


# GUIAS PRÁTICOS DE SEGURANÇA: ITIL, NIST, FIPS, CIS BENCHMARKS E GUIAS DE FORNECEDORES

The slide features a dark blue header with white text. Below the header, there are several horizontal lines of varying lengths and colors (teal, light blue, and white) that create a decorative, layered effect across the width of the slide.

# ITIL



**ITIL (Information Technology Infrastructure Library)** é um conjunto de práticas e estruturas de gerenciamento de serviços de TI que tem sido amplamente adotado em organizações ao redor do mundo.



Embora o ITIL tenha sido originalmente desenvolvido para melhorar a qualidade e a eficiência dos serviços de TI, ele pode ser adaptado e aplicado de maneira eficaz ao campo da Segurança da Informação.



Veremos como o ITIL pode ser voltado para a Segurança da Informação e como essas duas áreas se complementam.



**Alinhamento Estratégico:** Um dos princípios fundamentais do ITIL é o alinhamento das práticas de TI com as metas e objetivos estratégicos da organização.



Para a Segurança da Informação, isso significa alinhar as práticas de segurança com as necessidades de negócios e conformidade regulatória.



O ITIL fornece estruturas para definir estratégias de segurança, avaliar riscos e alinhar a segurança com os objetivos gerais da organização.



**Gerenciamento de Serviços de Segurança:** ITIL oferece uma estrutura para o gerenciamento de serviços de TI, que pode ser adaptada para a gestão de serviços de segurança da informação.



Isso inclui a criação de catálogos de serviços de segurança, o estabelecimento de níveis de serviço (SLAs) para garantir que as práticas de segurança atendam às expectativas da organização e a criação de processos para a entrega eficiente de serviços de segurança.



**Gerenciamento de Incidentes de Segurança:** A Segurança da Informação está intrinsecamente ligada à resposta a incidentes.



O ITIL oferece estruturas para o gerenciamento de incidentes de TI, que podem ser facilmente adaptadas para o gerenciamento de incidentes de segurança.



Garantindo que a organização esteja preparada para responder eficazmente a violações de segurança e eventos cibernéticos.



**Gerenciamento de Mudanças de Segurança:** O ITIL também fornece diretrizes para o gerenciamento de mudanças em ambientes de TI.



No contexto da Segurança da Informação, isso é crucial, pois as mudanças nos sistemas e nas políticas de segurança podem afetar significativamente a postura de segurança da organização.



O ITIL ajuda a planejar e gerenciar mudanças de segurança de maneira controlada.



**Melhoria Contínua:** O ciclo de vida do serviço do ITIL inclui a etapa de melhoria contínua, que é fundamental para a Segurança da Informação.



À medida que as ameaças cibernéticas evoluem, é essencial que as práticas de segurança sejam continuamente avaliadas e aprimoradas.



O ITIL oferece estruturas para monitorar e melhorar constantemente os processos de segurança.



**Gestão de Fornecedores:** A maioria das organizações depende de fornecedores para serviços de TI e segurança.




O ITIL inclui práticas para gerenciar relacionamentos com fornecedores, o que é importante para garantir que os parceiros de segurança cumpram os requisitos da organização.




**Conformidade e Auditoria:** O ITIL pode ser usado para definir e monitorar controles de segurança, ajudando na conformidade com regulamentações e padrões, como o GDPR, ISO 27001, entre outros.

**Treinamento e Conscientização:** O ITIL também pode ser adaptado para incluir práticas de treinamento e conscientização em segurança da informação, garantindo que todos os funcionários estejam cientes das políticas de segurança e saibam como agir corretamente.

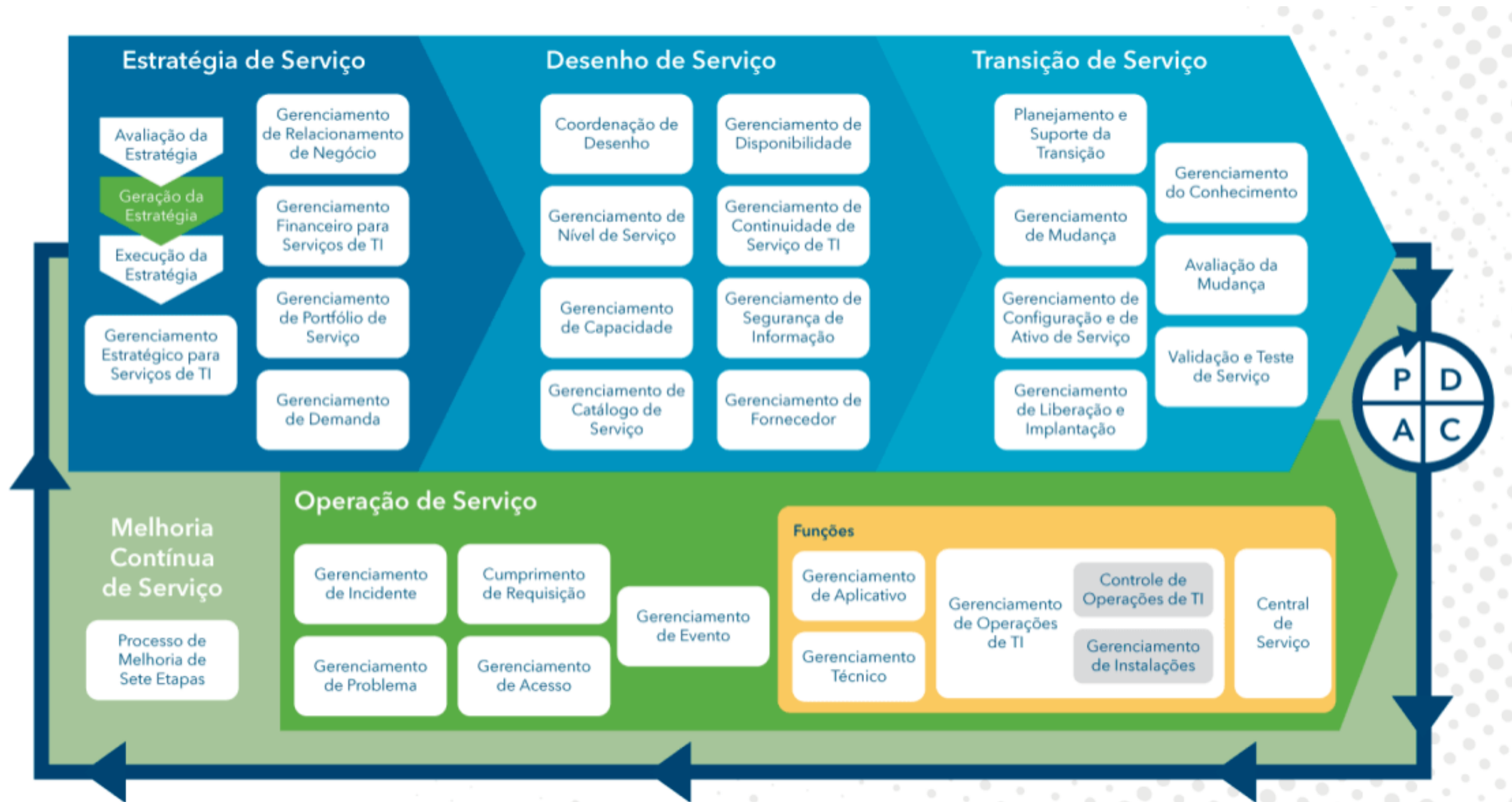
Em resumo, o ITIL pode ser uma abordagem valiosa para melhorar a gestão da Segurança da Informação em uma organização.



Fornece uma estrutura sólida para o gerenciamento de serviços de segurança, alinhamento estratégico e melhoria contínua, garantindo que as práticas de segurança sejam eficazes e estejam alinhadas com os objetivos gerais da organização.



Adaptar as diretrizes do ITIL para a Segurança da Informação pode contribuir significativamente para a proteção dos ativos e dados críticos da organização.



Estrutura de processos do ITIL v3 ([AXELOS](#), 2019)

## Transição de Serviço:

Planejamento e Suporte a Transição  
G. Ativo e Configuração de Serviço  
G. Mudança  
G. Liberação e Implantação  
Validação e Teste de serviço  
Avaliação da Mudança  
G. Conhecimento

Melhoria Contínua de Serviço:  
Metodologia

**Principais Processos da Operação de Serviços de TI**  
**A seta aponta para a etapa da Operação de Serviços no**  
**Ciclo de Vida do Serviço da ITIL**

## Estratégia de Serviço:

G. Estratégico para serviços de TI  
G. de Portfólio  
G. da Demanda  
G. Financeiro  
G. Relacionamento com o Negócio

## Desenho de Serviço:

Coordenação do Desenho  
G. Nível de Serviço  
G. Catálogo de Serviço  
G. Disponibilidade  
G. Segurança da Informação  
G. Fornecedor  
G. Capacidade  
G. Continuidade

## Operação de Serviço:

G. Incidentes  
G. Problemas  
G. Eventos  
Cumprimento de Requisição  
G. de Acesso

# Vídeo

- **O que é ITIL e para que serve?**
  - <https://www.youtube.com/watch?v=uxw9RWRwExE>

# NIST

---

O Instituto Nacional de Padrões e Tecnologia (NIST- National Institute of Standards and Technology,) é uma agência governamental dos Estados Unidos que fornece diretrizes e padrões para uma ampla gama de áreas, incluindo Segurança da Informação.

---

O NIST desenvolveu o "Framework for Improving Critical Infrastructure Cybersecurity" (também conhecido como o NIST Cybersecurity Framework), que é uma referência importante para as organizações que desejam fortalecer suas práticas de segurança cibernética.

---

Veremos como o NIST se relaciona com a Segurança da Informação.

- **Estrutura de Controle e Gerenciamento de Risco:** oferece um conjunto de controles de segurança detalhados no "**NIST Special Publication 800-53**" e no "**NIST Special Publication 800-171**". Esses documentos descrevem controles de segurança abrangentes que podem ser implementados para proteger sistemas e informações. Eles fornecem uma estrutura robusta para o gerenciamento de riscos de segurança da informação.
- **Framework de Gerenciamento de Risco:** o **NIST Cybersecurity Framework** é um guia amplamente adotado para gerenciamento de riscos cibernéticos. Ele fornece diretrizes para a identificação, proteção, detecção, resposta e recuperação de incidentes de segurança cibernética. O framework ajuda as organizações a avaliar seu nível de maturidade em segurança e a implementar melhorias.

- **Padrões e Diretrizes:** desenvolve padrões e diretrizes que podem ser usados para garantir a segurança da informação. O "**NIST Special Publication 800-63**" é um exemplo, fornecendo orientações sobre autenticação e controle de acesso.
- **Segurança em Sistemas Críticos:** é especialmente conhecido por suas diretrizes para sistemas críticos, incluindo o "**NIST Cybersecurity Framework para Infraestrutura Crítica**". Isso é relevante para organizações que operam infraestruturas críticas, como energia, transporte e saúde.



- **Padrões de Criptografia:** responsável pelo desenvolvimento de padrões de criptografia amplamente utilizados, como os Padrões de Criptografia Avançada (Advanced Encryption Standard - AES). Esses padrões são fundamentais para proteger a confidencialidade dos dados.
- **Treinamento e Educação:** oferece recursos de treinamento e educação em Segurança da Informação, incluindo materiais de conscientização em segurança e diretrizes para a formação de profissionais de segurança.

- **Conformidade com Regulamentações:** muitas regulamentações, como o **Federal Information Security Modernization Act (FISMA)** dos EUA, exigem que as agências governamentais e organizações adotem as diretrizes do NIST em suas práticas de segurança. Isso ajuda a garantir a conformidade regulatória em relação à segurança da informação.
- **Avaliação de Terceiros:** fornece orientações sobre avaliação de segurança por terceiros, que são fundamentais para verificar a conformidade com os controles de segurança e identificar vulnerabilidades.
  - A avaliação de segurança por terceiros é um processo no qual uma entidade externa, que não faz parte da organização, é contratada para avaliar e testar a segurança dos sistemas, redes, processos e políticas de segurança.



---

O NIST desempenha um papel importante no fornecimento de diretrizes, padrões e melhores práticas para a segurança da informação.

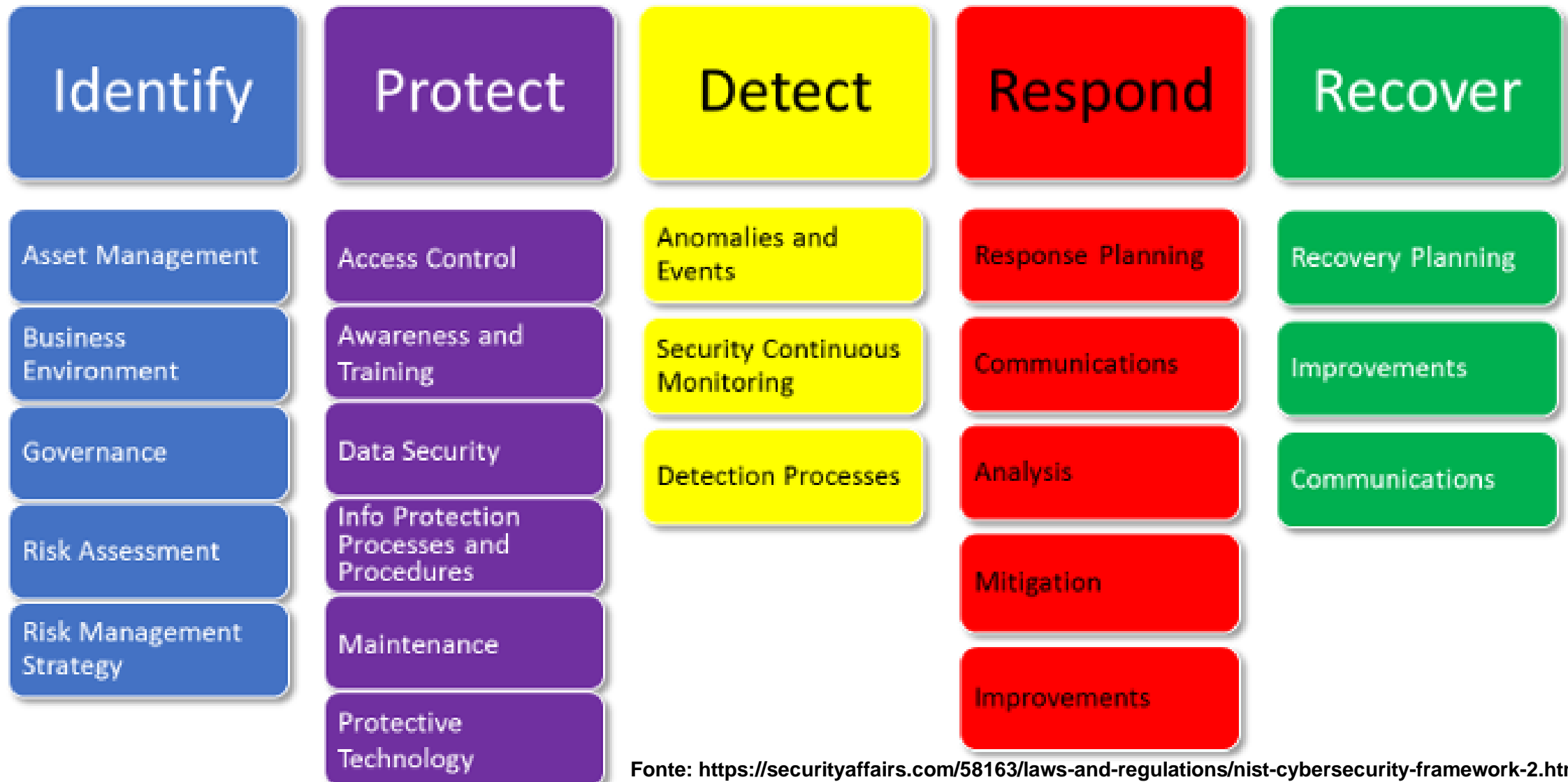
---

As organizações podem usar os recursos do NIST para fortalecer sua postura de segurança e garantir que estejam alinhadas com as melhores práticas reconhecidas internacionalmente.

---

A adoção das diretrizes do NIST pode ajudar a proteger os ativos e dados críticos da organização contra ameaças cibernéticas.

# NIST Cyber Security Framework





Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Fonte: <https://www.base4sec.com/research/pt/Cybersecurity-Framework-v2.0/>

- O NIST iniciou o processo de atualização do CSF, desde 2018 temos sua versão 1.1. Nesta nova atualização 2.0, o trabalho está sendo feito na evolução das ameaças, mapeando os padrões e visando um formato mais simples para permitir que as organizações lidem com os riscos.
- Nesse processo, novamente, conta ativamente com o feedback das partes interessadas (Comunidade, indústria, academia) e buscando opiniões diversas no processo de atualização.





# FIPS (Federal Information Processing Standards)

- O Federal Information Processing Standards (FIPS) é um conjunto de padrões e diretrizes de segurança de informações emitido pelo governo dos Estados Unidos, especificamente pelo National Institute of Standards and Technology (NIST), uma agência do Departamento de Comércio dos EUA.
- O FIPS desempenha um papel crucial na segurança da informação, especialmente em ambientes governamentais e em organizações que lidam com informações sensíveis.

- **Padrões de Criptografia:** inclui padrões para criptografia, como o **FIPS PUB 140-2**, que especifica os requisitos de segurança para módulos criptográficos. Isso é fundamental para proteger dados confidenciais e sensíveis, garantindo que os algoritmos de criptografia e os módulos criptográficos sejam seguros.
- **Conformidade com Leis e Regulamentos:** é amplamente reconhecido como um padrão de segurança para proteger informações sensíveis e, portanto, é crucial para garantir a conformidade com regulamentações governamentais e setoriais, como o **Health Insurance Portability and Accountability Act (HIPAA)** e o **Federal Information Security Management Act (FISMA)**.



- **Acesso Seguro a Sistemas:** os padrões FIPS incluem requisitos para autenticação forte e métodos de controle de acesso a sistemas. Isso ajuda a garantir que apenas pessoas autorizadas tenham acesso a informações sensíveis.
- **Proteção de Dados em Trânsito:** também inclui diretrizes para proteger a segurança das comunicações, especificando protocolos seguros de comunicação e criptografia de dados em trânsito.
- **Verificação de Identidade:** define padrões para a verificação da identidade, como a autenticação de dois fatores, o que é fundamental para garantir que as pessoas sejam quem afirmam ser antes de acessar informações sensíveis.

- **Segurança de Hardware e Software:** os padrões FIPS se aplicam não apenas à criptografia, mas também a hardware e software de segurança. Isso inclui a segurança de módulos criptográficos e a conformidade com requisitos rigorosos de segurança.
- **Teste e Certificação:** o FIPS exige testes e certificação rigorosos para sistemas e produtos de segurança de TI, garantindo que eles atendam aos padrões especificados de segurança.

- **Proteção de Sistemas Críticos:** é particularmente relevante para a proteção de sistemas e infraestrutura crítica, como os utilizados em setores como energia, transporte e saúde. Os padrões ajudam a garantir a resiliência desses sistemas contra ameaças cibernéticas.
- **Políticas de Segurança e Auditoria:** Os padrões FIPS também abrangem o desenvolvimento de políticas de segurança da informação e práticas de auditoria para garantir a conformidade com as diretrizes de segurança.

- Em resumo, o FIPS é uma série de padrões e diretrizes de segurança de informações desenvolvida pelo governo dos Estados Unidos, desempenhando um papel fundamental na segurança da informação.
- Ele estabelece requisitos rigorosos para a proteção de informações sensíveis, criptografia, autenticação e controle de acesso. Além disso, o FIPS é amplamente adotado em organizações governamentais e em setores que lidam com informações sensíveis, contribuindo para a segurança cibernética e a conformidade regulatória.

# Some Specifications of FIPS



## **FIPS 140**

Security Requirements for  
Cryptographic Module in 4  
Levels



## **FIPS 199**

Standards for Security  
Categorization



## **FIPS 180**

Secure Hash Standard



## **FIPS 200**

Minimum Security Requirements



## **FIPS 186**

Digital Signature Standard



## **FIPS 201**

Personal Identity Verification (PIV)



## **FIPS 197**

Advanced Encryption  
Standard (AES)



## **FIPS 202**

SHA-3 Standard:  
Permutation-Based Hash and  
Extendable-Output Functions



## **FIPS 198**

Keyed-Hash Message  
Authentication Code (HMAC)

# CIS (Center for Internet Security) Benchmarks

1

Os CIS (Center for Internet Security) Benchmarks são uma série de guias e melhores práticas para a configuração segura de sistemas de TI e redes de computadores.

2

Eles são uma referência valiosa para melhorar a postura de SI em organizações.

3

Os CIS Benchmarks abrangem uma ampla gama de SOs, aplicativos e dispositivos e fornecem diretrizes específicas para a configuração de cada um.



- **Padronização de Configurações Seguras:** os CIS Benchmarks estabelecem configurações seguras recomendadas para sistemas operacionais, aplicativos e dispositivos. Isso ajuda as organizações a padronizar suas configurações de segurança, minimizando assim possíveis pontos fracos de configuração que poderiam ser explorados por invasores.
- **Redução de Superfície de Ataque:** seguindo as diretrizes do CIS Benchmark, as organizações podem reduzir a superfície de ataque, ou seja, a quantidade de pontos de entrada potenciais para invasores. Isso é fundamental para minimizar os riscos de segurança.

- **Proteção contra Ameaças Conhecidas:** os CIS Benchmarks são frequentemente atualizados para refletir as ameaças cibernéticas mais recentes. Isso ajuda as organizações a se proteger contra vulnerabilidades conhecidas, mantendo suas configurações de segurança atualizadas.
- **Alinhamento com Padrões de Segurança:** os CIS Benchmarks são frequentemente alinhados com padrões de segurança reconhecidos, como os padrões do NIST, ISO 27001 e outros. Isso facilita a conformidade com regulamentações e a adoção de boas práticas amplamente aceitas.



- **Avaliação e Auditoria:** os CIS Benchmarks também podem ser usados para avaliar a conformidade com as configurações de segurança recomendadas. Isso é útil para auditorias de segurança internas e externas, garantindo que a organização esteja aderindo a padrões de configuração segura.
- **Melhoria Contínua:** as diretrizes do CIS incentivam a melhoria contínua das configurações de segurança. À medida que as ameaças evoluem e novas vulnerabilidades são descobertas, as organizações podem atualizar suas configurações com base nas últimas recomendações do CIS.

- **Redução de Erros Humanos:** ao seguir os CIS Benchmarks, as organizações podem reduzir a probabilidade de erros de configuração que podem levar a violações de segurança. As configurações recomendadas são cuidadosamente elaboradas para minimizar riscos.
- **Flexibilidade e Customização:** embora os CIS Benchmarks forneçam configurações seguras recomendadas, eles também permitem alguma flexibilidade e customização para atender às necessidades específicas da organização. Isso significa que as organizações podem adaptar as recomendações aos seus ambientes específicos.

- **Apoio à Conscientização em Segurança:** os CIS Benchmarks podem ser usados para educar a equipe de TI e conscientizar os funcionários sobre as melhores práticas de segurança. Eles fornecem uma referência clara sobre como configurar sistemas de forma segura.

Em resumo, os CIS Benchmarks desempenham um papel importante na Segurança da Informação, fornecendo diretrizes detalhadas e atualizadas para configurar sistemas e redes de forma segura. Seguir essas diretrizes ajuda as organizações a proteger seus ativos e dados críticos, reduzindo os riscos de segurança cibernética e mantendo a conformidade com padrões e regulamentações de segurança.

## Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

## Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

## Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

# Guias de Fornecedores

Os guias de fornecedores relacionados à segurança da informação são documentos criados por fabricantes de sistemas operacionais, bancos de dados, servidores de aplicação e outros produtos de software e hardware.

Esses guias são projetados para ajudar as organizações a configurar, implementar e manter esses sistemas de forma segura, seguindo as melhores práticas e recomendações de segurança específicas do fornecedor.

- Algumas razões pelas quais esses guias são importantes na área de Segurança da Informação:
- **Padronização da Configuração Segura:** os guias de fornecedores estabelecem padrões específicos para a configuração segura de sistemas. Isso ajuda as organizações a padronizar suas configurações, minimizando possíveis pontos fracos de configuração que poderiam ser explorados por invasores.
- **Melhores Práticas do Fornecedor:** os guias são geralmente desenvolvidos pelos próprios fabricantes, que possuem conhecimento profundo sobre seus produtos. Eles incluem as melhores práticas específicas do fornecedor para proteger e manter seus sistemas.

- **Segurança Integrada:** geralmente abordam recursos de segurança integrados aos produtos, como firewalls, monitoramento de segurança e controles de acesso. Isso ajuda as organizações a aproveitar ao máximo as capacidades de segurança oferecidas pelos sistemas.
- **Resposta a Ameaças Conhecidas:** podem incluir recomendações para lidar com vulnerabilidades e ameaças específicas que são conhecidas para o produto ou plataforma. Isso ajuda a proteger contra ataques direcionados.

- **Conformidade Regulatória:** podem ajudar as organizações a atender aos requisitos de conformidade regulatória. Eles fornecem orientações para garantir que as configurações estejam alinhadas com regulamentações específicas.
- **Avaliação de Riscos:** os guias muitas vezes oferecem orientações sobre como avaliar riscos e ameaças associados ao produto ou sistema, permitindo que as organizações identifiquem e mitiguem eficazmente esses riscos.



- **Documentação de Segurança:** fornecem documentação oficial e referências relacionadas à segurança do produto, o que é essencial para auditorias internas e externas.
- **Atualizações e Revisões:** à medida que novas ameaças e vulnerabilidades surgem, os guias de fornecedores são geralmente atualizados. Isso permite que as organizações se mantenham atualizadas com as últimas recomendações de segurança.

- Exemplos de guias de fornecedores notáveis incluem:
  - "Microsoft Security Baseline" para sistemas operacionais Windows;
  - Guias de segurança do Oracle Database;
  - "Red Hat Security Guide" para sistemas baseados no Red Hat Enterprise Linux.
- Esses guias fornecem detalhes específicos para configurar e manter esses sistemas de forma segura.
- Os guias de fornecedores relacionados à segurança da informação são recursos valiosos que ajudam as organizações a proteger seus sistemas e dados contra ameaças cibernéticas. Eles oferecem orientações específicas do fabricante para configurar sistemas de forma segura, manter a conformidade regulatória e responder a ameaças conhecidas.

- **Para saber mais...**
- **Linhas de base de segurança Microsoft**
  - <https://learn.microsoft.com/pt-br/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines>
- **Segurança do banco de dados Oracle**
  - <https://www.oracle.com/br/security/database-security/>
- **Security Guide RED HAT ENTERPRISE LINUX 7**
  - [https://access.redhat.com/documentation/pt-br/red\\_hat\\_enterprise\\_linux/7/html/security\\_guide/index](https://access.redhat.com/documentation/pt-br/red_hat_enterprise_linux/7/html/security_guide/index)