Versão 1.0

NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0

16 de janeiro de 2020

Esta publicação está disponível gratuitamente em:
https://doi.org/10.6028/NIST.CSWP.01162020pt

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

Síntese

Por mais de duas décadas, a Internet e as tecnologias de informação associadas impulsionaram inovações, crescimentos econômicos, e melhorias nos serviços sociais de maneira sem precedentes. Muitos benefícios são proporcionados por meio de dados sobre indivíduos que fluem através de um ecossistema complexo. Como resultado, os indivíduos talvez não consigam entender as possíveis consequências para sua privacidade à medida que interagem com sistemas, produtos e serviços. Da mesma forma as organizações podem não perceber toda a extensão dessas consequências para os indivíduos, a sociedade como um todo ou suas empresas, o que pode afetar as suas marcas, resultados e perspectivas futuras de crescimento.

Usando um processo transparente, baseado em consenso, e incluindo as partes interessadas no âmbito privado e público para produzir essa ferramenta voluntária, o Instituto Nacional de Normas e Tecnologia (NIST) lançou o Privacy Framework (Estrutura de Privacidade): uma ferramenta para aumentar o nível de privacidade por meio do gerenciamento de riscos corporativos (pelo Privacy Framework), assim permitindo melhores práticas de engenharia de privacidade, e oferecendo apoio à privacidade por meio de conceitos de design que ajudam as organizações a proteger a privacidade dos indivíduos. O Privacy Framework pode oferecer suporte às organizações das seguintes maneiras:

- Alavancando a confiança dos clientes apoiando a tomada de decisões éticas referentes ao design ou implantação de produtos e serviços que otimizam o uso benéfico de dados, minimizando as consequências adversas para a privacidade dos indivíduos e para a sociedade como um todo;[1]
- Cumprindo as obrigações em vigor sobre compliance, bem como produtos e serviços que possam ser utilizados no futuro, visando a cumprir tais obrigações em um ambiente tecnológico e normativo em constante mudança;
- Facilitando a comunicação sobre práticas de privacidade com indivíduos, parceiros de negócios, assessores e reguladores.

Obtendo benefícios dos dados capturados e simultaneamente gerenciando riscos à privacidade dos indivíduos, o que não significa que uma única abordagem seja a ideal para todos. Usando como analogia a construção de uma casa, os proprietários escolhem os layouts e os designs que preferem, mas dependem de uma estrutura de engenharia bem alicerçada. Assim também, a proteção à privacidade deve permitir escolhas individuais, desde que mitigações eficazes de risco de privacidade já façam parte da engenharia dos produtos e serviços. O Privacy Framework — por meio de uma abordagem baseada em riscos e resultados — é flexível o suficiente para atender às diversas necessidades de privacidade, permitindo soluções mais inovadoras e eficazes que possam levar a resultados mais positivos para indivíduos e organizações, estando sempre atualizado, integrando tendências tecnológicas, como inteligência artificial e a Internet das Coisas.

O Privacy Framework segue a estrutura do Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) [1] para facilitar o uso conjunto dos dois frameworks. Assim como o Cybersecurity Framework, o Privacy Framework é composto por três partes: Core (núcleo), Profiles (perfis), e Implementation Tiers (níveis de implementação). Cada componente reforça o gerenciamento de risco de privacidade por meio da conexão entre a empresa e os responsáveis pela missão, funções e responsabilidades organizacionais, e atividades de proteção à privacidade.

[1] Não há uma norma objetiva para a tomada de decisões éticas; ele está fundamentado nas normas, valores e expectativas legais em determinada sociedade.

- O núcleo permite um diálogo — do nível executivo ao nível de implementação/operações — sobre atividades importantes de proteção à privacidade e os resultados desejados.
- Os perfis permitem a priorização dos resultados e atividades que melhor atendam aos valores de privacidade organizacional, às necessidades de missão, ou aos negócios e riscos.
- Os níveis de implementação apoiam a tomada de decisão e a comunicação sobre a suficiência de processos e recursos organizacionais para gerenciar riscos de privacidade.

Em suma, o Privacy Framework tem o objetivo de ajudar as organizações a construir uma base sólida quanto à privacidade, colocando esse requisito na mesma paridade do seu portfólio de riscos corporativos.

Reconhecimentos

Esta publicação é resultado de um esforço colaborativo entre o NIST e as partes interessadas organizacionais e individuais nos setores público e privado. Para desenvolver o Privacy Framework, o NIST contou com a ajuda de três workshops públicos, uma solicitação por informações (RFI), uma solicitação por comentários (RFC), cinco webinars e centenas de interações diretas com as partes interessadas.[2] O NIST reconhece e agradece a todos aqueles que contribuíram para esta publicação.

[2] Um arquivo completo sobre o desenvolvimento deste material pode ser encontrado em https://www.nist.gov/privacy-framework.

Tabela de Conteúdo

Síntese ..... ***i***

Reconhecimentos ..... ***ii***

1.0 Introdução ao Privacy Framework **1**
1.1 Visão Geral do Privacy Framework 2
1.2 Gerenciamento de Riscos de Privacidade 3
1.2.1 Gerenciamento de riscos de segurança cibernética e privacidade 3
1.2.2 Avaliação de risco de privacidade 5
1.3 Visão geral do documento 6

2.0 Informações básicas sobre o Privacy Framework **6**
2.1 Núcleo 7
2.2 Perfis 9
2.3 Níveis de implementação 10

3.0 Como usar o Privacy Framework **10**
3.1 Mapeamento para referências informativas 11
3.2 Aumentando o nível de responsabilização 12
3.3 Como estabelecer ou aprimorar um programa de privacidade 13
3.4 Aplicação ao ciclo de vida de desenvolvimento de sistemas 14
3.5 Utilização dentro do ecossistema de processamento de dados 15
3.6 Decisões informadas sobre compras 16

Referências ***17***

Apêndice A: Núcleo do Privacy Framework ***19***

Apêndice B: Glossário ***31***

Apêndice C: Siglas ***35***

Apêndice D: Práticas de gerenciamento de risco de privacidade ***36***

Apêndice E: Definições dos níveis de implementação ***42***

Lista das Figuras

Figura 1: Núcleo, Perfis e Níveis de Implementação **2**
Figura 2: Relação entre risco de segurança cibernética e privacidade **3**
Figura 3: Relação entre risco de privacidade e risco organizacional **5**
Figura 4: Estrutura do Núcleo do Privacy Framework **7**
Figura 5: Usando as funções para gerenciar riscos de privacidade e segurança cibernética **7**
Figura 6: Relação entre núcleo e perfis **9**
Figura 7: Colaboração abstrata e fluxos de comunicação dentro de uma organização **12**
Figura 8: Relacionamentos do ecossistema de processamento de dados **15**

Lista das Tabelas

Tabela 1: Identificadores exclusivos das categorias e funções do Privacy Framework **21**
Tabela 2: Núcleo do Privacy Framework **22**
Tabela 3: Engenharia de privacidade e objetivos de segurança **38**

1.0 Introdução ao Privacy Framework

Por mais de duas décadas, a Internet e as tecnologias de informação associadas impulsionaram inovações, crescimentos econômicos e melhorias nos serviços sociais, de maneira sem precedentes. Muitos benefícios são proporcionados por *dados* sobre *indivíduos* que fluem através de um ecossistema complexo. Como resultado, os indivíduos talvez não consigam entender as possíveis consequências para sua privacidade à medida que interagem com sistemas, produtos e serviços. Como também, as organizações podem não perceber o impacto dessas consequências. Quando as empresas não administram o *risco de privacidade*, isso pode resultar em consequências adversas que impactam diretamente os indivíduos e a sociedade, com consequências negativas para as marcas, resultados financeiros e perspectivas futuras de crescimento das organizações. Encontrar maneiras de derivar benefícios do *processamento de dados* e ao mesmo tempo gerenciar riscos à privacidade dos indivíduos não significa que uma única abordagem seja ideal para todos.

A privacidade é desafiadora porque não é apenas um conceito abrangente que ajuda a salvaguardar valores importantes, como a autonomia e a dignidade humana, pois os meios para alcançá-la podem ser bem diferentes.[3] Por exemplo, a privacidade pode ser alcançada através do isolamento, observação limitada, ou o controle de certas facetas da identidade dos indivíduos (ex: corpo, dados, reputação).[4] Além disso, a autonomia e a dignidade humana não são elementos fixos e quantificáveis, mas são filtrados através da diversidade de culturas e diferenças individuais. Esta natureza abrangente e mutante da privacidade faz com que seja difícil comunicar claramente os riscos de privacidade dentro de organizações e entre elas e indivíduos. O que está faltando é uma linguagem comum e uma ferramenta prática que seja flexível o suficiente para atender às várias e diversificadas necessidades de privacidade.

Este NIST Privacy Framework voluntário consiste em uma ferramenta para aumentar o nível de privacidade por meio da Gestão de Riscos Corporativos (Privacy Framework) cujo intuito é ser amplamente utilizada por organizações de todos os tamanhos e agnósticas a qualquer tipo de tecnologia, setor, lei ou jurisdição. Usando uma abordagem comum —adaptável às funções de qualquer organização dento do *ecossistema de processamento de dados*— o objetivo do Privacy Framework é ajudar as organizações a gerenciar riscos de privacidade da seguinte maneira:

- Levar em conta a privacidade durante o design e implantação de sistemas, produtos e serviços que afetam os indivíduos;
- Comunicar suas práticas de privacidade; e
- Incentivar a colaboração cruzada da força de trabalho em uma organização — por exemplo, entre executivos, departamento jurídico e tecnologia da informação (TI) — por meio do desenvolvimento de perfis, seleção de níveis e obtenção de resultados.

---

[3] Autonomia e dignidade são conceitos abordados na Declaração Universal dos Direitos Humanos das Nações Unidas https://www.un.org/en/universal-declaration-human-rights/.

[4] Existem muitas publicações que oferecem explicações aprofundadas sobre o contexto da privacidade ou diferentes aspectos do conceito. Dois exemplos de publicações: Solove D (2010) *Understanding Privacy* [Compreendendo a Privacidade] (Harvard University Press, Cambridge, MA), https://ssrn.com/abstract=1127888; e Selinger E, Hartzog W (2017) Obscurity and Privacy, *Spaces for the Future [*Obscuridade e privacidade*, espaços para o futuro]: A Companion to Philosophy of Technology* [um companheiro para a filosofia da tecnologia]:, eds Pitt J, Shew A (Taylor & Francis, Nova York, NY), Capítulo 12, 1ª Ed. https://doi.org/10.4324/9780203735657.

1.1 Visão Geral do Privacy Framework

Conforme demonstrado na **Figura 1**, o Privacy Framework é composto por três partes: Core (núcleo), Profiles (perfis), e Implementation Tiers (níveis de implementação). Cada componente reforça como as organizações gerenciam o risco de privacidade por meio da conexão entre a empresa e os responsáveis pela missão, funções e responsabilidades organizacionais e atividades de proteção à privacidade. Como explicado ainda na seção 2:

Figura 1: Núcleo, Perfis e Níveis de Implementação

- O *Núcleo* é um conjunto de atividades de proteção à privacidade que permite comunicar atividades e resultados de proteção à privacidade e o impacto em toda a organização, desde o nível executivo até o nível de implementação/operações O Núcleo é dividido ainda em categorias-chave e subcategorias—que são resultados discretos—para cada função.
- Um *Perfil* representa as atividades de privacidade atuais de uma organização ou os resultados desejados. Para desenvolver um perfil, uma organização deve analisar todos os resultados e atividades do núcleo para determinar quais são as que merecem maior enfoque com base nos impulsionadores dos negócios e da missão, qual a função do ecossistema de processamento de dados e quais são as necessidades de privacidade dos indivíduos. Uma organização pode criar ou acrescentar Funções, Categorias e Subcategorias, conforme necessário. Os perfis podem ser usados para identificar oportunidades para melhorar a postura de privacidade, comparando um perfil "atual" (a situação de "como ele é") com um perfil "alvo" (como ele deveria "ser"). Os perfis podem ser usados para realizar autoavaliações e se comunicar dentro de uma organização, ou entre organizações, sobre como os riscos de privacidade estão sendo gerenciados.
- *Os Níveis de Implementação* ("Níveis") oferecem um ponto de referência sobre como uma organização enxerga o risco de privacidade e se ela tem processos e recursos suficientes para gerenciar esse risco. Os níveis refletem uma sequência de respostas informais e reativas a uma série de abordagens que são ágeis e contêm informações sobre risco. Ao selecionar os níveis, uma organização deve considerar o seu perfil-alvo e como esse alvo pode ser atingido quando a organização é beneficiada ou prejudicada pelas suas práticas atuais de gestão de risco. Ela deve também considerar o grau de integração do risco de privacidade em seu portfólio de gestão de riscos corporativos, suas relações com o ecossistema de processamento de dados, e como é a atual composição da força de trabalho e programas de treinamento.

1.2 Gerenciamento de Riscos de Privacidade

Embora algumas organizações tenham uma compreensão profunda sobre o *gerenciamento dos riscos de privacidade,*elas ainda não possuem um entendimento básico sobre muitos aspectos relativos a este tópico.[5] Para que haja uma compreensão mais ampla, esta seção abrange conceitos e considerações que as organizações podem usar para desenvolver, melhorar ou comunicar o gerenciamento de riscos de privacidade. O Apêndice D fornece informações adicionais sobre as principais práticas de gerenciamento de riscos de privacidade.

1.2.1 Gerenciamento de riscos de segurança cibernética e privacidade

Desde o seu lançamento em 2014, o Cybersecurity Framework tem ajudado as organizações a comunicar e gerenciar o risco de segurança cibernética. [1] Mesmo sabendo que o gerenciamento do risco de segurança cibernética contribui para o gerenciamento do risco de privacidade, isso não é suficiente, pois os riscos de privacidade também podem surgir de fontes não relacionadas aos *incidentes de cibersegurança*, conforme ilustrado na **Figura 2.** Ter uma compreensão geral das diferentes origens da segurança cibernética e dos riscos de privacidade é importante para determinarmos quais são as soluções mais eficazes para solucionarmos tais riscos.

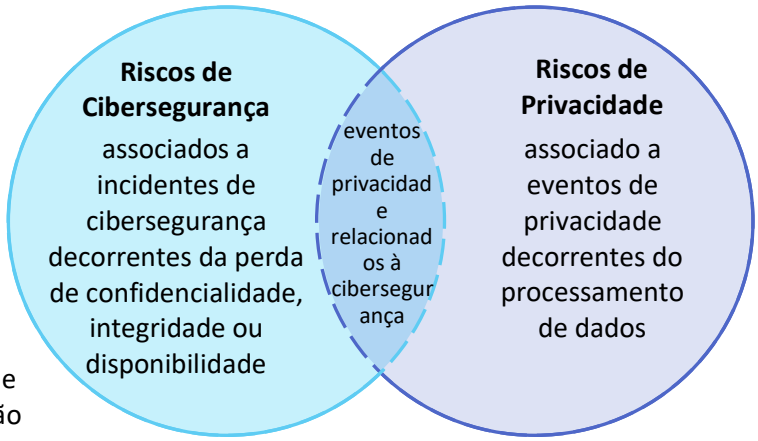

Figura 2: Relação entre risco de segurança cibernética e privacidade

A abordagem do Privacy Framework quanto ao risco de privacidade é considerar os *eventos de privacidade* como sendo problemas potenciais que podem afetar os indivíduos e que são decorrentes de operações de sistemas, produtos ou serviços contendo dados, seja em formato digital ou não digital, no decorrer do ciclo de vida completo, desde a coleta de dados até o descarte.

> ***Ação de Dados***
> Uma operação de ciclo de vida referente a dados, incluindo, dentre outros, coleta, retenção, registro, geração, transformação, uso, divulgação, compartilhamento, transmissão e descarte.
>
> ***Processamento de dados***
> O conjunto coletivo de ações referentes aos dados.

O Privacy Framework descreve as operações de dados no singular, como sendo uma *ação de dados*, e coletivamente, como processamento de dados. Os problemas que os indivíduos possivelmente enfrentem como resultado do processamento de dados podem ser expressos de várias maneiras, porém, o NIST os descreve de formas variadas, como tipos de efeitos que afetam a dignidade - ou seja, constrangimento ou estigmas que levam a danos mais tangíveis, como discriminação, perda econômica, ou dano físico.[6]

A base dos problemas que impactam as pessoas pode variar. Conforme descrito na **Figura 2**, os problemas surgem como um efeito adverso do

[5] Leia a *Análise resumida das respostas do NIST Privacy Framework às solicitações por informações* [2] na pg. 7.

[6] O NIST criou um catálogo ilustrativo de problemas para uso na avaliação de risco de privacidade. Leia *NIST Privacy Risk Assessment Methodology* [Metodologia para Avaliação do Risco de Privacidade do NIST] [3]. Outras organizações talvez tenham criado outras categorias de problemas, ou se referiram a eles como consequências ou danos adversos.

processamento de dados que as organizações executam para cumprir seus objetivos de missão ou negócios. Um exemplo disso, foi o receio de certas comunidades sobre a instalação de "medidores inteligentes" como parte do Smart Grid, um esforço tecnológico nacional para aumentar a eficiência energética.[7] Os medidores tinham a capacidade de coletar, registrar e distribuir informações altamente granulares sobre o uso de eletricidade nas residências, o que, por sua vez, fornecia informações sobre o comportamento das pessoas dentro de suas casas.[8] Os medidores estavam operando conforme planejado, mas o processamento de dados poderia fazer com que as pessoas se sentissem vigiadas.

Em um mundo cada vez mais conectado, alguns problemas podem surgir simplesmente devido às interações dos indivíduos com sistemas, produtos e serviços, mesmo quando os dados que estão sendo processados não estejam diretamente ligados aos indivíduos identificados. Por exemplo, as tecnologias das cidades inteligentes podem ser usadas para alterar ou influenciar o comportamento das pessoas, isto é, para onde ou como se deslocam pela cidade.[9] Problemas também podem surgir quando não mais existe *confidencialidade*, *integridade*, ou *disponibilidade* em algum momento no processamento de dados, como roubo de dados por invasores externos ou o acesso ou uso não autorizado de dados pelos funcionários. **Figura 2** mostra esses tipos de eventos de privacidade relacionados à segurança cibernética como uma sobreposição entre riscos de privacidade e segurança cibernética.

Assim que uma organização conseguir identificar a probabilidade de qualquer problema decorrente do processamento de dados, que o Privacy Framework se refere como sendo uma *ação de dados problemática*, ela poderá avaliar o impacto caso a ação problemática venha a ocorrer. Essa avaliação de impacto é onde o risco de privacidade e o *risco* organizacional se cruzam. As pessoas, seja individualmente ou em grupos (inclusive em camadas da sociedade), passam pela experiência do impacto direto dos problemas. Como resultado dos problemas que as pessoas enfrentam, uma organização pode sofrer impactos, por exemplo, custos decorrentes de não estar em conformidade, perda de receita decorrente do abandono de produtos e serviços pelo cliente, ou danos à sua reputação de marca externa ou cultura interna. As organizações geralmente gerenciam esses tipos de impactos no âmbito do gerenciamento de riscos empresariais. Ao fazer uma conexão dos problemas que os indivíduos enfrentam com os impactos organizacionais identificados, as organizações podem colocar o risco de privacidade em paridade com outros riscos que estão gerenciando em um portfólio mais amplo, assim promovendo tomadas de decisão mais informadas sobre alocação de recursos para fortalecer programas de privacidade. **Figura 3** Ilustra a relação entre risco de privacidade e risco organizacional.

---

[7] Leia, como exemplo, o Relatório Interno ou Interagências do NIST (IR) 7628 Revisão 1 Volume 1, *Guidelines for Smart Grid Cybersecurity (Diretrizes para segurança cibernética de rede inteligente): Volume 1 – Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements (Volume 1 - Estratégia, arquitetura e requisitos de alto nível de segurança cibernética de rede inteligente)*na [4] pg. 26.

[8] Leia NIST IR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* (*Uma introdução à engenharia de privacidade e gerenciamento de risco em sistemas federais*) na [5] pg. 2. Para outros tipos de riscos de privacidade que provocam efeitos adversos em indivíduos que trabalham com processamento de dados, consulte o apêndice E do NIST IR 8062.

[9] Leia Newcombe T (2016) Security, Privacy, Governance Concerns About Smart City Technologies Grow [Preocupações com segurança, privacidade e governança sobre o crescimento das tecnologias da cidade inteligente]. *Government Technology* [Tecnologia Governamental]. Disponível em http://www.govtech.com/Security-Privacy-Governance-Concerns-About-Smart-City-Technologies-Grow.html.

Problema
surge do processamento de dados

Indivíduo
sente o impacto direto (ex: constrangimento, discriminação, perda econômica)

Organização
impacto resultante (ex: abandono pelo cliente, custo de não estar em conformidade, danos à reputação ou cultura

Figura 3: Relação entre risco de privacidade e risco organizacional

1.2.2 Avaliação de risco de privacidade

O gerenciamento de risco de privacidade é um conjunto interorganizacional de processos que ajudam as organizações a entender como os seus sistemas, produtos e serviços podem criar problemas para os indivíduos e como desenvolver soluções eficazes para gerenciar tal risco. *A avaliação de risco de privacidade* é um subprocesso para identifica e avaliar riscos específicos de privacidade. Em termos gerais, as avaliações de risco de privacidade produzem informações que podem ajudar as organizações a ponderar os benefícios e os riscos do processamento de dados, e determinar a resposta apropriada—também referida como proporcionalidade.[10] As organizações podem optar por priorizar e responder ao risco de privacidade de diferentes maneiras, dependendo do impacto potencial para os indivíduos e os impactos resultantes para as organizações. As abordagens de respostas podem ser:[11]

- Mitigar o risco (ex: as organizações podem adotar medidas técnicas e/ou normativas referentes aos sistemas, produtos ou serviços que minimizem o risco a um grau aceitável);
- Transferir ou compartilhar o risco (ex: os contratos representam uma maneira de compartilhar ou transferir riscos para outras organizações, sendo que, os avisos de privacidade e os mecanismos de consentimento são um meio de compartilhar riscos com as pessoas);
- Evitar o risco (ex: as organizações podem determinar que os riscos superam os benefícios e, portanto, abandonam ou encerram o processamento de dados); ou
- Aceitar o risco (ex: as organizações podem determinar que os problemas para os indivíduos são mínimos ou improváveis de ocorrer, portanto, os benefícios superam os riscos, não sendo necessário investir recursos em mitigação).

As avaliações de risco de privacidade são particularmente importantes porque, conforme observado acima, a privacidade é uma condição que oferece salvaguardas a múltiplos valores. Os métodos para salvaguardar esses valores podem diferir, ou além disso, podem estar em conflito uns com os outros. Dependendo dos objetivos de uma organização, caso ela tente alcançar a privacidade desejada limitando a observação, isso pode levar à implementação de medidas como arquiteturas de dados distribuídos ou técnicas criptográficas que reforçam a privacidade e escondem dados até mesmo da organização. Caso a organização esteja também tentando permitir que haja controle individual, essas

[10] Consulte o Comitê Europeu de Proteção de Dados (2019) Necessity & Proportionality [Necessidade & Proporcionalidade]. Disponível em https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en.

[11] Consulte a Publicação Especial NIST (SP) 800-39, *Managing Information Security Risk:* [Gerenciamento de riscos de segurança da informação:] *Organization, Mission, and Information System View* [Organização, missão e visão do sistema de informações] [6].

medidas podem entrar em conflito. Por exemplo, se um indivíduo solicitar acesso aos dados, a organização talvez não consiga produzir os dados se eles tiverem sido distribuídos ou criptografados de maneira que a organização não possa acessar. Avaliações de risco de privacidade podem ajudar uma organização a entender, em um determinado contexto, os valores a serem protegidos, os métodos a serem utilizados e como equilibrar a implementação de diferentes tipos de medidas.

Por fim, avaliações de risco de privacidade ajudam as organizações a distinguir entre risco de privacidade e risco de compliance. Isto é, identificar se o processamento de dados pode criar problemas para os indivíduos, mesmo quando uma organização está em compliance com as leis e regulamentos aplicáveis, podendo ajudar na tomada de decisões éticas referentes ao sistema, produto, ou quanto ao design e implantação de serviços. Mesmo que não haja um padrão objetivo para a tomada de decisões éticas, o padrão deve estar fundamentado nas normas, valores e expectativas jurídicas em determinada sociedade. Isso facilita a otimização dos usos benéficos dos dados, minimizando as consequências adversas quanto à privacidade dos indivíduos e a sociedade como um todo, além de evitar perdas de confiança que prejudicam a reputação das organizações, reduzem o nível de adoção de produtos, ou causam o abandono de produtos e serviços.

Consulte o Apêndice D para obter mais informações sobre os aspectos operacionais da avaliação de risco de privacidade.

1.3 Visão geral do documento

O restante deste documento contém as seguintes seções e apêndices:

- **A Seção 2** descreve os componentes do Privacy Framework: Core (núcleo), Profiles (perfis), e Implementation Tiers (níveis de implementação).
- **A Seção 3** apresenta exemplos de como o Privacy Framework pode ser usado.
- A **seção de referências** lista as referências contidas no documento.
- **O Apêndice A** apresenta o núcleo do Privacy Framework em formato tabular: Funções, Categorias e Subcategorias.
- **O Apêndice B** contém um glossário de termos selecionados.
- **O Apêndice C** lista as siglas usadas neste documento.
- **O Apêndice D** aborda as principais práticas que contribuem para um gerenciamento bem-sucedido dos riscos de privacidade.
- **O Apêndice E** define os níveis de implementação.

2.0 Informações básicas sobre o Privacy Framework

O Privacy Framework oferece uma linguagem comum para que se possa entender, gerenciar e comunicar riscos de privacidade com as partes interessadas internas e externas. Ele é adaptável às funções de qualquer organização no ecossistema de processamento de dados. Ele pode ser usado para ajudar a identificar e priorizar ações que visam reduzir o risco de privacidade, sendo uma ferramenta para alinhar políticas, negócios e abordagens tecnológicas para gerenciar o risco identificado.

2.1 Núcleo

Conforme explicado no Apêndice A, o núcleo fornece um conjunto cada vez mais granular de atividades e resultados que permitem manter um diálogo sobre o gerenciamento do risco de privacidade. Conforme descrito na **Figura 4**, o núcleo é composto por Funções, Categorias e Subcategorias.

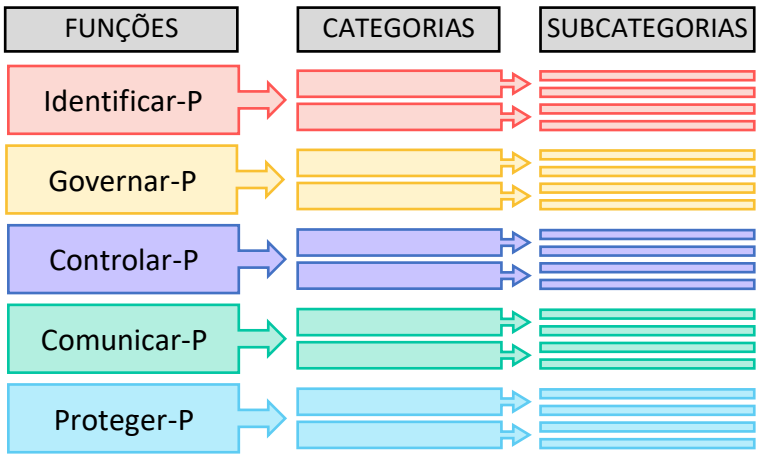

Figura 4: Estrutura do Núcleo do Privacy Framework

Os elementos do núcleo trabalham juntos:

- *As funções* organizam as atividades fundamentais de privacidade em seu mais alto nível. Elas ajudam uma organização a expressar a sua gestão do risco de privacidade, ao entender e gerenciar o processamento de dados, possibilitando decisões concernentes à *gestão de risco*, e ao determinar como interagir com os indivíduos, além de estabelecer melhorias ao aprender com atividades anteriores. As funções não foram criadas para estabelecer um caminho serial de dados ou levar a um estado final estático desejado. Ao contrário, as funções devem ser desempenhadas simultaneamente e continuamente para formar ou melhorar uma cultura operacional que trate da natureza dinâmica do risco de privacidade.
- *As Categorias* são as subdivisões de uma função em grupos de resultados de privacidade intimamente ligados às necessidades programáticas e atividades específicas.
- *As subcategorias* dividem ainda mais uma categoria em resultados específicos de atividades técnicas e/ou de gestão. Elas fornecem um conjunto de resultados que, embora não sejam completos, ajudam a validar o efeito do que foi encontrado em cada categoria.

As cinco funções, Identificar-P Governar-P, Controlar-P, Comunicar-P e Proteger-P, definidas abaixo, podem ser usadas para gerenciar riscos de privacidade decorrentes do processamento de dados.[12] A função Proteger-P é especificamente focada na gestão de riscos dos eventos de privacidade relacionados à cibersegurança (ex: *violação de privacidade*). Embora o Cybersecurity Framework tenha sido criado para cobrir todos os tipos de incidentes de cibersegurança, ele pode ser usado para alavancar mais apoio à gestão de riscos dos eventos de privacidade

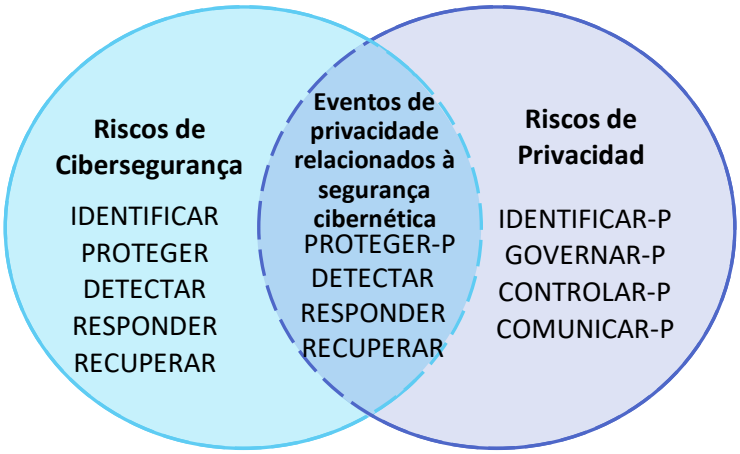

Figura 5: Usando as funções para gerenciar riscos de privacidade e segurança cibernética

[12] O "-P" no final de cada nome da função indica que ela pertence ao Privacy Framework, pois assim não haverá confusão com as Funções do Cybersecurity Framework.

relativos à cibersegurança usando as Funções de Detectar, Responder e Recuperar. Como alternativa, as organizações podem usar todas as cinco funções do Cybersecurity Framework juntamente com Identificar-P, Governar-P, Controlar-P, e Comunicar-P para que os riscos de privacidade e segurança cibernética possam ser abordados coletivamente. **Figura 5** usa o diagrama de Venn na seção 1.2.1 para demonstrar como as funções de ambos os frameworks podem ser usadas em combinações variadas para gerenciar diferentes aspectos dos riscos de privacidade e segurança cibernética. As cinco funções do Privacy Framework são definidas como segue:

- *Identificar P* – Desenvolve o entendimento organizacional para gerenciar riscos de privacidade de indivíduos decorrentes do processamento de dados.

  As atividades na função Identificar-P são fundamentais para o uso eficaz do Privacy Framework. Avaliar as circunstâncias em que os dados são processados, entendendo os interesses de privacidade dos indivíduos que são servidos ou afetados direta ou indiretamente por uma organização, além de realizar avaliações de risco, permite que uma organização entenda o ambiente de negócios em que está funcionando, e identifique e priorize riscos de privacidade.

- *Governar-P* – Desenvolve e implementa a estrutura de governança organizacional para permitir uma compreensão contínua das prioridades de gestão de riscos da organização que são transmitidas pelo risco de privacidade.

  A Função Governar-P é igualmente fundamental, mas se concentra em atividades de nível organizacional, como estabelecer valores e políticas de privacidade organizacional, identificar requisitos legais/regulatórios e entender a *tolerância ao risco* organizacional que permite que uma organização concentre e priorize esforços que sejam consistentes com a sua estratégia de gestão de riscos e necessidades de negócios.

- *Controlar-P* – Desenvolver e implementar atividades adequadas para permitir que organizações ou indivíduos gerenciem dados com granularidade suficiente para gerenciar riscos de privacidade.

  A Função Controlar-P considera o gerenciamento do processamento de dados do ponto de vista da organização e também do indivíduo.

- *Comunicar-P* – Desenvolve e implementa atividades adequadas para permitir que organizações e indivíduos tenham uma compreensão confiável e permaneçam engajados em um diálogo sobre como os dados são processados, além dos riscos de privacidade a eles associados.

  A função Comunicar-P reconhece que tanto as organizações quanto os indivíduos gostariam de saber como os dados são processados para gerenciar o risco de privacidade de forma eficaz.

- *Proteger-P* – Desenvolve e implementa as devidas salvaguardas para o processamento de dados.

  A função Proteger-P abrange a proteção de dados para evitar eventos de privacidade relacionados à cibersegurança e a sobreposição entre privacidade e gerenciamento de riscos de cibersegurança.

2.2 Perfis

Os Perfis são uma seleção de Funções, Categorias e Subcategorias específicas do Núcleo que foram priorizadas por uma organização para auxiliá-la no gerenciamento do risco de privacidade. Os perfis podem ser usados para descrever a situação atual e a situação-alvo desejada para as atividades de privacidade específicas. Um Perfil Atual indica resultados de privacidade que uma organização está conseguindo atualmente, enquanto um Perfil-Alvo indica os resultados necessários para se alcançar os objetivos desejados de gerenciamento de risco de privacidade. As diferenças entre os dois perfis permitem que uma organização identifique lacunas, desenvolva um plano de ação para melhorar e avaliar os recursos que seriam necessários (ex: pessoal, financiamento) para alcançar os resultados de privacidade. Isto forma a base do plano de uma organização para reduzir o risco de privacidade de forma econômica e priorizada. Os perfis também podem auxiliar na comunicação de risco dentro e entre organizações, ajudando as organizações a entender e comparar a situação atual dos resultados de privacidade e a situação que desejam ter efetivamente.

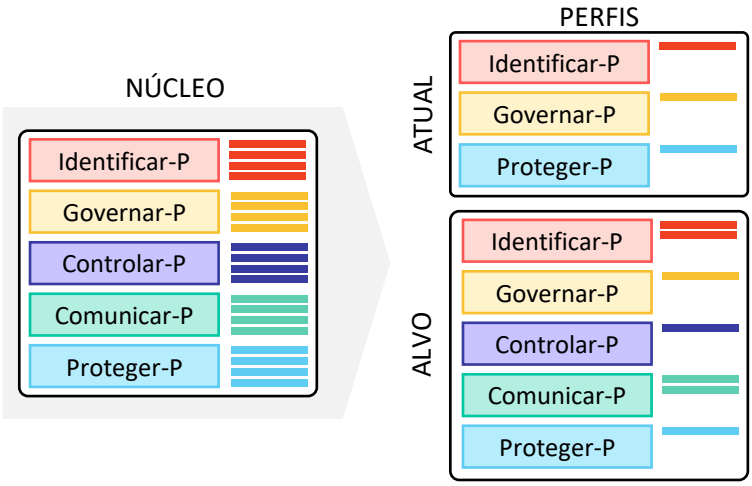

Figura 6: Relação entre núcleo e perfis

O Privacy Framework não prescreve modelos de perfil para permitir flexibilidade na implementação. De acordo com a abordagem baseada em riscos do Privacidade Framework, as organizações talvez não precisem alcançar todos os resultados ou atividades refletidas no núcleo. Ao desenvolver um perfil, a organização pode selecionar ou adaptar as funções, categorias e subcategorias para satisfazer necessidades específicas, incluindo o desenvolvimento das suas próprias funções, categorias e subcategorias para acomodar riscos organizacionais exclusivos. Uma organização determina quais são essas necessidades tendo em mente a sua missão ou objetivos de negócio, valores de privacidade, e tolerância ao risco, funções no ecossistema de processamento de dados ou setor da indústria, requisitos legais/regulatórios e melhores práticas do setor, prioridades de gerenciamento de riscos e recursos, bem como necessidades de privacidade dos indivíduos que são servidos ou afetados direta ou indiretamente pelos sistemas, produtos e serviços da organização.

Conforme ilustrado na **Figura 6**, não existe uma ordem especificada para o desenvolvimento de perfis. Uma organização pode primeiro desenvolver um Perfil-Alvo para focar nos resultados desejados de privacidade, e depois desenvolver um Perfil Atual para identificar lacunas. Alternativamente, uma organização pode começar identificando suas atividades atuais para depois considerar como ajustar essas atividades ao seu Perfil-Alvo. Uma organização pode optar por desenvolver vários perfis para diferentes funções, sistemas, produtos e serviços, ou categorias de indivíduos (ex: funcionários, clientes) para permitir uma melhor priorização das atividades e resultados, já que pode haver diferentes graus de risco à privacidade. Organizações que pertencem a um determinado setor industrial ou que tenham funções semelhantes no ecossistema de processamento de dados podem trabalhar coordenadamente para desenvolver perfis comuns.

2.3 Níveis de implementação

Os níveis oferecem apoio à tomada de decisão organizacional sobre como gerenciar riscos de privacidade levando em conta a natureza de tais riscos gerados pelos sistemas, produtos ou serviços de uma organização, e a suficiência dos processos e recursos que vigoram em uma organização para que ela possa gerenciar os riscos. Ao selecionar os níveis, uma organização deve considerar o seu Perfil-Alvo e como esse alvo pode ser atingido quando a organização é beneficiada ou prejudicada pelas suas práticas atuais de gestão de riscos. Ela deve também considerar o grau de integração do risco de privacidade em seu portfólio de gestão de riscos empresariais, suas relações com o ecossistema de processamento de dados, e a atual composição da força de trabalho e programas de treinamento.

Existem quatro níveis distintos, parcial (nível 1), informado pelo risco (nível 2), repetível (nível 3) e adaptável (nível 4), cujas descrições estão no Apêndice E. Os níveis representam uma progressão, embora ela não seja obrigatória. E embora as organizações do nível 1 provavelmente se beneficiem de uma mudança para o nível 2, nem todas as organizações precisam atingir os níveis 3 e 4 (ou podem se concentrar apenas em certas áreas desses níveis). A progressão para níveis mais altos é adequada quando os processos ou recursos de uma organização em seu nível atual são insuficientes para ajudá-la a gerenciar riscos de privacidade.

Uma organização pode usar os níveis para comunicações internas sobre alocações de recursos necessários para progredir para um nível mais elevado, ou para atingir um benchmark geral para medir o progresso quanto à sua capacidade de gerenciar riscos de privacidade. Uma organização também pode usar os níveis para entender a escala de recursos e processos de outras organizações no ecossistema de processamento de dados e como eles se alinham com as suas prioridades de gerenciamento de riscos de privacidade. No entanto, a implementação do Privacy Framework baseia-se no alcance dos resultados descritos no Perfil-Alvo de uma organização, e não na determinação do nível.

3.0 Como usar o Privacy Framework

Quando o Privacy Framework é usado como uma ferramenta de gerenciamento de risco, ele pode auxiliar uma organização em seu empenho para otimizar o uso benéfico dos dados e o desenvolvimento de sistemas, produtos e serviços inovadores, minimizando consequências adversas para os indivíduos. O Privacy Framework pode ajudar as organizações a responderem à uma pergunta fundamental: "como estamos considerando os impactos aos indivíduos à medida que desenvolvemos nossos sistemas, produtos e serviços?" Para acomodar as necessidades únicas de uma organização, o uso do Privacy Framework torna-se flexível, embora tenha sido conceitualizado para complementar as operações de desenvolvimento de negócios e sistemas vigentes. A decisão sobre como aplicá-lo cabe à organização de implementação. Por exemplo, uma organização pode ter atualmente, processos robustos de gerenciamento de risco de privacidade, mas talvez não esteja usando as cinco funções do núcleo como uma maneira simplificada de analisar e articular a existência de lacunas. Alternativamente, uma organização que busca estabelecer um programa de privacidade pode usar as categorias e subcategorias do núcleo como referência. Outras organizações podem comparar os perfis ou níveis para alinhar prioridades de gerenciamento de risco de privacidade em diferentes funções no ecossistema de processamento de dados. A variedade de maneiras pelas quais as organizações podem usar o Privacy Framework não deve promover a ideia de que o "compliance com o Privacy Framework" é um conceito generalizado que pode ser usado externamente como referência. As seguintes subseções apresentam algumas opções para uso do Privacy Framework.

3.1 Mapeamento para referências informativas

As referências informativas representam mapeamentos para as subcategorias que oferecem suporte de implementação, incluindo mapeamentos de ferramentas, orientação técnica, normas, leis, regulamentos e melhores práticas. As descrições comparativas que mapeiam as provisões sobre normas, leis e regulamentos referentes às subcategorias podem ajudar as organizações a determinar quais são as atividades ou resultados que devem ser priorizados para facilitar o compliance. O Privacy Framework é neutro em tecnologia, mas apoia a inovação tecnológica já que qualquer organização ou setor da indústria pode desenvolver esses mapeamentos, conforme a tecnologia e as necessidades de negócios relacionados evoluem. Ao depender de normas, diretrizes e práticas baseadas em consenso, as ferramentas e métodos disponíveis para alcançar resultados positivos de privacidade podem ganhar escala, atravessando fronteiras e acomodando a natureza global dos riscos à privacidade. O uso de normas existentes e emergentes viabilizará economias de escala e impulsionará o desenvolvimento de sistemas, produtos e serviços que atendam às necessidades de mercado identificadas, sem perder de vistas as necessidades de privacidade dos indivíduos.

Lacunas nos mapeamentos também podem ser usadas para identificar onde implementar normas, diretrizes e práticas adicionais ou modificadas para ajudar uma organização a abordar necessidades emergentes. Uma organização que tenha implementado uma determinada subcategoria, ou desenvolvido uma nova , pode perceber que a orientação não é suficiente para determinada atividade ou resultado relacionado. Para atender a essa necessidade, uma organização pode colaborar com líderes em tecnologia e/ou órgãos de padrão da indústria para elaborar, desenvolver e coordenar normas, diretrizes e práticas.

Um repositório de referências informativas pode ser encontrado em https://www.nist.gov/privacy-framework. Esses recursos podem servir de referência para as organizações usarem o Privacy Framework e conseguirem adotar as melhores práticas de privacidade.

3.2 Aumentando o nível de responsabilização

A responsabilização é geralmente considerada um princípio fundamental em se tratando de privacidade, embora conceitualmente não seja usada exclusivamente para a privacidade.[13] A responsabilização ocorre em toda a organização, e pode ser expressa em vários graus de abstração, por exemplo, como valor cultural, como políticas e procedimentos de governança, ou como relações de rastreabilidade entre os *requisitos de privacidade* e os *controles*. O gerenciamento de risco de privacidade pode ser um meio de alavancar a responsabilização em todos os níveis organizacionais, conforme a empresa faz a conexão entre executivos seniores, que podem comunicar os valores de privacidade da organização e a tolerância ao risco, e os que atuam no nível de gerência de negócios/processos, que podem colaborar no desenvolvimento e implementação de políticas e procedimentos de governança, respaldados nos valores de privacidade organizacional. Essas políticas e procedimentos podem então ser comunicados aos que atuam no nível de implementação/operações, e que colaboram na definição dos requisitos de privacidade que promovem a expressão das políticas e procedimentos nos sistemas, produtos e serviços da organização. O pessoal que trabalha no setor de implementação/operações também seleciona, implementa e avalia controles como sendo medidas técnicas e normativas que atendem aos requisitos de privacidade, bem como relatam o progresso feito, lacunas e deficiências, gerenciamento de incidentes e riscos de privacidade (que mudam sempre), para que as pessoas que atuam no nível

Figura 7: Colaboração abstrata e fluxos de comunicação dentro de uma organização

[13] Leia, por ex: Organização para a Cooperação e Desenvolvimento Econômico (OCDE) (2013) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [Diretrizes da OCDE sobre a proteção da privacidade e fluxos transfronteiriços de dados pessoais], disponível em https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) (2011) ISO/IEC 29100:2011 – *Information technology – Security techniques – Privacy framework* [Organização Internacional para a Padronização (ISO)/Comissão Eletrotécnica Internacional (CEI) (2011) ISO/IEC 29100:2011 – Tecnologia da informação – Técnicas de segurança – Estrutura de privacidade] (ISO, Genebra, Suíça), disponível em https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip; e Alliance of Automobile Manufacturers, Inc., Association of Global Automakers, Inc. [Aliança dos Fabricantes de Automóveis, Inc., Associação de Montadoras Globais, Inc.] (2014) *Consumer Privacy Protection Principles:*[Princípios de Proteção à Privacidade do Consumidor:] *Privacy Principles for Vehicle Technologies and Services* [Princípios de Privacidade para Tecnologias e Serviços de Veículos] disponível em https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf.

gerencial de negócios/processos e os executivos seniores possam melhor entender e responder adequadamente.

Figura 7 fornece uma representação gráfica dessa colaboração e comunicação bidirecional, e como os elementos do Privacy Framework podem ser incorporados para facilitar o processo. Portanto, as organizações podem usar o Privacy Framework como uma ferramenta de suporte ao senso de responsabilização. Elas também podem usar a Estrutura de Privacidade juntamente com outras estruturas e orientações que fornecem práticas adicionais para alcançar o nível de responsabilização desejado dentro e entre as organizações.[14]

3.3 Como estabelecer ou aprimorar um programa de privacidade

Usando modelos de frases simples, como "preparar, apontar, já" o Privacy Framework serve de suporte para a criação de um novo programa de privacidade ou para a melhoria a um programa existente. Conforme a organização atravessa essas fases, ela poderá usar referências informativas para orientar sobre como priorizar e alcançar os resultados. Leia a seção 3.1 para obter mais informações sobre referências informativas. Ademais, um repositório pode ser encontrado em https://www.nist.gov/privacy-framework.

Preparar

Para que haja uma gestão eficaz de riscos de privacidade, a organização precisa entender a sua missão ou ambiente de negócios, bem como o seu ambiente jurídico, tolerância ao risco, quais os riscos de privacidade gerados pelos sistemas, produtos e serviços, e o papel que ela exerce no ecossistema de processamento de dados. Uma organização pode usar as funções Identificar-P e Governar-P para "se preparar" analisando as categorias e subcategorias, para depois começar a desenvolver o seu Perfil Atual e o Perfil-Alvo.[15] Para que uma organização tenha uma base sólida para completar os perfis na categoria "estabelecer", ela deve estar atenta às atividades e resultados, isto é, como estabelecer valores e políticas de privacidade organizacional, determinar e expressar tolerância aos riscos organizacionais, e realizar avaliações de risco de privacidade (consulte o Apêndice D para obter mais informações sobre avaliações de risco de privacidade).

Um método simplificado para criar ou aprimorar um programa de privacidade

Preparar: usado com as Funções Identificar-P e Governar-P para ficar "pronto".

Apontar: "apontar" um plano de ação com base nas diferenças entre o perfil atual e o Perfil-Alvo.

Já: "vá" adiante com a implementação do plano de ação.

Apontar

Uma organização completa o seu Perfil Atual, indicando quais os resultados da Categoria e Subcategoria das funções restantes estão sendo alcançados. Se um resultado for parcialmente alcançado, observar esse fato ajudará a validar as etapas subsequentes, fornecendo informações de linha de base. Após

[14] Leia, por ex:, NIST SP 800-37, Rev. 2, *Management Framework for Information Systems and Organizations:* [Estrutura de Gerenciamento de Risco para Sistemas de Informação e Organizações]: *A System Life Cycle Approach for Security and Privacy* [Uma abordagem do ciclo de vida do sistema para segurança e privacidade] [7]; e Organization for the Advancement of Structured Information Standards [Organização para o Avanço das Normas de Informação Estruturada] (OASIS) (2016) Privacy Management Reference Model and Methodology [Modelo de Referência de Gestão de Privacidade e Metodologia] (PMRM) Versão 1.0, https://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.pdf.

[15] Para informações adicionais, leia a etapa "preparar", Seção 3.1, NIST SP 800-37, Rev. 2 [7].

estar informada das atividades nas categorias Identificar e Governar, como valores e políticas de privacidade organizacional, tolerância ao risco organizacional e resultados de avaliação do risco de privacidade, uma organização pode completar o Perfil-Alvo, focada na avaliação das Categorias e Subcategorias que descrevem os resultados de privacidade por ela desejados. Uma organização também pode desenvolver suas próprias funções, categorias e subcategorias para abordar riscos organizacionais singulares. Ao criar o seu Perfil-Alvo a empresa também pode considerar influências e requisitos das partes interessadas externas, como clientes e parceiros de negócios. Uma organização pode desenvolver vários perfis para dar sustentação a diferentes linhas de negócios ou processos, que podem ter diferentes necessidades de negócios e, consequentemente, diferentes tolerâncias ao risco.

Uma organização compara o Perfil Atual e o Perfil-Alvo para identificar lacunas. Em seguida, cria um plano de ação priorizado para eliminar as lacunas - o plano deve refletir os determinantes da missão, custo-benefício e riscos - para que a empresa possa atingir os resultados do Perfil-Alvo. Uma organização que usa o Cybersecurity Framework e o Privacy Framework conjuntamente, pode desenvolver planos de ação integrados. Depois disso, a empresa determina os recursos necessários, incluindo as necessidades de financiamento e mão-de-obra para fechar as lacunas, o que pode esclarecer qual o Nível adequado a ser selecionado. Quando a organização usa os Perfis dessa maneira ela se sente incentivada a tomar decisões informadas sobre atividades de privacidade, o que valida o gerenciamento de riscos e permite que a organização execute melhorias direcionadas e economicamente viáveis.

Já

Juntamente com o plano de ação "estabelecer", uma organização deve priorizar quais as medidas a serem tomadas para fechar as lacunas, devendo depois ajustar as suas práticas de privacidade atuais para atingir o Perfil-Alvo.[16]

Uma organização pode passar por todas as fases de uma maneira não sequencial, conforme necessário, para que haja avaliação e melhoria contínuas da sua postura de privacidade. Por exemplo, uma organização pode determinar que a repetição mais frequente da fase Preparar provoca uma melhoria na qualidade das avaliações de risco de privacidade. Além disso, uma organização pode monitorar o progresso por meio de atualizações iterativas do Perfil Atual ou do Perfil-Alvo para se ajustar às mudanças de riscos, depois comparando o Perfil Atual com o Perfil-Alvo.

3.4 Aplicação ao ciclo de vida de desenvolvimento de sistemas

O Perfil-Alvo pode estar alinhado ao ciclo de vida de desenvolvimento de sistemas (SDLC) no que se refere às fases de planejamento, design, construção/compra, implantação, operação e desativação para apoiar a obtenção dos resultados de privacidade que foram priorizados.[17] Começando com a fase de planejamento, os resultados de privacidade priorizados podem ser transformados em recursos e requisitos de privacidade para o sistema, entendendo que os requisitos provavelmente evoluirão durante o restante do ciclo de vida do sistema. Um marco importante na fase de design é validar se os recursos e requisitos de privacidade correspondem às necessidades e tolerância ao risco de uma organização, conforme identificado no Perfil-Alvo. Este mesmo Perfil-Alvo pode servir como uma lista interna que pode ser avaliada durante a implantação do sistema, para verificar se todos os recursos e requisitos de privacidade foram efetivamente implementados. Os resultados de privacidade que foram

[16] Nist SP 800-37, Rev. 2 [7] fornece informações adicionais sobre as etapas a serem executadas no plano de ação, incluindo a seleção, implementação e avaliação do controle, para fechar todas as lacunas.

[17] Dentro do SDLC, as organizações podem empregar uma variedade de metodologias de desenvolvimento (ex: em cascata, espiral ou ágil).

identificados pelo uso do Privacy Framework devem então servir de base para o funcionamento contínuo do sistema. Isso inclui reavaliações ocasionais, capturando os resultados em um Perfil Atual, para verificar se os recursos e requisitos de privacidade ainda estão sendo atendidos.

As avaliações de risco de privacidade geralmente se concentram no ciclo de vida dos dados e nos estágios pelos quais os dados passam, geralmente caracterizados como criação ou coleta, processamento, disseminação, uso, armazenamento e descarte, incluindo destruição e exclusão. Alinhar o SDLC e o ciclo de vida dos dados, identificando e entendendo como os dados são processados durante todas as etapas do SDLC, ajuda as organizações a melhor gerenciar os riscos de privacidade e orienta na seleção e implementação de controles para atender aos requisitos de privacidade.

3.5 Utilização dentro do ecossistema de processamento de dados

Um fator-chave na gestão do risco de privacidade é o papel de uma entidade no ecossistema de processamento de dados, o que pode afetar não apenas suas obrigações legais, mas também as medidas que ela pode tomar para gerenciar o risco de privacidade. Conforme descrito na **Figura 8**, o ecossistema de processamento de dados abrange uma variedade de entidades e funções que podem ter relacionamentos complexos e multidirecionais entre si e com os indivíduos. A complexidade pode aumentar quando as entidades são suportadas por uma cadeia de entidades; por exemplo, os provedores de serviços podem ser suportados por uma série de provedores de serviços, ou os fabricantes podem ter vários fornecedores de componentes. **Figura 8** exibe entidades como tendo funções distintas, mas algumas podem ter várias funções, como uma organização que fornece serviços a outras organizações e fornece produtos de varejo aos consumidores. As funções na **Figura 8** têm a intenção de ser classificações abstratas. Na prática, as funções de uma entidade podem ser legalmente codificadas - por exemplo, algumas leis classificam as organizações como controladoras ou processadoras de dados - ou as classificações podem ser derivadas de designações de setores da indústria.

Figura 8: Relacionamentos do ecossistema de processamento de dados

Quando uma entidade desenvolve um ou mais perfis relevantes para as suas funções, ela pode optar por usar o Privacy Framework como orientação para gerenciar o risco de privacidade, não apenas em relação às suas próprias prioridades, mas também em relação ao impacto que essas medidas podem ter na gestão de risco de privacidade de outras entidades dentro do ecossistema de processamento de dados. Por exemplo:

- Uma organização que toma decisões sobre como coletar e usar dados sobre indivíduos pode usar um Perfil para expressar requisitos de privacidade a um provedor de serviços externo (ex: um provedor de nuvem para o qual está exportando dados); o provedor de serviços externos

que processa os dados pode usar o seu Perfil para demonstrar as medidas que tem adotado para processar dados em consonância com as obrigações contratuais.

- Uma organização pode expressar sua postura de privacidade por meio de um Perfil Atual para relatar resultados ou para compará-los com os requisitos de aquisição.
- Um setor da indústria pode estabelecer um Perfil comum que pode ser usado pelos membros que integram o setor para customizar os seus próprios Perfis.
- Um fabricante pode usar um Perfil-Alvo para determinar os recursos a serem integrados em seus produtos, de maneira que seus clientes comerciais possam, por sua vez, atender às necessidades de privacidade dos seus usuários finais.
- Um desenvolvedor pode usar um Perfil-Alvo para criar o design de um aplicativo que incorpora proteções de privacidade quando usado em ambientes de sistemas de outras organizações.

O Privacy Framework fornece uma linguagem comum para comunicar requisitos de privacidade com entidades dentro do ecossistema de processamento de dados. A necessidade desse tipo de comunicação torna-se ainda mais importante quando o ecossistema de processamento de dados ultrapassa fronteiras nacionais, como acontece com as transferências internacionais de dados. As práticas organizacionais que oferecem suporte à comunicação podem ser:

- Determinar os requisitos de privacidade;
- Implementar requisitos de privacidade por meio de acordos formais (ex: contratos, estruturas de múltiplas partes interessadas);
- Comunicar como esses requisitos de privacidade serão verificados e validados;
- Verificar se os requisitos de privacidade estão sendo atendidos por meio de uma variedade de metodologias de avaliação;
- Governar e gerenciar as atividades acima.

3.6 Decisões informadas sobre compras

Visto que um Perfil Atual ou Perfil-Alvo pode ser usado para gerar uma lista priorizada de requisitos de privacidade, os mesmos Perfis também podem ser usados para decisões informadas sobre a compra de produtos e serviços. Ao selecionar primeiramente os resultados relevantes para cumprir os objetivos de privacidade, uma organização pode então avaliar os sistemas, produtos e serviços dos parceiros em relação a esses resultados. Por exemplo, se um dispositivo está sendo comprado para monitoramento ambiental de uma floresta, a *gerenciabilidade* pode ser importante para apoiar os recursos e minimizar o processamento de dados sobre pessoas que usam a floresta, o que deve orientar uma avaliação do fabricante em relação às subcategorias aplicáveis do Núcleo (ex: CT.DP-P4: configurações de sistemas ou dispositivos permitem a coleta seletiva ou divulgação de *elementos de dados*).

Em determinadas circunstâncias, talvez não seja possível impor um conjunto de requisitos de privacidade ao fornecedor, nesse caso, o objetivo deve ser optar pela melhor decisão de compra entre vários fornecedores mediante uma lista detalhada de requisitos de privacidade. Muitas vezes, isso significa ter que sopesar, comparando vários produtos ou serviços com as lacunas identificadas no Perfil. Se o sistema, produto ou serviço adquirido não atender a todos os objetivos descritos no Perfil, a organização poderá resolver o risco residual adotando medidas de mitigação ou outras abordagens de gerenciamento.

Referências

[1] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. [Instituto Nacional de Normas e Tecnologia (2018) Guia para Melhorar a Segurança Cibernética da Infraestrutura Crítica. Versão 1.1] (Instituto Nacional de Normas e Tecnologia, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[2] National Institute of Normas and Technology (2019) Summary Analysis of the Responses to the NIST Privacy Framework Request for Information. [Instituto Nacional de Normas e Tecnologia (2019) Análise resumida das respostas à solicitação de informações sobre o NIST Privacy Framework]. (Instituto Nacional de Normas e Tecnologia, Gaithersburg, MD). https://www.nist.gov/sites/default/files/documents/2019/02/27/rfi_response_analysis_privacyframework_2.27.19.pdf

[3] National Institute of Standards and Technology (2019) NIST Privacy Risk Assessment Methodology (PRAM). [Instituto Nacional de Normas e Tecnologia (2019) NIST - Metodologia de Avaliação de Risco de Privacidade (PRAM)]. (Instituto Nacional de Normas e Tecnologia, Gaithersburg, MD). https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources

[4] The Smart Grid Interoperability Panel—Smart Grid Cybersecurity Committee (2014) Guidelines for Smart Grid Cybersecurity: [O Painel de Interoperabilidade da Rede Inteligente — Comitê de Cibersegurança de Rede Inteligente (2014) Diretrizes para Cibersegurança de Rede Inteligente:] Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements. [Volume 1 - Estratégia, Arquitetura e Requisitos de Alto nível de Segurança Cibernética da Rede Inteligente]. (Instituto Nacional de Normas e Tecnologia, Gaithersburg, MD), Relatório Interno ou Interagências do NIST (IR) 7628, Rev. 1, Vol. 1. https://doi.org/10.6028/NIST.IR.7628r1

[5] Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. [Uma Introdução à Engenharia de Privacidade e Gestão de Riscos em Sistemas Federais]. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), Relatório Interno ou Interagências do NIST (IR) 8062. https://doi.org/10.6028/NIST.IR.8062

[6] Joint Task Force Transformation Initiative (2011) Managing Information Security Risk: [Iniciativa de Transformação da Força Tarefa Conjunta (2011) Gerenciando o Risco de Segurança da Informação]: Organization, Mission, and Information System View. [Organização, Missão e Visão do Sistema de Informação]. (Instituto Nacional de Normas e Tecnologia, Gaithersburg, MD). Publicação Especial do NIST (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39

[7] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: [Força Tarefa Conjunta (2018) Estrutura de Gestão de Risco para Sistemas de Informação e Organizações]: A System Life Cycle Approach for Security and Privacy. [Uma Abordagem do Ciclo de Vida do Sistema para Segurança e Privacidade]. (Instituto Nacional de Normas e Tecnologia, Gaithersburg, MD), Publicação Especial do NIST (SP) 800-37 Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[8] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. [Diretrizes para Identidade Digital]. (Instituto Nacional de Normas e Tecnologia, Gaithersburg, MD), Publicação Especial do NIST (SP) 800-63-3, inclui atualizações a partir de 1º de dezembro de 2017. https://doi.org/10.6028/NIST.SP.800-63-3

[9] Office of Management and Budget (2017) Preparing for and Responding to a Breach of Personally Identifiable Information [Escritório de Gestão e Orçamento (2017) Como estar preparado para responder a uma violação de informações pessoalmente identificáveis]. (Casa Branca,

Washington, DC), OMB Memorando M-17-12, 3 de janeiro de 2017. Disponível em https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf

[10] Joint Task Force Transformation Initiative (2013) Security and Privacy Controls for Federal Information Systems and Organizations. [Iniciativa de Transformação da Força Tarefa Conjunta (2013) Segurança e Controles de Privacidade para Organizações e Sistemas de Informação Federais]. (Instituto Nacional de Padrões e Tecnologia, Gaithersburg, MD), Publicação Especial do NIST (SP) 800-53, Rev. 4, inclui atualizações a partir de 22 de janeiro de 2015. https://doi.org/10.6028/NIST.SP.800-53r4

[11] Grassi PA, Lefkovitz NB, Nadeau EM, Galluzzo RJ, Dinh AT (2018) Attribute Metadata: [Atributo Metadata]: A Proposed Schema for Evaluating Federated Attributes. [Um Esquema Proposto para Avaliar Atributos Federados]. (Instituto Nacional de Normas e Tecnologia, Gaithersburg, MD), Relatório Interno ou Interagências do NIST (IR) 8112. https://doi.org/10.6028/NIST.IR.8112

[12] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. [Iniciativa de Transformação da Força Tarefa Conjunta (2012) Guia para a Realização de Avaliações de Risco. (Instituto Nacional de Normas e Tecnologia, Gaithersburg, MD), Publicação Especial do NIST (SP) 800-30 Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

[13] "Definições", Título 44 do *Código dos EUA*, Seção 3542. Edição de 2011 https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542

Apêndice A: Núcleo do Privacy Framework

Este apêndice apresenta o Núcleo: uma tabela de funções, categorias e subcategorias que descrevem atividades e resultados específicos que podem dar suporte ao gerenciamento de riscos de privacidade quando sistemas, produtos e serviços estão processando dados.

Nota aos usuários

Abordagem baseada em risco:

- **O Núcleo não é uma lista de verificação de ações a serem executadas. Uma organização seleciona subcategorias consistentes com a sua estratégia de risco para proteger a privacidade dos indivíduos, conforme observado nas declarações de categoria.** Uma organização pode não precisar alcançar todos os resultados ou atividades refletidas no Núcleo. Espera-se que uma organização use os Perfis para selecionar e priorizar as funções, categorias e subcategorias que melhor atendam às suas necessidades específicas, considerando objetivos, funções no ecossistema de processamento de dados ou setor industrial, requisitos legais/regulamentares e melhores práticas do setor, prioridades de gerenciamento de risco e as necessidades de privacidade dos indivíduos que são direta ou indiretamente servidos ou afetados pelos sistemas, produtos ou serviços de uma organização.
- Não é obrigatório alcançar um resultado na íntegra. Uma organização pode usar os seus Perfis para expressar a realização parcial de um resultado, pois nem todos os aspectos de um resultado podem ser relevantes para a gestão do risco de privacidade da organização, ou ela pode usar um Perfil-Alvo para expressar um aspecto de um resultado que presentemente ela não tenha a capacidade de alcançar.
- Talvez seja necessário considerar a combinação de vários resultados para gerenciar adequadamente o risco de privacidade. Por exemplo, uma organização que responde às solicitações dos indivíduos para acesso aos dados pode selecionar a Subcategoria CT.DM-P1: "Os elementos dos dados podem ser acessados para revisão", e selecionar também a categoria "Gerenciamento de Identidade, Autenticação e Controle de Acesso" (RP. AC-P), para garantir que apenas o indivíduo a quem os dados pertencem tenha acesso.

Implementação: O formato tabular do Núcleo não tem a intenção de sugerir uma ordem de implementação específica ou insinuar que existe grau de importância entre as Funções, Categorias e Subcategorias. A implementação pode ser não sequencial, simultânea ou iterativa, dependendo da etapa do SDLC, do status do programa de privacidade, da escala da força de trabalho ou das funções de uma organização no ecossistema de processamento de dados. Além disso, o Núcleo não é exaustivo - ele é extensível, permitindo que organizações, setores e outras entidades adaptem ou acrescentem funções, categorias e subcategorias aos seus Perfis.

Funções:

- **Funções do ecossistema:** O Núcleo foi criado para ser usado por qualquer organização ou entidade, independentemente das suas funções no ecossistema de processamento de dados. Embora o Privacy Framework não classifique as funções do ecossistema, uma organização deve analisar o Núcleo do seu ponto de vista no ecossistema. As funções de uma organização podem ser legalmente codificadas — por exemplo, algumas leis classificam as organizações como controladoras de dados ou processadoras de dados — ou as classificações podem ser derivadas de designações do setor. Como os elementos principais não são atribuídos pela função do

ecossistema, uma organização pode usar os Perfis para selecionar Funções, Categorias e Subcategorias relevantes para as suas funções.

- **Funções organizacionais:** Diferentes partes da força de trabalho de uma organização podem assumir a responsabilidade por diferentes categorias ou subcategorias. Por exemplo, o departamento jurídico pode ser responsável pela realização de atividades em "Políticas, Processos e Procedimentos de Governança", enquanto o departamento de TI trabalha em "Inventário e Mapeamento". O ideal é que o Núcleo incentive a colaboração entre organizações para desenvolver Perfis e alcançar resultados.

Escalabilidade: Certos aspectos dos resultados podem ser formulados de forma ambígua. Por exemplo, os resultados podem incluir termos como "comunicado" ou "divulgado" sem indicar para quem as comunicações ou divulgações estão sendo feitas. A ambiguidade é intencional para permitir que uma ampla gama de organizações com diferentes casos de uso determine o que é adequado ou necessário em um determinado contexto.

Repositório de recursos: Recursos autônomos que podem fornecer mais informações sobre como priorizar ou obter resultados podem ser encontrados em https://www.nist.gov/privacy-framework.

Alinhamento com o Cybersecurity Framework:

- Conforme observado na seção 2.1, as organizações podem usar as cinco funções do Privacy Framework - Identificar-P, Governar-P, Controlar-P, Comunicar-P e Proteger-P - para gerenciar os riscos de privacidade decorrentes do processamento de dados. O Proteger-P está especificamente focado no gerenciamento de riscos associados a eventos de privacidade relacionados à segurança (ex: violações de privacidade). Para apoiar ainda mais o gerenciamento de riscos associados a eventos de privacidade relacionados à segurança, as organizações podem optar por usar as funções de Detectar, Responder e Recuperar do Cybersecurity Framework. Por esse motivo, essas funções estão incluídas na **Tabela 1,** mas estão acinzentadas. Alternativamente, as organizações podem usar todas as cinco Funções do Cybersecurity Framework juntamente com Identificar-P, Governar-P, Controlar-P e Comunicar-P para abordar coletivamente os riscos de privacidade e de segurança. Veja a **Figura 5** para um exemplo ilustrado de como as Funções de ambas as estruturas podem ser usadas em combinações variadas para gerenciar diferentes aspectos dos riscos de privacidade e de segurança cibernética.
- Certas Funções, Categorias ou Subcategorias podem ser idênticas ou foram adaptadas do Cybersecurity Framework. A legenda abaixo pode ser usada para identificar essa relação na **Tabela 2**. Uma descrição comparativa completa entre as duas estruturas pode ser encontrada no repositório de recursos em https://www.nist.gov/privacy-framework.

A Função, Categoria ou Subcategoria se alinha com o Cybersecurity Framework, mas o texto foi adaptado para o Privacy Framework.

A Categoria ou Subcategoria é idêntica ao Cybersecurity Framework.

Identificadores do Núcleo: Para facilitar o uso, cada componente do Núcleo recebe um identificador exclusivo. Cada Função e Categoria possui um identificador alfabético exclusivo, conforme mostrado na **Tabela 1**. As subcategorias dentro de cada categoria tem um número adicionado ao identificador alfabético - o identificador exclusivo para cada Subcategoria está incluído na **Tabela 2**.

Tabela 1: Identificadores exclusivos das categorias e funções do Privacy Framework

Identificador exclusivo da função	Função	Identificador exclusivo da categoria	Categoria
ID-P	Identificar-P	ID.IM-P	Inventário e mapeamento
		ID.BE-P	Ambiente de negócios
		ID.RA-P	Avaliação de risco
		ID.DE-P	Gestão de riscos do ecossistema de processamento de dados
GV-P	Governar-P	GV.PO-P	Normas, processos e procedimentos de governança
		GV.RM-P	Estratégia de gestão de riscos
		GV.AT-P	Conscientização e treinamento
		GV.MT-P	Monitoramento e revisão
CT-P	Controlar-P	CT.PO-P	Políticas, processos e procedimentos de processamento de dados
		CT.DM-P	Gerenciamento do processamento de dados
		CT.DP-P	Processamento desassociado
CM-P	Comunicar-P	CM.PO-P	Normas, processos e procedimentos de comunicação
		CM.AW-P	Conscientização sobre processamento de dados
PR-P	Proteger-P	PR.PO-P	Normas, processos e procedimentos de proteção de dados
		PR.AC-P	Controle de acesso, autenticação e gerenciamento de identidade
		PR.DS-P	Segurança de dados
		PR.MA-P	Manutenção
		PR.PT-P	Tecnologia protetiva
DE	Detectar	DE.AE	Anomalias e eventos
		DE.CM	Monitoramento contínuo de segurança
		DE.DP	Processos de detecção
RS	Responder	RS.RP	Planejamento de resposta
		RS.CO	Comunicações
		RS.AN	Análise
		RS.MI	Mitigação
		RS.IM	Melhorias
RC	Recuperar	RC.RP	Planejamento de recuperação
		RC.IM	Melhorias
		RC.CO	Comunicações

Tabela 2: Núcleo do Privacy Framework

Função	Categoria	Subcategoria
IDENTIFICAR-P (ID-P): Desenvolver um entendimento organizacional para gerenciar o risco de privacidade para indivíduos, decorrentes do processamento de dados.	**Inventário e mapeamento (ID.IM-P):** O processamento de dados por sistemas, produtos ou serviços é compreendido e mantém os administradores informados sobre o risco de privacidade.	**ID.IM-P1:** Sistemas/produtos/serviços que processam dados são inventariados.
		ID.IM-P2: Proprietários ou operadores (ex: a organização ou terceiros, como prestadores de serviços, parceiros, clientes e desenvolvedores) e suas funções em relação aos sistemas/produtos/serviços e componentes (ex: internos ou externos) que processam dados são inventariados.
		ID.IM-P3: Categorias de indivíduos (ex: clientes, funcionários ou potenciais funcionários, consumidores) cujos dados estão sendo processados são inventariadas.
		ID.IM-P4: As ações de dados dos sistemas/produtos/serviços são inventariadas.
		ID.IM-P5: Os propósitos para as ações de dados são inventariados.
		ID.IM-P6: Os elementos de dados dentro das ações de dados são inventariados.
		ID.IM-P7: O ambiente de processamento de dados é identificado (ex: localização geográfica, interno, nuvem, terceiros).
		ID.IM-P8: O processamento de dados é mapeado, ilustrando as ações e os elementos de dados associados referentes aos sistemas/produtos/serviços, incluindo componentes; funções dos proprietários/operadores de componentes; e interações de indivíduos ou terceiros com os sistemas/produtos/serviços.
	Ambiente de negócios (ID. BE-P): A missão, objetivos, partes interessadas e atividades da organização são compreendidos e priorizados; essas informações são usadas para informar funções de privacidade, responsabilidades e decisões sobre gerenciamento de riscos.	**ID.BE-P1:** As funções da organização no ecossistema de processamento de dados são identificadas e comunicadas.
		ID.BE-P2: Prioridades para a missão organizacional, objetivos e atividades são estabelecidas e comunicadas.
		ID.BE-P3: Sistemas/produtos/serviços que suportam prioridades organizacionais são identificados e os principais requisitos são comunicados.

	Função	Categoria	Subcategoria
		Avaliação de risco (ID.RA-P): A organização entende os riscos de privacidade para os indivíduos e como eles podem impactar futuramente as operações organizacionais, incluindo a missão, funções, outras prioridades de gerenciamento de risco (ex: compliance, financeiro), reputação, força de trabalho e cultura.	**ID.RA-P1:** Fatores contextuais relacionados aos sistemas/produtos/serviços e às ações de dados são identificados (ex: dados demográficos dos indivíduos e interesses ou percepções de privacidade, sensibilidade dos dados e/ou tipos de dados, visibilidade do processamento de dados para indivíduos e terceiros).
			ID.RA-P2: As entradas e saídas de análise de dados são identificadas e avaliadas para saber se há algum viés.
			ID.RA-P3: Potenciais ações de dados problemáticas e problemas associados são identificados.
			ID.RA-P4: Ações de dados problemáticas, probabilidades e impactos são usados para determinar e priorizar o risco.
			ID.RA-P5: As respostas de risco são identificadas, priorizadas e implementadas.
		Gerenciamento de risco do ecossistema de processamento de dados (ID.DE-P): As prioridades, restrições, e tolerância ao risco e premissas da organização são estabelecidas e utilizadas para apoiar decisões associadas ao risco de privacidade e risco a terceiros dentro do ecossistema de gerenciamento de dados. A organização estabeleceu e implementou os processos para identificar, avaliar e gerenciar os riscos de privacidade dentro do ecossistema de processamento de dados.	**ID.DE-P1:** As políticas, processos e procedimentos de gerenciamento de risco do ecossistema de processamento de dados são identificados, estabelecidos, avaliados, gerenciados e acordados pelas partes interessadas organizacionais.
			ID.DE-P2: As partes do ecossistema de processamento de dados (ex: provedores de serviços, clientes, parceiros, fabricantes de produtos, desenvolvedores de aplicativos) são identificadas, priorizadas e avaliadas por um processo de avaliação de risco de privacidade.
			ID.DE-P3: Os contratos com as partes do ecossistema de processamento de dados são usados para implementar medidas apropriadas, que foram elaboradas para atender aos objetivos do programa de privacidade de uma organização.
			ID.DE-P4: Estruturas de interoperabilidade ou abordagens similares de várias partes são usadas para gerenciar riscos de privacidade do ecossistema de processamento de dados.

	Função	Categoria	Subcategoria
			ID.DE-P5: As partes do ecossistema de processamento de dados são rotineiramente avaliadas por meio de auditorias, resultados de testes ou outras formas de avaliação, para confirmar se estão efetivamente enquadradas na estrutura contratual de interoperabilidade, ou outras obrigações.
	GOVERNAR-P (GV-P): Desenvolver e implementar a estrutura de governança organizacional para permitir uma compreensão contínua das prioridades de gerenciamento de riscos da organização que são informadas pelo risco de privacidade.	**Políticas, processos e procedimentos de governança (GV. PO-P):** As políticas, processos e procedimentos para gerenciar e monitorar os requisitos regulatórios, legais, de risco, ambientais e operacionais da organização são compreendidos servem para informar a administração sobre o gerenciamento do risco de privacidade.	**GV.PO-P1:** Valores e políticas de privacidade organizacional (ex: condições sobre o processamento de dados como o uso dos dados ou períodos de retenção, prerrogativas dos indivíduos em relação ao processamento de dados) são estabelecidos e comunicados.
			GV.PO-P2: Processos para incutir valores de privacidade organizacional dentro do sistema/desenvolvimento de produtos/serviços e operações são estabelecidos e implementados.
			GV.PO-P3: Funções e responsabilidades para a força de trabalho são estabelecidas no que diz respeito à privacidade.
			GV.PO-P4: As funções e responsabilidades de privacidade são coordenadas e alinhadas com partes interessadas de terceiros (ex: provedores de serviços, clientes, parceiros).
			GV.PO-P5: Os requisitos legais, regulatórios e contratuais relativos à privacidade são compreendidos e gerenciados.
			GV.PO-P6: As políticas, processos e procedimentos de governança e gestão de risco abordam os riscos de privacidade.
		Estratégia de gestão de risco (GV. RM-P): As prioridades, restrições, tolerâncias ao risco e premissas da organização são estabelecidas e utilizadas para apoiar as decisões de risco operacional.	**GV.RM-P1:** Os processos de gestão de risco são estabelecidos, gerenciados e aceitos pelas partes interessadas organizacionais.
			GV.RM-P2: A tolerância ao risco organizacional é determinada e expressa claramente.
			GV.RM-P3: A determinação de tolerância ao risco da organização é informada por meio das suas funções no ecossistema de processamento de dados.
		Conscientização e treinamento (GV. AT-P): A força de trabalho da organização, juntamente com terceiros envolvidos no processamento de dados são instruídos e	**GV.AT-P1:** A força de trabalho é informada e treinada sobre suas funções e responsabilidades.
			GV.AT-P2: Executivos seniores entendem suas funções e responsabilidades.

	Função	Categoria	Subcategoria
		conscientizados sobre privacidade, sendo treinados para desempenhar suas funções e responsabilidades relacionadas à privacidade de acordo com as políticas, processos, procedimentos, acordos e valores de privacidade organizacional.	**GV.AT-P3:** Os funcionários da área de privacidade entendem suas funções e responsabilidades.
			GV.AT-P4: Terceiros (ex: prestadores de serviços, clientes, parceiros) entendem suas funções e responsabilidades.
		Monitoramento e revisão (GV. MT-P): As normas, processos e procedimentos para revisão contínua da postura de privacidade da organização são compreendidos e mantêm a administração informada sobre o risco de privacidade.	**GV.MT-P1:** O risco de privacidade é reavaliado continuamente como um fator-chave, incluindo o ambiente de negócios da organização (ex: introdução de novas tecnologias), governança (ex: obrigações legais, tolerância ao risco), processamento de dados e mudança de sistemas/produtos/serviços.
			GV.MT-P2: Os valores, políticas e treinamento sobre privacidade são revisados e todas as atualizações são comunicadas.
			GV.MT-P3: Políticas, processos e procedimentos para avaliar o compliance com os requisitos legais e políticas de privacidade são estabelecidos e implementados.
			GV.MT-P4: Políticas, processos e procedimentos para comunicar o progresso na gestão dos riscos de privacidade são estabelecidos e em vigor.
			GV.MT-P5: Políticas, processos e procedimentos são estabelecidos e implementados para receber, analisar e responder às ações de dados problemáticas divulgadas para a organização a partir de fontes internas e externas (ex: descoberta interna, pesquisadores de privacidade, eventos profissionais).
			GV.MT-P6: Políticas, processos e procedimentos incorporam lições aprendidas e derivadas das ações de dados problemáticas.
			GV.MT-P7: Políticas, processos e procedimentos para recebimento, rastreamento, e resposta a reclamações, preocupações e perguntas dos indivíduos sobre práticas de privacidade organizacional são estabelecidos e em vigor.

	Função	Categoria	Subcategoria
	CONTROLE-P (CT-P): Desenvolver e implementar atividades apropriadas para permitir que organizações ou indivíduos gerenciem dados com granularidade suficiente para gerenciar riscos de privacidade.	**Políticas, processos e procedimentos de processamento de dados (CT.PO-P):** Políticas, processos e procedimentos são mantidos e usados para gerenciar o processamento de dados (ex: finalidade, escopo, funções e responsabilidades dentro do ecossistema de processamento de dados e compromisso de gerenciamento) condizentes com a estratégia de risco da organização para proteger a privacidade dos indivíduos.	**CT.PO-P1:** Políticas, processos e procedimentos para autorizar o processamento de dados (ex: decisões organizacionais, consentimento individual), revogação de autorizações e manutenção de autorizações são estabelecidos e em vigor.
			CT.PO-P2: Políticas, processos e procedimentos para permitir a revisão, transferência, compartilhamento ou divulgação, alteração e exclusão de dados, são estabelecidos e em vigor (ex: para manter a qualidade dos dados, gerenciar a retenção de dados).
			CT.PO-P3: Políticas, processos e procedimentos para habilitar as preferências e solicitações de processamento de dados dos indivíduos são estabelecidos e em vigor.
			CT.PO-P4: O ciclo de vida dos dados a serem gerenciados está alinhado e implementado no ciclo de vida de desenvolvimento e gerenciamento de sistemas.
		Gerenciamento de processamento de dados (CT.DM-P): Os dados são gerenciados em conformidade com a estratégia de risco da organização para proteger a privacidade dos indivíduos, aumentar a gerenciabilidade e permitir a implementação de princípios de privacidade (ex: participação individual, qualidade dos dados, minimização de dados).	**CT.DM-P1:** Os elementos de dados podem ser acessados para revisão.
			CT.DM-P2: Os elementos de dados podem ser acessados para transmissão ou divulgação.
			CT.DM-P3: Os elementos de dados podem ser acessados para alteração.
			CT.DM-P4: Os elementos de dados podem ser acessados para exclusão.
			CT.DM-P5: Os dados são destruídos de acordo com a política.
			CT.DM-P6: Os dados são transmitidos usando formatos padronizados.
			CT.DM-P7: Mecanismos de transmissão de permissões de processamento e valores de dados relacionados aos elementos de dados são estabelecidos e em vigor.
			CT.DM-P8: Os registros de auditoria/log são identificados, documentados, implementados e revisados de acordo com as normas e incorporando o princípio de minimização de dados.
			CT.DM-P9: As medidas técnicas implementadas para gerenciar o processamento de dados são testadas e avaliadas.

	Função	Categoria	Subcategoria
			CT.DM-P10: As preferências de privacidade das partes interessadas estão incluídas nos objetivos do projeto algorítmico e as saídas são avaliadas em relação a essas preferências.
		Processamento Desassociado (CT.DP-P): As soluções de processamento de dados aumentam a dissociabilidade de acordo com a estratégia de risco da organização para proteger a privacidade dos indivíduos e viabilizar a implementação de princípios de privacidade (ex: minimização de dados).	**CT.DP-P1:** Os dados são processados para limitar a observabilidade e a linkabilidade (ex: ações de dados ocorrem em dispositivos locais, criptografia que preserva a privacidade).
			CT.DP-P2: Os dados são processados para limitar a identificação de indivíduos (ex: técnicas de privacidade de desidentificação, tokenização).
			CT.DP-P3: Os dados são processados para limitar a formulação de inferências sobre o comportamento ou atividades dos indivíduos (ex: o processamento de dados é descentralizado, arquiteturas distribuídas).
			CT.DP-P4: As configurações do sistema ou do dispositivo permitem a coleta seletiva ou a divulgação de elementos de dados.
			CT.DP-P5: As referências de atributos são substituídas por valores de atributos.
	COMUNICAR-P (CM-P): Desenvolver e implementar atividades apropriadas para permitir que organizações e indivíduos tenham um entendimento confiável e se envolvam em um diálogo sobre como os dados são processados e sobre os riscos de	**Políticas, processos e procedimentos de comunicação (CM.PO-P):** Políticas, processos e procedimentos são mantidos e usados para aumentar a transparência das práticas de processamento de dados da organização (ex: finalidade, escopo, funções e responsabilidades no ecossistema de processamento de dados, compromisso de gestão) e riscos de privacidade associados.	**CM.PO-P1:** Políticas, processos e procedimentos de transparência para comunicação de propósitos, práticas e riscos de privacidade associados estão estabelecidos e em vigor.
			CM.PO-P2: Funções e responsabilidades (ex: relações públicas) para comunicação de propósitos, práticas e riscos de privacidade associados são estabelecidas.
		Conscientização sobre processamento de dados (CM.AW-P): Indivíduos e organizações têm conhecimento confiável sobre práticas de processamento de dados e riscos de privacidade associados, e mecanismos eficazes são usados e mantidos para aumentar a previsibilidade consistente com a	**CM.AW-P1:** Mecanismos (ex: avisos, relatórios internos ou públicos) para comunicar propósitos, práticas, riscos de privacidade associados e opções para permitir as preferências e solicitações de processamento de dados dos indivíduos estão estabelecidos e em vigor.
			CM.AW-P2: Mecanismos para obter o feedback dos indivíduos (ex: pesquisas ou grupos de enfoque) sobre processamento de dados e riscos associados à privacidade foram estabelecidos e estão em vigor.

	Função	Categoria	Subcategoria
	privacidade associados.	estratégia de risco da organização para proteger a privacidade dos indivíduos.	**CM.AW-P3:** O design do sistema/produto/serviço permite a visibilidade do processamento de dados.
			CM.AW-P4: Registros de divulgação e compartilhamento de dados são mantidos e podem ser acessados para revisão ou transmissão/divulgação.
			CM.AW-P5: Correções de dados ou exclusões podem ser comunicadas a indivíduos ou organizações (ex: fontes de dados) no ecossistema de processamento de dados.
			CM.AW-P6: A proveniência e linhagem dos dados são mantidas e podem ser acessadas para revisão ou transmissão/divulgação.
			CM.AW-P7: Os indivíduos e organizações afetados são notificados sobre uma violação ou evento de privacidade.
			CM.AW-P8: Os indivíduos recebem mecanismos de mitigação (ex: monitoramento de crédito, retirada de consentimento, alteração ou exclusão de dados) para lidar com os impactos de ações de dados problemáticas.
	PROTEGER-P (PR-P): Desenvolver e implementar salvaguardas adequadas de processamento de dados.	**Políticas, processos e procedimentos de proteção de dados (PR.PO-P):** Políticas de segurança e privacidade (ex: finalidade, escopo, funções e responsabilidades no ecossistema de processamento de dados, e compromisso de gestão), processos e procedimentos são mantidos e usados para gerenciar a proteção de dados.	**PR.PO-P1:** Uma configuração de linha de base de tecnologia da informação é criada e mantida incorporando princípios de segurança (ex: conceito de menor funcionalidade).
			PR.PO-P2: Os processos de controle de mudança de configuração estão estabelecidos e em vigor.
			PR.PO-P3: Os backups de informações são realizados, mantidos e testados.
			PR.PO-P4: As políticas e regulamentos relativos ao ambiente operacional físico para ativos organizacionais são atendidos.
			PR.PO-P5: Os processos de proteção são aprimorados.
			PR.PO-P6: A eficácia das tecnologias de proteção é compartilhada.
			PR.PO-P7: Planos de resposta (Resposta a Incidentes e Continuidade de Negócios) e planos de recuperação (Recuperação de Incidentes e Recuperação de Desastres) são estabelecidos, vigentes e gerenciados.
			PR.PO-P8: Os planos de resposta e recuperação são testados.

	Função	Categoria	Subcategoria
			PR.PO-P9: Os procedimentos de privacidade são incluídos nas práticas de recursos humanos (ex: desprovisionamento, triagem de pessoal).
			PR.PO-P10: Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado.
		Gerenciamento, autenticação e controle de acesso de identidade (PR.AC-P): O acesso aos dados e dispositivos é limitado a indivíduos, processos e dispositivos autorizados, sendo gerenciado de acordo com o risco avaliado de acesso não autorizado.	**PR.AC-P1:** Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para indivíduos, processos e dispositivos autorizados.
			PR.AC-P2: O acesso físico aos dados e dispositivos é gerenciado.
			PR.AC-P3: O acesso remoto é gerenciado.
			PR.AC-P4: As permissões e autorizações de acesso são gerenciadas, incorporando os princípios de privilégio mínimo e separação de funções.
			PR.AC-P5: A integridade da rede é protegida (ex: segregação de rede, segmentação de rede).
			PR.AC-P6: Indivíduos e dispositivos são testados e vinculados a credenciais e autenticados de acordo com o risco da transação (ex: riscos de segurança e riscos de privacidade dos indivíduos e outros riscos organizacionais).
		Segurança de dados (PR.DS-P): Os dados são gerenciados de forma consistente com a estratégia de risco da organização para proteger a privacidade dos indivíduos e manter a confidencialidade, integridade, e disponibilidade dos dados.	**PR.DS-P1:** Os dados em repouso são protegidos.
			PR.DS-P2: Os dados em trânsito são protegidos.
			PR.DS-P3: Sistemas/produtos/serviços e dados associados são formalmente gerenciados durante a remoção, transferências e disposição.
			PR.DS-P4: A capacidade adequada para garantir a disponibilidade é mantida.
			PR.DS-P5: Proteções contra vazamentos de dados são implementadas.
			PR.DS-P6: Mecanismos de verificação de integridade são usados para verificar software, firmware e integridade das informações.
			PR.DS-P7: Os ambientes de desenvolvimento e teste são separados do ambiente de produção.

	Função	Categoria	Subcategoria
			PR.DS-P8: Mecanismos de verificação de integridade são usados para verificar a integridade do hardware.
		Manutenção (PR.MA-P): A manutenção e os reparos do sistema são executados de acordo com as políticas, processos e procedimentos.	**PR.MA-P1:** A manutenção e reparação dos ativos organizacionais são realizadas e registradas, com ferramentas aprovadas e controladas.
			PR.MA-P2: A manutenção remota dos ativos organizacionais é aprovada, registrada e executada de forma a impedir o acesso não autorizado.
		Tecnologia de proteção (PR.PT-P): Soluções técnicas de segurança são gerenciadas para garantir a segurança e a resiliência de sistemas/produtos/serviços e dados associados, consistentes com as políticas, processos, procedimentos e acordos relacionados.	**PR.PT-P1:** A mídia removível é protegida e o seu uso é restrito de acordo com as políticas.
			PR.PT-P2: O princípio de menor funcionalidade é incorporado pela configuração de sistemas para fornecer apenas recursos essenciais.
			PR.PT-P3: As redes de comunicação e controle são protegidas.
			PR.PT-P4: Mecanismos (ex: à prova de falhas, balanceamento de carga, hot swap) são implementados para cumprir os requisitos de resiliência em situações normais e adversas.

Apêndice B: Glossário

Este apêndice define termos selecionados que foram utilizados para os fins desta publicação.

Referência de atributo (NIST SP 800-63-3 [8])	Uma declaração afirmando uma propriedade de um assinante sem necessariamente conter informações de identidade, independente do formato. Por exemplo, para o atributo "aniversário", uma referência pode ser "acima de 18 anos" ou "nascido em dezembro".
Valor do atributo (NIST SP 800-63-3 [8])	Uma declaração completa afirmando uma propriedade de um assinante, independente do formato. Por exemplo, para o atributo "aniversário", um valor poderia ser "1/12/1980" ou "1º de dezembro de 1980".
Disponibilidade (44 U.S.C. [13])	Garantir acesso oportuno e confiável e o uso da informação.
Categoria	A subdivisão de uma Função em grupos de resultados de privacidade intimamente ligados às necessidades programáticas e atividades específicas.
Comunicar-P (Função)	Desenvolver e implementar atividades adequadas para permitir que organizações e indivíduos tenham um entendimento confiável e se envolvam em um diálogo sobre como os dados são processados e sobre os riscos de privacidade associados.
Confidencialidade (44 U.S.C. [13])	Preservar as restrições autorizadas ao acesso e divulgação de informações, incluindo meios para proteger a privacidade pessoal e informações proprietárias.
Controle-P (Função)	Desenvolver e implementar atividades adequadas para permitir que organizações ou indivíduos gerenciem dados com granularidade suficiente para gerenciar riscos de privacidade.
Núcleo	Um conjunto de atividades e resultados de proteção à privacidade. A Estrutura do Núcleo compreende três elementos: Funções, Categorias e Subcategorias.
Incidente de cibersegurança	
(Guia para Melhorar a Segurança Cibernética da Infraestrutura Crítica [1])	Um evento de cibersegurança que foi determinado como tendo impacto na organização, gerando a necessidade de resposta e recuperação.
(OMB 17-12 [9])	Uma ocorrência que (1) real ou iminentemente põe em risco, sem autoridade legal, a integridade, confidencialidade ou disponibilidade de informações ou um sistema de informações; ou (2) constitui uma violação ou ameaça iminente de violação da lei, políticas e procedimentos de segurança ou normas de uso aceitável.

Dados	Uma representação de informações, incluindo formatos digitais e não digitais.
Ação de dados (adaptado do NIST IR 8062 [5])	Uma operação do ciclo de vida de dados de sistemas/produtos/serviços, incluindo, por exemplo, a coleta, retenção, registro, geração, transformação, uso, divulgação, compartilhamento, transmissão e descarte.
Elemento de dados	O menor item nomeado de dados que transmite informações significativas.
Processamento de dados (adaptado do NIST IR 8062 [5])	O conjunto de ações coletivas de dados (ex: o ciclo completo de vida dos dados, incluindo, mas não se limitando à coleta, retenção, registro, geração, transformação, uso, divulgação, compartilhamento, transmissão e descarte).
Ecossistema de processamento de dados	Os relacionamentos complexos e interconectados entre as entidades envolvidas na criação ou implantação de sistemas, produtos ou serviços ou de qualquer componente que processa dados.
Dissociabilidade (adaptado do NIST IR 8062 [5])	Habilitar o processamento de dados ou eventos sem associação a indivíduos ou dispositivos além dos requisitos operacionais do sistema.
Função	Um componente do Núcleo que fornece o mais alto nível de estrutura para organizar atividades básicas de privacidade em Categorias e Subcategorias.
Governar-P (Função)	Desenvolver e implementar a estrutura de governança organizacional para permitir uma compreensão contínua das prioridades de gerenciamento de risco da organização que são informadas pelo risco de privacidade.
Identificar-P (Função)	Desenvolver um entendimento organizacional para gerenciar o risco de privacidade para indivíduos, decorrentes do processamento de dados.
Nível de implementação	Fornecer um ponto de referência sobre como uma organização identifica o risco de privacidade e se ela tem processos e recursos suficientes para gerenciar esse risco.
Indivíduo	Uma única pessoa ou um grupo de pessoas, inclusive de um determinado nível social.
Integridade (44 U.S.C. [13])	Proteger contra modificações ou destruição indevida de informações, incluindo a garantia do não repúdio e da autenticidade das informações.
Linhagem	O histórico de processamento de um elemento de dados, que pode incluir fluxos de dados ponto-a-ponto e as ações de dados realizadas no elemento de dados.

Gerenciabilidade (adaptado do NIST IR 8062 [5])	Proporcionar a capacidade de administração granular de dados, incluindo alteração, exclusão e divulgação seletiva.
Metadados (adaptado do NIST SP 800-53 [10])	Informações que descrevem as características dos dados. Isso pode incluir, por exemplo, metadados estruturais descrevendo estruturas de dados (ex: formato de dados, sintaxe, semântica) e metadados descritivos, descrevendo o conteúdo dos dados.
Previsibilidade (adaptado do NIST IR 8062 [5])	Permitir suposições confiáveis por indivíduos, proprietários e operadores sobre os dados e seu processamento por um sistema, produto ou serviço.
Violação de Privacidade (adaptado do OMB M-17-12 [9])	A perda de controle, comprometimento, divulgação não autorizada, aquisição não autorizada, ou qualquer ocorrência semelhante onde (1) uma pessoa que não seja um usuário autorizado acessa ou potencialmente acessa dados ou (2) um usuário autorizado acessa dados para uma finalidade diferente da autorizada.
Controle de Privacidade (Adaptado do NIST SP 800-37 [7])	As salvaguardas administrativas, técnicas e físicas empregadas dentro de uma organização para satisfazer os requisitos de privacidade.
Evento de privacidade	A ocorrência ou potencial ocorrência de ações de dados problemáticas.
Requisitos de privacidade	Uma especificação para a funcionalidade do sistema/produto/serviço para atender aos resultados de privacidade desejados pelas partes interessadas.
Risco de privacidade	A probabilidade de que os indivíduos tenham problemas resultantes do processamento de dados e o impacto caso os problemas ocorram.
Avaliação de risco de privacidade	Um subprocesso de gerenciamento de riscos de privacidade para identificar e avaliar riscos de privacidade específicos.
Gerenciamento de riscos de privacidade	Um conjunto de processos interorganizacionais para identificar, avaliar e responder aos riscos de privacidade.
Ação de dados problemática (Adaptado do NIST IR 8062 [5])	Uma ação de dados que pode causar um efeito adverso para os indivíduos.
Processamento	Consulte *Processamento de dados*.
Perfil	Uma seleção de Funções, Categorias e Subcategorias específicas do Núcleo que uma organização priorizou para ajudá-la a gerenciar o risco de privacidade.
Proteger-P (Função)	Desenvolver e implementar salvaguardas adequadas de processamento de dados.

Proveniência (adaptado do NIST IR 8112 [11])	Metadados relativos à originação ou fonte de dados especificados.
Risco (NIST SP 800-30 [12])	Uma medida da extensão em que uma entidade é ameaçada por uma circunstância ou evento potencial, que é tipicamente uma função: (i) dos impactos adversos que surgiriam se a circunstância ou evento ocorresse; e (ii) a probabilidade de ocorrência.
Gestão de risco	O processo de identificação, avaliação e resposta ao risco.
Tolerância ao Risco (NIST SP 800-39 [6])	O nível de risco ou grau de incerteza que é aceitável para as organizações.
Subcategoria	As divisões adicionais de uma Categoria em resultados específicos de atividades técnicas e/ou gerenciais.

Apêndice C: Siglas

Este apêndice define as siglas selecionadas que foram utilizadas nesta publicação.

IEC	International Electrotechnical Commission [Comissão Eletrotécnica Internacional]
IR	Relatório Interno ou Interagências
ISO	International Organization for Standardization [Organização Internacional para Normalização]
TI	Tecnologia da Informação
NIST	National Institute of Standards and Technology [Instituto Nacional de Normas e Tecnologia]
OASIS	Organization for the Advancement of Structured Information Standards [Organização para o Avanço das Normas de Informações Estruturadas]
OECD	Organização para a Cooperação e Desenvolvimento Econômico
OMB	Office of Management and Budget [Escritório de Gestão e Orçamento]
PMRM	Privacy Management Reference Model and Methodology [Modelo de Referência e Metodologia de Gerenciamento de Privacidade]
PRAM	Privacy Risk Assessment Methodology [Metodologia de Avaliação de Riscos de Privacidade]
RFC	Request for Comment [Solicitação de Comentário]
RFI	Request for Information [Solicitação de Informações]
SDLC	System Development Life Cycle [Ciclo de Vida de Desenvolvimento do Sistema]
SP	Special Publication [Publicação Especial]

Apêndice D: Práticas de gerenciamento de risco de privacidade

A Seção 1.2 introduz uma série de considerações sobre o gerenciamento de riscos de privacidade, incluindo a relação entre segurança cibernética e risco de privacidade, e a função da avaliação de risco de privacidade. Este apêndice considera algumas das principais práticas que contribuem para um gerenciamento de risco de privacidade bem-sucedido, incluindo a organização de recursos preparatórios, determinação de recursos de privacidade, definição de requisitos de privacidade, realização de avaliações de risco de privacidade, criação de rastreabilidade de requisitos de privacidade e monitoramento de mudanças de riscos de privacidade. Referências para as categorias e subcategorias são incluídas para facilitar o uso do Núcleo e para incentivar essas práticas, sendo que as referências aparecem entre parênteses.

Organização de recursos preparatórios

Os recursos adequados facilitam a tomada de decisão informada sobre os riscos de privacidade em todos os níveis de uma organização. Na prática, a responsabilidade pelo desenvolvimento de vários recursos pode pertencer a diferentes componentes de uma organização. Portanto, um componente de uma organização que depende de certos recursos pode descobrir que eles não existem ou que talvez não estejam abordando a questão da privacidade suficientemente. Nessas circunstâncias, o componente dependente pode considerar a finalidade do recurso e buscar as informações em outras fontes, ou tomar a melhor decisão possível com as informações disponíveis. Em suma, bons recursos são úteis, mas as deficiências não devem impedir os componentes organizacionais de tomar as melhores decisões de risco dentro de suas capacidades.

Os seguintes recursos, embora não exaustivos, criam a base para uma melhor tomada de decisão.

- **Atribuições de funções de gerenciamento de risco** (GV.PO-P3, GV.PO-P4)

  Para que haja uma tomada de decisão acertada, é necessário estabelecer e possibilitar uma compreensão interorganizacional para determinar quem será o responsável e quem responderá pela gestão de risco de privacidade, bem como outras tarefas de gerenciamento de risco em uma organização, pois isso facilita uma melhor coordenação e responsabilização. Além disso, uma ampla gama de perspectivas pode melhorar o processo de identificação, avaliação e resposta aos riscos de privacidade. Uma equipe diversificada e multifuncional pode ajudar a identificar uma faixa mais abrangente de riscos à privacidade dos indivíduos e selecionar um conjunto mais amplo de mitigações. Determinar quais funções incluir nas discussões de gerenciamento de risco depende do contexto organizacional e da composição da empresa, embora a colaboração entre os programas de privacidade e segurança cibernética seja um aspecto importante. Se um indivíduo estiver sendo atribuído a várias funções, deve-se considerar o gerenciamento de potenciais conflitos de interesse.

- **Estratégia de gestão de risco empresarial** (GV.RM-P)

  A estratégia de gestão de risco empresarial de uma organização ajuda a alinhar a sua missão e valores com as suposições, restrições, prioridades e tolerância ao risco organizacional. As limitações de recursos para cumprir a missão ou objetivos de negócios e para gerenciar um amplo portfólio de riscos, provavelmente exigirão escolhas apropriadas que sejam compensatórias. Permitir que o pessoal envolvido no processo de gerenciamento de risco de privacidade compreenda melhor a tolerância ao risco de uma organização certamente ajudará na orientação das decisões sobre como alocar recursos e sobre escolhas mais acertadas para as respostas ao risco.

- **Principais partes interessadas** (GV.PO-P4, ID.DE-P)

  As partes interessadas em privacidade são aquelas que têm interesse ou se preocupam com os resultados de privacidade do sistema, produtos ou serviços. Por exemplo, as questões legais provavelmente se concentram em saber se o sistema, produto ou serviço está operando de maneira que possa colocar organização em descumprimento aos deveres de compliance, ou desobediência às leis, regulamentos de privacidade e acordos comerciais. Os empresários que desejam maximizar o uso podem estar preocupados com a perda de confiança no sistema, produto ou serviço devido à falta de privacidade. Indivíduos cujos dados estão sendo processados ou que estão interagindo com o sistema, produto ou serviço não desejam ter problemas ou consequências adversas. Compreender as partes interessadas, e os tipos de resultados de privacidade que necessitam, facilitará o design do sistema/produto/serviço que atenda de forma adequada às necessidades desse público-alvo.

- **Requisitos de privacidade em nível organizacional** (GV.PO-P)

  Os requisitos de privacidade em nível organizacional são um meio de expressar as obrigações legais, valores de privacidade e as normas às quais uma organização pretende aderir. Entender esses requisitos é fundamental para garantir que o design do sistema/produto/serviço esteja em conformidade com suas obrigações. Os requisitos de privacidade em nível organizacional podem derivar de uma variedade de fontes, como segue:

  - Ambiente jurídico (ex: leis, regulamentos, contratos);
  - Políticas organizacionais ou valores culturais;
  - Normas relevantes; e
  - Princípios de privacidade.

- **Artefatos de design de sistema/produto/serviço** (ID.BE-P3)

  Os artefatos de design podem assumir muitas formas, como arquiteturas de design de sistema ou diagramas de fluxo de dados. Esses artefatos ajudam uma organização a determinar como seus sistemas, produtos e serviços estarão funcionando. Portanto, eles podem auxiliar os programas de privacidade a entender como os sistemas, produtos e serviços precisam funcionar para que os controles ou medidas que ajudam a mitigar o risco de privacidade possam ser selecionados e implementados de forma a manter a funcionalidade enquanto protegem a privacidade.

- **Mapas de dados** (ID.IM-P)

  Os mapas de dados ilustram o processamento de dados e as interações dos indivíduos com sistemas, produtos e serviços. Um mapa de dados mostra o ambiente de processamento de dados e inclui os componentes por meio dos quais os dados estão sendo processados ou com os quais os indivíduos estão interagindo. Além disso, o mapa mostra os proprietários ou operadores dos componentes, as ações de dados discretas e os elementos de dados específicos que estão sendo processados. Os mapas de dados podem ser ilustrados de diferentes maneiras, e o nível de detalhamento pode variar de acordo com as necessidades de uma organização. Um mapa de dados pode ser sobreposto em artefatos de design de sistemas/produtos/serviços já instalados para maior conveniência e facilidade de comunicação entre componentes organizacionais. Conforme discutido abaixo, um mapa de dados é um artefato importante na avaliação de risco de privacidade.

Determinando recursos de privacidade

Os recursos de privacidade podem ser usados para descrever a propriedade ou recurso do sistema, produto ou serviço, ou a função que atinge o resultado de privacidade desejado (ex: "o serviço permite a minimização de dados"). Os objetivos de segurança, confidencialidade, integridade e disponibilidade, juntamente com os requisitos de segurança, são usados para informar os recursos de segurança de um sistema, produto ou serviço. Conforme estabelecido na **Tabela 3**, um conjunto adicional de objetivos de engenharia de privacidade pode validar a determinação dos recursos de privacidade. Uma organização também pode usar os objetivos de engenharia de privacidade como uma ferramenta de priorização de alto nível. Sistemas, produtos ou serviços que são de baixa previsibilidade, capacidade de gerenciamento ou dissociabilidade podem ser um sinal de aumento do risco de privacidade e, portanto, merecem uma avaliação mais abrangente do risco de privacidade.

Ao determinar os recursos de privacidade, uma organização pode considerar quais os objetivos de engenharia de privacidade e segurança que são mais importantes no que diz respeito às suas necessidades de missão ou negócios, tolerância ao risco e requisitos de privacidade em nível organizacional (consulte a Organização de Recursos Preparatórios acima). Nem todos os objetivos podem ser igualmente importantes, ou talvez seja necessário fazer trocas apropriadas que sejam compensatórias. Embora os recursos de privacidade informem a avaliação de risco de privacidade que está validando as decisões de priorização de riscos, os recursos de privacidade também podem ser informados através da avaliação de risco, sendo depois ajustados para confirmar a gestão de riscos de privacidade específicos ou abordar mudanças no ambiente, incluindo alterações de design no sistema, produto ou serviço.

Tabela 3: Engenharia de privacidade e objetivos de segurança[18]

	Objetivo	**Definição**	**Principais funções relacionadas do Núcleo do Privacy Framework**
Objetivos de engenharia de privacidade	Previsibilidade	Permitir suposições confiáveis por indivíduos, proprietários e operadores sobre os dados e o seu processamento por um sistema	Identificar-P, Governar-P, Controlar-P, Comunicar-P, Proteger-P
	Gerenciabilidade	Fornecer a capacidade para a administração granular de dados, incluindo coleta, alteração, exclusão e divulgação seletiva	Identificar-P, Governar-P, Controlar-P
	Dissociabilidade	Viabilizar o processamento de dados ou eventos sem associação a indivíduos ou dispositivos além dos requisitos operacionais do sistema	Identificar-P, Governar-P, Controlar-P

[18] Os objetivos da engenharia de privacidade foram adaptados do NIST IR 8062 [5]. Os objetivos de segurança foram retirados do NIST SP 800-37, Rev. 2 [7].

	Objetivo	Definição	Principais funções relacionadas do Núcleo do Privacy Framework
Objetivos de segurança	Confidencialidade	Preservar as restrições autorizadas ao acesso e divulgação de informações, incluindo meios para proteger a privacidade pessoal e informações proprietárias.	Identificar-P, Governar-P, Proteger-P
	Integridade	Proteger contra modificação ou destruição de informações indevidas, incluindo a garantia de não repúdio e autenticidade das informações	Identificar-P, Governar-P, Proteger-P
	Disponibilidade	Garantir acesso oportuno e confiável e o uso das informações.	Identificar-P, Governar-P, Proteger-P

Definindo requisitos de privacidade

Os requisitos de privacidade especificam a maneira em que um sistema, produto ou serviço precisa funcionar para satisfazer os resultados de privacidade desejados pelas partes interessadas (ex: "o aplicativo é configurado para permitir que os usuários selecionem elementos de dados específicos"). Para definir os requisitos de privacidade, considere os requisitos de privacidade em nível organizacional (consulte Organização de Recursos Preparatórios acima) e as saídas de uma avaliação de risco de privacidade. Esse processo ajuda uma organização a responder a duas perguntas: 1) O que um sistema, produto ou serviço *pode* fazer com o processamento de dados e interações com os indivíduos? 2) O que o sistema *deve* fazer? Portanto, uma organização pode alocar recursos para criar o design de um sistema, produto ou serviço de maneiras a atingir os requisitos definidos. Em última análise, a definição de requisitos de privacidade pode levar ao desenvolvimento de sistemas, produtos e serviços mais atentos à privacidade dos indivíduos, e que são criados com base nas decisões informadas sobre risco.

Realizando avaliações de risco de privacidade

A realização de uma avaliação de risco de privacidade ajuda uma organização a identificar riscos de privacidade gerados pelo sistema, produto ou serviço, e priorizá-los para tomar decisões informadas sobre como responder aos riscos (ID.RA-P, GV.RM-P). As metodologias para a realização de avaliações de risco de privacidade podem variar, mas as organizações devem considerar as seguintes características:[19]

[19] O NIST desenvolveu a Privacy Risk Assessment Methodology [Metodologia de Avaliação de Risco de Privacidade] (PRAM) que pode ajudar as organizações a identificar, avaliar e responder aos riscos de privacidade. Ela é composta por um conjunto de planilhas disponíveis em [3].

- **Modelo de risco** (ID. RA-P, GV.MT-P1)

  Os modelos de risco definem os fatores de risco a serem avaliados e as relações entre tais fatores.[20] Caso uma organização não esteja usando um modelo de risco pré-definido, ela deve especificar claramente quais os fatores de risco que serão avaliados e as relações entre esses fatores. Embora a cibersegurança tenha um modelo de risco amplamente usado com base nos fatores de risco de ameaças, vulnerabilidades, probabilidade e impacto, não existe um modelo de risco de privacidade comumente aceito. O NIST desenvolveu um modelo de risco de privacidade para calcular o risco com base na probabilidade de uma ação de dados problemática multiplicada pelo impacto de uma ação de dados problemática - cada um dos três fatores de risco é explicado abaixo.

  Fatores de risco de privacidade:
  Ação de dados problemática | Probabilidade | Impacto

  - Uma ação de dados problemática é qualquer ação que um sistema executa para processar dados que podem resultar em um problema para os indivíduos. As organizações consideram os tipos de problemas que são relevantes para a população de indivíduos. Os problemas podem assumir qualquer forma e podem levar em consideração a experiência dos indivíduos.[21]
  - A probabilidade é definida como uma análise contextual de que uma ação de dados provavelmente criará um problema para um conjunto representativo de indivíduos. O contexto pode incluir fatores organizacionais (ex: localização geográfica, a percepção do público sobre as organizações participantes no que diz respeito à privacidade), fatores do sistema (ex: a natureza e o histórico das interações dos indivíduos com o sistema, visibilidade do processamento de dados para indivíduos e terceiros), ou fatores individuais (ex: dados demográficos dos indivíduos, interesses ou percepções de privacidade, sensibilidade dos dados).[22] Um mapa de dados pode ajudar nessa análise contextual (consulte Organização de Recursos Preparatórios).
  - O impacto é uma análise dos custos caso o problema ocorra. Conforme observado na seção 1.2, as organizações não enfrentam esses problemas diretamente. Além disso, as experiências dos indivíduos podem ser subjetivas. Portanto, pode ser difícil avaliar o impacto com precisão. As organizações devem considerar os melhores meios de internalizar o impacto para os indivíduos, a fim de priorizar e responder adequadamente aos riscos de privacidade.[23]

---

20 Leia o NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments* [*Guia para a realização de avaliações de risco]* [12] na pg. 8.

21 Como parte do seu PRAM, o NIST criou um catálogo ilustrativo de ações de dados problemáticas e outros problemas a serem considerados [3]. Outras organizações podem ter criado conjuntos de problemas adicionais ou podem se referir a eles como consequências ou danos adversos.

22 Consulte o PRAM do NIST para obter mais informações sobre fatores contextuais. Id. na planilha 2.

23 O PRAM do NIST usa custos organizacionais como custos de não conformidade, custos diretos de negócios, custos de reputação, e custos de cultura interna como motivadores por considerar como avaliar o impacto individual. Id. na Planilha 3, Aba sobre Impacto.

- **Abordagem de avaliação**

  A abordagem de avaliação é o mecanismo pelo qual os riscos identificados são priorizados. As abordagens de avaliação podem ser categorizadas como quantitativas, semiquantitativas ou qualitativas.[24] [25]

- **Priorizando riscos** (ID.RA-P4)

  Devido aos limites aplicáveis dos recursos das organizações, elas priorizam os riscos para facilitar a comunicação sobre como responder a tais riscos.[26]

- **Resposta aos riscos** (ID.RA-P5)

  Conforme descrito na seção 1.2.2, as abordagens de respostas incluem mitigação, transferência/compartilhamento, prevenção ou aceitação.[27]

Criação de rastreabilidade de requisitos de privacidade

Assim que uma organização determinar quais os riscos a serem mitigados, ela poderá refinar os requisitos de privacidade, para depois selecionar e implementar controles (ex: proteções técnicas, físicas e/ou salvaguardas para as normas) para atender aos requisitos.[28] Uma organização pode usar uma variedade de fontes para selecionar controles, como o NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations* [*Controles de Segurança e Privacidade para Sistemas de Informação e Organizações]*.[29] Após a implementação, uma organização avalia iterativamente os controles quanto à sua eficácia no cumprimento dos requisitos de privacidade e no gerenciamento do risco de privacidade. Dessa forma, uma organização cria rastreabilidade entre os controles e os requisitos de privacidade e demonstra responsabilização entre sistemas, produtos e serviços, e seus objetivos de privacidade organizacional.

Monitoramento das Mudanças

O gerenciamento de riscos de privacidade não é um processo estático. Uma organização monitora como as mudanças em seu ambiente de negócios podem estar afetando o risco de privacidade — incluindo novas leis, regulamentos e tecnologias emergentes — bem como mudanças correspondentes em seus sistemas, produtos e serviços, e utiliza iterativamente as práticas neste apêndice para fazer ajustes conforme necessário. (GV.MT-P1)

---

[24] Leia NIST SP 800-30Rev. 1, *Guide for Conducting Risk Assessments* [Guia para a realização de avaliações de risco] na [12] pg. 14.

[25] O PRAM do NIST usa uma abordagem semiquantitativa baseada em escala de 1-10.

[26] O PRAM do NIST oferece várias representações de priorização, incluindo um mapa de calor. Veja a [3] Planilha 3.

[27] O PRAM do NIST proporciona um processo para responder aos riscos de privacidade que foram priorizados. Id. na Planilha 4.

[28] Leia o NIST SP 800-37, Rev. 2 [7].

[29] Leia o NIST SP 800-53 conforme atualizado [10].

Apêndice E: Definições dos níveis de implementação

Os quatro níveis resumidos abaixo são definidos individualmente com quatro elementos:

Nível 1: Parcial

- **Processo de gerenciamento de riscos de privacidade** – As práticas de gerenciamento de risco de privacidade organizacional não são formalizadas e o risco é gerenciado de forma ad hoc ou então de maneira reativa. A priorização das atividades de privacidade talvez não seja informada diretamente pelas prioridades de gerenciamento de risco organizacional, avaliações de risco de privacidade, missão ou objetivos de negócios.
- **Programa integrado de gerenciamento de riscos de privacidade** – Existe uma percepção limitada quanto ao risco de privacidade no nível organizacional. A organização implementa o gerenciamento de risco de privacidade de forma irregular, caso a caso, devido aos diversos tipos de experiências ou de informações obtidas de fontes externas. A organização pode não ter processos que permitam o compartilhamento de informações sobre o processamento de dados e os riscos de privacidade resultantes dentro da organização.
- **Relacionamentos com o ecossistema de processamento de dados** – Há uma compreensão limitada das funções de uma organização no ecossistema mais amplo, em relação a outras entidades (ex: compradores, fornecedores, prestadores de serviços, associados de negócios, parceiros). A organização não possui processos para identificar como os riscos de privacidade podem se proliferar em todo o ecossistema ou como ela deve comunicar riscos ou requisitos de privacidade a outras entidades do ecossistema.
- **Força de trabalho** – Alguns funcionários podem ter uma compreensão limitada dos riscos de privacidade ou processos de gerenciamento de risco de privacidade, mas não têm responsabilidades específicas relativas à privacidade. Caso exista treinamento disponível, ele é ad hoc e o conteúdo não é devidamente atualizado com as melhores práticas.

Nível 2: Risco informado

- **Processo de gerenciamento de risco de privacidade** – As práticas de gerenciamento de risco são aprovadas pela administração, mas talvez não sejam estabelecidas como uma política para toda a organização. A priorização das atividades de privacidade é informada diretamente pelas prioridades de gerenciamento de risco organizacional, avaliações de risco de privacidade, pela missão ou objetivos de negócios.
- **Programa integrado de gerenciamento de risco de privacidade** – Existe uma percepção do risco de privacidade no nível organizacional, entretanto, ainda não foi estabelecida uma abordagem em toda a organização para gerenciar tal risco. Informações sobre processamento de dados e riscos de privacidade resultantes são compartilhadas dentro da organização de maneira informal. A consideração necessária à questão da privacidade nos objetivos e programas organizacionais pode ocorrer em alguns níveis, mas não em todos os níveis da organização. A avaliação do risco de privacidade acontece, mas normalmente não é repetível ou recorrente.
- **Relacionamentos do ecossistema de processamento de dados** – Existe algum entendimento sobre as funções de uma organização no ecossistema mais amplo em relação a outras entidades (ex: compradores, fornecedores, prestadores de serviços, associados de negócios, parceiros). A organização está ciente dos riscos do ecossistema de privacidade associados aos produtos e

serviços que fornece e usa, mas não age de forma consistente ou formal para solucionar esses riscos.

- **Força de trabalho** – Existem funcionários com responsabilidades específicas na área de privacidade, mas talvez tenham também outras responsabilidades não relacionadas à privacidade. O treinamento sobre privacidade é realizado regularmente para o pessoal de privacidade, embora não haja um processo consistente para atualizações sobre as melhores práticas.

Nível 3: Repetível

- **Processo de gerenciamento de risco de privacidade** – As práticas de gerenciamento de riscos da organização são formalmente aprovadas e expressas como normas. As práticas de privacidade organizacional são atualizadas regularmente com base na aplicação de processos de gerenciamento de risco para haver mudanças na missão ou objetivos de negócios e uma mudança no cenário de risco, políticas e tecnologia.
- **Programa integrado de gerenciamento de riscos de privacidade** – Existe uma abordagem em toda a organização para gerenciar o risco de privacidade. Políticas, processos e procedimentos informados sobre riscos são definidos, implementados e revisados conforme pretendido. Métodos consistentes estão em vigor para responder efetivamente às mudanças de risco. A organização monitora de forma consistente e precisa o risco de privacidade. Executivos seniores que atuam área de privacidade e não-privacidade se comunicam regularmente sobre o risco de privacidade. Executivos seniores garantem que estarão considerando a importância da privacidade em todas as linhas operacionais da organização.
- **Relacionamentos do ecossistema de processamento de dados** – A organização entende as suas funções, dependências e dependentes no ecossistema mais amplo, e pode contribuir para que a comunidade tenha uma compreensão mais profunda do que são os riscos. A organização está ciente dos riscos do ecossistema de privacidade associados aos produtos e serviços que fornece e utiliza. Além disso, a organização geralmente age formalmente em relação a esses riscos, incluindo mecanismos como acordos escritos para comunicar requisitos de privacidade, estruturas de governança, implementação e monitoramento de políticas.
- **Força de trabalho** – O pessoal dedicado à privacidade possui os conhecimentos e habilidades necessárias para desempenhar suas funções e responsabilidades. O treinamento de privacidade atualizado é oferecido regularmente para todo o pessoal.

Nível 4: Adaptativo

- **Processo de gerenciamento de riscos de privacidade** – A organização adapta suas práticas de privacidade com base em lições aprendidas nos eventos de privacidade e na identificação de novos riscos de privacidade. Por meio de um processo de melhoria contínua que incorpora tecnologias e práticas de privacidade avançadas, a organização se adapta efetivamente a um cenário em constante mudança no tocante às normas e tecnologia, respondendo de maneira oportuna e eficaz aos riscos evolutivos de privacidade.
- **Programa integrado de gerenciamento de riscos de privacidade** – Existe uma abordagem em toda a organização para gerenciar riscos de privacidade que usa normas, processos e procedimentos informados sobre risco para lidar com ações de dados problemáticas. A relação entre o risco de privacidade e os objetivos organizacionais é claramente entendida e considerada no processo decisório. Executivos seniores monitoram o risco de privacidade no

mesmo contexto do risco de cibersegurança, risco financeiro e outros riscos organizacionais. O orçamento organizacional baseia-se no entendimento do ambiente de risco atual e previsto, e na tolerância ao risco. As unidades de negócios implementam a visão executiva e analisam os riscos de nível de sistema no contexto das tolerâncias ao risco organizacional. O gerenciamento de risco de privacidade faz parte da cultura organizacional e evolui a partir das lições aprendidas e da consciência contínua do processamento de dados e dos consequentes riscos à privacidade. A organização pode se responsabilizar de forma rápida e eficiente pelas mudanças nos objetivos de negócios/missão sobre a maneira em que o risco é abordado e comunicado.

- **Relacionamentos do ecossistema de processamento de dados** – A organização entende as suas funções, dependências e dependentes dentro do ecossistema mais amplo, e pode contribuir para que a comunidade tenha uma compreensão mais profunda do que são os riscos. A organização usa informações em tempo real ou quase-real para entender e agir de forma consistente sobre os riscos do ecossistema de privacidade associados aos produtos e serviços que fornece e utiliza. Além disso, ela se comunica proativamente, utilizando mecanismos formais (ex: acordos) e informais para desenvolver e manter relações sólidas com o ecossistema.
- **Força de trabalho** – A organização possui conhecimentos específicos na área de privacidade que permeiam toda a estrutura organizacional; pessoas com perspectivas diversificadas contribuem para a gestão dos riscos de privacidade. O treinamento sobre privacidade atualizado é oferecido regularmente para todo o pessoal. O pessoal em todos os níveis entende os valores de privacidade organizacional e o seu papel em mantê-los.