# Introdução ao Framework de Privacidade do NIST: Um guia rápido para pequenas e médias empresas

### O que é o Framework de Privacidade do NIST e como a minha organização pode usá-lo?

O <u>Framework de Privacidade do NIST</u>¹ é uma ferramenta voluntária que pode ajudar sua organização a criar ou melhorar um programa de privacidade. O gerenciamento eficaz de riscos de privacidade pode ajudá-lo a criar confiança em seus produtos e serviços, comunicar melhor suas práticas de privacidade e cumprir suas obrigações de conformidade. Uma boa segurança cibernética é importante, mas não consegue abordar todos os riscos de privacidade.

Comece a usar o Framework de Privacidade seguindo um modelo simples de fases "Preparar, apontar, fogo" e alinhe seus negócios ou agência com cinco áreas de gerenciamento de risco de privacidade: Identificação, governança, controle, comunicação e proteção.

# 01

#### PREPARAR...

Prepare-se para criar ou melhorar seu programa de privacidade usando o Framework de Privacidade para elaborar uma base sólida de forma a identificar e gerenciar os riscos de privacidade.

#### Identificação:

- Identifique os dados sendo processados (como coleta, uso, compartilhamento, armazenamento) e mapeie seu fluxo em seus sistemas durante todo o ciclo de vida dos dados da coleta ao descarte. Isso não precisa ser perfeitamente abrangente, especialmente no início, mas é uma base para entender seus riscos de privacidade.
- Conduza uma <u>avaliação de risco de privacidade</u><sup>2</sup> usando seu mapa de dados para avaliar como suas atividades de processamento de dados podem criar problemas para indivíduos (como constrangimento, discriminação ou perda econômica). Em seguida, avalie os impactos na sua organização se esses problemas ocorrerem (como perda de confiança do cliente ou danos à reputação), podendo afetar negativamente seus resultados.
- Pergunte sobre as opções de contratos e os produtos e serviços que você usa para administrar seus negócios para garantir que eles sejam configurados de forma a refletir suas prioridades de privacidade.

"É difícil justificar a criação de um programa de privacidade, mas o Framework de Privacidade do NIST tem sido uma das ferramentas que conseguimos usar, mesmo quando não é possível contratar uma grande equipe de privacidade."

## **JAIME LEES**

DIRETORA DE DADOS

GOBIERNO DEL CONDADO DE ARLINGTON

#### **Governanca:**

- A cultura de privacidade começa no topo. Determine em quais valores de privacidade (por exemplo, autonomia humana, anonimato, dignidade, transparência, controle de dados) sua organização está focada. Conecte os valores e políticas de privacidade da sua organização com sua avaliação de risco de privacidade para promover a confiança em seus produtos e serviços.
- Conheça suas obrigações legais relacionadas à privacidade para que você possa criar produtos e serviços compatíveis.
- Ajude sua força de trabalho a conhecer suas funções e responsabilidades para tomar melhores decisões sobre como gerenciar efetivamente os riscos de privacidade no projeto e na implantação de seus produtos e serviços.
- Reavalie regularmente para ver se seus riscos de privacidade mudaram. Isso pode acontecer quando você faz melhorias em seus produtos e serviços, altera seu processamento de dados ou aprende sobre novas obrigações legais.

<sup>&</sup>lt;sup>1</sup>https://www.nist.gov/privacy-framework

<sup>&</sup>lt;sup>2</sup> https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources



#### APONTAR...

Agora que você conhece seus riscos de privacidade e obrigações legais e tem uma estrutura de governança, sua organização pode se concentrar nas políticas e recursos técnicos para seus sistemas, produtos e serviços.

## **Controle:**

- Você coleta, compartilha ou mantém dados desnecessários? Considere como suas políticas ajudam você ou outras organizações a manter o controle sobre os dados e como os indivíduos também podem ter um papel.
- Leve em consideração seus riscos de privacidade e obrigações legais ao decidir sobre a funcionalidade de seus sistemas, produtos ou serviços de processamento de dados. Considere um design flexível para que você possa responder de forma mais econômica às mudanças nas preferências de privacidade do cliente e a um ambiente jurídico dinâmico.
- Quais tipos de processamento de dados você faz? Quanto mais você puder desassociar dados de indivíduos e dispositivos, maiores serão os ganhos de privacidade. Considere como diferentes medidas técnicas, como desidentificação, processamento descentralizado de dados ou outras técnicas, podem permitir que você atenda aos objetivos dos seus negócios ou agência enquanto protege a privacidade.

### Proteção:

- Controle quem faz login em sua rede e usa seus computadores e outros dispositivos.
- Use software de segurança para proteger os dados.
- Criptografe dados confidenciais, em repouso e em trânsito.
- Faça backups regulares dos dados.
- Atualize o software de segurança regularmente, automatizando essas atualizações, se possível.
- Tenha políticas formais para o descarte seguro de dados e dispositivos antigos.

"Se você precisa estabelecer um programa de privacidade, o Framework de Privacidade do NIST é o lugar perfeito para começar."

# **JEEWON SERRATO**

PARCEIRA

BAKERHOSTETLER

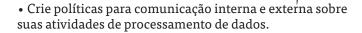
"O Framework de Privacidade pode ser um diferencial de mercado para que a organização consiga expandir seus negócios."

# MARY N. CHANEY, ADVOGADA., CISSP, CIPP

DIIRETORA DE SEGURANÇA E PRIVACIDADE DA INFORMAÇÃO

ESPERION THERAPEUTICS, INC.

### Comunicação:



- Aumente a transparência e a compreensão do cliente fornecendo avisos e relatórios claros e acessíveis ou implementando alertas ou outros sinais para informar as pessoas sobre suas atividades de processamento de dados e suas escolhas..
- Você realiza pesquisas ou grupos de discussão para informar o design do seu produto ou serviço? Inclua privacidade para saber mais sobre as preferências de privacidade do cliente.
- Considere o que você fará no caso de uma violação de dados. Como você fornecerá notificações ou quaisquer soluções, como monitoramento de crédito ou congelamentos?

# FOGO!

Agora é a hora de colocar tudo em prática.

- Como seu programa se compara ao que sugerimos aqui?
- Priorize os resultados desejados e crie um plano de ação.
- Discuta sobre seu plano como organização e use-o para trabalhar no sentido de adquirir os recursos e criar a força de trabalho necessária para atingir suas metas.
- Coloque seu plano em ação! Você está a caminho de criar mais confiança em seus produtos e serviços, comunicar de forma mais eficaz sobre privacidade com seus parceiros e clientes e cumprir suas obrigações de conformidade.

