividades Fundamentais de Segurança Cibernética para Fabricantes de Dispositivos IoT* [1] e NISTIR 8259A, *Base Básica de Capacidade de Segurança Cibernética de Dispositivos IoT.* A NISTIR 8259 discute considerações para os fabricantes ajudarem a orientá-los na escolha e implementação dos recursos de segurança cibernética de dispositivos que seus dispositivos de IoT fornecerão. 8259A discute os recursos técnicos de segurança cibernética do dispositivo, que são recursos ou funções de segurança cibernética que os dispositivos fornecem por meio de seus próprios meios técnicos (ou seja, hardware e software do dispositivo) e estabelece uma base central dos recursos de segurança cibernética do dispositivo que os clientes de dispositivos de IoT geralmente precisam.

Para complementar a base principal da NISTIR 8259A, a base principal da capacidade de suporte não técnico da IoT é um conjunto de ações realizadas pelos fabricantes e/ou terceiros de suporte designados (chamados de *partes de suporte*). Essas ações ajudarão outras pessoas (por exemplo, clientes, usuários finais) a usar os recursos de segurança cibernética dos dispositivos IoT e apoiarão a segurança cibernética contínua do dispositivo IoT e do sistema e das redes às quais o dispositivo se conecta (o ecossistema digital). Fornecer esse suporte não técnico de segurança cibernética por meio de materiais educacionais ou outros tipos de ferramentas e ações não técnicas pode beneficiar todo o ecossistema de dispositivos de IoT e permitir que os fabricantes ofereçam melhor suporte à segurança cibernética de dispositivos durante todo o ciclo de vida do dispositivo. Tanto os recursos de segurança cibernética do dispositivo quanto os recursos de suporte não técnicos são vitais para que os clientes atinjam suas necessidades e objetivos. Semelhante à base principal de *capacidade de segurança cibernética do dispositivo* IoT na NISTIR 8259A, esta base principal de capacidade de suporte não técnico da IoT destina-se a fornecer às organizações um ponto de partida para o estabelecimento de ações não técnicas para suportar o gerenciamento de riscos de segurança cibernética do dispositivo IoT.

Especificamente, esta publicação descreve quatro recursos de suporte não técnicos recomendados relacionados ao ciclo de vida completo do gerenciamento de segurança cibernética que os fabricantes devem implementar para oferecer suporte aos dispositivos IoT que fabricam durante toda a vida útil: 1) Documentação; 2) Recepção de Informações e Consultas; 3) Divulgação de Informações; e 4) Educação e Conscientização.

A escolha do fabricante de recursos de suporte não técnicos considera a finalidade do dispositivo IoT e os usos pretendidos. Essas ações tornam mais fácil para os clientes entender e identificar como os dispositivos de IoT são construídos para atender às suas necessidades de segurança cibernética, bem como as expectativas dos fabricantes de como o dispositivo de IoT deve ser

usado com segurança. A Figura 1 mostra os quatro recursos de suporte não técnicos incluídos nesta base.

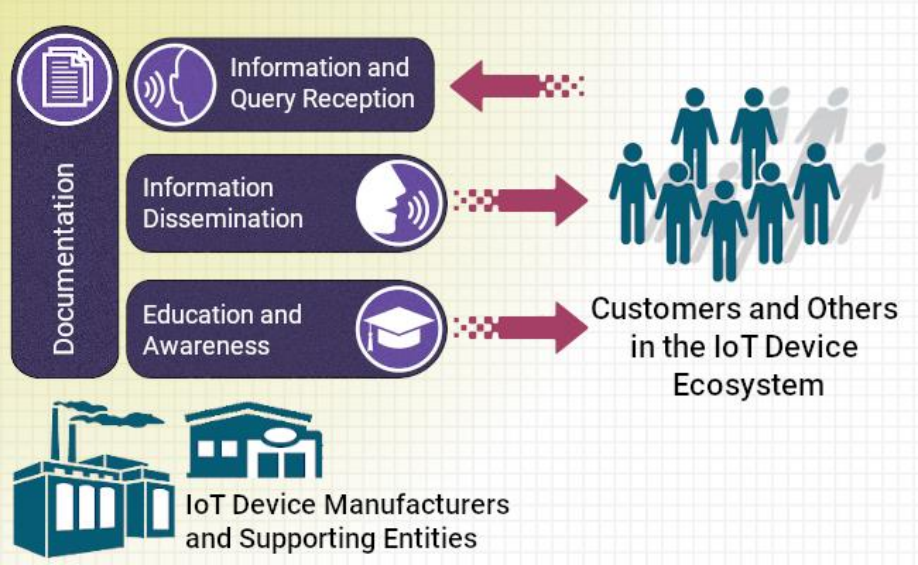

Figura 1: Como os clientes e outras pessoas no ecossistema de dispositivos de IoT usarão os recursos na base, se fornecidos pelos fabricantes de dispositivos de IoT e entidades de suporte.

A documentação captura informações que os clientes em potencial e outras pessoas no ecossistema podem precisar saber sobre os dispositivos de IoT e as maneiras pelas quais eles e os dados e sistemas associados podem ser protegidos. Essa documentação também é frequentemente necessária antes da compra e durante todo o ciclo de vida do dispositivo IoT para o cliente e outros no ecossistema (por exemplo, auditores e avaliadores). Esta documentação suporta o tratamento apropriado de risco, conformidade e garantia de perspectivas internas e externas quando o dispositivo IoT e os sistemas associados são implementados no ambiente do cliente. Conforme mostrado na Figura 1, a documentação atua como um pilar de suporte para outras capacidades não técnicas. Isso ocorre porque outros recursos não técnicos, incluindo aqueles na base de suporte não técnico da IoT, usarão as informações capturadas por meio de documentação para personalizar sua entrega.

A Recepção de Informações e Consultas ocorre após a compra e permite que clientes e outros no ecossistema (por exemplo, pesquisadores, organizações de classificação de produtos) enviem perguntas e outras informações relacionadas à proteção do dispositivo IoT e sistemas associados. O fabricante e as partes de suporte podem, então, responder. A recepção de informações e consultas pode ajudar os clientes e outras pessoas de várias maneiras ao longo do ciclo de vida de um dispositivo IoT, permitindo que os fabricantes e entidades de terceiros se adaptem e atualizem seus serviços de suporte (por exemplo, fornecidos por meio de outros recursos de suporte não técnicos) para as necessidades e objetivos de segurança cibernética dos clientes.

A disseminação de informações permite que as informações continuem a fluir para clientes e outros no ecossistema sobre a segurança cibernética de seus dispositivos IoT e sistemas associados. Clientes e outros se beneficiarão de 1) a divulgação de vulnerabilidades de segurança cibernética recém-descobertas para o dispositivo, sistemas e software associados, etc. e 2) notificações sobre atualizações de dispositivos IoT, como atualizações de software, alterações de

algoritmo, novos protocolos ou alterações nos fornecedores usados pelo fabricante para atualizar a segurança cibernética, que podem impactar os riscos de segurança cibernética.[1]

A Educação e Conscientização fornece o conteúdo educacional necessário para apoiar clientes e outras pessoas no uso e proteção seguros de dispositivos IoT e sistemas, software e hardware associados. Ao tornar os clientes e outras pessoas no ecossistema mais bem informados sobre como proteger os dispositivos IoT e como usar de forma mais eficaz os recursos de segurança cibernética do dispositivo, os fabricantes podem ajudar a reduzir o número de ocorrências e a gravidade relacionada aos comprometimentos de dispositivos IoT, impedir ataques contra os dispositivos e reduzir o número de vulnerabilidades que são exploradas e levam a dispositivos comprometidos.

Os clientes são os destinatários típicos dos recursos de suporte não técnicos, mas alguns clientes podem não ser capazes de usar esses recursos de suporte não técnicos diretamente. Neste último caso, a capacidade pode ser usada por outras entidades no ecossistema de dispositivos de IoT (por exemplo, fornecedores, organizações comerciais ou profissionais, grupos de defesa e mídia de tecnologia) para ajudar os clientes a atender às suas necessidades e objetivos.

Essa base foi desenvolvida após a revisão de uma variedade de documentos de orientação de várias fontes e o recebimento de contribuições das partes interessadas. Representa um esforço coordenado para produzir uma definição de capacidades comuns, não uma lista exaustiva. A base principal pretende ser um ponto de partida flexível. Os fabricantes e as partes de suporte podem usar a base principal de capacidade de suporte não técnico da IoT no contexto das atividades na NISTIR 8259 e isso é apropriado para eles. É importante observar que os fabricantes e terceiros de suporte devem implementar os recursos de suporte não técnicos que suportam as necessidades de gerenciamento de risco dos clientes do dispositivo IoT dentro do ecossistema digital pretendido. Isso resultará em cada um dos recursos de suporte não técnicos individuais na base sendo implementados de maneira consistente com as necessidades e expectativas desses clientes. Se forem necessários recursos de suporte adicionais para permitir o uso seguro dos dispositivos, as organizações são encorajadas a considerar a definição de recursos de suporte adicionais que melhor se adaptem ao(s) seu(s) caso(s) de uso.

[1] Um recurso que suporta tanto a Recepção de Informações quanto a Divulgação de Informações para outras pessoas no ecossistema sobre vulnerabilidades é encontrado no *Projeto NIST SP 800-216: Diretrizes Federais de Divulgação de Vulnerabilidade* [17]. Este documento recomenda orientações para o estabelecimento de uma estrutura federal de divulgação de vulnerabilidades e destaca a importância do tratamento adequado dos relatórios de vulnerabilidades e da comunicação da minimização ou eliminação de vulnerabilidades.

2 A Base Principal da Capacidade de Suporte Não Técnico da IoT

A Tabela 1 define a base principal de capacidade de suporte não técnico do dispositivo IoT, que, em combinação com a base principal de capacidade de segurança cibernética (técnica) do dispositivo da NISTIR 8259A, pode tornar possível proteger um dispositivo IoT. A tabela abaixo se baseia nos conceitos da Seção 4 da NISTIR 8259, que destaca a importância da comunicação com clientes e outras pessoas no ecossistema de dispositivos IoT sobre segurança cibernética, e na Seção 3, que fornece muitos exemplos de informações que os clientes e outras pessoas podem precisar saber sobre dispositivos IoT ou o design do dispositivo.

A Tabela 1 é um ponto de partida de alto nível para os fabricantes de dispositivos de IoT entenderem como eles podem ter que planejar e apoiar as necessidades e metas de segurança cibernética do cliente de maneiras não técnicas. As complexidades da fabricação de dispositivos IoT podem resultar em organizações diferentes do fabricante do dispositivo fornecendo suporte crítico de segurança cibernética, como alguns ou todos os recursos de suporte não técnicos descritos nesta publicação. Portanto, o alvo para esta orientação inclui partes de suporte (por exemplo, provedor de serviços em nuvem e prestador de serviços contratado) que podem desempenhar um papel em uma ou mais das ações na Tabela 1, além do fabricante.

As capacidades de suporte não técnico na Tabela 1 descrevem o destinatário pretendido do valor da capacidade como o *cliente* (ou seja, aqueles com quem as *comunicações* ocorrem). Isso decorre de uma suposição de que o cliente de um dispositivo de IoT terá necessidades, metas e responsabilidades de segurança cibernética relacionadas ao dispositivo de IoT. Para um cliente ou caso de uso específico, pode haver outros indivíduos ou entidades do ecossistema de dispositivos IoT que podem fazer parte dessa comunicação. Por exemplo, um cliente empresarial pode ter vários contratados ou entidades de apoio, bem como funcionários a quem as informações descritas na tabela podem precisar ser comunicadas. Como alternativa, um proprietário de edifício que incorpore dispositivos IoT precisará passar informações para os inquilinos do edifício usando esses dispositivos IoT. Neste caso, também é digno de nota como futuros proprietários/usuários dos dispositivos IoT (ou seja, futuros inquilinos) podem não ser considerados *clientes* no sentido tradicional. Finalmente, além do cliente, para alguns setores, pode haver entidades robustas do ecossistema de terceiros (por exemplo, revisores e avaliadores de produtos, varejistas e fornecedores) que podem usar recursos de suporte não técnicos para ajudar a melhorar a segurança cibernética do setor em geral.

As ações específicas listadas na tabela destinam-se a refletir as ações típicas que muitos clientes e outros no ecossistema de dispositivos de IoT esperam que os fabricantes e as partes de apoio tomem para apoiar as necessidades e metas de segurança cibernética. Os fabricantes podem escolher e personalizar recursos não técnicos com base nos casos de uso pretendidos e nos clientes do dispositivo IoT, com exemplos e justificativas fornecidos para fornecer informações adicionais sobre as expectativas do cliente ou por que essas ações são importantes. Tal como acontece com a NISTIR 8259A, seria necessário mais contexto para articular capacidades específicas de suporte não técnico. Outros tipos de recursos de suporte não técnicos podem ser necessários para melhor abordar o contexto do

sistema dentro do qual o dispositivo IoT é usado e também em consideração aos riscos de segurança cibernética do[2] sistema de cada organização de usuário de dispositivo IoT. As organizações que optam por adotar os principais recursos não técnicos de base para qualquer um dos dispositivos IoT que produzem, integram ou adquirem têm uma flexibilidade considerável na identificação das ações para implementar esses recursos que podem abordar de forma mais eficaz o uso de dispositivos IoT dentro do próprio sistema dos clientes e seus objetivos e finalidade para o uso de dispositivos IoT.

Cada linha na Tabela 1 cobre uma das capacidades de suporte não técnico do dispositivo na base principal de capacidade de suporte não técnico de IoT:

- A primeira coluna descreve a capacidade de suporte não técnico.
- A segunda coluna fornece uma lista numerada de ações comuns dentro dessa capacidade de suporte. Estas são ações que uma organização que implementa a capacidade de suporte não técnico frequentemente (mas nem sempre) usaria para alcançar a capacidade. É importante entender que as ações não se destinam a ser abrangentes nem são apresentadas em nenhuma ordem específica.[3]
- A terceira coluna explica a justificativa para a necessidade da capacidade de suporte não técnico.
- A última coluna lista exemplos de referência de IoT que indicam fontes existentes de orientação de segurança cibernética de dispositivos IoT, especificando um recurso semelhante ou relacionado. Como a tabela cobre apenas o básico das capacidades, as referências podem ser inestimáveis para entender cada capacidade com mais detalhes e aprender como implementar cada capacidade de maneira razoável. A seguir estão as referências usadas na Tabela 1:
    - **AGELIGHT**: Grupo Consultivo de Segurança Digital AgeLight, “Kit de Ferramentas de Arquitetura de Segurança e Risco para IoT v4.0” [7]
    - **CTA**: Associação de Tecnologia para Consumidores, “Instituto Nacional Americano de Padrões (ANSI)/Padrão CTA - Padrão Básico de Cibersegurança para Dispositivos e Sistemas de Dispositivos: ANSI/CTA-2088” [8]
    - **CSDE**: Conselho para Proteger a Economia Digital (CSDE), 'O Consenso C2 sobre Capacidades Básicas de Segurança de Dispositivos IoT' [9]
    - **ETSI**: Instituto Europeu de Normas de Telecomunicações, “Cibersegurança para Internet das Coisas para Consumidores: Requisitos de Base v2.1.0” [10]
    - **IoTSF**: Fundação de Segurança para IoT (IoTSF), 'Estrutura de Conformidade de Segurança para IoT v2.1' [11]

[2] Observe que as "organizações de usuários" podem ser diferentes das "organizações de clientes". Por exemplo, um sistema HVAC conectado pode ser adquirido pelo proprietário do edifício (organização do cliente), mas usado pelos inquilinos do edifício (usuários).

[3] Essas ações comuns geralmente mencionam dados típicos envolvidos; no entanto, os elementos de dados específicos envolvidos em muitas dessas ações podem variar amplamente devido à variedade de dispositivos IoT disponíveis.

Tabela 1: Recursos de Suporte Não Técnicos

Recurso de Suporte Não Técnico	Ações Comuns	Rationale	Exemplos de Referência IoT
Documentação: A capacidade do fabricante e/ou da entidade de suporte do fabricante de criar, reunir e armazenar informações relevantes para a segurança cibernética do dispositivo IoT antes da compra do cliente e durante todo o desenvolvimento de um dispositivo e seu ciclo de vida subsequente.	1. Documentar as premissas feitas durante o processo de desenvolvimento e outras expectativas relacionadas ao dispositivo IoT, como: a. Clientes e casos de uso esperados b. Uso físico e características c. Acesso e requisitos de rede (por exemplo, requisitos de largura de banda) d. Dados criados e tratados pelo dispositivo e. Entradas e saídas de dados esperadas (incluindo códigos de erro, frequência, tipo/forma, faixa de valores aceitáveis, etc.) f. Requisitos de segurança cibernética assumidos para o dispositivo IoT g. Leis e regulamentos com os quais o dispositivo IoT e as atividades de suporte relacionadas estão em conformidade h. Vida útil esperada, custos de segurança cibernética previstos relacionados ao dispositivo IoT (por exemplo, preço de manutenção) e prazo de suporte 2. Documentar os **recursos de segurança cibernética do dispositivo**, como os detalhados na NISTIR 8259A, que são implementados no dispositivo IoT e como configurá-los e usá-los. 3. Documentar o design do dispositivo e as considerações de suporte relacionadas ao dispositivo IoT, como:[4] a. Plataforma IoT[5] usada no desenvolvimento e operação do dispositivo IoT e documentação relacionada b. Proteção de componentes de software e hardware do dispositivo IoT (por exemplo, inicialização segura, raiz de confiança de hardware e enclave seguro) c. Consideração dos riscos conhecidos relacionados ao dispositivo IoT e potenciais usos indevidos conhecidos d. Práticas seguras de desenvolvimento de software e cadeia de suprimentos usadas e. Resultados de credenciamento, certificação e/ou avaliação para práticas relacionadas à segurança cibernética	• Esta capacidade apoia a Disseminação da Informação e a Educação e Conscientização. • Os fabricantes e/ou entidades de suporte devem considerar a documentação durante todo o seu ciclo de vida de desenvolvimento, a fim de capturar informações relevantes para a segurança cibernética quando estiverem disponíveis, de modo a garantir o acesso a essas informações quando necessário. A documentação começará como recursos internos para um fabricante e/ou entidade de suporte que podem ser usados de várias maneiras. • A documentação das informações de segurança cibernética é fundamental para a avaliação de risco que um fabricante deve realizar (conforme discutido na NISTIR 8259). • A documentação de informações de segurança cibernética pode ser fornecida para apoiar potenciais clientes de dispositivos IoT na tomada de decisões de compra. As organizações do cliente podem exigir essa documentação para garantir que o dispositivo IoT ofereça suporte a todos os requisitos de segurança cibernética da organização do cliente. • A documentação fornece uma fonte importante de informações de segurança cibernética que ajuda a permitir o uso seguro do dispositivo IoT pelos clientes. • A documentação também pode ser importante para auditorias, credenciamentos ou outras certificações. • A documentação sobre os requisitos de manutenção, especialmente no que diz respeito às partes de suporte contratadas pelo fabricante e fornecedor para realizar manutenção, alterações de dispositivos, etc., apoia a necessidade do fabricante, da entidade de suporte e/ou dos clientes de planejar adequadamente as atividades de manutenção.	• **AGELIGHT**: 11, 12 • **ETSI**: Disposição 4.1 • **IoTSF**: 2.4.3.4, 2.4.3.5, 2.4.3.6, 2.4.3.7, 2.4.12.5 • **CSDE**: 5.2.3

Recurso de Suporte Não Técnico	Ações Comuns	Rationale	Exemplos de Referência IoT
Documentação (*continuação*)	4. Documentar os requisitos de *manutenção* para o dispositivo IoT, tais como: a. Expectativas de manutenção de segurança cibernética e instruções ou procedimentos associados para o cliente (por exemplo, gerenciamento de contas, atividades de manutenção local e/ou remota e plano de gerenciamento de vulnerabilidades/patches) b. Quando a manutenção será realizada por partes de suporte que precisarão de acesso (remoto ou no local) aos dispositivos IoT do cliente e seus requisitos de contrato de segurança da informação c. Considerações de cibersegurança no processo de manutenção (por exemplo, como os dados dos clientes que não estão relacionados ao processo de manutenção permanecem confidenciais, mesmo para os responsáveis pela manutenção).	• A documentação das informações de segurança cibernética permite uma melhor compreensão dos riscos potenciais relacionados ao dispositivo IoT, o que pode informar os clientes e outras pessoas no ecossistema do dispositivo IoT e orientar o suporte contínuo à mitigação de riscos. • A documentação ajuda o pessoal com a responsabilidade de proteger os dispositivos IoT dentro do sistema a entender a implementação e operação dos controles e evitar o uso indevido e o comprometimento por entidades não autorizadas. • A documentação pode ser usada para fornecer informações e apoiar a gestão do risco da cadeia de suprimentos, resposta a incidentes e outras funções críticas de segurança cibernética.	*(ver acima)*

[4] Embora essas informações sejam fornecidas por uma Lista de Materiais de Software (SBOM), o que está sendo discutido aqui é significativamente menor do que o que normalmente se entende por uma SBOM. Mais detalhes sobre o SBOM podem ser encontrados em https://www.ntia.gov/SBOM.

[5] Uma plataforma IoT é tipicamente uma ferramenta baseada em SaaS fornecida/hospedada por terceiros que é usada para suportar gerenciamento de dispositivos e terminais IoT, conectividade e gerenciamento de rede, gerenciamento, processamento e análise de dados, desenvolvimento de aplicativos, segurança cibernética, controle de acesso, monitoramento, processamento de eventos e interface/integração. A documentação sobre esse terceiro pode fornecer informações importantes sobre as práticas e vulnerabilidades de segurança cibernética da cadeia de suprimentos para permitir que o usuário de IoT determine com mais precisão os riscos relacionados ao uso de uma plataforma de IoT.

Recurso de Suporte Não Técnico	Ações Comuns	Rationale	Exemplos de Referência IoT
Recepção de Informações e Consultas: A capacidade do fabricante e/ou entidade de suporte de receber informações e consultas do cliente e outros relacionados à segurança cibernética do dispositivo IoT.	1. A capacidade do fabricante e/ou entidade de suporte de receber informações de manutenção e vulnerabilidade (por exemplo, recursos de relatório de bugs e programas de recompensas por bugs) de seus clientes e outros no ecossistema de dispositivos IoT 2. A capacidade do fabricante e/ou entidade de suporte de responder a consultas de clientes e terceiros sobre segurança cibernética do dispositivo IoT (por exemplo, suporte ao cliente).	• Esse recurso fornece informações de clientes e outros no ecossistema de dispositivos IoT para o fabricante usar nos recursos de suporte não técnico de Divulgação de Informações e Educação e Conscientização. • Clientes e outros no ecossistema de dispositivos IoT podem querer, ou ser obrigados, a relatar vulnerabilidades que identificam em um dispositivo IoT. • Os fabricantes podem usar relatórios de consultas e vulnerabilidades comuns para identificar maneiras de melhorar a segurança cibernética do dispositivo IoT. • Alguns clientes podem precisar de suporte adicional para provisionar e usar com segurança um dispositivo IoT. • Apoia as responsabilidades dos clientes relacionadas à cibersegurança, como permitir que obtenham informações especializadas em cibersegurança que podem ser usadas de forma proativa (por exemplo, inteligência sobre ameaças e mitigação, investigações de forense digital, e reaprovisionamento e descarte seguro).	• **CTA**: VUL-002, VUL-003 • **AGELIGHT**: 9 • **ETSI**: Disposição 5.2-1 • **IoTSF**: 2.4.3.11, 2.4.3.12 • **CSDE**: 5.2.1, 5.2.2

Recurso de Suporte Não Técnico	Ações Comuns	Rationale	Exemplos de Referência IoT
Divulgação de Informações: A capacidade do fabricante e/ou da entidade de suporte de divulgar e distribuir (por exemplo, para o cliente ou outros no ecossistema de dispositivos IoT) informações relacionadas à cibersegurança do dispositivo IoT.	1. Os procedimentos para apoiar a capacidade do fabricante e/ou entidade de suporte de alertar os clientes do dispositivo IoT e outros sobre informações relevantes de segurança cibernética, como: a. Documentação aplicável capturada durante o design e desenvolvimento do dispositivo IoT b. Termos de suporte de atualização de software (por exemplo, frequência de atualizações e mecanismo(s) de aplicação) e aviso de disponibilidade e/ou aplicação de atualizações de software c. Fim do prazo de suporte ou funcionalidade para o dispositivo IoT d. Operações de manutenção necessárias e. Alertas de cibersegurança e vulnerabilidade e informações sobre a resolução de qualquer vulnerabilidade f. Uma visão geral das práticas e salvaguardas de segurança da informação usadas pelo fabricante e/ou entidade de suporte g. Resultados de acreditação, certificação e/ou avaliação das práticas relacionadas à cibersegurança do fabricante e/ou da entidade de suporte. h. Um relatório ou resumo de avaliação de riscos sobre a postura de risco do ambiente de negócios do fabricante. 2. Os procedimentos para apoiar a capacidade do fabricante e/ou entidade de suporte de notificar os clientes sobre eventos e informações relacionados à segurança cibernética relacionados a um dispositivo IoT durante todo o ciclo de vida do suporte, como: a. Novas vulnerabilidades de dispositivos IoT, detalhes associados e ações de mitigação b. Descoberta de violação relacionada a um dispositivo IoT usado pelos clientes e explicações de como fazer quaisquer correções ou ações associadas para evitar violações semelhantes de outros dispositivos.	• Esse recurso suporta a segurança cibernética contínua do dispositivo, mantendo os clientes informados sobre os desenvolvimentos e novas informações e recursos de configuração após o desenvolvimento e fornecimento da documentação inicial. A disseminação de informações permite o suporte, a administração e a manutenção necessários para garantir o desempenho e a segurança cibernética de dispositivos e sistemas de IoT eficazes e eficientes. • As organizações clientes podem precisar ser informadas sobre atividades relacionadas à segurança cibernética no dispositivo IoT, como atualizações de software, alterações de algoritmos, novos protocolos ou alterações nos fornecedores usados pelo fabricante para atualizar a segurança cibernética, especialmente se o dispositivo IoT for fundamental para suas operações. • As organizações clientes vão querer se manter informadas sobre a segurança cibernética dos dispositivos de IoT para que possam ajustar suas mitigações e manter um nível adequado de garantia de risco. • As organizações clientes podem precisar conhecer as práticas de segurança cibernética do fabricante e/ou entidades de suporte que fizeram ou terão acesso ocasional ou contínuo aos dispositivos IoT para garantir que as outras partes não aumentem inaceitavelmente o risco de segurança cibernética do cliente. • As organizações clientes podem usar essas informações para obter informações sobre o compromisso do fabricante com a segurança da informação e para determinar o nível de risco considerado pelo fabricante relacionado ao dispositivo. • As organizações clientes podem visualizar certificações, credenciamentos e avaliações de segurança cibernética para o que normalmente é uma garantia de terceiros de informações aceitáveis que descrevem cibersegurança, redes, aplicativos e práticas de segurança cibernética relacionadas.	• **CTA**: REP-005 EoL/EoS-001, EoL/EoS-002, DIN-001, DIN-002 • **AGELIGHT**: 1, 4, 20, 21, 22, 23, 32, 36 • **ETSI**: Disposições 5.3-11, 5.3-12, 5.3-13, 5.3-14, 5.3-16 • **IoTSF**: 2.4.3.9, 2.4.3.14, 2.4.5.35, 2.4.5.36 • **CSDE**: 5.2.3

Recurso de Suporte Não Técnico	Ações Comuns	Rationale	Exemplos de Referência IoT

Educação e Conscientização: A capacidade do fabricante e/ou da entidade de suporte de criar conscientização e educar os clientes e outros no ecossistema de dispositivos IoT sobre informações, considerações, recursos, etc., relacionados à cibersegurança do dispositivo IoT.	1. Educar os clientes do dispositivo IoT e outros no ecossistema sobre a presença e o uso de recursos de segurança cibernética do dispositivo. Por exemplo, pode ser importante educar os clientes e outras pessoas sobre:
	a. Como usar *identificadores de dispositivo*
	b. Como alterar as definições de configuração
	c. Como configurar e usar a funcionalidade de controle de acesso
	d. Como usar a funcionalidade de atualização de software, incluindo aspectos como validação e/ou reversão de atualizações que podem fazer parte do recurso de segurança cibernética do dispositivo.
	2. Informar os clientes e outras pessoas sobre como um dispositivo IoT pode ser reprovisionado ou descartado com segurança.
	3. Conscientizar os clientes e outras pessoas sobre suas responsabilidades de segurança cibernética relacionadas ao dispositivo IoT e como as responsabilidades podem ser compartilhadas entre eles e outras pessoas, como o fabricante do dispositivo IoT. (por exemplo, relacionado à manutenção do dispositivo IoT)
	4. Conscientizar os clientes e outras pessoas sobre as principais suposições e expectativas relacionadas à segurança cibernética do dispositivo IoT que foram documentadas, ao longo de todo o ciclo de vida de uso dos dispositivos IoT, levando em consideração a finalidade do dispositivo IoT e os usos pretendidos. Essas premissas devem incluir as principais dependências do dispositivo de IoT que afetam a segurança cibernética (por exemplo, requisitos de conectividade e uso de serviços de terceiros quando em operação).
	5. Educar os clientes e outras pessoas sobre como fazer backup dos dados coletados ou derivados pelo dispositivo IoT e como acessar esses dados armazenados no armazenamento em nuvem ou em outros repositórios.
	6. Educar os clientes e outras pessoas sobre as opções de gerenciamento de vulnerabilidades (por exemplo, configuração e gerenciamento de patches e antimalware) disponíveis para o dispositivo IoT ou sistema associado que pode ser usado pelos clientes.
		• Esse recurso suporta provisionamento seguro e suporte contínuo à segurança cibernética.
		• Para dispositivos IoT com uma ampla gama de casos de uso, alguns clientes podem precisar de mais educação do que outros para provisionar e usar com segurança um dispositivo IoT.
		• As complexidades dos sistemas, dispositivos e casos de uso de IoT significam que é importante que os fabricantes criem conscientização e conscientizem os clientes e outras pessoas sobre a segurança cibernética de seus dispositivos de IoT.
		• Os regulamentos e leis existentes exigem que o fabricante e/ou as entidades de suporte forneçam aos clientes acesso aos dados que o fabricante e/ou as entidades de suporte possuem sobre eles e também tornem esses dados portáteis para que os clientes possam pegar esses dados e usá-los em outro lugar.
		• Treinamento reforçado por comunicações ocasionais e contínuas de conscientização. Exemplos de treinamento incluem o fornecimento de:
		  • conscientização sobre segurança cibernética,
		  • instrução sobre o uso de recursos de segurança cibernética, e
		  • compreensão das responsabilidades relevantes para a segurança cibernética.
		O treinamento pode resultar em um uso mais seguro do dispositivo IoT e dos sistemas associados e evitar erros que possam resultar em incidentes de segurança cibernética. O treinamento eficaz também pode reduzir o número de vulnerabilidades que são exploradas e levam a dispositivos comprometidos.
			• **AGELIGHT**: 20, 21, 22, 23, 32, 34, 36
			• **ETSI**: Disposições 5.2-1, 5.11-3, 5.12-2, 5.12-3, 6-1, 6-5
			• **IoTSF**: 2.4.12.9, 2.4.12.10, 2.4.12.11, 2.4.12.12
			• **CSDE**: 5.2.3

Referências

[1] Fagan M, Megas KN, Scarfone K, Smith M (2020) Atividades Fundamentais de Cibersegurança para Fabricantes de Dispositivos IoT. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), Relatório Interno ou Interinstitucional (IR) 8259 do NIST. https://doi.org/10.6028/NIST.IR.8259

[2] Fagan M, Megas KN, Scarfone K, Smith M (2020) Base Fundamental de Capacidades de Cibersegurança para Dispositivos IoT. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), Relatório Interno ou Interinstitucional (IR) 8259A do NIST. https://doi.org/10.6028/NIST.IR.8259A

[3] Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas K, Nadeau E, Piccarreta B, O'Rourke DG, Scarfone K (2018) Considerações para Gerenciamento de Riscos de Cibersegurança e Privacidade na Internet das Coisas (IoT). (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), Relatório Interno ou Interinstitucional (IR) 8228 do NIST. https://doi.org/10.6028/NIST.IR.8228

[4] Fagan M, Megas, KN, Marron, J, Brady KG, Jr, Cuthill BB, Herold R (2020) Criando um Perfil Usando a Base Fundamental de IoT e a Base Não-Técnica. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), Rascunho do Relatório Interno ou Interinstitucional (IR) 8259C do NIST. https://doi.org/10.6028/NIST.IR.8259C-draft

[5] Catálogos de Requisitos de Segurança Cibernética de Dispositivos IoT do Instituto Nacional de Padrões e Tecnologia (2020). (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD). Disponível em https://github.com/usnistgov/IoT-Device-Cybersecurity-Requirement-Catalogs.

[6] Iniciativa de Transformação da Força-Tarefa Conjunta (2012) Guia para a Condução de Avaliações de Risco. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), Publicação Especial (SP) 800-30, Rev. 1 do NIST. https://doi.org/10.6028/NIST.SP.800-30r1

[7] Grupo Consultivo de Segurança Digital AgeLight (2020) Kit de Ferramentas de Arquitetura de Segurança e Risco para IoT v4.0. Atualizado em 24/02/20. Disponível em https://www.agelight.com/iot

[8] Associação de Tecnologia para Consumidores (2020) *ANSI/CTA-2088 - Padrão Básico de Cibersegurança para Dispositivos e Sistemas de Dispositivos* (Associação de Tecnologia para Consumidores, Arlington, VA). Disponível em https://csde.org/projects/c2-consensus/

[9] Conselho para Proteger a Economia Digital (2019) O Consenso C2 sobre Capacidades Básicas de Segurança de Dispositivos IoT. Disponível em https://csde.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf

[10] Instituto Europeu de Normas de Telecomunicações (2020) ETSI EN 303 645 v2.1.0 - Cibersegurança para Internet das Coisas para Consumidores. *Requisitos de Base* (Instituto Europeu de Normas de Telecomunicações, Valbonne, França). Disponível em https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[11] Fundação de Segurança para IoT (2020) Estrutura de Conformidade de Segurança para IoT v2.1. (Fundação de Segurança para Internet das Coisas, Livingston, Reino Unido). Disponível em https://www.iotsecurityfoundation.org/iotsf-issues-update-to-popular-iot-security-compliance-framework/

[12] Johnson A, Dempsey K, Ross R, Gupta S, Bailey D (2011) Guia para o Gerenciamento de Configurações de Sistemas de Informação com Foco em Segurança. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), Publicação Especial (SP) 800-128 do NIST. https://doi.org/10.6028/NIST.SP.800-128

[13] Força-Tarefa Conjunta (2020) Controles de Segurança e Privacidade para Sistemas de Informação e Organizações. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), Publicação Especial (SP) 800-53, Rev. 5 do NIST. Inclui atualizações a partir de 10 de dezembro de 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[14] Souppaya M, Scarfone K (2013) Guia para Tecnologias de Gerenciamento de Patches Empresariais. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), Publicação Especial (SP) 800-40, Rev. 3 do NIST. https://doi.org/10.6028/NIST.SP.800-40r3

[15] Barker E, Chen L, Roginsky A, Vassilev A, Davis R (2019) Recomendação para Esquemas de Estabelecimento de Chaves Pareadas Usando Criptografia de Logaritmo Discreto. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), Publicação Especial (SP) 800-56A, Rev. 3 do NIST. https://doi.org/10.6028/NIST.SP.800-56Ar3

[16] Comitê de Sistemas de Segurança Nacional (2015) Comitê de Sistemas de Segurança Nacional (CNSS) Glossário. (Agência de Segurança Nacional, Ft. Meade, MD), Instrução CNSS (CNSSI) nº 4009. Disponível em https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[17] Schaffer K, Mell P, Trinh H. (2021) Recomendações para diretrizes federais de divulgação de vulnerabilidades. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), Rascunho da Publicação Especial (SP) 800-216 do NIST. https://doi.org/10.6028/NIST.SP.800-216-draft

Appendix A Siglas

As siglas e abreviaturas selecionadas usadas neste artigo são definidas abaixo.

ACD	Divisão de Segurança Cibernética Aplicada
CNSS	Comitê de Sistemas de Segurança Nacional
FISMA	Lei Federal de Modernização da Segurança da Informação
IoT	Internet das Coisas
ITL	Laboratório de Tecnologia da Informação
RI	Relatório Interno
MAC	Controle de Acesso à Mídia
NIST	Instituto Nacional de Padrões e Tecnologia
SBOM	Lista de Materiais do Software
SP	Publicação Especial

Appendix B Glossário

Os termos selecionados usados neste documento são definidos abaixo.

Comunicações	As ações e atividades associadas que são usadas para trocar informações, fornecer instruções, dar detalhes, etc. No contexto deste artigo, as comunicações referem-se a toda a gama de atividades envolvidas no fornecimento de informações para apoiar o uso seguro de dispositivos IoT. As comunicações incluem o uso de ferramentas como telefonemas, e-mails, guias do usuário, aulas presenciais, manuais de instruções, webinários, instruções escritas, vídeos, questionários, documentos de perguntas frequentes (FAQ) e qualquer outro tipo de ferramenta para essas trocas de informações.
Configuração [7, Adaptado]	As possíveis condições, parâmetros e especificações com as quais um sistema de informação ou componente do sistema pode ser descrito ou organizado. A capacidade de Configuração do Dispositivo não define quais definições de configuração devem existir, simplesmente que existe um mecanismo para gerenciar as definições de configuração.
Base Principal	Um conjunto de recursos de dispositivos técnicos necessários para oferecer suporte a controles comuns de segurança cibernética que protegem os dispositivos e os dados, sistemas e ecossistemas do dispositivo do cliente.
Cliente [12]	A organização ou pessoa que recebe um produto ou serviço.
Capacidade de Segurança Cibernética de Dispositivos	Recursos ou funções de segurança cibernética que os dispositivos de computação fornecem por seus próprios meios técnicos (ou seja, hardware e software do dispositivo).
Identificador de Dispositivo [10, Adaptado]	Um valor exclusivo de contexto - um valor exclusivo dentro de um contexto específico - que está associado a um dispositivo (por exemplo, uma cadeia de caracteres que consiste em um endereço de rede).
Entidade	Uma pessoa, dispositivo, serviço, rede, domínio, fabricante ou outra parte que possa interagir com um dispositivo IoT.

Plataforma IoT	Uma plataforma IoT é tipicamente uma ferramenta baseada em SaaS[6] fornecida/hospedada por terceiros que é usada para suportar gerenciamento de dispositivos e terminais IoT, conectividade e gerenciamento de rede, gerenciamento, processamento e análise de dados, desenvolvimento de aplicativos, segurança cibernética, controle de acesso, monitoramento, processamento de eventos e interface/integração. A documentação sobre esse terceiro pode fornecer informações importantes sobre as práticas e vulnerabilidades de segurança cibernética da cadeia de suprimentos para permitir que o usuário de IoT determine com mais precisão os riscos relacionados ao uso de uma plataforma de IoT.
Manutenção [11]	Qualquer ato que evite a falha ou mau funcionamento do dispositivo IoT e do equipamento de suporte ou restaure sua capacidade operacional.
Recurso de Suporte Não Técnico	Capacidades de suporte não técnicas são ações que uma organização realiza em apoio à cibersegurança de um dispositivo IoT.
Base Principal da Capacidade de Suporte Não Técnico	A base principal de recursos de suporte não técnico é um conjunto de recursos de suporte não técnicos geralmente necessários de fabricantes ou outros terceiros para oferecer suporte a controles comuns de segurança cibernética que protegem os dispositivos de uma organização, bem como dados, sistemas e ecossistemas de dispositivos.
Software	Programas de computador e dados associados que podem ser gravados ou modificados dinamicamente durante a execução do dispositivo (por exemplo, código de aplicativo, bibliotecas).
Partes de Suporte	Fornecedores de serviços de sistemas externos ao fabricante por meio de uma variedade de relações consumidor-produtor, incluindo, mas não se limitando a: joint ventures; parcerias comerciais; acordos de terceirização (ou seja, por meio de contratos, acordos interinstitucionais, acordos de linhas de negócios); acordos de licenciamento; e/ou trocas de cadeia de suprimentos. Os serviços de suporte incluem, por exemplo, Telecomunicações, serviços de engenharia, energia, água, software, suporte técnico e segurança.
Termo de Suporte	O período de tempo durante o qual o dispositivo será suportado pelo fabricante ou pelas partes de suporte para tais ações e materiais como substituições de peças, atualizações de software, avisos de vulnerabilidade, perguntas de suporte técnico, etc.
Treinamento	Ensinar às pessoas o conhecimento e as habilidades e competências de segurança cibernética relevantes e necessárias que lhes permitirão entender como usar e configurar os dispositivos IoT para permitir que eles usem com mais segurança os dispositivos IoT.

[6] Software como Serviço

Atualizar [9]	Um patch, atualização ou outra modificação no código que corrige problemas de segurança e/ou funcionalidade no software.