

Gartner®

# Diretriz de TI para segurança cibernética



# Como as organizações bem-sucedidas desenvolvem programas de segurança baseados em risco para apoiar a agilidade e a resiliência dos negócios?

A transformação digital dos negócios e os sistemas ciberfísicos emergentes criam um risco de segurança sem precedentes. Até 2027, 75% dos funcionários vão adquirir, modificar ou criar tecnologia fora da visibilidade da TI, contra 41% em 2022\*. Em resposta, muitas organizações adotam novas abordagens de segurança cibernética.

Mas as organizações têm dificuldade para equilibrar a segurança cibernética com a necessidade de administrar a empresa. Diretores de segurança da informação podem ajudar desenvolvendo processos que permitam decisões baseadas em risco e, ao mesmo tempo, protejam contra ameaças à segurança e impeçam violações de dados e outros eventos de segurança cibernética.

A partir de nossa pesquisa especializada e interações com milhares de empresas de diversas indústrias, compilamos as práticas recomendadas para segurança cibernética em uma diretriz personalizável. Use esta diretriz para entender os principais estágios, recursos e pessoas necessários para planejar e executar uma iniciativa de segurança cibernética eficaz.

**67%**

dos diretores executivos e executivos seniores querem mais trabalho de tecnologia feito diretamente dentro das áreas funcionais/ departamentos da empresa e menos pela área de TI.

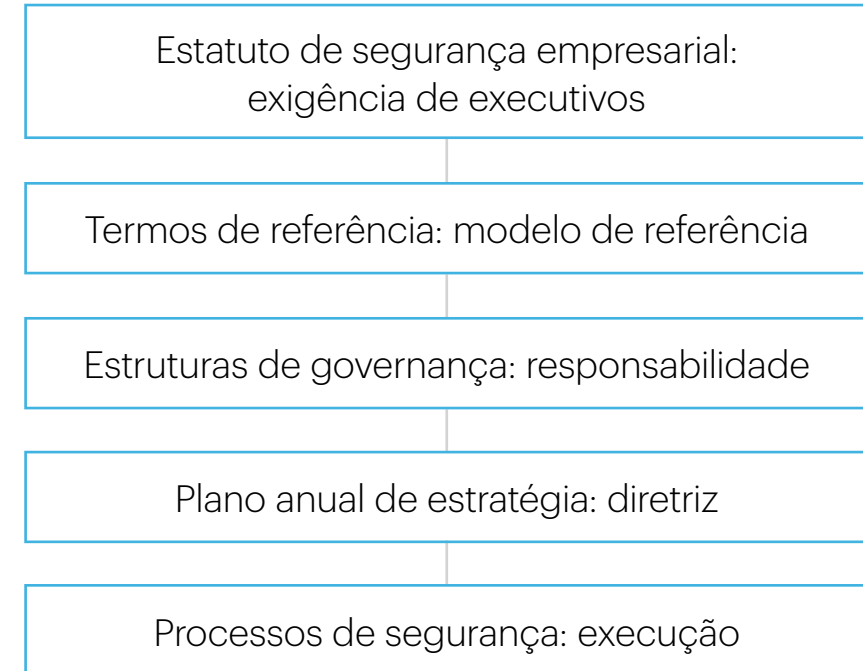
Fonte: Pesquisa Gartner para diretores executivos e executivos seniores de 2022

## Desenvolvendo e implementando um programa de segurança cibernética robusto e defensivo

A única maneira de lidar de forma eficaz com a evolução dos riscos de digitalização e o aumento das ameaças cibernéticas é instituir um programa de segurança contínuo. Infelizmente, muitas organizações apenas “seguem o fluxo” ao estabelecer recursos de segurança, ou seja, geralmente produzem muita documentação e investem fortemente em tecnologia. No entanto, elas dedicam pouco ou nenhum tempo para garantir a eficácia da governança ou da capacidade de avaliar e interpretar riscos.

Um programa de segurança defensivo evidencia a resposta à importante pergunta das partes interessadas: “A organização está fazendo o suficiente para proteger razoavelmente seus recursos de informação?”.

### Componentes de um programa de segurança cibernética



Fonte: Gartner

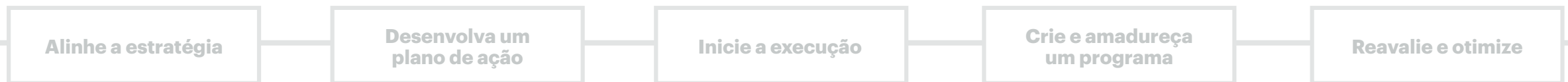
## Algumas das principais questões da iniciativa de segurança cibernética são:

- 1** Como isso dará suporte à resiliência dos negócios e às metas de crescimento, reduzindo ao mesmo tempo os riscos?
- 2** Como podemos usar uma abordagem orientada a resultados para estabelecer prioridades de segurança cibernética e investimentos?
- 3** Quais líderes e equipes precisam estar envolvidos?

## Quais são os principais estágios?

Este insight de práticas recomendadas é um compilado de interações com clientes que implementaram iniciativas de segurança cibernética com êxito. Este roteiro oferece uma sequência de objetivos e resultados desejados, e é útil para alinhar todas as partes interessadas.

Destacamos a seguir as principais etapas e algumas amostras de recursos associados da Gartner, mas a diretriz completa inclui detalhes de todas as etapas e recursos para cada estágio.



Alinhe a estratégia

Desenvolva um plano de ação

Inicie a execução

Crie e amadureça um programa

Reavalie e otimize



## Alinhe a estratégia

### Defina objetivos e crie um estudo de viabilidade

#### Tarefas selecionadas

Entender as principais prioridades de negócios; definir missão e visão do programa; identificar fatores determinantes de negócios, tecnologias e ameaças

Identificar metas, valor do programa e cargos e responsabilidades das principais partes interessadas

Definir os controles de segurança de acordo com as estratégias organizacionais e mapeá-las para obter um modelo de segurança padronizado

Obter feedback das partes interessadas, definir os principais objetivos e finalizar o resumo inicial do documento da estratégia de segurança

+ mais

#### Exemplo de recursos associados da Gartner

- **Consulta com analistas:** interaja com um analista para finalizar as métricas capazes de medir o impacto da segurança cibernética
- **Consulta com analistas:** interaja com um analista para discutir a abordagem certa de modo a comunicar o impacto comercial da segurança cibernética às partes interessadas
- **Pesquisa:** [Como criar um programa de segurança robusto e defensivo que permita a agilidade e o crescimento dos negócios](#)

+ mais



## Desenvolva um plano de ação

### Crie um modelo de priorização de riscos

#### Tarefas selecionadas

Conduzir uma avaliação de vulnerabilidade e um teste de penetração

Estabelecer o parâmetro de maturidade atual, definir o estado pretendido e conduzir uma análise de lacunas

Obter o apoio de executivos ou da diretoria e suporte para os recursos

Desenvolver arquitetura de segurança, modelo de política e camada de soluções

+ mais

#### Exemplo de recursos associados da Gartner

- **Pesquisa:** Fundamentos do diretor de segurança da informação – conjunto de ferramentas: apresentação do planejamento estratégico e painéis
- **Ferramenta:** [IT Score para gestão de riscos e segurança](#)
- **Pesquisa:** Ignition Guide para criar um orçamento anual de segurança cibernética

+ mais

Alinhe a estratégia

Desenvolva um plano de ação

Inicie a execução

Crie e amadureça um programa

Reavalie e otimize



## Inicie a execução

Projete e ajuste a estrutura da equipe

### Tarefas selecionadas

Integrar recursos, ferramentas e tecnologias

Estabelecer funções e responsabilidades para a equipe de segurança e identificar quais partes interessadas devem ser responsabilizadas, consultadas e informadas

Desenvolver competências essenciais e treinar para suprir habilidades ausentes ou desejadas

Usar métricas e incentivos para promover a responsabilização entre os proprietários

+ mais

### Exemplo de recursos associados da Gartner

- **Consulta pelo telefone:** interaja com um especialista para discutir “o padrão CARE para segurança cibernética”
- **Pesquisa:** leia sobre a ameaça à segurança cibernética e seu impacto sobre os negócios
- **Pesquisa:** [Como criar uma organização de segurança prática](#)

+ mais



## Crie e amadureça um programa

Mantenha a responsabilidade e a garantia por meio da governança

### Tarefas selecionadas

Desenvolver um recurso de resposta a incidentes graves e um plano de ação no caso de violações

Desenvolver uma estrutura de programa para monitorar e combater ameaças avançadas

Incentivar uma cultura de comportamento seguro nos funcionários e iniciar campanhas personalizadas de treinamento e conscientização

Desenvolver a elaboração de relatórios e respostas avançadas, além de criar um plano de comunicações para violações cibernéticas

+ mais

### Exemplo de recursos associados da Gartner

- **Consulta com analistas:** interaja com um analista para finalizar as métricas capazes de medir o impacto da segurança cibernética
- **Consulta com analistas:** interaja com um analista para discutir a abordagem certa de modo a comunicar o impacto comercial da segurança cibernética às partes interessadas
- **Pesquisa:** [Como criar um programa de segurança robusto e defensivo que permita a agilidade e o crescimento dos negócios](#)

+ mais

**Estabeleça  
um parâmetro**

**Identifique  
oportunidades**

**Implemente**

**Institucionalize**

**Reavalie e otimize**



## Reavalie e otimize

### Comunique o valor do programa

#### Tarefas selecionadas

- Criar um plano para comunicar o valor à organização e à diretoria
- Rastrear métricas e buscar feedback para avaliar e melhorar a eficácia do programa
- Revisitar a avaliação de maturidade para obter mais otimização

+ mais

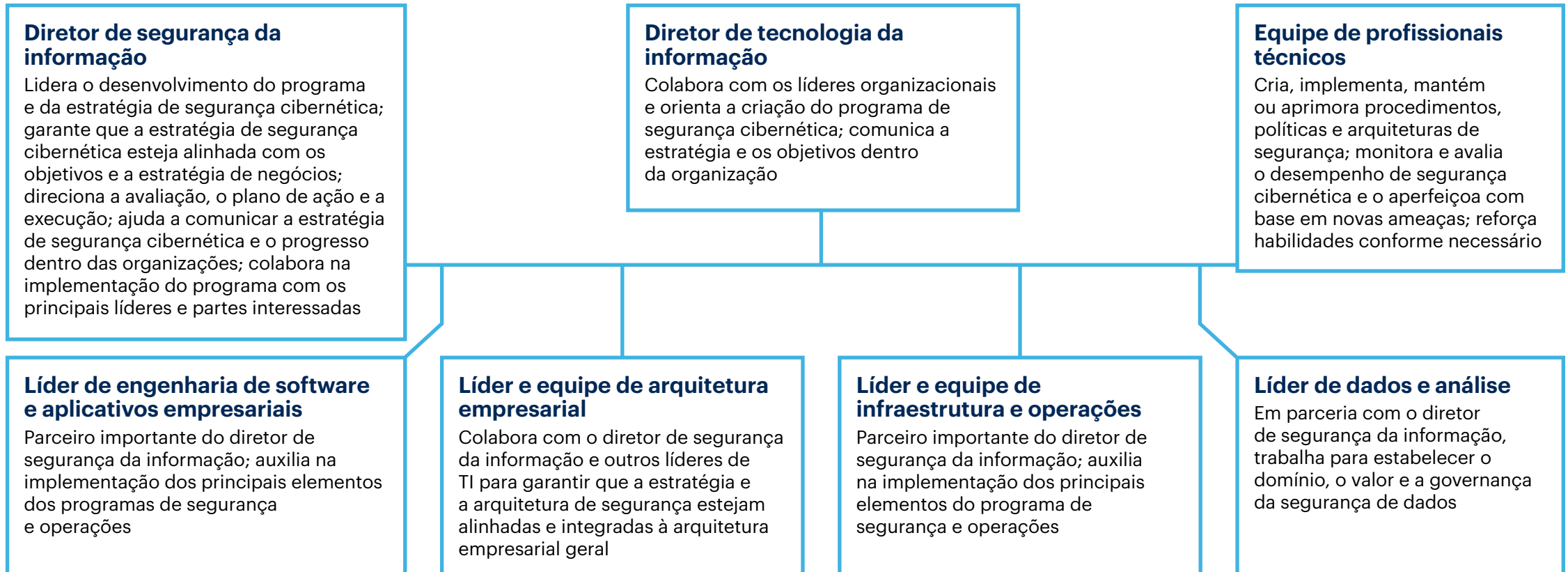
#### Exemplo de recursos associados da Gartner

- **Consulta pelo telefone:** discuta os principais pontos para ajudar na futura otimização da segurança cibernética da organização
- **Consulta com analistas:** refaça a avaliação Gartner IT Score para medir o progresso e priorizar novamente
- **Pesquisa:** Ferramenta – sessão de instrução da diretoria: como comunicar a postura de risco cibernético da sua organização

+ mais

# Quem precisa estar envolvido?

As empresas mais bem-sucedidas estabelecem equipes multifuncionais para suas iniciativas de segurança cibernética. Descrevemos nossas recomendações de cargos a serem envolvidos e suas funções para garantir o sucesso em cada etapa.





# História de sucesso do cliente: como viabilizar a conformidade de TI com uma diretriz de segurança cibernética

## Principal prioridade estratégica

Com o objetivo de simplificar os processos de negócios e desenvolver um ambiente pronto para o negócio digital, a Pacific Textiles queria desenvolver um modelo em conformidade com a TI para minimizar riscos de segurança cibernética.



## Como a Gartner ajudou

Com acesso aos especialistas, pesquisas e ferramentas da Gartner, a Pacific Textiles conseguiu digitalizar informações por meio de um sistema de planejamento de recursos empresariais (ERP), automatizar processos de manufatura com novas tecnologias e elaborar uma diretriz de segurança cibernética pronta para ser executada.



## Missão cumprida

Com a ajuda da Gartner, a Pacific Textiles foi capaz de:

- Adotar uma abordagem holística para os procedimentos de gestão de riscos e governança;
- Criar uma base sólida para o negócio digital;
- Otimizar processos de negócios, economizando tempo e energia para a alta gestão.

Gartner para diretores de segurança da informação

# Gere valor por toda a empresa com orientação especializada, ferramentas, redes de relacionamento com colegas do setor e eventos direcionados.



## Demonstre valor comercial

Seja um líder em cibersegurança melhor em áreas-chave:

- Função, relacionamentos, talento e cultura;
- Criação de orçamentos fáceis de defender;
- Estratégia e visão de um programa de cibersegurança.

Evite riscos com programas de cibersegurança cotidianos e sólidos:

- Gestão de risco empresarial;
- Futuro do trabalho, estratégias de resposta a riscos, gestão de mudanças.

Otimize investimentos e execução em tecnologia:

- Tendências em avanços tecnológicos emergentes;
- Ferramentas de medição e processo decisório com pragmatismo;
- Guias aprofundados de implementação técnica;
- Insights contextualizados do setor.

Saiba mais



## Acelere importantes iniciativas

Transforme estratégia em ação com ferramentas que aceleram a execução e atingem resultados de negócios:

- Diagnóstico de eficácia do diretor de segurança da informação;
- Avaliação de controles de cibersegurança;
- IT Score;
- Modelos de sessão de instrução para a diretoria.



## Redes de relacionamento com colegas

Conecte-se com outros líderes da indústria de segurança em chats individuais, discussões conduzidas por colegas e sondagens, além de acessar classificações e avaliações de tecnologia.



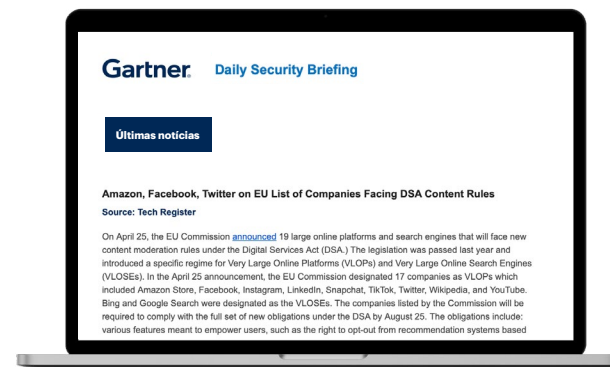
## Eventos motivadores

Tenha acesso VIP na Conferência Gartner Segurança & Gestão de Risco com diversas sessões de discussão educacionais e diversas oportunidades para se conectar com colegas do setor e especialistas da Gartner. Além disso, se inscreva para participar do CISO Circle e aproveite sessões e oportunidades de networking exclusivas.



## Informações diárias sobre segurança

Fique por dentro das notícias mais urgentes com um resumo de artigos de fontes de notícias confiáveis, inclusive um resumo global sobre diversas indústrias sobre as ameaças mais recentes e notícias de segurança do dia.



**“É a primeira coisa que leio todas as manhãs. Eu uso para conhecer as preocupações dos executivos, encaminhar qualquer nova vulnerabilidade a minha equipe e assegurar que estamos adotando as medidas necessárias para minimizar os riscos.”**

Diretor de segurança da informação, provedor global de tecnologia wireless

# Insights práticos e objetivos

Explore estas ferramentas e recursos adicionais gratuitos para líderes de segurança cibernética:

## Pesquisa

### [Manual para os primeiros 100 dias do diretor de segurança da informação](#)

Conheça as ações que o diretor de segurança da informação deve executar em seus primeiros 100 dias.

## Webinar

### [Trate a segurança cibernética como um investimento empresarial para obter melhores resultados](#)

Entenda como comunicar as métricas orientadas a resultados à diretoria.

## ebook

### [Visão da liderança para líderes de segurança e gestão de risco](#)

Explore as três principais prioridades estratégicas para líderes de segurança e gestão de risco.

## Conferência

### [Explore as conferências da Gartner sobre segurança cibernética](#)

Invista em sua estratégia de gestão de riscos e segurança cibernética participando de conferências da Gartner.

## Acesse outras diretrizes nesta série

[Proteja seus ativos empresariais com uma diretriz feita para amadurecer a segurança da informação](#)

[Diretriz: Impulsione o crescimento digital de sucesso com dados e análise](#)

[Como migrar arquiteturas de dados e análise para a nuvem: Diretriz](#)

[Aprimore sua diretriz para a governança de dados eficaz](#)

[Diretriz: Como formular uma estratégia na nuvem eficaz](#)

Já é um cliente?

Obtenha acesso a mais recursos no seu portal do cliente. [Conectar](#)

# Conecte-se conosco

Obtenha insights práticos e objetivos para cumprir suas principais prioridades estratégicas. A nossa orientação e ferramentas especializadas possibilitam decisões mais ágeis, inteligentes e desempenho mais sólido. Fale conosco e torne-se cliente:

**EUA:** +1 855 811 7593

**Internacional:** +44 (0) 3330 607 044

Torne-se cliente

**Saiba mais sobre Gartner para líderes de segurança cibernética**

[gartner.com/en/cybersecurity](https://gartner.com/en/cybersecurity)

**Mantenha-se conectado com os insights mais recentes**

