Guia de requisitos mínimos de segurança e privacidade para APIs

Secretaria de Governo Digital

Setembro/2021

Lei Geral de Proteção de Dados – Lei 13.709/18

Estratégia de Governo Digital 2020-2022 / Um Governo Confiável

Objetivo 10: Implementação da Lei Geral de Proteção de Dados - LGPD no Governo
Iniciativa 10.1: Estabelecer método de adequação e conformidade dos órgãos com os requisitos da Lei Geral de Proteção de Dados, até 2020

Objetivo 11: Garantia da segurança das plataformas de governo digital e de missão crítica
Iniciativa 11.3. Definir padrão mínimo de segurança cibernética a ser aplicado nos canais e serviços digitais.

PROJETO ADEQUAÇÃO À LGPD

Objetivo: **Definir e implementar estratégia para atuar preventivamente nas frentes de segurança da informação e privacidade de dados, com o intuito de fomentar a cultura de proteção de dados, implementando ações que visam avançar no processo de adequação à LGPD, minimizando os riscos.**

gov.br

OBJETIVO DO GUIA

- **Fomentar a adequação à Lei Geral de Proteção de Dados Pessoais e a ampliar a proteção de APIs da Administração Pública Federal;**

- **Auxiliar os profissionais de desenvolvimento e manutenção de APIs a atenderem os requisitos mínimos de privacidade e segurança da informação, antes e durante o desenvolvimento da aplicação.**

AGENDA


1
Cenários e Desafios
2
Incidentes - Desafios
3
Alinhamento de expectativas
4
Referências
5
Conhecendo o Guia
6
Diretrizes Gerais
7
Requisitos Gerais
8
Requisito Geral 1: Privacy by Design
9
Requisito Geral 2: Security by Design
10
Requisito Específico 1: Privacidade
11
Requisito Específico 2: Segurança

CENÁRIOS E DESAFIOS

3.000 (72%)
serviços digitais

279 Sistemas de missão crítica na APF

GOV.BR
84 Mi de usuários
70 Mi Visitas/mês

Até 60% de servidores em trabalho remoto

Demanda por digitalização

Riscos de Segurança da Informação e proteção a privacidade

"Novo vazamento de dados do Ministério da Saúde expõe 200 milhões de brasileiros" (12/2020)

"Ataque hacker ao STJ é o pior da história do Brasil" (11/2020)

"Ataque hacker: portal do TRF-1 é tirado do ar como medida preventiva" (12/2020)

$1.12 Mi
Prejuízo médio no Brasil para um vazamento de dados em 2020*

gov.br

INCIDENTES - DESAFIOS

Brasil 1º em Phishing em 2021

O Brasil teve um aumento de 23% nos casos de cibercrimes nos primeiros oito meses de 2021 em comparação ao mesmo período no ano anterior. Foram 481 milhões de tentativas de infecção com os 20 malwares mais populares.

Kaspersky Lab

Brasil 2º em DDoS em 2021

O Brasil sofreu entre 1º de janeiro e 3 de agosto de 2021 mais de 439.000 ataques cibernéticos, 7,1% de um total de 6,4 milhões realizados em todo o mundo. Os ataques registrados foram do tipo de negação de serviço distribuído (DDoS, na sigla em inglês)

NETSCOUT SYSTEMS, INC.

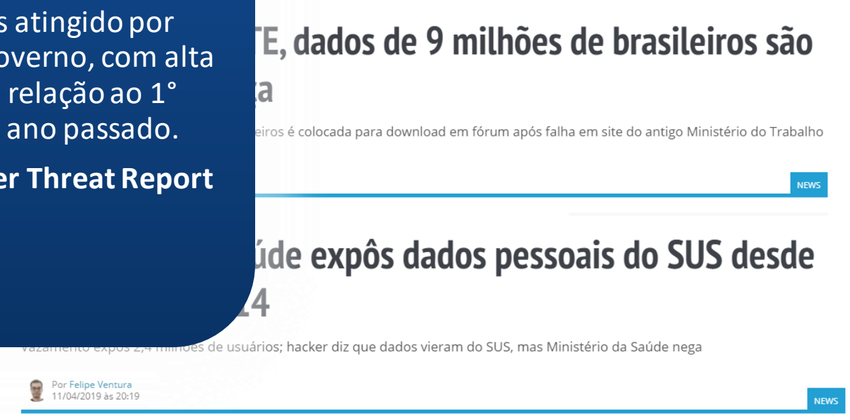
Brasil 5º em Ransomware em 2021

Só nos seis primeiros meses deste ano, os registros no país já superaram o total de ocorrências de 2020. Se considerados apenas os casos de ransomware, já foram 9,1 milhões de casos em 2021.

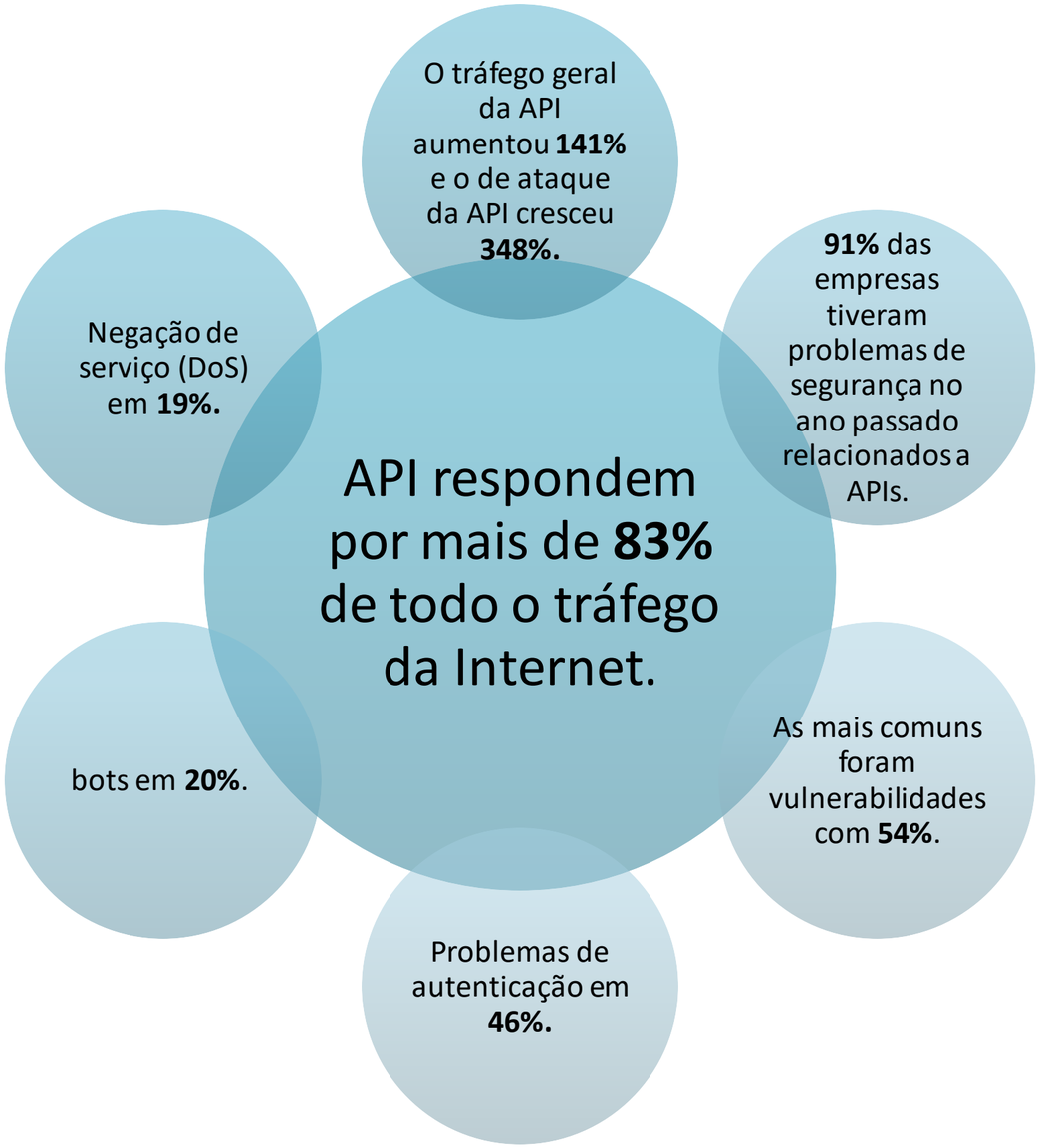
SonicWall Cyber Threat Report

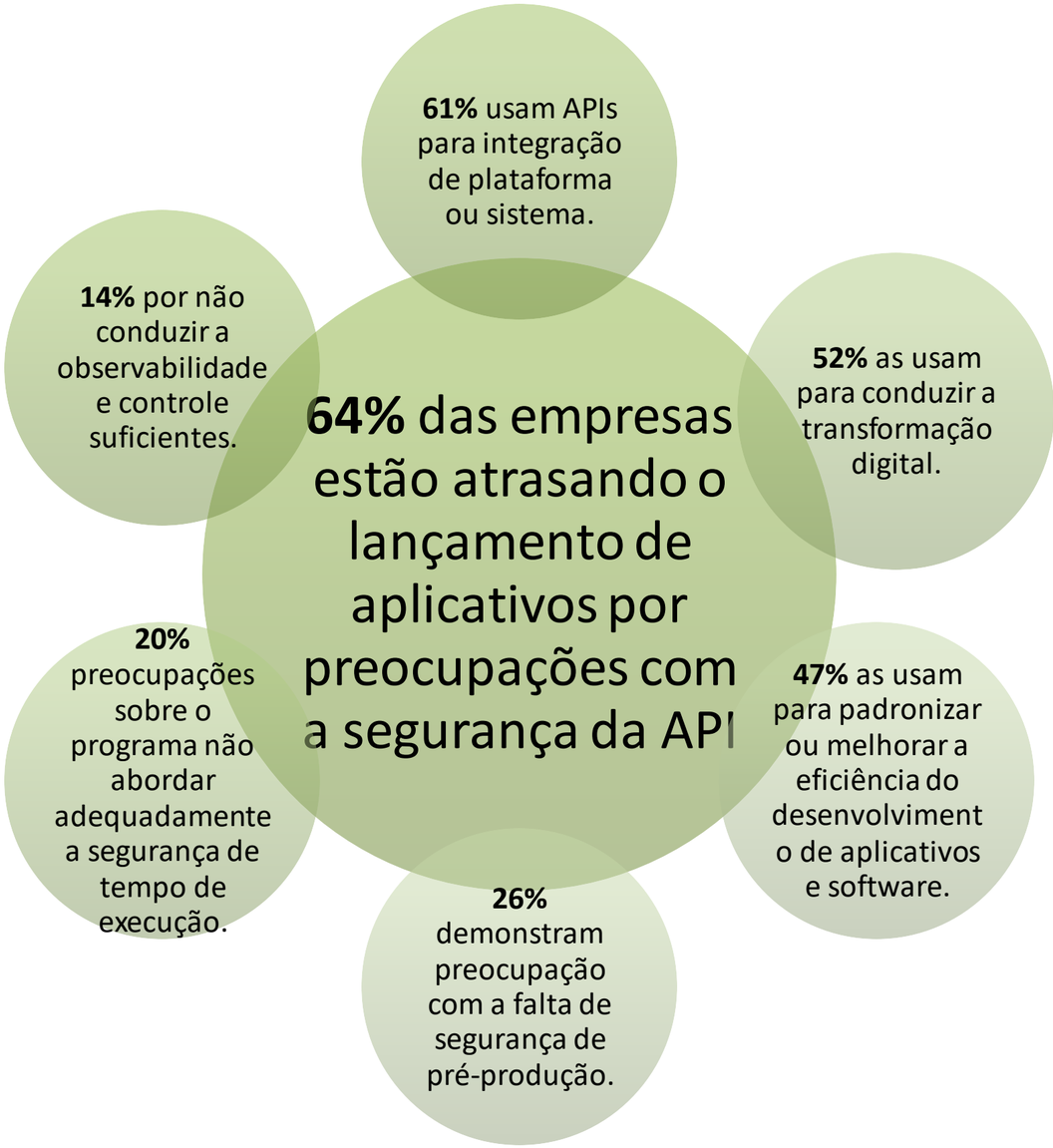
O setor mais atingido por ataques foi o governo, com alta de 917% em relação ao 1° semestre do ano passado.

SonicWall Cyber Threat Report



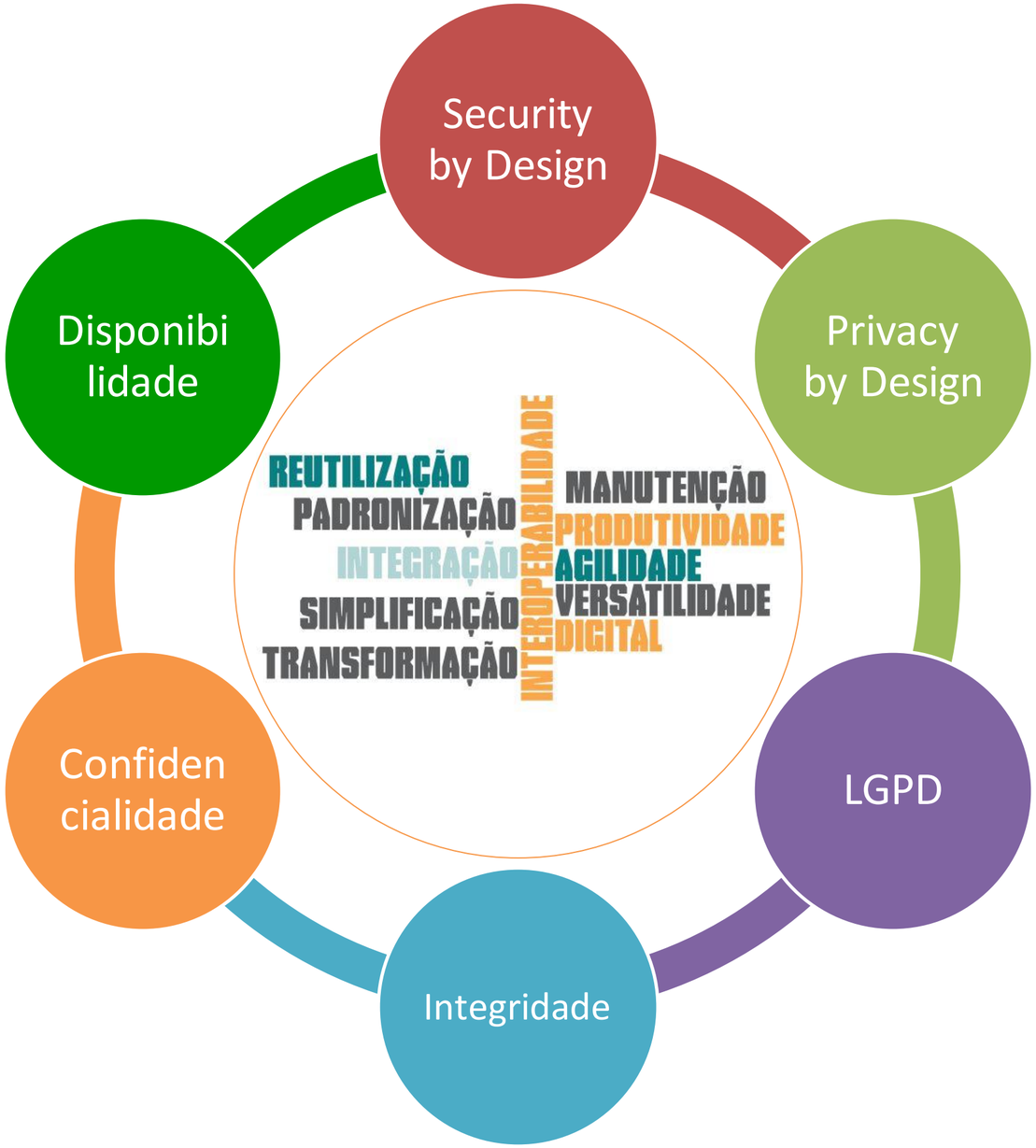
INCIDENTES - DESAFIOS





Fonte: PALO ALTO, Calif. – July 28, 2021 – Salt Security, API security company, Cool Vendor Gartner - Salt Labs State of API Security Report, Q3 2021

ALINHAMENTO DE EXPECTATIVAS - BENEFÍCIOS

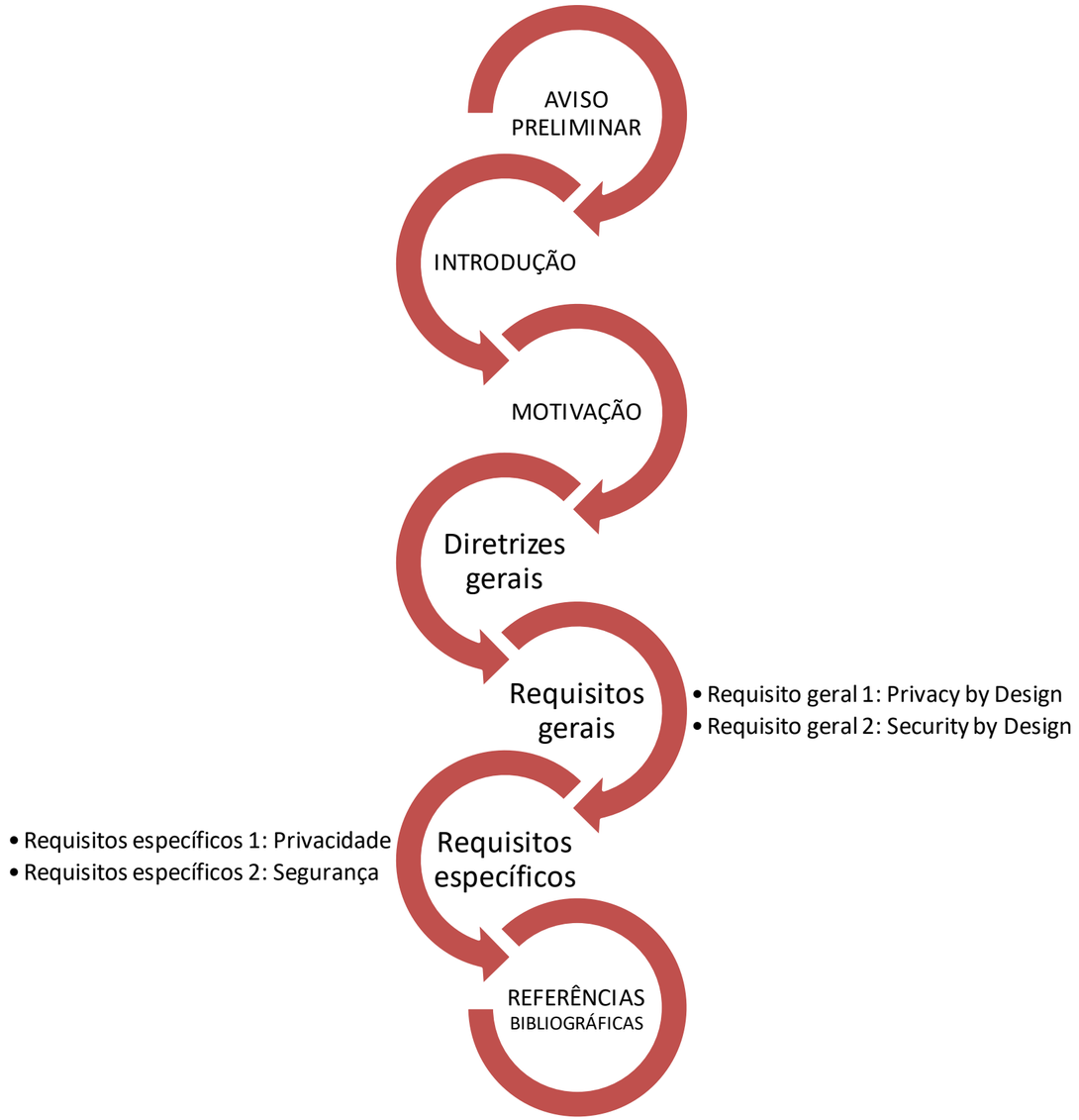


REFERÊNCIAS

gov.br

REFERÊNCIAS

DIVISÃO DO GUIA



DIRETRIZES GERAIS

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

Framework de Segurança Cibernética NIST versão 1.1.

Função	Categoria	Subcategoria	Referencias Informativas		
			CIS Controls Version 8	NIST SP 800-53 Rev. 5	ISO/IEC 27001:2013
IDENTIFICAR (ID)	**Gestão de ativos (ID.AM):** Os dados, pessoal, dispositivos, sistemas e recursos que permitem à organização atingir os objetivos de negócios são identificados e gerenciados de acordo com sua importância relativa para os objetivos organizacionais e a estratégia de risco da organização.	**ID.AM-2:** Plataformas de software e aplicativos dentro da organização são inventariados.	2 – 2.1 2 – 2.2 16 – 16.4	CM-8	A.8.1.1, A.8.1.2, A.12.5.1
		ID.AM-3: A comunicação organizacional e os fluxos de dados são mapeados.	3 – 3.8	AC-4, CA-3, CA-9, PL-8, SA-17	A.13.2.1, A.13.2.2
		ID.AM-4: Os sistemas de informação externos são catalogados.	12 – 12.4	AC-20, PM-5, SA-9	A.11.2.6
		ID.AM-5: Recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software) são priorizados com base em sua classificação, criticidade e valor comercial.	3 – 3.2 3 – 3.7	CP-2, RA-2, RA-9, SA-20, SC-6	A.8.2.1
		ID.AM-6: As funções e responsabilidades de segurança cibernética para toda a força de trabalho e partes interessadas terceirizadas (por exemplo, fornecedores, clientes, parceiros) são estabelecidas.	14 – 14.1	CP-2, PS-7, PM-2, PM-29	A.6.1.1
	Ambiente de Negócios (ID.BE): A missão, os objetivos, as partes interessadas e as atividades da organização são	**ID.BE-1:** O papel da organização na cadeia de abastecimento é identificado e comunicado.	–	SR-1, SR-3	A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
		ID.BE-4: Dependências e funções críticas para entrega de serviços críticos são	–	PM-8	A.11.2.2, A.11.2.3, A.12.1.3

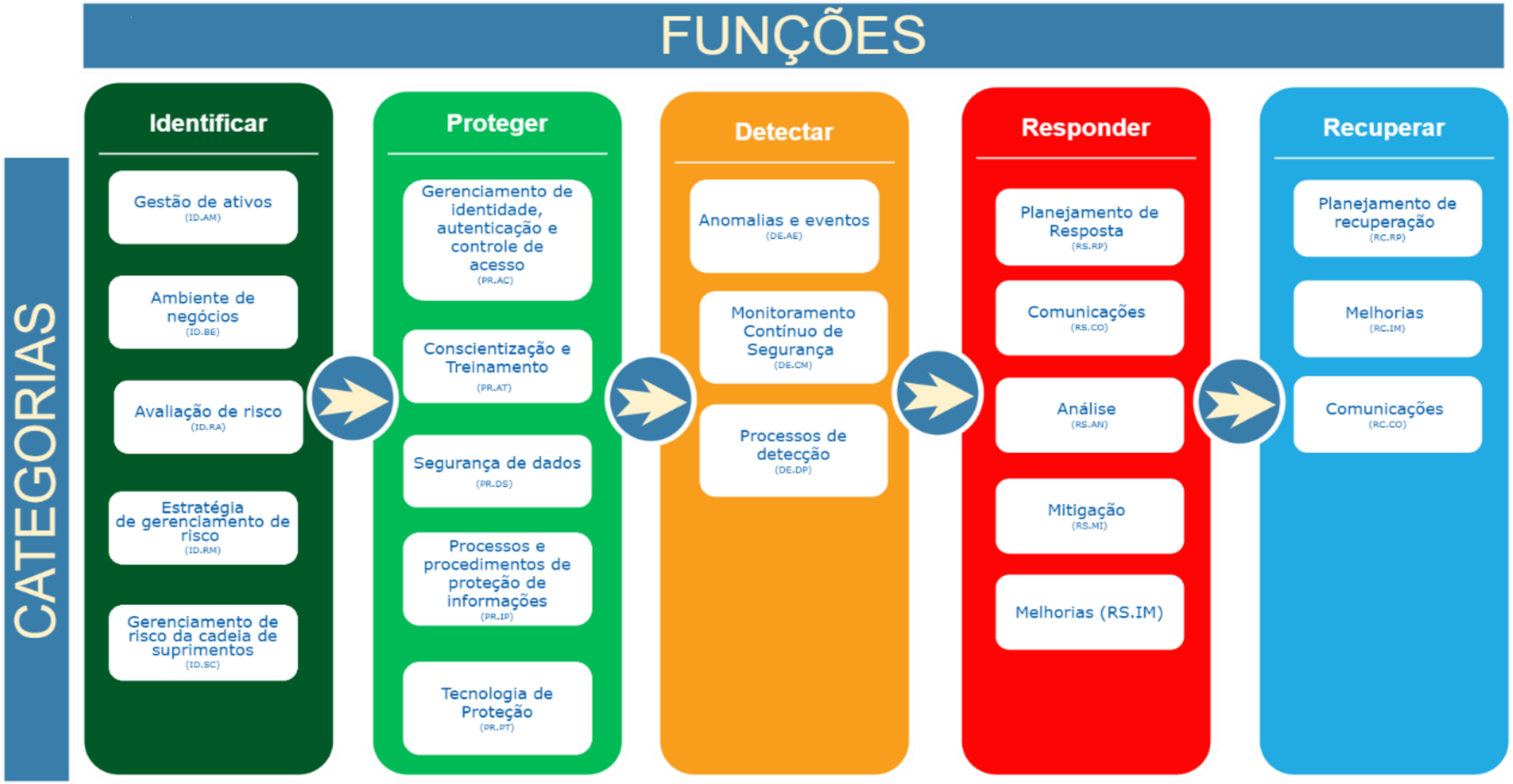
Disponível em https://www.nist.gov/cyberframework

gov.br

DIRETRIZES GERAIS

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

Framework de Segurança Cibernética NIST versão 1.1.



Disponível em https://www.nist.gov/cyberframework

gov.br

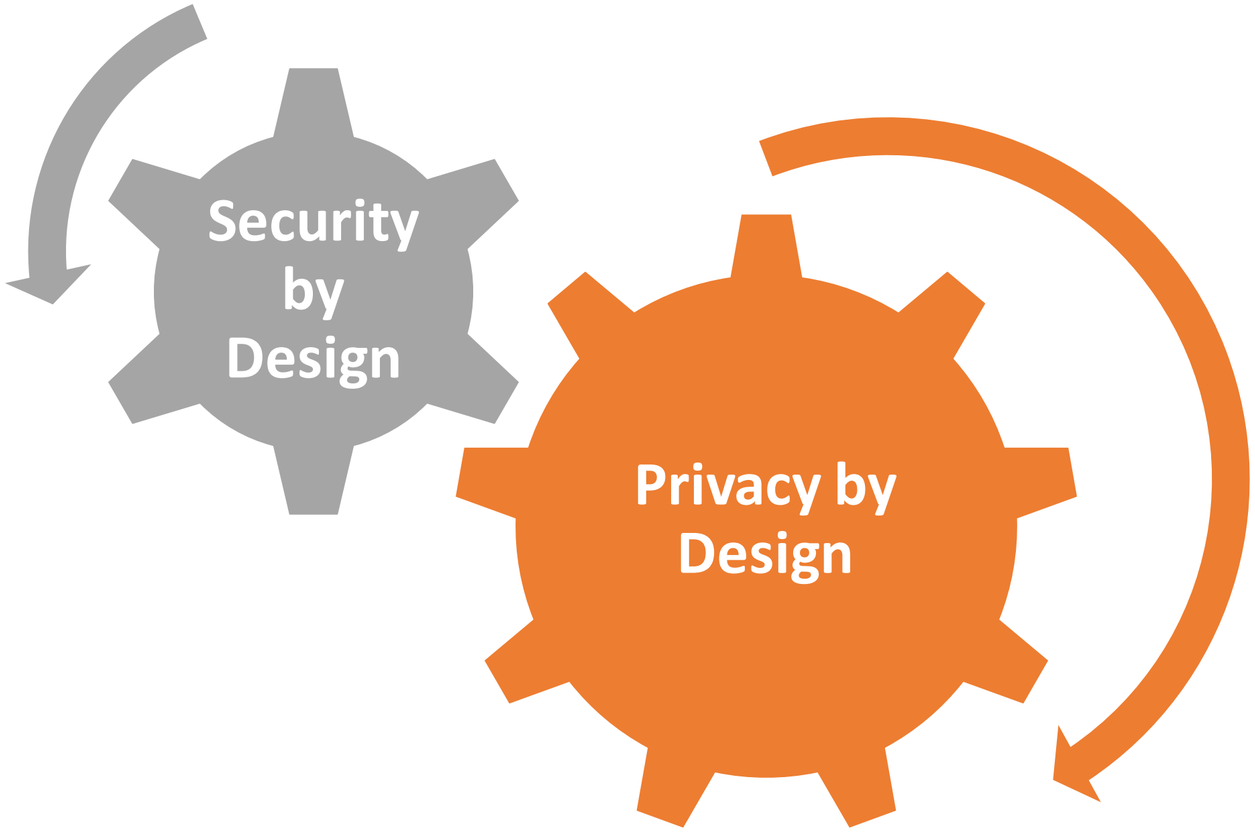
DIRETRIZES GERAIS

Objetivos da função identificar na estrutura de segurança cibernética para API

REQUISITOS GERAIS

Word Wide Web Consortium

OWASP
Open Web Application Security Project



gov.br

REQUISITO GERAL 1: Privacy by Design

Word Wide Web Consortium

Nota do Grupo de Trabalho

Princípios de Privacidade

1. **Aviso** aos usuários sobre os dados coletados por meio de APIs de dispositivo;

Princípio da Transparência, Art. 6º Inciso VI da Lei Geral de Proteção de Dados – LGPD.

2. **Consentimento** do usuário para compartilhar dados por meio de APIs de dispositivo;

Princípio de Livre Acesso, art. 6º Inciso I da Lei Geral de Proteção de Dados - LGPD.

3. **Minimização** da quantidade e o nível de detalhe dos dados coletados por meio de APIs de dispositivo;

Princípio da Necessidade, art. 6º, Inciso III da Lei Geral de Proteção de Dados - LGPD.

4. **Controle** de acesso do usuário aos seus dados, uma vez que tenham consentido em que sejam coletados por meio de APIs de dispositivo;

Princípio da Adequação, art. 6º, Inciso II da Lei Geral de Proteção de Dados - LGPD.

5. **Acesso** aos usuários a informações sobre os dados que foram coletados sobre eles por meio de APIs de dispositivo;

Princípio de Livre Acesso, art. 6º Inciso IV da Lei Geral de Proteção de Dados - LGPD.

6. **Retenção** por tempo limitado dos dados coletados em aplicativos por meio de APIs do dispositivo;

Princípio da Segurança, art. 6º, Inciso VII da Lei Geral de Proteção de Dados - LGPD.

7. **Uso Secundário** de dados coletados em aplicativos por meio de APIs de dispositivo para fins diferentes do propósito para o qual foram coletados devem ser limitados.

Princípio da Prevenção, art. 6º, Inciso VIII da Lei Geral de Proteção de Dados - LGPD.

8. **Compartilhamento** por aplicativos limitados para dados coletados por meio de APIs de dispositivo com terceiros.

Princípio da Prevenção, art. 6º, Inciso VIII da Lei Geral de Proteção de Dados - LGPD.

REQUISITO GERAL 2: Security by Design

OWASP
Open Web Application Security Project

Princípios de Segurança

gov.br

REQUISITO ESPECÍFICO 1: Privacidade

Word Wide Web Consortium

Nota do Grupo de Trabalho

Melhores Práticas de Privacidade

Privacy by Design	Design Centrado no Usuário	Minimize a coleta e transmissão de dados pessoais	Manter a confidencialidade dos dados pessoais
• **MELHOR PRÁTICA 1**:	• **MELHOR PRÁTICA 2** • **MELHOR PRÁTICA 3** • **MELHOR PRÁTICA 4** • **MELHOR PRÁTICA 5** • **MELHOR PRÁTICA 6** • **MELHOR PRÁTICA 7** • **MELHOR PRÁTICA 8**	• **MELHOR PRÁTICA 9** • **MELHOR PRÁTICA 10**	• **MELHOR PRÁTICA 11**

• **MELHOR PRÁTICA 9**: Solicite o número mínimo de itens de dados no nível mínimo de detalhe necessário para fornecer um serviço.

Princípio da MINIMIZAÇÃO

• **MELHOR PRÁTICA 10:** Retenha a quantidade mínima de dados no nível mínimo de detalhe pelo mínimo de tempo necessário.

Princípio da RETENÇÃO

gov.br

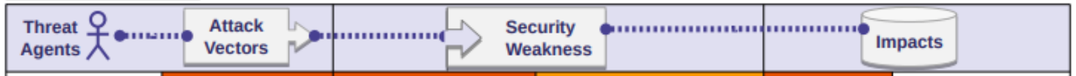
REQUISITO ESPECÍFICO 2: Segurança

OWASP
Open Web Application Security Project

API Security Top 10

10 maiores risco extraídos do guia.

API1:2019 Broken Object Level Authorization



API Specific	Exploitability: 3	Prevalence: 3	Detectability: 2	Technical: 3	Business Specific
Attackers can exploit API endpoints that are vulnerable to broken object level authorization by manipulating the ID of an object that is sent within the request. This may lead to unauthorized access to sensitive data. This issue is extremely common in API-based applications because the server component usually does not fully track the client's state, and instead, relies more on parameters like object IDs, that are sent from the client to decide which objects to access.		This has been the most common and impactful attack on APIs. Authorization and access control mechanisms in modern applications are complex and wide-spread. Even if the application implements a proper infrastructure for authorization checks, developers might forget to use these checks before accessing a sensitive object. Access control detection is not typically amenable to automated static or dynamic testing.		Unauthorized access can result in data disclosure to unauthorized parties, data loss, or data manipulation. Unauthorized access to objects can also lead to full account takeover.	

Is The API Vulnerable?

Object level authorization is an access control mechanism that is usually implemented at the code level to validate that one user can only access objects that they should have access to.

Every API endpoint that receives an ID of an object, and performs any type of action on the object, should implement object level authorization checks. The checks should validate that the logged-in user does have access to perform the requested action on the requested object.

Failures in this mechanism typically leads to unauthorized information disclosure, modification, or destruction of all data.

Example Attack Scenarios

Scenario #1

An e-commerce platform for online stores (shops) provides a listing page with the revenue charts for their

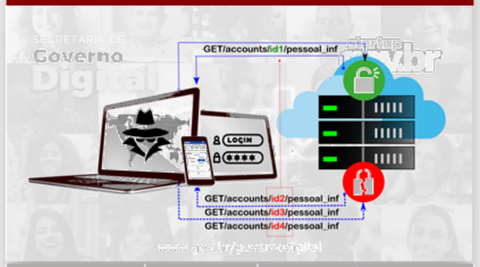
gov.br

REQUISITO ESPECÍFICO 2: Segurança

OWASP
Open Web Application Security Project

API Security Top 10
10 maiores risco extraídos do guia.

API1. Quebra de Autorização a Nível de Objeto



Explorabilidade	Prevalência	Detecção	Impacto
Fácil: 3	Difundida: 3	Média: 2	Severo: 3

Conceito

A validação de autorização insuficiente de uma solicitação de acesso a objeto permite que um atacante realize uma ação não autorizada reutilizando um token de acesso. Esta ameaça é causada por uma configuração incorreta de validações de autorização.

Como acontece?

- ✓ Descobrindo API, ID de recurso ou objeto e utilizando-o para fins maliciosos.
- ✓ Os dados não têm validação do usuário e são acessíveis a qualquer pessoa.
- ✓ Mensagens de erros retornam muitas informações, apresentando para os atacantes como abusar da API.
- ✓ Atacantes utilizam técnicas de enumeração para coletar dados.

Como prevenir?

- ✓ Implementar verificações de autorização com políticas e hierarquia do usuário.
- ✓ O desenvolvimento de aplicativos deve colaborar com a segurança para implementar uma autorização forte para garantir que a API valide os privilégios do usuário para todas as funções.
- ✓ A API deve ser projetada para usar IDs aleatórios.
- ✓ Verificar a autorização cada vez que houver uma requisição do cliente para acessar o banco de dados.
- ✓ Construir casos de teste específicos de segurança a nível de função para recursos relacionados à autorização.

Título do Risco

Definição do risco

Como acontece a falha

Como prevenir o risco

Categorias e Medidas do Risco

Explorabilidade	Prevalência da Fraqueza	Detecção da Fraqueza	Impacto Técnico
Fácil: 3	Difundida: 3	Fácil: 3	Severo: 3
Médio: 2	Comum: 2	Média: 2	Moderado: 2
Difícil: 1	Difícil: 1	Difícil: 1	Menor: 1

Atende ao:

**** Princípio do menor privilégio***

**** Princípio da Segregação de funções***

gov.br

Contato

cgsin@economia.gov.br

SECRETARIA DE GOVERNO DIGITAL
SECRETARIA ESPECIAL DE DESBUROCRATIZAÇÃO, GESTÃO E GOVERNO DIGITAL
MINISTÉRIO DA ECONOMIA
PÁTRIA AMADA BRASIL GOVERNO FEDERAL