

**NISTIR 8228**

# **Considerações para Gerenciar Riscos de Privacidade e Segurança Cibernética na Internet das Coisas (IoT)**

Katie Boeckl  
Michael Fagan  
William Fisher  
Naomi Lefkowitz  
Katerina N. Megas  
Ellen Nadeau  
Danna Gabel O'Rourke  
Ben Piccarreta  
Karen Scarfone

Esta publicação está disponível gratuitamente em:  
<https://doi.org/10.6028/NIST.IR.8228pt>

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

**NISTIR 8228**

# **Considerações para Gerenciar Riscos de Privacidade e Segurança Cibernética na Internet das Coisas (IoT)**

Katie Boeckl  
Michael Fagan  
William Fisher  
Naomi Lefkowitz  
Katerina N. Megas  
Ellen Nadeau  
Ben Piccarreta

*Divisão de Segurança Cibernética Aplicada  
Laboratório de Tecnologia da Informação*

Danna Gabel O'Rourke  
*Deloitte & Touche LLP  
Arlington, Virginia*

Karen Scarfone  
*Scarfone Cybersecurity  
Clifton, Virginia*

Esta publicação está disponível gratuitamente em:  
<https://doi.org/10.6028/NIST.IR.8228pt>

Junho 2019



Departamento de Comércio dos EUA  
*Wilbur L. Ross, Jr., Secretário*

Instituto Nacional de Padrões e Tecnologia  
*Walter Copan, Diretor do NIST e Subsecretário de Comércio para Padrões e Tecnologia*

Relatório Interno do Instituto Nacional de Padrões e Tecnologia 8228  
45 páginas (Junho 2019)

Esta publicação está disponível gratuitamente em:  
<https://doi.org/10.6028/NIST.IR.8228pt>

Certas entidades comerciais, equipamentos ou materiais podem ser identificados neste documento para descrever adequadamente determinado procedimento ou conceito experimental. Esta identificação não tem a intenção de sugerir recomendação ou endosso do NIST, nem tem a intenção de sugerir que as entidades, materiais ou equipamentos sejam necessariamente os melhores disponíveis para tal propósito.

Esta publicação pode conter referências a outras publicações atualmente sendo produzidas pelo NIST de acordo com suas responsabilidades estatutárias atribuídas. As informações nesta publicação, incluindo conceitos e metodologias, podem ser usadas por agências federais mesmo antes da conclusão de tais publicações complementares. Assim sendo, até que cada publicação seja concluída, os requisitos, diretrizes e procedimentos atuais, onde existam, permanecem operacionais. Para fins de planejamento e transição, as agências federais podem desejar acompanhar de perto o desenvolvimento dessas novas publicações produzidas pelo NIST.

As organizações são incentivadas a revisar todos os esboços preliminares das publicações durante os períodos de comentários públicos e fornecer feedback ao NIST. Muitas publicações do NIST sobre segurança cibernética, além das mencionadas acima, estão disponíveis em <https://csrc.nist.gov/publications>.

**Os 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](mailto:iotsecurity@nist.gov)

Todos os comentários estão sujeitos a divulgação no âmbito da Lei de Liberdade de Informação (FOIA).

**Disclaimer**

This document was translated by the U.S. Department of State, Office of Language Services with support from the [Digital Connectivity and Cybersecurity Partnership \(DCCP\)](#).

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.8228>.

## **Relatórios sobre Tecnologia de Sistemas Informáticos**

O Laboratório de Tecnologia da Informação (ITL) do Instituto Nacional de Normas e Tecnologia (NIST) promove a economia e o bem-estar público dos EUA, fornecendo liderança técnica para a infraestrutura de medição e normas da Nação. O ITL desenvolve testes, métodos de testes, 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 do ITL incluem o desenvolvimento de padrões e diretrizes de gestão, administrativos, técnicos e físicos para a segurança economicamente viável e a privacidade de outras informações além das relacionadas à segurança nacional em sistemas federais de informação.

### **Resumo**

A Internet das Coisas (IoT) é uma coleção em rápida evolução e expansão de diversas tecnologias que interagem com o mundo físico. Muitas organizações não estão necessariamente cientes do grande número de dispositivos IoT que já estão usando e como eles podem afetar a segurança cibernética e os riscos de privacidade de diferentes maneiras, comparado aos dispositivos convencionais de tecnologia da informação (TI). O objetivo desta publicação é ajudar as agências federais e outras organizações a compreender e melhor gerenciar os riscos de segurança cibernética e privacidade associados a seus dispositivos IoT individuais durante todo o ciclo de vida de tais dispositivos. Esta publicação é um documento introdutório que serve de base para uma série planejada de publicações sobre alguns aspectos mais específicos relacionados a este tópico.

### **Palavras-chave**

risco de cibersegurança; internet das coisas (IoT); risco de privacidade; gestão de risco; mitigação de risco.

## Reconhecimentos

Os autores desejam agradecer a todos os que contribuíram com esta publicação, incluindo os participantes dos workshops e outras sessões interativas, e também aos indivíduos e organizações dos setores público e privado que forneceram comentários sobre as ideias preliminares e aos seguintes indivíduos do NIST: Curt Barker, Matt Barrett, Barbara Cuthill, Donna Dodson, Jim Foti, Ned Goren, Nelson Hastings, Jody Jacobs, Suzanne Lightman, Jeff Marron, Vicky Pillitteri, Tim Polk, Matt Scholl, Eric Simmon, Matt Smith, Murugiah Souppaya, Jim St. Pierre, Kevin Stine e David Wollman.

## Público-alvo

O público-alvo para esta publicação são os funcionários de agências federais com responsabilidades relacionadas à gestão de risco de privacidade e segurança cibernética para dispositivos IoT, embora os funcionários de outras organizações também possam usufruir deste conteúdo. Os funcionários que integram as seguintes categorias da força de trabalho e áreas de especialidade da Estrutura da Força de Trabalho em Segurança Cibernética da Iniciativa Nacional para Educação em Cibersegurança (NICE) [1] provavelmente serão os mais interessados nesta publicação, assim como as suas contrapartes no setor de privacidade:

- Provisão de segurança (SP): Gestão de Risco (RSK), Arquitetura de Sistemas (ARC), Desenvolvimento de Sistemas (SYS)
- Operar e Manter (OM): Administração de Dados (DTA), Serviços de Rede (NET), Administração de Sistemas (ADM), Análise de Sistemas (ANA)
- Supervisionar e Governar (OV): Gerenciamento de Segurança Cibernética (MGT), Liderança Cibernética Executiva (EXL), Gerenciamento de Programas/Projetos (PMA) e Aquisição
- Proteger e Defender (PR): Análise de Defesa de Segurança Cibernética (CDA), Suporte de Infraestrutura de Defesa de Segurança Cibernética (INF), Resposta a Incidentes (CIR), Avaliação e Gerenciamento de Vulnerabilidades (VAM)
- Investigar (IN): Forense Digital (FOR)

Além disso, os fabricantes e integradores de dispositivos IoT podem considerar esta publicação útil, pois poderão melhor compreender as preocupações relacionadas à gestão de risco de privacidade e segurança cibernética para dispositivos IoT.

## Nota aos leitores

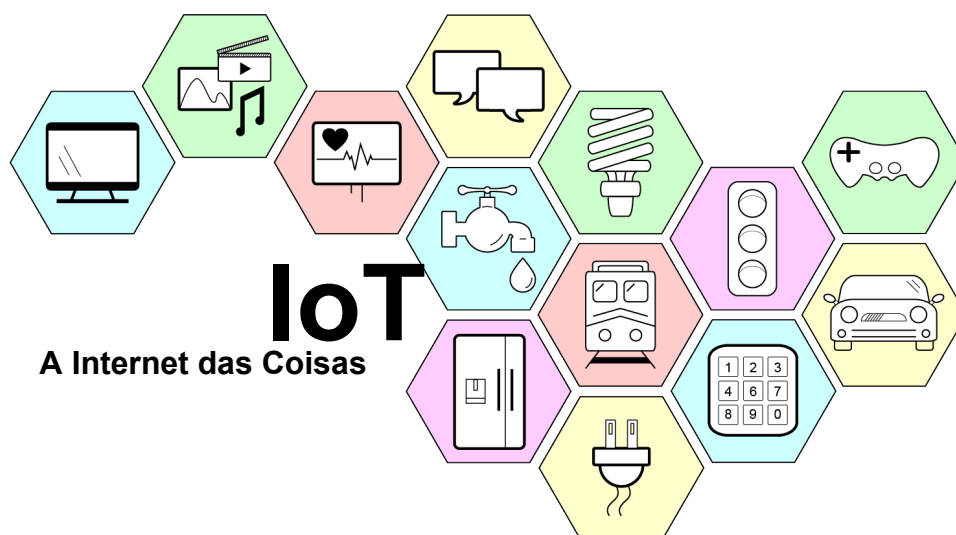
Anteriormente, o Apêndice A apresentava exemplos de possíveis recursos de segurança cibernética e privacidade que as organizações desejariam integrar em seus dispositivos IoT. Esse conteúdo foi retirado desta publicação e será aprimorado para ser lançado em uma publicação separada.

## Informações sobre marcas registradas

Todas as marcas registradas e marcas comerciais pertencem às suas respectivas organizações.

## Síntese

A Internet das Coisas (IoT) é uma coleção em rápida evolução e expansão de diversas tecnologias que interagem com o mundo físico. Os dispositivos IoT são o resultado da combinação de dois mundos - o da tecnologia da informação (TI) e o da tecnologia operacional (OT). Muitos dispositivos IoT são o resultado da convergência de computação em nuvem, computação móvel, sistemas incorporados, big data, hardware de baixo preço e outros avanços tecnológicos. Os dispositivos IoT proporcionam funcionalidade de computação, armazenamento de dados e conectividade de rede para equipamentos que antes não tinham tais recursos, permitindo novas eficiências e avanços tecnológicos, como o acesso remoto para monitoramento, configuração e solução de problemas. A IoT também pode acrescentar habilidades de análise de dados sobre o mundo físico, usando os resultados para melhor informar antes de uma tomada de decisão, para alterar o ambiente físico e antecipar eventos futuros.



Embora o escopo completo da IoT não seja definido com precisão, ele é obviamente muito vasto. Cada setor tem seus próprios tipos de dispositivos IoT, como equipamentos hospitalares especializados no setor de saúde, e tecnologias rodoviárias inteligentes no setor de transporte, havendo ainda um grande número de dispositivos IoT corporativos que todos os setores podem utilizar. Versões de quase todos os dispositivos eletrônicos de consumo, muitos dos quais também estão presentes nas instalações das organizações, tornaram-se dispositivos IoT conectados - eletrodomésticos, termostatos, câmeras de segurança doméstica, fechaduras, lâmpadas e TVs. [2]

Muitas organizações não estão necessariamente cientes de que estão usando um grande número de dispositivos IoT. É importante que as organizações entendam o uso de IoT já que muitos dispositivos IoT afetam a segurança cibernética e os riscos de privacidade de diferentes maneiras, se comparado aos dispositivos de TI convencionais. Quando as organizações se tornam cientes do uso atual e futuro de dispositivos IoT, precisam também entender como as características de IoT afetam a gestão de riscos de privacidade e segurança cibernética, especialmente em termos de resposta a riscos - isto é, aceitar, evitar, mitigar, compartilhar e transferir riscos.

Esta publicação identifica três considerações de alto nível que podem afetar a gestão de riscos de segurança cibernética e privacidade para dispositivos IoT em comparação com dispositivos de TI convencionais:

1. **Muitos dispositivos IoT interagem com o mundo físico de maneira diferente dos dispositivos convencionais de TI.** O impacto potencial de alguns dispositivos IoT que provocam alterações em sistemas físicos e, portanto, afetam o mundo físico, precisa ser explicitamente reconhecido e abordado, levando-se em consideração perspectivas de segurança cibernética e privacidade. Além disso, os requisitos operacionais de desempenho, confiabilidade, resiliência e segurança podem estar em conflito com as práticas comuns de segurança cibernética e privacidade para dispositivos de TI convencionais.
2. **Muitos dispositivos IoT não podem ser acessados, gerenciados ou monitorados da mesma forma que os dispositivos convencionais de TI.** Isso pode exigir a execução de tarefas manualmente para vários dispositivos IoT, o que amplia o conhecimento e as ferramentas da sua equipe, pois inclui uma ampla variedade de softwares de dispositivos IoT, tendo também que abordar riscos com fabricantes e terceiros que tenham acesso remoto ou controle dos dispositivos IoT.
3. **A disponibilidade, eficiência e eficácia dos recursos de segurança cibernética e privacidade são muitas vezes diferentes para dispositivos IoT comparado aos dispositivos convencionais de TI.** Isso significa que as organizações terão que selecionar, implementar e gerenciar controles adicionais, bem como determinar como responder ao risco quando controles suficientes para mitigar o risco não estiverem disponíveis.

Os riscos de cibersegurança e privacidade para dispositivos IoT podem ser considerados em termos de três objetivos de mitigação de risco de alto nível:

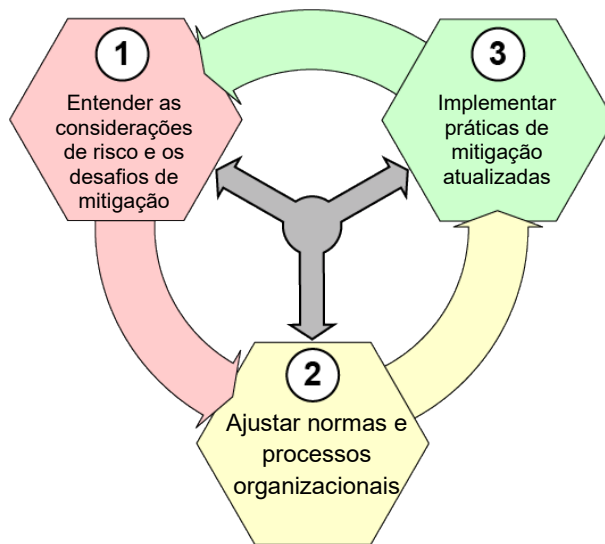
1. **Proteger a segurança do dispositivo.** Em outras palavras, evitar que um dispositivo seja usado para conduzir ataques, incluindo a participação em ataque distribuído de negação de serviço (DDoS) contra outras organizações e a espionagem de tráfego de rede, ou comprometer outros dispositivos no mesmo segmento de rede. Este objetivo se aplica a todos os dispositivos IoT. Este objetivo se aplica a todos os dispositivos IoT.
2. **Proteger a segurança de dados.** Proteger a confidencialidade, integridade e/ou disponibilidade dos dados (incluindo informações pessoalmente identificáveis [PII]) coletadas, armazenadas, processadas ou transmitidas para ou do dispositivo IoT. Este objetivo se aplica a cada dispositivo IoT, exceto aqueles que não contenham dados que precisem de proteção.
3. **Proteger a privacidade dos indivíduos.** Proteger a privacidade das pessoas afetadas pelo processamento de PII, além dos riscos gerenciados por meio de dispositivos e proteção de segurança de dados. Este objetivo se aplica a todos os dispositivos IoT que processam PII ou que afetam indivíduos direta ou indiretamente.

Cada objetivo se baseia no objetivo anterior e não o substitui ou nega a sua necessidade. Atender a cada um dos objetivos de mitigação de risco envolve abordar um conjunto de áreas de mitigação de risco. Cada área de mitigação de risco define um aspecto da mitigação de risco de privacidade ou segurança cibernética que se acredita ser mais significativo ou que tenha inesperadamente afetado a IoT no âmbito das considerações de risco. Para cada área de mitigação de risco, existem algumas expectativas das organizações sobre como os dispositivos de TI convencionais ajudam a mitigar os riscos de segurança cibernética e privacidade para determinada área. Como também, existem alguns desafios que os dispositivos IoT podem apresentar para cada expectativa. A figura abaixo mostra o resultado final dessas lincagens, isto é, a identificação de um conjunto estruturado de desafios potenciais para mitigar os riscos de segurança cibernética e privacidade para dispositivos IoT, que podem ser rastreados e associados às considerações de risco relevantes.



As organizações devem estar seguras de que estão abordando as considerações e desafios de risco de privacidade e segurança cibernética em todo o ciclo de vida do dispositivo IoT nas áreas e objetivos de mitigação de risco apropriados. Esta publicação fornece as seguintes recomendações para que isto seja feito:

1. Compreender as considerações de risco dos dispositivos IoT e os desafios que possam apresentar no sentido de mitigar os riscos de segurança cibernética e privacidade para dispositivos IoT nas devidas áreas de mitigação de risco.
2. Ajustar as políticas e processos organizacionais para lidar com os desafios de mitigação de risco de segurança cibernética e privacidade em todo o ciclo de vida dos dispositivos IoT. Esta publicação cita muitos exemplos de possíveis desafios, porém, cada organização deverá customizá-los, levando em consideração os seus próprios requisitos de missão e outras características específicas da organização.
3. Implementar práticas de mitigação atualizadas para os dispositivos IoT, assim como você faria no caso de qualquer outra mudança nas práticas da organização.





## Tabela de Conteúdo

<b>Síntese</b> .....	<b>iv</b>
<b>1 Introdução</b> .....	<b>1</b>
1.1 Propósito e Escopo .....	1
1.2 Estrutura da Publicação .....	1
<b>2 Recursos dos dispositivos IoT</b> .....	<b>3</b>
<b>3 Considerações sobre riscos de segurança cibernética e privacidade</b> .....	<b>5</b>
3.1 Consideração 1: Interações do dispositivo com o mundo físico .....	6
3.2 Consideração 2: Recursos de acesso, gerenciamento e monitoramento de dispositivos .....	7
3.3 Consideração 3: Disponibilidade, eficiência e eficácia da capacidade de segurança cibernética e de privacidade .....	9
<b>4 Desafios de segurança cibernética e mitigação de risco de privacidade para dispositivos IoT</b> .....	<b>11</b>
4.1 Desafios potenciais para alcançar o objetivo 1 - Proteger a Segurança do Dispositivo .....	12
4.2 Desafios potenciais para alcançar o objetivo 2 - Proteger a Segurança de Dados .....	22
4.3 Desafios potenciais para alcançar o objetivo 3, proteger a privacidade dos indivíduos .....	23
<b>5 Recomendações para abordar desafios de mitigação de riscos de segurança cibernética e privacidade para dispositivos IoT</b> .....	<b>27</b>
5.1 Ajustando normas e processos organizacionais .....	27
5.2 Implementando práticas atualizadas de mitigação de risco .....	29

## Lista dos Apêndices

<b>Apêndice A - [Retirado]</b> .....	<b>31</b>
<b>Apêndice B - Siglas e Abreviações</b> .....	<b>32</b>
<b>Apêndice C - Glossário</b> .....	<b>33</b>
<b>Apêndice D - Referências</b> .....	<b>35</b>

## Lista das Figuras

Figura 1: Tópicos abordados nesta publicação .....	2
--	---

Figura 2: Recursos do dispositivo IoT que potencialmente afetam a segurança cibernética .....	4
Figura 3: Relação entre segurança cibernética e riscos de privacidade .....	5
Figura 4: Objetivos de mitigação de risco .....	11
Figura 5: Relações entre os conceitos da Seção 3 e da Seção 4 .....	13
Figura 6: Resumo da recomendação .....	27

### Lista das Tabelas

Tabela 1: Desafios potenciais para alcançar o objetivo 1, Proteger a Segurança do Dispositivo .....	14
Tabela 2: Desafios potenciais para alcançar o objetivo 2, proteger a segurança de dados.....	22
Tabela 3: Desafios potenciais para alcançar o objetivo 3, proteger a privacidade dos indivíduos .....	24

## 1 Introdução

### 1.1 Propósito e Escopo

O objetivo desta publicação é ajudar as organizações a compreender e melhor gerir os riscos de segurança cibernética e privacidade associados aos dispositivos individuais da Internet das Coisas (IoT) durante todo o ciclo de vida dos dispositivos. Esta publicação enfatiza o que torna diferente o gerenciamento de risco para dispositivos IoT em termos gerais, comparado aos dispositivos convencionais de tecnologia da informação (TI), inclusive em se tratando de dispositivos IoT para consumidores, empresas e indústria. A publicação omite todos os aspectos de gestão de risco que são basicamente os mesmos para IoT e TI convencional, omitindo ainda todos os aspectos de gestão de risco que vão além dos próprios dispositivos IoT, já que esses aspectos são abordados por muitas outras publicações sobre gestão de risco.

A publicação fornece insights para informar os processos de gestão de risco das organizações. Depois de ler esta publicação, uma organização deverá estar apta a melhorar a qualidade das suas avaliações de risco para dispositivos IoT, bem como a sua resposta ao risco identificado sob a ótica da segurança cibernética e privacidade. No entanto, isso não significa que os riscos de segurança cibernética e privacidade para um dispositivo IoT possam ser resolvidos dentro do próprio dispositivo. Cada dispositivo IoT opera em um ambiente IoT mais amplo, onde interage com outros dispositivos IoT e não IoT, serviços baseados em nuvem, pessoas e outros componentes.

Para alguns dispositivos IoT, existem outros tipos de risco, incluindo segurança, confiabilidade e resiliência, que precisam ser gerenciados simultaneamente com os riscos de segurança cibernética e privacidade, já que os efeitos de lidar com um tipo de risco podem impactar outros riscos. Apenas os riscos de segurança cibernética e privacidade estão incluídos nesta publicação. Os leitores que estão particularmente interessados em entender melhor outros tipos de riscos e sua relação com a segurança cibernética e privacidade podem se beneficiar da leitura da Publicação Especial do NIST (SP) 800-82 Revisão 2, *Guia para Segurança de Sistemas de Controle Industrial (ICS)*, que oferece uma perspectiva de tecnologia operacional (OT) sobre cibersegurança e privacidade. [3]

Os leitores não precisam ter conhecimento técnico da composição e dos recursos do dispositivo IoT, mas devem ter um conhecimento básico dos princípios de privacidade e segurança cibernética.

### 1.2 Estrutura da Publicação

O restante desta publicação está organizado nas seguintes seções principais e apêndices:

- A Seção 2 define os recursos que os dispositivos IoT podem oferecer e que são de interesse primário em termos de potencialmente afetar a segurança cibernética e o risco de privacidade.
- A Seção 3 descreve as considerações que podem afetar o gerenciamento de risco de segurança cibernética e privacidade para dispositivos IoT.
- A Seção 4 explora como as considerações de risco podem afetar a mitigação dos riscos de segurança cibernética e privacidade para dispositivos IoT. A seção lista as expectativas de como esses riscos são mitigados em ambientes de TI convencionais e, em seguida, explica como a IoT apresenta desafios para essas expectativas e quais são as implicações potenciais desses desafios.
- A Seção 5 fornece recomendações para as organizações sobre como lidar com os desafios de mitigação de riscos de segurança cibernética e privacidade para seus dispositivos IoT..

- Anteriormente, o Apêndice A apresentava exemplos de possíveis recursos de segurança cibernética e privacidade que as organizações desejariam integrar em seus dispositivos IoT. Esse conteúdo foi retirado desta publicação e será aprimorado para ser lançado em uma publicação separada.
- O Apêndice B fornece uma lista de siglas e abreviações.
- O Apêndice C contém um glossário de termos selecionados usados na publicação.
- O Apêndice D lista as referências da publicação.

Figura 1: descreve os tópicos abordados em cada seção e subseção desta publicação.

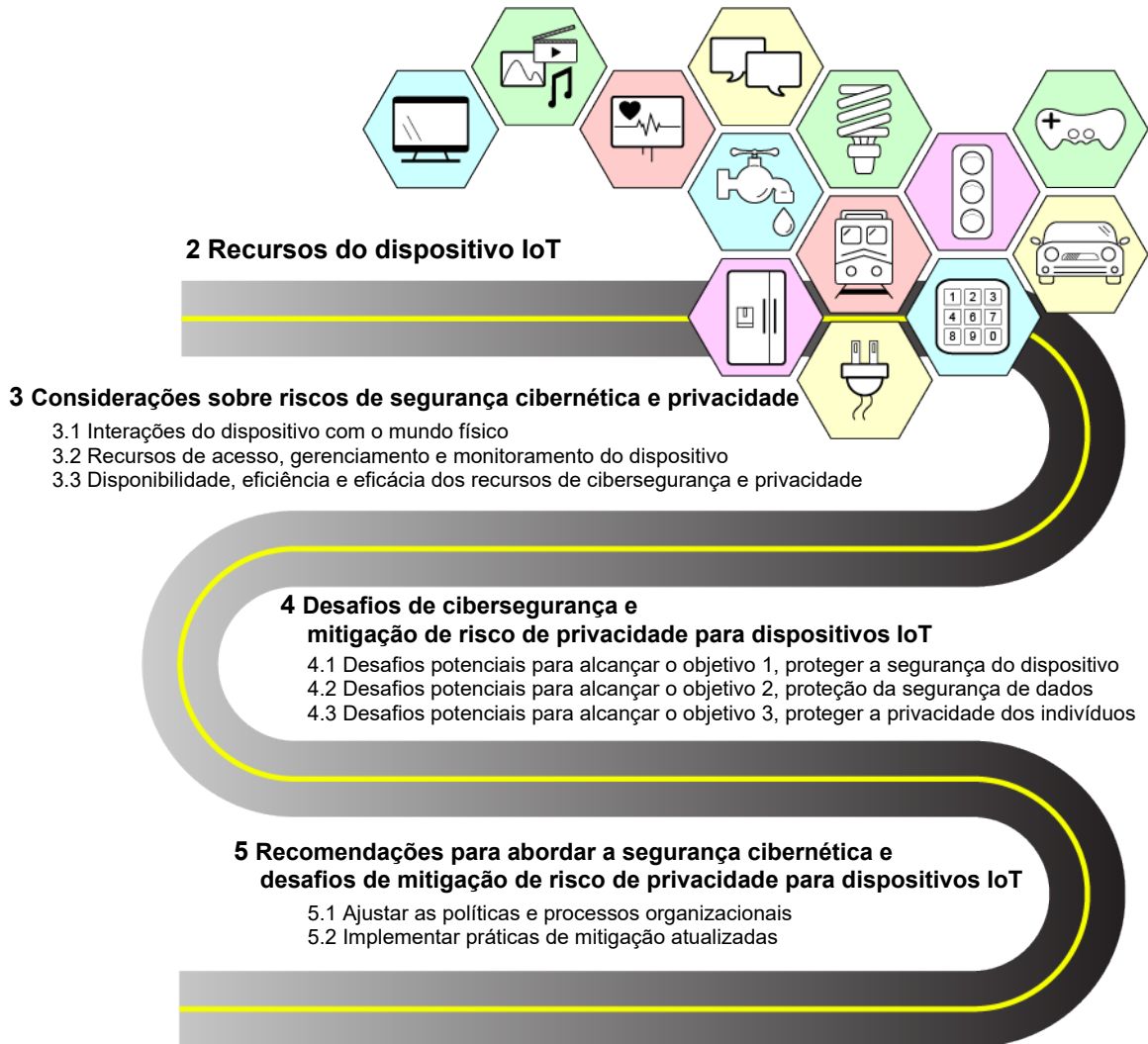


Figura 1: Tópicos abordados nesta publicação

## 2 Recursos dos dispositivos IoT

Cada dispositivo IoT oferece recursos - atributos ou funções - que podem ser usados isoladamente ou junto com outros dispositivos IoT e não IoT para atingir um ou mais objetivos. Esta publicação faz referência aos seguintes tipos de recursos que os dispositivos IoT podem oferecer, que são de principal interesse em termos de potencialmente afetar a segurança cibernética e os riscos de privacidade de forma diferente dos dispositivos de TI convencionais. Esta não é uma lista abrangente contendo todos os recursos possíveis dos dispositivos IoT.

- Os recursos do transdutor interagem com o mundo físico e servem como uma fronteira entre os ambientes digital e físico. Os recursos do transdutor fornecem capacidade para que os dispositivos de computação possam interagir diretamente com entidades físicas de interesse. Cada dispositivo IoT tem pelo menos um recurso de transdutor. Os dois tipos de recursos do transdutor são:
  - *Sensor*: a capacidade de fornecer uma observação de um aspecto do mundo físico na forma de dados de medição. Os exemplos incluem medição de temperatura, imagens radiográficas, detecção óptica e detecção de áudio.
  - *Atuador*: a capacidade de mudar algo no mundo físico. Exemplos de capacidades do atuador incluem bobinas de aquecimento, aplicação de choque elétrico cardíaco, fechaduras eletrônicas para portas, operação de veículo aéreo não tripulado, servo motores e braços robóticos.
- Os *recursos de interface* permitem interações do dispositivo (ex.: comunicações de dispositivo para dispositivo, comunicações de humanos para dispositivo). Os tipos de recursos de interface são:
  - *Interface do aplicativo*: a capacidade de outros dispositivos de computação se comunicarem com um dispositivo IoT por meio de um aplicativo do dispositivo IoT. Um exemplo de capacidade de interface do aplicativo é uma interface de programação de aplicativos (API).
  - *Interface de usuário humano*: a capacidade de um dispositivo IoT e as pessoas se comunicarem diretamente entre si. Exemplos de recursos de interface de usuário humano incluem telas sensíveis ao toque, dispositivos táteis, microfones, câmeras e alto-falantes.
  - *Interface de rede*: a capacidade de fazer interface com uma rede de comunicação com o objetivo de comunicar dados de ou para um dispositivo IoT - ou seja, usar uma rede de comunicação. Uma capacidade de interface de rede inclui hardware e software (ex.: uma placa ou chip de interface de rede e a implementação de software do protocolo de rede que usa um cartão ou chip). Exemplos de recursos de interface de rede incluem Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution (LTE) e ZigBee. Cada dispositivo IoT tem pelo menos um recurso de interface de rede habilitado e pode ter mais do que um.
- *Recursos de suporte* viabilizam a funcionalidade que dá suporte a outros recursos de IoT. Por exemplo, gerenciamento de dispositivos, segurança cibernética e recursos de privacidade. [2]

Figura 2 resumo dos recursos dos dispositivos IoT.

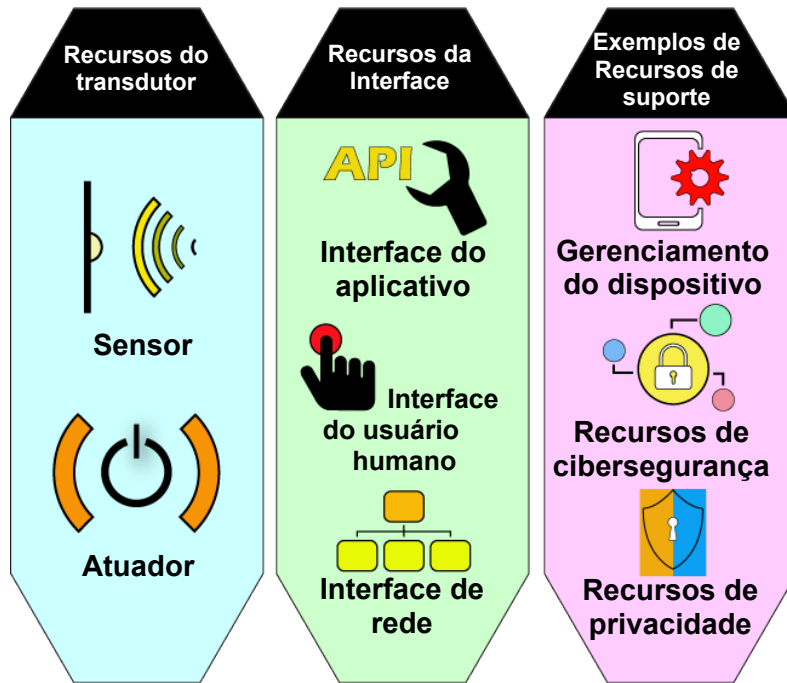
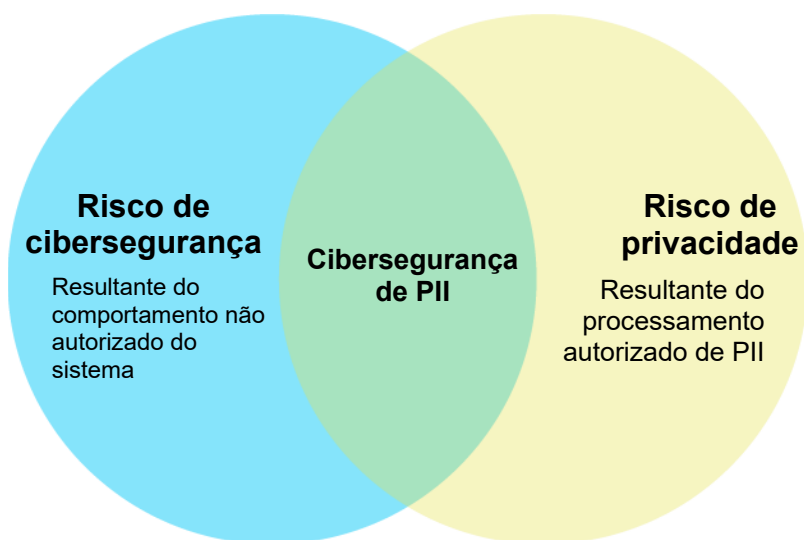


Figura 2: Recursos do dispositivo IoT que potencialmente afetam a segurança cibernética e o risco de privacidade

### 3 Considerações sobre riscos de segurança cibernética e privacidade

O risco de segurança cibernética e o risco de privacidade são conceitos relacionados, porém, distintos. *Risco* é definido na Publicação Especial do NIST (SP) 800-37 Revisão 2 como "uma medida da extensão em que uma entidade é ameaçada por uma circunstância ou evento potencial, sendo normalmente uma função do: (i) impacto adverso, ou magnitude do dano que surgiria se a circunstância ou evento ocorresse; e (ii) a probabilidade da ocorrência." [4] No tocante à segurança cibernética, o risco refere-se a ameaças - a exploração de vulnerabilidades por atores de ameaças para comprometer a confidencialidade, integridade ou disponibilidade de dados ou dispositivos. No tocante à privacidade, o risco envolve *ações problemáticas de dados* - operações que processam informações pessoalmente identificáveis (PII) durante o ciclo de vida das informações para atender às necessidades de missão ou negócios de uma organização ou processamento de PII "autorizado" e, como efeito colateral, causam alguns tipos de problemas aos indivíduos. Conforme mostra a Figura 3 os riscos de privacidade e segurança cibernética se sobrepõem em se tratando de preocupações sobre segurança cibernética de PII. Isto significa que existem preocupações sobre privacidade sem implicações quanto à segurança cibernética, como também, existem preocupações com a segurança cibernética sem implicações quanto à privacidade. [5]



**Figura 3: Relação entre segurança cibernética e riscos de privacidade**

Os dispositivos IoT geralmente enfrentam os mesmos tipos de riscos de segurança cibernética e privacidade que os dispositivos de TI convencionais, embora a prevalência e a gravidade desses riscos sejam diferentes. Por exemplo, os riscos de segurança de dados geralmente são uma preocupação significativa quanto aos dispositivos de TI convencionais, porém, para alguns dispositivos IoT, pode não haver riscos de segurança de dados, já que eles não têm nenhum dado que precise de proteção.

Esta seção define três considerações de risco de privacidade e segurança cibernética que podem afetar o gerenciamento de riscos de segurança cibernética e privacidade para dispositivos IoT. As organizações devem garantir que estão abordando essas considerações de risco durante todo o ciclo de vida dos seus dispositivos IoT. A Seção 4 fornece mais informações sobre como essas considerações de risco podem afetar a mitigação de risco e a Seção 5 fornece recomendações para as organizações sobre como lidar com os desafios de mitigação de risco.

### 3.1 Consideração 1: Interações do dispositivo com o mundo físico

**Muitos dispositivos IoT interagem com o mundo físico de maneira diferente dos dispositivos convencionais de TI.**

As interações com o mundo físico que os dispositivos IoT habilitam podem afetar a segurança cibernética e os riscos à privacidade de várias maneiras. Aqui estão alguns exemplos:

- Os dados do sensor IoT, que representam medições do mundo físico, sempre apresentam incertezas associadas a eles. O gerenciamento eficaz dos dados do sensor IoT, incluindo a compreensão das incertezas, é necessário para avaliar a qualidade e o significado dos dados para que a organização possa tomar decisões sobre o uso dos dados e evitar a introdução de novos riscos. Sem essa abordagem, os índices de erro podem ser desconhecidos nos diferentes contextos em que um dispositivo IoT é usado.<sup>1</sup> O gerenciamento eficaz dos dados do sensor IoT é importante ao mitigar ataques físicos à tecnologia do sensor, como ataques realizados por meio de sinais sem fio, que podem fazer com que os sensores produzam resultados falsos.
- A ubiquidade dos sensores IoT em ambientes públicos e privados pode contribuir para a agregação e análise de um grande volume de dados sobre indivíduos. Essas atividades podem ser usadas para influenciar o comportamento dos indivíduos ou a tomada de decisão de uma maneira que eles não compreendem, ou levar à revelação de informações que os indivíduos não desejam que sejam reveladas, incluindo a reidentificação de PII previamente desidentificados - o que pode estar além do escopo originalmente intencionado para a operação do dispositivo IoT.
- Os dispositivos IoT com atuadores têm a capacidade de fazer alterações nos sistemas físicos, consequentemente afetando o mundo físico. O impacto potencial disso precisa ser explicitamente reconhecido e abordado no tocante à segurança cibernética e privacidade. Na pior das hipóteses, uma autorização pode permitir que um invasor use um dispositivo IoT para colocar em risco a segurança humana, danificar ou destruir equipamentos e instalações, ou causar grandes interrupções operacionais. Assim, podem surgir preocupações relativas à privacidade e liberdades civis a ela relacionadas devido às alterações autorizadas nos sistemas físicos que podem impactar a autonomia física dos indivíduos ou o comportamento em espaços pessoais e públicos. Por exemplo, controles de acesso físico, como fechaduras de portas automatizadas, podem ser usados para limitar o acesso a salas ou edifícios ocupados por indivíduos, como também, controles ambientais, como iluminação ou temperatura, podem ser usados para influenciar o movimento dos indivíduos nos edifícios.
- As interfaces de rede IoT geralmente permitem o acesso remoto a sistemas físicos que antes só podiam ser acessados localmente. Fabricantes, fornecedores e outros terceiros podem usar o acesso remoto a dispositivos IoT para fins de gerenciamento, monitoramento, manutenção e solução de problemas. Isso pode colocar os sistemas físicos acessíveis por meio dos dispositivos IoT em um risco de comprometimento muito maior. Além disso, essas funções de processamento de dados descentralizadas podem exacerbar alguns riscos de privacidade, tornando mais difícil para os indivíduos entenderem como o sistema IoT está operando, para que possam tomar decisões informadas sobre o processamento de suas informações e interações com o sistema IoT.

Outro aspecto importante das interações do dispositivo IoT com o mundo físico são os requisitos operacionais que os dispositivos devem atender em vários ambientes e casos de uso. Muitos dispositivos IoT devem cumprir requisitos rigorosos de desempenho, confiabilidade, resiliência, segurança e outros

---

<sup>1</sup> Para obter mais informações sobre a incerteza de medição, consulte <https://www.nist.gov/itl/sed/topic-areas/measurement-uncertainty>.



objetivos. Esses requisitos podem estar em desacordo com as práticas de privacidade e segurança cibernética comuns quando se trata de TI convencional. Por exemplo, práticas como patching automático são geralmente consideradas essenciais para TI convencional, mas essas práticas podem ter impactos negativos muito maiores em alguns dispositivos IoT com atuadores, o que pode fazer com que serviços críticos tornem-se indisponíveis e colocando em risco a segurança humana. Uma organização pode tomar uma decisão sensata de que os patches devem ser instalados na data e horário escolhidos pela organização junto com os funcionários no local, estando pronta para reagir imediatamente se ocorrer um problema. Uma organização também pode decidir evitar a correção de certos dispositivos IoT em circunstâncias normais e, em vez disso, restringir o acesso lógico e físico a eles para evitar a exploração de vulnerabilidades não corrigidas.

Outra maneira de abordarmos a questão é pensando em objetivos gerais de segurança cibernética: confidencialidade, integridade e disponibilidade. Para dispositivos convencionais de TI, a confidencialidade costuma receber mais atenção devido ao valor dos dados e das consequências de uma violação da confidencialidade. Para muitos dispositivos IoT, a disponibilidade e a integridade são mais importantes do que a confidencialidade, devido ao impacto potencial no mundo físico. Imagine um dispositivo IoT que é fundamental para evitar danos a uma instalação. Talvez um invasor possa visualizar os dados armazenados ou transmitidos do dispositivo IoT, mas provavelmente não obterá nenhuma vantagem ou valor com isso. Porém, um invasor que possa alterar os dados, tem a capacidade de desencadear uma série de eventos que causam um incidente.

### **3.2 Consideração 2: Recursos de acesso, gerenciamento e monitoramento de dispositivos**

#### **Muitos dispositivos IoT não podem ser acessados, gerenciados ou monitorados da mesma forma que os dispositivos convencionais de TI.**

Os dispositivos convencionais de TI geralmente conferem às pessoas, processos e dispositivos autorizados os recursos de acesso, gerenciamento e monitoramento de hardware e software. Em outras palavras, um administrador, processo ou dispositivo autorizado pode acessar diretamente o firmware, sistema operacional e aplicativos de um dispositivo de TI convencional, gerenciar totalmente o dispositivo e seu software durante todo o ciclo de vida do dispositivo conforme necessário, além de monitorar as características internas e o estado do dispositivo em todos os momentos. Os usuários autorizados também podem acessar um subconjunto restrito de recursos de acesso, gerenciamento e monitoramento.

Ao contrário disso, muitos dispositivos IoT são opacos, muitas vezes chamados de "caixas pretas". Eles fornecem pouca ou nenhuma visibilidade sobre o estado e a composição em que se encontram, incluindo a identidade de quaisquer serviços e sistemas externos com os quais interagem, e pouco ou nenhum acesso e gerenciamento do seu software e configuração. A organização pode não estar ciente dos recursos que um dispositivo IoT pode fornecer ou está fornecendo atualmente. Em casos extremos, pode ser difícil determinar se um produto caixa preta é realmente um dispositivo IoT devido à falta de transparência.

Pessoas, processos e dispositivos autorizados podem se deparar com um ou mais dos seguintes desafios ao acesso, gerenciamento e monitoramento de dispositivos IoT que afetam a segurança cibernética e o risco de privacidade:

- **Falta de recursos de gerenciamento.** Os administradores talvez não consigam gerenciar totalmente o firmware, sistema operacional e aplicativos de um dispositivo IoT durante todo o seu

ciclo de vida. Os recursos indisponíveis podem incluir a capacidade de adquirir, verificar a integridade, instalar, configurar, armazenar, recuperar, executar, encerrar, remover, substituir, atualizar e corrigir o software. Além disso, o software de um dispositivo IoT pode ser reconfigurado automaticamente quando ocorre um evento adverso, como uma queda de energia ou perda de conectividade de rede.

- **Falta de interfaces.** Alguns dispositivos IoT carecem de aplicativos e/ou interfaces de usuário humanas para uso e gerenciamento de dispositivos. Quando tais interfaces existem, elas talvez não possam fornecer a funcionalidade normalmente oferecida pelos dispositivos convencionais de TI. Um exemplo disso é o desafio de notificar os usuários sobre o processamento de PII por um dispositivo IoT para que eles possam fornecer consentimento significativo para tal processamento. Um problema adicional é a falta de padrões universalmente aceitos para interfaces de aplicativos IoT, incluindo para expressar e formatar dados, emitir comandos e alguma forma de promover a interoperabilidade entre dispositivos IoT.
- **Dificuldades de gerenciamento em escala.** A maioria dos dispositivos IoT não oferece suporte a mecanismos padronizados para gerenciamento centralizado, sendo que o grande número de dispositivos IoT a serem gerenciados pode ser esmagador.
- **Grande variedade de softwares a serem gerenciados.** Há uma grande variedade de softwares usados por dispositivos IoT, incluindo firmware, sistemas operacionais padrão e em tempo real, e aplicativos. Isso complica significativamente o gerenciamento de software em todo o ciclo de vida do dispositivo IoT, afetando áreas como configuração e gerenciamento de patch.
- **Diferentes perspectivas para a expectativa de vida.** Um fabricante pode decidir que um determinado dispositivo IoT seja usado por apenas alguns anos e depois descartado. Uma organização que compra esse dispositivo pode querer usá-lo por mais tempo, mas o fabricante pode parar de oferecer suporte ao dispositivo (ex.: liberar patches para vulnerabilidades conhecidas) por opção própria ou devido a limitações da cadeia de suprimento (ex.: o fornecedor não mais irá liberar patches para um componente de dispositivo IoT específico). O problema de diferentes expectativas de vida útil não é novidade nem é específico da IoT, mas pode ser particularmente importante para alguns dispositivos IoT devido a segurança, confiabilidade e outros riscos potencialmente envolvidos no uso de dispositivos após a vida útil pretendida.
- **Hardware sem manutenção.** O hardware do dispositivo IoT pode não receber manutenção, o que significa que não pode ser reparado, customizado ou inspecionado internamente.
- **Falta de recursos de estoque.** Os dispositivos IoT utilizados em uma organização não podem ser inventariados, registrados, ou sequer provisionados por meio dos processos normais de TI. Isso acontece especialmente em se tratando de tipos de dispositivos que não tinham recursos de rede anteriormente.
- **Propriedade heterogênea.** Muitas vezes, verificamos propriedade heterogênea nos dispositivos IoT. Por exemplo, um dispositivo IoT pode transferir dados para processamento e armazenamento de serviços baseados em nuvem fornecidos pelo fabricante. Os dados também podem ser enviados a um serviço de nuvem para agregar dados de vários dispositivos IoT em um único local. Esses serviços em nuvem podem ter acesso a partes ou a todos os dados dos dispositivos, ou até mesmo acesso e controle dos próprios dispositivos para fins de monitoramento, manutenção e solução de problemas. Em alguns casos, apenas os fabricantes têm autoridade para fazer a manutenção; uma organização que tenta instalar patches ou fazer outras tarefas de manutenção em um dispositivo IoT pode anular a garantia. Além disso, pode haver pouca ou nenhuma informação disponível na IoT sobre a propriedade do dispositivo, especialmente em dispositivos IoT caixa preta. Isso poderia exacerbar as dificuldades existentes de reparação de privacidade, já que a falta de responsabilização limita a capacidade de \os indivíduos localizarem a fonte e corrigir ou excluir informações sobre si mesmos ou de resolver outros problemas. Outra preocupação com a propriedade heterogênea é o efeito no reprovisionamento do dispositivo -

quais são os dados que ainda podem estar disponíveis após a transferência do controle de um dispositivo.

### 3.3 Consideração 3: Disponibilidade, eficiência e eficácia da capacidade de segurança cibernética e de privacidade

**A disponibilidade, eficiência e eficácia dos recursos de segurança cibernética e de privacidade são muitas vezes diferentes para dispositivos IoT comparado a dispositivos convencionais de TI.**

Para os fins desta publicação, os recursos integrados de privacidade e segurança cibernética são chamados de *recursos pré-mercado*. Os recursos pré-mercado são integrados aos dispositivos IoT pelo fabricante ou fornecedor antes de serem enviados às organizações do cliente. *Recursos pós-mercado* são aqueles que as organizações selecionam, adquirem e implantam, além dos recursos pré-mercado. Os recursos de segurança cibernética e privacidade pré e pós-mercado podem ser bastante diferentes para dispositivos IoT comparado a dispositivos convencionais de TI. As principais razões para tal:

- Muitos dispositivos IoT não oferecem ou não podem oferecer suporte à vasta gama de recursos de segurança cibernética e privacidade normalmente integrados aos dispositivos de TI convencionais. Por exemplo, uma “caixa preta” do dispositivo IoT pode não registrar seus eventos de segurança cibernética e privacidade ou pode não permitir que as organizações acessem seus registros. Se os recursos pré-mercado estiverem disponíveis para dispositivos IoT, talvez sejam inadequados em termos de força ou desempenho - por exemplo, usar criptografia forte e autenticação mútua para proteger as comunicações pode causar atrasos inaceitáveis.<sup>2</sup> Os recursos pós-mercado não podem ser instalados em muitos dispositivos IoT. Além disso, os recursos de pré-mercado e pós-mercado existentes podem não conseguir operar em escala para atender às necessidades de IoT - por exemplo, um dispositivo de segurança cibernética baseado em rede existente para dispositivos convencionais de TI pode não conseguir processar também o volume de tráfego de rede e dados gerados de um grande número de dispositivos IoT.
- O nível de esforço necessário para gerenciar, monitorar e manter os recursos de pré-mercado em cada dispositivo IoT pode ser excessivo. Especialmente quando os dispositivos IoT não suportam gerenciamento centralizado, talvez seja mais eficiente implementar e usar recursos pós-mercado centralizados que ajudam a proteger vários dispositivos IoT em vez de tentar alcançar o nível equivalente de proteção em cada dispositivo IoT individual. Um exemplo é ter um único gateway IoT baseado em rede ou gateway de segurança IoT protegendo muitos dispositivos IoT em vez de ter que projetar, gerenciar e manter um conjunto exclusivo de recursos de proteção dentro de cada dispositivo IoT.
- Alguns recursos pós-mercado para TI convencional, como sistemas de prevenção de intrusão baseados em rede, servidores anti-malware e firewalls, podem não ser tão eficazes na proteção de dispositivos IoT quanto são na proteção de TI convencional. Os dispositivos IoT geralmente usam protocolos que os controles de segurança cibernética e de privacidade para TI convencional não conseguem entender e analisar. Além disso, os dispositivos IoT podem manter comunicação direta uns com os outros, por exemplo, através de comunicação sem fio ponto a ponto, em vez de usar uma rede de infraestrutura monitorada.

Um dispositivo IoT pode não precisar de alguns recursos de segurança cibernética e privacidade dos quais os dispositivos de TI convencionais dependem - um exemplo disso é um dispositivo IoT sem recursos de armazenamento de dados, sem necessidade de proteger os dados em repouso. Um dispositivo IoT também

---

<sup>2</sup> Para obter mais informações sobre dispositivos de computação de poucos recursos, consulte Solicitação de Comentários (RFC) 7228 da Internet Engineering Task Force (IETF) (Força-Tarefa de Engenharia da Internet), "Terminology for Constrained-Node Networks" ("Terminologia para redes de nós restritos"), maio de 2014 (<https://doi.org/10.17487/RFC7228>).

pode precisar de recursos adicionais que a maioria dos dispositivos de TI convencionais não utiliza, especialmente se o dispositivo IoT permitir novas interações com o mundo físico.

## 4 Desafios de segurança cibernética e mitigação de risco de privacidade para dispositivos IoT

Os riscos de segurança cibernética e privacidade para dispositivos IoT podem ser considerados em termos de três *objetivos de mitigação de risco de alto nível*, conforme demonstrado na Figura 4:

1. **Proteger a segurança do dispositivo.** Em outras palavras, evitar que um dispositivo seja usado para realizar ataques, incluindo a participação em ataque distribuído de negação de serviço (DDoS) contra outras organizações, e a espionagem no tráfego de rede, ou comprometer outros dispositivos no mesmo segmento de rede. Esse objetivo se aplica a todos os dispositivos IoT.
2. **Proteger a segurança de dados.** Proteger a confidencialidade, integridade e/ou disponibilidade de dados (incluindo PII) coletados, armazenados, processados ou transmitidos para ou pelo dispositivo IoT. Esse objetivo se aplica a cada dispositivo IoT, exceto aqueles que não contêm dados que precisam de proteção.
3. **Proteger a privacidade dos indivíduos.** Proteger a privacidade das pessoas afetadas pelo processamento de PII, além dos riscos gerenciados por meio de dispositivos e proteção de segurança de dados. Este objetivo se aplica a todos os dispositivos IoT que processam PII ou que afetam indivíduos direta ou indiretamente.

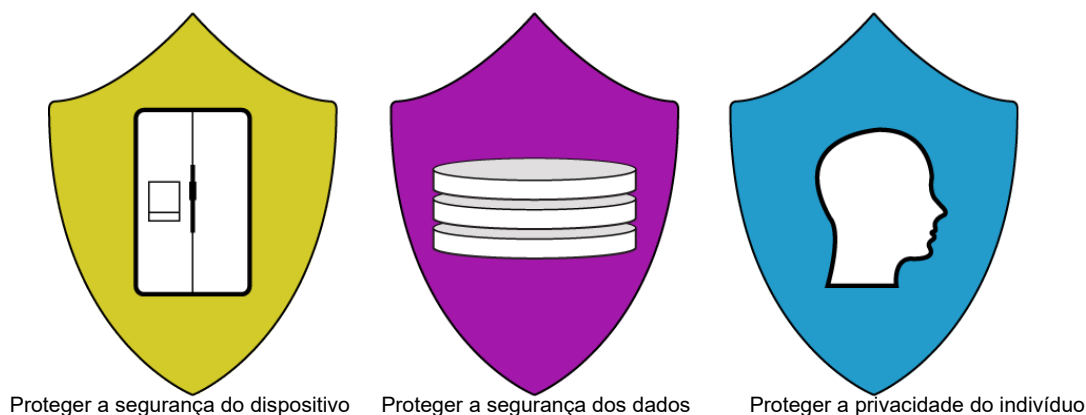


Figura 4: Objetivos de mitigação de risco

Cada objetivo se baseia no objetivo anterior e não o substitui ou nega que seja necessário. O cumprimento de cada um dos objetivos de mitigação de risco envolve a abordagem de um conjunto de áreas de *mitigação de risco*, que são definidas abaixo. Cada área de mitigação de risco define um aspecto da mitigação de risco de segurança cibernética ou privacidade considerado mais significativo ou inesperadamente afetado pela IoT de acordo com as considerações de risco definidas na Seção 3.

Áreas de mitigação de risco para o objetivo 1- Proteger a Segurança do Dispositivo:

- **Gerenciamento de ativos:** Manter um inventário atual e preciso de todos os dispositivos IoT e suas características relevantes ao longo dos ciclos de vida dos dispositivos, com o intuito de usar tais informações para fins de gestão de risco de privacidade e segurança cibernética.
- **Gerenciamento de vulnerabilidades:** Identificar e eliminar vulnerabilidades conhecidas no software e firmware do dispositivo IoT para reduzir a probabilidade e facilidade de exploração e comprometimento.
- **Gerenciamento de acesso:** Impedir o acesso não autorizado e impróprio, seja físico ou lógico, ao uso e administração de dispositivos IoT por pessoas, processos e outros dispositivos de computação.

- **Detecção de incidente de segurança do dispositivo:** Monitorar e analisar a atividade do dispositivo IoT quanto aos sinais de incidentes envolvendo a segurança do dispositivo.

Áreas de mitigação de risco para o objetivo 2 - Proteger a Segurança de Dados:

- **Proteção de dados:** Prevenir o acesso e a violação de dados em repouso ou em trânsito que possam expor informações confidenciais ou permitir a manipulação ou interrupção das operações do dispositivo IoT.
- **Detecção de incidente de segurança de dados:** Monitorar e analisar a atividade do dispositivo IoT quanto aos sinais de incidentes envolvendo segurança de dados.

Áreas de mitigação de risco para o objetivo 3 - Proteger a Privacidade dos Indivíduos:

- **Gerenciamento do fluxo de informação:** Manter um mapeamento atual e preciso do ciclo de vida das informações de PII, incluindo o tipo de ação de dados, os elementos de PII sendo processados pela ação de dados, a parte que faz o processamento e qualquer outro fator contextual relevante sobre o processamento a ser usado para o propósito de privacidade de gestão de risco.
- **Gerenciamento de permissões de processamento de PII:** Manter as permissões de processamento de PII para evitar processamentos não permitidos.
- **Tomada de decisão informada:** Permitir que os indivíduos entendam os efeitos do processamento de PII e das interações com o dispositivo, participem da tomada de decisões sobre o processamento ou interações de PII para que possam solucionar problemas.
- **Gerenciamento de dados desassociados:** Identificar o processamento de PIIs autorizados e determinar como as PIIs podem ser minimizadas ou desassociadas de indivíduos e dispositivos IoT.
- **Detecção de violação de privacidade:** Monitorar e analisar as atividades do dispositivo IoT quanto aos sinais de violações envolvendo a privacidade dos indivíduos.

As Seções 4.1, 4.2, e 4.3 examinam como as considerações de risco apresentam desafios para os gestores de risco de privacidade e segurança cibernética com o cumprimento de cada uma das três metas de mitigação de risco para os dispositivos IoT de uma organização — em outras palavras, como a mitigação pode ser diferente para IoT versus TI convencional. A seção 5 fornece recomendações sobre como as organizações devem enfrentar esses desafios.

#### 4.1 Desafios potenciais para alcançar o objetivo 1 - Proteger a Segurança do Dispositivo

Figura 5: mostra as relações entre os conceitos da Seção 3 e da Seção 4. A Seção 3 define as três considerações de risco, que explicam por que e como os dispositivos IoT afetam o gerenciamento de risco relacionado à segurança cibernética e privacidade. Em seguida, a introdução da Seção 4 define as metas e áreas de mitigação de risco, que especificam quais tipos de riscos de segurança cibernética e privacidade são importantes para dispositivos IoT e que podem ser mais afetados pelas considerações de risco. O restante da Seção 4 lista as expectativas, isto é, como as organizações esperam que os dispositivos de TI convencionais ajudem a mitigar os riscos de segurança cibernética e privacidade referentes aos objetivos e áreas de mitigação de risco, e os desafios que os dispositivos IoT podem representar mediante tais expectativas, além das implicações que esses desafios apresentam. O resultado final dessas lincagens é a identificação de um conjunto estruturado de desafios potenciais para mitigar os riscos de segurança cibernética e privacidade para dispositivos IoT, que podem ser rastreados desde o início para se verificar as considerações de risco relevantes.



**Figura 5: Relações entre os conceitos da Seção 3 e da Seção 4**

Muitos leitores talvez não precisem usar as informações em todos os níveis de detalhes descritos na Figura 5, e alguns leitores podem precisar apenas das informações em um único nível, como a lista de desafios. Este documento inclui todos os níveis para explicar a base para a identificação de desafios específicos como sendo potencialmente significativos para os dispositivos IoT. Além disso, alguns leitores podem usar todos os níveis para prestar informações sobre o trabalho que estão fazendo na área de gerenciamento de risco.

Tabela 1 - lista as expectativas comuns para os recursos de pré-mercado para dispositivos de TI convencionais que são frequentemente usados para ajudar a mitigar o risco de segurança do dispositivo. Embora essas expectativas nem sempre sejam verdadeiras para dispositivos de TI convencionais, elas são verdadeiras na maioria das vezes, e influenciam as práticas comuns de segurança de dispositivos no que se refere aos dispositivos de TI convencionais. Para cada expectativa, a Tabela 1 define um ou mais desafios potenciais que os dispositivos IoT individuais podem representar para certa expectativa. Cada desafio tem sua própria fileira na tabela:

- Primeira coluna: contém uma breve declaração do desafio, sendo que todos possuem um número exclusivo para facilitar a referência e contêm também os números das considerações de risco da Seção 3 que causam o desafio
- Segunda coluna: contém exemplos de controles preliminares do NIST SP 800-53 Revisão 5 [7] que podem ser potencialmente afetados negativamente para alguns dispositivos IoT individuais
- Terceira coluna: contém possíveis implicações para a organização se um número substancial de dispositivos IoT for afetado pelo desafio



- Quarta coluna: contém exemplos de Subcategorias de Estrutura de Segurança Cibernética [6] que podem ser potencialmente afetadas negativamente pelas implicações

As tabelas nesta seção não definem ou implicam equivalência entre os controles do NIST SP 800-53 e as subcategorias da Estrutura de Segurança Cibernética em cada fileira. Por exemplo, em muitos casos, um desafio afeta um aspecto dos controles do SP 800-53 e um aspecto diferente das subcategorias da estrutura de segurança cibernética. Além disso, os dispositivos IoT que não atendem às expectativas tradicionais podem ser um fator positivo para a mitigação de risco, uma vez que essas limitações podem representar *menos* risco do que quando a capacidade ou função mais robusta está presente conforme a expectativa. A tabela não define essas considerações, mas visa ajudar os gerentes de segurança cibernética e de risco de privacidade a entenderem como os dispositivos IoT podem ou não se encaixar em suas atuais mitigações e/ou impactar como os resultados de privacidade e segurança cibernética são alcançados atualmente em suas organizações .

**Tabela 1: Desafios potenciais para alcançar o objetivo 1 - Proteger a Segurança do Dispositivo**

<b>Desafios para dispositivos IoT individuais e considerações de risco que causam os desafios</b>	<b>Controles preliminares afetados NIST SP 800-53 Revisão 5</b>	<b>Implicações para a organização</b>	<b>Subcategorias de estrutura de segurança cibernética afetadas</b>
<b>Gestão de ativos</b>			
Expectation 1: O dispositivo possui um identificador exclusivo integrado.			
1. O dispositivo IoT talvez não tenha um identificador exclusivo que o sistema de gerenciamento de ativos da organização possa acessar ou entender.  Consideração de risco 2	<ul style="list-style-type: none"> <li>• CM-8, Inventário de componentes do sistema</li> </ul>	<ul style="list-style-type: none"> <li>• Pode complicar o gerenciamento de dispositivos, incluindo acesso remoto e gerenciamento de vulnerabilidades.</li> </ul>	<ul style="list-style-type: none"> <li>• ID.AM-1: Dispositivos físicos e sistemas dentro da organização são inventariados</li> </ul>
Expectation 2: O dispositivo pode fazer interface com sistemas de gerenciamento de ativos corporativos.			
2. O dispositivo IoT talvez não possa participar de um sistema de gerenciamento de ativos centralizado.  Consideração de risco 2	<ul style="list-style-type: none"> <li>• CM-8, Inventário de componentes do sistema</li> </ul>	<ul style="list-style-type: none"> <li>• Talvez tenha que usar vários sistemas de gerenciamento de ativos.</li> <li>• Talvez tenha que executar tarefas de gerenciamento de ativos manualmente.</li> </ul>	<ul style="list-style-type: none"> <li>• ID.AM-1: Dispositivos físicos e sistemas dentro da organização são inventariados</li> <li>• ID.AM-2: Plataformas de software e aplicativos dentro da organização são inventariados</li> <li>• PR.DS-3: Os ativos são gerenciados formalmente durante a remoção, transferência e disposição</li> </ul>
3. O dispositivo IoT não pode ser conectado diretamente a nenhuma rede da organização.  Consideração de risco 2	<ul style="list-style-type: none"> <li>• CM-8, Inventário de componentes do sistema</li> </ul>	<ul style="list-style-type: none"> <li>• Talvez tenha que usar um sistema ou serviço de gerenciamento de ativos separado, ou processos manuais de gerenciamento de ativos para dispositivos IoT externos.</li> </ul>	<ul style="list-style-type: none"> <li>• ID.AM-1: Dispositivos físicos e sistemas dentro da organização são inventariados</li> <li>• ID.AM-2: Plataformas de software e aplicativos dentro da organização são inventariados</li> <li>• PR.DS-3: Os ativos são gerenciados formalmente durante a remoção, transferência e disposição</li> </ul>



Desafios para dispositivos IoT individuais e considerações de risco que causam os desafios	Controles preliminares afetados NIST SP 800-53 Revisão 5	Implicações para a organização	Subcategorias de estrutura de segurança cibernética afetadas
Expectation 3: O dispositivo pode fornecer à organização visibilidade suficiente das suas características.			
4. O dispositivo IoT pode ser uma caixa preta que fornece pouca ou nenhuma informação sobre seu hardware, software e firmware.  Consideração de risco 2	<ul style="list-style-type: none"> <li>CM-8, Inventário de componentes do sistema</li> </ul>	<ul style="list-style-type: none"> <li>Pode complicar todos os aspectos do gerenciamento de dispositivos e gestão de riscos.</li> </ul>	<ul style="list-style-type: none"> <li>ID.AM-1: Dispositivos físicos e sistemas dentro da organização são inventariados</li> <li>ID.AM-2: Plataformas de software e aplicativos dentro da organização são inventariados</li> <li>ID.AM-4: Sistemas de informação externos são catalogados</li> </ul>
Expectation 4: O dispositivo ou o fabricante do dispositivo pode informar a organização sobre todos os softwares e serviços externos que o dispositivo usa, como software em execução ou baixado dinamicamente da nuvem.			
5. Nem todas as dependências externas do dispositivo IoT podem ser reveladas.  Consideração de risco 2	<ul style="list-style-type: none"> <li>AC-20, Uso de sistemas externos</li> </ul>	<ul style="list-style-type: none"> <li>Não é possível gerenciar riscos para software e serviços externos.</li> </ul>	<ul style="list-style-type: none"> <li>DE.CM-8: São realizados escaneamentos de vulnerabilidades</li> <li>PR.IP-1: Uma configuração de linha de base de sistemas de tecnologia da informação/controlado industrial é criada e mantida incorporando princípios de segurança (ex.: conceito de menor funcionalidade)</li> <li>PR.PT-3: O princípio de menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais</li> </ul>
<b>Gerenciamento de vulnerabilidades</b>			
Expectation 5: O fabricante fornecerá patches ou atualizações para todo o software e firmware durante a vida útil de cada dispositivo.			
6. O fabricante não pode lançar patches ou atualizações para o dispositivo IoT.  Considerações de risco 3	<ul style="list-style-type: none"> <li>SI-2, Correção de falhas</li> </ul>	<ul style="list-style-type: none"> <li>Não é possível remover vulnerabilidades conhecidas.</li> </ul>	<ul style="list-style-type: none"> <li>PR.IP-1: Uma configuração de linha de base de sistemas de tecnologia da informação/controlado industrial é criada e mantida incorporando princípios de segurança (ex.: conceito de menor funcionalidade)</li> </ul>
7. O fabricante pode parar de lançar patches e atualizações para o dispositivo IoT enquanto ele ainda está em uso.  Considerações de risco 3	<ul style="list-style-type: none"> <li>SI-2, Correção de falhas</li> </ul>	<ul style="list-style-type: none"> <li>Talvez não seja possível remover vulnerabilidades conhecidas no futuro.</li> </ul>	<ul style="list-style-type: none"> <li>PR.IP-1: Uma configuração de linha de base de sistemas de tecnologia da informação/controlado industrial é criada e mantida incorporando princípios de segurança (ex.: conceito de menor funcionalidade)</li> </ul>

Desafios para dispositivos IoT individuais e considerações de risco que causam os desafios	Controles preliminares afetados NIST SP 800-53 Revisão 5	Implicações para a organização	Subcategorias de estrutura de segurança cibernética afetadas
Expectation 6: O dispositivo tem seu próprio patch seguro integrado, atualização e recursos de gerenciamento de configuração ou pode fazer interface com sistemas de gerenciamento de vulnerabilidade empresarial com tais recursos.			
8. O dispositivo IoT pode não ter a capacidade de ter um patch para corrigir ou atualizar o software.  Considerações de risco 2 e 3	<ul style="list-style-type: none"> <li>SI-2, Correção de falhas</li> </ul>	<ul style="list-style-type: none"> <li>Não é possível remover vulnerabilidades conhecidas.</li> </ul>	<ul style="list-style-type: none"> <li>PR.IP-1: Uma configuração de linha de base de sistemas de tecnologia da informação/controle industrial é criada e mantida incorporando princípios de segurança (ex.: conceito de menor funcionalidade)</li> </ul>
9. Pode ser muito arriscado instalar patches ou atualizações ou fazer alterações na configuração sem testes prolongados e preparação preliminar, sendo que implementar alterações pode exigir interrupções operacionais ou causar interrupções inadvertidamente.  Considerações de risco 1	<ul style="list-style-type: none"> <li>CM-3, Controle de mudança de configuração</li> <li>CM-6, Definições de configuração</li> <li>SI-2, Correção de falhas</li> </ul>	<ul style="list-style-type: none"> <li>Pode haver atrasos significativos na remoção de vulnerabilidades conhecidas.</li> </ul>	<ul style="list-style-type: none"> <li>PR.IP-1: Uma configuração de linha de base de sistemas de tecnologia da informação/controle industrial é criada e mantida incorporando princípios de segurança (ex.: conceito de menor funcionalidade)</li> </ul>
10. O dispositivo IoT talvez não possa participar de um sistema de gerenciamento de vulnerabilidades centralizado.  Considerações de risco 2	<ul style="list-style-type: none"> <li>CM-3, Controle de mudança de configuração</li> <li>SI-2, Correção de falhas</li> </ul>	<ul style="list-style-type: none"> <li>Pode ter que usar vários sistemas de gerenciamento de vulnerabilidades, e não apenas um.</li> <li>Pode ser necessário executar tarefas de gerenciamento de vulnerabilidades manualmente e periodicamente (ex.: instalar patches e verificar se há erros de configuração de software manualmente).</li> </ul>	<ul style="list-style-type: none"> <li>PR.IP-1: Uma configuração de linha de base de sistemas de tecnologia da informação/controle industrial é criada e mantida incorporando princípios de segurança (ex.: conceito de menor funcionalidade)</li> </ul>
11. O dispositivo IoT pode não oferecer a capacidade de alterar a configuração do software ou pode não oferecer os recursos que as organizações desejam.  Considerações de risco 2	<ul style="list-style-type: none"> <li>CM-2, Configuração de linha de base</li> <li>CM-3, Controle de mudança de configuração</li> <li>CM-6, Definições de configuração</li> <li>CM-7, Menor funcionalidade</li> <li>SC-42, Capacidade do sensor e dados</li> </ul>	<ul style="list-style-type: none"> <li>Não é possível remover vulnerabilidades conhecidas.</li> <li>Não é possível atingir o princípio de menor funcionalidade desativando serviços e funções desnecessários.</li> <li>Não é possível restringir a ativação e uso do sensor.</li> </ul>	<ul style="list-style-type: none"> <li>PR.IP-1: Uma configuração de linha de base de sistemas de tecnologia da informação/controle industrial é criada e mantida incorporando princípios de segurança (ex.: conceito de menor funcionalidade)</li> <li>PR.IP-3: Os processos de controle de mudança de configuração estão em vigor</li> <li>PR.PT-3: O princípio de menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais</li> </ul>

Desafios para dispositivos IoT individuais e considerações de risco que causam os desafios	Controles preliminares afetados NIST SP 800-53 Revisão 5	Implicações para a organização	Subcategorias de estrutura de segurança cibernética afetadas
Expectation 7: O dispositivo suporta o uso de scanners de vulnerabilidade ou então fornece identificação de vulnerabilidade integrada e recursos de relatório.			
12. Pode não haver um scanner de vulnerabilidade que possa ser executado no dispositivo IoT ou através dele.  Considerações de risco 3	<ul style="list-style-type: none"> <li>RA-5, Escaneamento de vulnerabilidades</li> </ul>	<ul style="list-style-type: none"> <li>Não é possível identificar vulnerabilidades conhecidas automaticamente.</li> </ul>	<ul style="list-style-type: none"> <li>DE.CM-8: Escaneamentos de vulnerabilidades são executados</li> </ul>
13. O dispositivo IoT talvez não ofereça recursos integrados para identificar e relatar vulnerabilidades conhecidas.  Considerações de risco 3	<ul style="list-style-type: none"> <li>RA-5, Scaneamento de vulnerabilidades</li> </ul>	<ul style="list-style-type: none"> <li>Não é possível identificar vulnerabilidades conhecidas automaticamente.</li> </ul>	<ul style="list-style-type: none"> <li>DE.CM-8: Escaneamentos de vulnerabilidades são executados</li> </ul>
<b>Gerenciamento de Acesso</b>			
Expectation 8: O dispositivo pode identificar exclusivamente cada usuário, dispositivo e processo que tenta acessá-lo logicamente.			
14. O dispositivo IoT pode não suportar o uso de identificadores.  Considerações de risco 2 e 3	<ul style="list-style-type: none"> <li>IA-2, Identificação e autenticação (usuários organizacionais)</li> <li>IA-3, Identificação e autenticação de dispositivo</li> <li>IA-4, Gerenciamento de identificador</li> <li>IA-8, Identificação e autenticação (usuários não-organizacionais)</li> <li>IA-9, Identificação e autenticação de serviço</li> </ul>	<ul style="list-style-type: none"> <li>Não pode identificar ou autenticar usuários, dispositivos e processos.</li> </ul>	<ul style="list-style-type: none"> <li>PR.AC-1: Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados</li> <li>PR.AC-7: Usuários, dispositivos e outros ativos são autenticados (ex.: fator único, multifator) de acordo com o risco da transação (ex.: riscos de segurança e privacidade dos indivíduos e outros riscos organizacionais)</li> </ul>
15. O dispositivo IoT pode suportar apenas o uso de um ou mais identificadores compartilhados.  Considerações de risco 2 e 3	<ul style="list-style-type: none"> <li>IA-2, Identificação e autenticação (usuários organizacionais)</li> <li>IA-3, Identificação e autenticação de dispositivo</li> <li>IA-4, Gerenciamento de identificador</li> <li>IA-8, Identificação e autenticação (usuários não-organizacionais)</li> <li>IA-9, Identificação e autenticação de serviço</li> </ul>	<ul style="list-style-type: none"> <li>Não pode identificar usuários, dispositivos e processos com exclusividade. Complica o gerenciamento de credenciais devido às credenciais compartilhadas.</li> </ul>	<ul style="list-style-type: none"> <li>PR.AC-1: Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados</li> </ul>

Desafios para dispositivos IoT individuais e considerações de risco que causam os desafios	Controles preliminares afetados NIST SP 800-53 Revisão 5	Implicações para a organização	Subcategorias de estrutura de segurança cibernética afetadas
<p>16. O dispositivo IoT pode exigir o uso de identificadores, mas apenas em certos casos (ex.: para acesso remoto, mas não para acesso local, ou para fins de administração, mas não para uso regular).</p> <p>Considerações de risco 2 e 3</p>	<ul style="list-style-type: none"> <li>IA-2, Identificação e autenticação (usuários organizacionais)</li> <li>IA-3, Identificação e autenticação de dispositivo</li> <li>IA-4, Gerenciamento de identificador</li> <li>IA-8, Identificação e autenticação (usuários não-organizacionais)</li> <li>IA-9, Identificação e autenticação de serviço</li> </ul>	<ul style="list-style-type: none"> <li>Não pode identificar ou autenticar alguns usuários, dispositivos e processos.</li> </ul>	<ul style="list-style-type: none"> <li>PR.AC-1: Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados</li> <li>PR.AC-7: Usuários, dispositivos e outros ativos são autenticados (ex.: fator único, fator múltiplo) de acordo com o risco da transação (ex.: riscos de segurança e privacidade dos indivíduos e outros riscos organizacionais)</li> </ul>
<p>Expectation 9: O dispositivo pode ocultar caracteres de senha, prevenindo que sejam exibidos quando uma pessoa insere uma senha para um dispositivo, usando um teclado ou tela sensível ao toque.</p>			
<p>17. O dispositivo IoT pode não oferecer suporte à ocultação de caracteres de senha exibidos.</p> <p>Considerações de risco 2 e 3</p>	<ul style="list-style-type: none"> <li>IA-6, Feedback do autenticador</li> </ul>	<ul style="list-style-type: none"> <li>Aumenta a probabilidade de roubo de credencial.</li> </ul>	<ul style="list-style-type: none"> <li>PR.AC-7: Usuários, dispositivos e outros ativos são autenticados (ex.: fator único, multifator) de acordo com o risco da transação (ex.: riscos de segurança e privacidade dos indivíduos e outros riscos organizacionais)</li> </ul>
<p>Expectation 10: O dispositivo pode autenticar cada usuário, dispositivo e processo que tenta acessá-lo logicamente.</p>			
<p>18. O dispositivo IoT pode não suportar o uso de credenciais não triviais (ex.: não suporta o uso de identificadores, não permite que as senhas padrão sejam alteradas).</p> <p>Considerações de risco 2 e 3</p>	<ul style="list-style-type: none"> <li>IA-5, Gerenciamento de autenticador</li> </ul>	<ul style="list-style-type: none"> <li>Não pode identificar ou autenticar usuários, dispositivos e processos, o que aumenta as chances de acesso não autorizado e adulteração.</li> </ul>	<ul style="list-style-type: none"> <li>PR.AC-7: Usuários, dispositivos e outros ativos são autenticados (ex.: fator único, multifator) de acordo com o risco da transação (ex.: riscos de segurança e privacidade dos indivíduos e outros riscos organizacionais)</li> </ul>
<p>19. O dispositivo IoT pode não suportar o uso de credenciais fortes, como tokens criptográficos ou autenticação multifator para as situações que exigem tais processos.</p> <p>Consideração de risco 3</p>	<ul style="list-style-type: none"> <li>IA-5, Gerenciamento de autenticador</li> </ul>	<ul style="list-style-type: none"> <li>Aumenta as chances de acesso não autorizado e adulteração pelo uso indevido de credenciais.</li> </ul>	<ul style="list-style-type: none"> <li>PR.AC-7: Usuários, dispositivos e outros ativos são autenticados (ex.: fator único, multifator) de acordo com o risco da transação (ex.: segurança e riscos de privacidade de indivíduos e outros riscos organizacionais)</li> </ul>

Desafios para dispositivos IoT individuais e considerações de risco que causam os desafios	Controles preliminares afetados NIST SP 800-53 Revisão 5	Implicações para a organização	Subcategorias de estrutura de segurança cibernética afetadas
Expectation 11: O dispositivo pode usar autenticadores empresariais e mecanismos de autenticação existentes.			
<p>20. O dispositivo IoT pode não suportar o uso de um sistema de autenticação de usuário empresarial existente.</p> <p>Consideração de risco 3</p>	<ul style="list-style-type: none"> <li>• IA-2, Identificação e autenticação (usuários organizacionais)</li> <li>• IA-5, Gerenciamento de autenticador</li> <li>• IA-8, Identificação e autenticação (usuários não-organizacionais)</li> </ul>	<ul style="list-style-type: none"> <li>• Precisa de uma ou mais contas e credenciais adicionais para cada usuário.</li> </ul>	<ul style="list-style-type: none"> <li>• PR.AC-1: Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados</li> <li>• PR.AC-7: Usuários, dispositivos e outros ativos são autenticados (ex.: fator único, multifator) de acordo com o risco da transação (ex.: segurança e riscos de privacidade de indivíduos e outros riscos organizacionais)</li> </ul>
Expectation 12: O dispositivo pode restringir cada usuário, dispositivo e processo aos privilégios mínimos de acesso lógico necessários.			
<p>21. O dispositivo IoT pode não suportar o uso de privilégios de acesso lógico dentro do dispositivo que seja suficiente para uma determinada situação.</p> <p>Considerações de risco 3</p>	<ul style="list-style-type: none"> <li>• AC-3, Controle de acesso</li> <li>• AC-5, Separação de deveres</li> <li>• AC-6, Privilégio mínimo</li> </ul>	<ul style="list-style-type: none"> <li>• Permite que usuários, dispositivos e processos autorizados usem intencionalmente ou inadvertidamente privilégios que não deveriam ter.</li> <li>• Permite que um invasor que obtém acesso não autorizado a uma conta tenha ainda maior acesso do que a conta deveria ter.</li> </ul>	<ul style="list-style-type: none"> <li>• PR.AC-4: As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de funções</li> <li>• PR.DS-5: Proteções contra vazamentos de dados são implementadas</li> <li>• PR.MA-1: A manutenção e o reparo dos ativos organizacionais são realizados e registrados, utilizando ferramentas aprovadas e controladas</li> </ul>
<p>22. O dispositivo IoT pode não suportar o uso de privilégios de acesso lógico para restringir as comunicações de rede dentro e fora do dispositivo que são suficientes para uma determinada situação.</p> <p>Considerações de risco 3</p>	<ul style="list-style-type: none"> <li>• AC-3, Aplicação do controle de acesso</li> <li>• AC-4, Aplicação do controle do fluxo de informação</li> <li>• AC-5, Separação de deveres</li> <li>• AC-6, Privilégio mínimo</li> <li>• AC-17, Acesso remoto</li> <li>• SC-7, Proteção de limites</li> </ul>	<ul style="list-style-type: none"> <li>• Permite que usuários, dispositivos e processos autorizados conduzam, intencionalmente ou inadvertidamente, comunicações de rede que não deveriam ter autoridade para fazer.</li> <li>• Permite que um invasor tenha mais acesso à rede do que o planejado.</li> </ul>	<ul style="list-style-type: none"> <li>• PR.AC-3: O acesso remoto é gerenciado</li> <li>• PR.AC-5: A integridade da rede é protegida (ex.: segregação de rede, segmentação de rede)</li> <li>• PR.DS-5: Proteções contra vazamentos de dados são implementadas</li> <li>• PR.MA-2: A manutenção remota dos ativos organizacionais é aprovada, registrada e realizada de maneira que evita o acesso não autorizado</li> </ul>

Desafios para dispositivos IoT individuais e considerações de risco que causam os desafios	Controles preliminares afetados NIST SP 800-53 Revisão 5	Implicações para a organização	Subcategorias de estrutura de segurança cibernética afetadas
Expectation 13: O dispositivo pode impedir tentativas de obter acesso não autorizado e esse recurso pode ser configurado ou desabilitado para evitar interrupções indesejadas na disponibilidade. (Os exemplos incluem bloquear ou desativar uma conta quando há muitas tentativas consecutivas de autenticação com falha, atrasar tentativas de autenticação adicionais após tentativas malsucedidas e bloquear ou encerrar sessões inativas.)			
<p>23. O uso desses recursos de segurança pelo dispositivo IoT pode não ser suficientemente modificável.</p> <p>Considerações de risco 1 e 3</p>	<ul style="list-style-type: none"> <li>• AC-7, Tentativas de login malsucedidas</li> <li>• AC-11, Bloqueio do dispositivo</li> <li>• AC-12, Término da sessão</li> <li>• IA-11, Reautenticação</li> </ul>	<ul style="list-style-type: none"> <li>• Não é possível obter acesso imediato aos dispositivos IoT quando necessário para usá-los ou gerenciá-los.</li> </ul>	<ul style="list-style-type: none"> <li>• PR.AC-3: O acesso remoto é gerenciado</li> <li>• PR.AC-4: As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de funções</li> <li>• PR.MA-1: A manutenção e o reparo dos ativos organizacionais são realizados e registrados, utilizando ferramentas aprovadas e controladas</li> <li>• PR.MA-2: A manutenção remota dos ativos organizacionais é aprovada, registrada e realizada de maneira que evita o acesso não autorizado</li> </ul>
Expectation 14: O dispositivo possui controles de segurança física embutidos adequados para protegê-lo contra adulteração (ex.: embalagem resistente a adulteração).			
<p>24. O dispositivo IoT pode ser implantado em uma área onde pessoas não autorizadas possam acessá-lo, ou onde pessoas autorizadas possam acessá-lo de maneiras não autorizadas.</p> <p>Considerações de risco 1 e 2</p>	<ul style="list-style-type: none"> <li>• MP-2, Acesso da mídia</li> <li>• MP-7, Uso da mídia</li> <li>• PE-3, Controle de acesso físico</li> </ul>	<ul style="list-style-type: none"> <li>• Permite que um invasor tenha acesso físico direto aos dispositivos e adultere-os, incluindo adição ou remoção de mídia de armazenamento, conexão de periféricos, etc.</li> </ul>	<ul style="list-style-type: none"> <li>• PR.AC-2: O acesso físico aos ativos é gerenciado e protegido</li> <li>• PR.PT-2: A mídia removível é protegida e seu uso é restrito de acordo com as políticas</li> <li>• PR.MA-1: A manutenção e o reparo dos ativos organizacionais são realizados e registrados, utilizando ferramentas aprovadas e controladas</li> </ul>
<b>Detecção de incidentes</b>			
Expectation 15: O dispositivo pode registrar seus eventos operacionais e de segurança.			
<p>25. O dispositivo IoT talvez não tenha a capacidade de registrar seus eventos operacionais e de segurança ou com detalhes suficientes.</p> <p>Consideração de risco 3</p>	<ul style="list-style-type: none"> <li>• AU-2, Eventos de auditoria</li> <li>• AU-3, Conteúdo dos registros de auditoria</li> <li>• AU-12, Geração de auditoria</li> <li>• SI-4, Monitoramento do sistema</li> </ul>	<ul style="list-style-type: none"> <li>• Aumenta a probabilidade de atividades maliciosas não serem detectadas.</li> <li>• Não é possível confirmar e reconstruir incidentes de entradas de log.</li> </ul>	<ul style="list-style-type: none"> <li>• DE.CM-7: É realizado o monitoramento de pessoal não autorizado, conexões, dispositivos e software</li> <li>• PR.PT-1: Os registros de auditoria/logs são identificados, documentados, implementados e revisados de acordo com as políticas</li> <li>• RS.AN-1: Notificações de sistemas de detecção são investigadas</li> </ul>

Desafios para dispositivos IoT individuais e considerações de risco que causam os desafios	Controles preliminares afetados NIST SP 800-53 Revisão 5	Implicações para a organização	Subcategorias de estrutura de segurança cibernética afetadas
<p>26. O dispositivo IoT pode continuar operando mesmo quando ocorre uma falha de registro.</p> <p>Considerações de risco 3</p>	<ul style="list-style-type: none"> <li>AU-5, Resposta às falhas de processamento de auditoria</li> </ul>	<ul style="list-style-type: none"> <li>Maior probabilidade de atividades maliciosas não serem detectadas.</li> </ul>	<ul style="list-style-type: none"> <li>DE.CM-7: É realizado o monitoramento de pessoal não autorizado, conexões, dispositivos e software</li> <li>PR.PT-1: Os registros de auditoria/logs são determinados, documentados, implementados e revisados de acordo com as políticas</li> </ul>
<p>Expectation 16: O dispositivo pode fazer a interface com os sistemas existentes de gerenciamento de log corporativo.</p>			
<p>27. O dispositivo IoT talvez não possa participar de um sistema de gerenciamento de log corporativo.</p> <p>Considerações de risco 2</p>	<ul style="list-style-type: none"> <li>AU-6, Revisão de auditoria, análise e relatórios</li> <li>SI-4, Monitoramento do sistema</li> </ul>	<ul style="list-style-type: none"> <li>Pode ter que usar vários sistemas de gerenciamento de log, e não apenas um.</li> <li>Talvez tenha que executar tarefas de gerenciamento de log manualmente.</li> <li>Aumenta a probabilidade de atividades maliciosas não serem detectadas.</li> </ul>	<ul style="list-style-type: none"> <li>DE.AE-3: Os dados do evento são coletados e correlacionados a partir de várias fontes e sensores</li> <li>DE.CM-7: É realizado o monitoramento de pessoal não autorizado, conexões, dispositivos e software</li> <li>PR.PT-1: Os registros de auditoria/logs são identificados, documentados, implementados e revisados de acordo com as políticas</li> </ul>
<p>Expectation 17: O dispositivo pode facilitar a detecção de possíveis incidentes por controles internos ou externos, como sistemas de prevenção de intrusão, utilitários anti-malware e mecanismos de verificação de integridade de arquivos.</p>			
<p>28. O dispositivo IoT talvez não possa executar controles de detecção internos ou interagir com controles de detecção externos sem afetar adversamente o funcionamento do dispositivo.</p> <p>Considerações de risco 1 e 3</p>	<ul style="list-style-type: none"> <li>SI-3, Proteção de código malicioso</li> <li>SI-7, Software, Firmware, e Integridade das informações</li> </ul>	<ul style="list-style-type: none"> <li>Aumenta a probabilidade de infecções de código malicioso e outras atividades não autorizadas que estejam ocorrendo ou passando despercebidas.</li> </ul>	<ul style="list-style-type: none"> <li>DE.CM-1: A rede é monitorada para detectar potenciais eventos de cibersegurança</li> <li>DE.CM-4: Código malicioso detectado</li> <li>PR.DS-6: Mecanismos de verificação de integridade são usados para verificar software, firmware e a integridade das informações</li> </ul>
<p>29. O dispositivo IoT talvez não forneça controles com a visibilidade necessária para detectar incidentes com eficiência e eficácia.</p> <p>Considerações de risco 2 e 3</p>	<ul style="list-style-type: none"> <li>IR-4 Como lidar com incidentes</li> <li>SI-4 Monitoramento do sistema</li> </ul>	<ul style="list-style-type: none"> <li>Aumenta a probabilidade de código malicioso e outras atividades não autorizadas que estejam passando despercebidas.</li> </ul>	<ul style="list-style-type: none"> <li>DE.CM-1: A rede é monitorada para detectar potenciais eventos de cibersegurança</li> <li>DE.CM-4: Código malicioso detectado</li> <li>PR.DS-6: Mecanismos de verificação de integridade são usados para verificar software, firmware e integridade da informação</li> </ul>



<b>Desafios para dispositivos IoT individuais e considerações de risco que causam os desafios</b>	<b>Controles preliminares afetados NIST SP 800-53 Revisão 5</b>	<b>Implicações para a organização</b>	<b>Subcategorias de estrutura de segurança cibernética afetadas</b>
Expectation 18: O dispositivo pode suportar atividades de análise de eventos e incidentes.			
30. O dispositivo IoT talvez não proporcione aos analistas acesso suficiente aos recursos do dispositivo para fazerem a análise necessária.  Considerações de risco 2 e 3	<ul style="list-style-type: none"> <li>SI-4, Monitoramento do sistema</li> </ul>	<ul style="list-style-type: none"> <li>Não pode usar ferramentas forenses para a coleta e análise de informações.</li> </ul>	<ul style="list-style-type: none"> <li>RS.AN-1: Notificações de sistemas de detecção são investigadas</li> <li>RS.AN-3: A análise forense é realizada</li> </ul>

#### 4.2 Desafios potenciais para alcançar o objetivo 2 - Proteger a Segurança de Dados

Tabela 2 - segue as mesmas normas convencionais, como a Tabela 1, porém, para proteger a segurança de dados. Presume-se que, se a segurança de dados precisa ser protegida, a segurança do dispositivo também precisa de proteção, portanto, os desafios em ambas as tabelas precisam ser considerados.

Observe que a seção Detecção de Incidentes da Tabela 1 também se aplica à proteção de segurança de dados. A Tabela 1 presume que apenas incidentes de segurança do dispositivo precisam ser protegidos; os mesmos desafios potenciais, controles afetados, implicações e subcategorias da Estrutura de Segurança Cibernética também se aplicam à detecção de incidentes de segurança de dados. As linhas de detecção de incidentes são omitidas da Tabela 2 por questões de brevidade.

**Tabela 2: Desafios potenciais para alcançar o objetivo 2 - Proteger a Segurança de Dados**

<b>Desafios para dispositivos IoT individuais</b>	<b>Controles preliminares afetados NIST SP 800-53 Revisão 5</b>	<b>Implicações para a organização</b>	<b>Subcategorias de estrutura de segurança cibernética afetadas</b>
<b>Proteção de dados</b>			
Expectation 19: O dispositivo pode impedir o acesso não autorizado a todos os dados confidenciais em seus dispositivos de armazenamento.			
31. O dispositivo IoT talvez não forneça recursos de criptografia suficientemente fortes para seus dados armazenados.  Considerações de risco 3	<ul style="list-style-type: none"> <li>MP-4, Armazenamento de mídia</li> <li>SC-28, Proteção de informações em repouso</li> </ul>	<ul style="list-style-type: none"> <li>Aumenta a probabilidade de acesso não autorizado ou adulteração de dados confidenciais.</li> </ul>	<ul style="list-style-type: none"> <li>PR.DS-1: Os dados em repouso são protegidos</li> <li>PR.PT-2: A mídia removível é protegida e seu uso é restrito de acordo com as políticas</li> </ul>
32. O dispositivo IoT pode não fornecer um mecanismo para higienizar dados confidenciais antes de descartar ou redirecionar o dispositivo.  Considerações de risco 3	<ul style="list-style-type: none"> <li>MP-6, Higienização de mídia</li> </ul>	<ul style="list-style-type: none"> <li>Aumenta a probabilidade de acesso não autorizado a dados confidenciais.</li> </ul>	<ul style="list-style-type: none"> <li>PR.IP-6: Os dados são destruídos de acordo com as políticas</li> </ul>



<b>Desafios para dispositivos IoT individuais</b>	<b>Controles preliminares afetados NIST SP 800-53 Revisão 5</b>	<b>Implicações para a organização</b>	<b>Subcategorias de estrutura de segurança cibernética afetadas</b>
Expectation 20: O dispositivo possui um mecanismo de suporte à disponibilidade de dados por meio de backups seguros.			
33. O dispositivo IoT pode não fornecer um mecanismo seguro de backup e restauração para seus dados.  Considerações de risco 3	<ul style="list-style-type: none"> <li>• CP-9, Backup do sistema</li> </ul>	<ul style="list-style-type: none"> <li>• Aumenta a probabilidade de perda de dados.</li> </ul>	<ul style="list-style-type: none"> <li>• PR.IP-4: Os backups de informações são realizados, mantidos e testados</li> </ul>
Expectation 21: O dispositivo pode impedir o acesso não autorizado a todos os dados confidenciais enviados em suas comunicações de rede.			
34. O dispositivo IoT talvez não forneça recursos de criptografia suficientemente fortes para proteger dados confidenciais enviados em suas comunicações de rede.  Considerações de risco 3	<ul style="list-style-type: none"> <li>• AC-18, Acesso sem fio</li> <li>• SC-8, Confidencialidade e integridade de transmissão</li> </ul>	<ul style="list-style-type: none"> <li>• Aumenta a probabilidade de espionagem nas comunicações.</li> </ul>	<ul style="list-style-type: none"> <li>• PR.DS-2: Os dados em trânsito são protegidos</li> </ul>
35. O dispositivo IoT pode não verificar a identidade de outro dispositivo de computação antes de enviar dados confidenciais em suas comunicações de rede.  Considerações de risco 3	<ul style="list-style-type: none"> <li>• SC-8, Confidencialidade e integridade de transmissão</li> <li>• SC-23, Autenticidade da sessão</li> </ul>	<ul style="list-style-type: none"> <li>• Aumenta a probabilidade de espionagem, interceptação, manipulação, falsificação de identidade e outras formas de ataque às comunicações.</li> </ul>	<ul style="list-style-type: none"> <li>• PR.DS-2: Os dados em trânsito são protegidos</li> </ul>

### 4.3 Desafios potenciais para alcançar o objetivo 3, proteger a privacidade dos indivíduos

Tabela 3 - lista os desafios potenciais para atingir o objetivo 3, protegendo a privacidade dos indivíduos ao mitigar o risco de privacidade decorrente do processamento autorizado de PII. A tabela segue as mesmas convenções das tabelas anteriores, mas omite os mapeamentos para as subcategorias da estrutura de segurança cibernética, uma vez que a estrutura de segurança cibernética não aborda os riscos de privacidade do processamento autorizado de PII.

Presume-se que, se a privacidade dos indivíduos precisa ser protegida, a segurança do dispositivo e dos dados também precisam de proteção, portanto, os desafios em todas as três tabelas precisam ser considerados. No entanto, as organizações podem usar as informações da Tabela 2 para abordar os riscos de privacidade decorrentes da perda de confidencialidade, integridade ou disponibilidade de PII..

**Tabela 3: Desafios potenciais para alcançar o objetivo 3 - proteger a privacidade dos indivíduos**

<b>Desafios para dispositivos IoT individuais</b>	<b>Controles preliminares afetados NIST SP 800-53 Revisão 5</b>	<b>Implicações para a organização</b>
<b>Gerenciamento de dados desassociados</b>		
Expectation 22: O dispositivo opera em um ambiente de identidade federada tradicional.		
36. O dispositivo IoT pode contribuir com dados que são usados para identificação e autenticação, mas estão fora dos ambientes federados tradicionais.  Consideração de risco 3	IA-8 (6), Identificação e autenticação (usuários não organizacionais)   Dissociabilidade	<ul style="list-style-type: none"> <li>Técnicas como o uso de tabelas de mapeamento de identificadores e técnicas criptográficas de aumento de privacidade para ocultar os provedores de serviços de credenciais e partes confiáveis uns dos outros, ou para tornar os atributos de identidade menos visíveis para as partes transmissoras, talvez não funcionem fora de um ambiente federado tradicional.</li> </ul>
<b>Tomada de decisão informada</b>		
Expectation 23: Existem interfaces tradicionais para engajamento individual com o dispositivo.		
37. O dispositivo IoT pode não ter interfaces que permitam aos indivíduos interagirem com ele.  Consideração de risco 2	IP-2, Consentimento	<ul style="list-style-type: none"> <li>Os indivíduos talvez não possam fornecer consentimento para o processamento de PII ou condicionar o processamento adicional de atributos específicos.</li> </ul>
38. As funções de processamento de dados descentralizados e a propriedade heterogênea de dispositivos IoT desafiam os processos tradicionais de responsabilidade.  Consideração de risco 3	IP-3, Correção	<ul style="list-style-type: none"> <li>Os indivíduos talvez não possam localizar a fonte imprecisa ou problemática de PII para corrigi-la ou resolver o problema.</li> </ul>
39. O dispositivo IoT pode não ter interfaces que permitam aos indivíduos ler os avisos de privacidade.  Consideração de risco 2	IP-4, Aviso de privacidade	<ul style="list-style-type: none"> <li>Os indivíduos podem não conseguir ler ou acessar os avisos de privacidade.</li> </ul>
40. O dispositivo IoT pode não ter interfaces para permitir o acesso a PIIs, ou as PIIs podem estar armazenadas em locais desconhecidos.  Consideração de risco 2	IP-6, Acesso individual	<ul style="list-style-type: none"> <li>Os indivíduos podem ter dificuldade em acessar suas informações, o que limita a capacidade de gerenciar informações e entender o que está acontecendo com os seus dados, o que aumenta os riscos de compliance.</li> </ul>
<b>Gerenciamento de permissões de processamento de PII</b>		
Expectation 24: Existem controles centralizados suficientes para se aplicar as normas ou requisitos regulatórios às PIIs.		
41. O dispositivo IoT pode coletar PII indiscriminadamente ou analisar, compartilhar ou agir sobre as PIIs com base em processos automatizados.  Consideração de risco 2	PA-2, Autoridade para coletar	<ul style="list-style-type: none"> <li>As PIIs podem ser processadas de maneiras que não estão em conformidade com os requisitos regulatórios ou com as políticas de uma organização.</li> </ul>

Desafios para dispositivos IoT individuais	Controles preliminares afetados NIST SP 800-53 Revisão 5	Implicações para a organização
<p>42. Os dispositivos IoT podem ser complexos e dinâmicos, com funcionalidades de detecção que podem coletar PII sendo frequentemente adicionados e removidos.</p> <p>Consideração de risco 1</p>	<p>PA-3, Especificação de finalidade</p>	<ul style="list-style-type: none"> <li>As PIIs podem ser difíceis de rastrear, portanto, os indivíduos, bem como os proprietários/operadores de dispositivos, podem não ter suposições confiáveis sobre como as PIIs estão sendo processadas, dificultando a tomada de decisões informadas.</li> </ul>
<p>43. O dispositivo IoT pode ser acessado remotamente, permitindo o compartilhamento de PII fora do controle do administrador.</p> <p>Considerações de risco 2</p>	<p>PA-4, Compartilhamento de informações com partes externas</p>	<ul style="list-style-type: none"> <li>As PIIs podem estar sendo compartilhadas em descumprimento aos deveres de compliance com os requisitos regulamentares ou com as políticas de uma organização.</li> </ul>
<b>Gerenciamento do fluxo de informação</b>		
Expectation 25: Existe controle centralizado suficiente para gerenciar PII.		
<p>44. Os dispositivos IoT podem ser complexos e dinâmicos, com funcionalidades de detecção que podem coletar PII sendo frequentemente adicionados e removidos.</p> <p>Consideração de risco 1</p>	<p>PM-29, Inventário de informações de identificação pessoal</p>	<ul style="list-style-type: none"> <li>PII pode ser difícil de identificar e rastrear usando métodos tradicionais de inventário.</li> </ul>
<p>45. Os dispositivos IoT podem não oferecer suporte a mecanismos padronizados para gerenciamento centralizado de dados, e o grande número de dispositivos IoT para gerenciar pode ser esmagador.</p> <p>Considerações de risco 2</p>	<p>SC-7 (24), Proteção de limite   Informação pessoalmente identificável</p>	<ul style="list-style-type: none"> <li>A aplicação das regras de processamento de PII destinadas a proteger a privacidade dos indivíduos pode ser interrompida.</li> </ul>
<p>46. O dispositivo IoT pode não ter a capacidade de suportar configurações como prevenção de ativação remota, relatório de dados limitado, aviso de coleta e minimização de dados.</p> <p>Considerações de risco 3</p>	<p>SC-42, Capacidade do sensor e dados</p>	<ul style="list-style-type: none"> <li>A falta de recursos diretos de mitigação de risco de privacidade pode exigir controles que compensem este fato, o que pode afetar a capacidade de uma organização de otimizar a redução de risco de privacidade.</li> </ul>
<p>47. O dispositivo IoT pode coletar PII indiscriminadamente. A propriedade heterogênea de dispositivos desafia as técnicas tradicionais de gerenciamento de dados.</p> <p>Consideração de risco 2</p>	<p>SI-12 (1), Gerenciamento e retenção de informações   Limitar elementos de informações pessoalmente identificáveis</p>	<ul style="list-style-type: none"> <li>É mais provável que PIIs operacionalmente desnecessários fiquem retidos.</li> </ul>

<b>Desafios para dispositivos IoT individuais</b>	<b>Controles preliminares afetados NIST SP 800-53 Revisão 5</b>	<b>Implicações para a organização</b>
<p>48. As funções de processamento de dados descentralizados e a propriedade heterogênea de dispositivos IoT desafiam os processos tradicionais de gerenciamento de dados com relação à verificação da precisão dos dados.</p> <p>Considerações de risco 2</p>	<p>SI-19, Operações de qualidade de dados</p>	<ul style="list-style-type: none"> <li>• É mais provável que PII imprecisas persistam com o potencial de criar problemas para os indivíduos.</li> </ul>
<p>49. As funções de processamento de dados descentralizados e a propriedade heterogênea de dispositivos IoT desafiam os processos tradicionais de desidentificação.</p> <p>Considerações de risco 2 e 3</p>	<p>SI-20, Desidentificação</p>	<ul style="list-style-type: none"> <li>• A agregação de conjuntos de dados díspares pode levar à reidentificação de PII.</li> </ul>

## 5 Recomendações para abordar desafios de mitigação de riscos de segurança cibernética e privacidade para dispositivos IoT

Esta seção fornece recomendações para lidar com os desafios de mitigação de riscos de segurança cibernética e privacidade para dispositivos IoT. A Figura 6 resume as recomendações, que estão listadas abaixo e, se indicado, descritas com mais detalhes em outra parte da publicação:

1. Compreender as considerações de risco do dispositivo IoT (Seção 3) e os desafios que eles podem causar para mitigar os riscos de segurança cibernética e privacidade para dispositivos IoT nas áreas de mitigação de risco apropriadas (Seção 4).
2. Ajustar as normas e processos organizacionais para lidar com os desafios de mitigação de riscos de segurança cibernética e privacidade em todo o ciclo de vida do dispositivo IoT. A Seção 5.1 fornece mais informações sobre este tópico. A Seção 4 desta publicação cita muitos exemplos de possíveis desafios, mas cada organização precisará customizá-los para levar em consideração os requisitos da missão e outras características específicas da organização.
3. Implementar práticas de mitigação atualizadas para os dispositivos IoT da organização como você faria com qualquer outra mudança nas práticas (Seção 5.2).

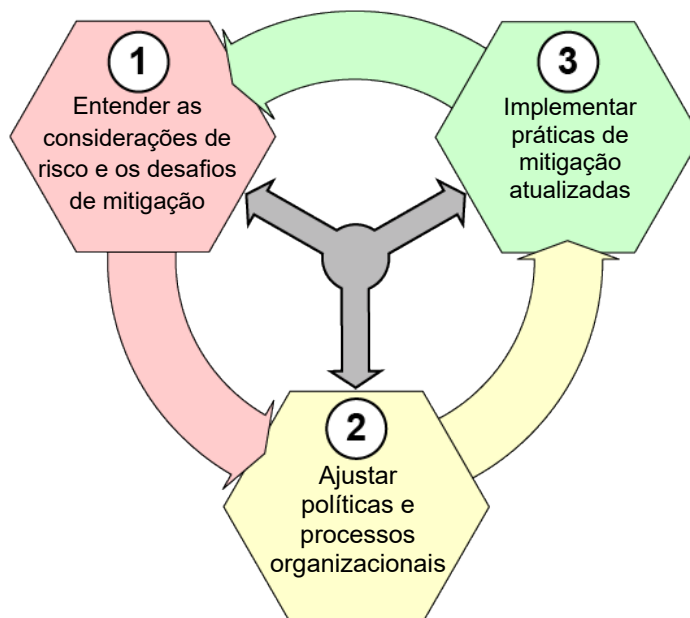


Figura 6: Resumo da recomendação

### 5.1 Ajustando normas e processos organizacionais

As organizações devem garantir que estão abordando as considerações em todo o ciclo de vida do dispositivo IoT em suas políticas e processos de segurança cibernética e privacidade. As organizações devem garantir que declaram especificamente como definem o escopo da IoT para evitar confusão e ambiguidade. Isso é particularmente importante para organizações que podem estar sujeitas a leis e regulamentos com diferentes definições de IoT.

Similarmente, as organizações devem garantir que seus programas de segurança cibernética, cadeia de suprimentos e gerenciamento de riscos de privacidade levem a IoT em consideração na devida maneira. Isto inclui o seguinte:

- Determinar quais os dispositivos que possuem recursos de dispositivos IoT. Ter mecanismos para determinar se um dispositivo que pode ser adquirido ou já foi adquirido é um dispositivo IoT, se isso não for aparente.
- Identificar tipos de dispositivos IoT. Saber quais tipos de dispositivos IoT estão em uso, quais os recursos que cada tipo suporta e quais as finalidades que cada tipo suporta.
- Avaliar o risco do dispositivo IoT. É importante levar em consideração o ambiente IoT específico em que os dispositivos IoT residem e não apenas avaliar os riscos dos dispositivos IoT

isoladamente. Por exemplo, anexar um atuador a um sistema físico pode afetar os riscos de forma muito diferente do que anexar o mesmo atuador a outro sistema físico.

- Determinar como responder a esse risco, aceitando, evitando, mitigando, compartilhando ou transferindo o risco. Conforme discutido anteriormente, algumas estratégias de mitigação de risco para TI convencional podem não funcionar bem para IoT. A Seção 4 desta publicação discute os desafios de mitigação de risco para dispositivos IoT em detalhe.

O gerenciamento dos riscos de segurança cibernética e privacidade para alguns dispositivos IoT pode afetar outros tipos de riscos e introduzir novos riscos à segurança, confiabilidade, resiliência, desempenho e outras áreas. As organizações devem considerar o que é mais compensador em termos de riscos ao tomar decisões sobre segurança cibernética e mitigação de riscos de privacidade. Por exemplo, suponha que um determinado dispositivo IoT seja crítico para a segurança. Exigir que o pessoal em uma área fisicamente protegida insira uma senha para obter acesso local ao dispositivo IoT pode atrasar a intervenção durante um mau funcionamento. Requisitos adicionais envolvendo o tamanho e complexidade da senha e bloqueios automáticos de conta após tentativas consecutivas de autenticação com falha podem causar atrasos muito mais longos, aumentando a probabilidade e magnitude do problema. As organizações devem aproveitar os programas que possuem para gerenciar outras formas de risco ao determinar como os riscos de privacidade e segurança cibernética do dispositivo IoT devem ser gerenciados.

Com base nos possíveis desafios de mitigação e nas implicações desses desafios, as implementações das seguintes subcategorias de estrutura de segurança cibernética [6] provavelmente precisarão de ajustes para que as políticas e processos organizacionais abordem adequadamente o risco de segurança cibernética em todo o ciclo de vida do dispositivo IoT:

- ID.AM (Identificar — Gestão de Ativos)
  - ID.AM-1: Dispositivos físicos e sistemas dentro da organização são inventariados
  - ID.AM-2: Plataformas de software e aplicativos dentro da organização são inventariados
- ID.BE (Identificar - Ambiente de Negócios)
  - ID.BE-4: Dependências e funções críticas para entrega de serviços críticos são estabelecidas
  - ID.BE-5: Os requisitos de resiliência para apoiar a entrega de serviços críticos são estabelecidos para todos os estados operacionais (ex.: sob coação/invasão, durante a recuperação, operações normais)
- ID.GV (Identificar — Governança)
  - ID.GV-1: As políticas de segurança cibernética organizacional são estabelecidas e comunicadas
  - ID.GV-2: As funções e responsabilidades da segurança cibernética são coordenadas e alinhadas com as funções internas e parceiros externos
  - ID.GV-3: Requisitos legais e regulamentares relativos à segurança cibernética, incluindo obrigações de privacidade e liberdade civil são compreendidos e gerenciados
  - ID.GV-4: Os processos de governança e gestão de risco tratam dos riscos de segurança cibernética
- ID.RA (Identificar — Avaliação de Risco)
  - ID.RA-1: Vulnerabilidades de ativos são identificadas e documentadas
  - ID.RA-3: Ameaças, tanto internas quanto externas, são identificadas e documentadas
  - ID.RA-4: Potenciais impactos e probabilidades de negócios são identificados
  - ID.RA-6: As respostas ao risco são identificadas e priorizadas
- ID.RM (Identificar - Estratégia de Gestão de Risco)
  - ID.RM-2: A tolerância ao risco organizacional é determinada e claramente expressa

- ID.RM-3: A determinação de tolerância ao risco da organização é informada de acordo com o seu papel na infraestrutura crítica e na análise de risco específica do setor
- ID.SC (Identificar — Gestão de risco da cadeia de abastecimento)
  - ID.SC-2: Fornecedores e parceiros terceirizados de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados usando um processo de avaliação de risco da cadeia de suprimentos cibernética
  - ID.SC-3: Os contratos com fornecedores e parceiros terceirizados são usados para implementar medidas adequadas destinadas a atender os objetivos do programa de segurança cibernética de uma organização e do Plano de Gerenciamento de Risco da Cadeia de Suprimentos Cibernéticos
- PR.IP (Proteger - Processos e procedimentos de proteção de informações)
  - PR.IP-3: Os processos de controle de mudança de configuração estão em vigor
  - PR.IP-9: Planos de resposta (Resposta a Incidentes e Continuidade de Negócios) e planos de recuperação (Recuperação de Incidentes e Recuperação de Desastres) estão em vigor e são gerenciados
  - PR.IP-12: Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado

Similarmente, as implementações das tarefas listadas abaixo, referentes ao NIST SP 800-37 Revisão 2 [4] provavelmente precisarão ser ajustadas para que as políticas e processos organizacionais abordem adequadamente os riscos de segurança cibernética e privacidade em todo o ciclo de vida do dispositivo IoT. Observe que, embora a Estrutura de Segurança Cibernética possa ser usada para gerenciar o aspecto da privacidade relacionado à segurança cibernética de PII, o NIST SP 800-37 Revisão 2 pode ser usado para gerenciar todo o escopo da privacidade, já que integra o processamento de PII autorizado na Estrutura de Gestão de Risco do NIST (RMF).

- Preparar, Nível de Organização, Tarefa P-1: Funções da gestão de risco
- Preparar, Nível de Organização, Tarefa P-2: Estratégia de gestão de risco
- Preparar, Nível de Organização, Tarefa P-3: Avaliação de Risco - Organização
- Preparar, Nível do Sistema, Tarefa P-8: Missão ou foco empresarial
- Preparar, Nível do Sistema, Tarefa P-13: Ciclo de vida da informação
- Preparar, Nível do Sistema, Tarefa P-14: Avaliação de Risco - Sistema
- Preparar, Nível do Sistema, Tarefa P-15: Definição de Requisitos

## 5.2 Implementando práticas atualizadas de mitigação de risco

As práticas de mitigação de risco de privacidade e segurança cibernética de uma organização podem precisar de mudanças significativas devido ao grande número de dispositivos IoT e aos vários tipos de dispositivos IoT. Para dispositivos convencionais de TI, a maioria das organizações possuem dezenas de tipos - desktops, laptops, servidores, smartphones, roteadores, switches, firewalls, impressoras, etc. Dispositivos convencionais de TI dentro de um único tipo tendem a ter recursos semelhantes. Por exemplo, a maioria dos laptops tem recursos semelhantes de armazenamento e processamento de dados; interface de usuário humana e recursos de interface de rede; e recursos de suporte, como gerenciamento centralizado. Isso permite que as organizações determinem como gerenciar o risco individual para as dezenas de tipos de dispositivos de TI convencionais, com algumas customizações para dispositivos e modelos específicos, sendo que as organizações geralmente estão acostumadas a esse tipo de trabalho.

Entretanto, várias organizações podem ter muito mais tipos de dispositivos IoT, mais do que os convencionais de TI, devido à natureza e propósito único da maioria dos dispositivos IoT. Uma organização pode precisar determinar como gerenciar o risco para centenas ou milhares de tipos de dispositivos IoT. Os recursos variam amplamente de um tipo de dispositivo IoT para outro. Pode haver

um tipo sem armazenamento de dados e recursos de gerenciamento centralizado e outro tipo com vários sensores e atuadores, usando armazenamento de dados local e remoto, além de recursos de processamento, sendo conectado a várias redes internas e externas de uma só vez. A variabilidade dos recursos causa variabilidade semelhante nos riscos de segurança cibernética e privacidade envolvendo cada tipo de dispositivo IoT, bem como as opções para mitigar esses riscos.

Além disso, uma organização pode precisar determinar como gerenciar o risco, não apenas pelo tipo de dispositivo, mas também pelo uso de tal dispositivo. A maneira como um dispositivo deve ser usado pode indicar que um objetivo de segurança, como integridade, é mais importante do que outro, como confidencialidade, que por sua vez pode exigir diferentes mecanismos para mitigação de risco. No mesmo sentido, um dispositivo pode ser usado de formas que alguns dos seus recursos não sejam necessários e possam ser desativados, o que pode reduzir o risco do dispositivo.



**Apêndice A - [Retirado]**

Anteriormente, o Apêndice A apresentava exemplos de possíveis recursos de segurança cibernética e privacidade que as organizações desejariam integrar em seus dispositivos IoT. Esse conteúdo foi retirado desta publicação e será aprimorado para ser lançado em uma publicação separada que será postada no nosso website de programas (<https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program>).

**Apêndice B - Siglas e Abreviações**

As siglas e abreviações selecionadas e usadas neste documento são definidas como segue:

API	Application Programming Interface (Interface de programação de aplicativos)
DDoS	Distributed Denial of Service (Negação de serviço distribuído)
FISMA	Federal Information Security Modernization Act (Lei Federal de Modernização da Segurança da Informação)
FOIA	Freedom of Information Act (Lei de Liberdade de Informação)
IETF	Internet Engineering Task Force (Força-Tarefa de Engenharia da Internet)
IoT	Internet das Coisas
IP	Protocolo da Internet
IR	Relatório Interno
IT	Tecnologia da Informação
ITL	Laboratório de Tecnologia da Informação
LTE	Evolução a longo prazo
NICE	National Initiative for Cybersecurity Education (Iniciativa Nacional para Educação em Segurança Cibernética)
NIST	National Institute of Standards and Technology (Instituto Nacional de Padrões e Tecnologia)
OMB	Office of Management and Budget (Escritório de Gestão e Orçamento)
OT	Tecnologia Operacional
PII	Informações Pessoalmente Identificáveis
RFC	Solicitação de comentários
RMF	Estrutura de gestão de risco
SLA	Acordo de Nível de Serviço
SP	Publicação Especial

**Apêndice C - Glossário**

Recurso do Atuador	A capacidade de mudar algo no mundo físico.
Recurso de interface do aplicativo	A capacidade de outros dispositivos de computação se comunicarem com um dispositivo IoT por meio de um aplicativo de dispositivo IoT.
Recursos	Uma característica ou função.
Ações dos dados	“Operações do sistema que processa PII.” [5]
Dissociabilidade	“Permitir o processamento de PII ou eventos sem associação a indivíduos ou dispositivos além dos requisitos operacionais do sistema.” [5]
Recurso de interface de usuário humano	A capacidade de um dispositivo IoT se comunicar diretamente com as pessoas.
Recursos de Interface	São recursos que permitem interações dos dispositivos IoT (ex.: comunicações de dispositivo para dispositivo, comunicações de humano para dispositivo). Os tipos de recursos de interface são aplicativo, usuário humano e rede.
Recurso de interface	A capacidade de fazer interface com uma rede de comunicação com o objetivo de comunicar dados de ou para um dispositivo IoT. Uma capacidade de interface de rede permite que um dispositivo seja conectado e use uma rede de comunicação. Cada dispositivo IoT tem pelo menos um recurso de interface de rede e pode ter mais do que um.
Informações Pessoalmente Identificáveis (PII)	“Informações que podem ser usadas para distinguir ou rastrear a identidade de um indivíduo isoladamente ou quando combinadas com outras informações que estão vinculadas ou vinculáveis a um indivíduo específico.” [8]
Processamento de PII	Uma operação ou conjunto de operações realizadas sobre PII que pode incluir, dentre outros, coleta, retenção, registro, geração, transformação, uso, divulgação, transferência e descarte de PII.
Recurso pós-mercado	Um recurso de segurança cibernética ou privacidade que uma organização seleciona, adquire e implanta; qualquer capacidade que não seja pré-mercado.
Recurso Pré-Mercado	Um recurso de cibersegurança ou privacidade embutido em um dispositivo IoT. Os recursos pré-mercado são integrados aos dispositivos IoT pelo fabricante ou fornecedor antes de serem enviados às organizações do cliente.
Ação de dados problemáticos	Uma operação de sistema que processa PII através do ciclo de vida da informação e, como efeito colateral, faz com que os indivíduos tenham algum tipo de problema.

Risco	"Uma medida da extensão em que uma entidade é ameaçada por uma circunstância ou evento potencial, sendo normalmente uma função de: (i) impacto adverso, ou magnitude do dano, que surgiria se a circunstância ou evento ocorresse; e (ii) a probabilidade de ocorrência." [4]
Recursos de sensor	A capacidade de fornecer uma observação sobre um aspecto do mundo físico na forma de dados de medição.
Recursos de Suporte	Recursos que fornecem funcionalidade compatível com os outros recursos de IoT. Exemplos de recursos de suporte são: gerenciamento de dispositivos, segurança cibernética e recursos de privacidade.
Recursos do transdutor	Recursos que fornecem capacidade para que os dispositivos de computação possam interagir diretamente com entidades físicas de interesse. Os dois tipos de recursos do transdutor são o sensor e o atuador.

**Apêndice D - Referências**

- [1] Newhouse W, Keith S, Scribner B, Witte G (2017) National Initiative for Cybersecurity Education (NICE) (Iniciativa Nacional para Educação em Cibersegurança) Cybersecurity Workforce Framework (Estrutura de força de trabalho de segurança cibernética). (National Institute of Standards and Technology, Gaithersburg, MD) (Instituto Nacional de Padrões e Tecnologia - NIST, Publicação Especial do NIST (SP) 800-181. <https://doi.org/10.6028/NIST.SP.800-181>
- [2] Simmon E (a ser publicado) A Model for the Internet of Things (IoT). (Um modelo para a Internet das Coisas) Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD).
- [3] Stouffer K, Pillitteri V, Lightman S, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security (Guia de 2015 para Segurança de Sistemas de Controle Industrial (ICS) (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), NIST Publicação Especial (SP) 800-82 Revisão 2. <https://doi.org/10.6028/NIST.SP.800-82r2>
- [4] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (Força Tarefa Conjunta (2018) Estrutura de gerenciamento de risco para sistemas de informação e organizações: Uma abordagem do ciclo de vida do sistema para segurança e privacidade). (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), NIST Publicação Especial (SP) 800-37 Revisão 2. <https://doi.org/10.6028/NIST.SP.800-37r2>
- [5] Brooks S, Garcia M, Lefkovitz N, Lightman S, Nadeau E (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems (Uma introdução à engenharia de privacidade e gerenciamento de risco em sistemas federais). (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD). Relatório Interno (IR) do NIST 8062. <https://doi.org/10.6028/NIST.IR.8062>
- [6] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (Estrutura para melhorar a segurança cibernética da infraestrutura crítica, versão 1.1. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD). <https://doi.org/10.6028/NIST.CSWP.04162018>
- [7] Joint Task Force (2017) Security and Privacy Controls for Information Systems and Organizations. (Força Tarefa Conjunta (2017) Segurança e controles de privacidade para sistemas de informação e organizações.) (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), Versão preliminar da publicação especial (SP) do NIST 800-53 Revisão 5. <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft>
- [8] Office of Management and Budget (2016) Managing Information as a Strategic Resource (Escritório de Gestão e Orçamento (2016) Gerenciando informações como um recurso estratégico). (Office of Management and Budget (OMB), Washington, DC), Circular do OMB No. A-130. <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf>