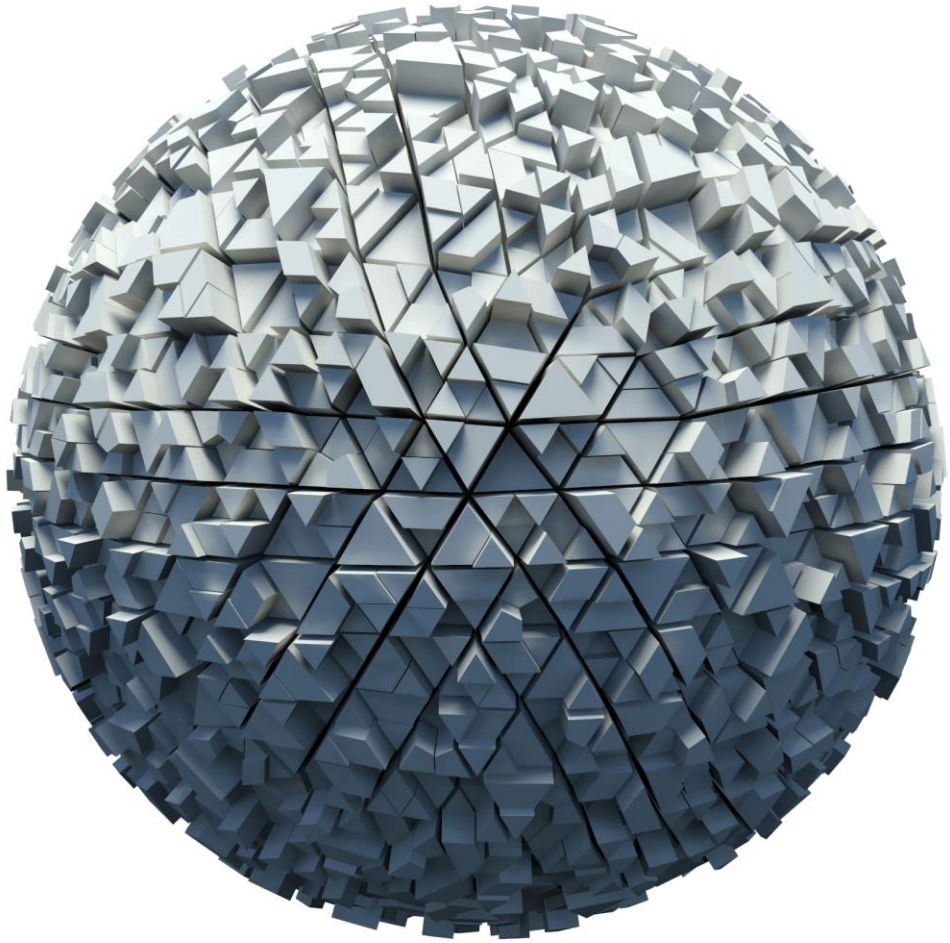
Deloitte.

FEBRABAN
/CYBER LAB



Padronização

Guia de Boas Práticas de Segurança da Informação

ÍNDICE

ÍNDICE

Introdução

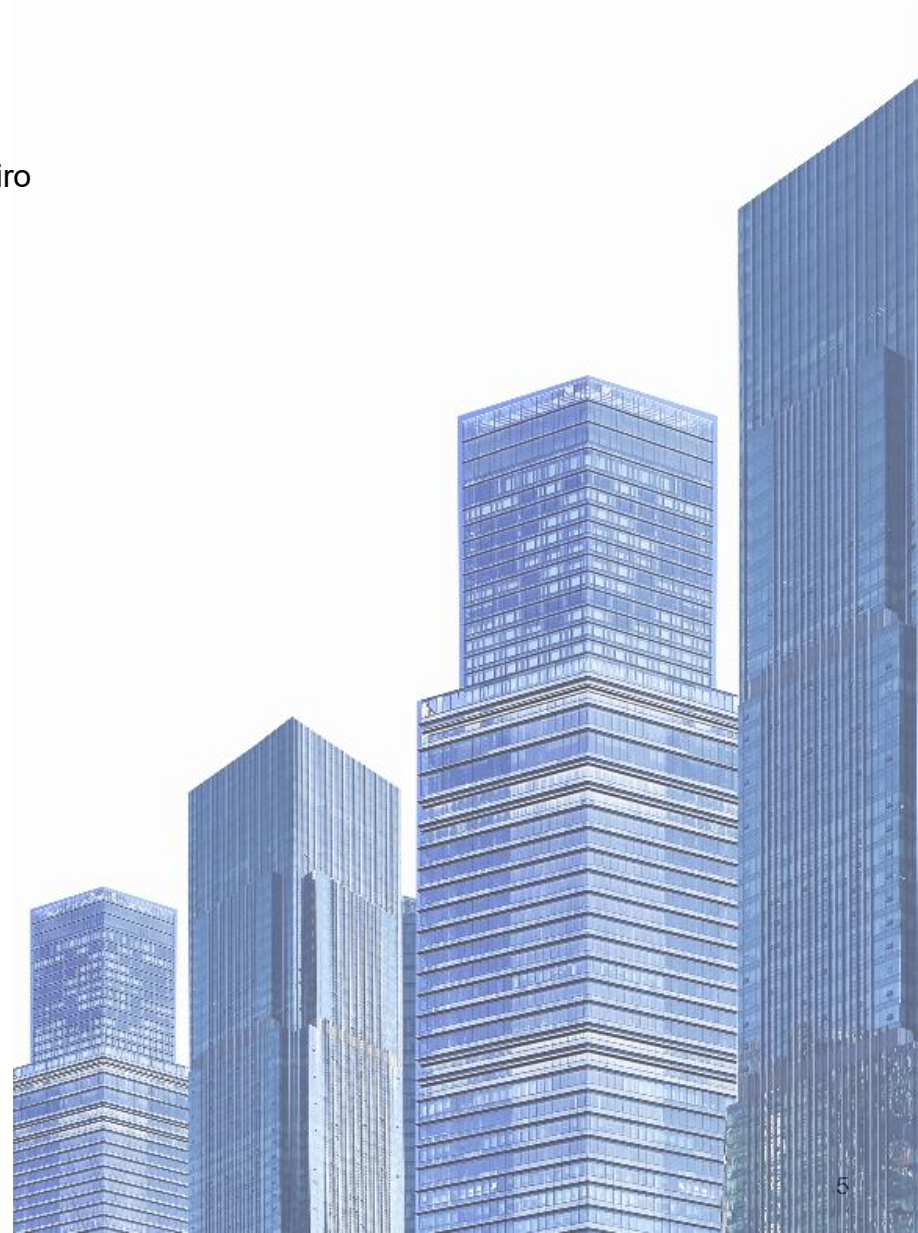
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

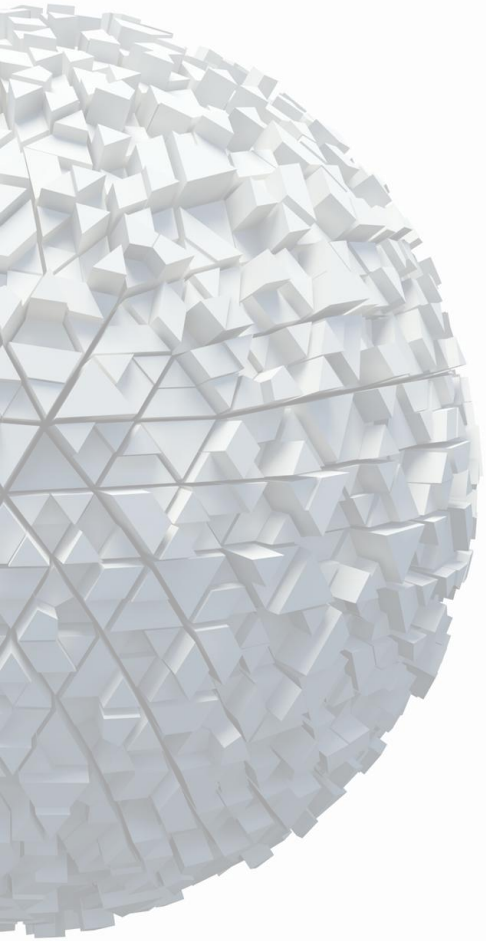
Ações preventivas conjuntas

- Guia de boas práticas de segurança da informação para prestadores de serviço do sistema financeiro
- Sessões/workshops de conscientização
- Métodos e boas práticas de gestão de risco em terceiros
- Assessment Compartilhado

Motivadores para o desenvolvimento do Guia

- Importância da segurança cibernética para os terceiros
- Ampla gama de frameworks disponíveis
- Grande quantidade de assessments de diferentes contratantes
- Conscientizar sobre os temas abordados nos assessments





- **19 Módulos**

✓ Desenvolvimento Seguro
✓ Teste de Invasão
✓ Gestão de Vulnerabilidades
✓ Gestão de Incidentes
✓ Privacidade
✓ Proteção de Dados
✓ Gestão de Identidades
✓ Continuidade de Negócios
✓ Segurança Física
✓ Conscientização e Treinamentos
✓ Cloud Security
✓ Monitoramento
✓ Gestão de Provedor de Serviço
✓ Gestão de Registros e Auditoria
✓ Fábricas de cartão
✓ Inteligência Artificial

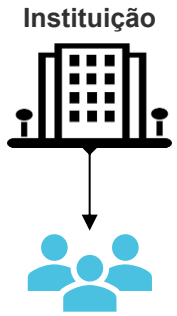
Novos módulos (2025)

✓ Proteção de APIs
✓ Zero Trust
✓ Gerenciamento de acesso privilegiado (PAM)

- Espírito de colaboração e melhores esforços.
- Iniciativa que faça sentido para os bancos e que seja incorporado nos processos já existentes.
- Não é mandatório ou regulatório.

Contexto - TPRM *(Third Party Risk Management)*

Os terceiros são uma parte importante do sucesso de um negócio. Organizações de todos os portes estão recorrendo cada vez mais a terceiros por sua inovação, seu crescimento e sua transformação digital. **Contudo, trabalhar com terceiros pode introduzir riscos ao negócio**, principalmente se eles tiverem acesso a dados confidenciais/sensíveis, poderão ser um risco à segurança. A **gestão de riscos de terceiros permite as organizações identificar e gerenciar riscos na cadeia de suprimentos**. **Dessa forma, é possível que as organizações tomem decisões informadas sobre os riscos e reduzam os riscos apresentados pelos fornecedores a um nível aceitável.**



Principais desafios e preocupações:

Fornecedores realizam e suportam processos e atividades importantes às Instituições.	Fornecedores que, nem sempre, possuem o mesmo nível de segurança e controles internos.	Fornecedores são alvos de fraudadores para o roubo de informações e tentativas de intrusão (incidentes cibernéticos).	Risco relacionado a quarteirização de serviços	Alto volume de terceiros operando pelas Instituições. Além disso, ao longo do tempo, manter uma gestão adequada se torna um grande desafio, assim como monitorar os terceiros ao longo do relacionamento.

Benefícios:

- Visibilidade dos relacionamentos com terceiros
- Aprimorar a gestão de riscos de segurança
- Redução de potenciais interrupção dos negócios
- Aprimorar a postura de segurança
- Mitigar riscos de segurança

Deloitte.

FEBRABAN
/CYBER LAB

Padronização
Guia de Boas Práticas

Módulo: Desenvolvimento Seguro de Software

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Requisitos – Desenvolvimento Seguro de Software

FEBRABAN

Este material foi elaborado de acordo com as diretrizes do Guia de Desenvolvimento do OWASP, bem como foram considerados os requisitos de segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

PCI DSS

- 6.1 Os processos e mecanismos para desenvolver e manter sistemas e softwares seguros são definidos e compreendidos.
- 6.2 O software sob medida e personalizado são desenvolvidos com segurança.
- 6.3 Vulnerabilidades de segurança são identificadas e tratadas.
- 6.4 Os aplicativos web voltados para o público são protegidos contra ataques.
- 6.5 Mudanças em todos os componentes de sistema são administradas com segurança.

ISO 27002

- 8.25 Ciclo de vida de desenvolvimento seguro
- 8.26 Requisitos de segurança do aplicativo
- 8.27 Arquitetura de sistema segura e princípios de engenharia
- 8.28 Codificação segura
- 8.29 Testes de segurança em desenvolvimento e aceitação
- 8.30 Desenvolvimento terceirizado
- 8.31 Separação dos ambientes de desenvolvimento, teste e produção

CIS Controls

- 16.1 Estabelecer e manter um processo seguro de desenvolvimento de aplicações
- 16.8 Separar sistemas de produção e não produção
- 16.9 Treinar desenvolvedores em conceitos de segurança de aplicações e codificação segura
- 16.10 Aplicar princípios de design seguro em arquiteturas de aplicações
- 16.12 Implementar verificações de segurança em nível de código
- 16.14 Conduzir aplicações de modelagem de ameaças

ISO 27701

- 6.11.1.1 Análise e especificação dos requisitos de segurança da informação
- 6.11.2.1 Política de desenvolvimento seguro
- 6.11.2.5 Princípios para projetar sistemas seguros
- 6.11.2.6 Ambiente seguro para desenvolvimento
- 6.11.2.7 Desenvolvimento terceirizado
- 6.11.2.8 Teste de segurança do sistema

NIST CSF

- PR.PS-06: As práticas seguras de desenvolvimento de software são integradas e seu desempenho é monitorado durante todo o ciclo de vida de desenvolvimento de software

Sumário

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Sumário

Contexto Cibernético

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Casos Reais

Netshoes

Vazamento de dados de 2,5 milhões de usuários

Multa de R$ 500.000,00

Colaborou com os órgãos responsáveis

Facebook

Cambridge Analytica

SENACON

Multa de R$6.600.000,00

Vazamento de dados

Banco Inter

Vazamento de dados chave de criptografia

Multa de R$ 1.500.000,00

Não colaborou com os órgãos responsáveis

Cyrela

Danos morais presumido

Fins de publicitários

Indenização de R$10.000,00

Outros órgãos além da ANPD estão atuando em casos dessa natureza, como PROCON, SENACON, MINISTÉRIOS PÚBLICOS, ASSOCIAÇÕES e PODER JUDICIÁRIO.

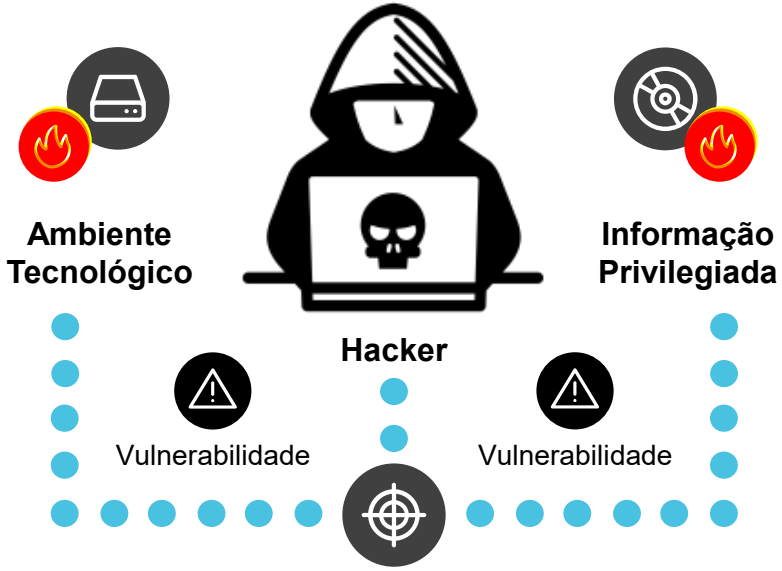
OWASP Top 10 Web Application Security Risks

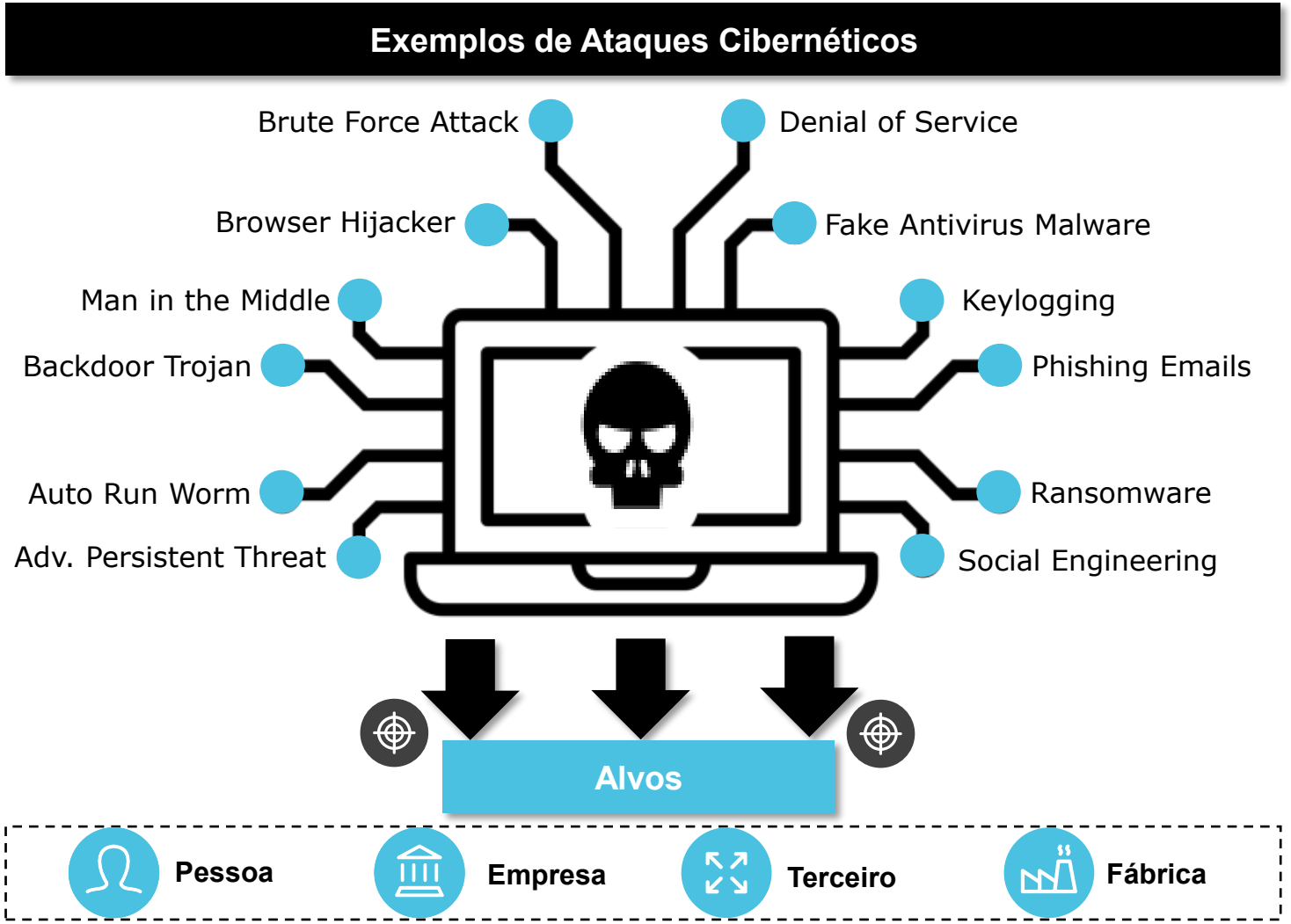
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Visão Geral - OWASP Top 10

Os **ataques cibernéticos** tem como objetivo **controlar**, **interromper** ou **destruir** um **ambiente tecnológico**, estes utilizados pelas organizações para processar e armazenar dados. Estas ameaças também visam a **interceptação** ou **roubo** de **informações privilegiadas**, danificando desta forma a segurança do ambiente tecnológico e impactando os pilares da Segurança da Informação, ou seja, a integridade, disponibilidade e confidencialidade.

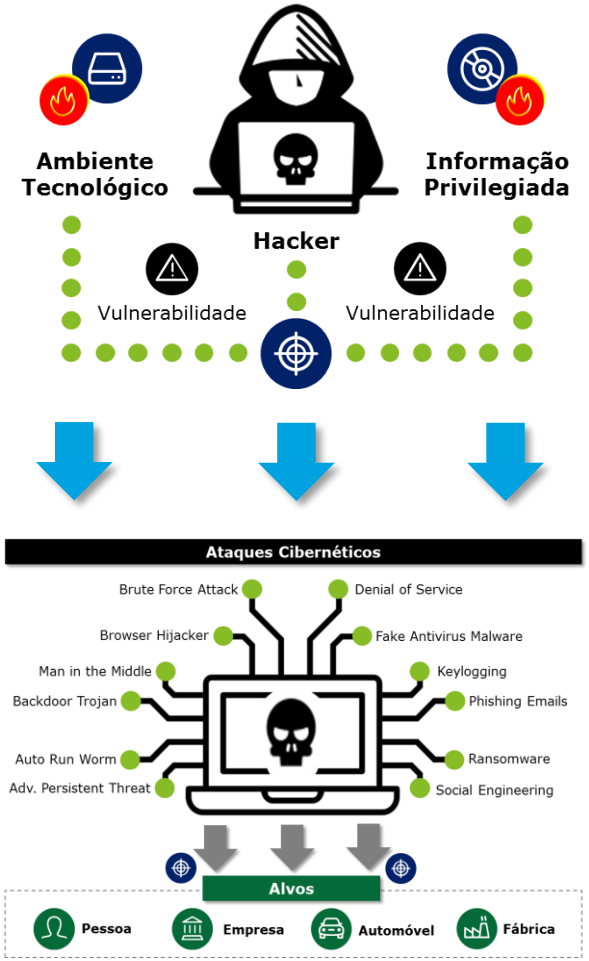
Neste sentido, o **OWASP Top 10 Web Application Security Risks** elenca os **10 principais riscos de segurança de aplicativos da web.**





OWASP Top 10 Web Application Security Risks

FEBRABAN



Riscos Cibernéticos de aplicativos WEB

A01:2021 Broken Access Control

O controle de acesso envolve a utilização de mecanismos de proteção que podem ser categorizados como: Autenticação; Autorização e Prestação de contas. O Controle de Acesso Quebrado ocorre quando o produto restringe incorretamente o acesso a um recurso de um ator não autorizado ou mal-intencionado. Quando um controle de segurança falha ou não é aplicado, os invasores podem comprometer a segurança do produto obtendo escalação de privilégios, acessando informações confidenciais, executando comandos, entre outras ações.

A02:2021 Cryptographic Failures

Falhas criptográficas ocorrem quando o controle de segurança criptográfica é quebrado ou não aplicado, e os dados são expostos a atores não autorizados – maliciosos ou não. É importante proteger os dados em repouso e trânsito, por meio da utilização de protocolos seguros e fortes.

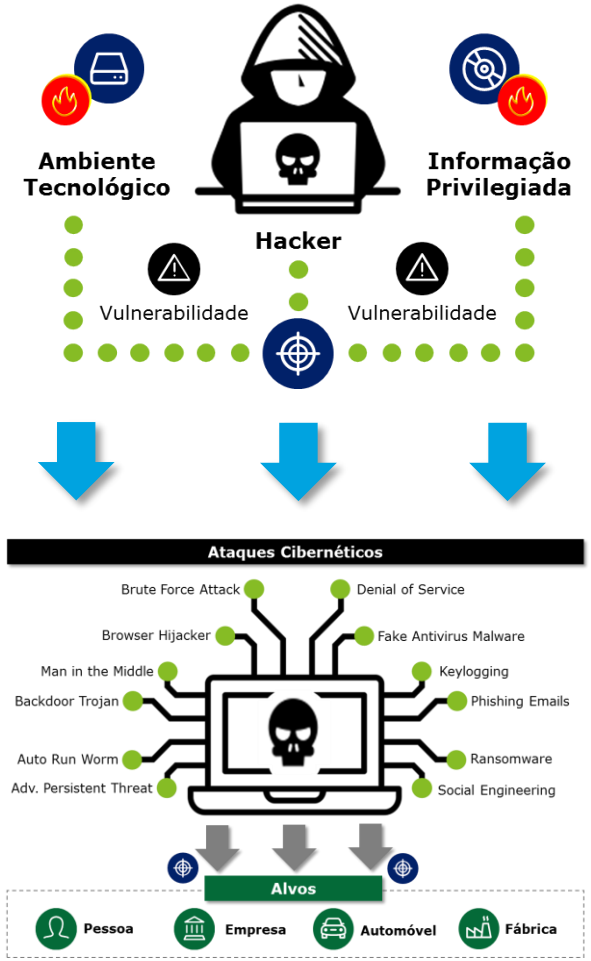
A03:2021 Injection

A falta de validação e sanitização de entradas (inputs) pode levar a explorações de injeção. Estas vulnerabilidades ocorrem quando dados hostis são utilizados diretamente na aplicação e podem resultar na utilização de dados maliciosos para subverter a aplicação

Todas as entradas provenientes de fontes não confiáveis devem ser higienizadas e validadas.

OWASP Top 10 Web Application Security Risks

FEBRABAN



Riscos Cibernéticos de aplicativos WEB

A04:2021 Insecure Design

É importante que a segurança seja incorporada aos aplicativos desde o início e não aplicada posteriormente. A categoria A04 Insecure Design reconhece isso e sugere que o uso de modelagem de ameaças, padrões de design seguros e arquiteturas de referência devem ser incorporados nas atividades de design e arquitetura de aplicativos visando mitigar riscos cibernéticos.

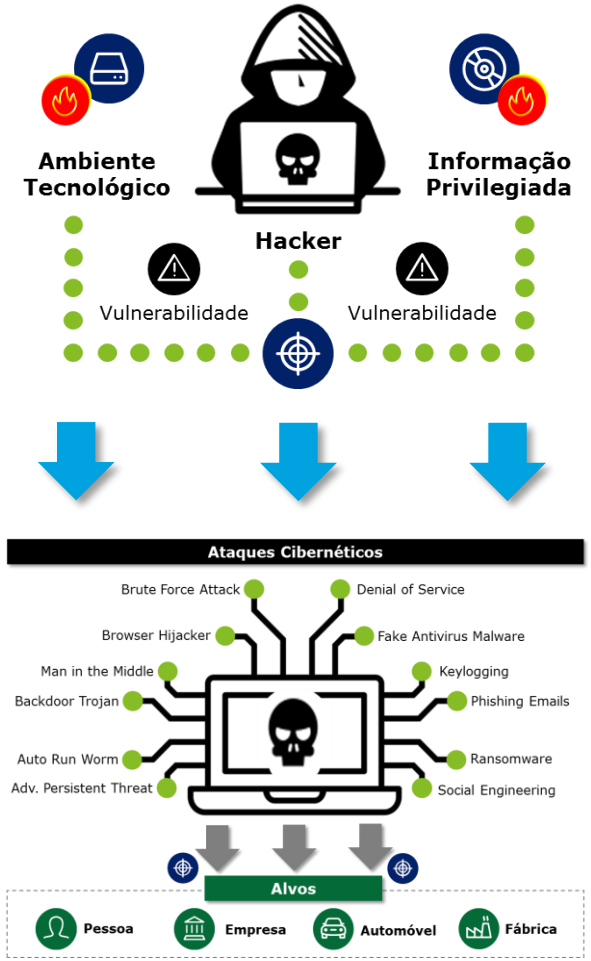
A05:2021 Security Misconfiguration

Sistemas e aplicativos podem ser configuráveis, e essa configuração é frequentemente usada para proteger o sistema/aplicativo. Se as configuração forem mal aplicadas, o aplicativo poderá não ser mais seguro e, em vez disso, ficará vulnerável a explorações conhecidas.

A06:2021 Vulnerable and Outdated Components

Caso uma dependência vulnerável for identificada por um ator malicioso durante a fase de reconhecimento de um ataque, existem bases de dados disponíveis, como a Exploit Database, que fornecerão uma descrição de qualquer exploração. Estas bases de dados podem também fornecer scripts e técnicas prontas a utilizar para atacar uma determinada vulnerabilidade, facilitando a exploração de dependências vulneráveis de software de terceiros.

OWASP Top 10 Web Application Security Risks



Riscos Cibernéticos de aplicativos WEB

A07:2021 Identification and Authentication Failures

A confirmação da identidade do utilizador, a autenticação e a gestão de sessões são fundamentais para proteger o sistema ou a aplicação contra ataques relacionados com a autenticação. Referindo-se ao risco A07 Falhas de identificação e autenticação, a autorização pode falhar de várias formas que frequentemente envolvem outros riscos OWASP Top Ten: controlos de acesso quebrados (A01); falha criptográfica (A02); palavras-passe predefinidas (A05); entre outros.

A08:2021 Software and Data Integrity Failures

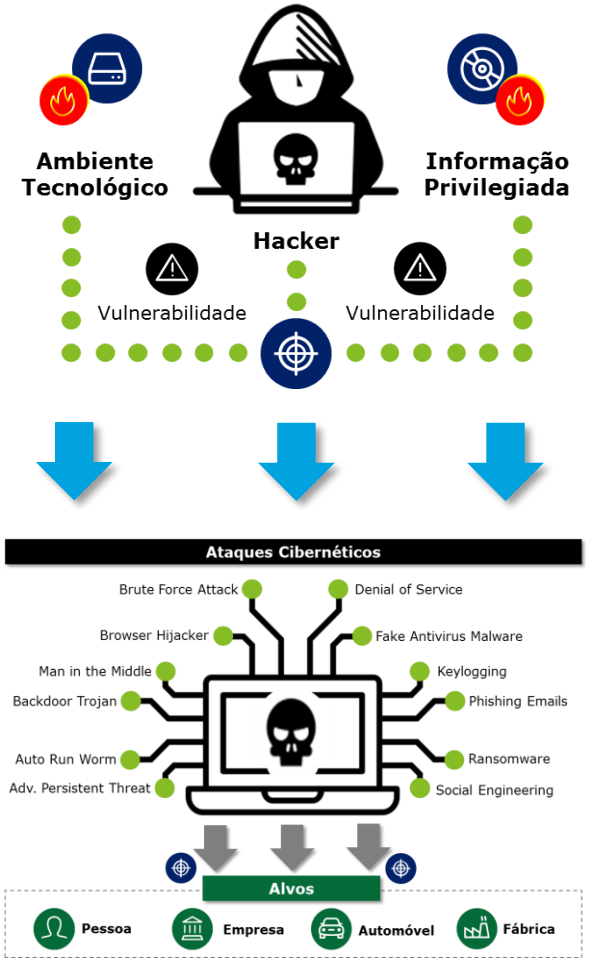
As falhas de integridade do software e dos dados estão relacionadas com o código e as infraestruturas que não protegem contra violações de integridade. Trata-se de uma categoria abrangente que descreve, por exemplo, ataques à cadeia de abastecimento, atualização automática comprometida e utilização de componentes não fiáveis.

A09:2021 Security Logging and Monitoring Failures

O registo e o monitoramento ajudam a detectar, escalar e responder a violações ativas; sem isso, as violações não serão detectadas e não poderão ser adequadamente tratadas. A09 Security Logging and Monitoring Failures lista várias técnicas de registo e monitoramento que devem ser conhecidas, mas também outras que podem não ser tão comuns; por exemplo, o monitoramento da cadeia de fornecimento DevOps pode ser tão importante como o monitoramento da aplicação ou do sistema.

OWASP Top 10 Web Application Security Risks

FEBRABAN



Riscos Cibernéticos de aplicativos WEB

A10:2021 Server-Side Request Forgery

Referindo-se à A10 Server-Side Request Forgery (SSRF), estas vulnerabilidades podem ocorrer sempre que uma aplicação web buscar um recurso remoto sem validar o URL fornecido pelo utilizador. Estas explorações permitem a um atacante coagir a aplicação a enviar um pedido elaborado para um destino inesperado, mesmo quando protegido por uma firewall, VPN ou outro tipo de lista de controlo de acesso à rede.

Desenvolvimento Seguro

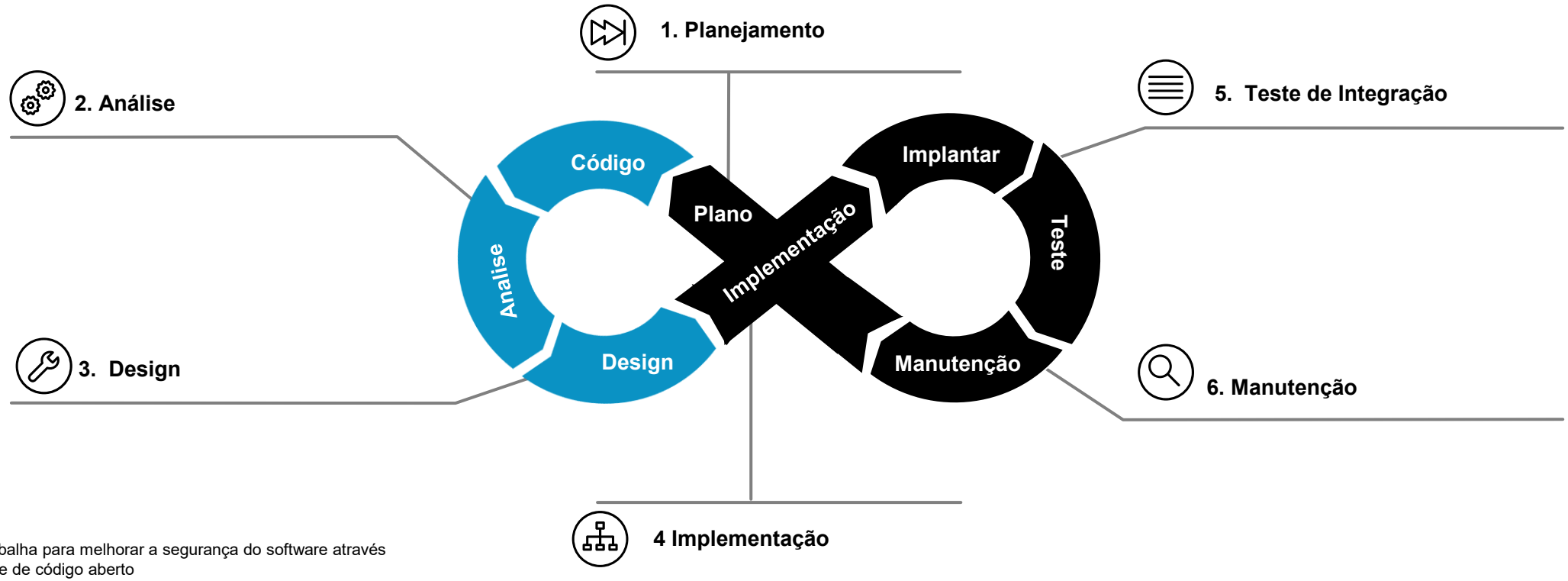
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Visão Geral

De acordo com o OWASP[1], com o **crescente número e sofisticação de explorações contra aplicativos ou sistemas, é recomendável que as organizações adotem o Ciclo de Vida Seguro de Desenvolvimento de Software**, ou do inglês, *Secure Software Development Lifecycle* (*SSDLC*).

Essa estrutura é destinada ao desenvolvimento de software seguro. Em outras palavras é um **conjunto de processos e atividades** que as organizações seguem para garantir que seu **software** seja **desenvolvido** focado na **segurança**.

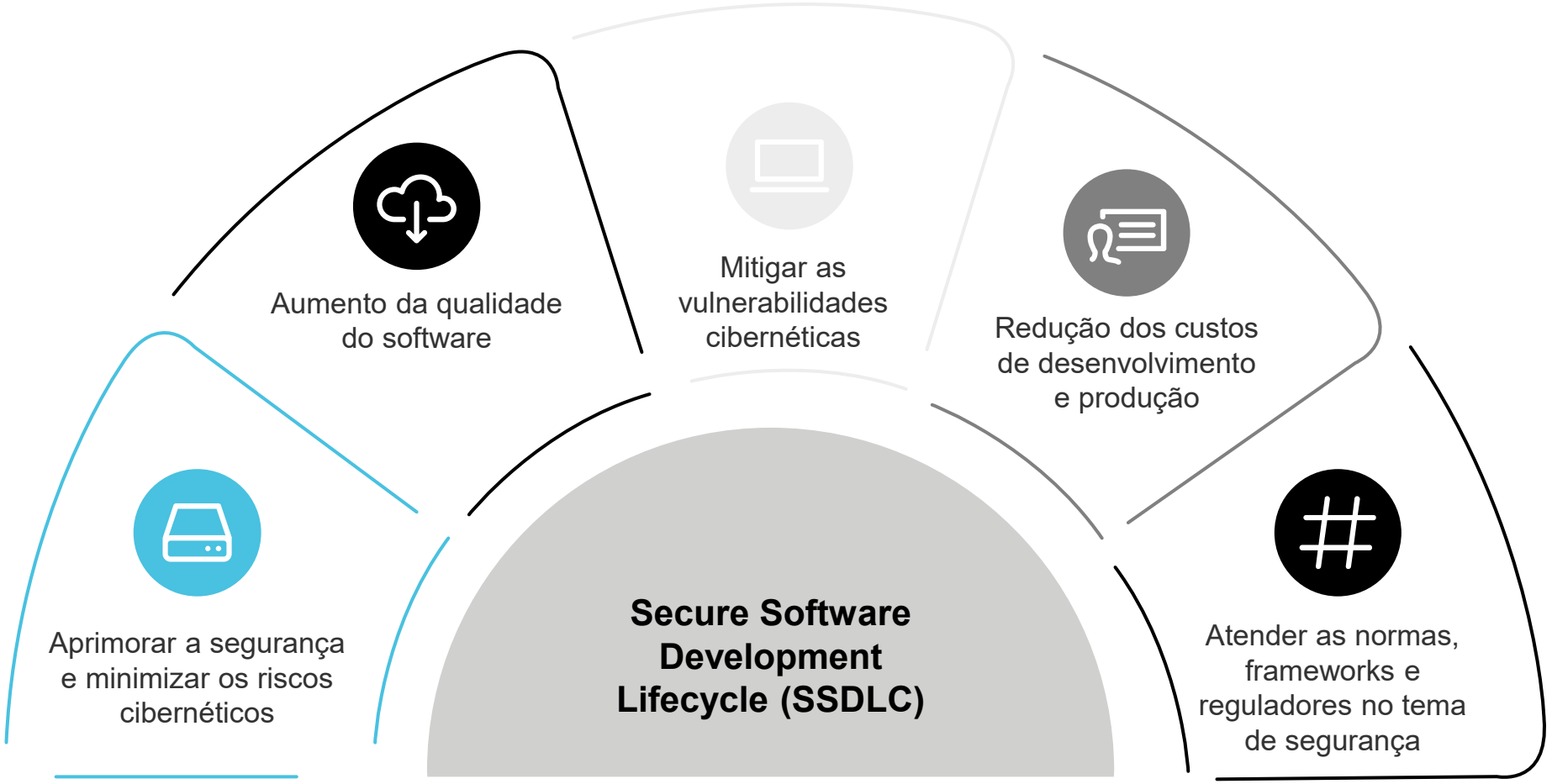
O objetivo do SSDLC é **identificar e mitigar potenciais vulnerabilidades e ameaças de segurança no processo de desenvolvimento de software**, para que o produto final seja o mais seguro possível. O SSDLC é composto pelas seguintes etapas, conforme demonstrado na representação a seguir.



[1] A Fundação OWASP® trabalha para melhorar a segurança do software através de seus projetos de software de código aberto

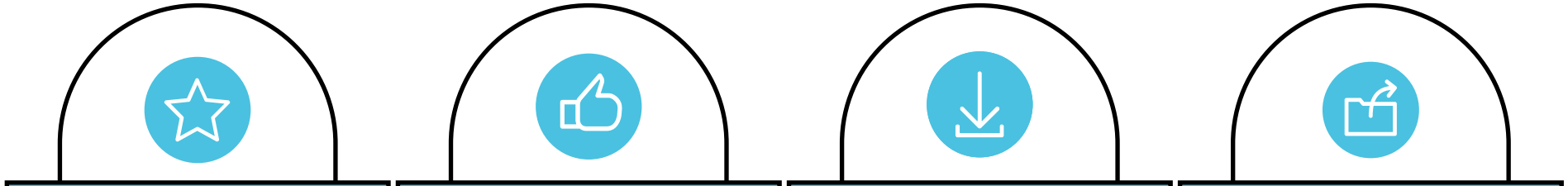
Quais são os benefícios do SSDLC?

A seguir são apresentadas alguns benefícios que a estrutura pode oferecer:



Preparação da Organização

Algumas maneiras de preparar a organização para o desenvolvimento seguro de software incluem:



Política de Desenvolvimento Seguro	Treinamentos e Recursos	Ambientes Segregados e Controlados	Gestão de Mudanças
Ter uma política clara que descreva as expectativas e os requisitos para o desenvolvimento de software seguro pode ajudar a garantir que todos os membros da equipe entendam a importância da segurança e estejam **cientes das etapas específicas que precisam tomar para garantir a segurança do software**.	**Fornecer treinamentos e recursos aos membros da equipe sobre as melhores práticas de desenvolvimento de software seguro** pode ajudar a garantir que eles sejam capazes de desenvolver softwares seguros. Isso pode incluir o **fornecimento** de **treinamento** sobre **práticas de codificação seguras, modelagem de ameaças e outros tópicos relevantes**.	Garantir que o **ambiente** de **desenvolvimento** seja seguro e **segregado** dos demais ambientes pode ajudar a **prevenir violações de segurança** durante o processo de desenvolvimento. Isto pode incluir a **implementação de controles como controles de acesso e gerenciamento de vulnerabilidades.**	Ter um processo seguro de **gerenciamento** de **mudanças** implementado pode ajudar a garantir que todas **as alterações no software sejam revisadas e aprovadas pelas partes apropriadas antes de serem implementadas**. Isso pode ajudar a evitar que **alterações não aprovadas possam introduzir vulnerabilidades no software.**

Planejamento e Análise

FEBRABAN

Os requisitos de segurança são **declarações de funcionalidade** de segurança que garantem que as **diferentes propriedades de segurança de uma aplicação de software sejam atendidas**.

Os requisitos de segurança definem **novos recursos** ou **acréscimos** aos recursos existentes para **resolver um problema de segurança** específico ou **eliminar potenciais vulnerabilidades.**

Os requisitos vêm de várias fontes, sendo três comuns:

01 **Requisitos** relacionados ao **software** que especificam **objetivos** e **expectativas para proteger o serviço e os dados** no centro da aplicação

02 **Práticas** e **defeitos** de codificação **comuns** e **dados históricos** que conduzem a vulnerabilidades de segurança da informação

03 Requisitos **regulamentares** e **estatutários**

Nota: A OWASP fornece projetos que auxiliam na identificação de requisitos de segurança para proteção dos serviços e dados da aplicação. O Padrão de Verificação de Segurança de Aplicativos fornece uma lista de requisitos para desenvolvimento seguro e isso pode ser usado como ponto de partida para os requisitos de segurança. Além disso, o Mobile Application Security fornece um conjunto semelhante de requisitos de segurança padrão para aplicativos móveis.

Exemplos práticas de maturidades relacionadas à Planejamento e Análise:

Baixa Maturidade: O aplicativo/código possui uma API unificada para consulta de dados. Os usuários do sistema serão funcionários do cliente. O aplicativo precisa ser acessível pela internet. A natureza dos dados acessados, os tempos de retenção, o método de transporte e os métodos de comunicação de back-end não são considerados.	**Alta Maturidade:** O desenvolvedor usa um SSDLC maduro, as equipes de engenharia recebem treinamento de segurança e uma lista detalhada de requisitos foi desenhada e verificada pelo cliente.

Design - Modelagem de Ameaças

FEBRABAN

A modelagem de ameaças é uma abordagem estruturada para identificar e priorizar ameaças potenciais a um sistema. Avaliar ameaças durante a fase de design do desenvolvimento pode economizar recursos significativos, se durante uma fase posterior do código for necessária a **restruturação** para incluir **mitigações de riscos**.

Um documento de modelo de ameaça é um registro do processo de modelagem de ameaça e geralmente inclui:

- Uma descrição/design/modelo do que o preocupa
- Uma lista de suposições que podem ser verificadas ou desafiadas no futuro à medida que o cenário de ameaças muda
- Remediação/ações a serem tomadas para cada ameaça
- Formas de validação do modelo e das ameaças, e verificação do sucesso das ações tomadas

Resultados das atividades de modelagem de ameaças

- Documentar como os dados fluem através de um sistema para identificar onde o sistema pode ser atacado
- Identificar o maior número possível de ameaças potenciais ao sistema
- Sugerir controles de segurança que podem ser implementados para reduzir a probabilidade ou o impacto de uma ameaça potencial

Exemplos práticas de maturidades relacionadas à modelagem de ameaças:

Baixa Maturidade: Seguindo requisitos vagos de recursos, o design inclui armazenar dados em cache em um banco de dados local não criptografado, utilizando senha fraca. Além disso, não foi realizado verificação quanto a segurança das bibliotecas para o desenvolvimento do código.

Alta Maturidade: Com base em um modelo de ameaça detalhado definido e atualizado por meio de código, a equipe decide sobre: Os caches criptografados locais precisam expirar e serem limpos automaticamente, canais de comunicação criptografados e autenticados, bibliotecas seguras, entre outros.

Implementação - Introdução

A implementação concentra-se nos processos e atividades relacionados a como a organização constrói e implanta componentes de softwares, bem como a mitigação das falhas/vulnerabilidades relacionados. As atividades de implementação possuem maior impacto na rotina dos desenvolvedores, e um objetivo importante da implementação é **fornecer software que funcione de maneira confiável e com o mínimo de vulnerabilidades possíveis**.

A implementação deve incluir práticas de segurança como: **I. Construção segura; II. Implantação segura; e III. Gerenciamento de vulnerabilidades**.

A implementação é onde a aplicação/sistema começa a tomar forma; o **código-fonte é escrito e os testes são criados**. A implementação do aplicativo segue um **ciclo de vida de desenvolvimento seguro**, com segurança integrada desde o início.

A implementação utilizará um método seguro de controle e armazenamento de código-fonte para atender aos requisitos de segurança do projeto. A equipe de desenvolvimento consultará a **documentação suporte** que contém as melhores práticas, utilização **bibliotecas seguras** sempre que possível, além de **verificar** e **rastrear dependências externas**.

Grande parte das competências de implementação advém da experiência, e ter em conta o que fazer e o que não fazer no desenvolvimento seguro é, por si só, uma atividade de conhecimento importante.

Exemplos práticas de maturidades relacionadas à Implementação:

Baixa Maturidade: A equipe usa bibliotecas GraphQL prontas para uso, mas as versões não são verificadas usando a Auditoria NPM.

Alta Maturidade: Os membros da equipe têm acesso a documentação abrangente e a uma biblioteca de trechos de código que podem usar para acelerar o desenvolvimento. Os testes executam um conjunto abrangente de testes, incluindo testes de segurança, testes de aceitação de serviço, bem como testes de regressão.

Implementação - Práticas de Codificação Segura

FEBRABAN

Introdução

O OWASP Go Secure Coding Practices (Go-SCP) é um **conjunto de práticas de codificação segura** de software para a linguagem de programação Go. O documento publicado pode ser baixado em vários formatos no repositório do GitHub.

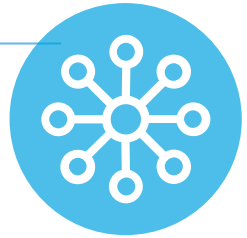
Porque utilizar?

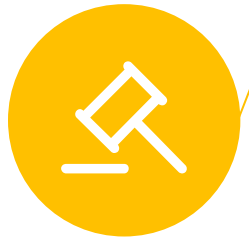
- As equipes de desenvolvimento geralmente precisam de ajuda e suporte para obter a segurança certa para aplicativos da Web, e parte dessa ajuda vem de **diretrizes e práticas recomendadas de codificação segura**. Go-SCP fornece esta orientação para uma ampla variedade de tópicos de codificação segura, além de fornecer exemplos práticos de código para cada prática de codificação.

Exemplos de Práticas de Codificação Segura

O Go-SCP fornece **exemplos e recomendações** para ajudar os programadores a evitar erros e armadilhas comuns, incluindo exemplos de código em Go que **fornecem orientações práticas sobre a implementação das recomendações**, por exemplo:

- Redução da superfície de ataque;
- Princípio do menor privilégio e minimização de dados;
- Codificação de saída de higienização de dados;
- Autenticação e gerenciamento de senhas;
- Gerenciamento de sessão;
- Controle de acesso;
- Práticas criptográficas;
- Tratamento e registro de erros;
- Realizar uma análise dos erros de programação mais comuns e documentar se estes foram mitigados;
- Entre outros.





Como utilizar?

- O público principal do Guia de práticas de codificação Go Secure são os desenvolvedores, especialmente aqueles com experiência anterior em outras linguagens de programação.
- Baixe o documento Go-SCP em um dos formatos: PDF, ePub, DocX e MOBI. Consulte o capítulo do tópico específico e use os exemplos de trechos de código Go para obter orientação prática sobre codificação segura.

Testes de Segurança

Novos sistemas, atualizações e novas versões devem ser **exaustivamente testados e verificados durante os processos de desenvolvimento**. Os testes podem ser realizados de várias maneiras e dependem muito da **natureza do software**, da **cadência** da organização e dos **requisitos regulamentares**, entre outros elementos relevantes. Podem ser realizados testes de **SAST** (Teste de Aplicação Estático), **DAST** (Teste de Aplicação Dinâmico) e **IAST** (Teste de Aplicação Interativo).

Observação: Na representação ao lado é possível entender as particularidades de cada tipo de teste, bem como alguns exemplos de ferramentas de mercado que podem ser considerados para a orquestração dos testes.

SAST

Permite que os desenvolvedores **encontrem vulnerabilidades de segurança no código-fonte** do aplicativo no início do ciclo de vida de desenvolvimento de software e **garante a conformidade com as diretrizes e padrões de codificação segura**.

sonarqube

Checkmarx

VERACODE

DAST

Pode **encontrar vulnerabilidades** e fraquezas de **segurança** em um **aplicativo em execução utilizando técnicas de injeção de falhas em um aplicativo**, além destacar problemas de tempo de execução que não podem ser identificados pela análise estática.

OWASP Zed Attack Proxy

Burp Suite

Acunetix by Invicti

IAST

Criado para suprir as deficiências do SAST e do DAST combinando elementos de ambas as abordagens. O IAST coloca um agente dentro de um aplicativo e **realiza toda a sua análise no aplicativo em tempo real** e em qualquer lugar no processo de desenvolvimento.

Contrast SECURITY

SYNOPSYS®

Exemplos práticas de maturidades relacionadas à Implementação:

Baixa Maturidade: A empresa implantou o sistema em produção sem testes. Logo depois, os pentests de rotina do cliente descobriram falhas profundas no acesso a dados e serviços de back-end. O esforço de remediação foi significativo.

Alta Maturidade: Os recursos do aplicativo receberam testes automatizados dinâmicos quando cada um atingiu o preparo, uma equipe de controle de qualidade treinada validou os requisitos de negócios que envolviam verificações de segurança. Uma equipe de segurança realizou um pentest adequado e deu um aval.

Manutenção

Neste estágio, o sistema e seus recursos já devem estar adequadamente projetados, escritos e testados (conforme observamos nas etapas anteriores do SSDLC). Na etapa de manutenção, a equipe **corrige bugs, soluciona problemas do cliente e gerencia as alterações do software**. Além disso, a equipe **monitora a performance geral do sistema, a segurança e a experiência do usuário para identificar novas formas de melhorar o software** existente. A seguir são apresentadas exemplos de atividades que fazem parte da etapa de manutenção:

Monitoramento de Ameaças

Por meio de uma solução de SIEM (*Security Information and Event Management*) que realiza a **coleta, monitoramento e correlacionamento dos eventos para detectar e alertar ameaças cibernéticas.**

Gestão de Vulnerabilidades

Informações sobre **vulnerabilidades** técnicas dos sistemas de informação em uso, **devem ser obtidas em tempo hábil**, com a exposição da organização a estas vulnerabilidades avaliadas e **tomadas as medidas apropriadas para lidar com os riscos associados.**

Patches de Segurança

Atualizações do sistema por meio da gestão automatizada de **patches**, bem como aplicação de **configurações seguras**, por exemplo, baselines CIS.

Gestão de Incidentes

Assegurar um enfoque consistente e efetivo para **gerenciar** os **incidentes de segurança** da informação, incluindo atividades para **identificar**, **avaliar**, **priorizar**, **responder**, **comunicar incidentes cibernéticos**.

Exemplos práticas de maturidades relacionadas à Implementação:

Baixa Maturidade: Não há segregação de ambientes, ou seja, no mesmo ambiente é realizado o desenvolvimento, testes de segurança e publicação do código. Além disso, não são aplicadas configurações de segurança de acordo com baselines de segurança, por exemplo, CIS. Não é realizado a coleta e monitoramento dos registros de atividades (logs), desta forma, incidentes não são detectados e tratados em tempo hábil.	**Alta Maturidade:** O sistema ao migrar do ambientes de controle de qualidade para a produção, aplica a configuração segura a todos os componentes, por exemplo, baselines de segurança. O registro em log de todos os componentes é agregado em SIEM e os alertas que são gerados são correlacionados com demais logs do ambiente. São realizados exercícios e simulações de incidentes para aperfeiçoamento dos processos internos.

Link – Material de Apoio

Considerações Finais

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Frameworks e Normas de Referência

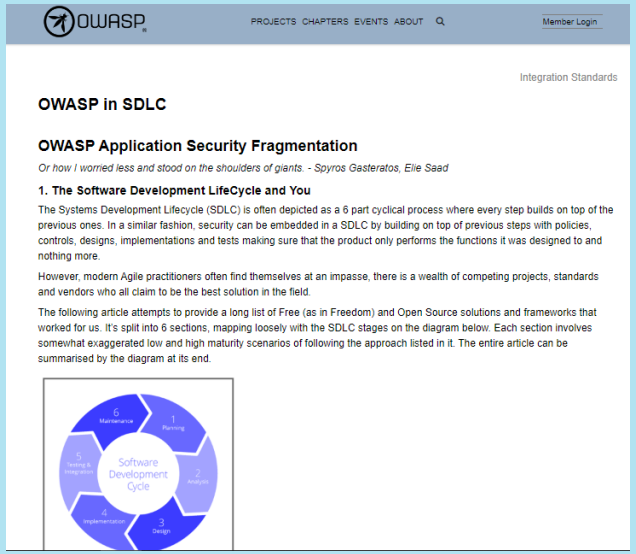
FEBRABAN

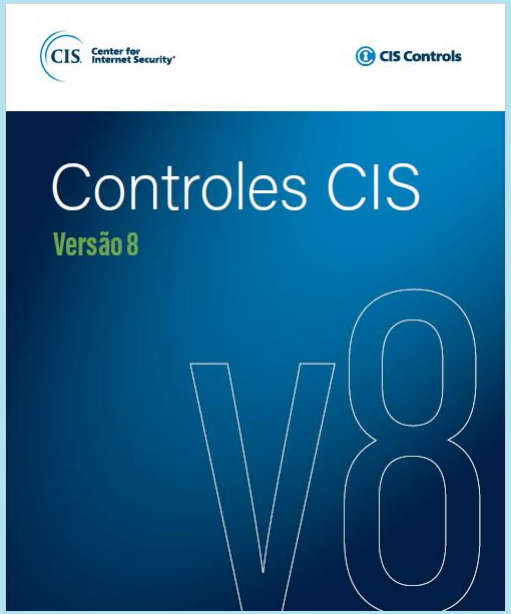
Para apoiar no entendimento e implementação de toda a metodologia apresentada neste material, a seguir são apresentados as normas e frameworks de referência no tema:

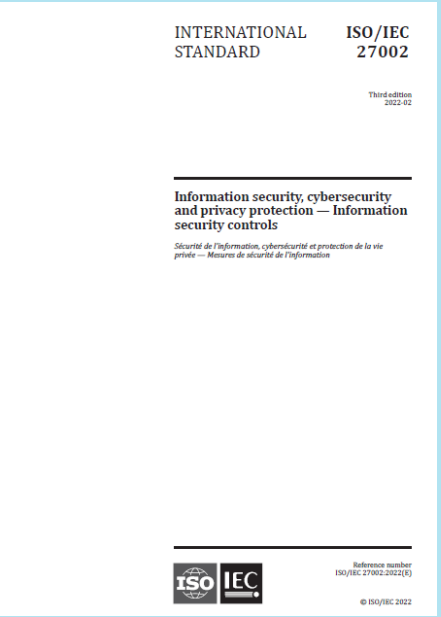
ISO 27001/27002

NIST CSF

CIS Controls







OWASP SSDLC

PCI DSS

ISO 27701

Relembrando os principais conceitos

Agora que aprendemos sobre as atividades relacionadas ao processo de desenvolvimento seguro de software, relembre os principais termos e conceitos apresentados neste material:

- **OWASP Top 10 Web Application Security Risks:** elenca os 10 principais riscos de segurança de aplicativos da web.
- **SSDLC**: ciclo de Vida Seguro de Desenvolvimento de Software, ou do inglês, Secure Software Development Lifecycle (SSDLC).
- **Etapas do SSDLC**: 1 Planejamento; 2 Análise; 3 Design; 4 Implementação; 5 Testes; e 6 Manutenção
- **A modelagem de ameaças:** é uma abordagem estruturada para identificar e priorizar ameaças potenciais a um sistema. Avaliar ameaças durante a fase de design do desenvolvimento pode economizar recursos significativos, se durante uma fase posterior do código for necessária a restruturação para incluir mitigações de riscos.
- **Testes de segurança**: podem ser realizados testes de SAST (Teste de Aplicação Estático), DAST (Teste de Aplicação Dinâmico) e IAST (Teste de Aplicação Interativo).

Módulo: Teste de Invasão

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Requisitos – Teste de Invasão

FEBRABAN

Este material foi elaborado de acordo com as diretrizes do PCI DSS e CIS Controls, bem como foram considerados os requisitos de segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

PCI DSS

- 11.1 Processos e mecanismos para testar regularmente a segurança de sistemas e redes são definidos e compreendidos.
- 11.3 Vulnerabilidades externas e internas são regularmente identificadas, priorizadas e tratadas.
- 11.4 Testes de penetração externos e internos são realizados regularmente e vulnerabilidades exploráveis e fragilidades de segurança são corrigidas.

CIS Controls

- 18.1 Estabelecer e manter um programa de teste de invasão
- 18.2 Realizar testes de invasão externos periódicos
- 18.3 Corrigir as descobertas do teste de invasão
- 18.4 Validar as Medidas de Segurança
- 18.5 Realizar testes de invasão internos periódicos

ISO 27002

- 8.29 Security testing

ISO 27701

- 6.11.2.8 Teste de segurança do sistema

NIST CSF

- ID.IM-02: As melhorias são identificadas a partir de testes e exercícios de segurança, incluindo aqueles feitos em coordenação com fornecedores e terceiros relevantes

Sumário

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Sumário

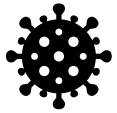
Introdução

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Introdução

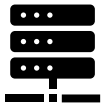
De acordo com o CIS Controls, uma postura defensiva bem-sucedida requer um programa abrangente de políticas e governança eficazes, fortes defesas técnicas, combinadas com a ação apropriada das pessoas. No entanto, raramente é perfeito. Em um ambiente complexo onde a tecnologia está em constante evolução e novas técnicas dos atacantes aparecem regularmente, as **empresas devem testar periodicamente seus controles para identificar fragilidades de segurança e avaliar sua resiliência**. **Este teste pode ser da perspectiva de rede externa, rede interna, aplicação, sistema ou dispositivo**. Pode incluir engenharia social de usuários ou desvios de controle de acesso físico.

Qual a finalidade dos testes de invasão?



Os testes de invasão podem fornecer percepções valiosas e objetivas sobre a **existência de vulnerabilidades em ativos corporativos tecnológicos**.

Testar, pelo menos uma vez ao ano, o **funcionamento correto das estratégias de defesas** da empresa.



Testar se a empresa **construiu as defesas certas** em primeiro lugar.

Demonstrar, de forma realista, a dinâmica de um ataque. Geralmente para **convencer** os **tomadores de decisão** das fraquezas da empresa.

Podem **revelar** as **fraquezas** do processo, como **gestão de configuração** ou **treinamento** do usuário final **incompletos** ou **inconsistentes**.

Testes e suas Diferenças

De acordo com o PCI, as vulnerabilidades são descobertas continuamente por indivíduos mal-intencionados, e sendo introduzidas por novos softwares. **Os componentes de sistemas, processos e softwares devem ser testados com frequência para garantir que os controles de segurança continuem a proteger ambientes em constantes mudanças**. Os testes podem ser realizados por um recurso **interno qualificado ou um terceiro externo qualificado**. A seguir são apresentados alguns tipos de teste e suas principais diferenças:

***Foco deste treinamento**

Teste de Invasão

- **Descrição**: Simular ataques reais para avaliar eficácia das medidas de segurança, por meio da exploração de vulnerabilidades presentes no ambiente da empresa.
- **Objetivo**: Avaliar o verdadeiro impacto das vulnerabilidades no ambiente de uma empresa.

Red Team Exercise

- **Descrição**: Esse tipo de teste é semelhante aos testes de invasão em que as vulnerabilidades são exploradas; no entanto, a diferença é o foco.
- **Objetivo**: Auxiliar a equipe de segurança a aprimorar as capacidades de detecção e resposta, e aumentar a resiliência de seus sistemas contra atacantes maliciosos.

Análise de Vulnerabilidades

- **Descrição**: Teste de vulnerabilidade realizado por meio de varreduras automatizadas, incluindo validação manual dos falsos positivos. Esse tipo de teste visa detectar e classificar possíveis pontos de fragilidade na segurança.
- **Objetivo**: Identificar as vulnerabilidades presentes no ambiente de uma empresa.

Link – Material de Apoio

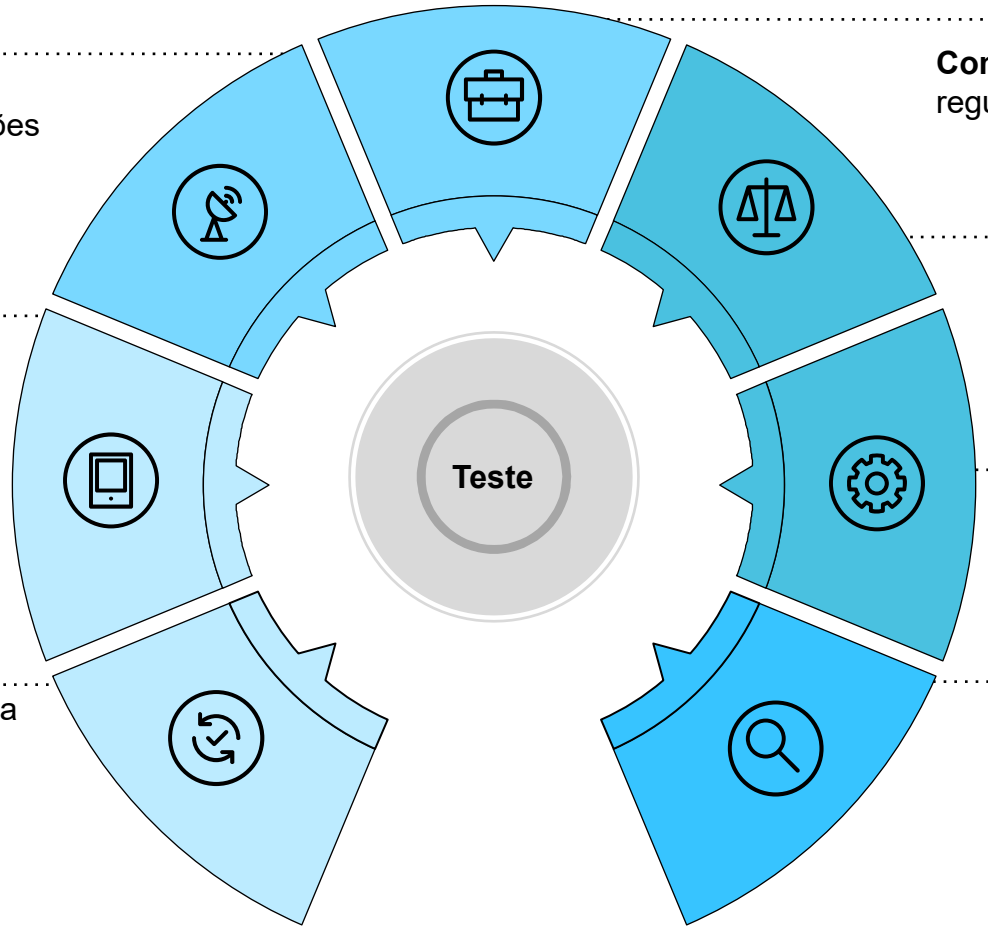
Principais Benefícios dos Testes de Invasão

FEBRABAN

Aumento da maturidade em segurança cibernética dos sistemas, redes e aplicações das organizações.

Identificar vulnerabilidades que podem ser exploradas por ameaças, bem como **identificar vulnerabilidades que não seriam detectadas por varreduras automatizadas**.

Fornecer evidências que podem auxiliar na **obtenção de investimentos em segurança** com executivos C-level, investidores e clientes.



Conformidade com normas e regulamentações.

Testar a **eficiência** do time de segurança em **detectar** e **bloquear ataques cibernéticos**.

Identificar outras **oportunidades** de **projetos estruturantes** em **segurança** da informação.

Analisar a magnitude real do **impacto ao negócio e operacional** em caso de **ataques cibernéticos**.

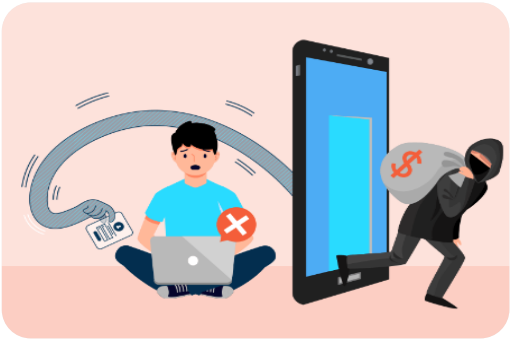
Componentes de um Ataque Cibernético

FEBRABAN

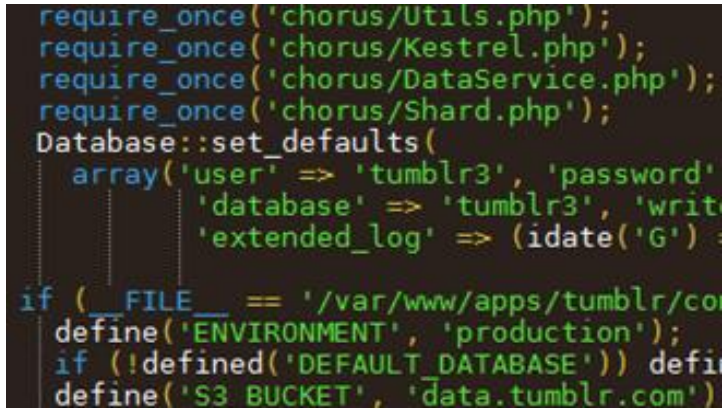
Um ataque cibernético é qualquer esforço intencional para roubar, expor, alterar, desativar ou destruir dados, aplicativos ou outros ativos por meio de acesso não autorizado a uma rede, sistema de computador ou dispositivo digital.

Agente da Ameaça

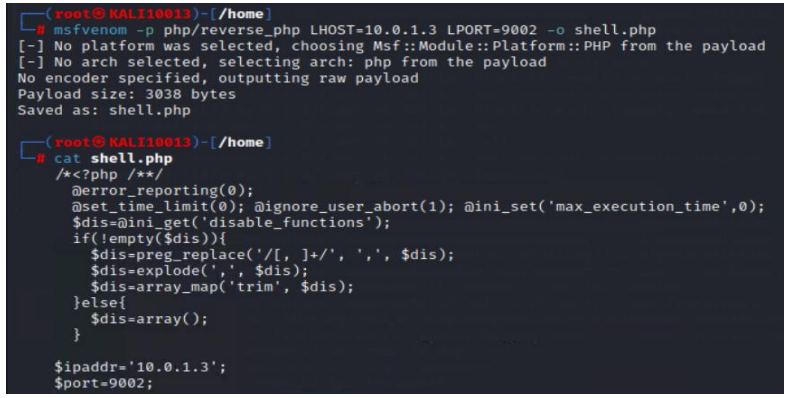
Vulnerabilidade



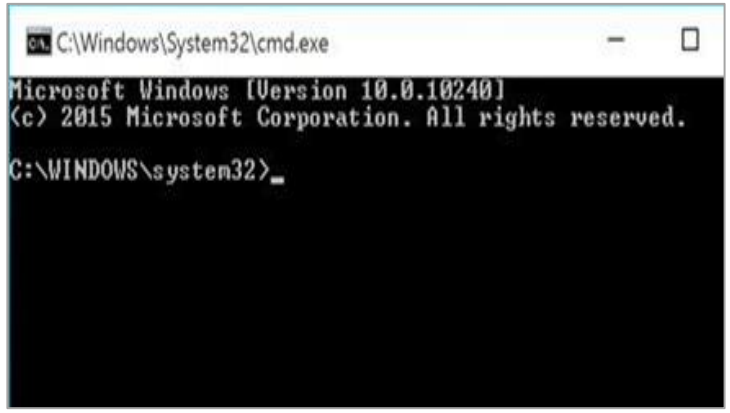
Backdoor (acesso remoto)



Exploit



Payload



Shell

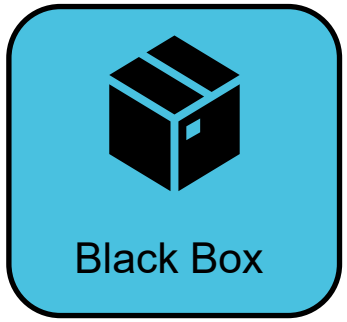
Metodologia

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Tipos de Testes

Testar a **eficácia** e a **resiliência dos ativos corporativos** por meio da **identificação e exploração de fraquezas nos controles** (pessoas, processos e tecnologia) e da simulação dos objetivos e ações de um atacante. **Existem algumas maneiras de realizar testes de intrusão**, sendo que cada uma delas terá uma **abordagem diferente**. Entre elas, podemos destacar a White Box, a Black Box e a Grey Box, conforme apresentado a seguir:

- Informações sobre sistemas conhecidas
- Geralmente utilizado na fase de testes de uma aplicação
- Autenticado ou não
- Teste mais profundo



- Simulação de ataque real
- Nenhuma ou poucas informações conhecidas
- Teste das medidas de proteção e resposta a ataques

- Combinação entre White e Black Box
- Existe uma troca de informações
- Frequente em teste de invasão para aplicações Web
- Autenticado ou não

Tipos de Testes

Os testes podem ser da **perspectiva de rede externa, rede interna, aplicação, sistema ou dispositivo**. Pode incluir engenharia social de usuários ou desvios de controle de acesso físico. Abaixo mostramos alguns dos principais tipos de testes de intrusão:

Principais Modalidades


Infraestrutura


Aplicação Web


Mobile


Wireless

API

IoT


Cloud

Escopo


Interno


Externo

Autenticação


Autenticado


Não autenticado

Tipos

Whitebox


Graybox


Blackbox

Testes Automatizados

O teste de penetração automatizado pode acelerar drasticamente o processo de proteção de aplicativos da Web. Isso beneficia a todos - incluindo os próprios testadores de penetração. Um exemplo disso, é quando o testador implanta um grande número de automatizações para procurar vulnerabilidades em seu alvo.

FORTRA | Cobalt Strike® Adversary Simulations and Red Team Operations

Ferramenta de acesso remoto comercial, com todos os recursos, que se apresenta como "software de simulação projetado para executar ataques direcionados e emular as ações pós-exploração de ameaças cibernéticas".

PortSwigger Burp Suite Professional by PortSwigger

Ajuda a automatizar tarefas de teste repetitivas e possui ferramentas de teste de segurança manuais e semiautomatizadas. Consegue ajudar a testar as vulnerabilidades OWASP Top 10 - bem como as mais recentes técnicas de hacking.

ImmuniWeb® AI for Application Security

Mantém suas defesas constantemente em alerta, simulando automaticamente ataques do mundo real. Isso identifica vulnerabilidades mais rapidamente, ajuda a corrigi-las antes que elas sejam exploradas e mantém suas defesas afiadas contra ameaças em evolução.

Abordagem

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Abordagem em Teste de Invasão

FEBRABAN

Testar a eficácia e a resiliência dos ativos corporativos por meio da identificação e exploração de fraquezas nos controle pessoas, processos e tecnologia) e da simulação dos objetivos e ações de um atacante. **A abordagem para a realização de testes de intrusão envolve várias etapas, para que se consiga adquirir o máximo de informações sobre o alvo, e garantir ataques mais eficientes**, a seguir apresentamos as **principais etapas e organização** do teste de intrusão:

Planejamento

- Antes do início do teste é necessário realizar o planejamento de todas as atividades que serão desenvolvidas, incluindo:
  - Definição de escopo dos testes;
  - Definição dos ambientes de terceiros;
  - Critérios que serão utilizados no teste;
  - Ferramentas que serão utilizadas no teste.

Descoberta e Coleta

- Entender funcionalidade e comportamento da aplicação;
- Identificar serviços e componentes ativos;
- Identificar a arquitetura da aplicação (EndPoint, API, Linguagem de programação);
- Coletar informações de autenticação e/ou autorização;
- Enumeração das informações coletadas.

Identificação e Análise

- Realizar varreduras através de ferramentas automatizadas e/ou manuais para identificar vulnerabilidades em cada sistema ou ativo identificado;
- Realizar análise dinâmica e estáticas nas aplicações;
- Mapear componentes relevantes e métodos de entradas de aplicações a fim de explorar controles de autenticação e manipulação de dados;
- Analisar vulnerabilidades com potencial de exploração;
- Validar vulnerabilidades para eliminar falso-positivos;
- Obter aprovações necessárias para prosseguir com a exploração.

Exploração

- Realizar exploração de vulnerabilidades para obter acesso não autorizado à rede, aplicação ou dados.
- Tentar escalar privilégios, bem como remover quaisquer evidências de ataque.
- Executar *exploits* públicos e privados, para confirmar a presença das vulnerabilidades identificadas e comprovar os efeitos reais na segurança do ambiente.

Relatório

- Categorizar os riscos associados as fragilidades identificadas.
- Detalhar e descrever as fragilidades identificadas.
- Definir as recomendações por fragilidade identificada.
- Apresentação Executiva dos resultados

Descoberta e Coleta de Informações

A primeira fase de um teste de invasão é fase de descoberta e coleta de informações, que consiste no processo de **levantamento de informações sobre o alvo**. Toda e qualquer informação pode ser relevante para ataques futuros.

Vale ressaltar que essa **fase é uma das mais importantes, e normalmente demanda muito tempo para a realização de uma descoberta e análise bem feita**. Uma coleta de informações **incompleta ou inconsistente pode resultar no fracasso do teste**. A seguir são apresentados 2 formas de realizar a descoberta e análise:

Passiva

- Não há contato direto com a infraestrutura do alvo.
- Não é possível detectar.

Ativa

- Há requisições e contato direto com a infraestrutura do alvo.
- É possível detectar.

Durante essa fase, é essencial coletar meticulosamente uma variedade de informações que possam ser exploradas em um ataque. Cada detalhe desempenha um papel crucial na compreensão do panorama de segurança e na identificação de possíveis vulnerabilidades. Abaixo estão os principais pontos a serem considerados durante o processo:

- ❑ Endereços IP
- ❑ Domínios
- ❑ URLs
- ❑ E-mails
- ❑ Informações de funcionários
- ❑ Vagas na empresa
- ❑ Subsidiárias
- ❑ Localizações
- ❑ Arquivos publicados na Internet
- ❑ Redes sociais de colaboradores

Exemplos de ferramentas para a descoberta e coleta de informações: Google; Registro.Br; Whois; DNS enumeration, N-Map (port scan); OSINT – Netcraft; Recon-NG; entre outras.

Identificação e Análise

De acordo com o CIS Controls, nesta etapa são realizadas **varreduras para identificar as vulnerabilidades que podem ser usadas como portas de entradas na empresa (superfície de ataque) por ameaças cibernéticas**. É importante certificar-se de que todos os ativos corporativos que estão dentro do escopo sejam descobertos, e não apenas com base em uma lista estática, que pode estar desatualizada ou incompleta. Em seguida, as vulnerabilidades serão identificadas nesses alvos.

A seguir são apresentadas as atividades relacionadas a etapa de identificação e análise de vulnerabilidades:

- Realizar varreduras através de ferramentas automatizadas e/ou manuais para identificar vulnerabilidades em cada sistema ou ativo identificado
- Realizar análise dinâmica e estáticas nas aplicações
- Mapear componentes relevantes e métodos de entradas de aplicações a fim de explorar controles de autenticação e manipulação de dados
- Formas de validação do modelo e das ameaças, e verificação do sucesso das ações tomadas
- Analisar vulnerabilidades com potencial de exploração
- Validar vulnerabilidades para eliminar falso-positivos
- Obter aprovações necessárias para prosseguir com a exploração

Exemplos de ferramentas para a descoberta e coleta de informações: Nessus, Open Vas, Qualys; Owasp Zap (Proxy); Burpsuite; entre outras ferramentas.

Exploração

De acordo com o CIS Controls, **as explorações as vulnerabilidades identificadas** (conforme os resultados da etapa anterior) **são executadas para demonstrar especificamente como uma ameaça cibernética pode subverter os controles de segurança da empresa** (por exemplo, a proteção de dados sensíveis específicos) ou até mesmo realizar ações maliciosas no ambiente (por exemplo, o estabelecimento de uma infraestrutura secreta de comando e controle, acesso não autorizado, escalação de privilégios, exfiltração de dados, entre outras). **Os resultados fornecem uma visão mais profunda, por meio de demonstração, dos riscos de negócios de várias vulnerabilidades**.

1 Exploração

- Cada ambiente possui aspectos/tecnologias especificas que exigem que o testador selecione a abordagem mais adequada e as ferramentas necessárias para realizar o teste de penetração;
- **Realizar exploração de vulnerabilidades para obter acesso não autorizado à rede, aplicação ou dados;**
- **Executar exploits** públicos e privados, para **confirmar a presença das vulnerabilidades** identificadas e **comprovar os efeitos reais na segurança do ambiente**.
- Observação: **Alguns riscos incluem desligamento inesperado de sistemas que podem ser instáveis, explorações que podem excluir ou corromper dados ou configurações**.

2 Pós-exploração

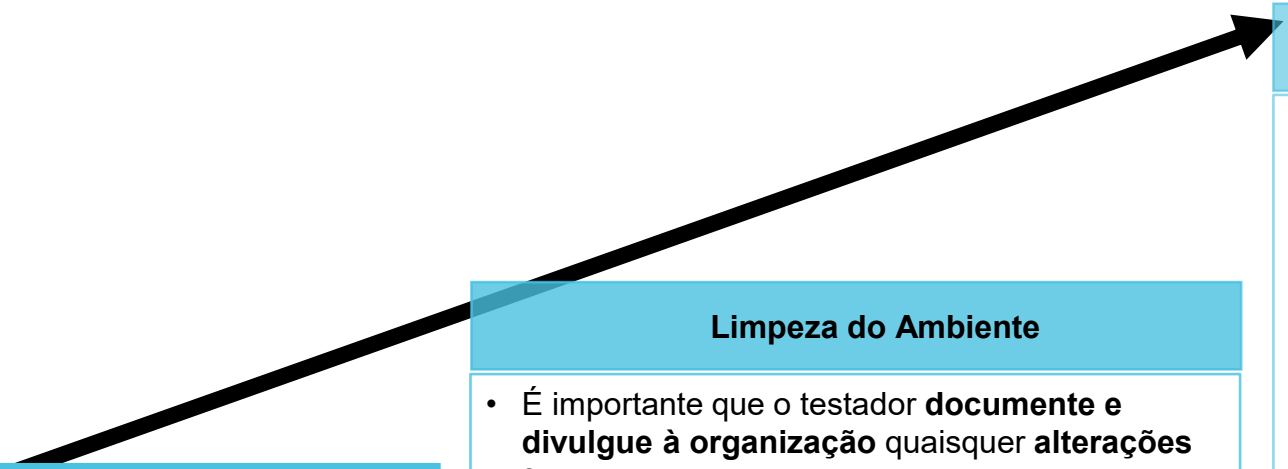
- **São as ações tomadas após o comprometimento inicial de um sistema ou dispositivo**, por exemplo, **movimentações laterais, escalonamento de privilégios ou técnicas de pivotamento** — o que permite que o testador, neste caso, estabeleça uma nova fonte de ataque a partir do novo ponto de vista no sistema — para obter acesso adicional a sistemas ou recursos de rede.

Exemplos de ferramentas para a descoberta e coleta de informações: Netcat, TCP Dump, The Metasploit Framework (MSF), Wireshark, entre outras.

Encerramento e Produção do Relatório

FEBRABAN

Nessa etapa os **riscos são categorizados** e os **resultados apresentados** aos executivos.



Vulnerabilidades encontradas

- É importante que a organização testada **investigue** cuidadosamente **sistemas** ou **aplicativos** com os **controles de segurança ineficazes**;
- A organização deve **tomar medidas para corrigir qualquer vulnerabilidade explorável** dentro de um período de tempo razoável;
- O testador deverá **executar um novo teste para validar os controles recém-implementados** para mitigar o risco original.

Limpeza do Ambiente

- É importante que o testador **documente e divulgue à organização** quaisquer **alterações** feitas no **ambiente**;
- **Contas que foram criadas** como parte da avaliação pela organização ou pelo testador devem ser **removidas**, assim como **ferramentas instaladas utilizadas nos tetes** (essas ferramentas devem ser removidas ao final do teste, para impedir a exploração contra a empresa).

Relatório

- Deve incluir: a **categorização dos riscos** associados as fragilidades identificadas, **detalhar e descrever as fragilidades** identificadas, bem como os **vetores de ataque**, as **recomendações para corrigir as vulnerabilidades** identificadas e **mitigar os riscos** associados.
- É recomendável que o relatório contenha quaisquer **constatações que impactem a postura de segurança da organização** avaliada.
- O relatório pode ser elaborado a nível técnico e executivo, bem como ser utilizado como **apoio para a tomada de decisão** sobre os **riscos** e **controles mitigatórios** no ambiente da organização.

Considerações Finais

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Frameworks e Normas de Referência

Para apoiar no entendimento e implementação de toda a metodologia apresentada neste material, a seguir são apresentados as normas e frameworks de referência no tema:

Frameworks Padrão Utilizados

NIST National Institute of Standards and Technology

SANS INSTITUTE

CWE

MITRE

PCI DSS COMPLIANT

OWASP Open Web Application Security Project

Conformidade: Dado o uso extensivo de padrões amplamente aceitos pela indústria, a orquestração dos testes deve ser alinhada com alguns dos requisitos de conformidade mais exigentes, permitindo estimar o nível de conformidade com PCI-DSS, FISMA, HIPAA, SOX, entre outros.

Relembrando os principais conceitos

Agora que aprendemos sobre as atividades relacionadas ao processo de teste de invasão, relembre os principais termos e conceitos apresentados neste material:

Testes de invasão: Testar a eficácia e a resiliência dos ativos corporativos por meio da identificação e exploração de fraquezas nos controles (pessoas, processos e tecnologia) e da simulação dos objetivos e ações de um atacante.

Descoberta de informações: Consiste no processo de levantamento de informações sobre o alvo, incluindo: endereços IPs, domínios, URL's, informações de funcionários, arquivos publicados na internet, entre outros.

Identificação e análise: Execução varreduras para identificar as vulnerabilidades que podem ser usadas como portas de entradas na empresa (superfície de ataque) por ameaças cibernéticas.

Exploração: As explorações as vulnerabilidades identificadas são executadas para demonstrar especificamente como uma ameaça cibernética pode subverter os controles de segurança da empresa (por exemplo, a proteção de dados sensíveis específicos) ou até mesmo realizar ações maliciosas no ambiente (por exemplo, acesso não autorizado, escalação de privilégios, exfiltração de dados, entre outras).

Módulo: Gestão de Vulnerabilidades

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Requisitos – Gestão de Vulnerabilidades

FEBRABAN

Este material foi elaborado de acordo com as diretrizes do CIS Controls, bem como foram considerados os requisitos de segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

PCI DSS

- 2.1 Processos e mecanismos para aplicar configurações seguras em todos os componentes de sistema são definidos e compreendidos.
- 2.2 Os componentes de sistema são configurados e administrados com segurança.
- 5.1 Processos e mecanismos para proteger todos os sistemas e redes de software malicioso são definidos e compreendidos.
- 5.2 O software malicioso (malware) é evitado ou detectado e resolvido.
- 5.3 Os mecanismos e processos antimalware são ativos, mantidos e monitorados.
- 5.4 Os mecanismos antiphishing protegem os usuários contra ataques de phishing.
- 11.3 Vulnerabilidades externas e internas são regularmente identificadas, priorizadas e tratadas.

CIS Controls

- 7.1 Estabelecer e manter um processo de gestão de vulnerabilidade
- 7.2 Estabelecer e manter um processo de remediação
- 7.3 Executar a gestão automatizada de patches do sistema operacional
- 7.4 Executar a gestão automatizada de patches de aplicações
- 7.5 Realizar varreduras automatizadas de vulnerabilidade em ativos corporativos internos
- 7.6 Realizar varreduras automatizadas de vulnerabilidade em ativos corporativos expostos externamente
- 7.7 Corrigir vulnerabilidades detectadas

ISO 27002

- 8.8 Management of technical vulnerabilities
- 8.9 Configuration management
- 8.19 Installation of software on operational systems

ISO 27701

- 6.9.6.1 Gestão de vulnerabilidades técnicas
- 6.9.6.2 Restrições quanto à instalação de software

NIST CSF

- ID.RA-01: Vulnerabilidades em ativos são identificadas, validadas e registradas
- ID.RA-08: Processos para receber, analisar e responder a divulgações de vulnerabilidades são estabelecidos

Sumário

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Sumário

Contexto e Introdução

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Contexto

As instituições são constantemente desafiados por atacantes que procuram vulnerabilidades em sua infraestrutura para explorar e obter acesso.

Compreender e **gerenciar vulnerabilidades** é uma atividade contínua, que requer foco de tempo, atenção e recursos.

Essa é um processo que nunca será perfeito, uma vez que a vulnerabilidade é conhecida na comunidade, o processo mencionado de remediação pode ser iniciado. No entanto os defensores devem estar cientes de que pode sempre haver vulnerabilidades que eles não podem remediar e, portanto, precisam usar outros controles para mitigar.

Os atacantes têm acesso às mesmas informações e muitas vezes podem tirar proveito das vulnerabilidades mais rapidamente do que uma empresa pode remediar, **eles podem desenvolver um exploit de "zero day", onde não há uma remediação conhecida para esse ataque.**

É necessário ter em mente que existe um tempo para a vulnerabilidade ser descoberta e os pesquisadores ou a comunidade desenvolver e implantar patches, indicadores de comprometimento (IOCs) e atualizações.

Por isso é importante as instituições **avaliar os riscos e priorizar** quais as **vulnerabilidades** são mais impactantes para a empresa e quais poderão ser **exploradas** primeiro.

Introdução

O que é gestão de vulnerabilidades?

O gerenciamento de vulnerabilidades é o processo contínuo e regular de segurança da TI que envolve a **identificar, avaliar, relatar, gerenciar e remediar vulnerabilidades** cibernéticas em **dispositivos**, **redes** e **aplicações** de modo a **reduzir** os **riscos** de ataques cibernéticos e **violações**.

Quais as normas/frameworks?

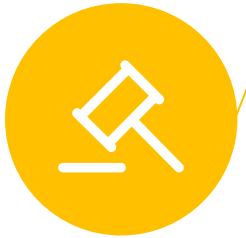
- ISO 27001/27002
- NIST Cyber Security Framework
- PCI-DSS (padrão de segurança de dados do setor de cartões de pagamento)
- Cis Controls

Quais os benefícios?

- Identificar fragilidades antes que sejam exploradas por *hackers* ou levem a outro tipo de ação nociva.
- Evitar problemas de segurança previne a paralisação das atividades, prejuízos e danos à imagem da organização e à sua relação com clientes e outros *stakeholders*.
- Contribui para que padrões de segurança mais robustos sejam adotados, mantendo a conformidade com a LGPD e outras diretrizes que se apliquem ao setor de atuação da empresa.

Como as vulnerabilidades são classificadas?

- Essa avaliação é feita considerando a classificação baseada no Common Vulnerability Scoring System (CVSS), um sistema que define pontuações para indicar a gravidade e as características das vulnerabilidades de softwares.



Abordagem

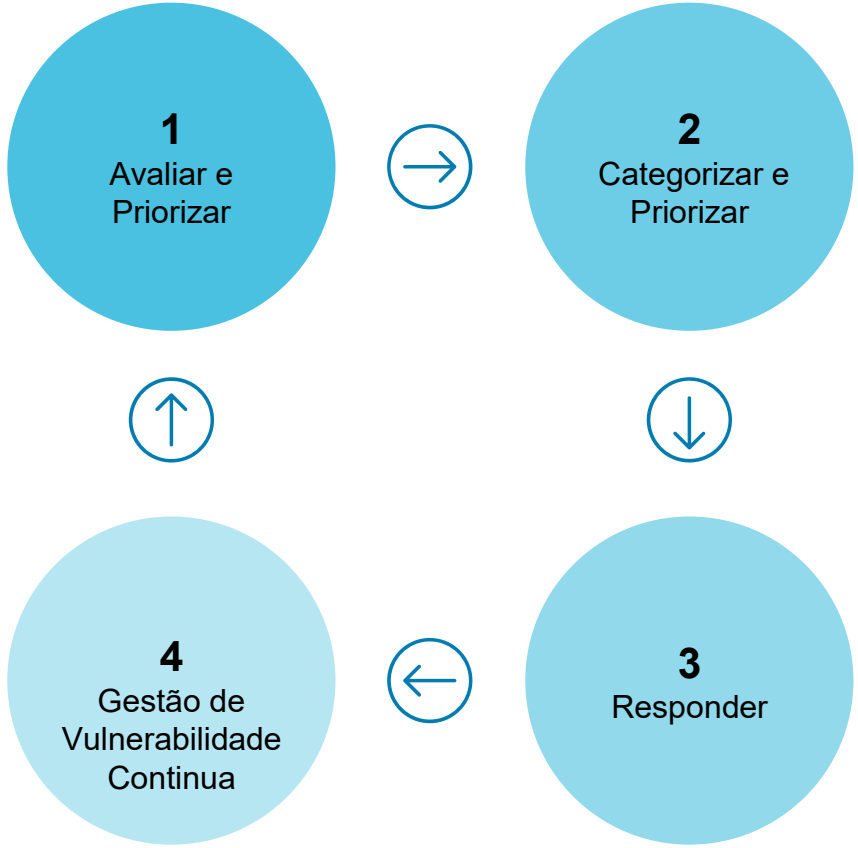
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Visão Geral - Gestão de Vulnerabilidades

FEBRABAN

As organizações devem obter informações oportunas de ameaças disponíveis sobre: **atualizações de software, patches, avisos de segurança, boletins de ameaças**, entre outras, e devem revisar regularmente seu ambiente para identificar essas vulnerabilidades antes de uma potencial exploração por agentes maliciosos.

Compreender e **gerenciar vulnerabilidades** é uma **atividade contínua, que requer foco de tempo, atenção e recursos.**



Exemplos práticas de maturidades relacionadas à Gestão de Vulnerabilidades:

Baixa Maturidade: Durante uma revisão interna, uma organização identificou um serviço de nuvem que não tinha a funcionalidade de autenticação multifator habilitada. Ao avaliar a situação, a organização decidiu que não valia a pena o tempo e o esforço para habilitar a funcionalidade, sem mencionar as reclamações que esperavam receber dos usuários. Então, a organização optou por simplesmente aceitar o risco de não implementar um controle compensatório forte.

Alta Maturidade: Durante uma revisão interna, uma organização identificou um servidor Microsoft Windows de baixo risco que não pôde ser corrigido. Como resultado, a organização implementou um plano para desativar o servidor dentro de dois meses. Nessa situação, ainda era importante que a organização aplicasse controles compensatórios para reduzir o risco identificado a um nível aceitável Como resultado, uma prioridade de risco foi designada e fortes controles de compensação foram implementados.

Etapas - Gestão de Vulnerabilidades

FEBRABAN

Identificar | **Categorizar e Priorizar** | **Responder** | **Gestão de Vulnerabilidade Continua**

- Essa é a **primeira etapa do processo** de gestão de vulnerabilidades técnicas.
- **É recomendável a utilização de ferramentas automatizadas para identificar vulnerabilidades de segurança nos ativos tecnológicos corporativos**, incluindo notebooks, servidores, endpoints, disponíveis móveis, entre outros ativos.
- As ferramentas realizam **varreduras de portas**, **detectando servidores** ativos e **simulando invasões para detectar vulnerabilidades.**
- Além disso, **informações sobre ameaça** cibernéticas também podem ser **obtidas** a partir de **fóruns e fontes de compartilhamento de informações e centros de inteligência**.

A seguir são apresentadas as atividades relacionadas a etapa de identificação de vulnerabilidades:

Realizar varreduras através de ferramentas automatizadas e/ou manuais para identificar vulnerabilidades em cada sistema ou ativo identificado (internos e externos)

Validar vulnerabilidades para eliminar falso-positivos

Potenciais impactos no negócio e probabilidades são identificados na organização

Vulnerabilidades dos ativos são identificadas e documentadas

Outros exemplos de ferramentas para descobrir vulnerabilidades: InsightVM, Qualys VMDR, Tripwire IP360, SanerNow Continuous Vulnerability and Exposure Management (CVEM), Falcon Spotlight e Open Vas.

Etapas - Gestão de Vulnerabilidades

Identificar | Categorizar e Priorizar | Responder | Gestão de Vulnerabilidade Continua

Exemplos de Ferramentas para Identificar Vulnerabilidades:

Nessus

Nessus é um programa que executa a verificação de falhas/vulnerabilidades de segurança. Ele realiza uma varredura de portas, detectando servidores ativos e simulando invasões para detectar vulnerabilidades. Uma característica importante é que o Nessus procura por servidores ativos não apenas nas portas padrão, mas em todas as portas TCP.

Nikto

O Nikto é um script (conjunto de instruções) que analisa vulnerabilidades comuns em servidores Web. Ela irá encontrar diversos tipos de arquivos, configurações e programas padrões inseguros, auxiliando a utilização de outros programas, como OpenVAS e Nessus.

Acunetix

Acunetix é uma ferramenta muito utilizada para realizar scans de vulnerabilidades em aplicações Web. Esta ferramenta testa ataques de SQL Injection, XSS, XXE, SSRF, Host Header Injection, entre outras vulnerabilidades Web existentes

Etapas - Gestão de Vulnerabilidades

Identificar | Categorizar e Priorizar | Responder | Gestão de Vulnerabilidade Continua

O Common Vulnerability Scoring System (CVSS) fornece uma maneira de capturar as principais características de uma vulnerabilidade e produzir um score numérico que reflita sua gravidade.

- **Avaliar** as **ameaças** como baixa, média, alta e crítica.
- Considerar o uso de uma metodologia formal, objetiva e justificável que retrate com precisão os riscos pertinentes à organização.
- Permite a **priorização** e **tratamento dos itens de maior risco** mais rapidamente.
- É necessário avaliar a **probabilidade** de um agente de ameaça usar uma **vulnerabilidade** ou potencial impacto de uma exploração na empresa.

Pontuação CVSS	Avaliação de gravidade
0.0	Nenhuma
0.1-3.9	Baixa
4.0-6.9	Média
7.0-8.9	Alta
9.0-10.0	Critica

Etapas - Gestão de Vulnerabilidades

Identificar → Categorizar e Priorizar → **Responder** → Gestão de Vulnerabilidade Continua

Após a priorização da vulnerabilidade, é necessário adotar a remediação de acordo a tolerância ao risco da instituição, usando uma metodologia formal, objetiva e justificável que retrate com precisão os riscos das vulnerabilidades pertinentes à organização.

Remediação

- **Corrigir totalmente** uma vulnerabilidade para que ela não possa ser explorada.
- Opção de tratamento ideal que as organizações buscam.

Mitigação

- **Diminuir a probabilidade** e/ou o **impacto** de uma vulnerabilidade ser explorada.
- Necessário quando uma correção ou patch adequado ainda não está disponível.
- Deve ser usada para ganhar tempo para que uma organização corrija uma vulnerabilidade.

Aceitação

- Não tomar nenhuma ação para corrigir ou diminuir a probabilidade/impacto.
- Justificado quando uma vulnerabilidade é considerada de baixo risco e o custo de corrigir a vulnerabilidade é substancialmente maior do que o custo incorrido por uma organização se a vulnerabilidade for explorada.

- **Obs.: Caso a vulnerabilidade não tenha sido remediada ou mitigada e seja de nível CRÍTICA ou ALTA, torna-se necessário realizar a comunicação e informar a instituição sobre a existência da vulnerabilidade.**

Exemplo

Gravidade	Tempo para correção
Critica	2 dias
Alta	7 dias
Media	25 dias
Baixa	90 dias

Etapas - Gestão de Vulnerabilidades

FEBRABAN

Identificar → Categorizar e Priorizar → Responder → Gestão de Vulnerabilidade Continua

Avaliação Contínua

Monitoramento Contínua

Correções Contínuas

Relatórios

Hardenização segura

- Implantar patches, indicadores de comprometimento (IOCs) e atualizações.
- Realizar testes de regressão nos patches e instalar o patch.
- Baseline de segurança com base nos requisitos de segurança ou classificação dos dados no ativo corporativo.

Todo o processo de gestão de vulnerabilidade deve ser comunicado com as ameaças, riscos e decisões tomadas. Além disso é importante documentar as atividades de resposta organizacionais para serem aperfeiçoadas pela incorporação de lições aprendidas de atividades anteriores de detecção/resposta.

Etapas - Gestão de Vulnerabilidades

Identificar | Categorizar e Priorizar | Responder | Gestão de Vulnerabilidade Continua

O **processo de gerenciamento de atualizações de software** deve ser implementado para garantir que os patches atualizados sejam instalados para todos os softwares autorizados.

Existe a possibilidade de que uma atualização não resolva o problema adequadamente e tenha efeitos colaterais negativos. **Por isso é importante manter o software original e testar a atualização.**

A organização pode considerar o fornecimento de um processo de **atualização automatizado em que essas atualizações são instaladas em sistemas ou produtos afetados sem a necessidade de intervenção do cliente ou do usuário**.

A gestão técnica de vulnerabilidades pode ser vista como uma subfunção da gestão da mudança, onde a introdução de novos sistemas e as grandes alterações aos sistemas existentes devem **seguir as regras acordadas e um processo formal de documentação, especificação, testes, controle de qualidade e implementação gerenciada.**

Os **CIS Benchmarks** são projetados como um componente-chave de um programa abrangente de segurança cibernética, para fornecer orientações prescritivas para estabelecer uma postura de **configuração segura do sistema operacional.**

As configurações, incluindo as **configurações de segurança, de hardware, software, serviços e redes** devem ser estabelecidas, documentadas, implementadas, monitorizadas e revistas.

O Cis Benchmark da definições recomendadas seguindo diversos componentes aplicáveis. Se caso os componentes não são aplicáveis, não estarão nas recomendações. **Nas recomendações é exposto se a configuração é automatizada ou manual, uma descrição, o impacto que ela pode ter, entre outras coisas.**

É importante que a organização defina e implemente processos e ferramentas para impor as **configurações definidas, incluindo configurações de segurança, para o hardware, software, serviços, redes e sistemas recém instalados, durante toda a sua vida útil.**

Considerações Finais

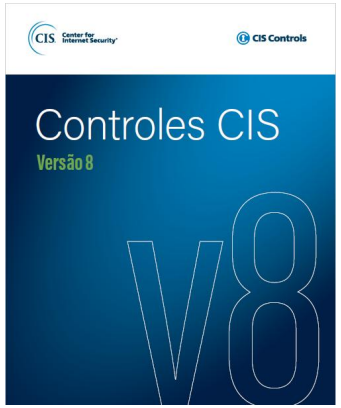
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Frameworks e Normas de Referência

Para apoiar no entendimento e implementação de toda a metodologia apresentada neste material, a seguir são apresentados as normas e frameworks de referência no tema:

Frameworks Padrão Utilizados

PCI DSS COMPLIANT



NIST National Institute of Standards and Technology

OWASP Open Web Application Security Project

Conformidade: Dado o uso extensivo de padrões amplamente aceitos pela indústria, a orquestração das varreduras deve ser alinhada com alguns dos requisitos de conformidade mais exigentes, permitindo estimar o nível de conformidade com ABNT NBR ISO, PCI-DSS, SOX, OWASP, entre outros.

Relembrando os principais conceitos

FEBRABAN

Agora que aprendemos sobre as atividades relacionadas ao processo de gestão de vulnerabilidades técnicas, relembre os principais termos e conceitos apresentados neste material:

- **Gestão de Vulnerabilidade:** O gerenciamento de vulnerabilidades é o processo contínuo e regular de identificar, avaliar, relatar, gerenciar e remediar vulnerabilidades cibernéticas.
- **Common Vulnerability Scoring System (CVSS)** : Fornece uma maneira de avaliar e priorizar as vulnerabilidades que podem afetar a instituição
- **Resolução**: Etapa em que as vulnerabilidades, já categorizadas, irão ser remedias, mitigadas ou aceitas.
- **Gerenciamento de atualizações de software:** Garante que as atualizações aprovadas de patches e aplicativos sejam implementadas e automatizadas.
- **Gestão de mudança:** Gerencia a introdução de novos sistemas e as grandes alterações aos sistemas.
- **CIS Benchmark**: Fornece orientações para estabelecer uma postura de configuração segura do sistema operacional..

Módulo: Gestão de Incidentes

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Requisitos – Gestão de incidentes

FEBRABAN

Este material foi elaborado de acordo com as diretrizes do PCI DSS e CIS Controls, bem como foram considerados os requisitos de segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

PCI DSS

- 12.10.1 Um plano de resposta a incidentes existe e está pronto para ser ativado
- 12.10.2 Pelo menos uma vez a cada 12 meses, o plano de resposta a incidentes de segurança é revisado
- 12.10.3 Pessoal específico é designado para estar disponível 24 horas por dia, 7 dias por semana
- 12.10.4 O pessoal responsável por responder a incidentes de segurança suspeitos e confirmados é adequada e periodicamente treinado em suas responsabilidades
- 12.10.5 O plano de resposta a incidentes de segurança inclui monitorar e responder a alertas de sistemas
- 12.10.6 O plano de resposta a incidentes de segurança é modificado e evoluído de acordo com as lições aprendidas

CIS Controls

- 17.1 Designar Pessoal para Gerenciar Tratamento de Incidentes
- 17.2 Estabelecer e manter informações de contato para relatar incidentes de segurança
- 17.3 Estabelecer e manter um processo corporativo para relatar incidentes
- 17.4 Estabelecer e manter um processo de resposta a incidentes
- 17.5 Atribuir funções e responsabilidades chave
- 17.6 Definir mecanismos de comunicação durante a resposta a incidente
- 17.7 Conduzir exercícios de resposta a incidentes rotineiros
- 17.8 Conduzir análises pós-incidente
- 17.9 Estabelecer e manter limites de incidentes de segurança

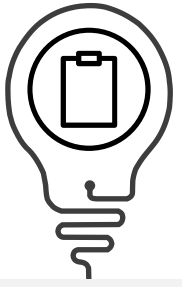
ISO 27002

- 5.24 Planejamento e preparação para gerenciamento de incidentes de segurança da informação
- 5.25 Avaliação e decisão sobre eventos de segurança da informação
- 5.26 Resposta a incidentes de segurança da informação
- 5.27 Aprendizagem com incidentes de segurança da informação
- 5.28 Coleta de evidências

ISO 27701

- 6.13.1.1 Responsabilidades e procedimentos em gestão de incidentes
- 6.13.1.2 Notificação de eventos de segurança da informação
- 6.13.1.3 Notificando fragilidades de segurança da informação
- 6.13.1.4 Avaliação e decisão dos eventos de segurança da informação
- 6.13.1.5 Resposta aos incidentes de segurança da informação
- 6.13.1.6 Aprendendo com os incidentes de segurança da informação
- 6.13.1.7 Coleta de evidências

NIST CSF



- RS. MA-01: O plano de resposta a incidentes é executado em coordenação com terceiros relevantes assim que um incidente é declarado
- RS. MA-02: Notificações de incidentes são triadas e validadas
- RS. MA-03: Os incidentes são categorizados e priorizados

Sumário

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Sumário

Contexto Cibernético

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Incidentes Cibernéticos

2023 Data Breach Investigations Report

Relatório anual com análise de casos reais de vazamentos de informações e incidentes de segurança com apoio de mais de 60 empresas especializadas.

Na última pesquisa **o mercado financeiro registrou 1830 incidentes** de segurança da informação onde **480 dos incidentes tiveram divulgação de dados confirmada.**

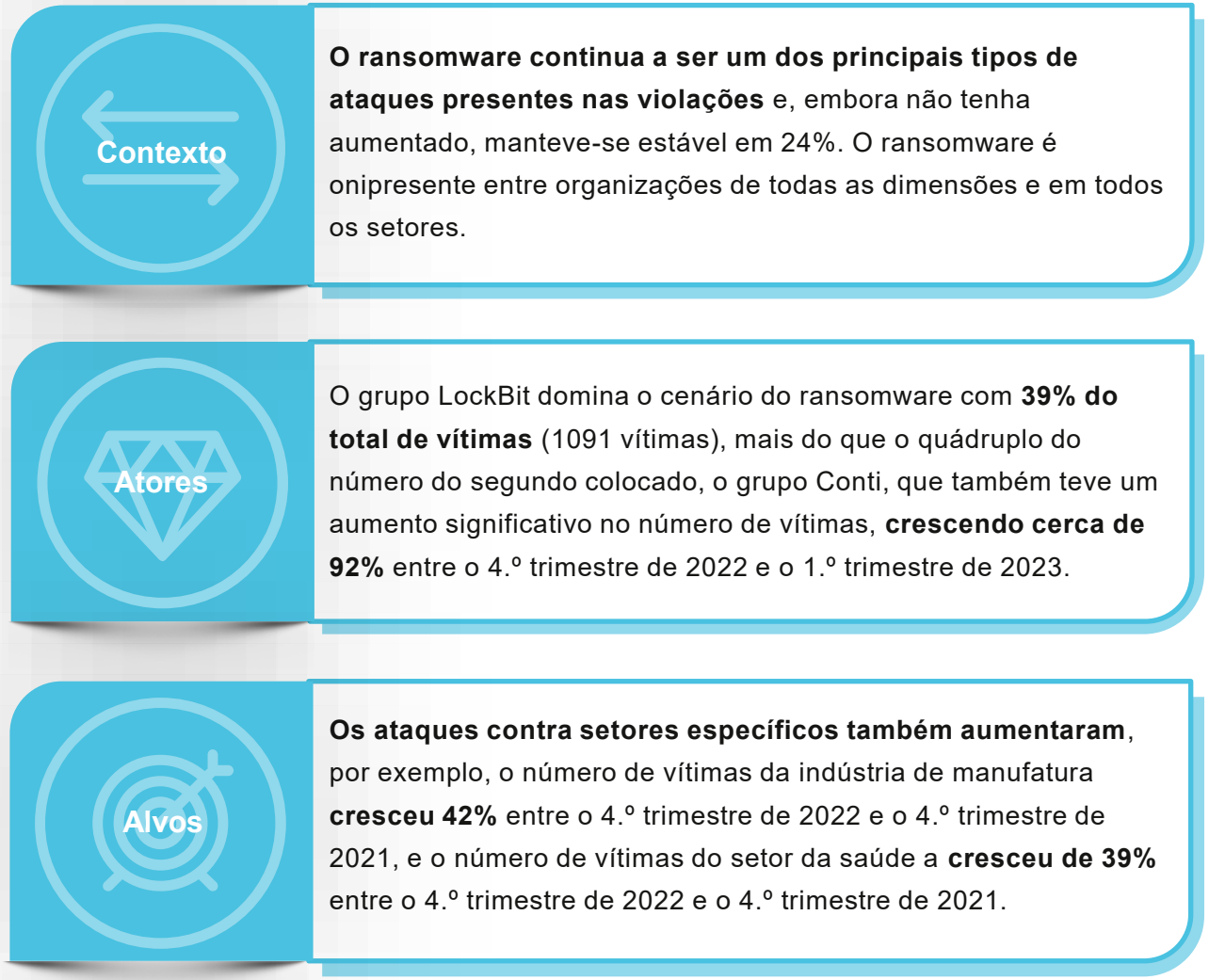
1 a cada 4 Incidentes
com divulgação de dados confirmada

77% de todos os incidentes de segurança no financeiro são:

- Ataques de Aplicações
- Erros humanos
- Exploração de vulnerabilidades.

Importância de Segurança da Informação para as instituições financeiras se faz necessária devido à complexidade do ambiente em um mercado alvo de ataques.

Fonte: DBIR 2023 Data Breach | Investigations Report



Fonte: Akamai Ransomware Report - 2023

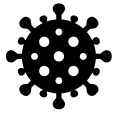
Introdução

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Introdução

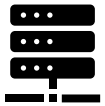
Segundo o CIS Control, as Organizações devem estabelecer um programa para **desenvolver e manter uma capacidade de resposta a incidentes** (por exemplo, políticas, planos, procedimentos, funções definidas, treinamento e comunicações) para **preparar, detectar e responder rapidamente a um incidente de segurança**. **O objetivo principal da resposta a incidentes é identificar ameaças na empresa, responder a elas antes que possam se espalhar e remediá-las antes que possam causar impactos.**

Principais conceitos em gestão de incidentes



Eventos:
Qualquer ocorrência observável em um sistema ou rede. As fontes de log de sistemas individuais, dispositivos de rede ou qualquer outro, conterão eventos.

Alertas:
Pode ser produzido com base em um único evento que mostra imediatamente uma ameaça em potencial ou em uma série de eventos correlatos que indicam uma ameaça em potencial.



Falso Positivos:
Evento que, após análise, conclui-se que não representa ação maliciosa ou desvio de procedimento. Após a identificação deste tipo de situação, o analista pode solicitar revisão de exceção ou da regra de detecção.

Alerta Relevante:
Quando o evento ou alerta é determinado como um possível incidente de segurança cibernética. Um alerta relevante requer uma investigação minuciosa para entender o Modus Operandi e realizar a validação se é um incidente ou um falso positivo.

Incidentes:
Violação de uma política ou controle de segurança explícito ou implícito, com capacidade de comprometer toda uma infraestrutura interna.

Plano de Resposta a Incidentes de Segurança

De acordo com o Art. 6º da resolução 4893 do Bacen, as instituições devem **estabelecer plano de ação e de resposta a incidentes** visando à implementação da política de segurança cibernética:

Exemplo de Plano

O plano deve conter no mínimo:

As ações a serem desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética

As rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética

A área responsável pelo registro e controle dos efeitos de incidentes relevantes

Funções, responsabilidades e estratégias de comunicação e contato no caso de um incidente

Processos de backup de dados (cópias de segurança)

SOC

O SOC (*Security Operations Center*) é um time interno ou terceirizado de profissionais de segurança de TI que **monitoram toda a infraestrutura de TI da Organização**, em formato 24/7 (24h nos 7 dias da semana), para **detectar eventos de segurança cibernética em tempo real e resolvê-los da maneira mais rápida e eficiente possível**.

Monitoramento Contínuo

O SOC monitora toda a infraestrutura de TI, 24/7/365: aplicativos, servidores, software do sistema, dispositivos de computação, cargas de trabalho na cloud e a rede, em busca de atividades suspeitas e sinais de invasão.

Ativos Críticos

Especialistas que apoia a Instituição na **identificação das informações mais críticas** a serem protegidas na Organização.

Risk-based

O SOC possui uma gestão baseada em risco, de forma a priorizar os ativos que trazem maior impacto para a organização.

Visão Global

O SOC pode ter uma estrutura global, **na qual todos os SOCs são interconectados** e compartilham informações de inteligência para uso da instituição.

Serviços

O portfólio de serviços do SOC geralmente incluí: monitoramento contínuo do ambientes tecnológicos da empresa, gestão de identidades e acessos, serviços gerenciados de segurança (por exemplo, dispositivos móveis) e gestão de incidentes/ crises.

Contatos Externos

O SOC pode realizar contato externo com outras instituições para a troca de informações sobre ameaças cibernéticas, além de **acompanhar informações que são publicadas por centros de inteligências, fóruns e sites que relatam sobre ameaças cibernéticas.**

Gestão de Incidentes de Segurança da Informação

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Visão Geral - Gestão de Incidentes

FEBRABAN

De acordo com a ISO 27002, o objetivo da gestão de incidentes é assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação. Esse **processo fornece uma abordagem padronizada e organizada para lidar com incidentes de segurança da informação.**

Detectar	Avaliar e Priorizar	Responder	Comunicar	Lições aprendidas
Os eventos de segurança da informação devem ser relatados através dos canais apropriados da Organização, o mais rapidamente possível.	Avaliar os incidentes utilizando uma escala de classificação, para decidir se o evento deve ser classificado como um incidente de segurança da informação, além disso, é necessário identificar o impacto e a abrangência do incidente.	Ações realizadas para reestabelecer a operação de segurança da Organização ao estado de normalidade, envolvendo: • análise detalhada; • coleta de evidências; • contenção do incidente; • erradicação do incidente; • Playbooks; e outros.	Realizar as comunicações sobre os incidentes relevantes de segurança para todas as partes interessadas relevantes, podendo ser partes internas e externas.	Identificar oportunidades de melhorias em processos internos, avaliar a efetividade do processo de gestão de incidentes, fortalecer as capacidades de resposta e melhorar os controles da instituição.

Ferramentas que podem ser utilizadas em gestão de incidentes: ITSM (Service Now), XDR, XSOAR, XSIAM, SIEM, Guardicore, SIMOC, entre outras.

Segundo a ISO 27002, os **eventos de segurança da informação devem ser relatados através dos canais apropriados da Organização**, o mais rapidamente possível.

1

Detecção de Eventos

A primeira fase do ciclo de vida de incidentes cibernéticos é a **detecção de qualquer evento adverso que possa indicar um comprometimento dos sistemas** da organização. Exemplos de tais eventos são:

- falhas suspeitas no sistema;
- acesso não autorizado a dados confidenciais;
- execução de código malicioso;
- notificações interna de colaboradores ou externas;
- processo de Threat Intel;
- violações de procedimentos de segurança física;
- alto número de tentativas de login com falha ou sucesso;
- alterações de usuários para grupos administrativos.

2

Alertas Relevantes

Alertas relevantes serão descobertos principalmente por meio de ferramentas de segurança e alertas; no entanto, **eventos também podem ser recebidos de usuários finais que notam atividades suspeitas**. Tais atividades podem incluir:

- anexos maliciosos;
- e-mails suspeitos;
- mensagens pop-up incomuns que aparecem na tela;
- violação de acesso;
- problemas com funcionamento de software ou hardware.

3

Canais de Notificação

Os funcionários e partes externas da Organização **devem notificar potenciais eventos** e/ou incidentes **para o ponto de contato adequado**, o mais rápido possível, de forma a prevenir incidentes de segurança da informação. O mecanismo de notificação deve ser fácil, acessível e disponível, sempre que possível, tais como:

- uma página/portal dedicado;
- e-mail;
- telefone;
- ferramenta de comunicação no local de trabalho (exemplo: Teams);
- redes sociais.

Segundo a ISO 27002, **após a detecção de um evento é necessário avaliá-los utilizando uma escala de classificação, para decidir se o evento deve ser classificado como um incidente de segurança da informação**. A **priorização** e a **classificação** de incidentes pode ajudar a **identificar** o **impacto** e a **abrangência** de um **incidente**.

A seguir são apresentadas as principais atividades que devem ser realizadas na triagem do incidente:

- determinar o escopo afetado (redes, sistemas ou aplicativos afetados);
- coletar e analisar informações/evidências;
- notificar à entidade, área ou empresa envolvida adequadamente;
- classificar os incidentes com a taxonomia;
- avaliar a criticidade do incidente e atribuir sua prioridade;
- determinar uma estratégia apropriada de contenção, erradicação e recuperação.

URGÊNCIA

- Crítica
- Alta
- Média
- Baixa

IMPACTO

- Nenhum
- Baixo
- Moderado
- Alto
- Extremo

CATEGORIA

- Atividade legítima
- Atividade ilegal
- Comprometimento de ativo
- Vazamento de dados
- E-mail
- Hacking
- Malware
- Threat Intelligence
- Violação de política

A seguir é apresentado um exemplo de priorização de incidentes de segurança, bem como os critérios utilizados e SLA para contenção dos incidentes:

Prioridade	Critério	SLA de contenção
Crítico	Maior prioridade. Incidentes que causam(ou tem potencial de) paralização de serviços críticos, comprometimento de informação ou ativo crítico. Impacto potencial é extremo ou ação maliciosa em andamento (exemplo, ransomware).	60 min/1 Hora
Alto	Incidentes que causam (ou tem potencial de) de paralização de serviços, comprometimento de informação ou ativo. Possibilidade de comprometimento de outros ativos. Ação maliciosa não está ocorrendo.	240 min/ 4 horas
Médio	Incidentes que podem indicar falha ou comprometimento de camadas de segurança.	2880 min/ 48 Horas
Baixo	Incidentes sem impacto potencial e atividades que não necessitam de SLA para conclusão.	-
Info	Menor prioridade. Incidentes do tipo informacionais, registros.	-

Detectar | Avaliar e Priorizar | Responder | Comunicar | Lições aprendidas

Segundo a ISO 27002, para ter uma resposta eficiente e eficaz, os incidentes devem ser respondidos de acordo com os procedimentos documentados na etapa anterior.

01

Análise detalhada (investigação)
Todos os incidentes devem ser analisados de forma consistente e em tempo hábil, de acordo com a sua severidade e prioridade.

02

Coleta de evidências
É imprescindível a coleta e o manuseio de evidências críticas à resolução do incidente, bem como a utilização de procedimentos legais relacionados ao caso investigado.

03

Resposta ao Incidente
Ela deve ser realizada de forma imediata e a área de segurança deve propor e elaborar planos de ação para corrigir e mitigar o incidente identificado.

04

Playbooks
Manuais técnicos podem ser utilizados e podem fornecer orientações específicas de como remediar os incidentes.

05

Contenção
O incidente deve ser contido antes que o invasor possa executar mais ações. A contenção deve ser rápida, mas é crucial entender completamente a extensão do comprometimento do incidente.

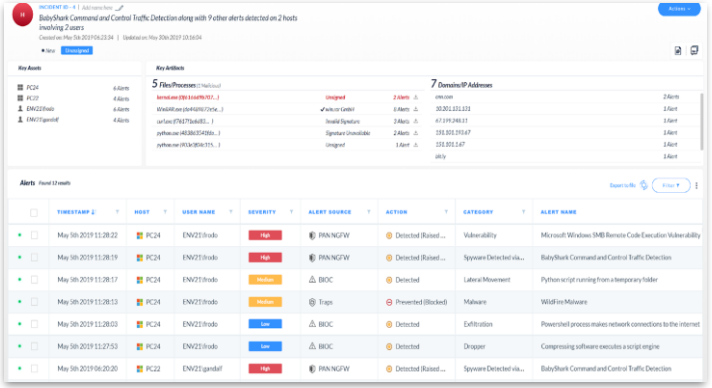
06

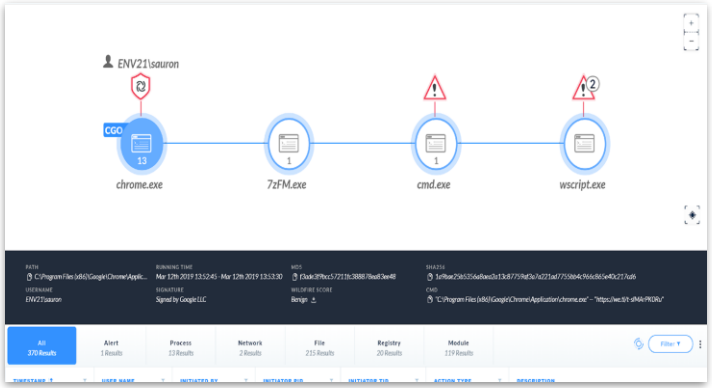
Erradicação e recuperação
Essa fase garante a remoção da ameaça. Se um sistema for comprometido, pode ser reconstruído a partir de uma imagem confiável e se for incidente de menor complexidade, o artefato pode ser removido através da desinstalação ou exclusão manual.

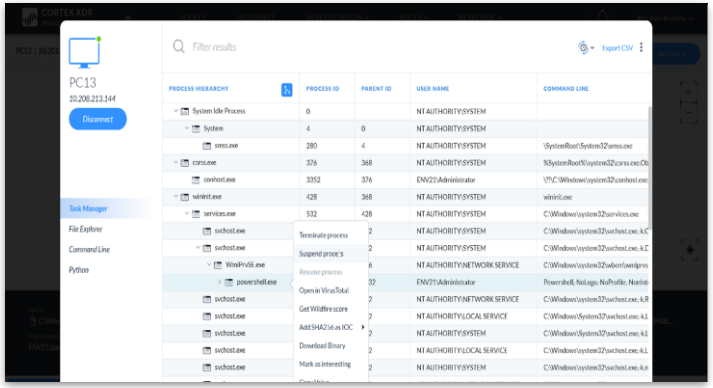
Detectar | Avaliar e Priorizar | Responder | Comunicar | Lições aprendidas

A etapa de análise é uma das mais importantes da gestão de Incidentes e é possível utilizar diversas ferramentas para apoiar nesta etapa. **As ferramentas podem ajudar a acelerar as investigações, fornecendo uma visão completa de cada incidente e com análise de causa raiz**, conforme os exemplos apresentados a seguir:

Investigação e resposta à ameaças detectadas:







✓ Mecanismo Unificado de Incidentes

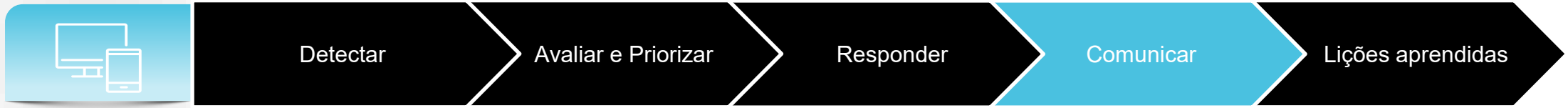
Agrupe alertas relacionados de forma inteligente em um incidente

✓ Análise automatizada de causa raiz

Revele a causa raiz dos ataques, bem como identifique as casualidades e comportamento dos eventos

✓ Resposta Integrada

Ações rápidas para conter ataques ou executar análises forenses personalizadas



Segundo a ISO 27002, a organização deve **estabelecer e comunicar procedimentos sobre os incidentes a todas as partes interessadas relevantes** e essa comunicação deve ser feita por uma equipe designada com as competências necessárias.

Nesta etapa, **em atendimento principalmente as exigências de reguladores, torna-se necessário realizar a notificação ao Controlador de dados** (no caso de Operadores em nome das Instituições)**, Titulares de Dados e ANPD** (Autoridade Nacional de Proteção de Dados)**, sobre a ocorrência de incidentes que possam acarretar risco ou dano relevante aos titulares.**

Exemplo Macro de Fluxo de Comunicação

Quando na posição de <u>Operador</u>

1

Reportar ao Controlador (Instituições) sobre a ocorrência de incidentes com potencial de impacto à privacidade dos titulares de dados, bem como enviar **relatório contendo as informações sobre o incidente**.

Quando na posição de <u>Controlador</u>

2

Reportar aos órgãos regulatórios (ANPD) e autoridades quanto a ocorrência de incidentes relevantes

3

Reportar sobre possíveis vazamentos de dados aos **titulares** dos dados de acordo com a LGPD

Notificação de incidentes de privacidade: Está disponível no site da ANPD formulários para a elaboração das comunicações quando há incidentes envolvendo titulares de dados pessoais, as **comunicações devem ocorrer em até 72 horas após a confirmação do incidente**, conforme definido na Lei.

Link – Material de Apoio

O objetivo dessa etapa é **identificar oportunidades de melhorias em processos internos, além de avaliar a efetividade do processo**. Segundo a ISO 27002, é necessário utilizar os conhecimentos adquiridos com os incidentes para fortalecer as capacidades de resposta e melhorar os controles da instituição. Com isso, é possível reduzir a probabilidade ou consequências de incidentes futuros. A seguir são apresentados alguns exemplos:

Fatores que podem ser considerados na análise

- Uma revisão do incidente
- Se o tempo de resposta estava apropriado
- Se os procedimentos foram seguidos
- Se faltou alguma informação.
- O que poderia ser feito de diferente
- O que é necessário para evitar que o incidente volte a acontecer
- Quais ferramentas ou recursos adicionais podem ser necessários

Produção de relatório

Após a conclusão do incidente é necessário uma reunião sobre as lições aprendidas, onde todas as partes interessadas e pessoas envolvidas vão entender todos os detalhes do incidentes e criar um relatório sobre áreas que precisam de melhorias e/ou um plano de ação.

Taxonomia

Nessa etapa também é necessário avaliar se as métricas e indicadores utilizados na contenção do incidentes foram suficientes ou é necessário adaptar elas para o próximo.

Exercícios

Dinâmicas de exercícios podem ser realizadas para aprimorar o nível de preparo dos profissionais em atuações em incidentes. Além disso, os exercícios ajudam a identificar nível de prontidão dos funcionários, tempo de resposta e recuperação à normalidade, processo de comunicação. Os resultados dos exercícios devem ser utilizados para aprimorar a gestão dos incidentes.

A **Taxonomia** contribui com a **eficiência** e **efetividade** do **gerenciamento** de incidentes:

Principais medições de tempo aplicadas nos incidentes

MTTD (Mean Time to Detect)

Tempo decorrido para que um analista inicie o tratamento do incidente em minutos

MTTA (Mean Time to Analyse)

Tempo decorrido para que o analista continua a triagem do incidente(confirmação, categorização) em minutos

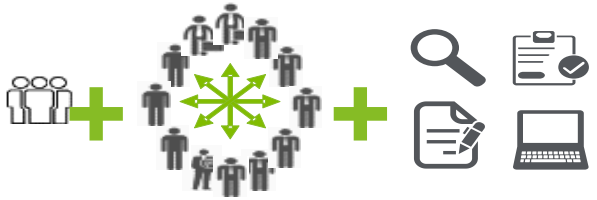
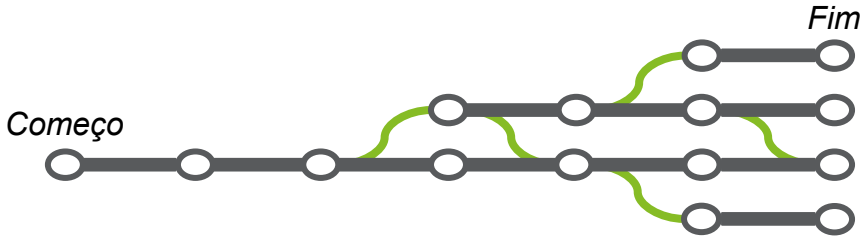
MTTC (Mean Time to Contain)

Tempo decorrido para que um analista aplique uma contenção especifica em um incidente, se necessário, em minutos

MTTR (Mean Time to Resolve)

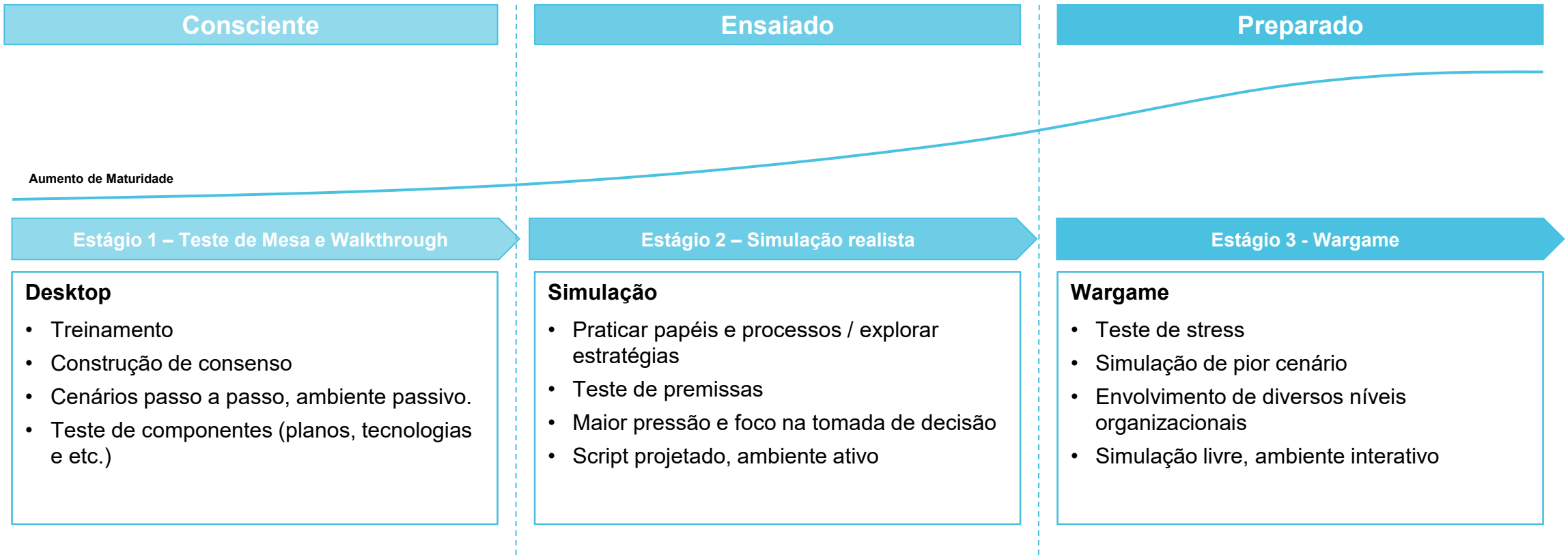
Tempo decorrido para que o analista finalize o tratamento do incidente, em minutos

Exemplos de Abordagem para Exercícios:

	Testes tradicionais	Simulações realistas
Estrutura do exercício	 Os jogadores participam de uma discussão teórica sobre as atividades de resposta a incidentes ou crises.	 Os jogadores, com o apoio de um facilitador, simulam a resposta a um incidente ou cenário de crise.
Progressão do exercício	 Os exercícios são de natureza estática - a progressão de cenários é planejada antecipadamente.	 Os exercícios são dinâmicos - a progressão de cenários baseia-se nas ações e decisões dos jogadores.

Os simulados realistas são mais dinâmicos do que as simulações tradicionais, resultando em maior envolvimento dos participantes e aprendizado com os resultados.

Os exercícios devem ser realizados conforme a maturidade da instituição no tema de segurança da informação e resposta a incidentes. Na tabela a seguir são apresentados os estágios dos exercícios, bem como sua respectiva dinâmica de orquestração:



Considerações Finais

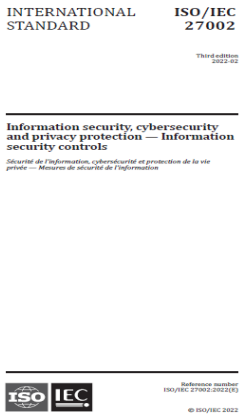
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Frameworks e Normas de Referência

Para apoiar no entendimento e implementação de toda a metodologia apresentada neste material, a seguir são apresentados as normas e frameworks de referência no tema:

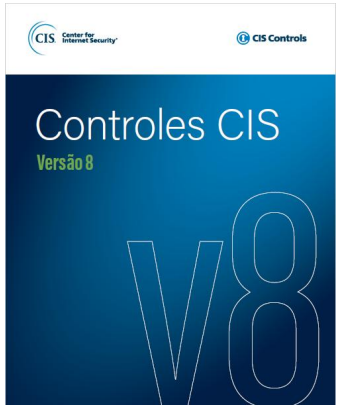
Frameworks Padrão Utilizados

NIST
National Institute of Standards and Technology



MITRE

PCI DSS COMPLIANT



Conformidade: Dado o uso extensivo de padrões amplamente aceitos pela indústria, a gestão dos incidentes de segurança deve ser alinhada com alguns dos requisitos de conformidade mais exigentes, permitindo estimar o nível de conformidade com PCI-DSS, LGPD, Bacen 4.893, SOX, NIST, entre outros.

Relembrando os principais conceitos

FEBRABAN

Agora que aprendemos sobre as atividades relacionadas ao processo de gestão de incidentes, relembre os principais termos e conceitos apresentados neste material:

Gestão de Incidentes: o objetivo da gestão de incidentes é assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação. Esse processo fornece uma abordagem padronizada e organizada para lidar com incidentes de segurança da informação.

SOC: O SOC (Security Operations Center) é um time interno ou terceirizado de profissionais de segurança de TI que monitoram toda a infraestrutura de TI da Organização, em formato 24/7 (24h nos 7 dias da semana), para detectar eventos de segurança cibernética em tempo real e resolvê-los da maneira mais rápida e eficiente possível.

Eventos: Qualquer ocorrência observável em um sistema ou rede. As fontes de log de sistemas individuais, dispositivos de rede ou qualquer outro, conterão eventos.

Incidentes: Violação de uma política ou controle de segurança explícito ou implícito, com capacidade de comprometer toda uma infraestrutura interna.

Módulo: Privacidade

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Requisitos – Privacidade

FEBRABAN

Este material foi elaborado de acordo com as exigências da LGPD, bem como foram considerados os requisitos de privacidade e segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

LGPD

- Artigos da Lei.

ISO 27701

- 7.1 Geral
- 7.2 Condições para coleta e tratamento
- 7.3 Obrigações dos titulares de DP
- 7.4 Privacy by Design e Privacy by Default
- 7.5 Compartilhamento, transferência e divulgação de DP

CIS Controls

- 3.3 Configurar listas de controle de acesso a dados
- 3.4 Aplicar retenção de dados
- 3.7 Estabelecer e manter um esquema de classificação de dados
- 3.13 Implantar uma solução de prevenção contra perda de dados
- 3.14 Registrar o acesso a dados sensíveis

ISO 27002

- 5.34 Privacidade e proteção de PII

NIST CSF

- GV. OC-03: Os requisitos legais, regulamentares e contratuais relativos à segurança cibernética - incluindo obrigações de privacidade e liberdades civis - são compreendidos e gerenciados

Sumário

Visão Geral

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Leis de Privacidade

De acordo com o

DLA Piper,

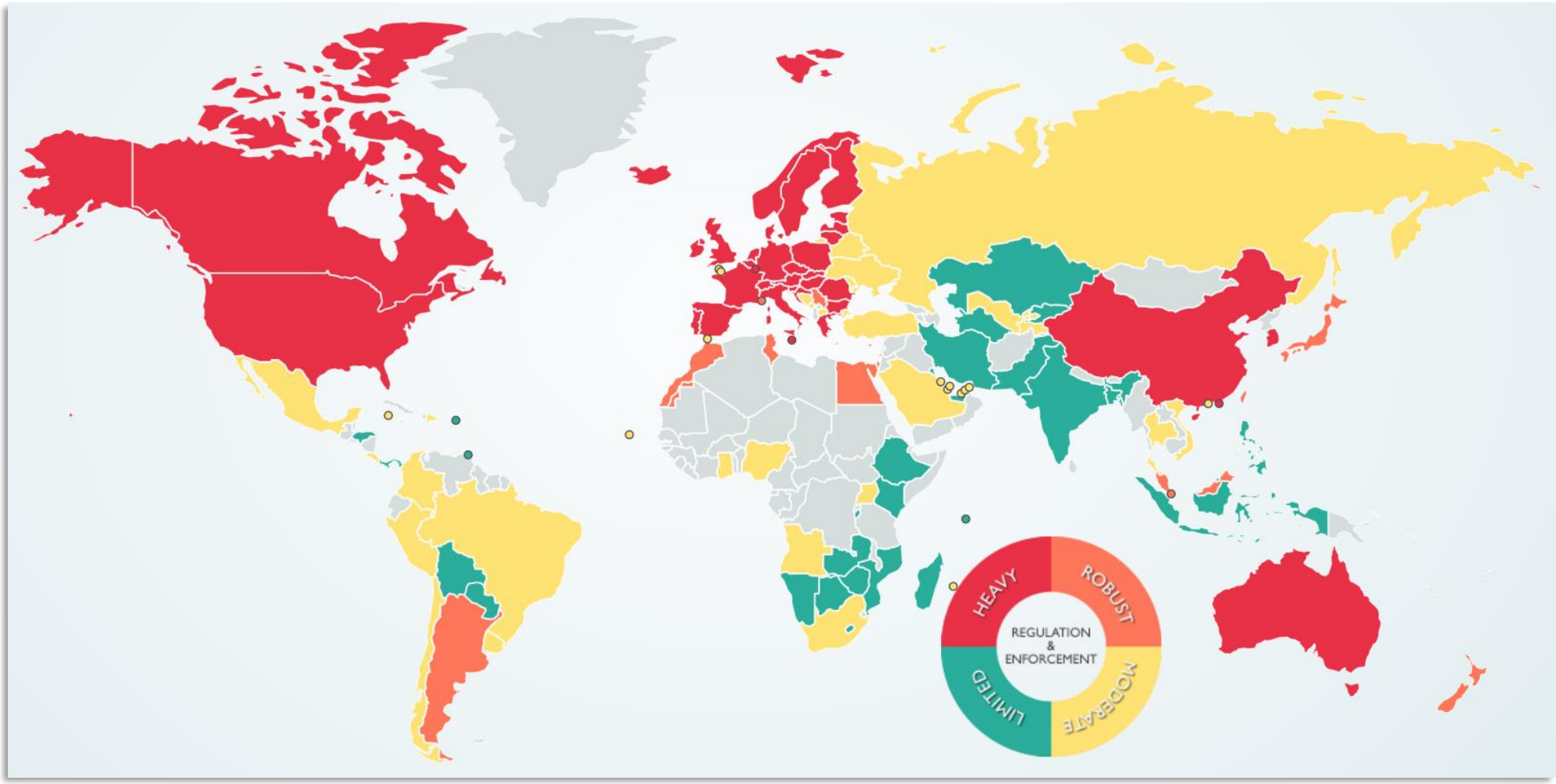
mais de **100**

países no **mundo**

possuem leis de

Privacidade e

Proteção de Dados Pessoais

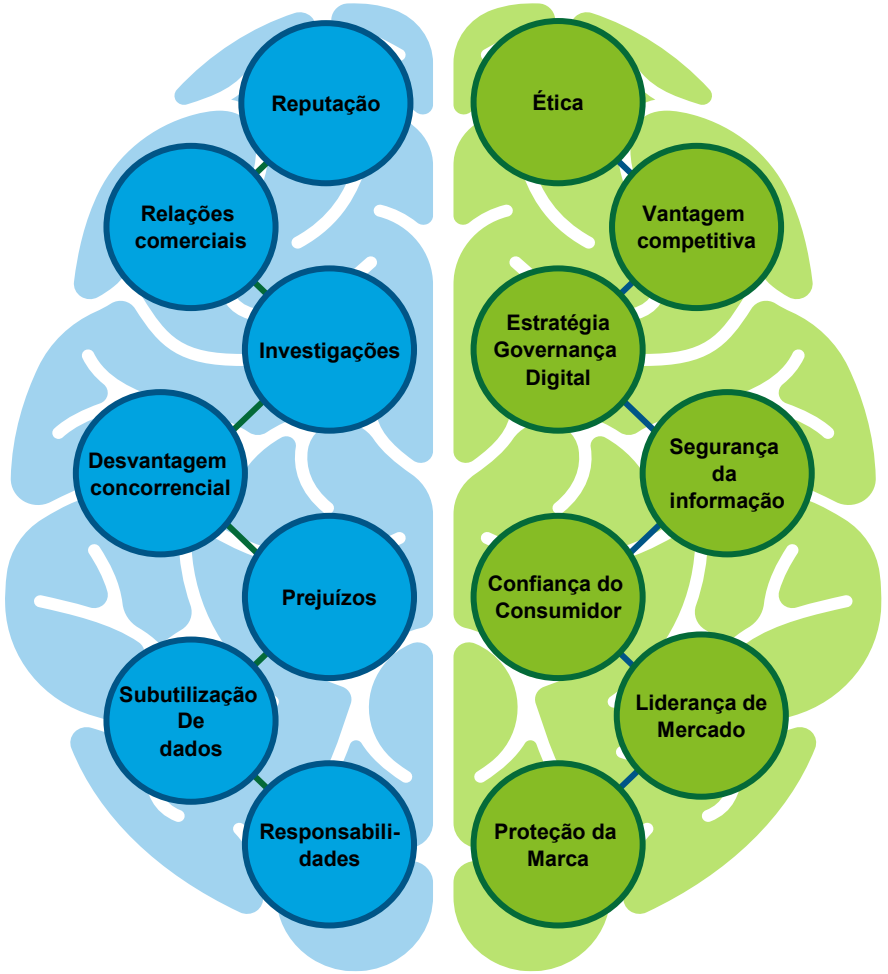


Fonte: DLA Piper – Data Protection Laws Around the World

Riscos e Oportunidades

Riscos

- Aplicação de penalidades pela ANPD
- Danos reputacionais e reflexos nas relações comerciais
- Prejuízos advindos da instauração de investigações e ajuizamento de processos judiciais por titulares dos dados e órgãos públicos, como Ministério Público e Procon
- Desvantagem concorrencial, redução da confiança de parceiros comerciais e fornecedores e rescisão de contratos
- Subutilização de dados e perda do valor de mercado



Oportunidades

- Vantagem competitiva perante clientes, parceiros e fornecedores
- Aumento da transparência e maior confiança por parte dos clientes e outros terceiros interessados
- Aceleração no processo da digitalização e modernização da empresa
- Maior conhecimento e domínio dos dados disponíveis, podendo gerar oportunidades para geração de receita
- Fortalecimento das capacidades de segurança da informação

Principais Aspectos da Lei

Não se aplica a:

- Dados de Pessoas Jurídicas;
- Dados pessoais tratados para fins não econômicos;
- Dados utilizados para segurança pública;
- Dados para fins artísticos ou jornalísticos;
- Dados acadêmicos;
- Dados anonimizados.

O que diz a lei?

A **Lei Geral de Proteção de Dados Pessoais** (LGPD) dispõe sobre o tratamento de dados pessoais, nos meios físicos e digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado. É uma legislação que estabelece direitos a titulares de dados pessoais e obrigações aos agentes de tratamento com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural

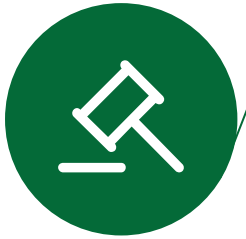
A quem se aplica?

- **Qualquer pessoa**, jurídica ou física, privada ou pública que realize **tratamento de dados**, para **fins comerciais**, com sede no Brasil;
- **Organizações** com **sede no exterior** que ofereçam **serviços** ou tenham **operações em território nacional,** envolvendo tratamento de dados;
- Dados pessoais **coletados em território nacional**.

Quais serão as sanções?

- **Multa** simples, de até **2% do faturamento**, limitada, a **R$50 MM** (cinquenta milhões de reais) por infração;
- **Multa diária**;
- **Divulgação** da infração;
- **Advertências;**
- **Suspensão das atividades de manipulação de dados;**
- **Bloqueio/eliminação dos dados pessoais**

Principais Obrigações?



- Nomear o Encarregado de Dados (DPO);
- Publicar a Política de Privacidade;
- Assegurar o Direito dos Titulares de Dados;
- Comunicação de Incidentes;
- Assegurar o sigilo e segurança dos dados; entre outros.

Termos e Definições

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Dados Pessoais

O conceito de tratamento de dados dentro da Lei Geral de Proteção de Dados Pessoais é amplo e considera todo o ciclo de vida do dado, englobando: **coleta, visualização, manipulação, transferência, arquivamento, descarte**, entre outros. Qualquer uso do dado pessoal será considerado como tratamento e, portanto, estará no escopo da legislação.

Informação relacionada a pessoa natural identificada ou identificável, ou seja, é a informação ou conjunto de informações distintas que possam levar à identificação de uma pessoa de forma direta ou indireta.

Informações relativas a pessoas jurídicas como CNPJ e razão social não são consideradas dados pessoais.

Exemplos

Nome e número de documentos

Telefones para contato

IP, MSISDN

E-mail

Endereço residencial

Geolocalização

Perfil Comportamental

Dados Pessoais Sensíveis

O conceito de tratamento de dados dentro da Lei Geral de Proteção de Dados Pessoais é amplo e considera todo o ciclo de vida do dado, englobando: **coleta, visualização, manipulação, transferência, arquivamento, descarte**, entre outros. Qualquer uso do dado pessoal será considerado como tratamento e, portanto, estará no escopo da legislação.

São dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Obs.: Por seu potencial discriminatório, dados pessoais sensíveis possuem maior cobertura da LGPD e, por isso, a atenção na coleta e tratamento deve ser redobrada.

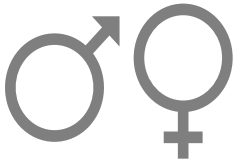
Exemplos

Saúde

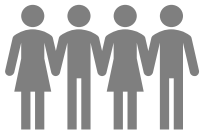
Opinião Política

Genético ou biométrico

Convicção religiosa



Relativos à vida sexual



Raça ou etnia

Filiação a sindicato ou organização religiosa, filosófica ou política

Princípios da LGPD

FEBRABAN

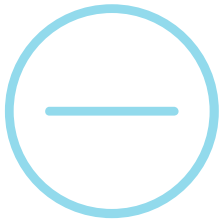
O Art. 6º da LGPD menciona que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes **princípios**:

Transparência

Informar no contrato de trabalho de todos os profissionais os cenários em que seus dados pessoais poderão ser tratados.

Finalidade

Todos os dados coletados precisam ter um propósito que justifique a coleta. Solicitar a clientes dados pessoais sem qualquer justificativa/finalidade relacionada fere este princípio.



Necessidade

Recursar o recebimento de planilhas e arquivos que contenham dados pessoais que não são necessários para execução dos serviços contratados.

Responsabilização e prestação de contas

O RoPA e treinamentos de conscientização são formas de atendimento a esse princípio

Adequação

Não utilizar endereços de e-mail de clientes para finalidades distintas daquelas relacionadas a prestação dos serviços.

Princípios da LGPD

O Art. 6º da LGPD menciona que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes **princípios**:

Qualidade dos dados

Manter em seu banco de dados informações atualizadas, corretas e precisas.

Segurança

A aplicação de múltiplo fator de autenticação (MFA) para acessar uma plataforma e a inclusão de senhas em arquivos são medidas que atendem ao princípio da segurança.

Livre Acesso

Os dados pessoais devem ser armazenados de forma a facilitar seu acesso aos titulares.

Prevenção

Programar os e-mails para apenas saírem da caixa após determinado período é uma forma de prevenção de incidentes decorrentes de envios para destinatários incorretos.

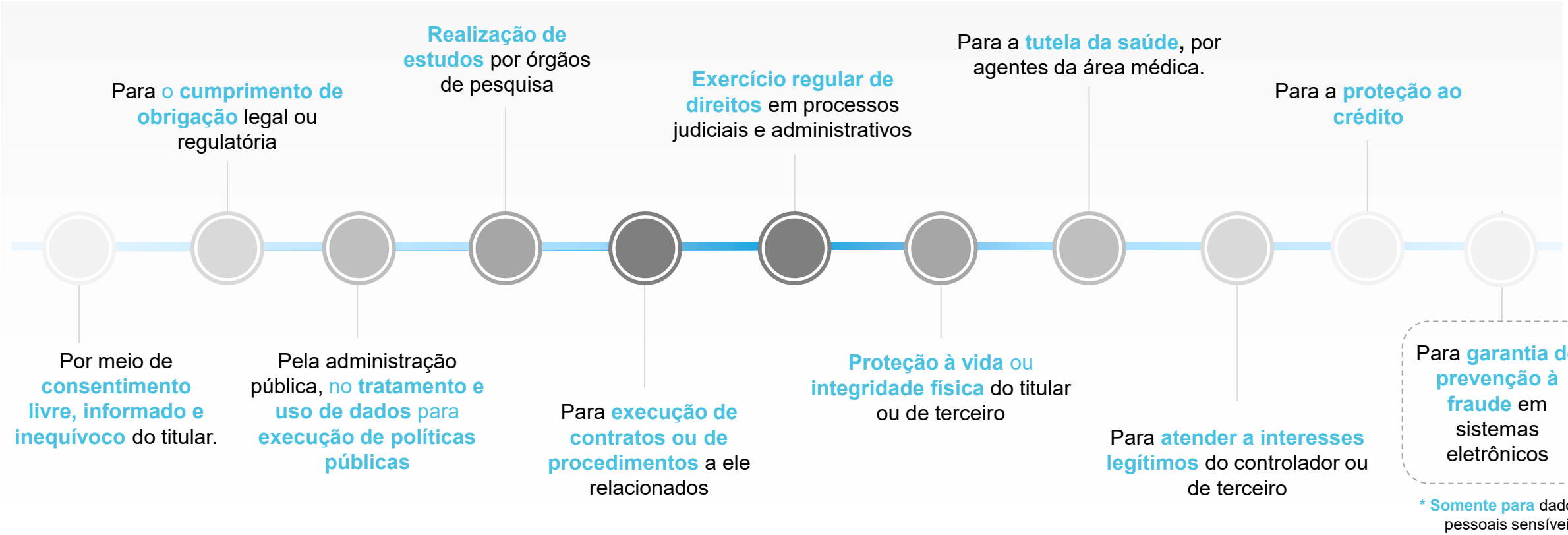
Não discriminação

Não utilizar eventual acesso a informações de orientação sexual de profissionais para aplicar medidas discriminatórias.

Bases legais para o tratamento de Dados Pessoais

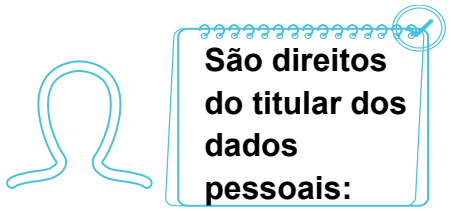
FEBRABAN

Cada **atividade de tratamento** está atrelada a uma **finalidade** e para cada finalidade é dever do Controlador apontar uma **base legal**:



** As hipóteses do **legítimo interesse e execução de contrato não se aplicam** para o tratamento de dados pessoais sensíveis!

Direitos dos Titulares



São direitos do titular dos dados pessoais:

- Confirmar a existência do tratamento
- Acessar os dados pessoais
- CorrIgir dados incompletos, inexatos ou desatualizados
- Anonimizar os dados pessoais
- Realizar a portabilidade de dados
- Eliminar os dados tratados com base em consentimento
- Obter informações de entidades públicas e privadas que secom quem os dados foram compartilhados
- Ser informado da possibilidade de não fornecer o consentimento
- Revogar o consentimento
- Revisão de decisões automatizadas e direito de se opor ao tratamento quando não tiver mais necessidade legítima ou legal de tratá-la

O Artigo 18 da LGPD dispõe sobre os direitos dos Titulares.

O Controlador deverá garantir o livre acesso, qualidade dos dados e a segurança dos dados.

O Controlador deverá respeitar a liberdade, intimidade e privacidade do titular.

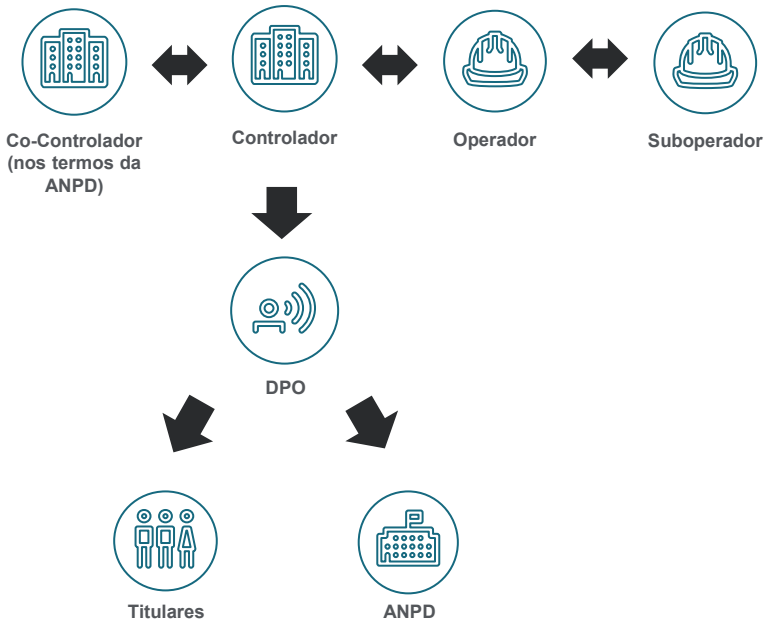
Principais Figuras

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Visão Geral

Titular do Dado

Pessoa natural relacionada ao dado objeto do tratamento.



Controlador

Entidade responsável pelas **decisões** no tratamento de dados pessoais, definindo **"O que?"** e **"como?"** os dados serão tratados.

Encarregado

Colaborador, área ou terceiro **representante do controlador e operador** que atuará como **canal de comunicação entre ele, titular e autoridade nacional.**

Operador

Entidade que **atua em nome** de um controlador e **não possui autonomia** para tomar decisões sobre a atividade de tratamento.

Autoridade Nacional de Proteção de Dados

Conhecida também por **ANPD**, é o órgão da administração pública responsável por **implementar** e **fiscalizar** o cumprimento da LGPD.

Agentes de Tratamento

Controlador

O Controlador é o agente que define a finalidade do tratamento, ou seja, indica o propósito para qual os dados pessoais serão tratados. É também quem define os meios de tratamento no que se refere aos elementos essenciais e não essenciais para o exercício de suas atividades.

Operador

A existência do Operador depende de uma decisão do Controlador, que pode optar por realizar as operações de tratamento de dados pessoais por si mesmo ou delegar a integralidade ou mesmo parte desse tratamento a terceiro que atuará como Operador.

Controlador

TEM o poder de decisão para iniciar o tratamento

DEFINE a finalidade do tratamento

Define os meios de tratamento:
- Elementos essenciais
- Elementos não essenciais

Operador

SEM o poder de decisão para iniciar o tratamento

NÃO determina a finalidade do tratamento

Define os meios de tratamento:
- ~~Elementos essenciais~~
- Elementos não essenciais

Agentes de Tratamento

Instituições - Controlador

Exemplos

- Tratamento de dados pessoais de profissionais das Instituições (pesquisas internas, dados financeiros para pagamento de salário, dados para e-social, atendimento ambulatorial, entre outros);
- Envios de e-mail marketing para potenciais clientes;
- Prestação de serviços financeiros;
- Prestação de serviços de Auditoria.

Terceiros - Operador

Exemplos

- Prestação de serviços de pocessamento de folha de pagamento;
- Prestação de serviços de call center;
- Prestação de serviços de suporte técnico e implementação de ferramentas;
- Prestação de serviços para geração de leads;

ANPD

A Autoridade Nacional de Proteção de Dados (ANPD) é um órgão da administração pública, integrante da Presidência da República, **responsável por zelar, implementar e fiscalizar o cumprimento da LGPD** em todo o território nacional.

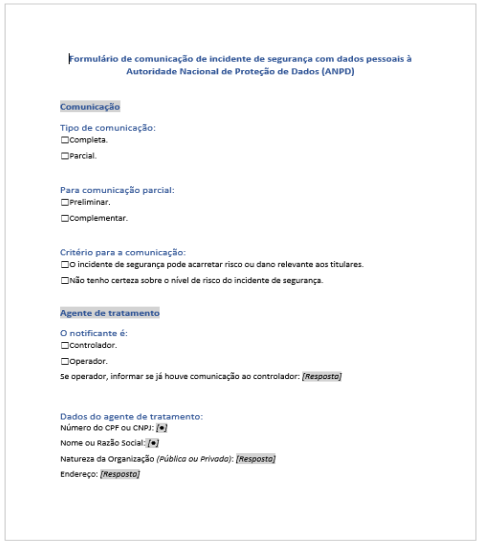
Medidas já adotadas pela ANPD

- Sítio eletrônico para publicação de informações e comunicação com a sociedade;
- Tomada de subsídios sobre alguns temas como notificação de incidentes e LGPD;
- Canal para reporte de incidentes;
- Guias e recomendações;
- Audiências Públicas;
- Assinatura de acordos com outros órgãos, entre outros.

Publicações

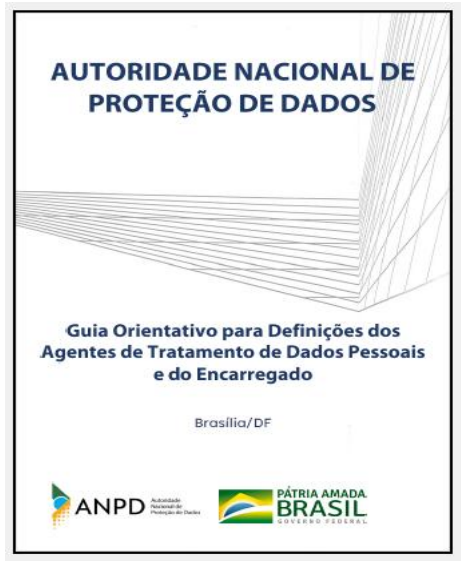
***Planejamento Estratégico** 2021-2023 e **Agenda Regulatória** 2021-2022*

Fonte: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/planejamento-estrategico/planejamento-estrategico-2021-2023.pdf



Orientações sobre reporte de incidentes e sanções administrativas

Fonte: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

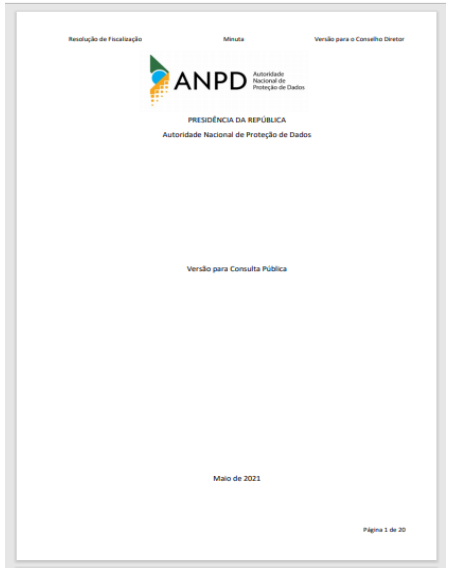


Guia Orientativo sobre Agentes de Tratamento e Encarregado de Dados

Fonte: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf

***Cartilha de Segurança** para Internet em parceria com a NIC*

Fonte: https://cartilha.cert.br/fasciculos/protecao-de-dados/fasciculo-protecao-de-dados.pdf



***- Tomadas de subsídios -** regulamentação em micro e pequenas empresas e notificação de incidentes*

Fonte: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-consulta-publica-sobre-norma-de-fiscalizacao/2021.05.29___Minuta_de_Resolucao_de_fiscalizacao_para_consultapblica.pdf

Programa de Privacidade

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Programa de Privacidade

A seguir são apresentadas alguns exemplos de atividades que fazem parte de um programa de privacidade:

01

Direito dos Titulares

O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: confirmação de tratamento, acesso, correção, descarte dos dados, etc.

02

Mapeamento de Dados Pessoais (RoPA)

O RoPA é o inventário de dados e contém o mapeamento de todos os dados pessoais dos processos da Organização.

03

Consentimento

Documento que formaliza o “de acordo” do titular para o tratamento de seus dados pessoais para uma finalidade determinada.

04

Comunicação de Incidentes

O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

05

Relatório de Impacto

Necessário para processos com maiores riscos de impacto à proteção dos dados pessoais e contém planos de mitigação.

06

Política de Privacidade

Documento que especifica como uma empresa coleta, usa e armazena as informações pessoais dos seus clientes e usuários. Ela também é chamada de Termos de Privacidade.

Comunicação de Incidentes de Privacidade

FEBRABAN

Conforme o Art. 6º e o Art. 9º da Resolução CD/ANPD nº 15, de 24 de abril de 2024 que Aprova o Regulamento de Comunicação de Incidente de Segurança, **a comunicação à ANPD e aos titulares deverá ser realizada pelo controlador no prazo de três (3) dias úteis**, ressalvada a existência de prazo para comunicação previsto em legislação específica.

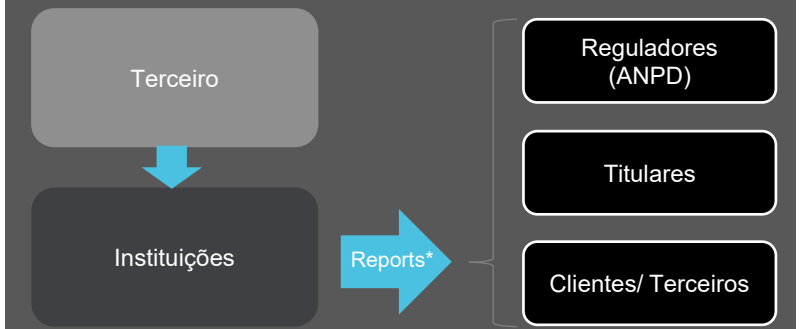
A comunicação voluntária do incidente pelo controlador é demonstração de transparência, cooperação e boa-fé do agente e será considerada em eventual ação de fiscalização da ANPD.

Exemplos: Tipos de Incidentes e Modelos de Comunicação

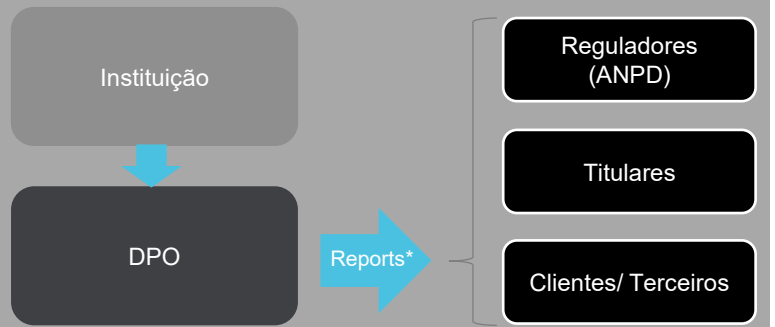
Principais Tipos de incidentes

- Envio de um e-mail contendo dados pessoais a um destinatário errado
- Perda/furto do computador com informações de dados pessoais
- Phishing/Malwares
- Softwares não homologados instalados na máquina
- Engenharia Social
- Ransomware

Modelo de Report para Operador



Modelo de Report para Controlador



Exemplos - Incidentes de Privacidade

	Cenário A	Cenário B
O que aconteceu	O profissional enviou um e-mail equivocadamente a um indivíduo de outra empresa com nome similar. O e-mail expôs dados pessoais dos clientes titulares de planos de previdência, como nome, CPF e valores de pagamento do benefício.	O profissional equivocadamente substituiu um template em branco em um sistema (que fica à disposição de todos os usuários para download) por um formulário preenchido com dados pessoais de funcionários de terceiros do cliente, como nome, previdência social número e salário.
O que deu errado?	O compartilhamento de dados confidenciais e privados ocorreu por e-mail e não via ferramenta homologada da Organização para essa finalidade.	Falha no monitoramento/ revisão das mudanças realizadas no sistema.
Qual a exposição?	- Número significativo de horas (executivos) na preparação de relatório de incidente robusto; - Risco de exposição a terceiros e / ou divulgação do incidente (comunicar ao regulador). - Impacto no relacionamento com o cliente (perda de credibilidade).	

Notificação de incidentes de privacidade: Está disponível no site da ANPD formulários para a elaboração das comunicações quando há incidentes envolvendo titulares de dados pessoais, as **comunicações devem ocorrer em até 3 dias úteis após a confirmação do incidente**, conforme definido na Lei.

RoPA (*Record of Processing Activities*)

O controlador e o operador devem manter **registro atualizado das operações de tratamento de dados pessoais que realizarem**. A seguir é apresentado alguns exemplos de informações que devem ser consideradas na construção do RoPA.

Para cumprir os requisitos de tratamento de dados da LGPD é necessário entender completamente quais dados são tratados e como este tratamento é feito.

Política de Privacidade

A LGPD, apresenta as definições e critérios esperados, para segurança e privacidade de dados e informações.

Política de Privacidade

ONDE POSSO ENCONTRAR ESTE TEMA NA LGPD?
Arts. 7º, 40º, 46º, 47º, 48º e 49º

Política de Privacidade

- **Refletir** os **tratamentos de dados pessoais** que são feitos pela organização em seus serviços, sites, portais e aplicativos.
- Instrumento de implementação do ***Privacy by Design*** e faz parte da estrutura de documentos para a **proteção de dados**.
- Objetiva dar **visibilidade** ao tratamento de dados pessoais em um determinado processo, atendendo aos **princípios** da LGPD.
- Endereçado aos **Titulares de dados** (usuários de sites, portais e aplicativos) de forma **pública, clara e precisa**.

Conteúdo da Política de Privacidade

- Informações sobre a **organização** responsável pelo tratamento;
- **Dados pessoais** e respectivas **finalidades** do tratamento, inclusive os dados não informados pelo titular (IP, localização, etc);
- **Base jurídica** do tratamento;
- Prazo de **retenção** dos dados pessoais;
- Informações de **contato do DPO** (*Data Protection Officer*) ou encarregado de proteção de dados da organização;
- Orientação para atendimento aos **Direitos dos titulares** de dados pessoais, bem como a indicação dos **canais apropriados para as solicitações**;
- Compartilhamento de dados com **terceiros** e suas finalidades;
- **Transferência internacional** e suas finalidades;
- Tratamento por **legítimo interesse** (caso aplicável);
- **Decisões automatizadas** e a possibilidade de revisa-las (caso aplicável);
- Proteção de **dados de menores**.

Mascaramento de Dados

FEBRABAN

Segundo a ISO 27002, o **mascaramento de dados** deve ser usado de acordo com a política de acesso específica do tópico da organização controle e outras políticas específicas de tópicos relacionados e requisitos de negócios, considerando legislação em consideração. Ele é usado para limitar a exposição de dados sensíveis, incluindo PII, e para cumprir as normas legais, estatutárias, regulamentares e requisitos contratuais.

Anonimização

Descrição: Processo que remove todos os identificadores do titular dos dados, ou seja, após a anonimização, não se poderá mais associar os dados a uma pessoa específica. Portanto, a partir do momento em que anonimiza-se um dado e deixa de ser um dado pessoal, torna-se impossível vincular quem é a pessoa a ele relacionada.

Caso de Uso: dados anonimizados são essenciais para o crescimento da inteligência artificial, da internet das coisas, do aprendizado das máquinas, das cidades Inteligentes, da análise de comportamentos, entre outros.

Pseudononimização

Descrição: Processo de substituição dos identificadores do titular dos dados por um código ou apelido. Esses identificadores são mantidos em separado em ambiente seguro, de forma que não possam ser associados a uma pessoa específica sem acesso a eles.

Caso de uso: análise de dados e marketing

Art. 12 - ”Os dados anonimizados **não** serão considerados dados pessoais para os fins **desta Lei**, salvo quando o processo de anonimização ao qual foram submetidos for **revertido**, utilizando exclusivamente meios próprios, ou quando, com **esforços razoáveis**, puder ser revertido.”

Link – Material de Apoio

O que mais você precisa saber?

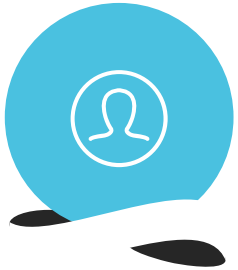
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

O que mais você precisa saber?

A seguir são apresentadas algumas dicas que podem ser seguidas no dia a dia e contribuem para o atendimento as exigências da Lei:

Use as Ferramentas Homologadas

Evite o compartilhamento de dados por e-mail e não armazene-os no seu notebook.



Aceite apenas os dados necessários

Devolva e exclua aqueles que não são necessários para as suas atividades.

Trate dados conforme finalidade da coleta

Os dados não podem ser aproveitados para finalidades distintas.

Restrinja o acesso aos dados

Atente-se aos destinatários dos e-mails e aos usuários aos quais concede acesso em ferramentas.

Cuidados ao enviar por e-mail

Classifique os dados, configure, configure o envio tardio de e-mail e inative o preenchimento automático.

Módulo: Proteção de Dados

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Requisitos – Proteção de dados

FEBRABAN

Este material foi elaborado de acordo com as diretrizes do PCI DSS e CIS Controls, bem como foram considerados os requisitos de segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

PCI DSS

- 3.1 Os processos e mecanismos para proteger os dados da conta armazenados são definidos e compreendidos.
- 3.2 O armazenamento de dados da conta é mínimo.
- 3.3 Os dados de autenticação confidenciais (SAD) não são armazenados após a autorização.
- 3.4 O acesso a exibição de PAN completo e a capacidade de copiar os dados do titular do cartão são restritos.
- 3.5 O número da conta principal (PAN) é protegido onde quer que seja armazenado.
- 3.6 As chaves criptográficas usadas para proteger os dados da conta armazenados são protegidas.
- 3.7 Onde a criptografia é usada para proteger os dados da conta armazenados, os processos e procedimentos de gerenciamento de chave cobrindo todos os aspectos do ciclo de vida da chave são definidos e implementados.
- 4.1 Processos e mecanismos para proteger os dados do titular do cartão com criptografia forte durante a transmissão em redes públicas abertas são definidos e documentados.
- 4.2 O PAN é protegido com criptografia forte durante a transmissão.
- 9.4.2 Todas as mídias com dados do titular do cartão são classificadas de acordo com a confidencialidade dos dados.

CIS Controls

- 3.1 Estabelecer e manter um processo de gestão de dados
- 3.2 Estabelecer e manter um inventário de dados
- 3.3 Configurar listas de controle de acesso a dados
- 3.4 Aplicar retenção de dados
- 3.5 Descartar dados com segurança
- 3.6 Criptografar dados em dispositivos de usuário final
- 3.8 Documentar Fluxos de Dados
- 3.7 Estabelecer e manter um esquema de classificação de dados
- 3.9 Criptografar dados em mídia removível
- 3.10 Criptografar dados sensíveis em trânsito
- 3.11 Criptografar dados sensíveis em repouso
- 3.12 Segmentar o processamento e o armazenamento de dados com base na sensibilidade
- 3.13 Implantar uma solução de prevenção contra perda de dados
- 3.14 Registrar o acesso a dados sensíveis

ISO 27002

- 5.33 Proteção de registros
- 5.35 Revisão independente da segurança da informação
- 5.36 Conformidade com políticas, regras e padrões para segurança da informação
- 8.15 Registro
- 8.16 Atividades de monitoramento
- 8.17 Sincronização de relógio
- 8.34 Proteção de sistemas de informação durante testes de auditoria

ISO 27701

- 6.5.1.1 Inventário dos ativos
- 6.5.2.1 Classificação da informação
- 6.5.2.2 Rótulos e tratamento da informação
- 6.5.2.3 Tratamento dos ativos
- 6.5.3.2 Descarte de mídias
- 6.7.1 Controles criptográficos
- 6.7.1.2 Gerenciamento de chaves
- 7.4.7 Retenção
- 7.4.8 Descarte

NIST CSF

- ID.AM-06: Os inventários de dados e metadados correspondentes para tipos de dados designados são mantidos
- ID.AM-08: Sistemas, hardware, software, serviços e dados são gerenciados ao longo de seus ciclos de vida
- PR.DS-01: A confidencialidade, integridade e disponibilidade dos dados em repouso são protegidas
- PR.DS-02: A confidencialidade, integridade e disponibilidade dos dados em trânsito são protegidas
- PR.DS-03: A confidencialidade, integridade e disponibilidade dos dados em uso são protegidas
- PR.PS-03: O hardware é mantido, substituído e removido proporcionalmente ao risco
- PR.PS-05: Instalação e execução de software não autorizado são impedidas

Sumário

Contexto

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Introdução

Segundo o CIS Controls, os dados não estão mais apenas dentro da fronteira da empresa; **estão na nuvem, ambientes on-premisses, em dispositivos portáteis, onde os usuários trabalham, e geralmente são compartilhados com parceiros ou serviços online** que podem tê-los em qualquer lugar no mundo. Com os dados cada vez mais expostos, a ISO 27002 coloca que **os dados devem ser protegidos contra perda, destruição, falsificação e acesso não autorizado**.

Como proteger os dados?

A **criptografia** é utilizada para converter caracteres de texto comum para um formato não legível, as chaves de criptografia **embaralham os dados** para que somente usuários **autorizados** possam lê-los.

A **segmentação** separa os controles de segurança da infraestrutura subjacente e permite às organizações a flexibilidade para **estender a proteção e a visibilidade em qualquer lugar**.

Controle de acesso aos **dados** com base na **necessidade** de acesso do usuário (privilégio mínimo).

Gestão de dados para tratar a **sensibilidade** dos dados, o proprietário dos dados, o **manuseio** dos dados, os limites de **retenção** de dados e os requisitos de **descarte.**

Descarte os dados com **segurança** para minimizar o risco de **vazamento de informações sensíveis** para pessoas **não autorizadas**.

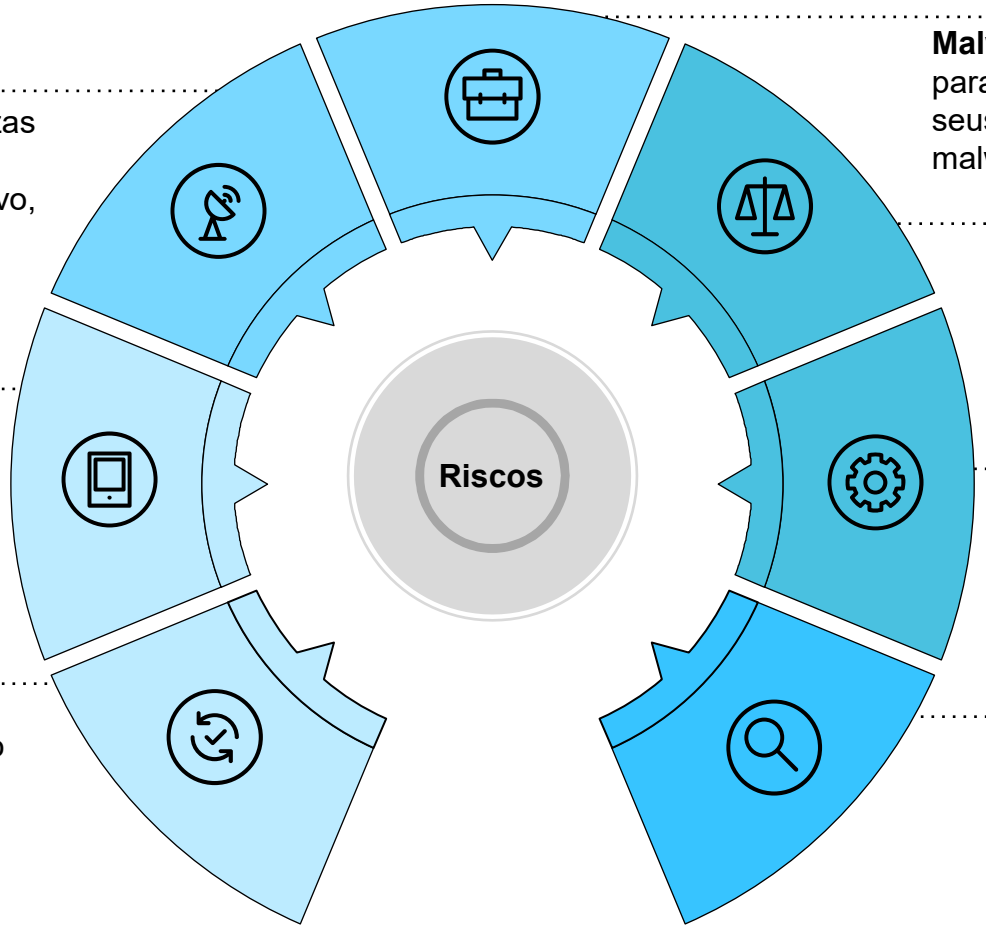
Principais Ameaças aos Dados

As ameaças visam a **interceptação ou roubo de informações privilegiadas**, danificando desta forma a segurança do ambiente tecnológico e impactando os pilares da Segurança da Informação, ou seja, a **integridade, disponibilidade e confidencialidade**. A seguir são apresentados alguns exemplos de ameaças cibernéticas:

Vulnerabilidades de segurança: fraquezas ou falhas na estrutura, código ou implementação de um aplicativo, dispositivo, rede ou outro ativo de TI que os hackers podem explorar.

Credenciais fracas ou roubadas: senhas que os hackers podem adivinhar facilmente ou senhas ou outras credenciais.

Ameaças internas: usuários autorizados que colocam dados em risco por descuido ou intenção maliciosa.



Malware: software criado especificamente para prejudicar um sistema de computador ou seus usuários. A forma mais conhecida de malware que ameaça dados é o ransomware.

Engenharia social: táticas de manipulação de pessoas para a execução de ações ou para a divulgação de informações confidenciais.

Roubo de dispositivo físico: roubo de um laptop, smartphone ou outro dispositivo que concede ao ladrão acesso à rede e permissão para acessar dados.

Negligência: as violações geralmente ocorrem devido à negligência de um funcionário ou de outra parte.

Ransomware

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Malwares - Ransomware

Segundo o CIS Controls, os malwares podem ter várias finalidades, desde **capturar credenciais, roubar dados, identificar outros alvos na rede e criptografar ou destruir dados**.

O que é um ransomware?

- **Ransomware** é um tipo de malware projetado para criptografar e ou extrair dados de áreas de armazenamento de computadores e servidores, tornando os dados inacessíveis até que um resgate seja pago. Os dados de sistema da vítima **são bloqueados e o hacker exige uma taxa de resgate**, normalmente vinculando o pagamento a uma moeda virtual como o Bitcoin, prometendo liberar o acesso aos dados após a realização do pagamento.

- Apesar do Ransomware também ser um malware *(código malicioso),* ele pode ou não possuir a capacidade de auto-replicação de um vírus ***(isso vai depender da variante em atuação).*** Enquanto a propagação de um vírus acontece de forma espontânea e sem controle, o Ransomware é distribuído via internet e ou inserido por um atacante nos computadores e servidores através da exploração de vulnerabilidades encontradas nos sistemas operacionais.

Tipos de ransomware

- O ransomware Diskcoder criptografa o disco completo e faz com o que usuário não consiga acessar o sistema operacional.
- O Screen locker bloqueia o acesso a tela do dispositivo.
- O Crypto-ransomware criptografa dados armazenados no disco da vítima.
- O PIN locker tem como alvo os dispositivos Android e muda seus códigos de acesso para bloquear seus usuários.
- O WannaCryptorakaWannaCry tem como alvo explorar vulnerabilidade nas versões mais populares dos sistemas operacionais Windows.
- O Petya tem como alvo explorar vulnerabilidade de softwares de contabilidade populares.
- O Ryuk é um cavalo de Troia de criptografia ele desabilita funções de recuperação dos sistemas operacionais Windows.
- O B0r0nt0k é um ransomware de criptografia que se concentra especificamente em servidores Windows e Linux. Este nocivo ransomware criptografa os arquivos de um servidor Linux e anexa a extensão de arquivo ".rontok".
- O Ransomware Dharma Brrr o novo ransomware Dharma, é instalado manualmente
  por hackers que invadem os serviços de desktop conectados à Internet.
  Assim que o ransomware é ativado pelo hacker, ele começa a criptografar os arquivos encontrados. Os dados criptografados recebem **a extensão ".id-[id].[email].brrr".** Este ransomware possui variantes e tem o mesmo comportamento em servidores.

Ransomware - Modo de Operação

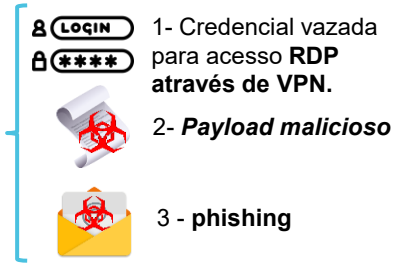
FEBRABAN

Como funciona o ataque?

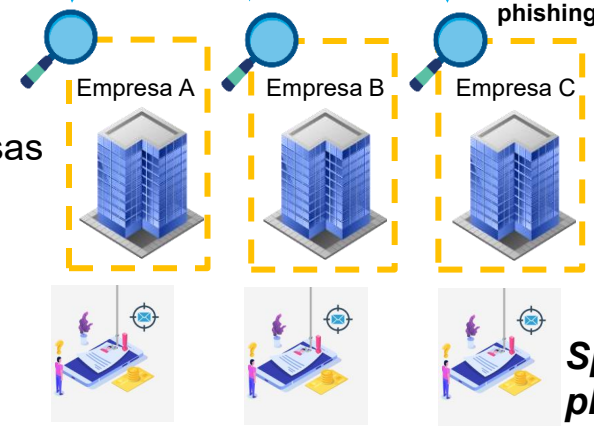
1- Atacante prepara um malware (**ransomware) com alvo específico** através de uma variante

Internet

2- Atacante escolhe tipos de vetores de ataque.



3- Após escolher o vetor de ataque e direcioná-lo, entra em ação as variantes ex: **spear phishing**



Empresas Alvo

Alvos

Spear phishing;

1º Modelo de comprometimento

1 Firewall (VPN)

1- Comprometimento do DNS
- Acesso remeto via protocolo RDP;
- Uso de credencial autorizada (DEEP Web);
- Controle do servidor ou desktop por usuário ADM;
- Infiltração do malware e instalação de código malicioso.

2 Usuários

2- Comprometimento da máquina do usuário
- Instalação de artefato malicioso nos desktops;
- Propagação do malware para o controlador de domínio através da **técnica de spyware**;
- Comprometimento das credencias administrativas;
- Execução criptografia das máquinas.

3 Aplicações

3- Comprometimento da máquina VMware
- Exploração da vulnerabilidade;
- Instalação do artefato malicioso no servidor por programa com lista direcionadora;
- Propagação do malware para o controlador de domínio através da **técnica de spyware;**
- Comprometimento das credencias administrativas;
- Execução criptografia das máquinas;
- Exclusão de comandos de SO para dificultar a recuperação.

4 Alvos principal

AD/LDAP

1- Comprometimento das credencias administrativas do domínio;
2- Execução de ataque lateral;
3- Proliferação do artefato malicioso e criptografia de dados pré-definhada.

Comprometimento do ambiente

Ransomware - Modo de Operação

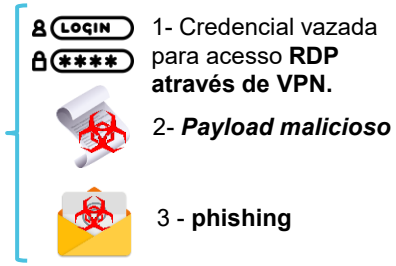
FEBRABAN

Como funciona o ataque?

1- Atacante prepara um malware (**ransomware) com alvo específico** através de uma variante

Internet

2- Atacante escolhe tipos de vetores de ataque.



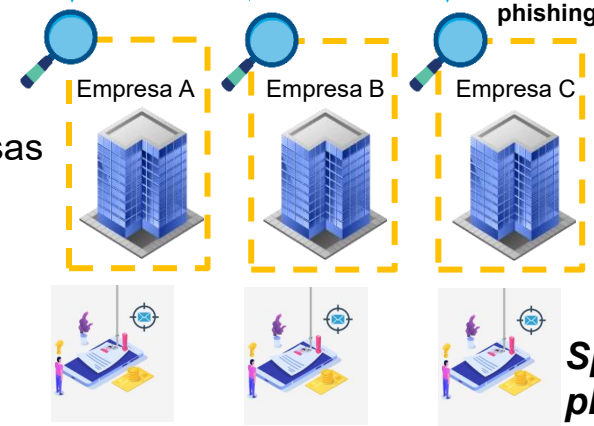
1- Credencial vazada para acesso **RDP através de VPN.**

2- ***Payload malicioso***

3 - **phishing**

3- Após escolher o vetor de ataque e direcioná-lo, entra em ação as variantes ex: **spear phishing**

Empresas Alvo



Alvos

Spear phishing;

2º Modelo de comprometimento

1 Aplicações

1- Comprometimento da aplicação
- Roubo de credencial;
- Sequestro da máquina;
- Criptografia de arquivos específicos do negócio;
- Pagamento de resgate;
- Extração de dados.

2 Banco de dados

2- Comprometimento da banco de dados
- Roubo de credencial;
- Sequestro da máquina;
- Criptografia de arquivos específicos do negócio;
- Pagamento de resgate;
- Extração de dados.

3 Legado

3- Comprometimento da banco de dados
- Roubo de credencial;
- Sequestro da máquina;
- Criptografia de arquivos específicos do negócio;
- Pagamento de resgate;
- Extração de dados.

Preservar

4 backup

1- Restore de dados;

2- Preservação e reestruturação dos dados e dos ambientes de produção.

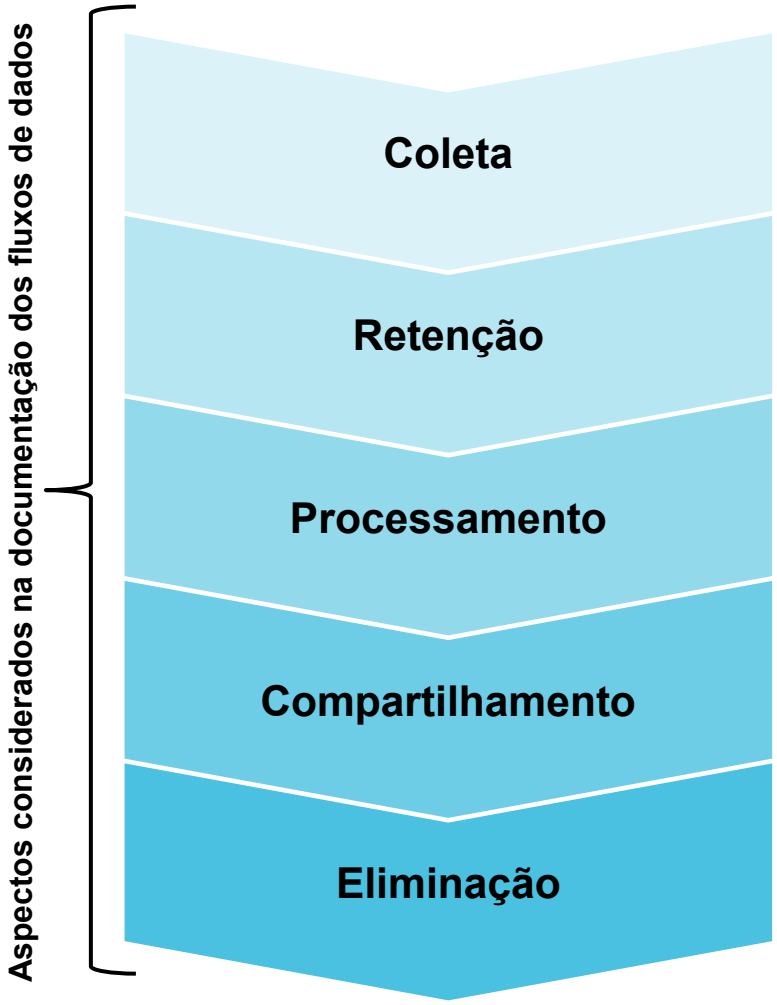
Comprometimento do ambiente

Práticas de
Proteção aos dados

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Gestão de Dados

Segundo o CIS Controls, é necessário estabelecer e manter um processo de gestão de dados. Esse processo **deve tratar sobre sensibilidade dos dados, o proprietário dos dados, o manuseio dos dados, os limites de retenção de dados e os requisitos de descarte**, com base em padrões de sensibilidade e retenção.



- Obtenção, recepção ou produção de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, sistema de informação, etc.).
- Qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais
- Qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais.
- Qualquer operação que envolva transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais.
- Qualquer operação que visa apagar ou eliminar dados pessoais. Esta fase também contempla descarte dos ativos organizacionais nos casos necessários ao negócio da instituição.

Controle de Acesso aos Dados

FEBRABAN

Segundo o CIS Controls, é necessário **aplicar listas de controle de acesso a dados**, também conhecidas como **permissões de acesso, a sistemas de arquivos, bancos de dados e aplicações locais e remotos**.

A gestão de acesso aos dados permite:

Gerenciamento de credenciais de identidade atribuídas a funcionários, contratados, fornecedores e clientes.

O **controle de acesso aos dados** autoriza com base na necessidade que apenas os usuários autorizados tenham **permissão para consultar, escrever e excluir os dados**.

Processos, incluindo **funções** e **responsabilidades**, estrutura organizacional e procedimentos administrativos.

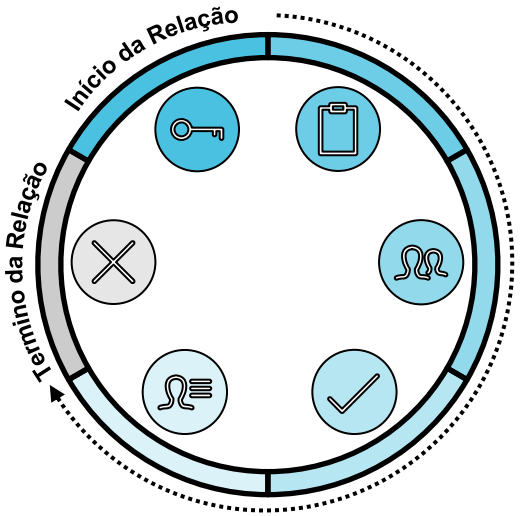
Informações, incluindo **políticas de gerenciamento** de riscos, **controles**, fluxos de informações e relatórios.

É importante ter um **registro dos acessos** aos dados sensíveis, onde inclui as **modificações** e **descartes** realizados.

1. Nova Identidade
Estabelecer uma nova relação com uma identidade

6. Revogar Acesso
Remover o acesso quando um relacionamento se encerra

5. Gerenciar Acesso
Atualizar o acesso conforme a evolução da relação



2. Comprovar
Comprovar que a pessoa ou coisa por trás da identidade é verdadeira

3. Verificar
Autenticar a identidade para transações futuras

4. Registrar
Registrar a identidade nos serviços com base no valor da relação

Ferramentas que podem ser utilizadas em gestão de acesso: Sailpoint, SAP, Salesforce, Oracle, CyberArk, entre outras.

Segmentação dos Dados

É importante **segmentar** o **processamento** e o **armazenamento** de **dados** com base na sensibilidade dos dados. A utilização de controles de segmentação pode mitigar riscos relacionados à:

Prevenção de Movimentação Lateral

- O **movimento lateral** é a tentativa dos invasores de **expandir seu nível de acesso**, mudar para ativos confiáveis adicionais e avançar ainda mais na direção de seu alvo final.

Reduzir a Superfície de Ataque

- A **superfície de ataque** de uma organização é o **soma das vulnerabilidades** ou dos **métodos** (vetores de ataque), que os hackers podem usar para **obter acesso não autorizado à rede ou a dados sensíveis**, ou para realizar um ataque cibernético.

Detecção de Ameaças em Tempo Hábil

- **Detecção** automática de potenciais **violações cibernéticas** no ambiente da Organização e **redução do tempo de análise de causa-raiz e resposta ao incidente.**

Impedir a Proliferação de Malwares

- O malware pode se **espalhar na rede da Organização** por anexos de e-mail, downloads em sites infectados ou mídias removíveis infectadas, como unidades USB.

A segmentação separa os controles de segurança da infraestrutura subjacente e permite às organizações a flexibilidade para estender a proteção e a visibilidade em qualquer lugar, possibilitando aplicar o princípio do menor privilégio de forma mais extensiva em ambientes de data center e nuvem, proporcionando uma postura de defesa mais eficaz do que os controles tradicionais de camada de rede. As políticas de segmentação podem assumir várias formas, incluindo controles baseados no tipo de ambiente, escopo regulatório, aplicação e nível de infraestrutura

Ferramentas que podem ser utilizadas para a segmentação de acesso: Akamai Guardicore Segmentation, Cisco Secure Workload, Microsoft Azure, Prisma Cloud, entre outras.

Link – Material de Apoio

Classificação da Informação

Segundo o CIS Controls, as empresas precisam **catalogar seus principais tipos de dados e sua criticidade** (impacto para sua perda ou corrupção) para a empresa. Essa análise deveria ser usada para criar um esquema geral de classificação de dados para a empresa.

Exemplo: esquema de classificação de dados

Público

- Os dados públicos não representam risco para a empresa se disponibilizado ao público em geral. Exemplo: material de publicidade pública, endereço da sede da empresa e informações de produtos.

Interno

- Dados internos são dados que a perda, corrupção ou divulgação não autorizada de que é de certa importância apenas dentro da empresa e, portanto, não resultaria em prejuízo considerável ao negócio, financeiro ou jurídico. Exemplo: Padrões de deslocamento, alocação de funcionários, organogramas e etc.

Confidencial

- Dados confidenciais são dados que a perda, corrupção ou divulgação não autorizada podem prejudicar gravemente a reputação da empresa ou posição de negócios, resultando em considerável perda financeira, de reputação e jurídica. Categorias de dados de exemplo: Dados de marketing, dados de clientes, dados sensíveis, entre outros.

Restritos

- Dados restritos são dados que a perda, corrupção ou divulgação não autorizada podem prejudicar gravemente a reputação da empresa ou posição de negócios, resultando em severa perda financeira, de reputação e jurídica. Categorias de dados de exemplo: Pré-lançamento de resultados financeiros, dados marcados pelo governo, segredos comerciais.

Descarte Seguro de Dados

Segundo a ISO 27002, procedimentos formais para o **descarte seguro** dos dados devem ser definidos para **minimizar o risco de vazamento de informações sensíveis para pessoas não autorizadas**. Os **procedimentos** para o descarte seguro, devem ser proporcionais à **sensibilidade dos dados.**

Todos os componentes, equipamento ou mídias que contenham dados e que forem retirados de sua utilização, devem ter seus dados plenamente apagados. O descarte deve garantir que todos os dados foram inutilizados e são irrecuperáveis.

Práticas de Descarte Seguro

- **Discos rígidos**: devem ser regravados usando o padrão binário 0 e 1 (*wipe*) de acordo com as melhores práticas de segurança quando não forem mais utilizados. Alternativamente, pode ser enviado para descarte através de empresa especializada com emissão de certificado de destruição.
- **Mídias eletrônicas (CDs e DVDs):** devem ser descartadas usando as fragmentadoras destinadas.
- **Papéis, folders e outros documentos impressos**: devem ser descartadas usando as fragmentadoras destinadas.
- **Fitas magnéticas (backups, pen drive, discos externos ou dispositivos de armazenamento)** devem ser destruído por empresas especializadas com certificação de proteção ambiental e emissão de certificado de destruição segura.
- **Aplicativos de comunicações**: devem ser estabelecidas configurações de segurança para exclusão automática de mensagens em aplicativos de comunicação, por exemplo, Microsoft Teams, WhatsApp, Skype, entre outros.
- Segundo a **resolução 4893**, a empresa contratada **deve excluir os dados** após a transferência dos dados para a nova empresa e/ou após o fim das atividades estabelecidas em contrato, além de **confirmar a integridade e a disponibilidade dos dados recebidos.**
  - **Obs.:** Após a eliminação dos dados, é necessário **enviar uma evidência** a **Instituição que demonstre e comprove a realização do descarte** de informações.

Prevenção de Vazamento de dados

FEBRABAN

Segundo a ISO 27002, as **medidas de prevenção de vazamentos devem ser aplicadas a sistemas, redes e quaisquer outros dispositivos que processam, armazenam ou transmitem informações confidenciais**. Essas medidas visam detectar e impedir a divulgação e extração não autorizada de informações por indivíduos ou sistemas.

A prevenção contra perda de dados (DLP) é uma estratégia para detectar e evitar a exfiltração ou a destruição de dados. Muitas soluções de DLP analisam o tráfego de rede e dispositivos de "endpoint" internos para identificar o vazamento ou perda de informações confidenciais.

Como as soluções podem ajudar?

Identificação e classificação dos dados: A classificação de dados permite que a organização aplique as políticas de DLP corretas aos tipos certos de dados. **Essas ferramentas geralmente podem examinar toda a rede para encontrar dados onde quer que estejam armazenados** (exemplos: nuvem, em pontos de extremidade físicos, nos dispositivos pessoais dos funcionários, entre outros).

Monitoramento de dados: **As ferramentas DLP podem usar várias técnicas para identificar e rastrear dados confidenciais em uso**. Como por exemplo: comparar o conteúdo do arquivo com dados confidenciais conhecidos, procurar dados que seguem um determinado formato, análise de conteúdo e detecção de rótulos, marcas e outros metadados que identificam explicitamente um arquivo como confidencial.

Aplicar proteções de dados: **As ferramentas conseguem detectar violações de políticas e responder em tempo real**. Como por exemplo: criptografando dados, encerrando transferências, avisando usuários sobre violações, sinalizando comportamento suspeito e acionando desafios de autentificação adicionais.

Relatórios: As ferramentas conseguem documentar e relatar os esforços gerando um relatório que permitem as equipes de segurança **acompanhar o desempenho das políticas ao longo do tempo**.

Exemplos de ferramentas para a Prevenção de Vazamento de Dados: Forcepoint DLP, Symantec Data Loss Prevention, Proofpoint Enterprise Data Loss Prevention, entre outras.

Cópias de Segurança (Backups)

Segundo a ISO 27002, **cópias de backup** de **informações**, **software** e **sistemas** devem ser **mantidas e testadas regularmente** para permitir a recuperação de perda de dados ou sistemas.

A política de backup deve ser estabelecida para definir os requisitos da organização relativos às cópias de segurança das informações, dos softwares e dos sistemas, contendo por exemplo, mas não limitado aos seguintes itens:

Um **cofre imutável**, permite bloquear todas as operações para garantir que o Backup esteja protegido e pode impedir que os atores mal-intencionados os excluem e afetem a capacidade de recuperação de dados.

Os backups precisam ser **armazenados em lugares com segurança adequados** para garantir que todas as informações e software essenciais possam ser recuperados de maneira eficiente.

As mídias de backup devem ser regularmente **testadas** para garantir que elas **são confiáveis, íntegros e completos** no caso do uso emergencial.

Backup completo, realizado com menos frequência, cópia todo o conjunto de dados, independentemente de alteração que tenha sido feita.

Backup incremental cópia somente os dados modificados desde o último backup.

Backup diferencial cópia somente os dados recém-adicionados e alterados desde o último backup completo, isso faz com que o tamanho do backup aumenta progressivamente até o próximo backup completo.

Exemplos de ferramentas para a Backup e Recuperação de Dados: Veeam Data Platform, Dell Data Protection Suite, Veritas NetBackup, Microsoft Azure Backup, Dell PowerProtect DP Series Appliances, entre outras.

Controles Criptográficos

Segundo o CIS Controls, a adoção da **criptografia** de dados, tanto em **trânsito** (comunicações) quanto em **repouso** (armazenamento) podem contribuir para **proteger** a **confidencialidade**, **autenticidade** e/ou a **integridade** da **informação**.

Principais Conceitos:

Em transito: Os dados são considerados em trânsito quando se movem entre dispositivos, como em redes privadas ou na Internet. A criptografia de dados durante a transferência garante que mesmo se os dados forem interceptados, sua privacidade é protegida. Tecnologias seguras: SSH, S-FTP, TLS ou VPN IPsec.

Em repouso: Os dados são considerados em repouso quando estão em um dispositivo de armazenamento de dados e não estão sendo ativamente usados ou transferido, e podem ser dados mais valiosos. A criptografia de dados em repouso reduz as oportunidades de roubo de dados criados por dispositivos perdidos ou roubados, compartilhamento inadvertido de senha ou concessão acidental de permissão.

Exemplos de protocolos criptográficos:

01

3DES (Triple Data Encryption Standard)
Esse é um algoritmo de chave simétrica. O Triple DES está sendo lentamente substituído, mas continua sendo uma solução de criptografia de hardware confiável para serviços financeiros.

02

Twofish
Considerado um dos mais rápidos do seu tipo, o twofish é usado tanto em hardware quanto em software e ele não é patenteado, sendo gratuitamente disponibilizado.

03

RSA (Rivest, Shamir e Adleman)
Primeiro algoritmo de criptografia assimétrica amplamente disponibilizado ao público e é popular devido ao tamanho da sua chave e, por isso, amplamente utilizado para transmissão de dados segura.

04

AES (Advanced Encryption Standard)
. Desenvolvido para atualizar o algoritmo DES original. Mais comum em aplicativos de mensagens

05

RC4
Usado em WEP e WPA, que são protocolos de criptografia comumente usados em roteadores sem fio

06

DAS (Algoritmo de Assinatura Digita)
É uma criptografia assimétrica adotado no processo de coleta de assinaturas digitais para documentos eletrônicos.

Segurança em Dispositivos Móveis

Segundo o CIS Controls, o malware entra em uma empresa por meio de vulnerabilidades em dispositivos de usuário final, anexos de e-mail, páginas da web, serviços em nuvem, dispositivos móveis e mídia removível.

- A Organização deve **publicar uma política ou norma contendo as regras e limitações** para o uso de dispositivos móveis particulares.
- A utilização de dispositivos móveis particulares deve ser **aprovada pela Organização antes do uso**.
- Manter **sigilo das credenciais de acesso** para ou com dispositivos móveis.
- **Usuários são responsáveis por todas transações** e atividades realizadas usando suas credenciais (ID, senha, pin, etc.).
- Utilizar **MFA** (autenticação multifator).

BYOD
(*Bring Your Own Device*)

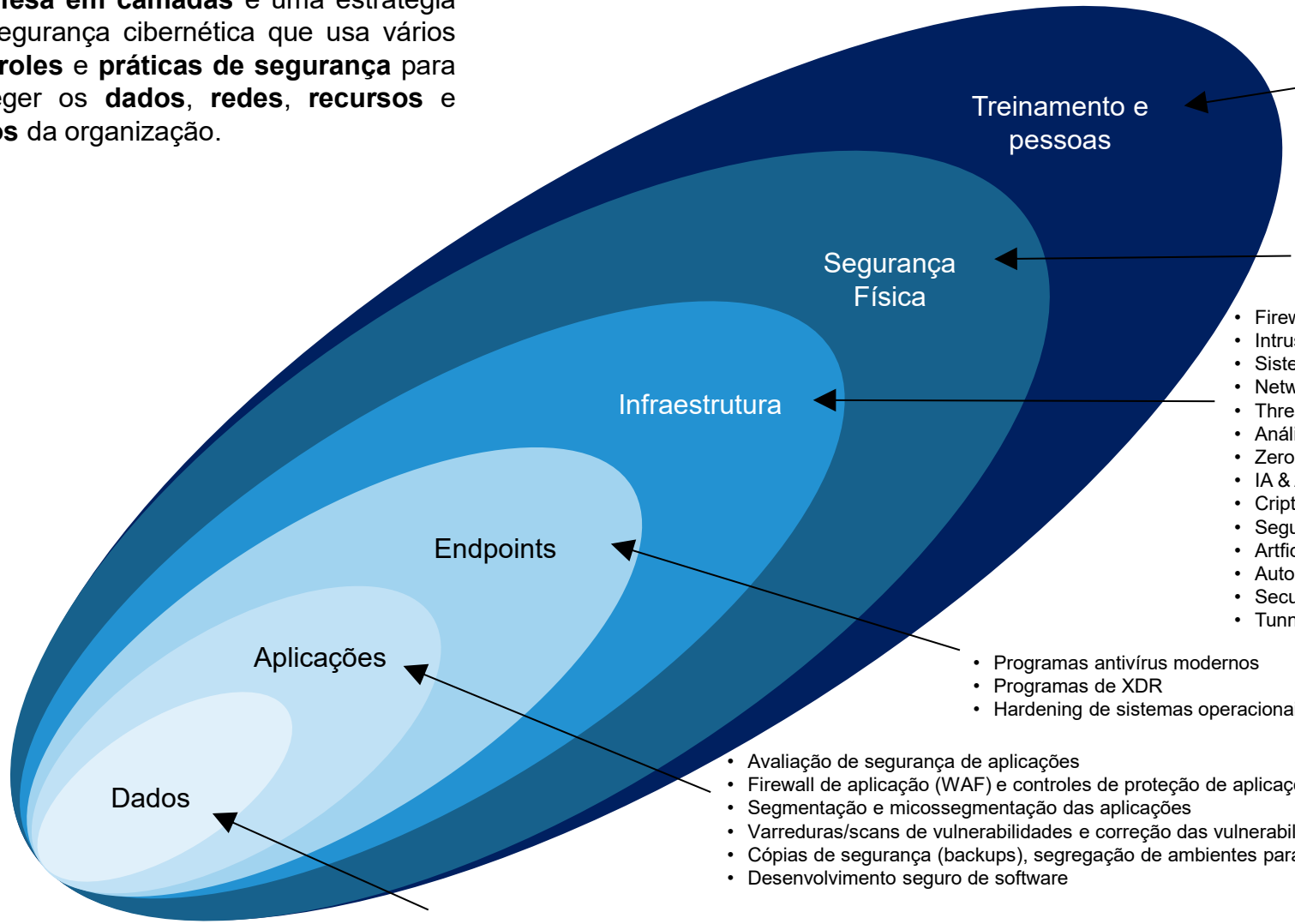
- Usuários com permissão de uso de dispositivos particulares devem permitir que **seus dispositivos sejam inspecionados para fins de segurança**.
- **Manter dispositivos** móveis **atualizados**.
- **Não é permitido instalar** produtos, sistemas ou aplicativos **sem autorização prévia**.
- **Utilizar VPN** (homologada) para realizar conexões seguras.
- A Organização deve realizar varreduras que buscam por **vulnerabilidades em dispositivos e aplicar as correções**.

Segundo a ISO 27002, qualquer dispositivo usado fora das instalações da organização que armazena ou processa informações incluindo dispositivos de propriedade da organização e dispositivos de propriedade privada e usados em nome da organização(BYOD) precisa de proteção.

Estratégia para Proteção de Dados

FEBRABAN

- A **defesa em camadas** é uma estratégia de segurança cibernética que usa vários **controles** e **práticas de segurança** para proteger os **dados**, **redes**, **recursos** e **ativos** da organização.



- Treinamentos de conscientização (dinâmicas tradicionais e realistas, por exemplo, metaverso e óculos de realidade aumentada)
- Exercícios e simulações reais de cenários de incidentes cibernéticos, por exemplo, ransomware
- Campanhas de phishing e engenharia social
- Desenvolvimento e aprimoramento de recursos e competências

- Controle de acesso físico
- Perímetro de segurança
- CFTV

- Firewall, proxy, anti-spam
- Intrusion detection/prevention sistemas (IDS/IPS)
- Sistemas de monitoramento - SIEM
- Network access control (NAC)
- Threat intelligence
- Análise de arquitetura de redes
- Zero Trust (ZTA)
- IA & Automação do SOC
- Criptografia em trânsito
- Segurança em cloud
- Artficial Intelligence IT Operations (AIOps) Platforms
- Automações
- Security and Privacy by Design
- Tunning das Ferramentas de segurança

- Programas antivírus modernos
- Programas de XDR
- Hardening de sistemas operacionais

- Avaliação de segurança de aplicações
- Firewall de aplicação (WAF) e controles de proteção de aplicações
- Segmentação e micossegmentação das aplicações
- Varreduras/scans de vulnerabilidades e correção das vulnerabilidades em tempo hábil
- Cópias de segurança (backups), segregação de ambientes para cópia e restauração, bem como imutabilidade
- Desenvolvimento seguro de software

- Criptografia em repouso
- Controle de acesso (principalmente com as contas administrativas) a informações sensíveis (seguindo princípios de privilégio mínimo)
- MFA
- Senhas fortes e renovação de senhas

Fonte: Deloitte Ransomware | Threat Activities, Trends, and Continuing Evolution (2023)

Considerações Finais

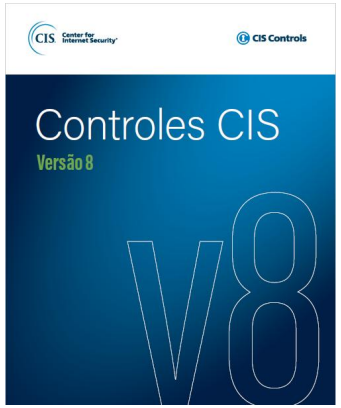
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

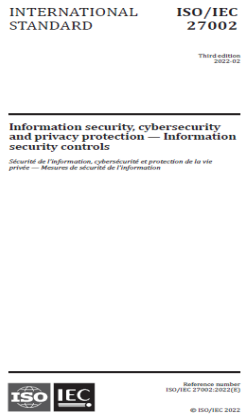
Frameworks e Normas de Referência

Para apoiar no entendimento e implementação de toda a metodologia apresentada neste material, a seguir são apresentados as normas e frameworks de referência no tema:

Frameworks Padrão Utilizados

PCI DSS COMPLIANT





NIST National Institute of Standards and Technology

Conformidade: Requisitos de conformidade mais exigentes, permitindo estimar o nível de conformidade com ABNT NBR ISO, PCI-DSS, NIST, CIS Controls, entre outros

Relembrando os principais conceitos

Agora que aprendemos sobre as atividades relacionadas ao Proteção de Dados, relembre os principais termos e conceitos apresentados neste material:

Gestão de Acesso : Gerenciamento de credenciais de identidade, ciclo de vida, controle de quem poder ter acesso aos dados

Gestão de dados: Todo o processo: desde a captação e a manipulação até o armazenamento de informações.

Mascaramento de dados: Usado para limitar a exposição de dados sensíveis, incluindo PII, e para cumprir as normas legais, estatutárias, regulamentares e requisitos contratuais.

Prevenção de vazamento de dados: Estratégia para detectar e evitar a exfiltração ou a destruição de dados.

Backup e Restauração: Práticas para fazer a cópia periódica dos dados e usar essas cópias para recuperar os dados.

Criptografia: Usada para proteger as informações, sensíveis ou críticas, quando armazenadas ou transmitidas.

Segmentação de dados: A segmentação separa os controles de segurança da infraestrutura subjacente e permite às organizações a flexibilidade para estender a proteção e a visibilidade em qualquer lugar

Módulo: Gestão de Identidades

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Requisitos – Gestão de identidades

FEBRABAN

Este material foi elaborado de acordo com as diretrizes do PCI DSS e CIS Controls, bem como foram considerados os requisitos de segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

PCI DSS

- 7.1 Processos e mecanismos para restringir o acesso aos componentes de sistema e dados do titular do cartão por necessidade de negócios são definidos e compreendidos
- 7.2 O acesso aos componentes de sistema e dados é definido e atribuído apropriadamente
- 7.3 O acesso aos componentes de sistema e dados é gerenciado por meio de um(s) sistema(s) de controle de acesso
- 8.1 Processos e mecanismos para identificar usuários e autenticar o acesso aos componentes de sistema são definidos e compreendidos
- 8.2 A identificação do usuário e contas relacionadas para usuários e administradores são estritamente gerenciadas ao longo do ciclo de vida de uma conta
- 8.3 Uma autenticação forte para usuários e administradores é estabelecida e gerenciada
- 8.4 A autenticação multifator (MFA) é implementada para proteger o acesso ao CDE
- 8.5 Os sistemas de autenticação multifator (MFA) são configurados para evitar o uso indevido
- 8.6 O uso de contas de aplicativo e sistema e fatores de autenticação associados é estritamente gerenciados

CIS Controls

- 5.1 Estabelecer e manter um inventário de contas
- 5.2 Usar senhas exclusivas
- 5.3 Desabilitar contas inativas
- 5.4 Restringir privilégios de administrador a contas de Administrador dedicadas
- 5.5 Estabelecer e manter um inventário de contas de serviço
- 5.6 Centralizar a gestão de contas
- 6.1 Estabelecer um Processo de Concessão de Acesso
- 6.2 Estabelecer um Processo de Revogação de Acesso
- 6.3 Exigir MFA para aplicações expostas externamente
- 6.4 Exigir MFA para acesso remoto à rede
- 6.5 Exigir MFA para acesso administrativo
- 6.6 Estabelecer e manter um inventário de sistemas de autenticação e autorização
- 6.7 Centralizar o controle de acesso
- 6.8 Definir e manter o controle de acesso baseado em funções

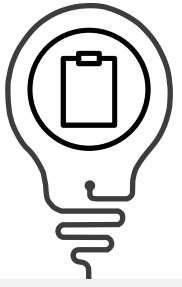
ISO 27002

- 9.1.1 Política de controle de acesso
- 9.2.1 Registro e cancelamento de usuário
- 9.2.2 Provisionamento para acesso de usuário
- 9.2.3 Gerenciamento de direitos de acesso privilegiados
- 9.2.4 Gerenciamento da informação de autenticação secreta de usuários
- 9.2.5 Análise crítica dos direitos de acesso de usuário
- 9.2.6 Retirada ou ajuste de direitos de acesso
- 9.3.1 Uso da informação de autenticação secreta
- 9.4.1 Restrição de acesso à informação
- 9.4.2 Procedimentos seguros de entrada no sistema (log-on)
- 9.4.3 Sistema de gerenciamento de senha
- 9.4.4 Uso de programas utilitários privilegiados

ISO 27701

- 6.6.2.1 Registro e cancelamento de usuário
- 6.6.2.2 Provisionamento para acesso de usuário
- 6.6.2.3 Gerenciamento de direitos de acesso privilegiado
- 6.6.2.4 Gerenciamento da informação de autenticação secreta de usuários
- 6.6.2.5 Análise crítica dos direitos de acesso de usuário
- 6.6.2.6 Retirada ou ajuste dos direitos de acesso
- 6.6.4.1 Restrição de acesso à informação
- 6.6.4.2 Procedimentos seguros de entrada no sistema (log-on)

NIST CSF



- PR. AA-01: Identidades e credenciais para usuários, serviços e hardware autorizados são gerenciados pela organização
- PR. AA-02: As identidades são provadas e vinculadas a credenciais com base no contexto das interações
- PR. AA-04: As asserções de identidade são protegidas, transmitidas e verificadas
- PR. AA-05: Permissões, direitos e autorizações de acesso são definidos em uma política, gerenciados, aplicados e revisados e incorporam os princípios de privilégio mínimo e separação de funções

Sumário

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Sumário

Contexto Geral

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Qual a Relevância do Tema para as Organizações?

FEBRABAN

Riscos Cibernéticos

Mitigação dos **riscos cibernéticos** associados com vazamento de dados, ataques internos e software maliciosos

Complexidade de TI e Eficiência de Custos

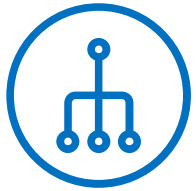
A necessidade de **redução na complexidade de TI** e **eficiência de custos** para manter infraestrutura de identidades e operações

Conformidade Regulamentar

Pressão contínua de **conformidade regulamentar** e necessidade de um processo eficiente para governança de identidades

Experiência do Usuário

Qualidade da experiência do usuário é a prioridade para identidade do consumidor e aplicativos móveis



Tendências da Tecnologia

Transformação digital e a rápida expansão de mídias sociais, dispositivos móveis e tecnologias de nuvem oferecem novas oportunidades

Principais Desafios

Principais Desafios	Objetivos
Apontamentos de Auditoria	**Aprimorar a precisão e efetividade do *compliance*** utilizando as capacidade de IAG (Inteligências Artificial Geral) como as certificações de acesso, segregação de funções (SoD), relatórios e outros
Controle de Acessos	**Implementar uma solução de Gestão de Acesso que forneça autenticação centralizada**, autorização e *Single Sign-On* (SSO)
Processos Manuais	**Padronizar, simplificar e automatizar os processos de gestão do ciclo de vida de usuários** aumentará a eficiência do provisionamento para todas as linhas de negócios
Linguagem Técnica	**Aumentar a conscientização dos gestores** utilizando descrições amigáveis durante as certificações de acesso
Usuários Genéricos	**A integração bidirecional das soluções** de IAG e PAM facilitará o *ownership* e responsabilização sobre usuários genéricos, por meio de **fluxos de aprovação robustos, provisionamento / deprovisionamento automatizado, e certificações de acesso**

Introdução

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Principais Aspectos

O que é Gestão de Identidades?

O gerenciamento de identidade e acesso (IAM) é a disciplina que permite que as **pessoas certas acessem os dados e recursos certos nos momentos certos pelas razões certas**. Principais características:

- Gerenciamento de credenciais de identidade atribuídas a funcionários, contratados, fornecedores e clientes;
- Gerenciamento do ciclo de vida de identidades e funções de acesso;
- Processos, incluindo funções e responsabilidades, estrutura organizacional e procedimentos administrativos; entre outros.

Gerenciamento do ciclo de vida da identidade (ILM)

É o ciclo de vida completo da identidade e do acesso para qualquer recurso. Ele abrange todos os aspectos do gerenciamento de identidade e acesso (IAM) desde o **momento em que uma pessoa ingressa na empresa, até a sua saída**. Exemplo de ciclo de vida:

- Estabelecer uma nova identidade;
- Validar e autenticar a identidade;
- Registrar a identidade nos serviços;
- Gerenciar e atualizar o acesso conforme sua evolução;
- Remover o acesso quando o relacionando se encerra.

O que são recursos?

São todos os **sistemas tecnológicos que compõem a infraestrutura** de uma empresa, tais como:

- Aplicações;
- Bases de Dados;
- Sistemas Operacionais;
- Serviços Web;
- Equipamentos de Comunicação;
- Físico (Smartphone, Notebook, Crachá, entre outros).

O que são mecanismos de autenticação?

A autenticação é usada para **verificar e validar as identidades antes de fornecer acesso a recursos e redes digitais**, exemplos:

- MFA (multifator);
- Senha e PIN;
- Tokens e Smartcard;
- SSO (Single Sign-On);
- Biometria.

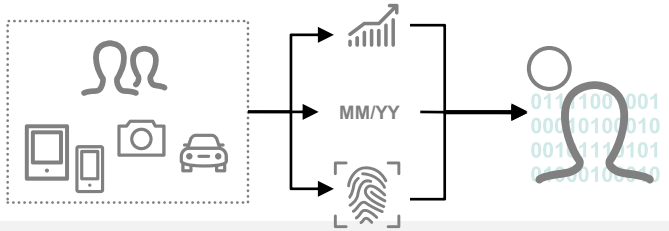
Principais Termos e Definições

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Identidade, Confiança e Acesso

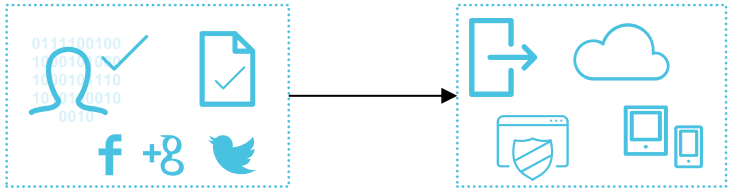
FEBRABAN

Gestão de Identidades



- As identidades representam **humanos**, **sistemas** e, cada vez mais, **dispositivos.**
- Os provedores de identidades, tais como agências governamentais, grandes empresas e serviços de mídias sociais estabelecem as **identidades.**
- A confiança é estabelecida por meio da mistura de **credenciais**, **contexto**, **histórico** e **comportamento.**

Controle de Acessos



- As identidades são **registradas** nas aplicações e serviços.
- Os usuários que acessam serviços e dados se **autenticam** nos níveis apropriados com base no risco.
- **O acesso é autorizado com base na necessidade** mútua e na **medida em que a relação evolui**.

O que mais eu preciso saber?

Autenticação: Autenticação **confirma** quem está acessando e autorização determina o que este pode fazer.

Provisionamento: É a terminologia do processo em que o IAM é o **ponto de entrada** para a administração automatizada de usuários nos recursos de destino.

Reconciliação: É a terminologia do processo para a **administração das contas** de usuário e recursos para manter a integridade dos dados do IAM.

Certificação: É o processo de **revisar o acesso** do usuário, por meio de aplicativos e plataformas, para **garantir que o princípio de ter o mínimo de privilégios** necessários para desenvolver a função / posição seja cumprido.

Usuário x Identidade Digital x Acesso à Recursos

Usuário

Identidade Digital

Controle de acesso aos recursos

Modelos de Gerenciamento de Identidades

A seguir é apresentado as principais diferenças entre os principais modelos de gerenciamento de identidade:

Disciplina de controle dos negócios que **"permite que os indivíduos certos acessem os recursos certos nos momentos certos e pelos motivos certos"**

Modelo de gestão de regras dos atributos das identidades, incluindo administração e gestão de todo o processo de contas, senhas, solicitações de acesso, provisionamento, concessão e revisão de acesso, e gestão de direitos.

O processo (e modelo) de concessão, monitoração e proteção de contas, como contas administrativas, contas de aplicações, contas de serviços e demais segredos corporativos.

Gestão de Identidades

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Introdução

Segundo o CIS Controls, é necessário um **processo e ferramentas para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas** de usuário, administrador e serviço para ativos e softwares corporativos.

Principais controles:

Ciclo de vida da identidade

O *Identity Lifecycle Management* (ILM) tem como objetivo gerenciar todo o processo de ciclo de vida da identidade digital para indivíduos afiliados a uma organização.

Modelos de controle de acesso

Estruturas ou abordagens utilizadas para gerenciar o acesso a recursos, sistemas ou informações em ambientes tecnológicos.

Mecanismos de autenticação

Os acessos aos sistemas e aplicações devem ser controlados por um procedimento seguro de entrada no sistema (log-on).

Segurança em senhas

Criar senhas de qualidade, que permitam garantir aspectos de proteção da Confidencialidade, Disponibilidade e Integridade das informações.

Segurança com contas administrativas

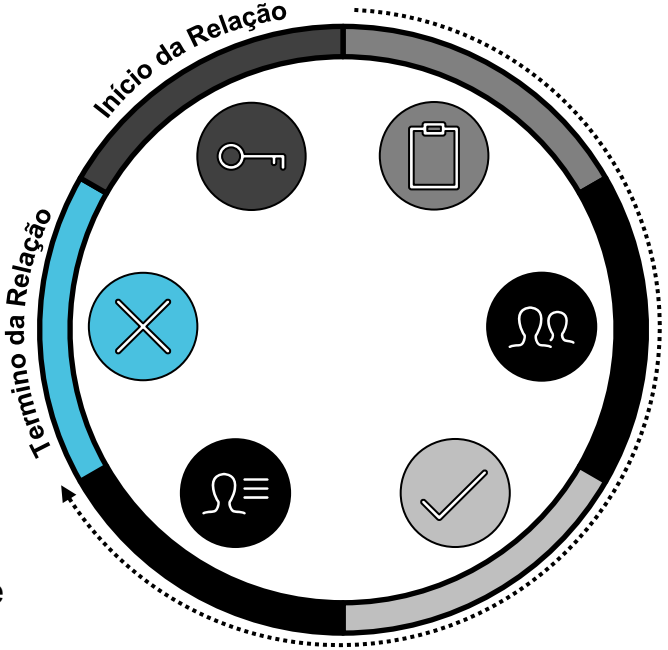
Uso inapropriado de privilégios de administrador de sistemas pode ser um grande fator de contribuição para falhas ou violações de sistemas, portanto, é necessário aplicar controle e restrições.

Gestão do Ciclo de Vida da Identidade

O gerenciamento do ciclo de vida da identidade é a base para a governança de identidade, e uma governança eficaz em escala requer a modernização da infraestrutura de gerenciamento do ciclo de vida da identidade para aplicativos. O *Identity Lifecycle Management* (ILM) tem como objetivo gerenciar todo o processo de ciclo de vida da identidade digital para indivíduos afiliados a uma organização.

1. Nova Identidade
Estabelecer uma nova relação com uma identidade

2. Comprovar
Comprovar que a pessoa por trás da identidade é verdadeira



6. Revogar Acesso
Remover o acesso quando um relacionamento se encerra

3. Verificar
Autenticar a identidade para transações futuras

5. Gerenciar Acesso
Atualizar o acesso conforme a evolução da relação

4. Registrar
Registrar a identidade nos serviços com base no valor da relação

Abordagem recomendada para gerenciar credenciais de identidade atribuídas a funcionários e terceiros.

Ferramentas que podem ser utilizadas em gestão de identidades: Sailpoint, SAP, Salesforce, Oracle, CyberArk, entre outras.

Gestão do Ciclo de Vida da Identidade

O gerenciamento do ciclo de vida da identidade é a base para a governança de identidade, e uma governança eficaz em escala requer a modernização da infraestrutura de gerenciamento do ciclo de vida da identidade para aplicativos. O *Identity Lifecycle Management* (ILM) tem como objetivo gerenciar todo o processo de ciclo de vida da identidade digital para indivíduos afiliados a uma organização.

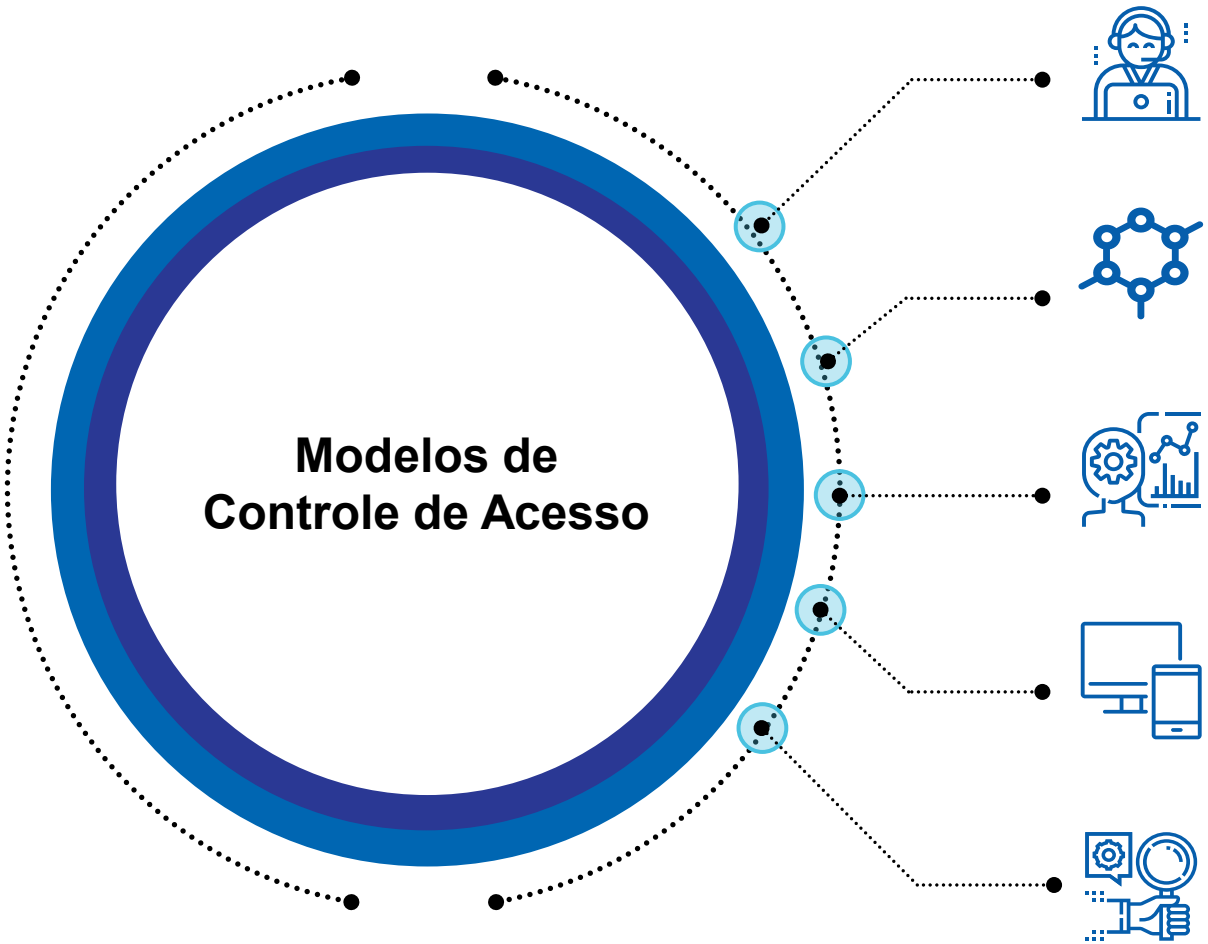
A gestão de identidades permite:

- O **registro e o monitoramento de** contas são componentes críticos das operações de segurança.
- Excluir ou **desabilitar quaisquer contas inativas após um período** de 45 dias de inatividade, onde for suportado.
- **Restringir os privilégios de administrador** a contas de administrador dedicadas nos ativos corporativos.
- **Realizar análises de contas de serviço** para validar se todas as contas ativas estão autorizadas em uma programação recorrente, no mínimo trimestralmente ou com mais frequência.
- **Centralizar a gestão de contas** por meio de serviço de diretório ou de identidade.

Ferramentas que podem ser utilizadas em gestão de identidades: Sailpoint, SAP, Salesforce, Oracle, CyberArk, entre outras.

Modelos de Controle de Acesso

Os modelos de controle de acesso são estruturas ou abordagens utilizadas para gerenciar o acesso a recursos, sistemas ou informações em ambientes tecnológicos. Esses modelos são projetados para garantir que apenas usuários autorizados obtenham acesso aos recursos necessários, de maneira que os acessos estejam em **conformidade com as políticas de segurança da organização**.



Controle de acesso baseado em função (RBAC)

O RBAC concede acesso com base nas necessidades do usuário de acordo com sua posição. As funções e os privilégios associados são definidos e as permissões são atribuídas para controlar o acesso, o escopo das operações aprovadas e o tempo de sessão.

Controle de acesso baseado em atributos (ABAC)

O controle de acesso baseado em atributos é uma solução de autorização de usuário que avalia os atributos ou características dos usuários, em vez de funções, para determinar privilégios de acesso com base nas diretivas de segurança de uma organização. Com o ABAC, as regras de acesso podem ser hiper granulares.

Controle de acesso discricionário (DAC)

O controle de acesso discricionário concede ou restringe o acesso a um objeto de acordo com a política determinada pelo proprietário, grupo ou sujeitos de um objeto. O DAC oferece aos usuários controle total sobre seus recursos, tornando-o menos restritivo do que outras opções de controle de acesso.

Controle de Acesso Obrigatório (MAC)

O controle de acesso obrigatório limita o acesso aos recursos de acordo com a sensibilidade das informações e o nível de permissões dos usuários. Os administradores definem critérios para MAC. A imposição do MAC é tratada pelo sistema operacional ou por um kernel de segurança, que os usuários não podem alterar.

Lista de controle de Acesso (ACL)

Uma lista de controle de acesso é uma tabela que lista as permissões associadas a um recurso. Para cada usuário, há uma entrada que detalha os atributos de segurança de cada objeto. A ACL também avalia as atividades e se elas são permitidas pela rede. Os sistemas de arquivos usam a ACL para filtrar e gerenciar o acesso a arquivos e diretórios por meio do sistema operacional.

Mecanismo de Autenticação

Segundo a ISO 27002, **os acessos aos sistemas e aplicações devem ser controlados por um procedimento seguro de entrada no sistema (log-on)**, por meio de técnicas de autenticação adequadas para validar a identificação dos usuários.

MFA

Método de verificação de identidade, que exige que os **usuários forneçam pelo menos um fator de autenticação além de uma senha** ou pelo menos dois fatores de autenticação em vez de uma senha.

Senha e PIN

A senhas servem para autenticar um usuário permitindo **direito de acesso ao ambiente** desejado, a senha também **garante autenticidade e não repudio da ação** realizada pelo usuário.

Biometria

Verificação de identidade usando **recursos biológicos**, como por exemplo, utilizando a digital ou escaneamento de rosto e retina.

Token e Smartcard

Geração de **um número exclusivo** chamado TOTP (PIN avulso por tempo limitado) **a cada 30 segundos**. Se os números coincidem, o sistema verifica que o usuário está com o dispositivo. O Smartcard é um hardware **capaz de gerar e armazenar as chaves criptográficas**, responsáveis por liberar um acesso.

Federação

Permite que os **usuários se autentiquem entre diferentes domínios e / ou empresas por meio de tokens ou "asserções",** sem precisar expor senhas ou todos os atributos de identidade.
Permite compartilhar alguns atributos entre diferentes domínios / empresas.

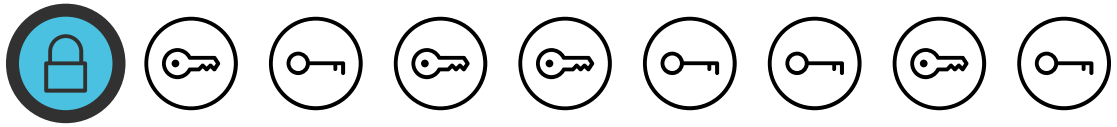
SSO (Single Sign-On)

Permite que os usuários façam **login uma vez usando um único conjunto de credenciais e acessem várias aplicações** durante a mesma sessão.

Segurança com as Senhas

É **NOSSA RESPONSABILIDADE** criar senhas de qualidade, que permitam garantir aspectos de proteção da Confidencialidade, Disponibilidade e Integridade das informações.

Além disso, é importante seguir as políticas estabelecidas para segurança das senhas de acesso ao ambiente interno e de clientes.



As boas práticas de segurança sugerem que as senhas sigam os seguintes aspectos.

Tamanho mínimo: utilizar senhas com a quantidade de caracteres que compõem a senha, com no mínimo 12 caracteres.

Complexidade: nível de complexidade de uma senha utilizando por exemplo, letras maiúsculas, letras minúsculas, números e caracteres especiais (!,@,#,$,%, entre outros).

Tempo de vida e Rotacionamento de Senhas: período de expiração ou troca das senhas, por exemplo, entre 60 - 90 dias.

Duplo Fator de Autenticação (MFA): utilizar duplo fator de autenticação para logins seguros.

Armazenamento: não salvar senhas em arquivos desprotegidos locais ou na rede.

Histórico: quantidade das últimas senhas não permitidas para reutilização.

Segurança em Contas Administrativos

FEBRABAN

Contas administrativas ou privilegiadas são um alvo específico porque permitem que atacantes adicionem outras contas ou façam alterações em ativos que podem torná-los mais vulneráveis a outros ataques. Segundo a ISO 27002, a concessão e uso de direitos de acesso privilegiado devem ser restritos e controlados.

Acessos Administrativos

- **Os direitos de acesso privilegiados**, associados a cada sistema ou processo, por exemplo, sistema operacional, sistemas de gerenciamento de banco de dados e cada aplicação, e de categorias de usuários para os quais estes necessitam ser concedido, **devem ser identificados**
- **Os direitos de acesso privilegiado devem ser concedidos a usuários conforme a necessidade de uso** e com base em eventos alinhados com a política de controle de acesso, **baseado nos requisitos mínimos para sua função**
- **Os direitos de acesso privilegiados devem ser atribuídos a um ID de usuário diferente daqueles usados nas atividades normais do negócio**. As atividades normais do negócio não devem ser desempenhadas usando contas privilegiadas
- **Utilizar cofre de senhas para os acessos privilegiados**. Um cofre de senha (às vezes chamado de gerenciador de senha ou armário de senha) é um **espaço criptografado usado para armazenar dados, como senhas e credenciais de login** (as informações usadas para acessar aplicativos e contas digitais), documentos, imagens e outras informações confidenciais em um local digital protegido

Política de Controle de Acesso

Segundo a ISO 27002, a **política de controle de acesso deve ser estabelecida, documentada e analisada criticamente**, baseada nos requisitos de segurança da informação e dos negócios. A política deve incluir as seguintes considerações:

Aspectos Gerais

- Diretrizes para requisitos de segurança de aplicações de negócios individuais;
- Diretrizes para gerenciamento de direitos de acesso em um ambiente distribuído e conectado à rede que reconhece todos os tipos de conexões disponíveis;
- Diretrizes para requisitos para autorização formal de pedidos de acesso;
- Diretrizes para requisitos para análise crítica periódica de direitos de acesso;
- Diretrizes para remoção de direitos de acesso;
- Diretrizes para regras para o acesso privilegiado; entre outros.

Aspectos Técnicos

- Identificação dos repositórios de identidade;
- Definição da estrutura de identidade digital;
- Identificação da origem da informação e fontes autorizadas;
- Definir a arquitetura detalhada da solução de gestão de identidades;
- As regras para definição da matriz SoD (Segregação de Funções);
- Integração das funções com IDM e aplicativos;
- Tecnologias para gestão de identidades comuns e administrativas;
- Integração com aplicativos externos;
- Definir conectores (unidirecional ou bidirecional) com aplicativos, entre outros.

Considerações Finais

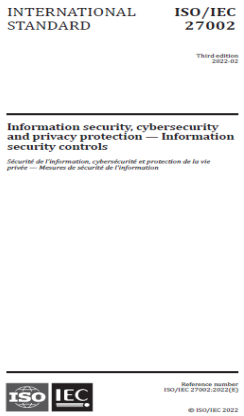
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Frameworks e Normas de Referência

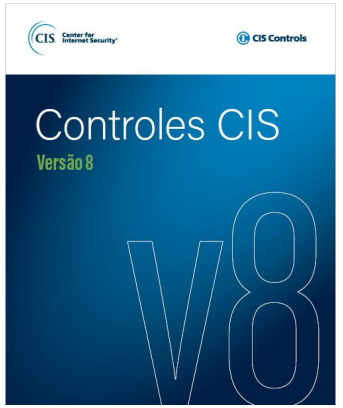
Para apoiar no entendimento e implementação de toda a metodologia apresentada neste material, a seguir são apresentados as normas e frameworks de referência no tema:

Frameworks Padrão Utilizados

NIST
National Institute of Standards and Technology



PCI DSS COMPLIANT



Conformidade: Dado o uso extensivo de padrões amplamente aceitos pela indústria, a gestão de identidades e controle de acesso devem ser alinhadas com alguns dos requisitos de conformidade mais exigentes, permitindo estimar o nível de conformidade com PCI-DSS, ISO, Bacen 4.893, NIST, entre outros.

Relembrando os principais conceitos

Agora que aprendemos sobre as atividades relacionadas ao processo de gestão de identidades, relembre os principais termos e conceitos apresentados neste material:

Ciclo de vida da identidade: base para a governança de identidade, e uma governança eficaz em escala requer a modernização da infraestrutura de gerenciamento do ciclo de vida da identidade para aplicativos. O Identity Lifecycle Management (ILM) tem como objetivo gerenciar todo o processo de ciclo de vida da identidade digital para indivíduos afiliados a uma organização.

Modelos de controle de acesso: são estruturas ou abordagens utilizadas para gerenciar o acesso a recursos, sistemas ou informações em ambientes tecnológicos. Esses modelos são projetados para garantir que apenas usuários autorizados obtenham acesso aos recursos necessários, de maneira que os acessos estejam em conformidade com as políticas de segurança da organização, exemplos: RBAC, ABAC, DAC, MAC e ACL.

Mecanismo de autenticação: mecanismo usado para identificar um usuário por meio da associação de uma solicitação de entrada a um conjunto de credenciais de identificação Exemplo: MFA, Token, Biometria, entre outros.

Senhas seguras: Criar senhas de qualidade, que permitam garantir aspectos de proteção da Confidencialidade, Disponibilidade e Integridade das informações.

Módulo: Gestão de Continuidade dos Negócios

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Requisitos – Gestão de Continuidade dos Negócios

FEBRABAN

Este material foi elaborado de acordo com as diretrizes da ISO e NIST, bem como foram considerados os requisitos de segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

ISO 22301

- 4. Contexto da organização
- 5. Liderança
- 6. Planejamento
- 7. Apoio
- 8. Operação
- 8.2 Análise de impacto nos negócios
- 8.2.3 Análise de riscos
- 8.3 Estratégias e soluções
- 8.4 Planos e procedimentos
- 8.5 Programa de exercícios
- 8. Avaliação da documentação e capacidade
- 9.2 Auditoria interna
- 9.3 Análise crítica da alta direção
- 10. Melhoria

ISO 27002

- 5.29 Segurança da informação durante interrupções
- 5.30 Preparação das TIC para continuidade dos negócios

ISO 27701

- 6.14.1.1 Planejando a continuidade da segurança da informação
- 6.14.1.2 Implementando a continuidade da segurança da informação
- 6.14.1.3 Verificação, análise crítica e avaliação da continuidade da segurança da informação

NIST CSF

- RC.RP-01: A parte de recuperação do plano de resposta a incidentes é executada uma vez iniciada a partir do processo de resposta a incidentes
- RC.RP-02: As ações de recuperação são selecionadas, com escopo, priorizadas e executadas
- RC.RP-05: A integridade dos ativos restaurados é verificada, os sistemas e serviços são restaurados e o status operacional normal é confirmado
- RC.RP-06: O fim da recuperação de incidentes é declarado com base em critérios e a documentação relacionada a incidentes é concluída
- RC. CO-01: As atividades de recuperação e o progresso na restauração das capacidades operacionais são comunicados às partes interessadas internas e externas designadas

Sumário

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

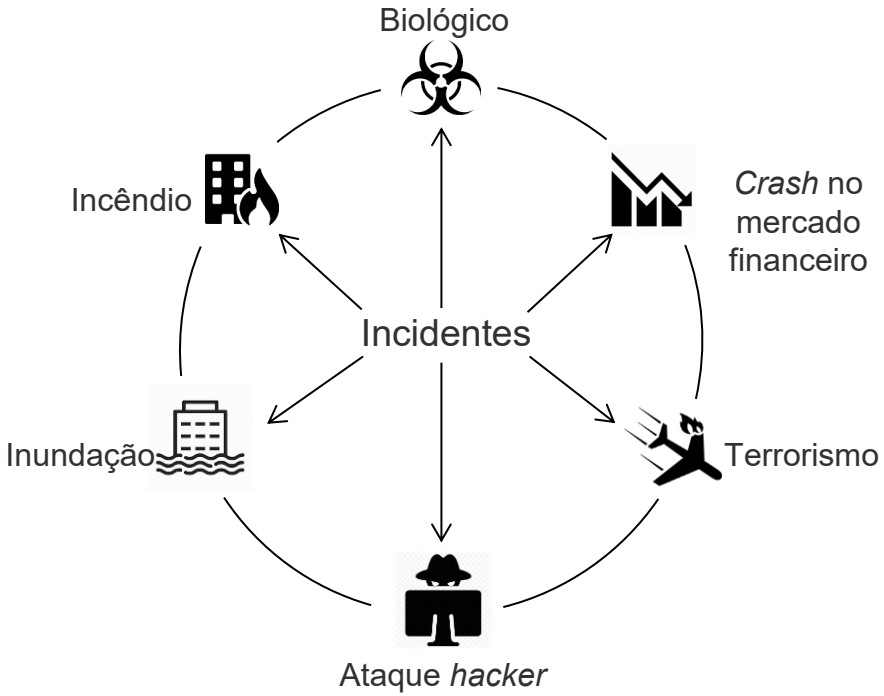
Sumário

Introdução e contexto

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Incidente e suas consequências

Segundo a ISO 22300, disrupção é um **incidente**, antecipado ou imprevisto, que resulta em **desvios negativos e não planejados** na entrega esperada de produtos e serviços. Veja a seguir alguns **exemplos de eventos disruptivos e suas consequências**:



- **São repentinos ou graduais e exigem ações imediatas**
- **Geram danos graves à segurança dos colaboradores, à reputação da organização e/ou aos seus resultados financeiros, e são originados por eventos não previstos ou negligenciados**
- **Independente do evento causador, podem afetar as operações de instituições de grande, médio ou pequeno porte**

Consequências

- Interrupção das operações
- Imagem da companhia comprometida por notícias
- Atrasos ou não entrega dos produtos e serviços aos clientes

Exemplos

Greve

UOL Notícias

Greve de ônibus em SP afeta 1,5 milhão de pessoas; confira empresas paradas

675 linhas diurnas, que operam 6.008 ônibus na capital paulista, estão paralisadas; Justiça prevê multa caso frota fique abaixo de 80% no...

https://noticias.uol.com.br/cotidiano/ultimas-noticias/2022/06/29/passageiros-enfrentam-frota-reduzida-de-onibus-em-meio-a-nova-greve.htm

Biológico

UOL Notícias

Futuras variantes do coronavírus podem enganar sistema imunológico, alertam USP e Sírio

"Decretar que a pandemia acabou e que o vírus foi vencido não é verdade", diz o líder do grupo de pesquisas em Bioinformática do Hospital...

https://noticias.uol.com.br/ultimas-noticias/agencia-estado/2022/04/26/pesquisa-da-usp-e-do-sirio-alerta-para-mais-variantes.htm

Ciberataque

Olhar Digital

Japão confirma ciberataque que fez parar 14 fábricas da Toyota no país

O porta-voz do governo do Japão, Hirokazu Matsuno, confirmou "um ciberataque" contra a fornecedora de peças Kojima Industries e declarou que a...

https://olhardigital.com.br/2022/03/01/seguranca/japao-confirma-ciberataque-que-fez-parar-14-fabricas-da-toyota-no-pais/

UOL

Após invasão, Renner diz que dados estão preservados; site segue fora do ar

Após ter sofrido um ataque cibernético nesta quinta-feira (19), o site e o aplicativo da varejista Lojas Renner seguiam indisponíveis na...

https://olhardigital.com.br/2022/03/01/seguranca/japao-confirma-ciberataque-que-fez-parar-14-fabricas-da-toyota-no-pais/

Crash no mercado financeiro

Exame

Com bitcoin em queda, empresas de mineração geram menos receita e veem suas ações despencarem

A queda nas ações de mineradoras listadas em bolsa pode estar ligada às suas receitas. Apenas no mês de maio, a receita gerada pela mineração de...

https://exame.com/future-of-money/com-bitcoin-em-queda-empresas-de-mineracao-geram-menos-receita-e-veem-suas-acoes-despencarem/

Incêndio

G1

Incêndio atinge indústria farmacêutica EMS em Hortolândia; imóveis no entorno foram evacuados

Um incêndio de grandes proporções atingiu a indústria farmacêutica EMS neste sábado (20), em Hortolândia (SP). Uma grande coluna de fumaça...

https://g1.globo.com/sp/campinas-regiao/noticia/2018/10/20/incendio-atinge-industria-farmaceutica-ems-em-hortolandia.ghtml

Ciberataque

O Globo

Guerra da Ucrânia: Brasil e outros 41 países foram alvo de ciberataques russos, diz Microsoft

... quarta-feira um relatório que indica que o Brasil e outros 41 países foram alvos de ciberataques russos durante o conflito na Ucrânia.

https://oglobo.globo.com/mundo/noticia/2022/06/guerra-da-ucrania-brasil-e-outros-41-paises-foram-alvo-de-ciberataques-russos-diz-microsoft.ghtml

Valor Econômico

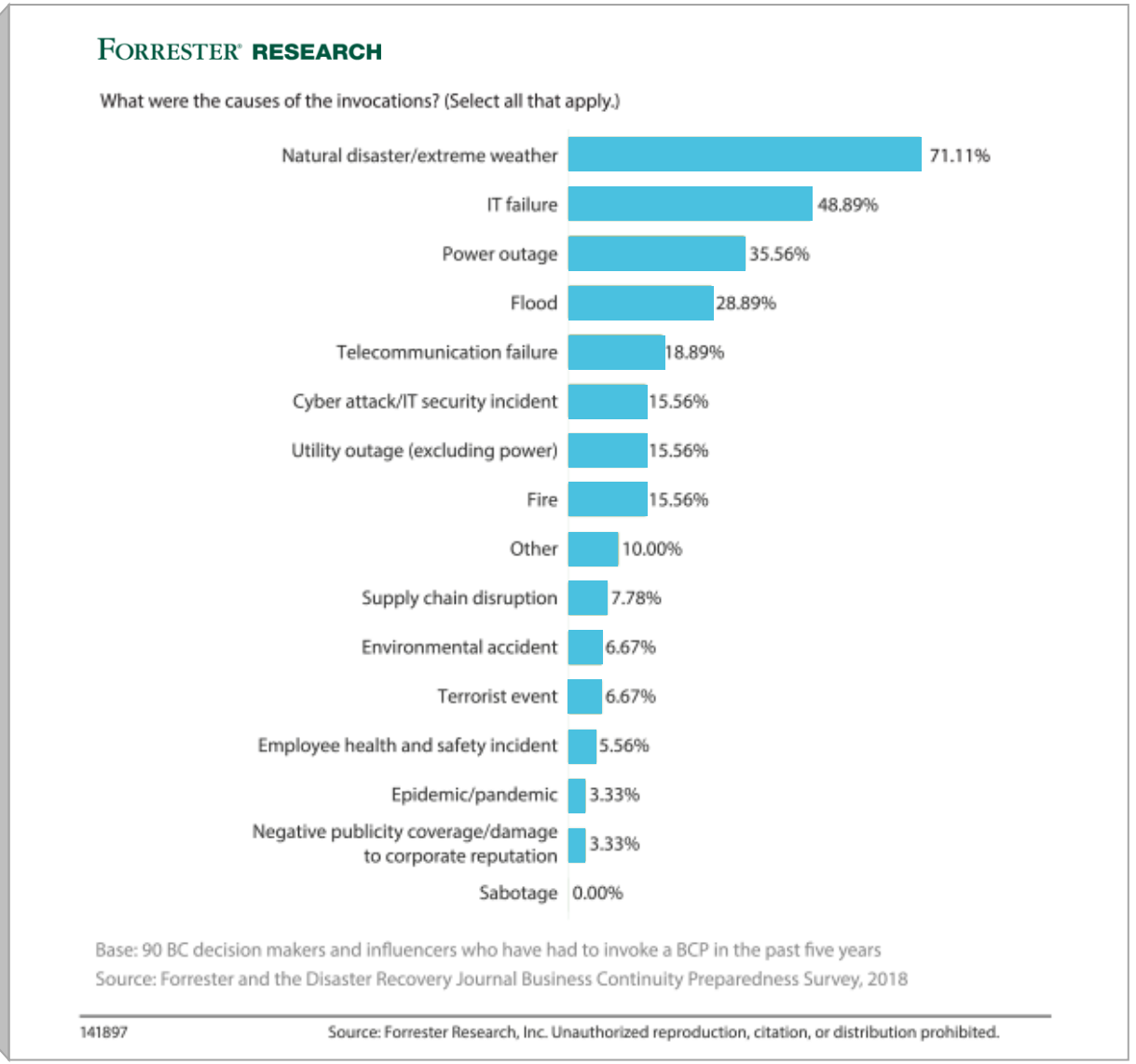
Mercado Livre sofre ataque de hackers; e-mail e telefone de 300 mil pessoas foram acessados

Depois da Renner e da Americanas, agora o Mercado Livre sofreu um ataque de hackers. A empresa relatou a invasão a seus sistemas, e o acesso...

https://valor.globo.com/empresas/noticia/2022/03/09/mercado-livre-sofre-ataque-de-hackers-e-mail-e-telefone-de-300-mil-pessoas-foram-acessados.ghtml

Principais causas de disrupções

Conforme estudo publicado pelo *Forrester Research*, o maior causador de indisponibilidade e impacto para as instituições está relacionado a **Desastres Naturais, seguido de falhas de TI**.



Gestão de continuidade x continuidade

GCN (Gestão de Continuidade de Negócios)

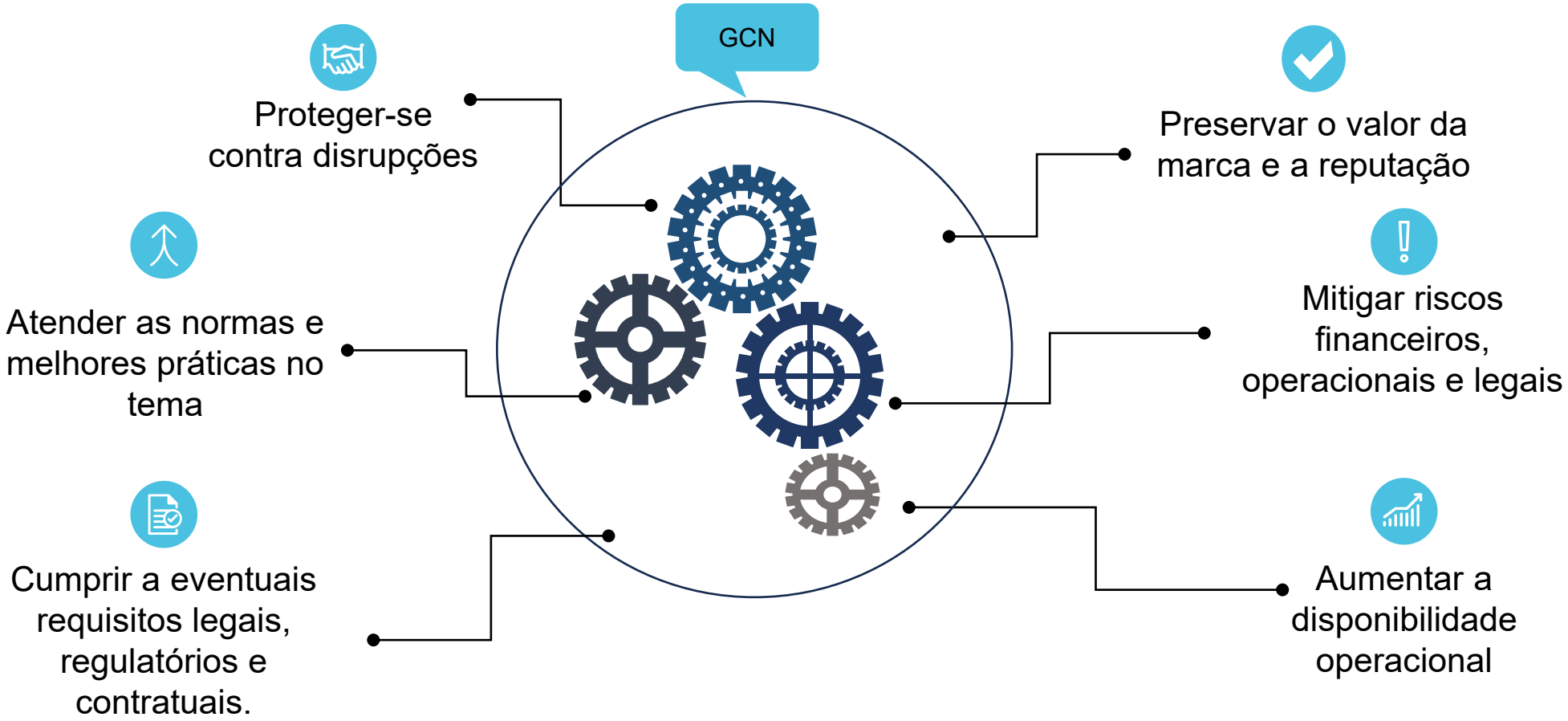
De acordo com a **ISO 22300** (*Security and resilience - Business continuity management systems*), **Gestão de Continuidade de Negócios** é o “processo de implementação e manutenção da continuidade de negócios”.

Continuidade de Negócios

De acordo com a **ISO 22300** (*Security and resilience - Business continuity management systems*), **Continuidade de Negócios** é a "capacidade de uma organização continuar a entrega de produtos e serviços em um nível aceitável com capacidade predefinida durante uma disrupção”.

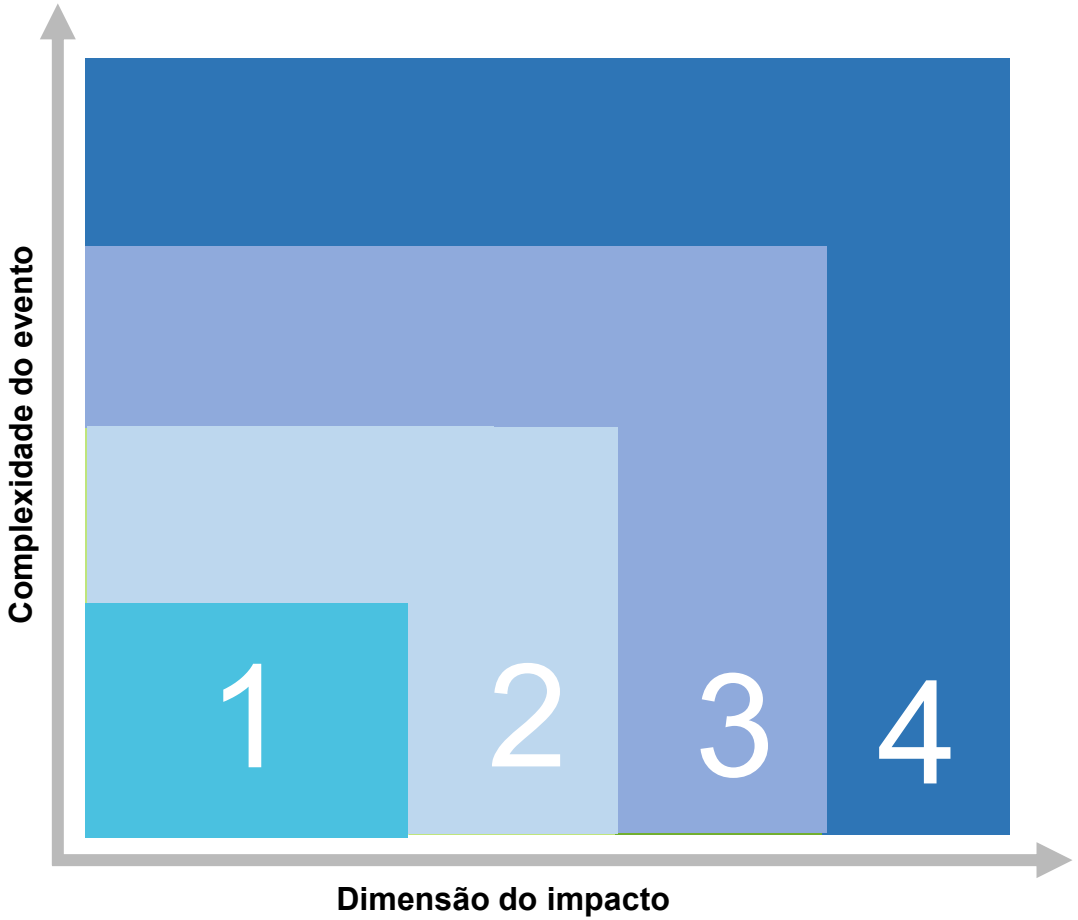
GCN e sua relevância

A Gestão de Continuidade de Negócios auxilia a:



Desafios enfrentados pelas Organizações

Categorização dos eventos



Crise

Grandes eventos com alto impacto negativo

Gestão de Crises

Incidente / Emergência

Situações específicas

Gestão de Continuidade de Negócios

Problema

Situações do dia a dia

Gestão de Riscos e Controles Internos

Situação normal

Por definição, as crises possuem alta complexidade para solução e grande dimensão de impacto. As crises muitas vezes exploram relevantes exposições das organizações, mas pode começar com pequenos eventos que combinados dificultam a resposta.

Exemplo - Impactos e Gatilhos de Acionamento

FEBRABAN

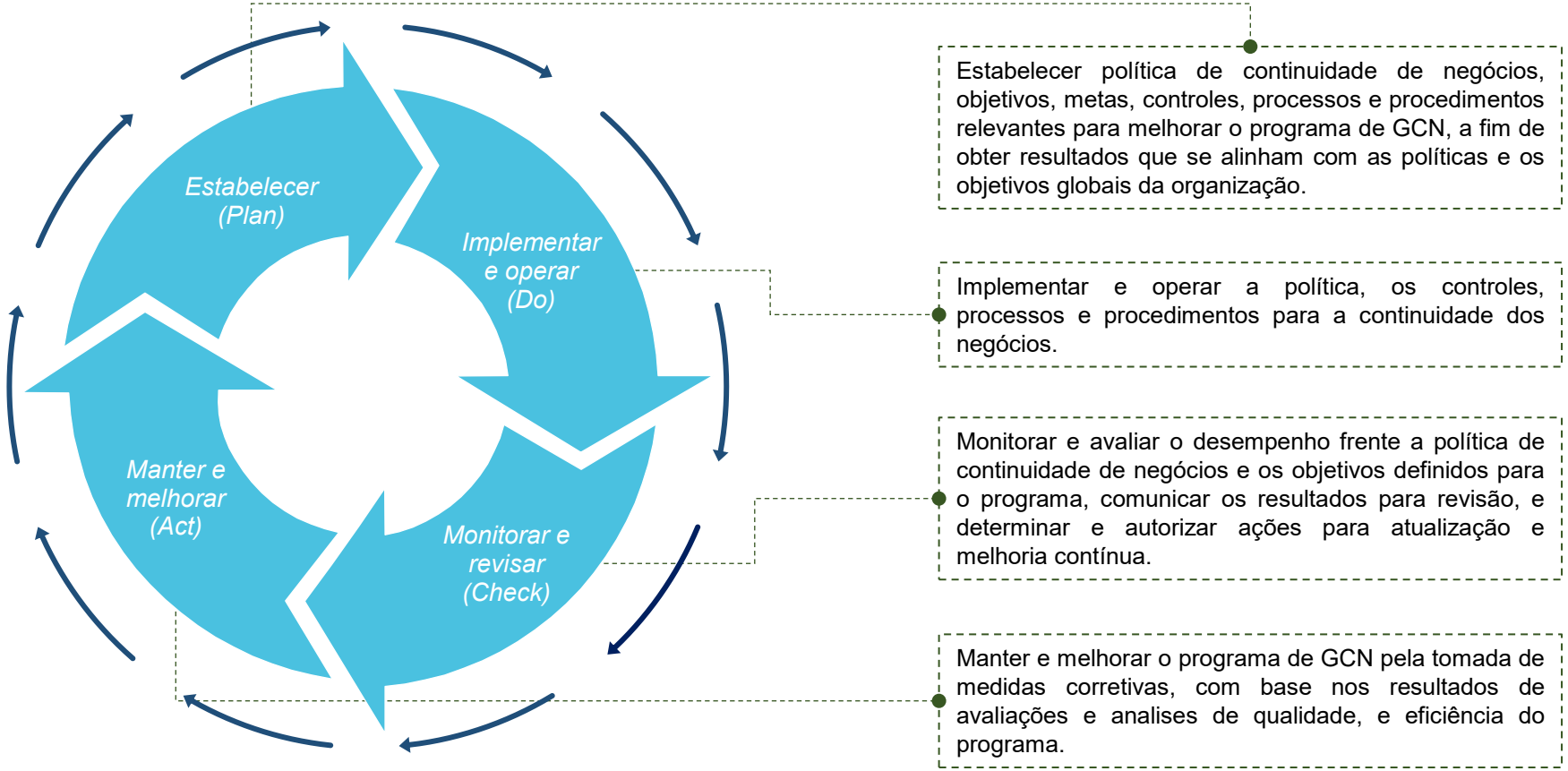
Dimensões	Muito baixo	Baixo	Médio	Alto	Muito alto
Imagem e reputação	O assunto tende a ficar limitado a poucos segmentos dos públicos de interesse na comunidade de influência da própria instalação	O assunto tende a ficar limitado aos públicos de interesse do meio na comunidade de influência da própria instalação, podendo repercutir regionalmente de forma pontual	O assunto tende a repercutir regionalmente e, de forma pontual, nacionalmente.	O assunto tende a repercutir nacionalmente e, de forma pontual, internacionalmente.	O assunto tende a ganhar alta repercussão nacional e internacionalmente.
Legal/ conformidade	Não há violações de questões contratuais ou regulatórias. Ponto de auditoria interna de baixo risco com penalidades aplicadas a certificações externas nulo.	As violações contratuais estão confinadas a incidentes isolados e sem geração de multas ou custos. Alerta ou ponto de atenção de auditoria externa com penalidades aplicadas à empresa de forma moderada e impacto em certificações externas baixo.	Presença de violações de questões regulatórias ou obrigações contratuais que acarretam no aumento das inspeções, observações e apontamentos do regulador. Ponto de auditoria interna e/ou externa relevante com penalidades aplicadas à empresa e impacto em certificações significativas.	Suspensão ou interdição parcial das atividades por órgãos de controle ou reguladores nacionais e internacionais. Impacto nas certificações externas significativo. Potencial de litígios de impacto relevante.	Suspensão total das atividades por órgãos de controle ou reguladores nacionais e internacionais. Impedimento para obtenção de certificações externas. Restrições ou grande potencial de litígio de grandes proporções aos negócios.
Financeira	Impacto desprezível na continuidade da cadeia produtiva, no atendimento ao mercado ou no resultado financeiro da empresa. Danos leves a equipamentos, sem comprometimento da continuidade operacional.	Impacto marginal na continuidade da cadeia produtiva, no atendimento ao mercado financeiro ou no resultado financeiro da empresa. Danos leves à sistemas e seus equipamentos, com baixo comprometimento da continuidade operacional.	Impacto médio na continuidade da cadeia produtiva, no atendimento ao mercado ou no resultado financeiro da empresa. Danos moderados a sistemas e seus equipamentos, com médio comprometimento da continuidade operacional.	Impacto crítico na continuidade da cadeia produtiva, no atendimento ao mercado ou no resultado financeiro da empresa. Danos severos a sistemas e seus equipamentos, com reparo lento, com alto comprometimento da continuidade operacional.	Impacto catastrófico na continuidade da cadeia produtiva, no atendimento ao mercado ou no resultado financeiro da empresa. Danos catastróficos a sistemas, podendo levar a perda da instalação, com muito alto comprometimento da continuidade operacional.
Acionamento					

Programa de GCN

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Ciclo de vida

Estão estruturadas em linha na metodologia ISO 22301 – Sistema de Gestão de Continuidade dos Negócios, que possui como Método de Gestão o modelo PDCA – Plan, Do, Check e Act.



Ciclo de vida do Sistema

de Gestão de Continuidade dos Negócios

Visão geral

Modelo de Governança de Continuidade de Negócios e TI

Definir o escopo e as prioridades para a Gestão de Continuidade de Negócios e TI

Análise de Impacto nos Negócios (*BIA*)

Priorizar os processos e os recursos críticos (instalações, pessoas, sistemas e fornecedores) na visão de disponibilidade considerando os impactos ao negócio (imagem, legal, financeiro e operacional)

Treinamento e Teste

Coordenar rotinas de testes das estratégias de continuidade de tecnologia da informação, identificando desvios, atualizações dos planos e níveis de prontidão para contingência

Análise de Riscos de Continuidade

Analisar possíveis ameaças que a Companhia pode estar exposta, verificando vulnerabilidades dos principais elementos relacionados à TI, instalações, fornecedores e colaboradores

Planos de Continuidade

Acompanhar, formalizar e prestar suporte implantação das estratégias de continuidade de Negócios e TI, bem como elaboração e aprovação dos planos

Estratégias de Continuidade de Negócios e TI

Definir estratégias e soluções de continuidade tecnológica para os processos críticos da Companhia, de acordo com os cenários de indisponibilidade definidos

Abordagem e metodologia

Etapas de um SGCN

1 Governança em GCN | 2 | 3 | 4 | 5 | 6 | 7

Objetivo: Introduzir governança ao programa de continuidade dos negócios, definindo os relacionamentos entre as áreas, os papéis e responsabilidades e as partes interessadas, para garantir a manutenção da GCN na organização.

Assuntos abordados e tratados

- Análise com base no **planejamento estratégico** para delimitar objetivos e possíveis planos de ação
- Avaliação de **políticas, normas e procedimentos** existentes
- Análise das capacidades de **monitoramento** implementadas
- Entendimento do processo e organização de ***compliance*** existentes
- Entendimento da **alocação e investimento de capital da companhia**
- Análise da estrutura organizacional e definição de **lideranças** quanto ao tema de GCN

Resultam

- **Política de GCN**
- **Modelo de Gestão de GCN**

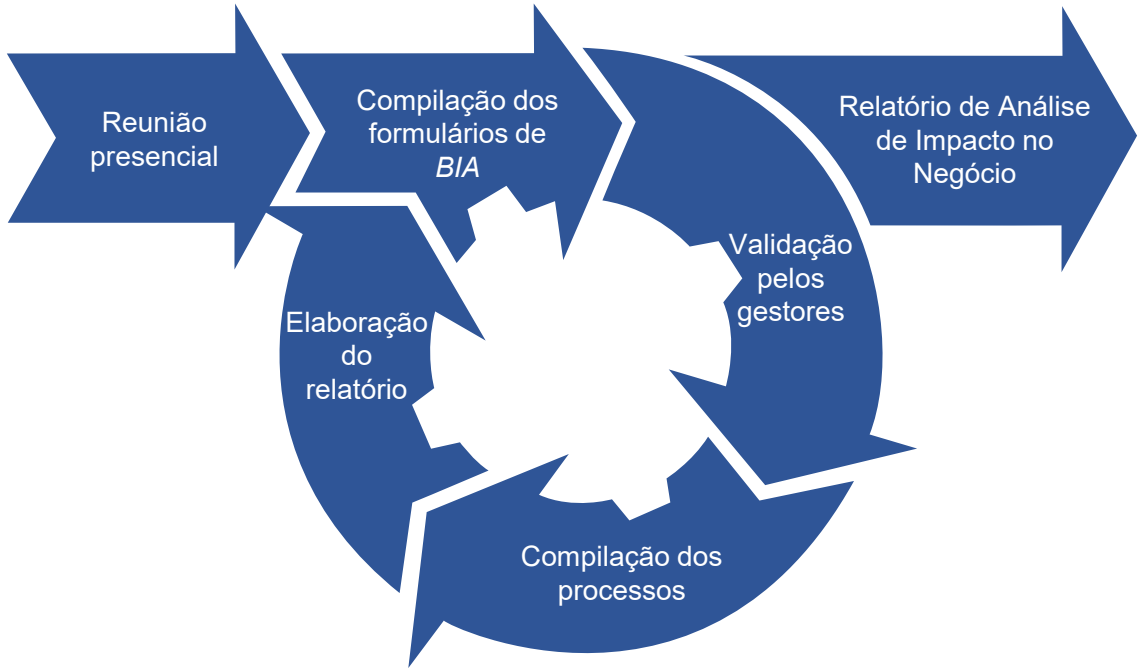
Abordagem e metodologia

Etapas de um SGCN

1 2 **Análise de Impacto nos Negócios (BIA)** 3 4 5 6 7

Objetivo: Desenvolver o entendimento e análise de criticidade dos processos de negócio, a fim de realizar a priorização daqueles mais críticos em caso de interrupção da organização.

Abordagem utilizada



Aspectos avaliados na Análise de Impacto no Negócio (*BIA*)

- **Análise do tempo máximo de indisponibilidade (*RTO*)** dos processos das áreas de negócios
- **Sistemas críticos** necessários para manter a operação, bem como seus ***RTOs*** e ***RPOs*** **(tempo máximo de perda de dados)**
- **Quantidade mínima de profissionais** que atuarão em estado de contingência e **centralização de conhecimento** em pessoas específicas
- Existência de cláusulas de ***Service Level Agreement*** (*SLA*), **Cláusulas de Gestão de Continuidade de Negócio** (GCN) e **fornecedores alternativos**
- **Interdependência** entre os processos de negócios e suas necessidades para continuidade das atividades
- **Níveis de impactos** (financeiro, imagem, legal e operacional) ocasionados pela indisponibilidade dos processos

Assim como mencionado no CMN n° 4893 – cap. II – seção I – § 3º - Art. 3º - inciso IV

Abordagem e metodologia

Etapas de um SGCN

1 2 3 **Análise de Riscos** 4 5 6 7

Objetivo: Analisar e avaliar possíveis ameaças que a empresa pode submeter-se, tais como a possibilidade de ocorrência e sua vulnerabilidade, através da verificação dos principais elementos como TI, pessoas, fornecedores e instalações.

Controles avaliados nas instalações físicas

- Avaliação das instalações relacionada a **controles de acessos, licenças, segurança física e patrulhamento**
- **Controles de ambiente** avaliando a redundância de ar condicionado e manutenção preventiva
- **Sistema de extinção de incêndios**, detectores de fumaça, extintores, alarmes, procedimentos, testes e manutenções periódicas
- Manutenção da **energia elétrica**, autonomia de geradores, *no-breaks*, testes e manutenções periódicas dos equipamentos, aterramento e para-raios
- Análise do **monitoramento** existentes nos acessos às dependências das Unidades e tempo a retenção de imagens

Nível de vulnerabilidade das instalações

+

Nível de impacto dos processos

Assim como mencionado no CMN nº 4893 – Seção III - Art. 20 - I

Abordagem e metodologia

FEBRABAN

Etapas de um SGCN

1 2 3 4 **Estratégias e Soluções de GCN** 5 6 7

Objetivo: Definir estratégias e soluções de continuidade para os serviços críticos de negócio e TI da organização, considerando as priorizações da análise de impacto nos negócios, avaliação de riscos e diretrizes da organização.

Possíveis investimentos em equipamentos de TI ou infraestrutura para áreas de negócio

Dependência de colaboradores terceiros

Mapeamento do deslocamento de colaboradores e atividades

Assim como mencionado no CMN nº 4893 – Seção III - Art. 6º - I e II, Art. 16º IV.

Abordagem e metodologia

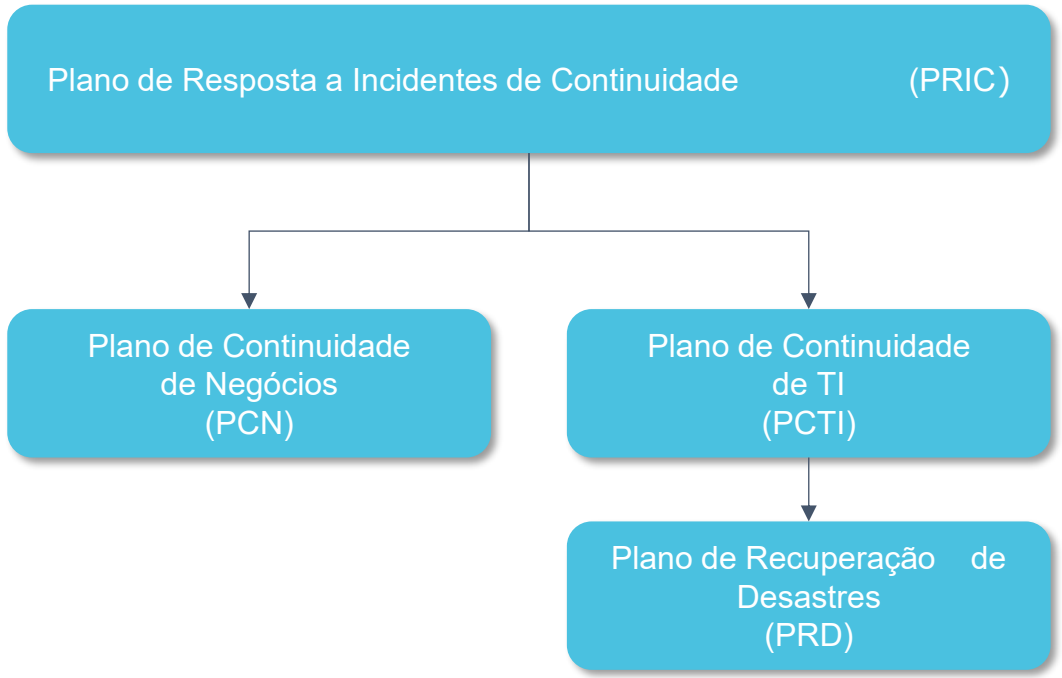
Etapas de um SGCN

1 2 3 4 **5 Planos e Procedimentos** 6 7

Objetivo: Documentar as estratégias de recuperação de desastres e continuidade dos negócios, em procedimentos estratégicos, táticos e operacionais considerando as ações de contingência para pessoas, processos e infraestrutura tecnológica.

Principais pontos documentados

- Aspectos práticos no **acionamento** e **execução** da contingência
- Pontos focais para a **tomada de decisões** quanto a resposta a incidentes de continuidade
- Atividades a serem **priorizadas** e **colaboradores chave** responsáveis pela restauração e recuperação das operações
- Fluxo de **deslocamento** de colaboradores e atividades
- Procedimentos para **preparação, operação, entrada, retorno** da contingência e **validação** quanto a infraestrutura tecnológica



Abordagem e metodologia

Etapas de um SGCN

1 2 3 4 5 **6 Treinar e Testar** 7

Objetivo: Conscientização dos colaboradores envolvidos na gestão, acionamento e operacionalização das estratégias de recuperação de desastres e continuidade dos negócios com o objetivo de garantir que em caso de necessidade de acionamento, as estratégias definidas atendam aos objetivos definidos e acordados com a organização.

Principais pontos abordados nos treinamentos

- Divulgação e equalização de conceitos e práticas adotadas em função da gestão de continuidade
- Abordagem de acordo com as estratégias definidas pela organização
- Garantir a compreensão dos procedimentos e planos documentados
- Avaliação do nível de conscientização dos colaboradores

Principais pontos avaliados nos testes

- Avaliar recursos e cenários de indisponibilidade conforme estratégia de contingência estabelecida
- Avaliar tempos de resposta, prática dos colaboradores e procedimentos
- Atingir os objetivos definidos para o teste
- Identificar não conformidades do plano e acionar fluxo de tratamento e melhoria dos mesmos

Assim como mencionado no CMN nº 4893 – Cap. II – Seção I – Art. 3º - V, Art. 8º - IV e Art. º 19 - III

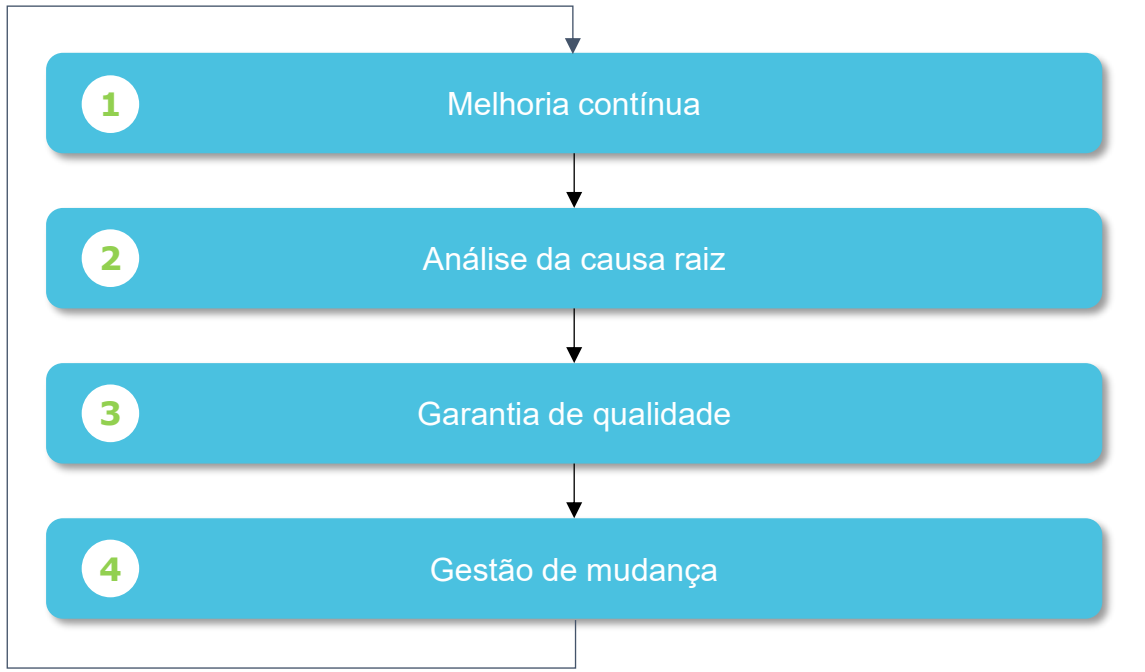
Abordagem e metodologia

Etapas de um SGCN

1 2 3 4 5 6 7 **Melhoria Contínua**

Objetivo: Desenvolver o modelo de gestão, processos e procedimentos para garantir que o programa de continuidade dos negócios torne-se dinâmico e atenda às necessidades da organização.

Abordagem utilizada



- Implementação de papéis, responsabilidades e processos que endereçam o ciclo do programa de continuidade de negócios
- Corrigir desvios observados nas fases do SGCN e implementar melhorias de processo através da criação de planos de ação
- Indicar que os planos de ação sejam implementados de forma completa de acordo com a gestão de mudança

Assim como mencionado no CMN nº 4893 – Cap. II – Seção III – Art. 10 e Seção I - § 3º - Art. 3º - VI - c

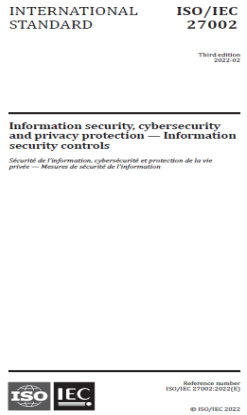
Considerações Finais

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Frameworks e normas de referência

Para apoiar no entendimento e implementação de toda a metodologia apresentada neste material, a seguir são apresentados as normas e frameworks de referência no tema:

Frameworks Padrão Utilizados



International Organization for Standardization
ISO
22301

NIST
National Institute of Standards and Technology

Conformidade: Dado o uso extensivo de padrões amplamente aceitos pela indústria, a continuidade dos negócios deve ser alinhada com alguns dos requisitos de conformidade mais exigentes, permitindo estimar o nível de conformidade com NIST, ISO, Bacen 4.893, DRI, entre outros.

Relembrando os principais conceitos

Agora que aprendemos sobre as atividades relacionadas ao processo de gestão de continuidade de negócios, relembre os principais termos e conceitos apresentados neste material:

Disrupção: é um incidente, antecipado ou imprevisto, que resulta em desvios negativos e não planejados na entrega esperada de produtos e serviços. Veja a seguir alguns exemplos de eventos disruptivos e suas consequências:.

Continuidade dos Negócios: capacidade de uma organização continuar a entrega de produtos e serviços em um nível aceitável com capacidade predefinida durante uma disrupção.

Análise de Impacto nos Negócios (BIA): avaliar possíveis ameaças que a empresa pode submeter-se, tais como a possibilidade de ocorrência e sua vulnerabilidade, através da verificação dos principais elementos como TI, pessoas, fornecedores e instalações.

Plano de Continuidade (PCN): documenta as estratégias de recuperação de desastres e continuidade dos negócios, em procedimentos estratégicos, táticos e operacionais considerando as ações de contingência para pessoas, processos e infraestrutura tecnológica.

Treinamentos e testes: conscientizar dos colaboradores envolvidos na gestão, acionamento e operacionalização das estratégias de recuperação de desastres e continuidade dos negócios com o objetivo de garantir que em caso de necessidade de acionamento, as estratégias definidas atendam aos objetivos definidos e acordados com a organização.

Módulo: Segurança Física

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

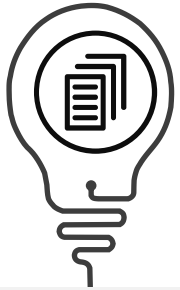
Requisitos – Segurança Física

Este material foi elaborado de acordo com as diretrizes da ISO 27002, bem como foram considerados os requisitos de segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

ISO 27002

- 7.1 Perímetros de segurança física
- 7.2 Entrada física
- 7.3 Segurança de escritórios, salas e instalações
- 7.4 Monitoramento de segurança física
- 7.5 Proteção contra ameaças físicas e ambientais
- 7.6 Trabalhando em áreas seguras
- 7.7 Limpar mesa e limpar tela

PCI DSS



- 9.1 Os processos e mecanismos para restringir o acesso físico aos dados do titular são definidos e compreendidos.
- 9.2 Os controles de acesso físico gerenciam a entrada em instalações e sistemas que contêm dados do titular do cartão.
- 9.3 O acesso físico para pessoal e visitantes é autorizado e gerenciado.
- 9.4 A mídia com os dados do titular do cartão é armazenada, acessada, distribuída e destruída com segurança.
- 9.5 Dispositivos de ponto de interação (POI) são protegidos contra adulteração e substituição não autorizada.

ISO 27701

- 6.8.1.1 Perímetro de segurança física
- 6.8.1.2 Controles de entrada física
- 6.8.1.3 Segurança em escritórios, salas e instalações
- 6.8.1.4 Proteção contra ameaças externas e do meio ambiente
- 6.8.1.5 Trabalhando em áreas seguras
- 6.8.1.6 Áreas de entrega e de carregamento

NIST CSF

- PR. AA-06: O acesso físico aos ativos é gerenciado, monitorado e aplicado proporcionalmente ao risco
- CM-02: O ambiente físico é monitorado para encontrar eventos potencialmente adversos

Sumário

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Sumário

Introdução

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Casos reais

INNOVATION • CYBERSECURITY

Toyota Parts Supplier Hit By $37 Million Email Scam

On August 14th, attackers managed to convince someone with financial authority to change account information on an electronic funds transfer. Both Toyota Boshoku Corporation and its subsidiary have been in contact with law enforcement officials and an investigation is under way.

Panrotas
https://www.panrotas.com.br › Hotelaria › Tecnologia

Dados de hotel da Marriott nos Estados Unidos são violados

8 de jul. de 2022 — Por meio do computador desse indivíduo, o grupo conseguiu exfiltrar **20 GB** de dados. A **Marriott** minimizou a importância da violação, afirmando à ...

Hotel Marriott: um grupo de hacking utilizou tácticas de engenharia social para roubar 20 GB de dados pessoais e financeiros de um Hotel Marriott. Os hackers enganaram um associado do Hotel Marriott para dar ao grupo de hacking acesso ao computador do associado.

Metrópoles

Vídeo: criminosos deixam rastro de explosivos após roubo a banco em SP

Equipe do Gate desativa explosivos após roubo à banco ... Por volta das 4h desta segunda-feira, a Polícia Militar foi acionada após alguns...

8 de abr. de 2024

g1 - O portal de notícias da Globo

Galpão pega fogo e chamas destroem parte dos materiais em empresa em Jacareí

Galpão pega fogo e chamas destroem parte dos materiais em empresa em Jacareí · De acordo com o Corpo de Bombeiros, o incêndio aconteceu por...

25 de fev. de 2024

Introdução

Segundo a ISO 27002, a segurança física ajuda a **prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e as informações da organização.**

Principais controles de segurança física:

Perímetro de segurança física

Perímetros definidos e usados para proteger tanto as áreas que contenham as instalações de processamento da informação como as informações críticas ou sensíveis

Monitoramento e vigilância

Sistemas de vigilância, que podem incluir guardas, alarmes de intrusão, sistemas de monitoramento de vídeo

Controle de acesso físico

Controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido

Proteção de equipamentos e infraestrutura

Proteção dos ativos contra falta de energia elétrica e outras interrupções, além de proteger o cabeamento de energia e telecomunicações que transporta dado ou dá suporte aos serviços, além de outros ativos utilizados pelos funcionários

Segurança Física

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Perímetro de segurança física

Segundo a ISO 27002, os perímetros de segurança precisam ser **definidos e usados para proteger tanto as áreas que contenham as instalações de processamento da informação como as informações críticas ou sensíveis**. Exemplos de controles:

Os **perímetros de segurança** precisam ser **claramente definidos** e que a localização e a capacidade de resistência de cada perímetro dependam dos requisitos de segurança dos ativos.

Sistemas adequados **de detecção de intrusos** são **instalados e testados em intervalos regulares**, e cubram todas as portas externas e janelas acessíveis.

É importante que os perímetros de um local que contenha as instalações de processamento da informação **não tenham brechas**.

Portas corta-fogo do perímetro de segurança sejam **providas de alarme, monitoradas e testadas juntamente com as paredes.**

Área de recepção, ou um outro meio para controlar o acesso físico ao local para **apenas pessoas autorizadas** entrar.

Barreiras físicas são importantes para **impedir** o **acesso físico não autorizado** e a contaminação do meio ambiente.

Monitoramento e Vigilância

Segundo a ISO 27002, **as instalações devem ser continuamente monitoradas quanto a acesso físico não autorizado**.

É importante as **instalações físicas serem monitoradas** por **sistemas de vigilância**, que podem incluir **guardas**, **alarmes de intrusão**, **sistemas de monitoramento de vídeo**, como circuito fechado de televisão, e software de gerenciamento de informações de segurança física gerenciado internamente ou por um provedor de serviços de monitoramento.

1 CFTV (Circuito Fechado de televisão)

- Sistema de **monitoramento** interno que consiste em **câmeras distribuídas** e conectadas a uma determinada central onde as **imagens são registradas, gravadas e disponibilizadas** através de monitores.
- Permite **avaliações comportamentais**, monitoramento de vias, monitoramento familiar, avaliação de ambientes altamente críticos ao ser humano, fenômenos ambientais, segurança do trabalho, entre outros.
- **Visualizar e registrar** o acesso a áreas sensíveis dentro e fora das instalações de uma organização
- Permite o **monitoramento em tempo real**.

2 Detector de Intrusão

- Instalar, de acordo com as normas aplicáveis pertinentes, e testar **periodicamente detectores de contato, som ou movimento** para acionar um alarme de intrusão**.**
- **Detectores de movimento baseados em tecnologia infravermelha** que disparam um alarme quando um objeto **passa por seu campo de visão.**
- Instalação de **sensores sensíveis ao som** de vidros quebrando que **podem ser usados para acionar um alarme** para alertar a segurança.
- Usar esses alarmes para **cobrir todas as portas externas e janelas acessíveis**. As áreas desocupadas devem ser alarmadas o tempo todo; deve também ser prevista cobertura para outras áreas.

Controles de entrada física

Segundo a ISO 27002, **áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.**

01 A **data e hora da entrada e saída de visitantes** sejam **registradas**, e todos os visitantes sejam **supervisionados**, a não ser que o seu acesso tenha sido previamente aprovado; as permissões de acesso só sejam concedidas para finalidades específicas e autorizadas.

02 **O acesso às áreas** em que são **processadas** ou **armazenadas informações sensíveis** seja **restrito apenas ao pessoal autorizado**

03 Trilha de auditoria eletrônica ou um livro de registro físico de todos os **acessos seja mantida e monitorada de forma segura**

04 O **acesso restrito** às áreas seguras ou as instalações de processamento da informação sensíveis sejam concedidos, somente quando necessário; este acesso seja **autorizado e monitorado**.

05 **Os direitos de acesso** a áreas seguras sejam **revistos e atualizados em intervalos regulares, e revogados quando necessário**

Segurança em escritórios, salas e instalações

Segundo a ISO 27002, **é necessário projetar e aplicar a proteção física contra desastres naturais, ataques maliciosos ou acidentes** para **proteger** os escritórios, salas e instalações e os profissionais trabalharem em áreas seguras.

1. Instalações-chave devem ser localizadas de maneira a **evitar o acesso do público**.
2. Instalações devem ser projetadas para **evitar que as informações confidenciais ou as atividades sejam visíveis e possam ser ouvidas da parte externa**.
3. **Não permitir** o uso de máquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, tais como câmeras em dispositivos móveis, **salvo se for autorizado**.
4. **Orientações de especialistas sejam obtidas sobre como evitar danos** oriundos de fogo, inundação, terremoto, explosão, manifestações civis e outras formas de desastre natural ou provocado pela natureza.
5. Conhecimento da existência de áreas seguras ou das atividades nelas realizadas, **apenas se for necessário**
6. Áreas seguras, não ocupadas, sejam **fisicamente trancadas e periodicamente verificadas**

Áreas de entrega e de carregamento

Segundo a ISO 27002, **os pontos de acesso**, tais como **áreas de entrega e de carregamento** e outros pontos em que pessoas não autorizadas possam entrar nas instalações, **devem ser controlados e, se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado**.

- Acesso a uma área de entrega e carregamento a partir do exterior do prédio fique **restrito ao pessoal identificado e autorizado**.
- Áreas de entrega e carregamento devem ser projetadas de tal maneira que seja possível **carregar e descarregar suprimentos sem que os entregadores tenham acesso a outras partes do edifício.**
- As portas externas de uma área de entrega e carregamento devem ser **protegidas enquanto as portas internas estiverem abertas**.
- Os materiais entregues devem ser **inspecionados e examinados** para detectar a presença de explosivos. Os materiais entregues devem ser **registrados de acordo com os procedimentos de gerenciamento de ativos**.
- As remessas entregues devem ser **segregadas fisicamente das remessas que saem**, sempre que possível.
- Os materiais entregues devem ser **inspecionados para evidenciar alteração indevida**. Caso alguma alteração indevida seja descoberta, ela deve ser **imediatamente notificado ao pessoal da segurança**.

Escolha do local e proteção do equipamento

Segundo a ISO 27002, **os equipamentos precisam ser colocados em local ou protegidos para reduzir os riscos de ameaças e perigos do meio-ambiente**, bem como as oportunidades de acesso não autorizado.

Os equipamentos devem ser colocados no local, a fim de **minimizar o acesso desnecessário** às áreas de trabalho

As instalações de processamento da informação que manuseiam dados sensíveis devem ser posicionadas cuidadosamente para **reduzir o risco** de que as informações sejam vistas por pessoal não autorizado durante a sua utilização.

É **necessário diretrizes** quanto a comer, beber e fumar nas proximidades das instalações de processamento da informação

Todos os edifícios devem **possuir proteção** contra raios e todas as linhas de entrada de força e de comunicações tenham **filtros de proteção** contra raios

Condições ambientais, como temperatura e umidade, devem ser **monitoradas para a detecção de condições que possam afetar negativamente** as instalações de processamento da informação

Os equipamentos que processam informações sensíveis **devem ser protegidos**, a fim de minimizar o risco de vazamento de informações em decorrência de emanações eletromagnéticas

Boas Práticas para Utilidades

FEBRABAN

Segundo a ISO 27002, **é necessário proteger as utilidades contra falta de energia elétrica e outras interrupções**, além de **proteger o cabeamento de energia e telecomunicações** que transporta dado ou dá suporte aos serviços.

1. É necessário conformidade com as **especificações do fabricante** do equipamento e com os requisitos legais da localidade.
2. É necessário que as utilidades sejam **avaliadas regularmente** quanto á sua capacidade para atender ao crescimento do negócio e ás interações com outras utilidades.
3. É necessário alarmes para **detectar mau funcionamento**, quando necessário.
4. É necessário **múltiplas alimentações** com rotas físicas diferentes..
5. É recomendado que as linhas de energia e de telecomunicações que entram nas instalações de processamento da informação sejam **subterrâneas**.
6. Os cabos de energia precisam ser **segregados** dos cabos de comunicações, para **evitar interferências**

Manutenção dos equipamentos

Segundo o ISO 27002, **é necessário que os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade permanente.**

- A manutenção dos equipamentos seja realizada nos **intervalos recomendados** pelo fornecedor e de acordo com as suas especificações.
- A manutenção e os consertos dos equipamentos só sejam realizados por **pessoal de manutenção autorizado**.
- É necessário **manter registros** de todas as falhas, suspeitas ou reais, e de todas as operações de manutenção preventiva e corretiva realizadas.
- É necessário a implementação de controles apropriados, na época programada para **a manutenção do equipamento**, dependendo da manutenção ser **realizada pelo pessoal local ou por pessoal externo** à organização; onde necessário, **informações sensíveis sejam eliminadas do equipamento.**
- **Antes de colocar o equipamento em operação, após a sua manutenção, é necessário realizar inspeção** para garantir que o equipamento não foi alterado indevidamente e que não está em mau funcionamento.

Segurança externa dos ativos

Segundo a ISO 27002, **os ativos não podem ser retirados das dependências sem a autorização prévia**, e quando forem operados fora do local, é necessário levar em conta os diferentes riscos e **tomar medidas para utilizar os ativos em segurança**.

Os controles para as localidades fora das dependências da organização, como, o trabalho em casa e localidades remotas e temporárias, **devem ser determinados por uma avaliação de riscos, devendo ser aplicados controles adequados.**

Quando o equipamento fora das dependências da organização é transferido entre diferentes pessoas ou partes externas, convém que seja mantido um **registro para definir a cadeia de custodia do equipamento**.

O Shoulder Surfing é uma das táticas utilizadas na Engenharia Social para **obter informações**, consiste no atacante se posicionar de maneira que seja **possível observar as informações** do alvo, geralmente por cima de seu ombro.

Os equipamentos e mídias removidos das dependências da organização **não devem ficar sem supervisão em lugares públicos.**

É necessário a documentação da identidade, atribuição e função de qualquer pessoa que manuseia ou utiliza os ativos, e que esta **documentação seja devolvida com o equipamento**, a informação ou software.

Sempre que necessário ou apropriado, é recomendado que seja feito um **registro da retirada e da devolução de ativos**, quando do seu retorno.

É necessário a identificação dos funcionários, fornecedores e partes externas tenham **autoridade para permitir a remoção de ativos para fora do local**

Comportamento Individual

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

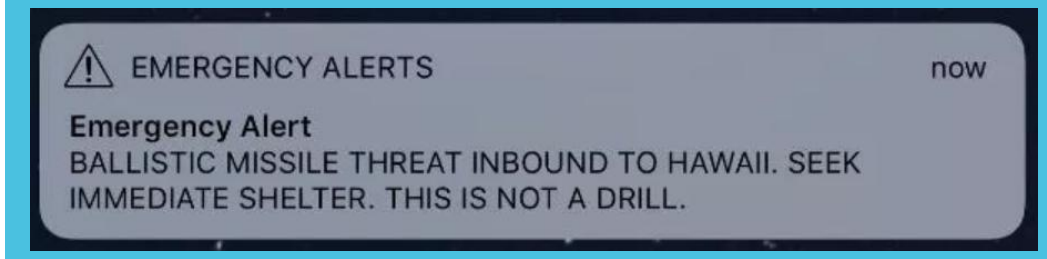
Exemplo - Cenário de Risco

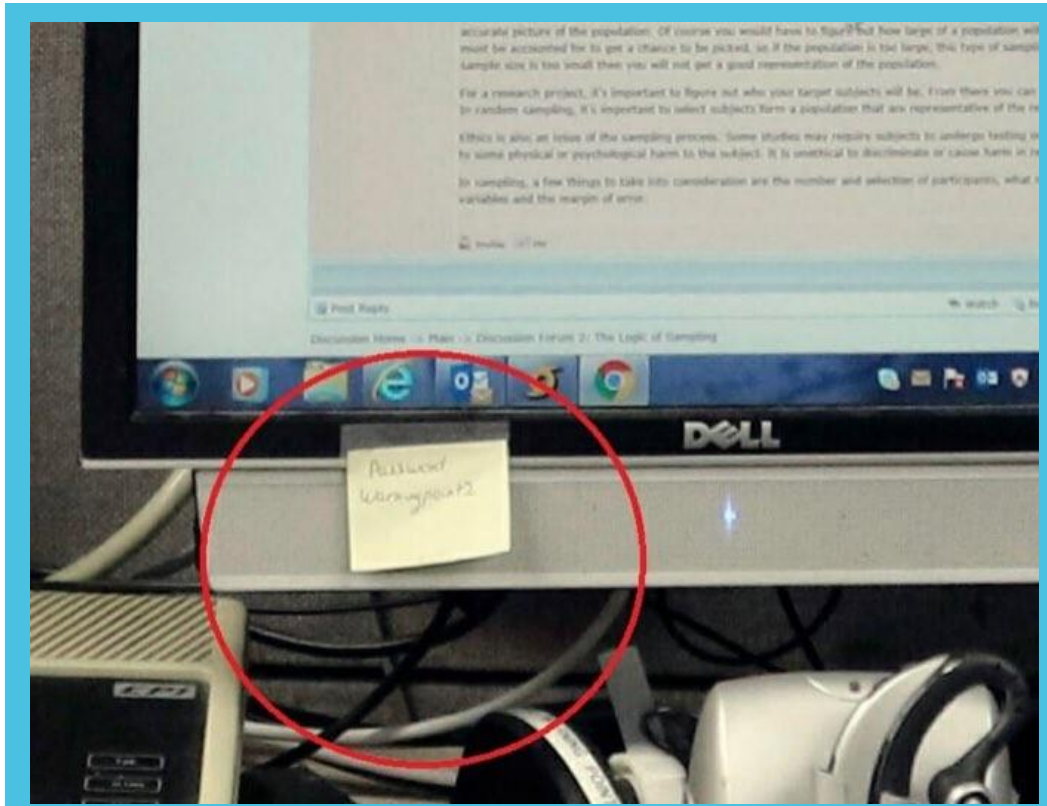
Segundo o PCI, **os dados do titular estão sujeitos à visualização, cópia ou digitalização não autorizada se estiverem desprotegidos** enquanto estiverem em uma mídia removível ou portátil, impressos ou deixados na mesa de alguém.

Política de mesa limpa e tela limpa

Um caso real relacionado à política de mesa limpa envolveu a agencia de gerenciamento de emergências do Havaí em 2018 onde a população do estado recebeu um alerta de ameaça de míssil, solicitando busca por abrigo com urgência.

Porém o caso não passou de uma falha humana. Logo algumas pessoas na internet notaram uma foto compartilhada um ano antes do acontecimento onde aparecia um **post-it com a senha e usuário de acesso ao sistema, colado à tela do computador que monitorava esse tipo de ameaça.**





Política de mesa limpa e tela limpa

Segundo o PCI, **os dados do titular estão sujeitos à visualização, cópia ou digitalização não autorizada se estiverem desprotegidos** enquanto estiverem em uma mídia removível ou portátil, impressos ou deixados na mesa de alguém.

Para reduzir os riscos de acesso não autorizado, perda ou danos as informações internas e confidencias durante e fora do horário de expediente, os colaboradores e terceiros devem seguir os critérios abaixo:

- ✓ Ao final do dia, ou no caso de ausência prolongada, **limpar a mesa de trabalho**;
- ✓ Informações Internas e Confidenciais devem ser mantidas em **local apropriado**;
- ✓ **Os papéis ou mídias de computador** não devem ser deixados sobre as mesas, quando não estiverem sendo usados devem ser guardados de maneira adequada para minimamente **evitar fácil acesso**.
- ✓ Sempre que não estiver utilizando o computador **não deixar nenhum arquivo aberto**, de modo que as informações possam ser visualizadas por outras pessoas que estiverem no setor;
- ✓ As chaves de gavetas, armários e de portas devem ser **guardadas em locais fechados**, evitando o acesso.

Política de mesa limpa e tela limpa

FEBRABAN

Seu lixo ou sua mesa podem:

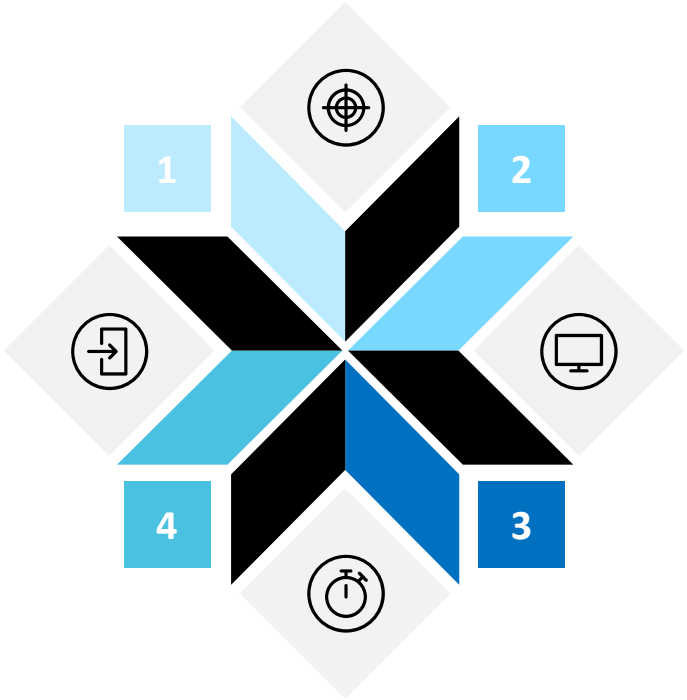
- ✓ Revelar seus dados e **informações pessoais**
- ✓ Fornecer **informações confidenciais da empresa** ao público externo ou a pessoas não autorizadas.
- ✓ **Possibilitar que outros colaboradores, ou até mesmo terceiros, tenham acesso a seus e-mails e/ou informações** restritas de seu computador, caso o bloqueio de tela não seja realizado ao deixar seu posto de trabalho.
- ✓ **Fornecer a visitantes suas credenciais de acesso** às instalações da Companhia com uso **de seu crachá deixado na mesa.**

- Cuidados simples, mas eficazes:
  - **Não deixe as portas abertas**. Isto facilita o acesso indevido de pessoas não autorizadas.
  - **Sempre acompanhe visitantes à área desejada**, não deixando que transitem desacompanhados pela empresa.
  - **Não aborde assuntos confidenciais em ambientes públicos.** Seja num almoço ou num telefonema.
  - **Realize descarte seguro**. Com uso de fragmentadoras para matérias impressos e DVDs e deleção segura para mídias magnéticas.

Comportamento individual

Algumas dicas e sugestões que você pode seguir para minimizar os riscos.

- Nunca conecte dispositivos USB desconhecidos ou de pessoas não confiáveis em seu computador.



- Desabilite a função de auto executar para mídias removíveis em seu computador.

- Caso encontre um dispositivo USB, entregue para a segurança da sua empresa ou para o departamento de TI, informando onde você o encontrou.

- Não utilize dispositivos pessoais em equipamentos da empresa.

Comportamento individual

FEBRABAN

Algumas dicas e sugestões que você pode seguir para minimizar os riscos.

1. **Bloqueio de tela**
   Sempre deixar a tela do computador em modo de descanso com senha ao sair de sua posição, e sempre conectar aparelhos à redes wi-fi conhecidas
2. **Segurança de documentos**
   Não deixar documentos com informações importantes espalhados pela mesa
3. **Controle de acesso**
   Sempre utilizar sua identificação para entrada e saída da empresa para manter o controle corretamente monitorado
4. **Proteção digital**
   Utilizar senhas fortes e realizar backups periodicamente
5. **Phishing**
   Não abrir e-mails suspeitos, sempre verificar o endereço remetente e se o conteúdo está coerente com os pedidos da empresa

Considerações Finais

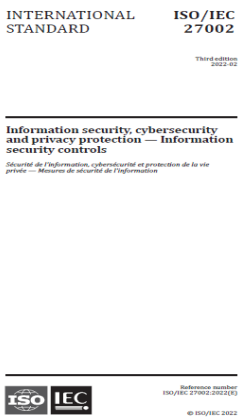
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Frameworks e Normas de Referência

Para apoiar no entendimento e implementação de toda a metodologia apresentada neste material, a seguir são apresentados as normas e frameworks de referência no tema:

Frameworks Padrão Utilizados

PCI DSS COMPLIANT



NIST National Institute of Standards and Technology

Conformidade: Requisitos de conformidade mais exigentes, permitindo estimar o nível de conformidade com ABNT NBR ISO, PCI-DSS, NIST, entre outros

Relembrando os principais conceitos

Agora que aprendemos sobre as atividades relacionadas à Segurança Física, relembre os principais termos e conceitos apresentados neste material:

Perímetro de Segurança: O perímetro de segurança tem como objetivo evitar o acesso não autorizado, maior restrição de acesso, rastreabilidade dos acessos e dano ou interferência aos sistemas de informação considerados sensíveis.

Controles de Entrada: Controles tecnológicos e processos para autenticar o acesso de pessoas..

Utilidades: Equipamentos que fornecem suprimento de energia elétrica, telecomunicações, suprimento de água, gás, esgoto, calefação/ventilação e ar-condicionado

Ativos: Equipamentos, mídias, informações de propriedade da empresa.

Shoulder Surfing: Prática que o atacante se posiciona de maneira que seja possível observar as informações do alvo, geralmente por cima de seu ombro.

Política da Mesa Limpa: Prática que tem como objetivo reduzir o risco de violação de segurança da informação, causadas por documentos e equipamentos deixados sozinhos e acessíveis nas mesas.

Módulo: Conscientização e Treinamentos

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Requisitos – Conscientização e Treinamentos

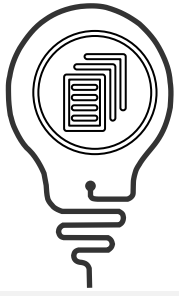
FEBRABAN

Este material foi elaborado de acordo com as diretrizes do CIS Controls e PCI DSS, bem como foram considerados os requisitos de segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

CIS Controls

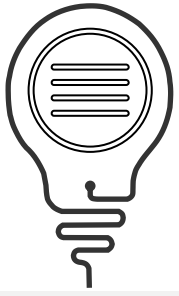
- 14.1 Estabelecer e manter um programa de conscientização de segurança
- 14.2 Treinar membros da força de trabalho para reconhecer ataques de engenharia social
- 14.3 Treinar membros da força de trabalho nas melhores práticas de autenticação
- 14.4 Treinar a força de trabalho nas Melhores Práticas de Tratamento de Dados
- 14.5 Treinar membros da força de trabalho sobre as causas da exposição não intencional de dados
- 14.6 Treinar Membros da força de trabalho no Reconhecimento e Comunicação de Incidentes de Segurança
- 14.7 Treinar a força de trabalho sobre como identificar e comunicar se o seus ativos corporativos estão faltando atualizações de segurança
- 14.8 Treinar a força de trabalho sobre os perigos de se conectar e transmitir dados corporativos em redes inseguras
- 14.9 Conduzir treinamento de competências e conscientização de segurança para funções específicas

PCI DSS



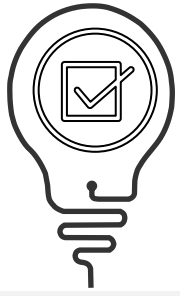
- 12.6 A educação de conscientização sobre segurança é uma atividade contínua.
- 12.6.1 Programa de conscientização
- 12.6.2 Abordagem de treinamento
- 12.6.3 Atualização de treinamento
- 12.6.3.1 Conteúdo de treinamento
- 12.6.3.2 Uso aceitável de tecnologias

ISO 27002



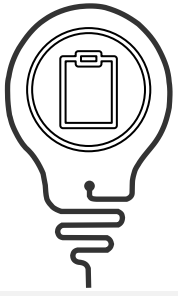
- 6.3 Conscientização, educação e treinamento em segurança da informação

ISO 27701



- 5.5.3 Conscientização
- 6.4.2.2 Conscientização, educação e treinamento em segurança da informação
- 6.4 Segurança em recursos humanos

NIST CSF



- PR.AT-02 Conscientização e treinamento para diferentes funções

Sumário

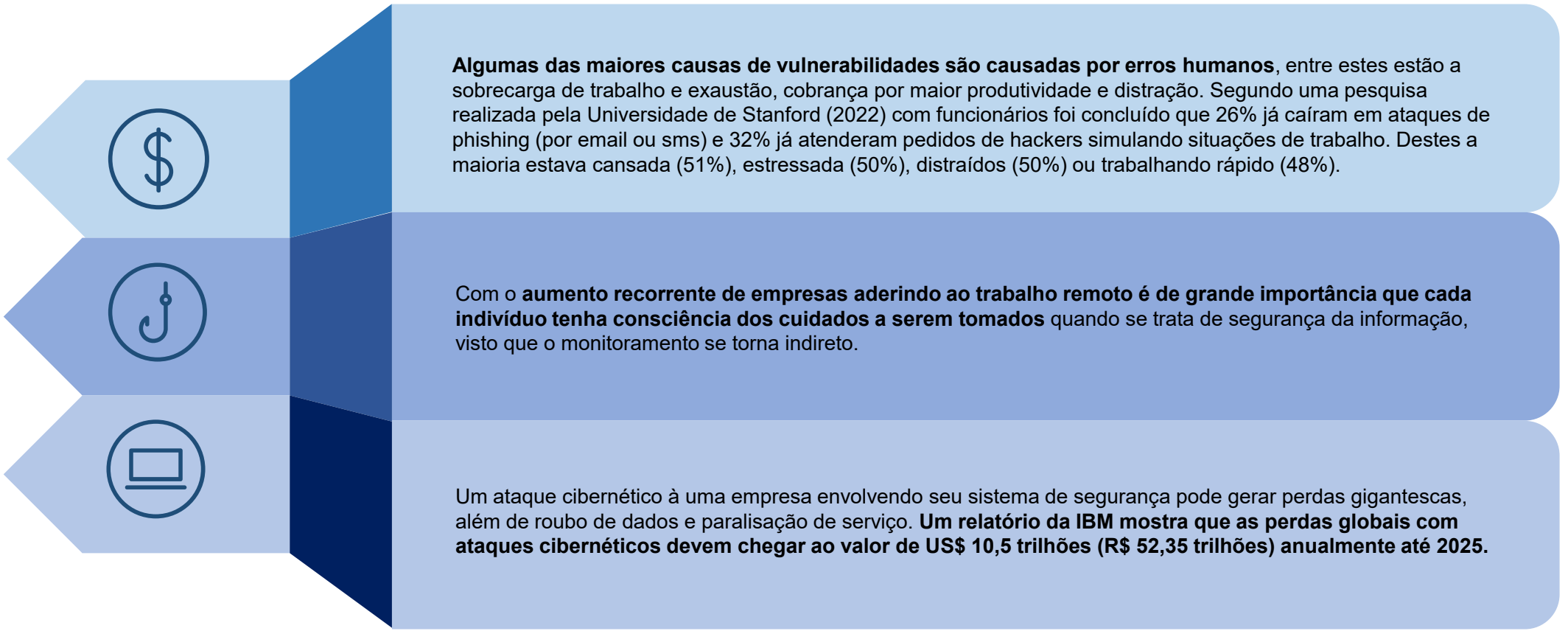
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Sumário

Contextualização

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Contextualização



Algumas das maiores causas de vulnerabilidades são causadas por erros humanos, entre estes estão a sobrecarga de trabalho e exaustão, cobrança por maior produtividade e distração. Segundo uma pesquisa realizada pela Universidade de Stanford (2022) com funcionários foi concluído que 26% já caíram em ataques de phishing (por email ou sms) e 32% já atenderam pedidos de hackers simulando situações de trabalho. Destes a maioria estava cansada (51%), estressada (50%), distraídos (50%) ou trabalhando rápido (48%).

Com o **aumento recorrente de empresas aderindo ao trabalho remoto é de grande importância que cada indivíduo tenha consciência dos cuidados a serem tomados** quando se trata de segurança da informação, visto que o monitoramento se torna indireto.

Um ataque cibernético à uma empresa envolvendo seu sistema de segurança pode gerar perdas gigantescas, além de roubo de dados e paralisação de serviço. **Um relatório da IBM mostra que as perdas globais com ataques cibernéticos devem chegar ao valor de US$ 10,5 trilhões (R$ 52,35 trilhões) anualmente até 2025.**

Casos Reais

Livecoins

[CEO explica como a Ledger foi hackeada: “ex-funcionário caiu em phishing”]

A Ledger, popular fabricante de carteiras de criptomoedas, revelou detalhes do hack que sofreu em seu sistema.

Forbes

Por que funcionários cometem erros que comprometem a cibersegurança

Exigência por maior produtividade, sobrecarga de trabalho e exaustão são algumas das causas de erros humanos no trabalho que comprometem a cibersegurança de seus empregadores, apontaram os funcionários entrevistados em um estudo da Universidade de Stanford de 2022. Dos respondentes, 26% já caíram em ataques de phishing – por e-mail ou mensagens de texto – e 32% já atenderam pedidos de hackers que simulavam situações reais no contexto de trabalho. A maioria deles teve esse tipo de comportamento quando estavam cansados (51%), estressados (50%), distraídos (50%) ou trabalhando rápido (48%).

CNN Brasil

Twitter diz que ataque de phishing a funcionários levou à invasão de contas

O Twitter, que teve seus sistemas internos invadidos há cerca de duas semanas, disse na quinta-feira (30) que o incidente atingiu um pequeno...

31 de jul. de 2020

CNN Brasil

Golpistas usam deepfake de diretor financeiro e roubam US$ 25 milhões

Um funcionário do setor financeiro de uma multinacional foi induzido a pagar US$ 25 milhões a fraudadores que usaram a tecnologia deepfake...

Olhar Digital

Como “Fraude do CEO” pode resultar em prejuízo de bilhões para empresas por meio de engenharia social

Entenda como funciona o o golpe do tipo Business Email Compromise (BEC), conhecido também como “Fraude do CEO”

Olhar Digital

Phishing já causa prejuízo de US$ 1.500 por funcionário em grandes empresas dos EUA

O uso de armadilhas digitais – o phishing – levou a prejuízos que aumentaram quase 4 vezes desde 2015, passando de US$ 3,8 milhões anuais...

De acordo com o CIS Controls, os próprios usuários, intencionalmente ou não, podem causar incidentes como resultado do manuseio incorreto de dados sensíveis, enviar um e-mail com dados sensíveis para o destinatário errado, perder um dispositivo de usuário final portátil, usar senhas fracas ou usar a mesma senha que usam em sites públicos.

Introdução

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Visão Geral - Implementação do Programa

FEBRABAN

Segundo a ISO 27002, o **programa de conscientização em segurança da informação** deve ser estabelecido alinhado com as **políticas e procedimentos relevantes de segurança da informação da organização**, levando em consideração as informações da organização a serem protegidas e os controles a serem implementados para proteger a informação.

De acordo com a resolução 4893, Art. 3º A política de segurança cibernética deve contemplar, a implementação de programas de capacitação e de avaliação periódica de pessoal.

Implementação do Programa de Treinamento

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Métodos

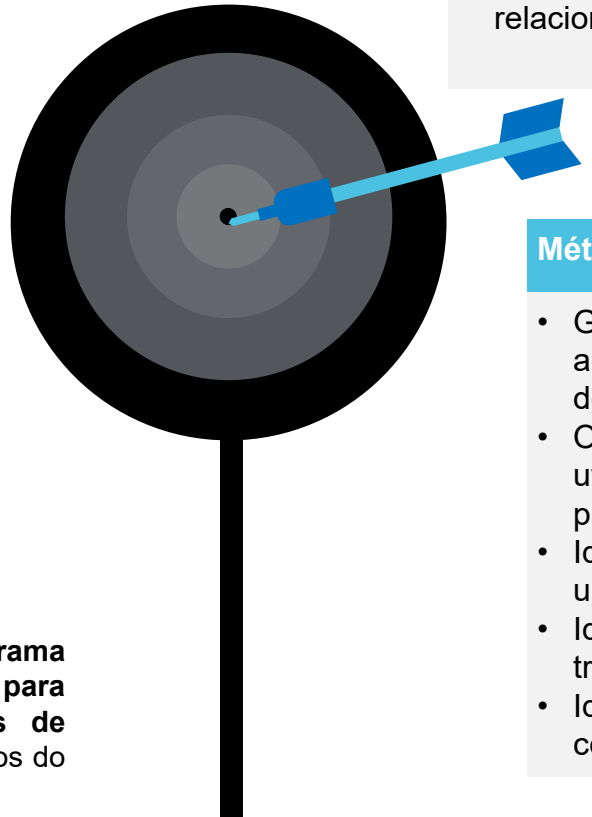
Práticas e abordagens

- Os treinamento de segurança devem conscientizar todo o pessoal sobre a política e procedimentos de segurança da informação.
- Disponibilizar de forma periódica publicações (exemplos: artigos, pílulas de conhecimento, e-books, infográficos) relacionadas ao tema de segurança, com situações práticas que podem impactar a empresa no dia a dia.
- Incluir ao final dos treinamentos (quando aplicável) testes, visando medir o nível de conhecimento dos colaboradores nas campanhas.
- Promover eventos, contendo por exemplo: palestras/workshops, novidades sobre o mercado, processos e em segurança, dinâmicas em grupo.

Atualizações

- Atualizar periodicamente os treinamentos obrigatórios aos novos colaboradores, incluindo práticas adotadas pela empresa em Segurança da Informação e Proteção dos Dados, essa medida aumentará a cultura de segurança na Organização.

De acordo com o PCI DSS, o requisito 12.6.1, menciona que o **programa formal de conscientização sobre segurança deve ser implementado para conscientizar todo o pessoal sobre a política e procedimentos de segurança da informação** da entidade e sua função na proteção dos dados do titular do cartão.



Liderança

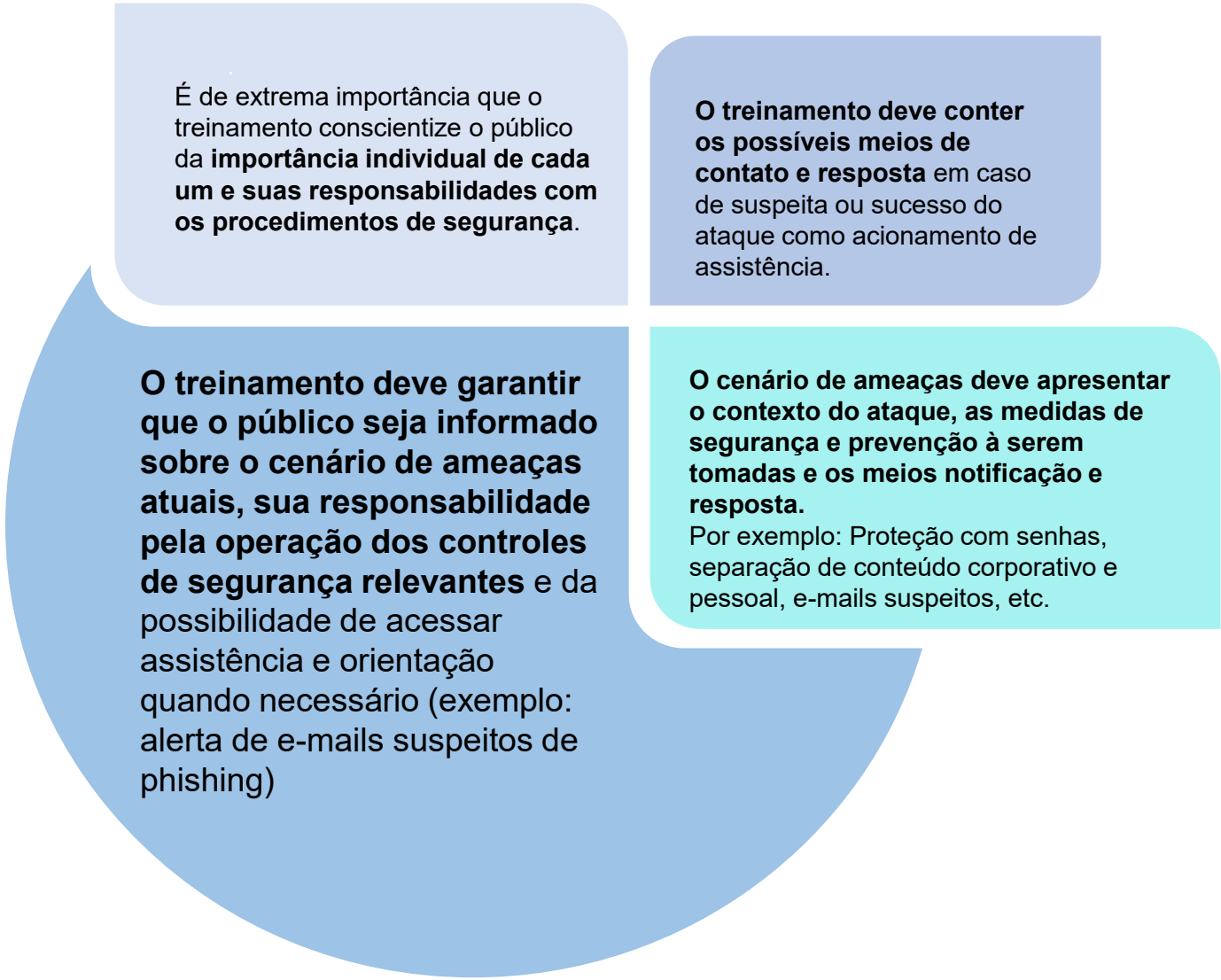
- Instruir os líderes das áreas a incentivarem os liderados a realizarem/participarem das campanhas de treinamentos disponibilizadas pela Organização. Essa medida pode ser implementada por meio do envio de comunicados direcionados para os líderes, por exemplo, envio de e-mail para a caixa dos executivos.
- Caso a empresa tenha um aplicativo de comunicação interna, considere a inclusão de temas relacionados à Segurança da Informação.

Métricas e indicadores

- Gerar e monitorar indicadores para fins de acompanhamento das participações e resultados dos treinamentos.
- Os resultados extraídos do treinamento podem ser utilizados para balizar ações de melhoria no processo, por exemplo:
- Identificar colaboradores ou áreas que não tiveram um desempenho aceitável nos treinamentos;
- Identificar colaboradores que não realizaram os treinamentos;
- Identificar ações de melhoria no plano de comunicação; entre outros.

Fatores de Sucesso

Cenário de ameaças e a política e procedimentos de segurança:



Como Definir o Conteúdo do Treinamento?

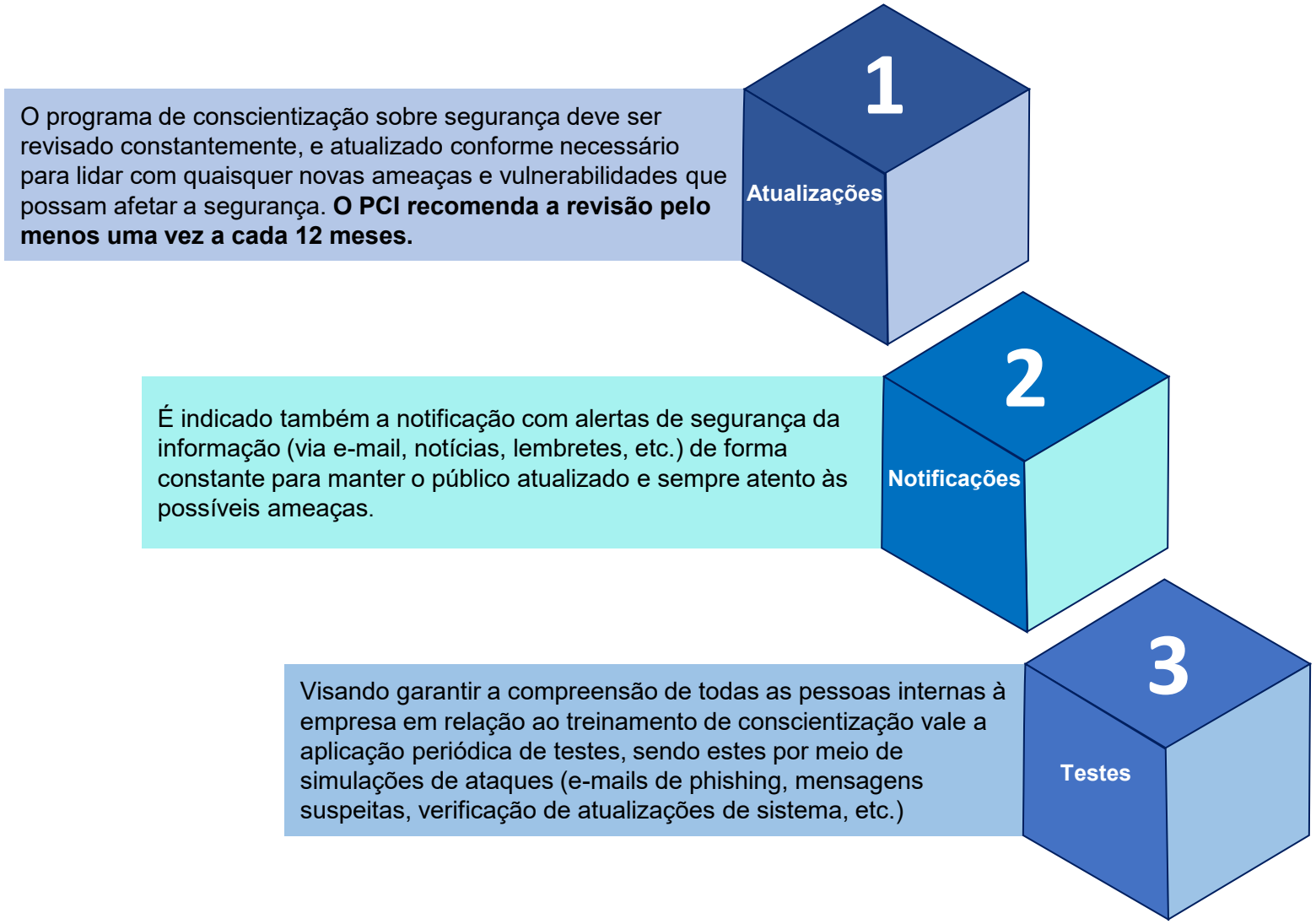
FEBRABAN

Os treinamentos devem considerar:

1. Conhecimento gerais de Segurança da informação no treinamento para funcionários, parceiros, fornecedores e outros relacionados , tais como: controle de acesso, proteção de dados, armazenamento e transmissão segura de informações, descarte seguro de ativos, entre outros.
2. Treinamento de funcionários para serem capazes de identificar ataques comuns como engenharia social, phishing, etc. E aplicarem cuidados básicos como higiene Cibernética, senhas seguras, proteção de credenciais, etc.
3. Explicar as consequências das violações de Segurança Cibernética e os possíveis prejuízos (tanto individuais como empresariais).
4. Conscientizar os funcionários sobre a importância de buscar assistência em caso de suspeita de infração ou primeiras respostas em caso de incidente, bem como divulgar os canais oficiais para notificar incidentes.
5. Implementar treinamento baseando-se em função, setor empresarial, incluindo diferentes métodos e abordagens.

Notificações e Testes

Aplicação de notificações e testes:



Especificação por Setor e Função

Os treinamentos podem ser mais específicos dependendo da área de atuação do setor ou da empresa em si.

Por exemplo, em caso de aplicação de treinamento no setor financeiro a equipe pode receber tentativas de BEC se passando por executivos pedindo para transferir dinheiro ou receberá e-mails de parceiros comprometidos ou fornecedores solicitando a alteração das informações da conta bancária para o próximo pagamento.

Métodos

Os diferentes métodos que podem ser usados para fornecer conscientização e educação sobre segurança incluem pôsteres, cartas, treinamento online, treinamento presencial, reuniões de equipe e incentivos.

Registros

Reconhecimentos de pessoal podem ser registrados por escrito ou eletronicamente.

Posturas regulatórias

O treinamento também deve levar em consideração as diferentes posturas regulatórias e de ameaças da empresa.

Treinamentos específicos

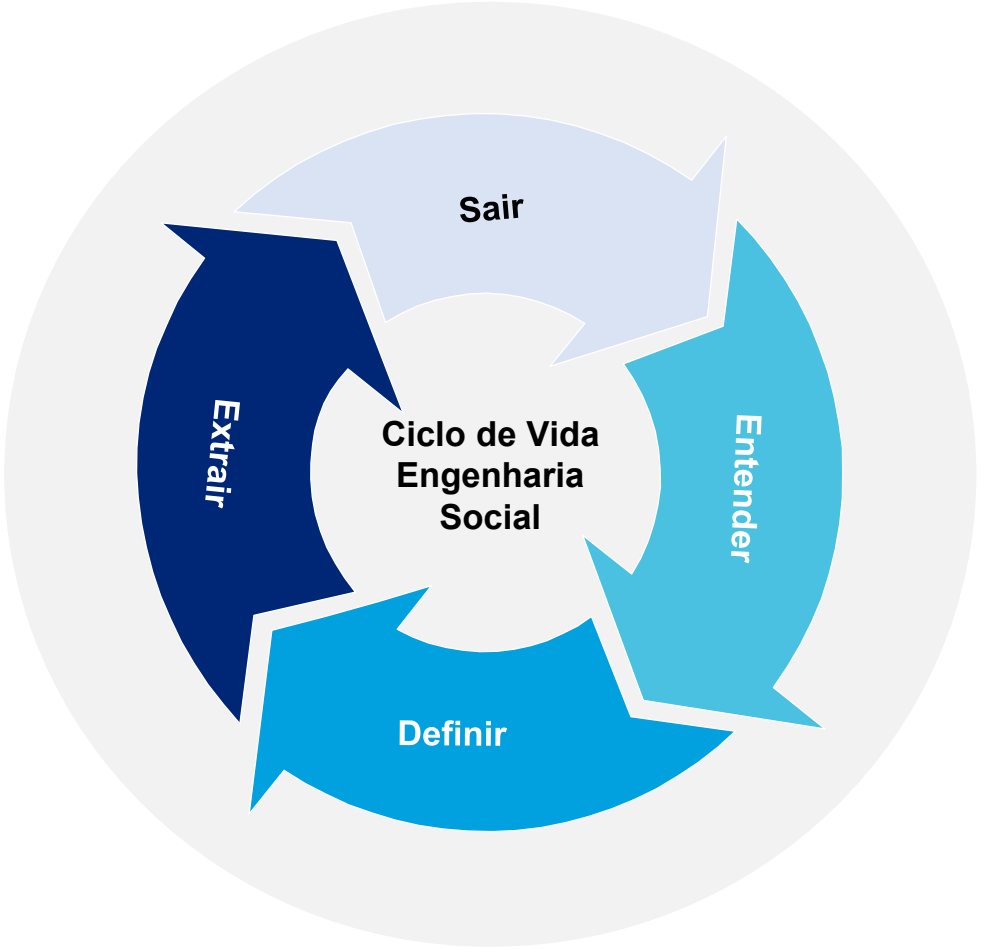
As empresas financeiras podem ter mais treinamento relacionado à conformidade sobre manuseio e uso de dados, empresas de saúde sobre como lidar com dados de saúde e comerciantes para dados de cartão de crédito.

Introdução ao Phishing

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

O que é Phishing?

"A aplicação deliberada de **técnicas fraudulentas** destinadas a **manipular alguém** a divulgar informações ou realizar ações que podem resultar na divulgação destas informações."

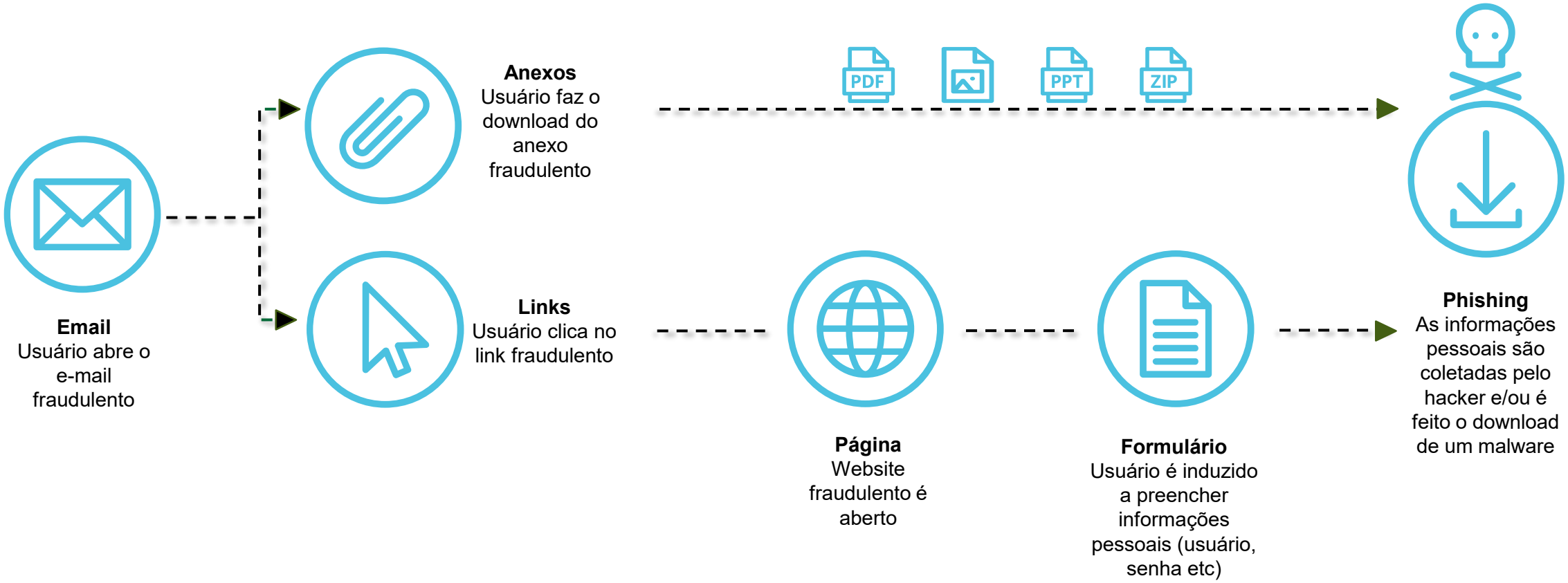


Vetores de Ataque

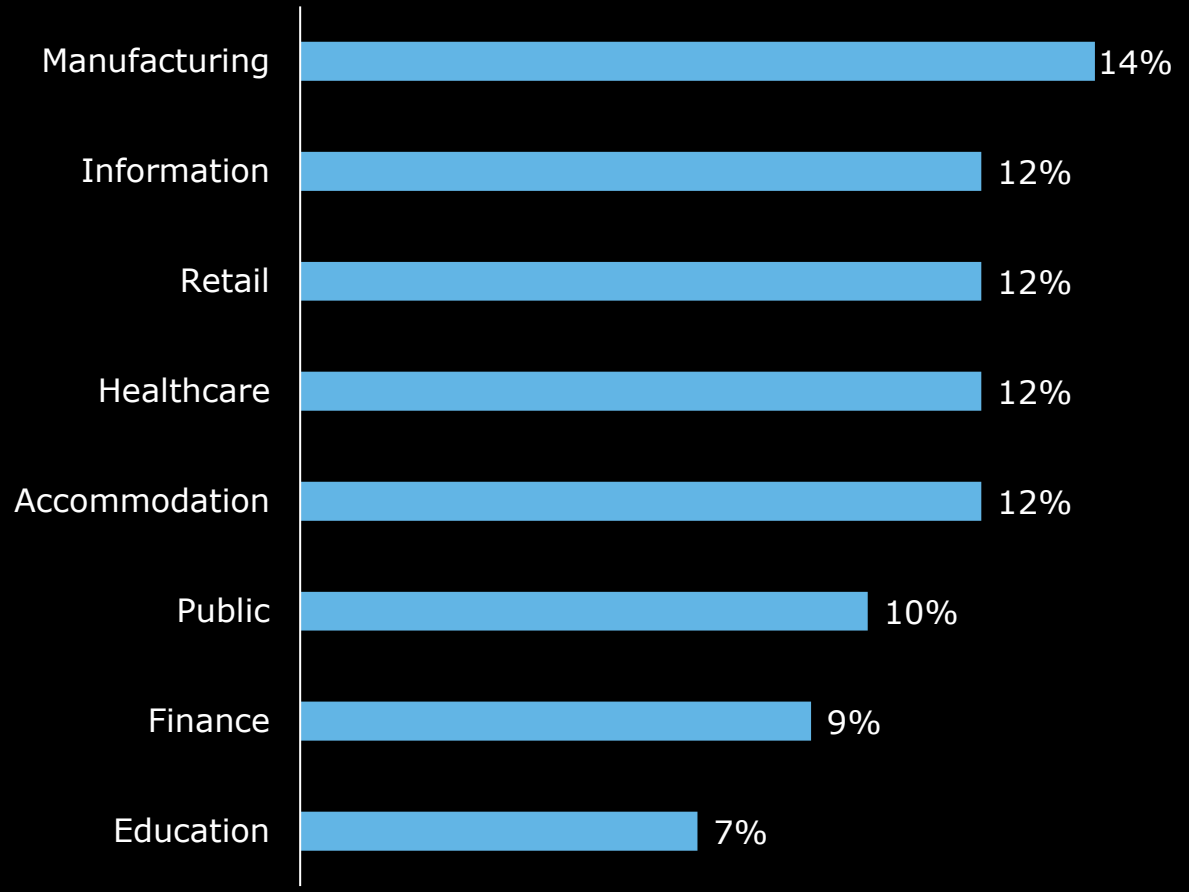
- Website
- Email
- Telefone
- Cara a Cara
- Correios

O que é Phishing?

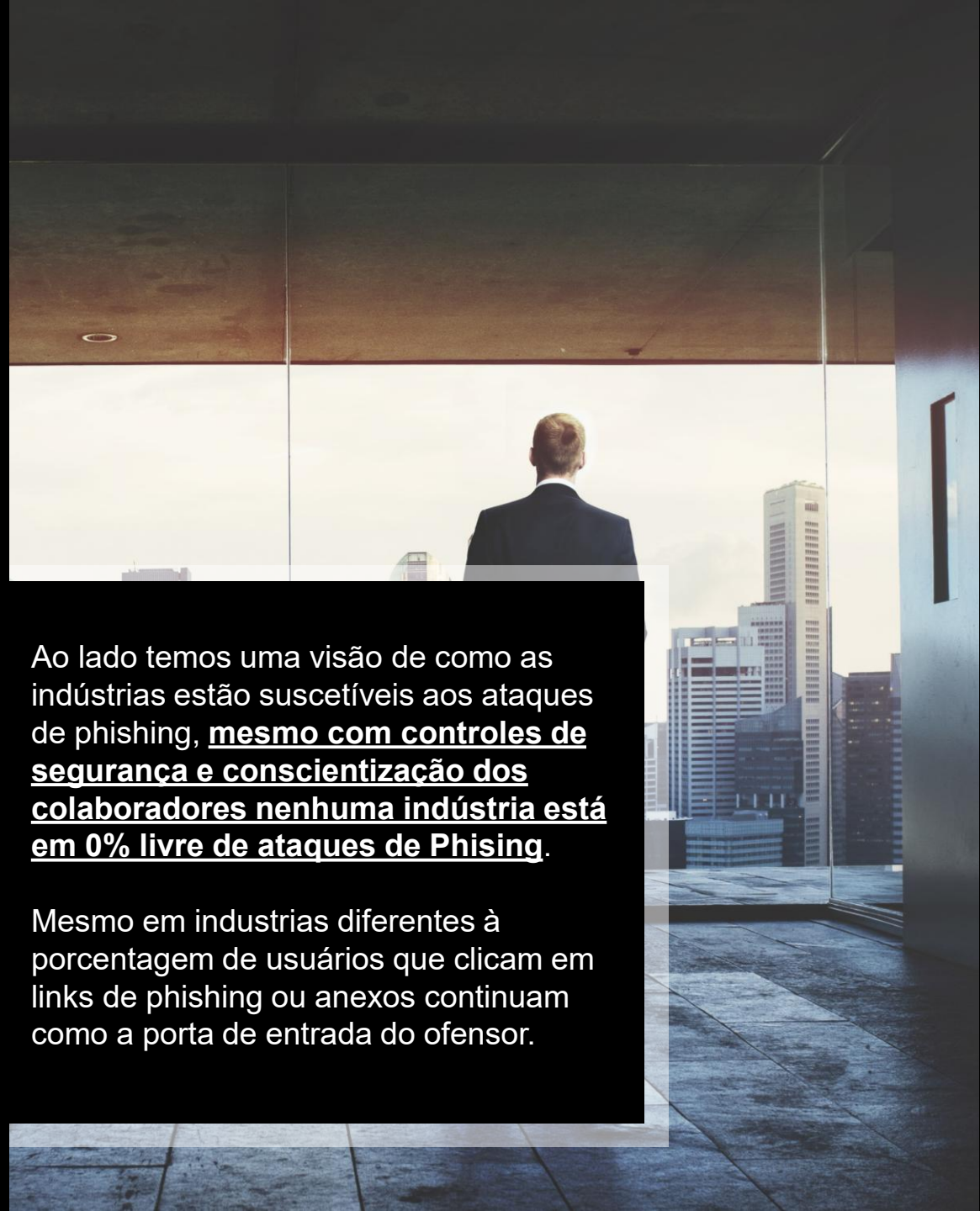
Phishing é uma tentativa de **roubar ilegalmente informações pessoais e financeiras** através do envio de uma mensagem **aparentemente legítima**. Uma mensagem de phishing normalmente inclui pelo menos **um link para uma página falsa** ou um anexo com conteúdo fraudulento.



Estatísticas por Indústria



Fonte: ***2023 DBIR***



Ao lado temos uma visão de como as indústrias estão suscetíveis aos ataques de phishing, **mesmo com controles de segurança e conscientização dos colaboradores nenhuma indústria está em 0% livre de ataques de Phising**.

Mesmo em industrias diferentes à porcentagem de usuários que clicam em links de phishing ou anexos continuam como a porta de entrada do ofensor.

Modus Operandi

1. Envio de e-mail contendo arquivo malicioso

- Um atacante desenvolve um malware específico para comprometimento do usuário alvo.
- O malware pode estar contido em um e-mail ou em um endereço na internet.
- O alvo abre o e-mail e é infectado sem que haja intervenção do antivírus.
- **Páginas idênticas as originais (facilidade em criar essas páginas)***

2. Controle Remoto da estação comprometida

- Uma vez comprometida, a estação passa a executar todas as tarefas orientadas pelo atacante.
- O atacante planta um sistema de persistência que permita maior resiliência no controle do alvo.

3. Comprometimento do core do sistema infectado

- São encontradas falhas na estação de trabalho controlada para a execução de uma escalação de privilégios.
- São extraídas credenciais de acesso para utilização em um posterior ataque de movimentação lateral.

4. Infecção de outros ativos do ambiente

- São identificadas estações de trabalho e servidores no ambiente que possam ser comprometidas a partir das informações já extraídas.
- Ataques seguidos de pass-the-hash ou pass-the-ticket podem ser utilizados para comprometer o ambiente inteiro

5. Atividade planejada pelo atacante

- O atacante obtém poder e controle o suficiente sobre o ambiente alvo para que suas ações de extração e espionagem possam ser executadas sem interferência dos administradores da rede que eventualmente identifiquem o ataque.

O que é Smishing e Vishing?

Smishing:

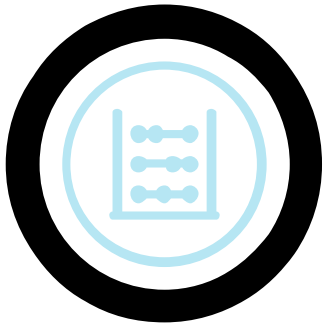
Smishing é um ataque de cibersegurança de phishing realizado por mensagens de texto móveis, também conhecido como phishing por SMS. Como uma variante de phishing, as vítimas são enganadas a fornecer informações sensíveis a um atacante disfarçado.

Como a definição de smishing sugere, o termo combina "SMS" (serviços de mensagens curtas, mais conhecido como mensagens de texto) e "phishing".

Vishing:

O vishing, ou phishing de voz, é um tipo de ataque de phishing que ocorre por meio de chamadas telefônicas.
Vishing é a prática de enganar as pessoas para que compartilhem informações confidenciais por meio de ligações telefônicas. As vítimas de vishing são levadas a acreditar que estão compartilhando informações confidenciais com uma entidade confiável, como autoridade fiscal, seu empregador, uma companhia aérea que usam, ou alguém que conhecem pessoalmente. O vishing também é conhecido como "phishing de voz".

Inteligência Artificial nos Ataques



Operações de influência (IO)

Engano de imagem por IA e deepfakes

- As imagens geradas por IA são visualmente mais impressionantes e eficazes em comparação com as campanhas anteriores. A IA foi concebida para criar imagens atraentes e provocadoras e melhorá-las ao longo do tempo, considerando as perspectivas:
    - A IO com IA aproveitando-se das redes sociais, e
    - A IO com IA incorporada nos ciberataques.

- **Exemplo prático 1**: Os agentes de ameaças utilizam imagens geradas por IA para difundir propaganda nas redes sociais.
- **Exemplo prático 2:** Os agentes da ameaça utilizam um vídeo deepfake passando-se por um executivo e enganando um funcionário das finanças para que envie milhões para uma conta.
- **Exemplo prático 3**: Imagens convincentes geradas por IA aumentam o envolvimento dos empregados em campanhas de phishing.

Engenharia Social

Phishing

- As ferramentas de IA oferecem aos agentes de ameaças capacidades sofisticadas, incluindo a criação de mensagens electrónicas fraudulentas.
- A IA melhora as campanhas de phishing com gramática, pontuação e pontos de discussão mais corretos nas campanhas de whaling e BEC.
- **Exemplo prático**: o agente da ameaça utiliza a IA para gerar uma mensagem de correio eletrônico que utiliza a linguagem para se passar por um executivo numa fraude.

Vishing

- Os agentes da ameaça podem utilizar ferramentas de clonagem de voz baseadas em IA no vishing para fraude financeira e acesso não autorizado a sistemas protegidos por autenticação biométrica.
- Os agentes da ameaça podem utilizar a clonagem de voz em vários esquemas, incluindo passando-se pela família de uma vítima, por um executivo que autoriza uma transação financeira ou enganando a autenticação biométrica para acessar um sistema protegido.
- Os agentes de ameaças podem utilizar ferramentas VCaaS pagas para efetuar operações de vishing.
- **Exemplo prático**: Um agente de ameaças utiliza uma ferramenta VCaaS para clonar a voz de um executivo ou de uma pessoa com autoridade para aprovar uma transação financeira.

Serviços clandestinos

IA como um serviço (AI-As-a-Service)

- A Deloitte CTI continua a observar agentes de ameaças que colaboram em fóruns clandestinos sobre formas de utilizar a IA e fraudes.
- As ferramentas de IA maliciosas identificam vulnerabilidades para potencial exploração.
- Os agentes clandestinos anunciaram chatbots de IA personalizados
- Personalizados concebidos para criar programas maliciosos.

Exemplo de Phishing

FEBRABAN

Fique atento ao e-mail remetente (se condiz com e-mail oficial da empresa que está enviando o e-mail)

De Atendimento FGTS <contato48@caixa.gov.br>

Assunto **Saque FGTS disponível. Protocolo Nº: 2C4D3B1A** 15:

Para financeiro

FUNDO DE GARANTIA DO TEMPO DE SERVIÇO

Prezado cidadão,

Encontra-se disponível o saque do FGTS. Confira o Calendário FGTS 2017.

No CPF vinculado a este e-mail, consta um saldo no valor de R$7212,35 disponível para saque.
Visto que o valor disponível é superior a R$3000,00 o titular deverá dirigir-se a uma agência da Caixa Econômica Federal portando:

- Carteira de Trabalho ou Termo de Rescisão
- Documento de identificação com foto
- Extrato completo do FGTS atualizado

Para clientes da Caixa, será possível através do site www.contasinativas.caixa.gov.br solicitar o crédito automático na conta. Caso não seja, na agência, solicite o depósito em um banco de sua preferência ou o saque em espécie.

O extrato que deverá ser levado junto com os outros documentos já citados, encontra-se abaixo. Clique no botão para fazer o download e depois imprimi-lo.

Extrato FGTS 2017

Atenciosamente,
Caixa Econômica Federal - FGTS

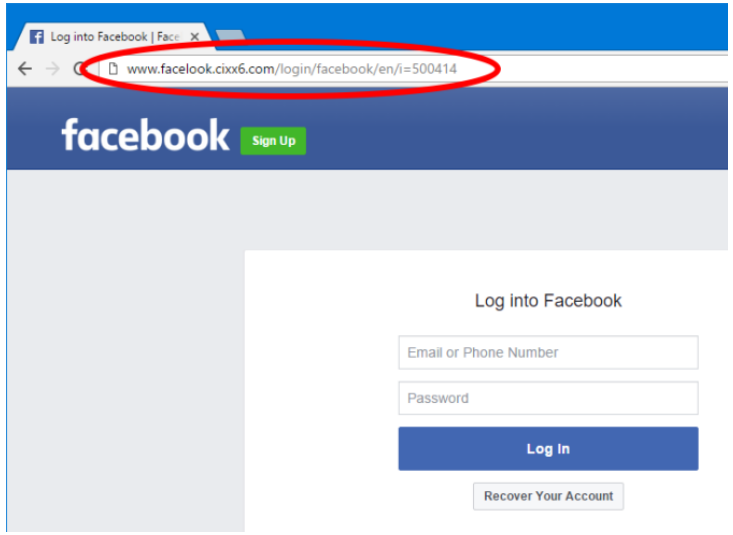
RTXP7K45IUQBO96LMF1ZS0AVYDNEHGJWC832

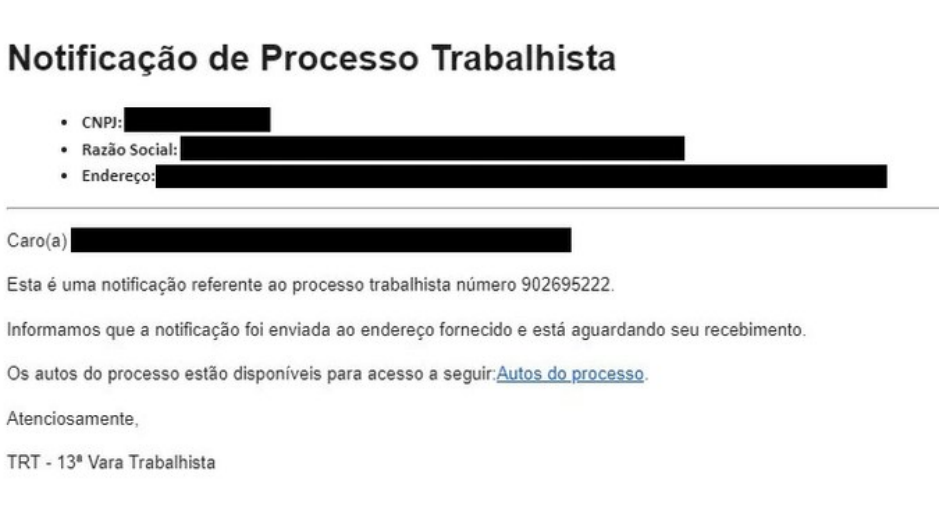
Fique atento à termos genéricos ao invés do contato direto pelo seu nome

Verificar se o conteúdo do e-mail de fato faz sentido em seu contexto aplicado (exemplo: nunca me cadastrei na plataforma x e estou recebendo e-mail de tal plataforma)

Verificar se o e-mail possui erros ortográficos ou links/ documentos anexados

Outros exemplos





Como Identificar um Phishing?

Veja a seguir cinco dicas para te ajudar a identificar um e-mail de phishing:

1 - Atente-se a e-mails inesperados

Se você receber um e-mail que não estava esperando ou que possua uma oferta de alto valor que parece boa demais para ser verdade, provavelmente trata-se um e-mail malicioso.

2 - Verifique o endereço de e-mail do remetente. Em seguida, verifique-o novamente

Veja se há algum texto desconhecido ou suspeito no endereço de e-mail e no nome de domínio do remetente. Os cibercriminosos costumam usar variações discretas, como substituir uma letra por um número (por exemplo, um 'o' por um '0'), para enganar os destinatários a acreditar que a mensagem é de um contato confiável.

Em algumas empresas, é utilizado a tag **[EXT]** no início da linha do assunto como um indicador de que o e-mail veio de um remetente externo. Use esse recurso para ajudar a determinar se o remetente é confiável.

3 - Use sua criatividade ao confirmar o remetente

Se você tiver um meio de contato alternativo para o remetente, como um número de telefone secundário, ligue ou envie uma mensagem de texto diretamente para essa pessoa para confirmar se o envio do e-mail suspeito foi legítimo.

4 - Se o remetente alegar ser alguém em quem você confia, compare o e-mail com mensagens anteriores

Você pode comparar a linguagem utilizada pela pessoa em conversas anteriores. Uma expressão incomum ou um tom de escrita divergente, por exemplo, são boas indicações de que o remetente foi falsificado ou comprometido.

5 - Lembre-se, você não precisa responder ao e-mail

Se você suspeitar que um e-mail foi enviado por um cibercriminoso, faça uma pausa de um minuto antes de agir sobre ele. Você não precisa responder. Em vez disso, as diretrizes acima podem te ajudar a decidir o que fazer a seguir. Afinal, denunciar e-mails suspeitos é sempre uma opção.

Comportamento Seguro

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

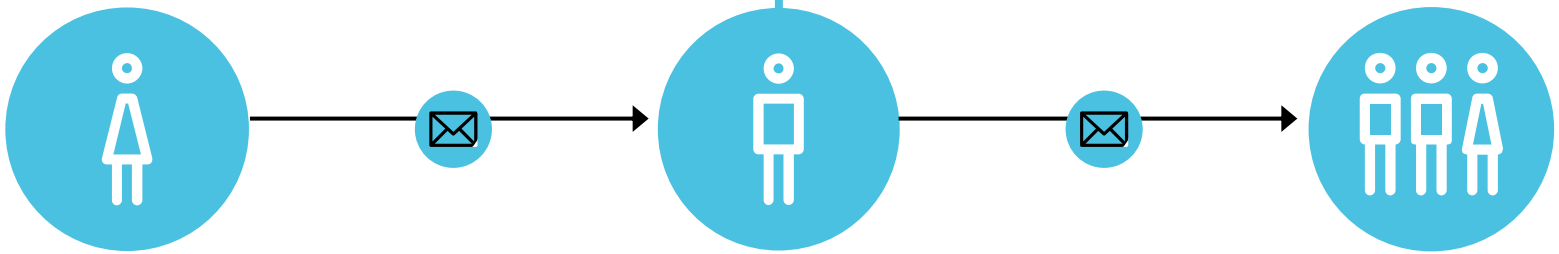
Ações Preventivas e Recomendações

Previna-se contra códigos maliciosos e phishing:

- Mantenha o seu computador seguro, com os programas atualizados e com todas as atualizações aplicadas; como antimalware e firewall pessoal;
- Seja cuidadoso ao acessar links reduzidos.

Respeite a privacidade:

- Não divulgue, sem autorização, imagens em que outras pessoas apareçam;
- Não divulgue mensagens ou imagens copiadas do perfil de pessoas que restrinjam o acesso;
- Tente imaginar como a outra pessoa se sentiria ao saber que aquilo está se tornando público.
- Seja cuidadoso nas redes sociais.
  - ❑ **Nota**: Essas informações podem ser utilizadas para elaboração de ataques.



Ações Preventivas e Recomendações

4 Passos para ficar atento

Questione
todo e-mail de negócios recebido de origem duvidosa

Check
se os links são legítimos antes de clicar

Evite
fornecer detalhes de senhas por Email ou telefone

Denuncie
e-mails suspeitos aparentemente legítimos, visitando diretamente seu website e formulário de contato

4 dicas para **NÃO** ser a próxima **VÍTIMA**

Aprenda a identificar e-mails fraudulentos

Phishing não se referem apenas a Internet Banking

No website, fique atento aos sinais de phishing

Falsa sensação de segurança e urgência

Ações Preventivas e Recomendações

FEBRABAN

Smishing

- Recebeu SMS solicitando para ligar no 0800 ou outro número que você desconhece? Procure um canal oficial.
- .
- Não clique em links ou execute arquivos anexados a mensagens suspeitas, recebidas por SMS.
- Não instale aplicativos de links recebidos via SMS.
- Desconfiou do SMS? Confirme o remetente e a mensagem por outros meios, por exemplo, ligação ou consulta ao site oficial da empresa.
- Analise o texto e verifique se contém erros ortográficos, pontuação, espaçamentos. Na maioria dos casos ocorrem erros de português.

Phishing

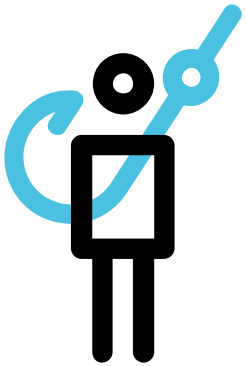
- Nunca digite sua senha ou chave de segurança após clicar em links recebidos por e-mail.
- Não acesse links ou execute arquivos anexados a mensagens suspeitas, recebidas por e-mail.
- Não instale aplicativos desconhecidos e que não tenham verificação da sua loja de aplicativos.
- Desconfiou do e-mail? Confirme o remetente e a mensagem em canais oficias da empresa.
- Quando estiver em um site, verifique se ele tem o símbolo de segurança e não clique em promoções com promessas milagrosas.
- Utilize sistema operacional e antivírus originais e os mantenha sempre atualizados.

Vishing

- Não forneça informações pessoais ou confidenciais por telefone, a menos que tenha certeza absoluta de que está lidando com uma fonte confiável. Se necessário, entre em contato diretamente com a instituição.
- Verifique a identidade de origem: Solicite informações como seu nome completo, número de funcionário ou qualquer outra informação relevante. Anote esses detalhes para referência futura.
- Pesquise o número de telefone: Antes de retornar uma chamada, pesquise o número de telefone online para ver se há relatos de golpes associados a ele.

Ações Preventivas e Recomendações

Você acha que foi “**pescado**”? Saiba o que fazer!



Comunique a equipe de Segurança da Informação e TI.

Verifique sua conta bancária e procure por transações suspeitas.

Troque as senhas de acesso a emails, internet banking etc.

Mantenha seu antivírus sempre Atualizado.

Considerações Finais

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Frameworks e Normas de Referência

Para apoiar no entendimento e implementação de toda a metodologia apresentada neste material, a seguir são apresentados as normas e frameworks de referência no tema:

Frameworks Padrão Utilizados

PCI DSS COMPLIANT


NORMA BRASILEIRA

ABNT NBR ISO/IEC 27701

Primeira edição 25.11.2019

Versão corrigida 11.02.2020

Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes

Security techniques — Extension to ABNT NBR ISO/IEC 27001 and ABNT NBR ISO/IEC 27002 for privacy information management — Requirements and guidelines


INTERNATIONAL STANDARD

ISO/IEC 27002

Third edition 2022-02

Information security, cybersecurity and privacy protection — Information security controls

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

ISO IEC

Reference number ISO/IEC 27002:2022(E)

© ISO/IEC 2022

NIST National Institute of Standards and Technology

Conformidade: Requisitos de conformidade mais exigentes, permitindo estimar o nível de conformidade com ABNT NBR ISO, PCI-DSS, NIST, entre outros

Relembrando os principais conceitos

Agora que aprendemos sobre as atividades relacionadas a Conscientização e Treinamentos, relembre os principais termos e conceitos apresentados neste material:

Implementação de treinamento: Deve ser realizado um programa de treinamento de conscientização de segurança da informação seguindo as políticas internas da empresa contendo boas práticas de segurança da informação e responsabilidades individuais, conhecimento de ameaças comuns e meios de resposta e contato.

Atualizações e testes: O treinamento deve ser atualizado e revisado periodicamente. Também deve ser aplicado a prática de notificações para funcionários visando o constante lembrete de conscientização, além de aplicação de testes para verificar a compreensão e preparação de internos diante à ameaças.

Especificação por setor: Os treinamentos e testes podem variar de acordo com o setor de aplicação interna, desta forma cada setor terá tópicos e prioridades variadas em relação à conscientização de possíveis ameaças.

Módulo: Cloud Security

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Requisitos – Cloud Security

FEBRABAN

Este material foi elaborado de acordo com as diretrizes da ISO 27017, bem como foram considerados os requisitos de segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

ISO 27017

- 5. Políticas de segurança da informação
- 6. Organização da segurança da informação
- 7. Segurança dos recursos humanos
- 8. Gestão de ativos
- 9. Controle de acesso
- 10. Criptografia
- 11. Segurança física e ambiental
- 12. Segurança de operações
- 13. Segurança das comunicações
- 14. Aquisição, desenvolvimento e manutenção de sistemas
- 15. Relacionamentos com fornecedores
- 16. Gestão de incidentes de segurança da informação
- 17. Aspectos de segurança da informação da gestão de continuidade de negócios
- 18. Conformidade

PCI DSS

- A1.1 Os prestadores de serviços multilocatários protegem e separam todos os ambientes e dados do cliente.
- A1.2 Os prestadores de serviços multilocatários facilitam o registro e a resposta a incidentes para todos os clientes.
- 11.4.3 O teste de penetração externa é realizado
- 11.4.4 Vulnerabilidades exploráveis e fragilidades de segurança encontradas durante o teste de penetração são corrigidas
- 11.4.7 Os prestadores de serviços em nuvem/hospedados por terceiros oferecem suporte a seus clientes para testes de penetração externa de acordo com os Requisitos 11.4.3 e 11.4.4.

CIS Controls

- 1.1 Estabelecer e manter um inventário detalhado de ativos corporativos
- 11.4 Estabelecer e manter uma instância isolada de dados de recuperação
- 13.3 Implantar uma solução de detecção de intrusão de rede
- 16.7 Usar modelos de configurações de segurança padrão para infraestrutura de aplicações

NIST

- ID.AM-04: Estoques de serviços prestados por fornecedores são mantidos
- CM-04: Atividades e serviços de prestadores de serviços externos são monitorados para encontrar eventos potencialmente adversos

Resolução nº 4893

- Art. 11
- Art. 12
- Art. 15
- Art. 16
- Art. 17
- Art. 21
- Art. 25

Sumário

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Sumário

Contexto

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Incidentes Cibernéticos

2024 Cloud Security Report

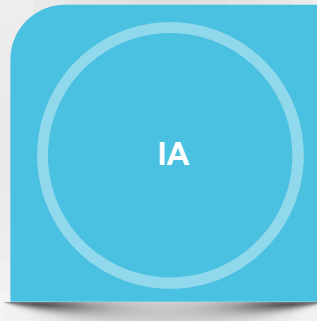
O Relatório Global de Segurança na Nuvem de 2024, da Check Point Software expõe um aumento nos incidentes de segurança na nuvem, marcando um crescimento de 24% em 2023 para 61% em 2024 – um aumento de 154%.

O relatório indica uma tendência preocupante: enquanto **a maioria das organizações continua a priorizar a detecção e monitoramento de ameaças**, com foco em vulnerabilidades conhecidas e padrões de comportamento malicioso, **apenas 21% delas enfatizam a prevenção.**

Importância de Segurança da Informação para as **instituições financeiras** se faz necessária devido à **complexidade do ambiente em um mercado alvo de ataques.**

91% dos entrevistados estão preocupados com o **aumento de ameaças cibernéticas** mais sofisticadas, relacionadas a riscos desconhecidos e **ataques *zero day* (dia zero)**, que não são detectadas por meio de ferramentas de segurança convencionais.

54% dos entrevistados enfrentam **desafios na manutenção de padrões regulatórios consistentes em ambientes de múltiplas nuvens (multicloud).** Além disso, 49% enfrentam dificuldades para integrar serviços em nuvem em sistemas legados, muitas vezes complicados por recursos de TI limitados.



A pesquisa sinaliza a adoção rápida de tecnologias de inteligência artificial, com 91% das organizações **priorizando à IA para melhorar a sua postura de segurança frente as ameaças cibernéticas**.

2024 Cloud Security Report - Check Point Software

Incidentes Cibernéticos

Casos Reais

Ataques ao setor industrial agora visam infraestruturas de nuvem

https://www.cisoadvisor.com.br/ataques-ao-setor-industrial-agora-visam-ambientes-de-nuvem/

Falha na nuvem da Microsoft atinge usuários em todo mundo

Empresa disse nesta quarta-feira que recuperou serviços de nuvem depois que um problema na rede derrubou sua plataforma Azure

https://www.cnnbrasil.com.br/economia/macroeconomia/falha-na-nuvem-da-microsoft-atinge-usuarios-em-todo-mundo/

97% das empresas já tiveram problemas de segurança na nuvem

https://canaltech.com.br/seguranca/97-das-empresas-ja-tiveram-problemas-de-seguranca-na-nuvem-247768/#google_vignette

Ataques ao setor industrial agora visam infraestruturas de nuvem

https://www.cisoadvisor.com.br/ataques-ao-setor-industrial-agora-visam-ambientes-de-nuvem/

Resolução 4.893 - Banco Central

Cloud computing é uma tecnologia ***on-demand*** **capaz de entregar serviços de tecnologia de infraestrutura e aplicações de TI** para seus usuários através de **serviços disponíveis na internet.**

Segundo a resolução CMN n° 4.893 de 26/2/2021 , Seção III - CAPÍTULO III, a definição de serviços Cloud que se aplicam as boas práticas recomendadas são sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

Resolução 4.893 - Banco Central

Dispõe sobre a política de segurança cibernética e sobre **os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições** autorizadas a funcionar pelo Banco Central do Brasil.

Art. 11. **As instituições devem assegurar que suas políticas, estratégias e estruturas para gerenciamento de riscos contemplem a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem**, no País ou no exterior.

Art. 12. As **instituições devem adotar procedimentos de segurança**, tais como: adoção de práticas de governança corporativa, proteção dos dados processados ou armazenados, segregação de dados, qualidade dos dados, entre outros.

Art. 16. **A contratação de serviços em nuvem prestados no exterior deve observar os seguintes requisitos**: **definir os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados**, processados e gerenciados, e **prever alternativas para a continuidade dos negócio em caso de disrupções**, entre outros.

Resolução 4.893 - Banco Central

É solicitado no Art. 15. que a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem seja comunicada pelas instituições referidas no art. 1º ao Banco Central do Brasil seguindo os seguintes requisitos:

As alterações contratuais que impliquem modificação das informações de que trata o § 1º devem ser comunicadas ao Banco Central do Brasil até dez dias após a alteração contratual.

A comunicação mencionada no caput deve conter as seguintes informações:

- a denominação da empresa contratada;
- os serviços relevantes contratados; e
- a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, definida nos termos do inciso III do art. 16, no caso de contratação no exterior.

A comunicação de que trata o caput deve ser realizada até dez dias após a contratação dos serviços.

Resolução 4.893 - Banco Central

As notificações solicitadas no Art. 15 devem seguir o seguinte modelo:

I. A comunicação da contratação de serviço relevante de processamento e armazenamento de dados e de computação em nuvem deverá ser feita por meio de Comunicação Relevante (CR) de assunto "Comunicação de contratação de serviço relevante" pela instituição contratante.

II. A solicitação de autorização para a contratação de serviço relevante de processamento e armazenamento de dados e de computação em nuvem quando não há convênio entre o Banco Central do Brasil e as autoridades supervisoras dos países onde o serviço será prestado deverá ser encaminhada por meio de CR de assunto "Solicitação de autorização para contratação de serviço relevante provido no exterior".

III. Os modelos de CR estarão disponíveis no Sistema APS-Siscom, disponível no endereço eletrônico “www3.bcb.gov.br/siscom/es”. Caso os modelos não estejam disponíveis, a instituição deverá contatar o supervisor responsável para regularização.

IV. As informações de contratos vigentes celebrados por cooperativa singular de crédito podem ser encaminhadas individualmente, ou de forma consolidada por cooperativa central de crédito ou confederação do sistema cooperativo ao qual pertença.

V. As informações de contratos vigentes celebrados por empresas individuais integrantes de conglomerados prudenciais podem ser enviados individualmente, ou de forma consolidada pela instituição líder do conglomerado.

Resolução 4.893 - Banco Central

FEBRABAN

As notificações solicitadas no Art. 15 devem seguir o seguinte modelo:

Em caso de dúvidas, as instituições podem entrar em contato com o Banco Central do Brasil, de acordo com o assunto a ser tratado, conforme a seguir:

I - esclarecimentos sobre o Sistema APS-Siscom podem ser obtidos por meio do endereço eletrônico: https://www.bcb.gov.br/estabilidadefinanceira/sistemacomunicacaosupervisao;

II – esclarecimentos sobre o uso de CRs estão disponíveis em "https://www.bcb.gov.br/content/estabilidadefinanceira/aps_siscom_docs/SisAPS-ManualModuloComunicacaoRelevante-ES.pdf"

III - dúvidas sobre o preenchimento das requisições citadas no parágrafo 2 podem ser enviadas para o e-mail seguranca.difis@bcb.gov.br; e

IV - dúvidas sobre o cadastro no Sistema de Informações Banco Central (Sisbacen) para acesso ao Sistema APS-Siscom, reabilitação de senha ou demais problemas técnicos podem ser encaminhados para a equipe de atendimento do BCB/Deinf/Diate, pelo telefone (61) 3414-2156 ou pelo e-mail suporte.ti@bcb.gov.br.

Para maiores informações acesse a página de referência da BACEN:
https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=41782

Resolução 4.893 - Banco Central

Dispõe sobre a política de segurança cibernética e sobre **os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições** autorizadas a funcionar pelo Banco Central do Brasil.

Art. 17. Os **contratos** para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem **devem prever: adoção de medidas de segurança para a transmissão e armazenamento dos dados**, além disso, a **manutenção da segregação dos dados e dos controles de acesso para proteção das informações dos clientes**, entre outros.

Art. 21. **As instituições devem instituir mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade** da política de segurança cibernética, do plano de ação e de resposta a incidentes e **dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem**, incluindo: **testes e trilhas de auditoria, métricas e indicadores, correção de eventuais deficiências**, entre outros.

Resolução 4.893 - Banco Central

As instituições referidas no art. 1º que, em 26 de abril de 2018, já tinham contratado a prestação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem devem adequar o contrato para a prestação de tais serviços:

A existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;

A instituição contratante deve assegurar que a prestação dos serviços referidos no caput não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil;

Aplicação do Art. 15. A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada pelas instituições referidas no art. 1º ao Banco Central do Brasil.
E aplicação do Art. 17.

A instituição contratante deve prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

Introdução

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Princípios básicos

Cloud computing é uma tecnologia ***on-demand*** **capaz de entregar serviços de tecnologia de infraestrutura e aplicações de TI** para seus usuários através de **serviços disponíveis na internet.**

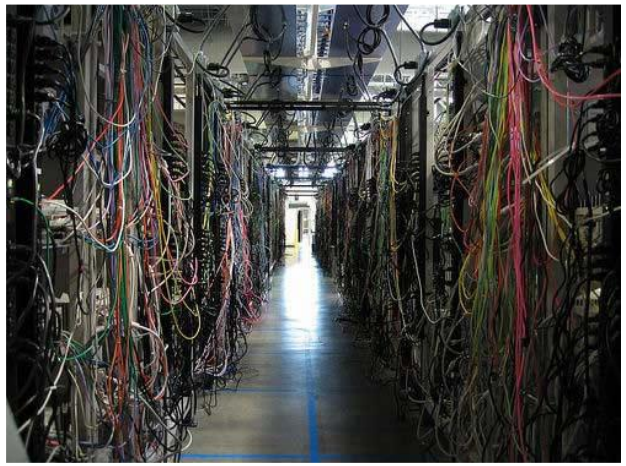
- Servidor de E-mail.
- Servidor de Arquivos.
- Sistema de Relacionamento e Gestão de Clientes (CRM).
  - Os servidores nos pertencem. Precisamos construir do zero, instalar HW, aplicação, atualizações, etc.

Gmail, Outlook
- A infraestrutura onde o serviço é entregue não nos pertence.

Dropbox, G-Drive
- Os serviços são oferecidos em formato de subscrição, ou conforme consumo.

SAP, Salesforce
- O serviço é escalado automaticamente conforme a demanda de utilização.

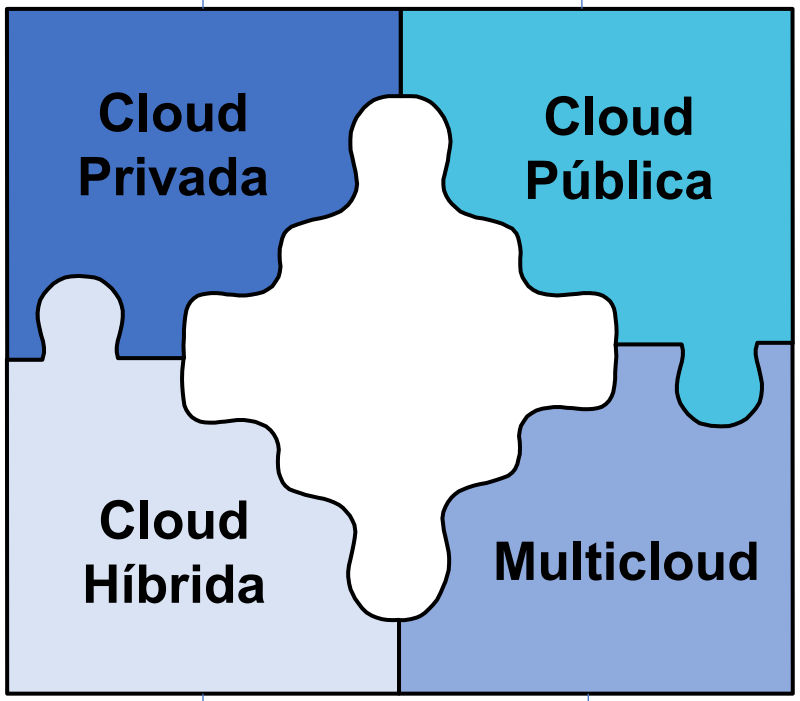
Princípios básicos



Princípios básicos

A seleção do tipo de *deployment* em Cloud dependerá dos requisitos do negócio. **Os serviços em Cloud poderão ser comissionados de diferentes formas a depender de: onde os serviços devem ser hosteados, requisitos de segurança, recursos cloud compartilhados**, possibilidade de gerenciar todo o recurso sem cloud e possibilidades de customizações. **Tipos de deployments em Cloud:**

A corporação realiza o deploy de toda a **infraestrutura e aplicações em seu próprio data center**.
Benefícios:
- Controle completo de toda a stack de hardware e software.
- Segurança. Alguns países não permitem que seus dados estejam sejam armazenados fora de suas fronteiras.



Os serviços de TI que são consumidos são **entregues por um terceiro**, podendo ser um CSP Cloud Service Provider que realiza a entrega através da internet.
Benefícios:
- Despesa variável.
- Economia ao escalar.
- Elasticidade para grande escala.

É uma **combinação** de on-premises / cloud privada e cloud pública.
Benefícios:
- Permite companhias armazenar aplicações críticas e dados sensíveis em data center próprio.
- Alto nível de segurança.
- Altamente escalável podendo ser cloud privada ou pública.

É o uso de **duas um mais cloud públicas simultaneamente**, e a possibilidade de múltiplas cloud privadas.
Benefícios:
- Podem haver aplicações que funcionem melhor no CSP A ou B.
- Maior flexibilidade.
- Menor custo se comparado com cloud privada.

Art. 15. A **contratação de serviços** relevantes de processamento, armazenamento de dados e de computação em nuvem **deve ser comunicada** pelas instituições referidas no art. 1º **ao Banco Central do Brasil**. A comunicação deve conter: **nome da empresa contratada, os serviços contratados, indicação dos países e regiões onde os serviços serão prestados e os dados armazenados**, entre outros.

Princípios básicos

Abaixo seguem as principais características de **Cloud Computing**:

On-demand Self-service:
O usuário pode utilizar recursos em cloud conforme houver necessidade, de forma automática sem interação humana.

Broad Network Access
Recursos de rede estão disponíveis na internet ou WAN –Wide Area Network através do uso de protocolos padrão.

Resource Pooling
Os recursos disponíveis são agrupados e podem servir múltiplos usuários através do modelo *multi-tenant*.

Rapid Elasticity
Os recursos são elásticos e podem escalar com base na demanda de uso.

Measured Services
Os recursos são monitorados e medidos conforme o uso. Pagamento através de pay as you go.

Princípios básicos

Principais **benefícios** em Cloud Computing:

- Agilidade para o negócio
- Menos custo de manutenção
- Pague menos de acordo com o uso
- Menos despesas com capital
- Ambiente amigável
- Custo de propriedade reduzido
- Menos consumo de energia

- Eficiente, efetiva, responsabilidade compartilhada
- Interfaces padrão de mercado para serviços de segurança gerenciados (MSS)
- Gestão de atualizações de patch e implementações de updates efetiva

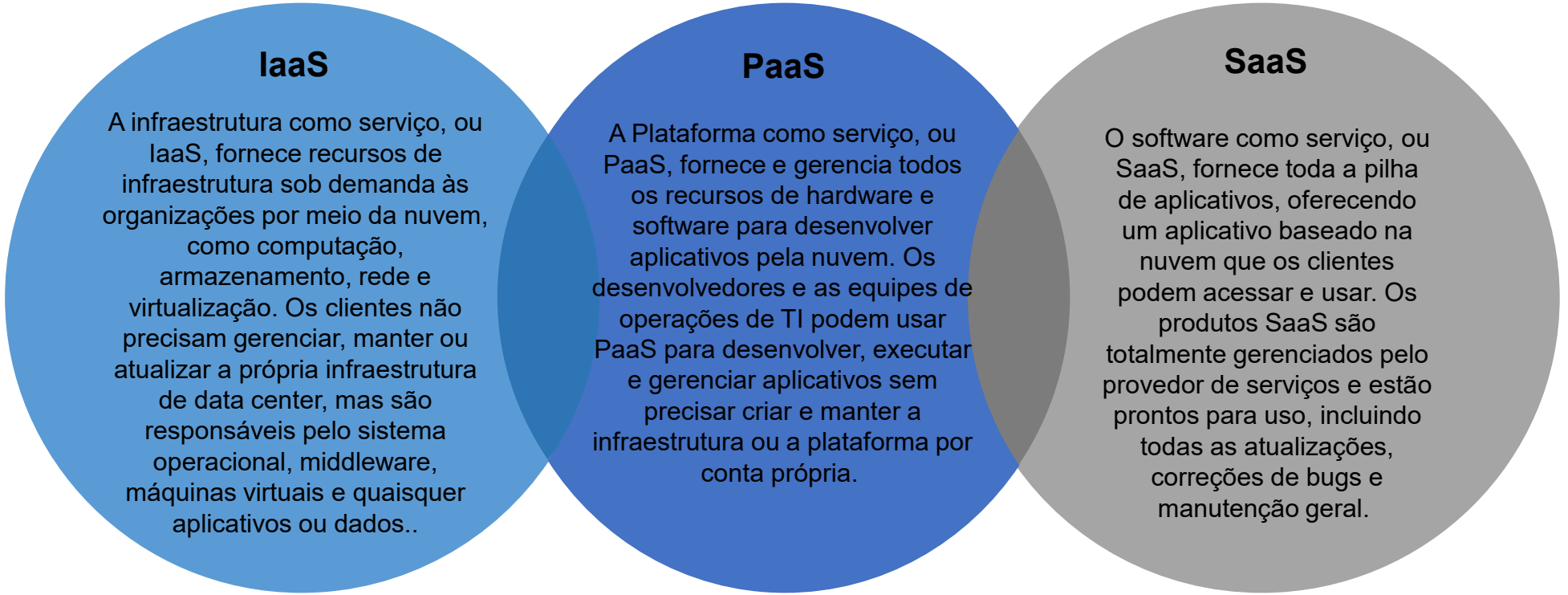
- Flexibilidade e eficiência
- Resiliência e redundância
- Escale conforme a necessidade
- Menos problemas operacionais
- Deploy de aplicações de forma rápida
- Backup e disaster recovery
- Atualizações de software automáticas

- Uso efetivo de recursos
- Treinamentos focados na tecnologia
- Múltiplos usuários podem utilizar os mesmos recursos
- Compartilhamento de pessoal para gestão da infraestrutura
- Trilhas de auditoria
- Acompanhamento com métricas e indicadores

Art. 21. **As instituições devem instituir mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade** da política de segurança cibernética, do plano de ação e de resposta a incidentes e **dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem**, incluindo: testes e trilhas de auditoria, métricas e indicadores, correção de eventuais deficiências, entre outros.

Princípios básicos

A computação em nuvem tem três modelos principais de serviços em nuvem: IaaS (infraestrutura como serviço), PaaS (plataforma como serviço) e SaaS (software como serviço), esses termos se referem a como você usa a nuvem na sua organização e o grau de gerenciamento em que é responsável nos seus ambientes de nuvem.



Cloud Security

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Visão Geral

A segurança em nuvem é uma disciplina de cibersegurança dedicada à proteção de sistemas de computação na nuvem, isso inclui resguardar a segurança e privacidade de dados em infraestrutura, aplicativos e plataformas on-line. Proteger esses sistemas envolve os esforços de provedores da nuvem e dos clientes que as utilizam, seja no caso de pessoa física, pequenas e médias empresas ou grandes organizações. De acordo com a ISO 27002**, a organização deve estabelecer e comunicar políticas específicas sobre o uso de serviços em nuvem a todas as partes interessadas relevantes.**

Principais controles:

Segurança de Infraestrutura

A segurança da infraestrutura e plataforma cloud é composta por um conjunto amplo de **políticas, aplicações, tecnologias e controles que mantém seguro a camada de virtualização IP, serviços, aplicações, dados**, entre outros.

Segurança de Dados

Manter os dados da organização seguros em cloud contra qualquer possibilidade de corrompê-los, acessos não autorizados em **repouso** ou em **trânsito**.

Segurança de Aplicação

Isolar o ambiente cloud para executar aplicações utilizando redes virtuais.

Implementar **verificação** de **vulnerabilidades** em repositório de imagens.

Monitoramento Contínuo

Monitorar continuamente os **recursos em nuvem**, de tal forma que, riscos e **vulnerabilidades sejam gerenciadas** em tempo hábil.

Políticas e procedimentos

Estabelecer e **comunicar políticas** específicas sobre o **uso de serviços em nuvem** a todas as partes interessadas relevantes.

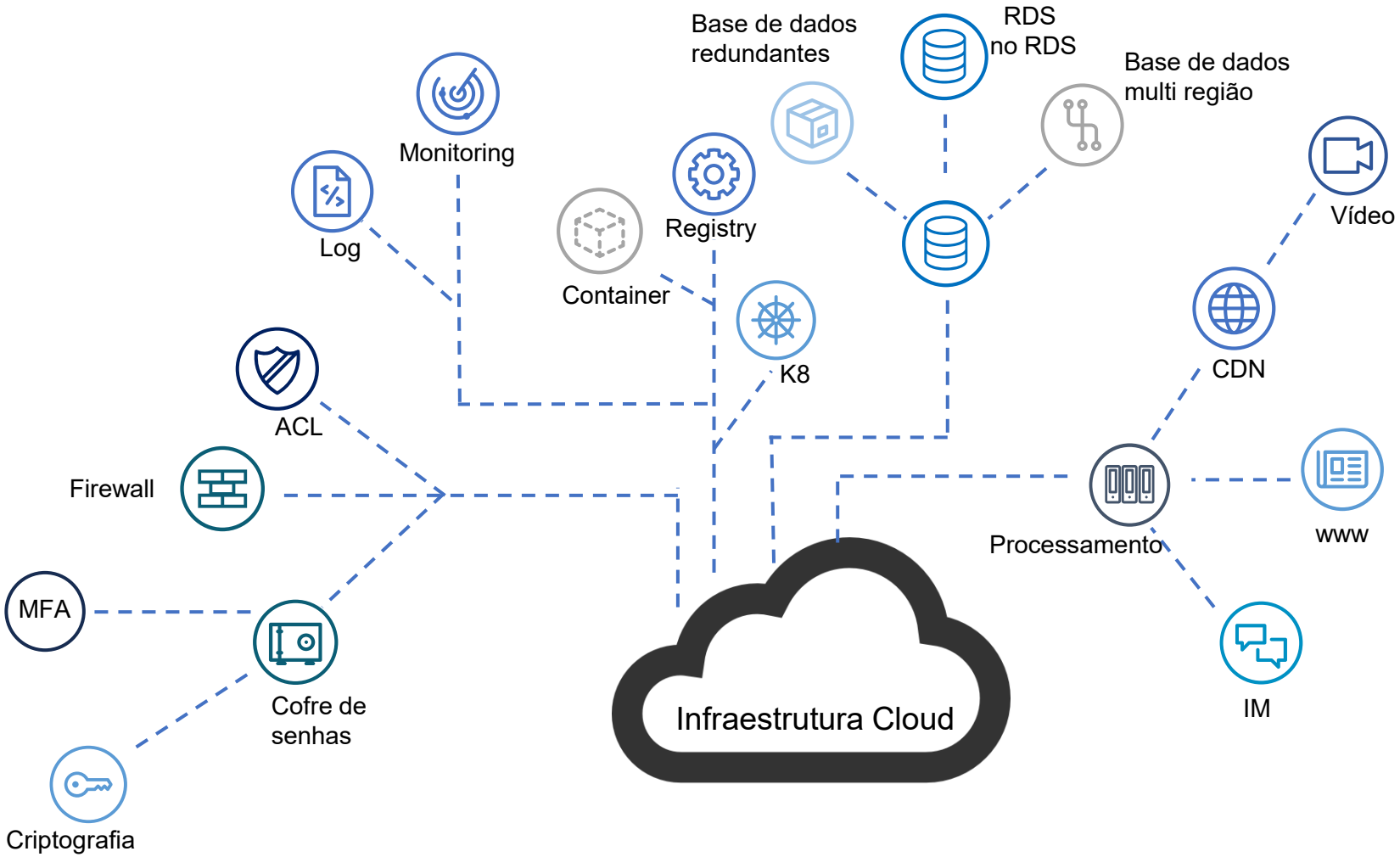
Segurança da infraestrutura

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Segurança de Infraestrutura em Cloud

Como é a Infraestrutura Cloud?

✓ A infraestrutura cloud abrange todos os elementos de hardware e software necessários para entregar os serviços de cloud para os usuários. Na infraestrutura cloud temos data center compostos por processamento computacional, armazenamento de dados, elementos de rede para switching e roteamento, softwares de virtualização e uma camada de gestão. Os componentes básicos de uma infraestrutura cloud são os mesmos nos três modelos de arquiteturas disponíveis (privado, público e híbrido).



Principais Componentes da Infraestrutura Cloud

- Software de gestão
- Software de deploy
- Hypervisor
- Rede
- Servidor
- Armazenamento

Segurança de Infraestrutura em Cloud - Ameaças

FEBRABAN

Prevenção:

Desastres naturais danificando a infraestrutura cloud

Desastres naturais como incêndio, terremotos são considerados desastres naturais e sérias ameaças considerando que eles podem trazer grandes problemas a infraestrutura cloud.

Realize risk assessment para reduzir consequências de um desastre natural. Implemente alternativas para GCN em caso de disrupções

Acesso físico não autorizado a equipamentos do ambiente cloud

Usuários que conseguem acesso físico ao ambiente cloud ou seus equipamentos podem causar ataques de negação de serviço (DoS).

Utilize ferramenta de assessment de risco para mitigar acesso não autorizado ao ambiente dos equipamentos da infraestrutura cloud.

Negligência do funcionário

A negligência pode levar a deleção acidental, perda de backups ou perda de segurança no acesso ao ambiente e a perda de logs de operação.

Utilize um plano de gestão de risco combinado a políticas de segurança.

Escalonamento de privilégios

Utilizando a memória compartilhada da máquina virtual ou da hypervisor do hostcloud, atacantes podem usar a máquina virtual para comprometer outro host/máquina virtual realizando tentativas de acesso laterais.

Realize atualizações de software para hypervisor quando possível, e implemente medidas para enforcement nos acessos privilegiados existentes.

Criptografia Obsoleta

Uma implementação não efetiva de criptografia ou de protocolos de encriptação é uma ameaça séria a infraestrutura e plataforma cloud.

Implementação de técnicas de segurança e algoritmos modernos, com técnicas de criptografias testadas no mercado de criptografia de chave pública e privadas.

Falta de Monitoramento e Logging

Quando não realizado o armazenamento de logs importantes e não realizado o monitoramento devido na infraestrutura, será muito difícil realizar a análise da causa raiz de problemas de serviço ou usuários sem todas as evidências possíveis.

Utilize um sistema de monitoramento de logging robusto. Utilize as ferramentas adequadas disponíveis, salve todos os logs possíveis e utilize políticas de retenção e políticas de acesso a logs.

Art. 16. A **contratação de serviços** relevantes de processamento, armazenamento de dados e de computação em **nuvem prestados no exterior** deve observar os seguintes requisitos: **a instituição contratante deve definir os países e as regiões** em cada país **onde os serviços poderão ser prestados e os dados poderão ser armazenados**, processados e gerenciados, além disso, **prever alternativas para a continuidade dos negócio em caso de disrupções**, entre outros.

Segurança de Infraestrutura em Cloud

✓ A segurança da infraestrutura e plataforma cloud é composta por um conjunto amplo de **políticas, aplicações, tecnologias e controles que mantém seguro a camada de virtualização IP, serviços, aplicações, dados** e etc.

Art. 12. As **instituições** mencionadas previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, **devem adotar procedimentos de segurança**, tais como: **adoção de práticas de governança corporativa, proteção dos dados processados ou armazenados, segregação de dados, qualidade dos dados, entre outros**.

Segurança de dados

A infraestrutura cloud armazena dados sensíveis. Manter uma arquitetura segura com os devidos protocolos de segurança, **minimiza a possibilidade de exfiltrar ou alterar dados em trânsito.**

Regulatório e Compliance

As soluções de segurança suportam as empresas a estarem em **conformidade** com os mais diversos **padrões regulatórios** da **indústria** em especial aqueles relacionados a **confidencialidade de dados financeiros e dados pessoais**.

Controle de acesso

Considerando algumas exceções, devemos **evitar o uso de repositórios públicos**. Atribuir somente o acesso necessário para qualquer situação.

Detecção de ameaças

Técnicas avançadas como escanear o endpoint, comparação de binários, **comparar com ameaças conhecidas e comportamentos fora de padrão**.

Alta disponibilidade

Boas práticas de segurança incluem **entregar serviço com alta disponibilidade**, funcionando em escala 24x7 e entregando monitoramento continuo.

Proteção DDoS

Soluções de segurança em nuvem focam em medidas de segurança que **previnem grandes volumes de dados** de serem direcionados à servidores da infraestrutura cloud.

Segurança de Infraestrutura em Cloud

FEBRABAN

✓ Os elementos presentes no data center como servidores, equipamentos de rede, bancos de dados e etc. e o próprio ambiente são protegidos de várias ameaças como desastres naturais, cyberataques, incêndio, roubo e etc.

Abaixo seguem algumas **boas práticas para segurança implementadas nos elementos** do ambiente físico da **infraestrutura** e plataforma cloud:

1. **Controle de Acesso**
   As instalações do data center devem conter múltiplas camadas de controle de acesso para prevenir o acesso não autorizado no ambiente.
2. **Impor Segurança Física**
   As instalações devem contar várias medidas físicas para preservar a integridade física do data center.
3. **Incêndio**
   O data center deve estar equipado com um ótimo sistema de detecção de incêndio.
4. **Monitoramento**
   O data center deve estar equipado com sistemas de monitoramento por câmeras em sua área interna e externa para detector atividades suspeitas.
5. **Múltiplos Níveis de Segurança**
   O data center deve conter múltiplas proteções de segurança e acesso ao ambiente, e o acesso deve ser limitado a empregados.

Segurança de Infraestrutura em Cloud

✓ O cloud servisse provider e seus usuários são **responsáveis pela segurança da virtualização da rede**.

Responsabilidades do Cloud Service Provider

- Implementar uma infraestrutura Segura de rede.
- Segregar e isolar o tráfego de rede para restringir que um tenant veja o tráfego de outro tenant é de responsabilidade do CSP.
- Desabilitar *packetsniffing* e se certificar de não haver vazamento de dados entre tenants.
- Habilitar firewall dentro de todas as redes virtuais.
- Detectar e mitigar ataques na plataforma de virtualização e na rede física.

Responsabilidades dos Usuários

- Configurar corretamente a rede virtual e suas regras de firewall.
- Desenhar a arquitetura de rede segundo boas práticas de arquitetura e segurança.
- Aplicar boas práticas de configuração de rede definindo templates para este uso onde poderão ser reutilizados.
- Configure os controles expostos na camada de gerenciamento.

Segurança de Infraestrutura em Cloud

Segurança Computacional

✓ O recurso computacional (instância) possui a capacidade de alocar e gerenciar recursos adicionais de forma eficaz.
✓ A utilização de alocação, limites e compartilhamento de recursos entrega capacidade de conhecimento para o “admin” do servidor alocar as instâncias.

Comportamento Seguro - Boas Práticas de Segurança Para Servidor

- **Implementar múltiplos níveis de segurança** para o servidor da infraestrutura cloud, no SO do **host virtual, habilitar firewall, regras de acesso** etc.
- **A instância deve escalar para mais ou menos recursos automaticamente** para atender os requisitos da aplicação.
- Várias **instâncias** executando na mesma máquina física **devem ser isoladas através da *hypervisor***.
- **Desabilite o acesso remoto**. Faça o uso da ferramenta adequada para esta atividade.
- Sempre que possível, faça o **refresh na infraestrutura**.
- A **criação de imagens** devem ser seguidas de **testes de segurança**.
- Realize o update na imagem e realize testes.
- Implemente agentes de *awareness* que não irão impactar em performance.
- **Logs importantes devem ser armazenados em um local seguro**, deve ser externo ao workload/instância.

Segurança de Infraestrutura em Cloud

Segurança de Imagem de Virtual Machine (Instâncias)

✓ Imagens de instâncias em cloud são parte da infraestrutura, elas trabalham em conjunto com a hypervisor.
✓ Para proteger as informações sensíveis de usuários e manter a integridade dos dados, **as imagens devem estar seguras e com boas práticas de segurança implementadas**

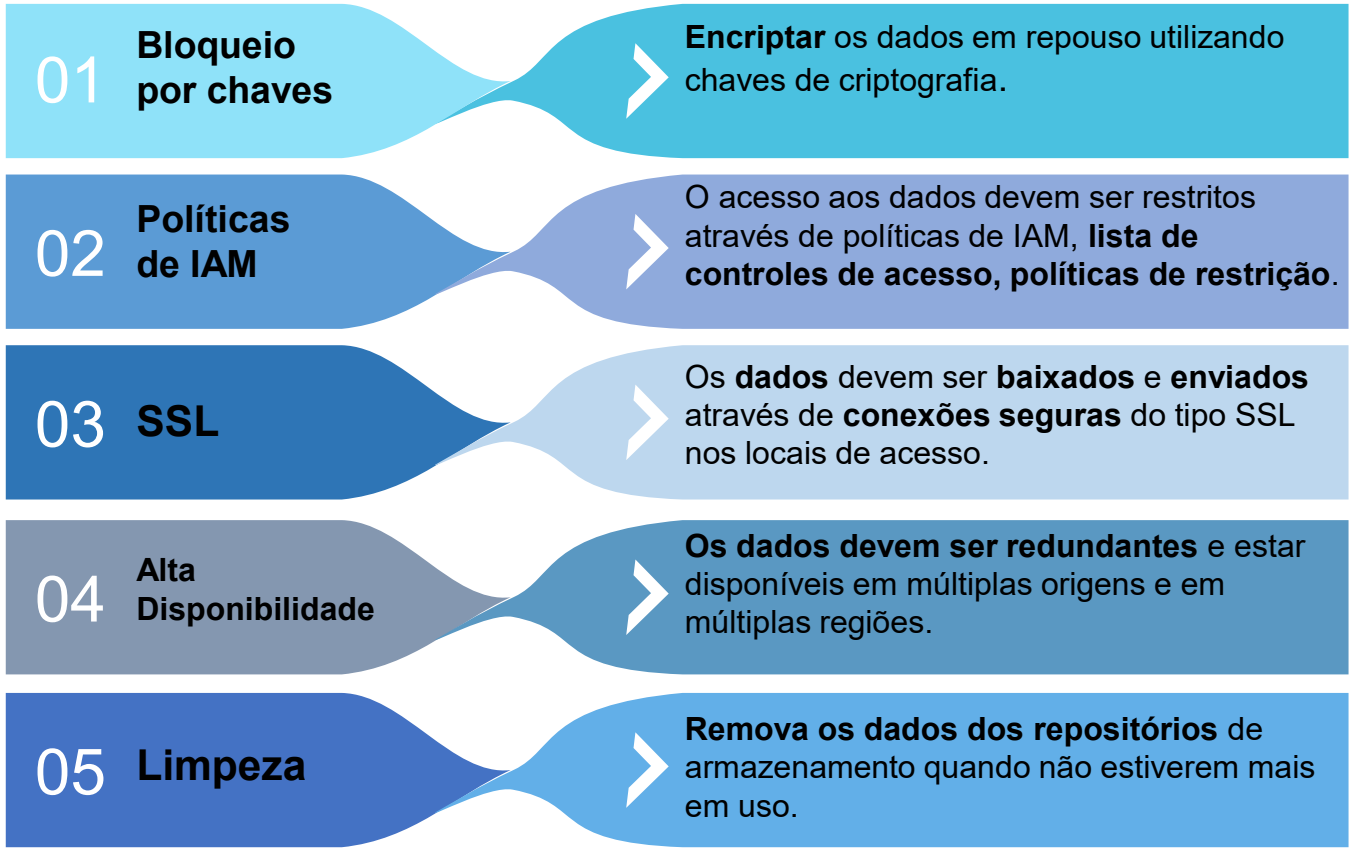
Comportamento Seguro - Boas Práticas de Segurança para Imagens de Instâncias

- Implementar criptografia nas imagens.
- Aplicar os últimos patches disponíveis para manter as imagens seguras.
- Realizar backup com frequência das imagens.
- Aplicar criptografia nos backups das imagens.
- Utilizar imagens prontas e hardenizadas de *marketplace*.

Segurança de Infraestrutura em Cloud

Segurança em Armazenamento

- ✓ Virtualizar o armazenamento é confiável e **mantém múltiplas cópias dos dados em diferentes localidades**, desta forma melhoramos a segurança, e disponibilidade dos dados.
- ✓ **Encriptar os repositórios de armazenamento reduz a superfície de exposição dos dados** caso seja necessário realizar a troca de hardware.



Art. 17. Os **contratos** para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem **devem prever: adoção de medidas de segurança para a transmissão e armazenamento dos dados**, além disso, a **manutenção da segregação dos dados e dos controles de acesso para proteção das informações dos clientes**, entre outros.

Segurança de Aplicação

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Segurança de Aplicação

O que é uma aplicação Cloud?

- ✓ **Uma aplicação cloud é baseada em uma conexão** de software **utilizando o acesso à internet**, **através de um navegador web** ou interface de aplicação programável (API) que é implementada no ambiente cloud.
- ✓ Aplicações cloud utilizam servidores instalados em ambientes remotos para armazenar dados e processamento lógico.

Ameaças de Segurança para Aplicações Cloud?

Configuração Incorreta

Soluções:

Salve logs, configure segmentação de redes e utilize aplicações de auditoria.

Acesso não Autorização a Aplicação

Soluções:

Utilize controle de acesso restrito, faça uso de políticas de acesso para delegar o mínimo privilégio.

Ataques DDoS Na Camada de Aplicação

Soluções:

Além de WAF, implemente balanceadores de carga para distribuir o tráfego entre os servidores de aplicações.

Interface de API Insegura

Soluções:

Implemente um processo de autenticação, controle de acesso a API, criptografia e monitore toda atividade de tráfego para APIs.

Vazamento de Dados

Soluções:

Tenha um plano de recuperação de dados com os procedimentos para realizar a recuperação sempre atualizados.

Segurança de Aplicação

✓ Boas Práticas de Segurança Para Design de Arquiteturas de Aplicações em Cloud

- Isole o ambiente cloud para executar aplicações utilizando redes virtuais.
- Utilize contas de produção, homologação e desenvolvimento.
- Utilize contas e estruturas de contas para possibilitar a segregação da gestão.

- Certifique-se de que a comunicação entre microsserviços está configurada corretamente.
- Implemente verificação de vulnerabilidades em repositório de imagens.
- Implemente verificação de vulnerabilidades em repositório de códigos de IaC.

- Desabilite o acesso remoto a servidores que não necessitam alteração.
- Implemente planos de recuperação de infraestrutura padrão.
- Implemente verificação de integridade e monitoramento de arquivos.

- Executar cargas de trabalho utilizando uma plataforma PaaS reduz a superfície de ataque. A gestão de serviços e sistema operacional é realizada diretamente pelo CSP.
- O CSP deve garantir a segurança da plataforma e serviços serverless. A responsabilidade para garantir a segurança do PaaS, e arquiteturas serverless são inteiramente do CSP.
- Plataformas serverless previnem ataques diretos a redes do cliente uma vez que utilizam redes privadas do CSP e toda comunicação é através de API ou tráfego HTTPS.

Segurança de Aplicação

✓ Assessment Contra Vulnerabilidades em Pipeline CI/CD (desenvolvimento)

Assessment Contra Vulnerabilidades

- Considere integrar um **assessment contra vulnerabilidades** automático em sua pipeline com ferramentas que irão **realizar scan em imagens, containers e códigos** em um local específico para esta finalidade, podendo ser um local de rede apartado de seu ambiente produtivo como uma pipeline de testes ou homologação.

Ambiente de Teste

- **Considere construir um ambiente de teste que possibilite testar toda a infraestrutura**. Uma opção rápida para construir e desconstruir é através de IaC Infrastructure as Code.

Ferramentas de Assessment Contra Vulnerabilidade Baseado em Host

- Considere utilizar aplicações que realizam **assessment** e checagens de boas práticas de segurança do tipo ***endpoint protection*** baseados em host.

Segurança de Aplicação

✓ Aplicações adicionais para proteção de aplicações em Cloud

Web Application Firewall

São capazes de inspecionar a troca de mensagens a nível de aplicação contra ataques que podem ocorrer em arquivos XMLs e chamadas de APIs. Muitas aplicações não possuem proteção contra estes ataques e necessitam de proteção adicional onde o web application firewall pode analisar, inspecionar e bloquear estas ameaças.

Database Activity Monitoring

Uma aplicação que monitora, analisa e armazena **atividades que ocorrem em base de dados em tempo real e envia alertas em caso de violação de políticas** pré estabelecidas, possibilitando a organização a monitorar de forma mais pró ativa suas bases de dados. Toda ação que é realizada em bases de dados através de aplicações são logadas para análise posterior. Logs podem ser enviados em tempo real para um SIEM para análise em tempo real de ameaças.

API Gateway

API Gateway costumam ser alvos de ataques pois tendem a expor dados e infraestrutura acima do necessário. API Gateway servem como um ponto único de entrada e precisam ser construídos e gerenciados de forma cautelosa. **API Gateways podem ser integrados com aplicações de IAM, log e monitoramento para proporcionar mais segurança**.

XML Gateway/DLP

XML Gateway (ou XML Firewall) proporcionar segurança para aplicações cloud através de inspeção e análise em tráfego SOAP, REST, JSON e XML **para detector tentativas maliciosas para comprometer a segurança da aplicação**. XML Gateway pode trabalhar em conjunto com DLP Data Loss Prevention para minimizar a possibilidade de vazamento dados.

Considerações Finais

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Frameworks e Normas de Referência

Para apoiar no entendimento e implementação de toda a metodologia apresentada neste material, a seguir são apresentados as normas e frameworks de referência no tema:

Frameworks Padrão Utilizados

ISO 27017 International Organization for Standardization

NIST National Institute of Standards and Technology

BANCO CENTRAL DO BRASIL

NIST 800-53 Revision 5 Security Controls

Conformidade: Dado o uso extensivo de padrões amplamente aceitos pela indústria, a segurança em cloud deve ser alinhada com alguns dos requisitos de conformidade mais exigentes, permitindo estimar o nível de conformidade com PCI-DSS, ISO, Bacen 4.893, NIST, entre outros.

Relembrando os principais conceitos

Agora que aprendemos sobre as atividades relacionadas ao processo de Cloud, relembre os principais termos e conceitos apresentados neste material:

Deployments de Cloud para cada necessidade: A seleção de Cloud será baseada nos requisitos do negócio, podendo variar entre Cloud Pública, Cloud Privada, Cloud híbrida e multicloud.

Segurança e infraestrutura em Cloud: são estruturas principais em Cloud: Software de gestão, software de deploy, hypervisor, rede, servidor, armazenamento. Para a maior proteção em Cloud existem camadas de segurança que buscam diminuir possíveis consequências de ativos negativos, entre estas camadas temos: Segurança de dados, controle de acesso, detecção de ameaças, proteção DDoS, alta disponibilidade, e regulatório e compliance

Segurança de aplicação em Cloud: A aplicação cloud é baseada em uma conexão de software utilizando o acesso à internet, e para esta também é necessário seguir algumas indicações principais de práticas de segurança, entre estas estão: o isolamento de ambientes, uma infraestrutura imutável, PaaS e arquitetura serverless, e microsserviços

Módulo: Monitoramento e Defesa de Rede

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Requisitos – Monitoramento e Defesa de Rede

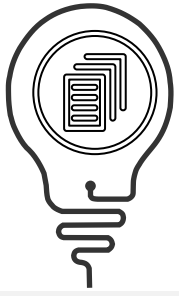
FEBRABAN

Este material foi elaborado de acordo com as diretrizes do CIS Controls e PCI DSS, bem como foram considerados os requisitos de segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

CIS Controls

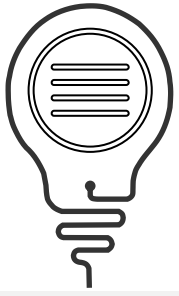
- 13.1 Centralizar o alerta de eventos de segurança
- 13.2 Implantar solução de detecção de intrusão baseada em host
- 13.3 Implantar uma solução de detecção de intrusão de rede
- 13.4 Realizar filtragem de tráfego entre segmentos de rede
- 13.5 Gerenciar controle de acesso para ativos remotos
- 13.6 Coletar logs de fluxo de tráfego da rede
- 13.7 Implantar solução de prevenção de intrusão baseada em host
- 13.8 Implantar uma solução de prevenção de intrusão de rede
- 13.9 Implantar controle de acesso no nível de porta
- 13.10 Executar filtragem da camada de aplicação
- 13.11 Ajustar Limites de Alerta de Eventos de Segurança

PCI DSS



- 1.1 Os processos e mecanismos para instalar e manter os controles de segurança da rede são definidos e compreendidos.
- 1.2 Os controles de segurança de rede (NSCs) são configurados e mantidos.
- 1.3 O acesso à rede de e para o ambiente de dados do titular do cartão é restrito.
- 1.4 As conexões de rede entre redes confiáveis e não confiáveis são controladas.
- 1.5 Os riscos para o CDE de dispositivos de computação que são capazes de se conectar a redes não confiáveis e ao CDE são mitigados.
- 2.3 Os ambientes wireless são configurados e administrados com segurança.
- 11.2 Os pontos de acesso wireless são identificados e monitorados, e os pontos de acesso wireless não autorizados são endereçados.
- 11.5 Intrusões de rede e mudanças inesperadas de arquivos são detectadas e respondidas.
- 11.6 Mudanças não autorizadas nas páginas de pagamento são detectadas e respondidas.

ISO 27002

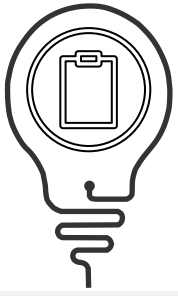


- 8.20 Segurança de redes
- 8.21 Segurança de serviços de rede
- 8.22 Segregação de redes
- 8.23 Filtragem da Web

ISO 27701

- 6.10.1.1 Controles de redes
- 6.10.1.2 Segurança dos serviços de rede
- 6.10.1.3 Segregação de redes

NIST CSF



- ID.AM-03: Representações da comunicação de rede autorizada da organização e fluxos de dados de rede interna e externa são mantidos
- PR.IR-01: Redes e ambientes são protegidos contra acesso lógico e uso não autorizados

Sumário

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Sumário

Contextualização

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Casos Reais

Incidentes

Microsoft notifica clientes atingidos na invasão de sua rede

https://www.cisoadvisor.com.br/microsoft-notifica-clientes-atingidos-na-invasao-de-sua-rede/

You don't often get email from mbsupport@microsoft.com. Learn why this is important

This notification is related to the prior attack against Microsoft by the threat actor known as Midnight Blizzard, as disclosed through our 8-K filings and our Microsoft

You are receiving this notification because emails were exchanged between Microsoft and accounts in your organization, and those emails were accessed by the thr Microsoft.

As part of our commitment to transparency, we are proactively sharing these emails. We have custom built a secure system to enable the approved members of yo Microsoft and your company.

In order to grant access to the above-referenced emails, you are required to identify authorized individuals within your organization who can nominate reviewers. A organization who have the authority to nominate reviewers to view these emails.

At the bottom of this email is a link which will take you to a secure form where you will be asked to provide the following information:

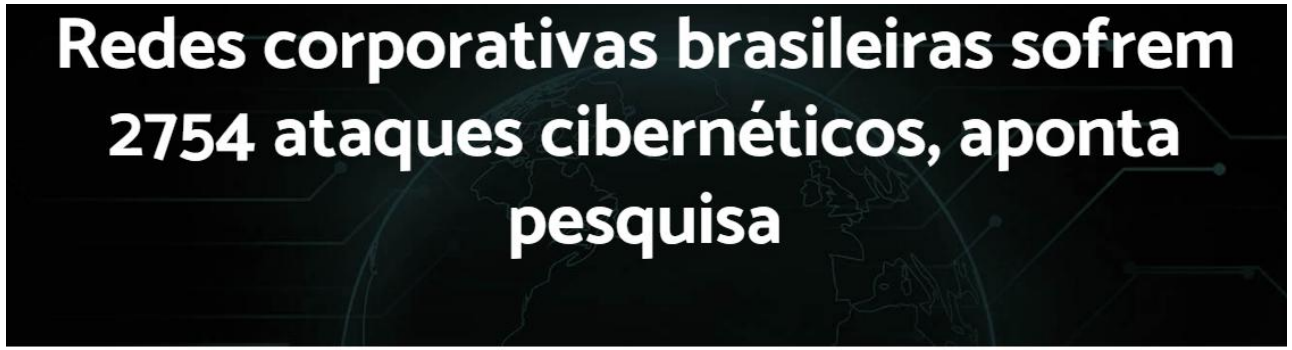
- Your organization's TenantID
  - If you do not know or are unsure of your TenantID, please follow the steps outlined here: https://aka.ms/gettenantid
- The access code located at the bottom of this email
- The email addresses for individuals within your organization who can nominate reviewers who will be granted access to the set of exfiltrated emails.

Once you complete this form, Microsoft will contact those who have been identified with instructions on how to identify reviewers.

Should you or your organization require support during this process please work with your Customer Success Account Manager (CSAM) or account representative(s Sharing. Microsoft continues to prioritize transparency and learnings from events like these to help protect customers and our own enterprise.

Our investigation is ongoing, if we discover new information, we will tell you as soon as practicable.

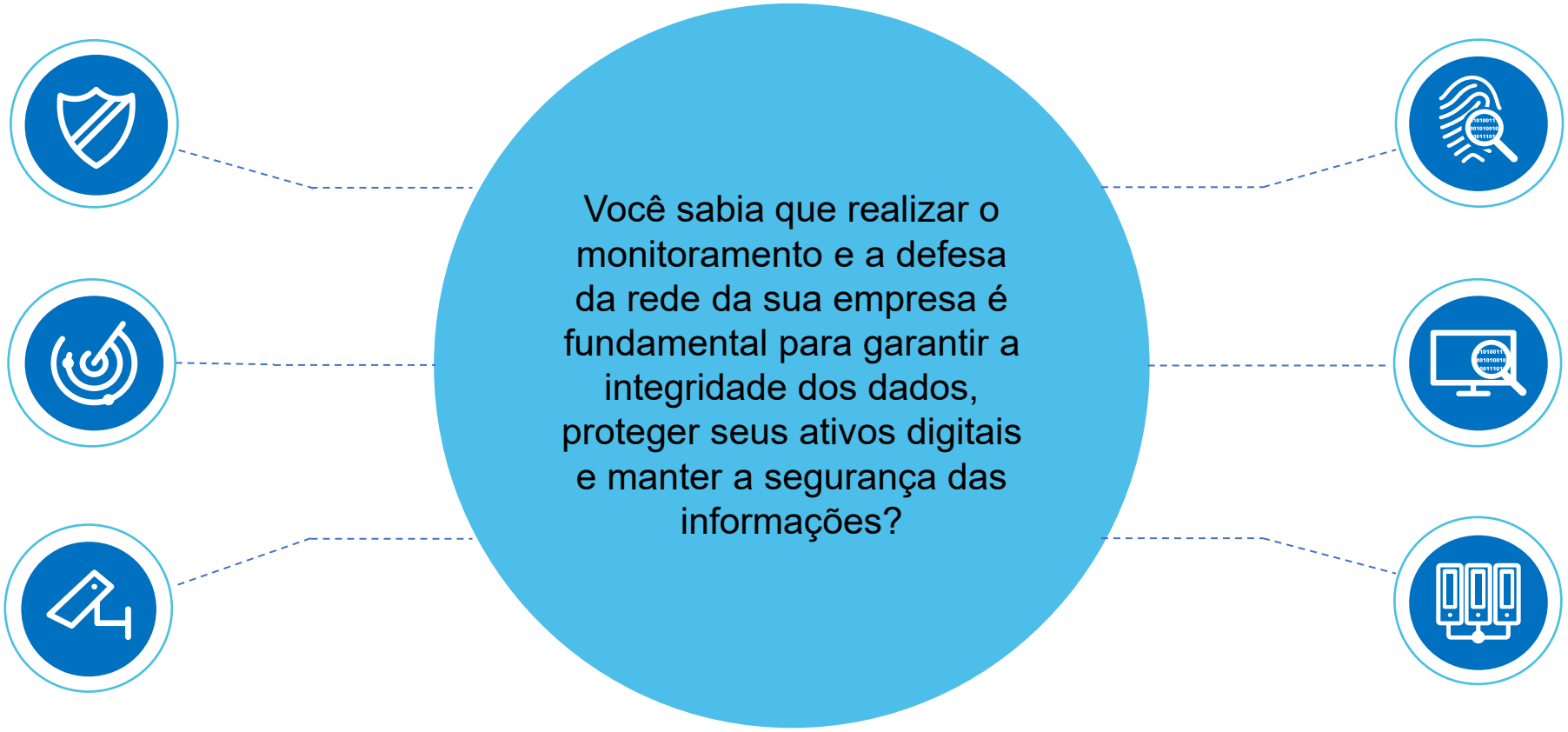
Secure Link: https://purviewcustomer.powerappsportals.com[redacted]
Access Code: [redacted]



Redes corporativas brasileiras sofrem 2754 ataques cibernéticos, aponta pesquisa

https://www.venkonetworks.com/noticias/redes-corporativas-brasileiras-sofrem-2754-ataques-ciberneticos.php#:~:text=No%20Brasil%2C%20o%20relat%C3%B3rio%20da,foram%20registrados%201.645%20ataques%20semanais.

Contexto


Você sabia que realizar o monitoramento e a defesa da rede da sua empresa é fundamental para garantir a integridade dos dados, proteger seus ativos digitais e manter a segurança das informações?

Introdução

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Introdução

De acordo com a ISO 27002, **as redes e dispositivos de rede devem ser protegidos, gerenciados e controlados para proteger informações em sistemas e aplicativos**. Além disso, os mecanismos de segurança, os níveis de serviço e os seus requisitos devem ser identificados, implementados e monitorizados.

Principais controles:

Monitoramento

O monitoramento constante permite **identificar atividades suspeitas, como acessos não autorizados, malware e comportamentos anormais**. Assim, é possível prevenir ameaças iniciais e tomar medidas imediatas para mitigá-las.

Detecção de Intrusão

Implemente **controles de segurança, como firewalls, sistemas de detecção e prevenção de intrusões (IDS/IPS), filtros de spam e antivírus**. Essas medidas ajudam a impedir ataques antes que eles afetem sua rede e sistemas.

Centralize os alertas de segurança

Centralize os alertas de eventos de segurança em ativos corporativos para correlação e análise de log, por exemplo, por meio de uma tecnologia de **SIEM**, que inclui alertas de correlação de eventos.

Proteção de dados sensíveis

Empresas armazenam dados valiosos, como informações financeiras, dados de clientes e propriedade intelectual. O monitoramento e a defesa de rede **ajudam a proteger essas informações contra acesso não autorizado e roubo.**

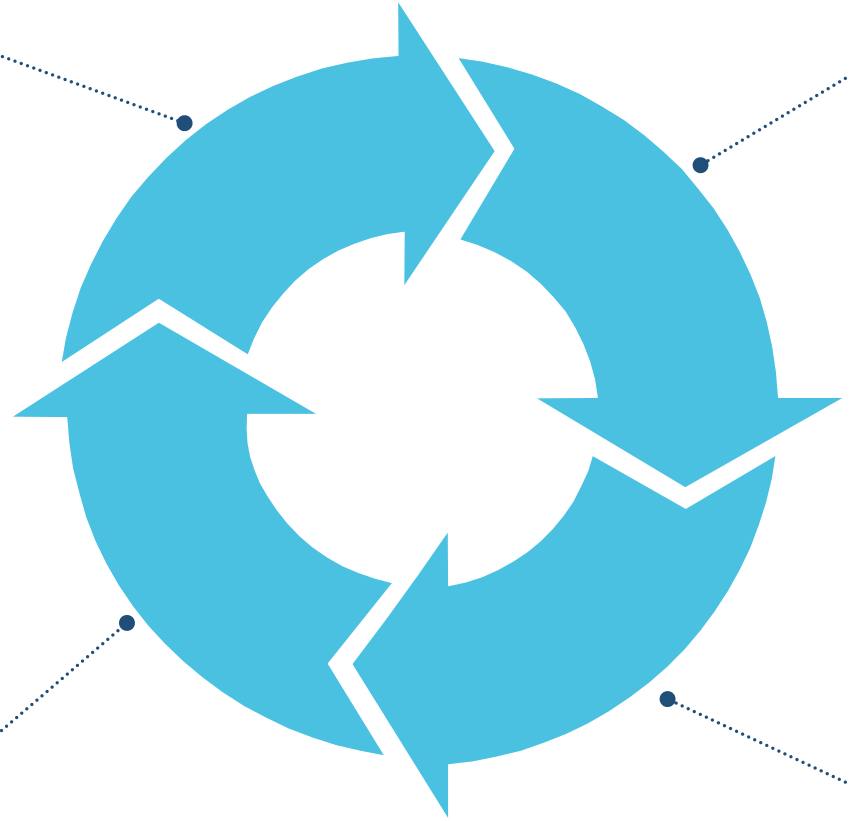
Boas Práticas

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Abordagem - Monitoramento de Rede

1 - Prevenção

Consiste em monitorar uma rede de maneira preventiva, visando identificar atividades maliciosas ou tráfegos suspeitos. Além de implementar controles para assegurar a confidencialidade, integridade e disponibilidade da rede, por exemplo: controle de dispositivos, criptografia de disco, firewall de host, entre outros.



2 - Detecção

Quando um problema é detectado, o sistema de monitoramento de rede pode enviar um alerta ao administrador com um relatório de análise de rede. Desta forma uma ação poderá ser definida imediatamente, buscando a resolução de potenciais problemas, com assertividade e eficácia.

3 - Rápida investigação

Identificar, preservar, analisar a causa raiz, recuperar e apresentar fatos acerca de uma informação em meio digital.

4 - Resposta e Adaptação

Resposta a incidentes refere-se aos processos e tecnologias de uma organização para detectar e responder a ameaças cibernéticas, violações de segurança ou ataques cibernéticos.

Soluções e Serviços - Prevenção de Intrusão

EDR, MDR e XDR

EDR

O EDR (*Endpoint Detection and Response*) é um **software** projetado para ajudar as empresas a **identificar, interromper e reagir a ameaças ou ataques que se manifestam por meio de dispositivos terminais** (laptops, desktops, tablets, smartphones, etc.).

Assim como outros softwares de segurança de endpoints, o EDR é implantado instalando agentes em endpoints e pode ser gerenciado por meio de software na infraestrutura local ou por meio de um portal baseado em nuvem.

As soluções de EDR podem detectar malwares que foram criados para evitar o software antivírus tradicional.

MDR

O MDR (*Managed Detection and Response*) é um **serviço de segurança** gerenciado avançado, **fornecendo monitoramento contínuo e resposta a incidentes**. Esse serviço é fornecido por uma equipe especializada, experiente e treinada do centro de operações de segurança, também chamado de SOC (*Security Operacion Center*).

Esses recursos normalmente aproveitam uma plataforma de gerenciamento de informações e eventos de segurança (*SIEM – Security Information Event Management*), que ingere e correlaciona arquivos de metadados de vários dispositivos de TI em toda a rede, incluindo aplicativos de missão crítica e ambientes de nuvem de terceiros.

XDR

Integração de Dados: **XDR (*Extended Detection and Response*) integra dados de várias fontes, incluindo endpoints, redes, nuvem e e-mail**.

Permite correlacionar dados para uma visão mais abrangente das ameaças em todo o ambiente. **Oferece análise contextual para compreender a extensão das ameaças**.

Fornece investigação, resposta e hunting de ameaças e detecção e resposta de endpoint, com a capacidade de escalar para ambientes de nuvem, **integrando-se com diversas fontes de registros de atividades (logs).**

Boas Práticas de Monitoramento de Rede

O processo de monitoramento e análise em tempo real de eventos de segurança e alertas para lidar com ameaças, identificar padrões e responder a incidentes é de grande importância no monitoramento de redes pois **possibilita uma visão centralizada** do mapa de **ameaças, identifica e responde à ameaças em tempo real**, realiza relatórios e identificação de possíveis ameaças e **auxilia na solução de problemas de segurança e vulnerabilidade**.

Centralize os alertas de eventos de segurança em ativos corporativos para correlação e análise de log. A melhor prática requer o uso de um **SIEM**, que inclui **alertas de correlação de eventos definidos** pelo fornecedor. Uma plataforma de análise de log configurada com alertas de correlação relevantes para a segurança também atende a esta medida de segurança.

Colete logs do fluxo de tráfego de rede a partir de dispositivos de rede, tais como: firewalls, VPN, roteadores, switches, entre outros. É recomendável todos esses logs sejam direcionados a ferramenta de SIEM para o correlacionamento e envio de alertas aos administradores.

Implemente uma solução de detecção de intrusão baseada em host em ativos corporativos, quando apropriado e/ou com suporte ou uma solução de detecção de intrusão de rede em ativos corporativos. Exemplos de implementações incluem o uso de um ***Network Intrusion Detection System*** (NIDS) ou serviço de provedor de serviço de nuvem equivalente (CSP).

Os limites de alerta de eventos de segurança devem ser atualizados mensalmente ou com mais frequência, assim como as **regras de correlacionamento e casos de uso** das ferramentas de monitoramento.

Boas Práticas de Monitoramento de Rede

Estabelecer controles para segurança da confidencialidade e integridade de dados ao atravessar redes públicas e terceiras:

Os dispositivos conectados à Internet fora do ambiente corporativo (por exemplo, desktops, laptops e outros endpoints) usados pelos funcionários - **são vulneráveis a ameaças de segurança da informação**.

Uso de controles de segurança, como **controles baseados em host** (por exemplo, soluções de proteção de endpoint), **controles de segurança baseados em rede** (por exemplo, firewalls, inspeção baseada em heurística de rede e simulação de malware) ou **hardware**, ajudam a **proteger os dispositivos de ataques baseados na Internet**, que podem usar o dispositivo para obter acesso aos sistemas e dados da organização quando o dispositivo for reconectado à rede.

Práticas indicadas:

Todos os pontos de acesso wireless devem ser identificados e monitorados, e os pontos de acesso wireless não autorizados são endereçados.

As definições de configuração específicas são determinadas pela entidade e devem ser consistentes com suas políticas e procedimentos de segurança de rede.

Qualquer desativação ou alteração desses controles de segurança, incluindo nos próprios dispositivos dos administradores, é realizada por pessoal autorizado.

É reconhecido que os administradores têm privilégios que podem permitir que desabilitem os controles de segurança em seus próprios computadores, mas devem haver mecanismos de alerta quando esses controles são desabilitados e o acompanhamento que ocorre para garantir que os processos sejam seguidos.

Implementação do NSCs (Controle de Segurança de Rede) em cada conexão que entra e sai de redes confiáveis permitindo que a entidade monitore e controle o acesso e **minimiza as chances de um indivíduo mal-intencionado obter acesso à rede interna por meio de uma conexão desprotegida**.

Os ambientes wireless devem ser configurados e administrados com segurança.

As senhas wireless devem ser construídas de forma que sejam resistentes a ataques de força bruta off-line.

Se as redes wireless não forem implementadas com configurações de segurança suficientes (incluindo a alteração das configurações padrão), os sniffers wireless podem espionar o tráfego, capturar facilmente dados e senhas e entrar e atacar facilmente a rede.

Boas Práticas de Monitoramento de Rede

Implementar solução de prevenção de **intrusão de rede:**

Sistema de detecção de intrusão baseado em rede (NIDS)

É implantado em toda a infraestrutura em pontos estratégicos, como as sub-redes mais vulneráveis. O NIDS **monitora todo o tráfego que flui entre os dispositivos na rede**, fazendo determinações com base no conteúdo dos pacotes e nos metadados.

Implantar uma solução de prevenção de intrusão de rede
Exemplos de implementações incluem o uso de um *Network Intrusion Prevention System* (NIPS) ou serviço CSP equivalente.

Sistema de detecção de intrusão baseado em host (HIDS)

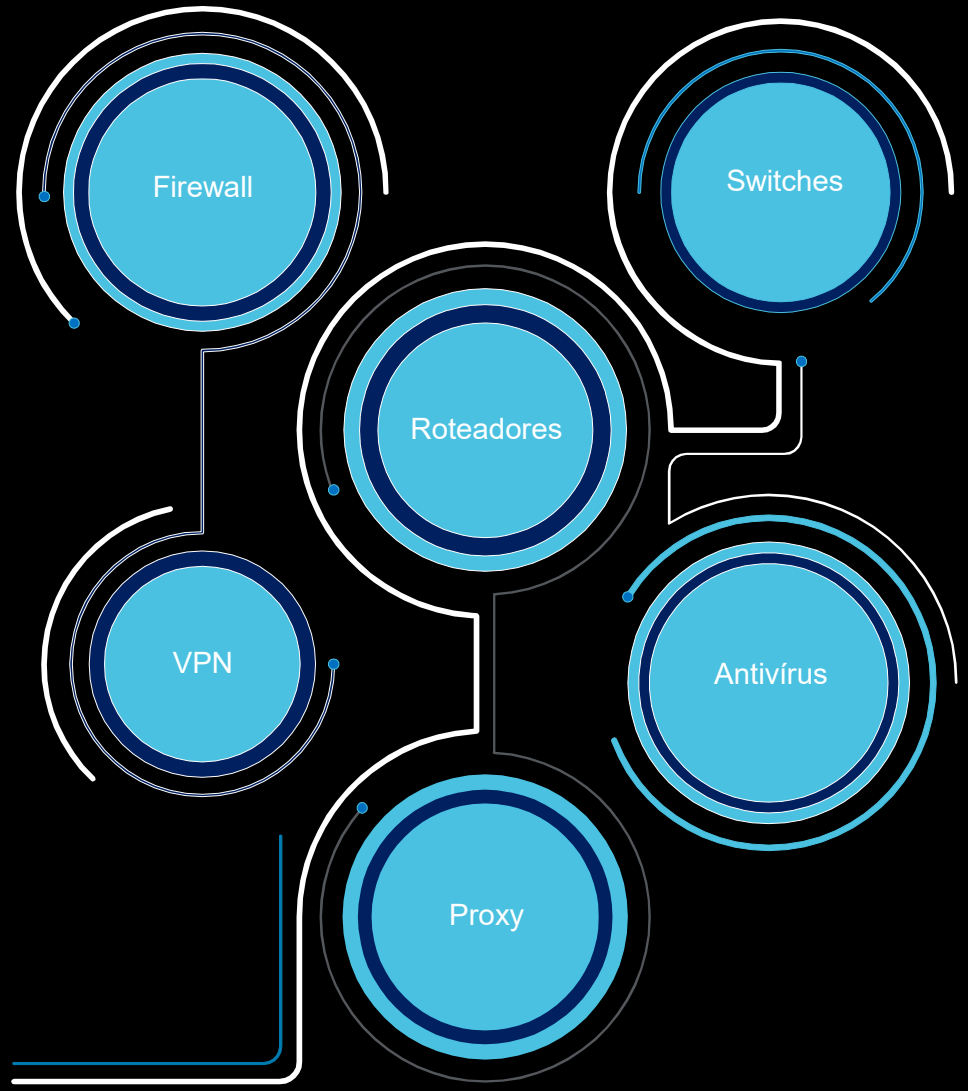
Um IDS baseado em host monitora a infraestrutura do computador na qual está instalado. Em outras palavras, ele é implantado em um endpoint específico para protegê-lo contra ameaças internas e externas. **O IDS faz isso analisando o tráfego, registrando atividades maliciosas e notificando as autoridades designadas**.

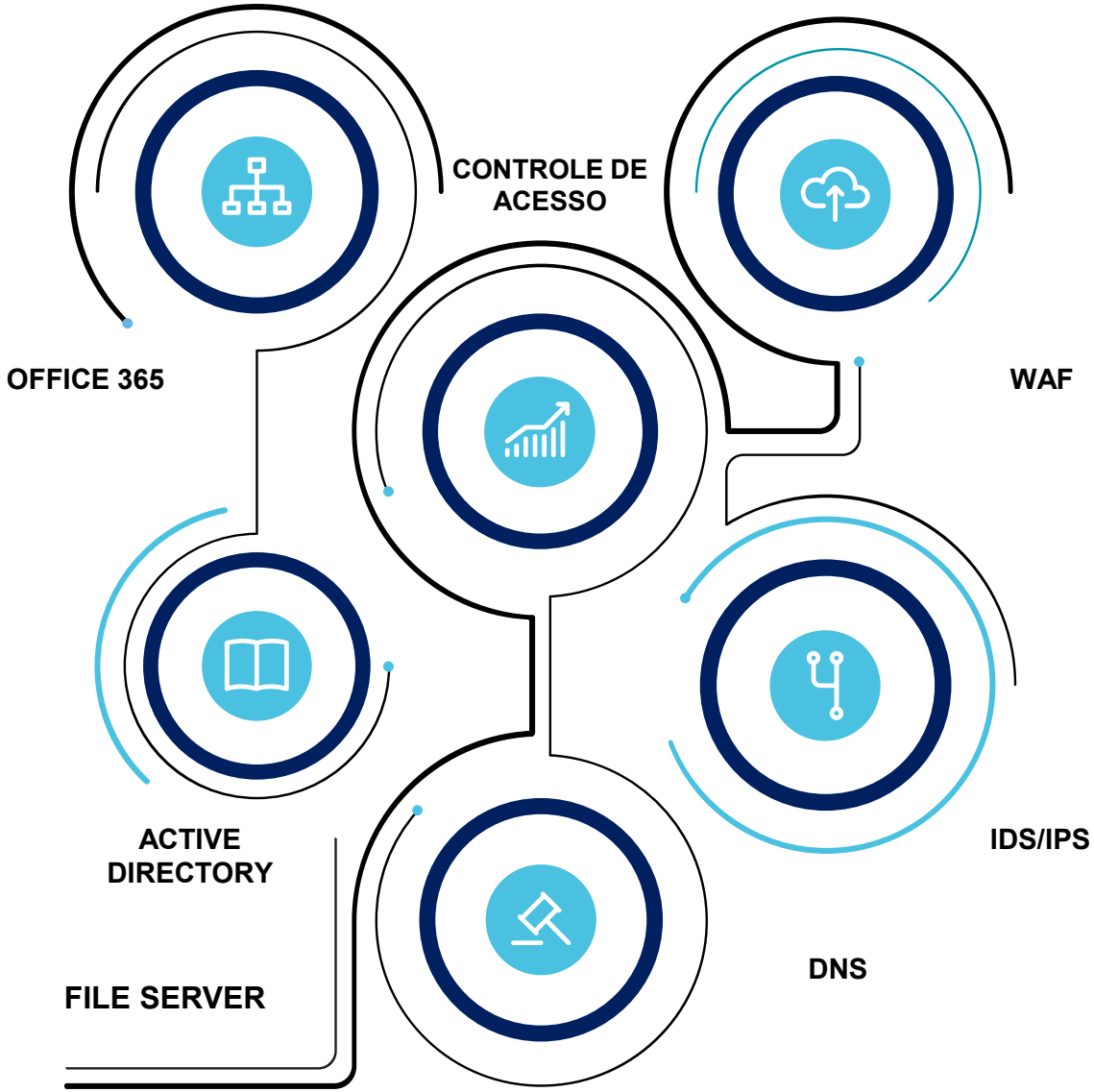
Implante uma solução de prevenção de intrusão baseada em host em ativos corporativos, quando apropriado e/ou com suporte.
Exemplos de implementações incluem o uso de um cliente *Endpoint Detection and Response* (EDR) ou agente IPS baseado em host.

Os alertas de segurança gerados por essas soluções devem ser monitorados continuamente, de modo que as tentativas ou intrusões reais possam ser interrompidas e os danos potenciais limitados.

SIEM

Ampliar a capacidade de monitoramento do ambiente sistêmico, integrando o SIEM com diversas fontes de logs:

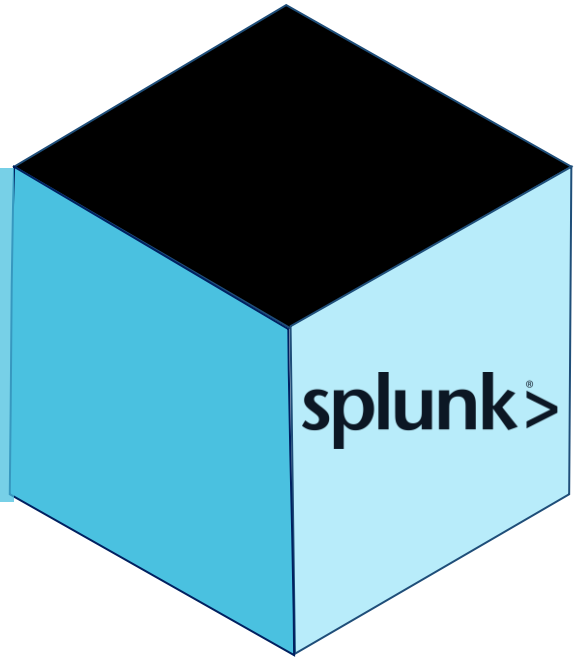




SIEM

O Splunk é uma solução de análise de dados com avançados recursos de SIEM que viabiliza estratégias baseadas em dados, explorando o potencial dos dados corporativos e gerando informações em tempo real. Sua função é monitorar e processar dados em tempo real, utilizando sistemas de análise avançados.

O Splunk é alimentado por soluções IA para segurança e monitoramento que aceleram a detecção, investigação e resposta. É auxiliado por plataforma que permite o compartilhamento de dados, contexto e fluxos de trabalho



O IBM Qradar é uma solução de detecção e resposta a ameaças cibernéticas, projetada para unificar a experiência do analista de segurança da informação e acelerar sua velocidade durante todo o ciclo de vida de incidentes.

É uma solução SIEM que oferece uma ampla gama de funcionalidades para monitoramento de eventos e detecção de ameaças. Ele utiliza a análise comportamental para identificar padrões suspeitos e possui uma interface intuitiva que facilita a visualização e a análise dos dados de segurança.

Mais algumas Boas Práticas...

A seguir são apresentadas algumas práticas recomendadas para o monitoramento e a defesa de rede da sua empresa:

- Implemente uma arquitetura de segurança em camadas, com firewalls, IDS/IPS, antivírus e criptografia.
- Mantenha seus sistemas e aplicativos atualizados com as últimas correções de segurança.
- Monitore o tráfego de rede e registre os logs de eventos em tempo real para detectar atividades suspeitas.
- Utilize ferramentas de análise de segurança para identificar ameaças e anomalias.
- Estabeleça políticas claras de segurança e treine seus funcionários sobre boas práticas de segurança cibernética.
- Realize testes de penetração regulares para identificar vulnerabilidades na rede e aplique as correções.
- Tenha um plano de resposta a incidentes para agir rapidamente em caso de ataques ou violações de segurança.

Threat Intelligence
Contexto

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Agentes de Ameaças

Atualmente, existem muitos tipos de agentes de ameaças, todos com atributos, motivações, níveis de habilidade e táticas variados. Alguns dos tipos mais comuns de agentes de ameaças incluem **hacktivistas, agentes de estados-nação, cibercriminosos, caçadores de adrenalina, agentes de ameaças internas e ciberterroristas**.

Nações e governos podem financiar agentes de ameaças com o objetivo de roubar dados, coletar informações confidenciais ou prejudicar a infraestrutura crítica de outro governo. Essas atividades frequentemente abrangem **espionagem ou guerra cibernética** e tendem a ser altamente financiadas, tornando as ameaças complexas e difíceis de detectar.

Cibercriminosos (indivíduos ou grupos) **visam o ganho financeiro**. Entre os crimes mais comuns cometidos por cibercriminosos estão ataques de **ransomware, golpes de phishing e engenharia social** que induzem as pessoas a fazer transferências de dinheiro ou divulgar informações de cartão de crédito, credenciais de login, propriedade intelectual ou outras informações privadas ou sensíveis.

Hacktivistas usam técnicas para promover causas políticas ou sociais, como disseminar a liberdade de expressão ou revelar violações dos direitos humanos. Os hacktivistas visam enaltecer mudanças sociais positivas e assim direcionam suas ações à indivíduos, organizações ou agências governamentais para expor segredos ou outras informações confidenciais. Um exemplo bem conhecido de um **grupo hacktivista é o Anonymous, um grupo de hackers internacional que afirma defender a liberdade de expressão na internet.**

A **ameaça interna nem sempre têm intenções maliciosas, alguns casos ocorrem devido a erros humanos**, **como a instalação acidental de malware ou a perda de um dispositivo** que um cibercriminoso encontra e utiliza para acessar a rede. Mas existem agentes internos maliciosos. Por exemplo, um funcionário descontente que aproveita dos privilégios de acesso para roubar dados em busca de ganho monetário e/ou realiza a venda de credenciais de acessos para cibercriminosos.

Introdução

A **inteligência de ameaças** ou "***Threat Intelligence***" é processo de **coleta de informações detalhadas** sobre ameaças que visam prevenir e combater possíveis incidentes de segurança cibernética que entornam uma organização. A inteligência de ameaças auxilia organizações para obter informações relevantes em tomadas de decisões.

Boas práticas relacionadas à aplicação da inteligência de ameaças:

Inclusão da inteligência de ameaças cibernéticas aplicadas de forma integrada em análises.

Monitore constantemente as fontes de inteligência de ameaças em relação à crescentes vulnerabilidades e tecnologias emergentes.

Fazer uso da inteligência de ameaças para manter a conscientização dos tipos de atores mais prováveis de realizar ataques focados em sua organização e os TTPs que eles podem utilizar.

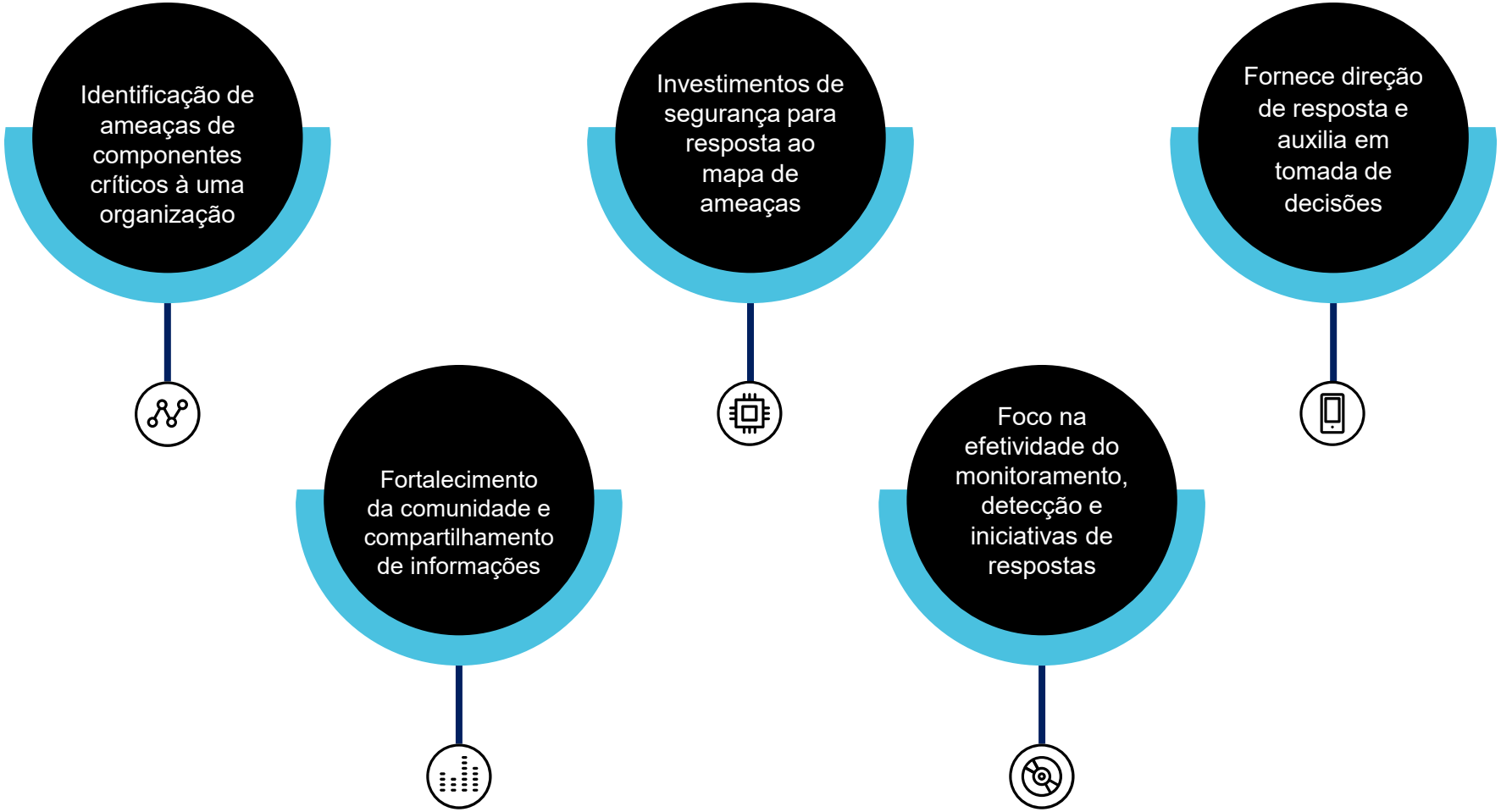
Utilizar a inteligência de ameaças para auxiliar na correlação de análise de logs.

Configure ferramentas de cibersegurança e tecnologias de detecção ou capacidades de resposta para ingerir informações de inteligência de ameaças.

Utilizar inteligência de ameaças em análises de log para aprimorar a precisão de detecção e características de atores, seus métodos e indicadores.

Quais os Benefícios da Inteligência de Ameaças?

Benefícios da aplicação de Inteligência de Ameaças



Threat Intelligence
Operação

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Principais Diretrizes

Inteligência de ameaças deve ser analisada e então utilizada:

- Para implementar processos e incluir informação coletada de fontes de inteligência de ameaças aos processos de gerenciamento de risco em Segurança da informação.
- Como input à prevenção técnica e controles de detecção como firewalls, detecção de intrusão em Sistema ou soluções anti-malware.
- Como input às técnicas de teste e processos de Segurança da informação

As atividades de inteligência de ameaças devem conter:

- Estabelecer objetivos para a produção de inteligência de ameaças;
- Identificar, vetorizar e selecionar fontes de informações internas e externas necessárias e apropriadas para providenciar os requisites para a produção de inteligência de ameaças;
- Coletar informação de fontes selecionadas;
- Processar informações coletadas para a realização de análise (tradução, formatação);
- Análise da informação para compreensão do impacto e relação com a organização.

- A organização deve compartilhar a inteligência de ameaças com outras organizações constantemente visando contribuir com a prevenção e conscientização geral
- Organizações podem usar a inteligência de ameaça para prevenção, detecção ou resposta à ameaças. As organizações podem produzir inteligência de ameaça, mas é comum receber e fazer uso de informações produzidas por outras fontes.
- A Inteligência de ameaças é produzida por fontes independentes, agências governamentais ou grupos/plataformas de inteligência de ameaças coletivas.

Métodos de Pesquisa

Monitoramento Deep e Dark Web

Um dos métodos de pesquisa para a análise de ameaças é o monitoramento na internet de redes abertas, *deep* e *dark* web em busca de atividades que possam trazer riscos cibernéticos para a organização.

Canais de monitoramento:

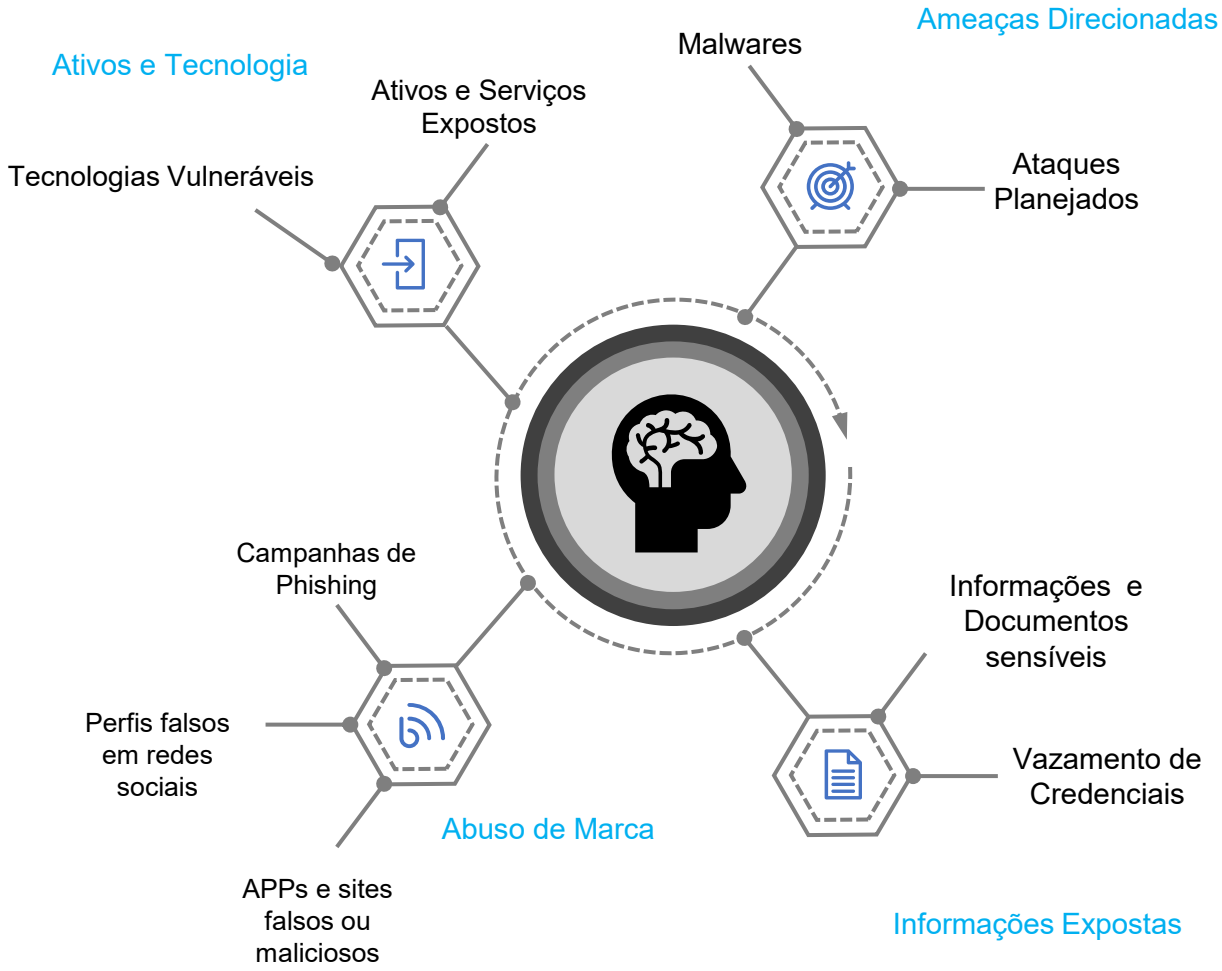
- Mídias sociais, tais como LinkedIn, Twitter, Facebook, Telegram e WhatsApp.
- Fóruns e sites da *surface*, *deep* e *dark web*.

Categorias de risco monitoradas:

- Informações Expostas
- Ativos e Tecnologias
- Abuso de Marca
- Ameaças Direcionadas

Resultados:

- Notificações imediatas.
- Relatório mensal com informações estruturadas de detecções, tipos de ameaças, volumetrias e criticidade dos eventos identificados.



Boas Práticas de Coleta e Conteúdo

FEBRABAN

Informações sobre ameaças existentes ou emergentes devem ser coletadas e analisadas para que:

- As devidas ações sejam informadas para prevenir ameaças de causarem danos à organização;
- Os impactos das ameaças seja reduzido.

Inteligência de ameaça pode ser dividida em três camadas que devem ser consideradas:

- Estratégia de inteligência de ameaça: troca de informações relevantes sobre possíveis atualizações do cenário da ameaça (ex: tipos de ataques ou atacantes).
- Táticas de inteligência de ameaças: Informações sobre metodologias do atacante, ferramentas e tecnologias envolvidas.
- Inteligência de ameaças operacional: detalhes sobre ataques específicos, incluindo indicadores técnicos.

Inteligência de ameaças deve conter:

- Relevância (relacionadas diretamente à proteção da organização)
- Insights (atribuir uma compreensão fiel e detalhada do cenário da ameaça à organização)
- Contexto, para conscientização (incluir contexto às informações baseando-se em tempo dos eventos, onde ocorreram, experiências anteriores e ocorrências em organizações similares)
- Ações (para que a organização possa atuar com as informações de forma rápida e efetiva)

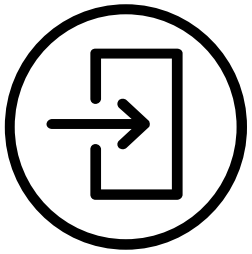
Proteção da Marca da Organização

FEBRABAN

- **Monitoramento na internet**, buscando por **informações** sensíveis ou confidenciais pertencentes à sua **organização**, **funcionários** ou **clientes**.

Exemplos de exposições comumente detectadas:

- Credenciais expostas em sites ou fóruns de mercados clandestinos
- Códigos de aplicativos expostos e documentos confidenciais em armazenados em repositórios.
- Informações confidenciais divulgadas por funcionários em fóruns.
- Exposição de informações sensíveis em sistemas de provedores de serviços terceirizados e mal protegidos.



- **Ativos de tecnologia expostos, mal protegidos e vulneráveis continuam sendo uma importante porta de entrada para ataques** nas organizações e muitas vezes, através de buscas específicas é possível detectá-los acessíveis ao público.

Exemplos de sistemas e serviços comumente detectados:

- Bancos de dados mal protegidos, especialmente com a proliferação de ambientes hospedados em nuvem.
- Armazenamento hospedado na nuvem.
- Serviços de gerenciamento remoto expostos.
- Dispositivos IoT e OT mal protegidos.

- Atacantes visam as organizações por motivos variados: oportunismo, financeiro, geopolítico, ideológico, etc.
- **O monitoramento detecta indicações de ameaças planejadas ou realizadas que visam especificamente sua organização.**

Exemplos de ameaças direcionadas comumente detectados:

- Planejamento de ataques.
- Indicações de comprometimento bem-sucedido.
- Infraestrutura configurada para ataques contra sua organização.
- E-mails de phishing destinados a seus funcionários ou clientes.
- Ferramentas de ataque e malware personalizados.

- A confiabilidade de sua marca está diretamente ligada a reputação construída.
- O **monitoramento** busca por **atividades** envolvendo o uso **indevido da marca** de sua organização e subsidiárias.

Exemplos de fraudes comumente detectados:

- Apps maliciosos.
- Perfis falsos em redes sociais.
- Campanhas de phishing.
- Malwares vinculados.
- Notícias falsas.

Proteção da Marca da Organização

Processo Inicial

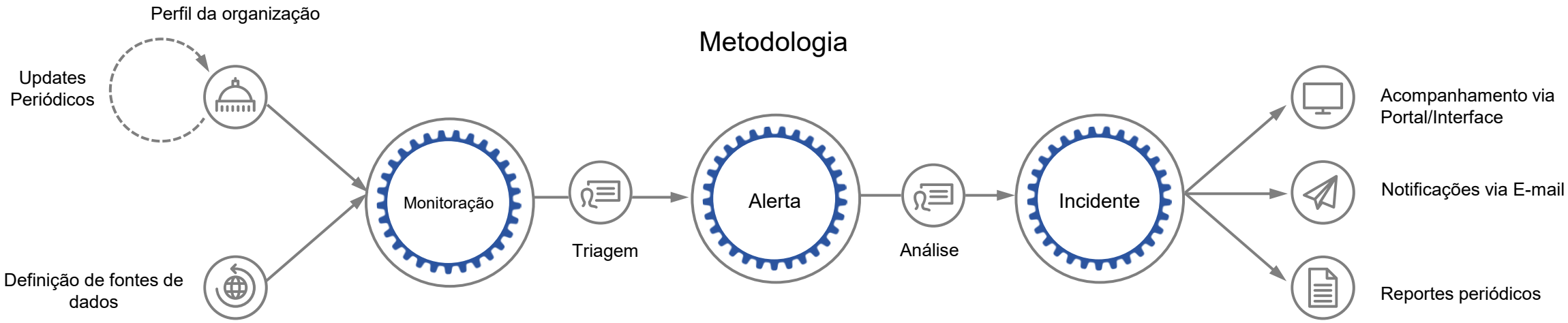
- A abordagem começa com a compreensão do seu negócio, bem como os riscos e ameaças inerentes.
- Isso envolve a coleta de informações sobre seus riscos de negócios, marcas e subsidiárias, perfil de ativos críticos, presença cibernética, incidentes passados e outros detalhes.

Monitoramento e Análises

- As descobertas devem ser validadas por analistas de inteligência, com objetivo de remover os falsos positivos e avaliar o risco que elas representam ao negócio da organização.

Notificações e Relatórios

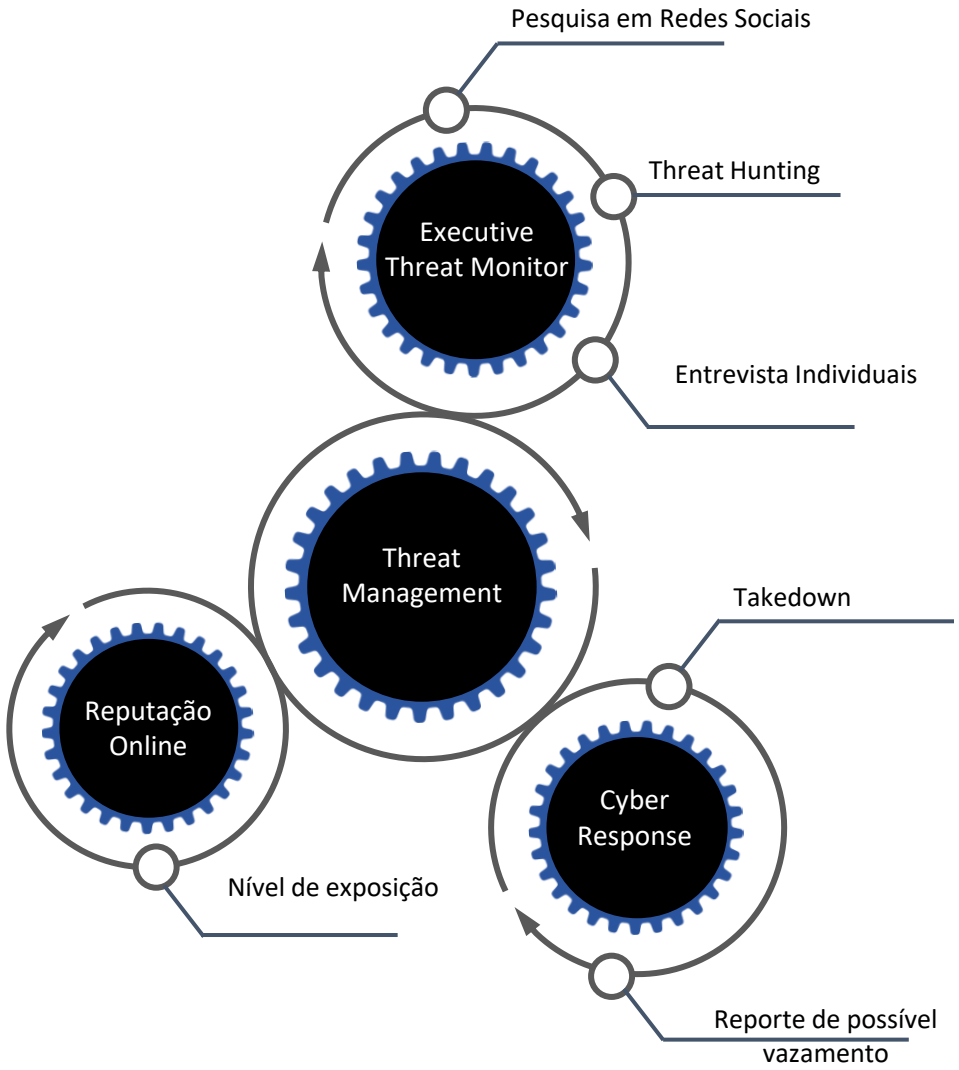
- Através de notificações imediatas a descoberta da ameaça, analistas orientam de forma prática sobre como responder aos incidentes identificados.
- As tendências em relação aos resultados observados são consolidadas em relatórios de serviço mensais.



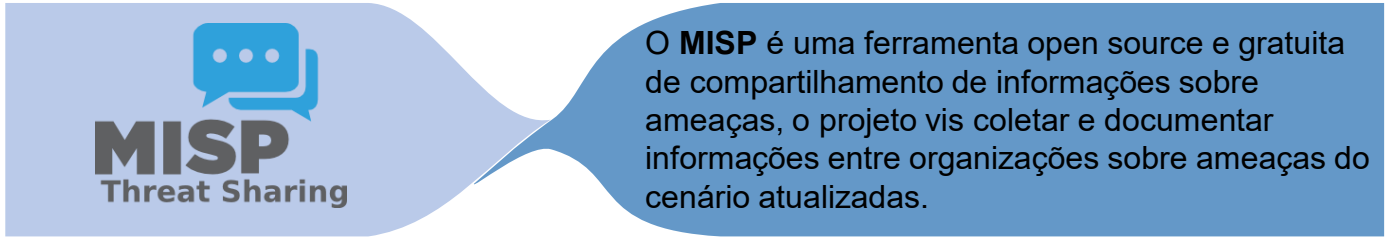
Proteção da Marca da Organização

Para as grandes organizações, com alta exposição de seus executivos, é recomendável o monitoramento de ameaças digitais focada nos principais executivos da Organização, incluindo por exemplo:

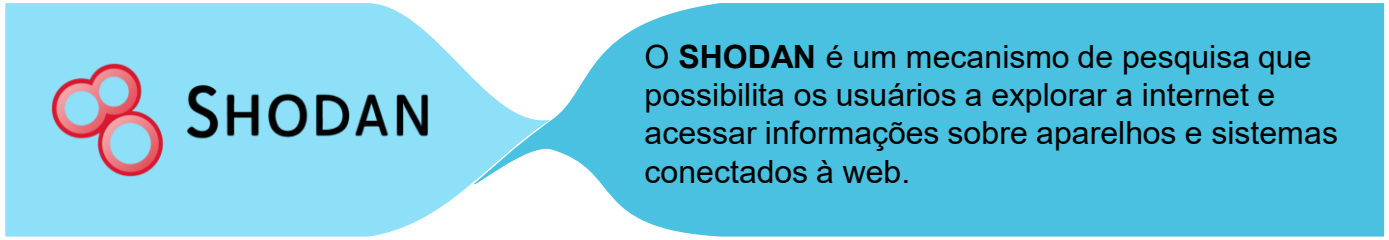
- Análise de sites, blogs, fóruns e redes sociais em busca de ameaças, sejam planejadas, iminentes ou em tempo real.
- Reputação *online* – pessoal e corporativo
- Superexposição de informações – pessoal e corporativo
- Uso indevido dos nomes dos executivos
- Roubo de identidade
- Perfis fraudulentos em redes sociais
- Ataques de phishing



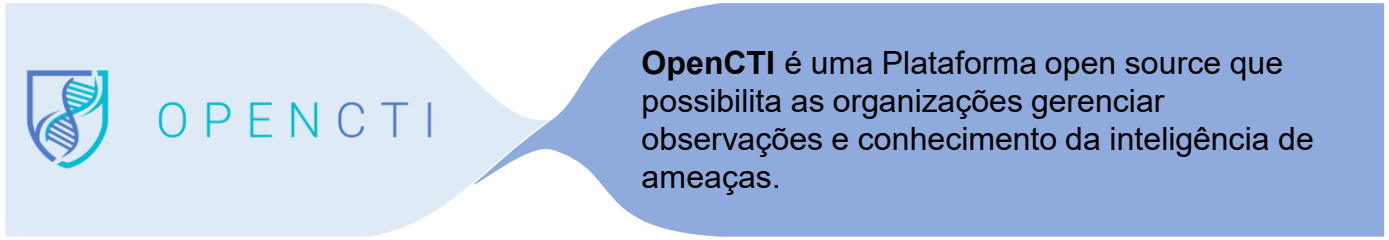
Ferramentas de Inteligência de Ameaças



O **MISP** é uma ferramenta open source e gratuita de compartilhamento de informações sobre ameaças, o projeto vis coletar e documentar informações entre organizações sobre ameaças do cenário atualizadas.



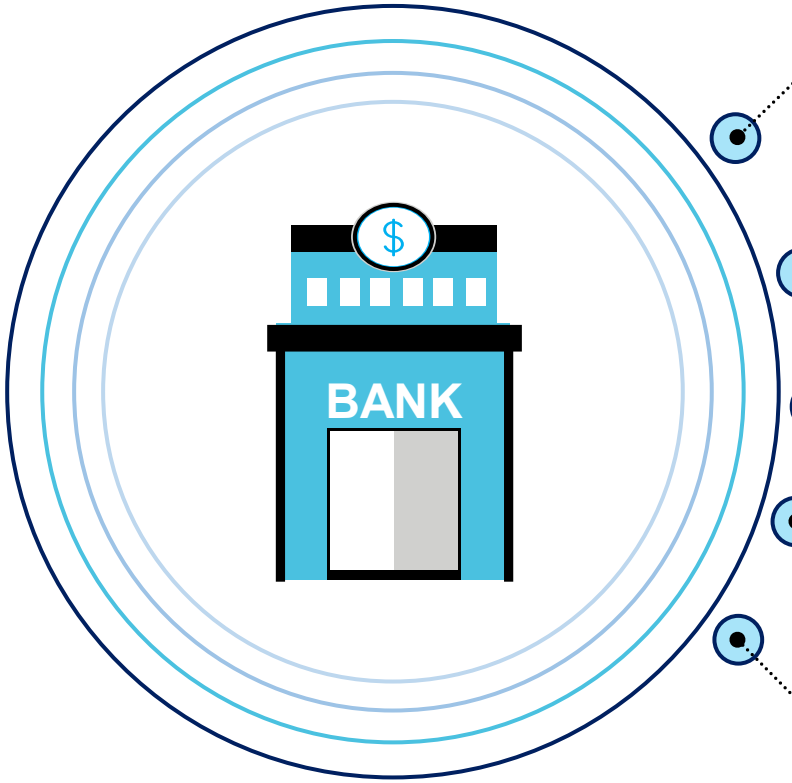
O **SHODAN** é um mecanismo de pesquisa que possibilita os usuários a explorar a internet e acessar informações sobre aparelhos e sistemas conectados à web.



OpenCTI é uma Plataforma open source que possibilita as organizações gerenciar observações e conhecimento da inteligência de ameaças.

Takedown

Takedown é uma solicitação de remoção rápida de conteúdo indevido ou fraudulento que pode impactar negativamente a imagem de uma Organização.



- Domínios ilegítimos, links e sites de *Phishing*
- Sistemas de terceiros expondo informações confidenciais da Organização
- Aplicativos e plataformas falsas ou maliciosos para dispositivos móveis
- Conteúdo fraudulento referenciando as marcas da Organização
- Aprimoramento dos Indicadores de Comprometimento – IOC (exemplos: IP maliciosos, assinaturas de malware e padrões de comportamento de ameaças)

Considerações Finais

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Frameworks e Normas de Referência

Para apoiar no entendimento e implementação de toda a metodologia apresentada neste material, a seguir são apresentados as normas e frameworks de referência no tema:

Frameworks Padrão Utilizados

PCI DSS COMPLIANT


NORMA BRASILEIRA

ABNT NBR ISO/IEC 27701

Primeira edição 25.11.2019

Versão corrigida 11.02.2020

Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes

Security techniques — Extension to ABNT NBR ISO/IEC 27001 and ABNT NBR ISO/IEC 27002 for privacy information management — Requirements and guidelines


INTERNATIONAL STANDARD

ISO/IEC 27002

Third edition 2022-02

Information security, cybersecurity and privacy protection — Information security controls

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

ISO IEC

Reference number ISO/IEC 27002:2022(E)

© ISO/IEC 2022

NIST National Institute of Standards and Technology

Conformidade: Requisitos de conformidade mais exigentes, permitindo estimar o nível de conformidade com ABNT NBR ISO, PCI-DSS, NIST, entre outros

Relembrando os principais conceitos

Agora que aprendemos sobre as atividades relacionadas a Monitoramento e Defesa da Rede, relembre os principais termos e conceitos apresentados neste material:

Segurança em Endpoint e redes terceiras: É o conjunto de práticas e tecnologias que protegem os dispositivos dos usuários finais, como desktops, celulares contra possíveis ameaças. As organizações devem proteger esses dispositivos para evitar o acesso não autorizado, uso por terceiros e a invasão na rede, aplicações e armazenamento de dados.

Alertas de eventos de segurança: O monitoramento e análise em tempo real de eventos de segurança e alertas é de grande importância no monitoramento de redes pois possibilita uma visão centralizada do mapa de ameaças, identifica e responde à ameaças em tempo real, realiza relatórios e auxilia na solução de problemas de segurança e vulnerabilidade.

Proteção de intrusão de rede: A prevenção de intrusão monitora o tráfego da rede em busca de possíveis ameaças e as bloqueia automaticamente, alertando a equipe de segurança, terminando conexões perigosas, removendo conteúdo malicioso ou acionando outros dispositivos de segurança.

Coleta de Logs: A coleta de Logs é um processo fundamental na proteção e monitoramento de redes pois estes registros possuem importantes informações de funcionamento de sistema, detecção, identificação de fatores e possíveis problemas ou ameaças, mapeando todas as atividades ou eventos ocorridos dentro de um sistema.

Módulo: Gestão de Provedor de Serviços

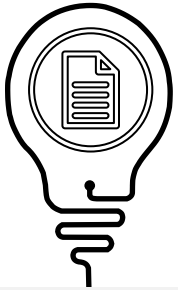
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Requisitos – Gestão de Provedor de Serviços

FEBRABAN

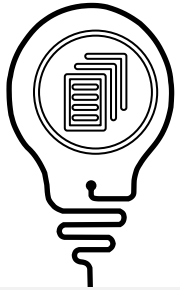
Este material foi elaborado de acordo com as diretrizes do CIS Controls, bem como foram considerados os requisitos de segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

CIS Controls



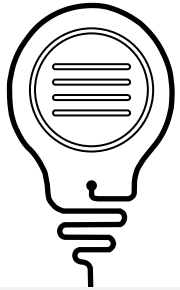
- 15.1 Estabelecer e manter um inventário de provedores de serviços
- 15.2 Estabelecer e manter uma política de gestão de provedores de serviços
- 15.3 Classificar provedores de serviços
- 15.4 Garantir que os contratos do provedor de serviços incluam requisitos de segurança
- 15.5 Avaliar provedores de serviços
- 15.6 Monitorar provedores de serviços
- 15.7 Descomissionar com segurança os provedores de serviços

ISO 27001



- 5.19 Segurança da informação em relacionamentos com fornecedores
- 5.20 Abordando a segurança da informação em acordos com fornecedores
- 5.21 Gerenciando a segurança da informação na cadeia de suprimentos de TIC
- 5.22 Monitoramento, revisão e gerenciamento de mudanças de serviços de fornecedores

NIST



- GV.SC-07: Os riscos de um fornecedor, seus produtos e serviços e outros terceiros são compreendidos, registrados, priorizados, avaliados, respondidos e monitorados ao longo do relacionamento
- ID.AM-04: Estoques de serviços prestados por fornecedores são mantidos
- CM-04: Atividades e serviços de prestadores de serviços externos são monitorados para encontrar eventos potencialmente adversos

ISO 27701

- 6.12.1 Segurança da informação na cadeia de suprimento
- 6.12.2 Gerenciamento da entrega do serviço do fornecedor

Sumário

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Sumário

Casos Reais e Principais Riscos

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Casos Reais de Incidentes

Ciberataque

Falha de fornecedor permitiu acesso a dados do KeyBank

Fonte: https://www.cisoadvisor.com.br/falha-de-fornecedor-permitiu-acesso-a-dados-do-keybank/

Ataque cibernético fechou todas as fábricas da Toyota no Japão por um dia

Atividade deve ser retomada nesta quarta (2); ciberataque atingiu fornecedor da gigante montadora e afetou a produção de 13 mil veículos

Satoshi Sugiyama, Maki Shiraki e Tim Kelly, da Reuters em Tóquio

01/03/2022 às 08:27 | Atualizado 13/12/2023 às 17:06

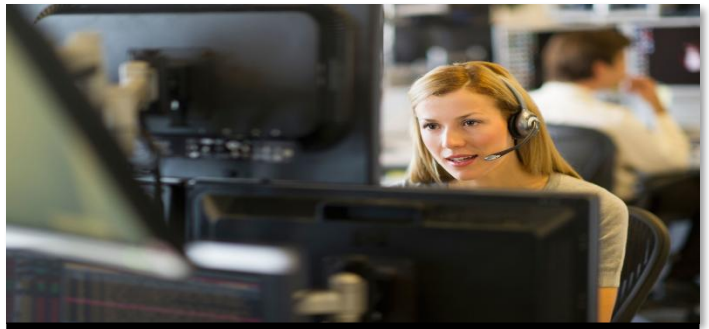
Fonte: https://www.cnnbrasil.com.br/auto/ataque-cibernetico-fechou-todas-as-fabricas-da-toyota-no-japao-por-um-dia/

Principais Riscos

FEBRABAN

Incidentes recentes destacam ainda mais os riscos significativos que estão ocultos no ecossistema

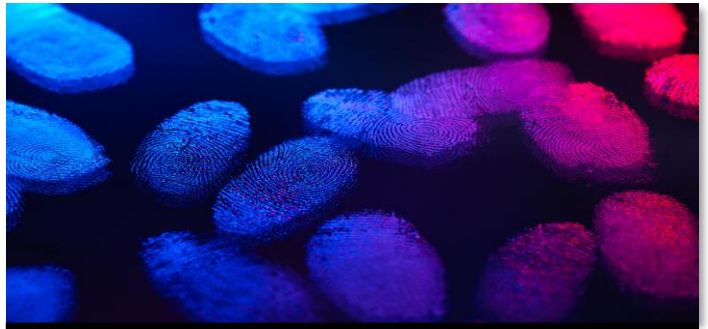
Roubo de dados mantidos ou gerenciados por terceiros



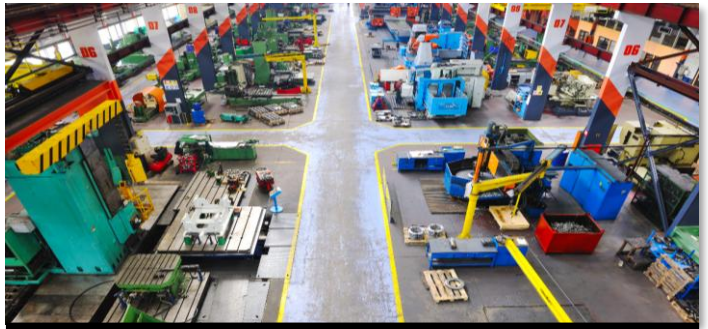
Crises de reputação que surgem de experiências negativas do cliente

Multas e litígios resultantes de ações movidas pelos terceiros

Restrições impostas por órgãos reguladores e alegações de corrupção



Indisponibilidade de sistemas e serviços críticos, levando a perdas materiais

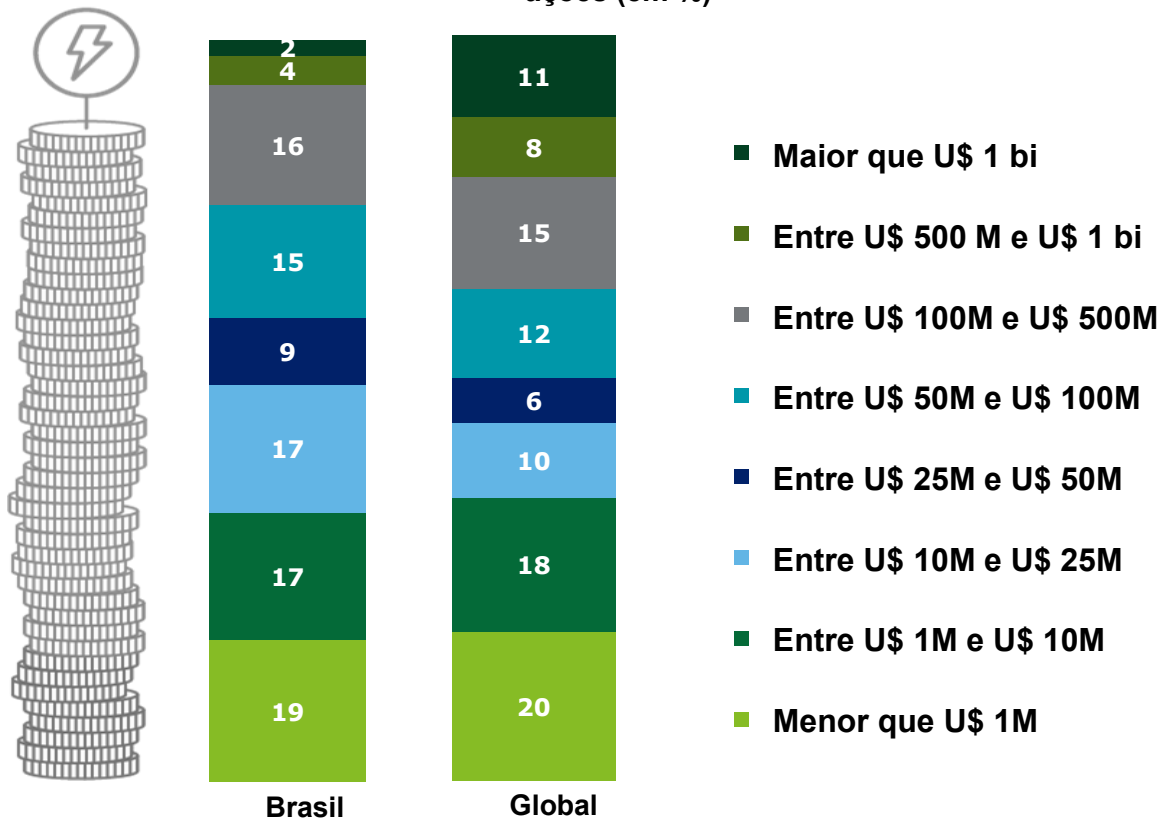


Perdas operacionais resultantes de problemas trabalhistas

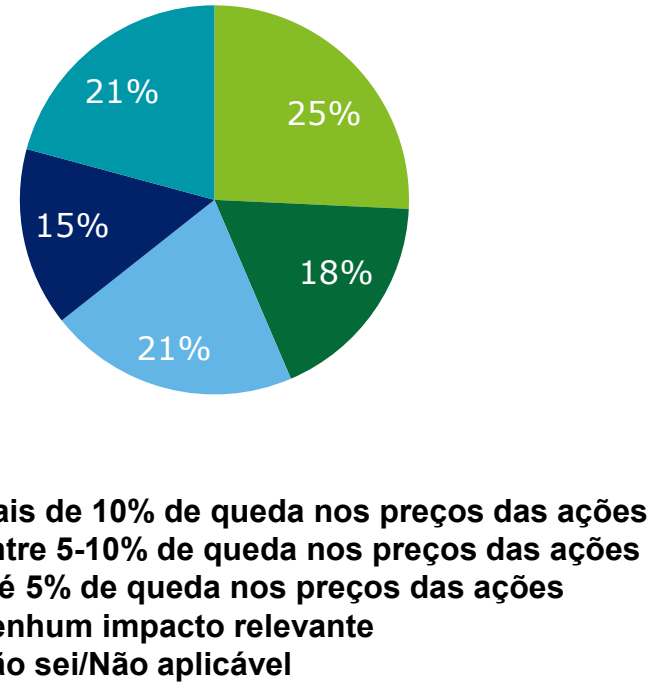
Custos relacionados a Incidentes

A exposição financeira devido à gestão inadequada de riscos relacionados a terceiros é estimada em valores elevados. 25% acreditam que o impacto potencial no preço das ações cairia em mais de 10%.*

Exposição financeira estimada pela não gestão adequada dos riscos relacionados a terceiros, após um incidente grave, considerando multas, custos de indenização direta e ações (em %)



Potencial impacto no preço das ações das empresas relacionado a incidentes graves em terceiros, segundo respostas de empresas de capital aberto no Brasil.



*Source: Research *Deloitte - Third Party Risk Management 2022*

Custos relacionados a Incidentes

FEBRABAN

Mais da metade (51%) das organizações enfrentaram um ou mais incidentes de risco de terceiros desde o início da pandemia de COVID-19*

RISCOS COM MAIOR IMPACTO

56%
Riscos de saúde e segurança

53%
Riscos Digitais

53%
Continuidade de negócios

OS RISCOS DIGITAIS SÃO A MAIOR PREOCUPAÇÃO

71%
dizem que o risco digital é uma área prioritária para o TPRM

Os riscos digitais surgem quando as organizações e suas cadeias de suprimentos adotam novas maneiras de automatizar o trabalho.

Os riscos digitais especificamente destacados incluem:

- Incapacidade de detectar oportunidades e ameaças de terceiros em tempo real (52%);
- Infraestrutura (47%);
- Cultura (44%) impedindo a implementação de iniciativas tecnológicas em terceiros.

OUTROS RISCOS EMERGENTES

41%
Resiliência financeira de terceiros em tempo real

40%
Diversidade e inclusão

38%
Saúde e segurança

*Source: Research *Deloitte - Third Party Risk Management 2020*

Contexto

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Governança de Terceiros

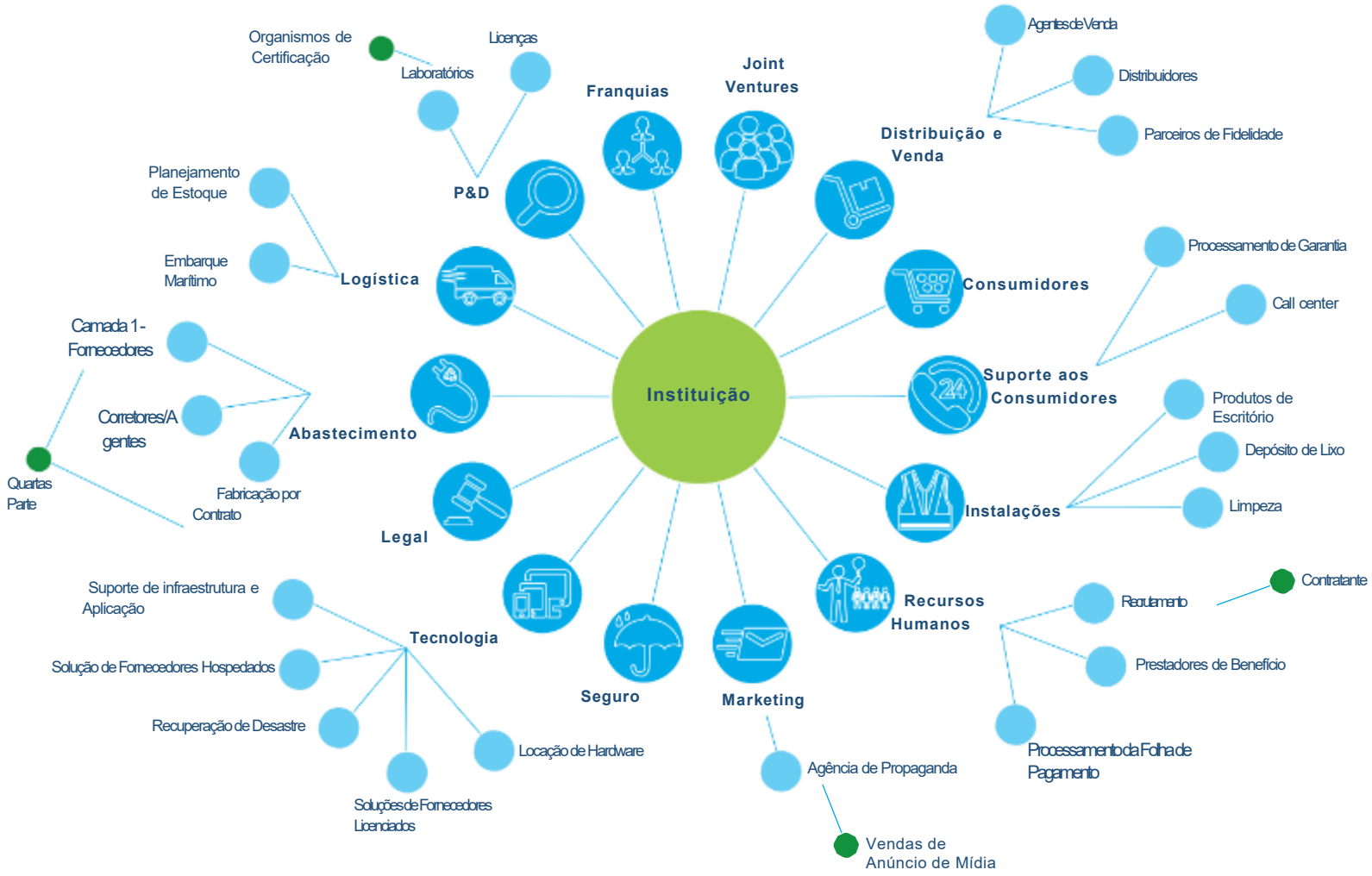
FEBRABAN

O ecossistema de Terceiros é complexo:

O conceito de empresa estendida é o de que uma Instituição não opera isoladamente. **Seu sucesso depende de uma rede complexa de relacionamentos entre terceiros.**

Fatores-chave

- Maior número de operações críticas e serviços de TI sendo terceirizados.
- Fornecedores que utilizam outros terceiros para execução das atividades podem novas camadas de risco.
- Dependências dispersas criam maior confiança e exposição ao risco de entidades fora do seu controle direto.
- Terceiros que não são fornecedores contínuos são raramente incorporados no Gerenciamento de Risco de Terceiros.

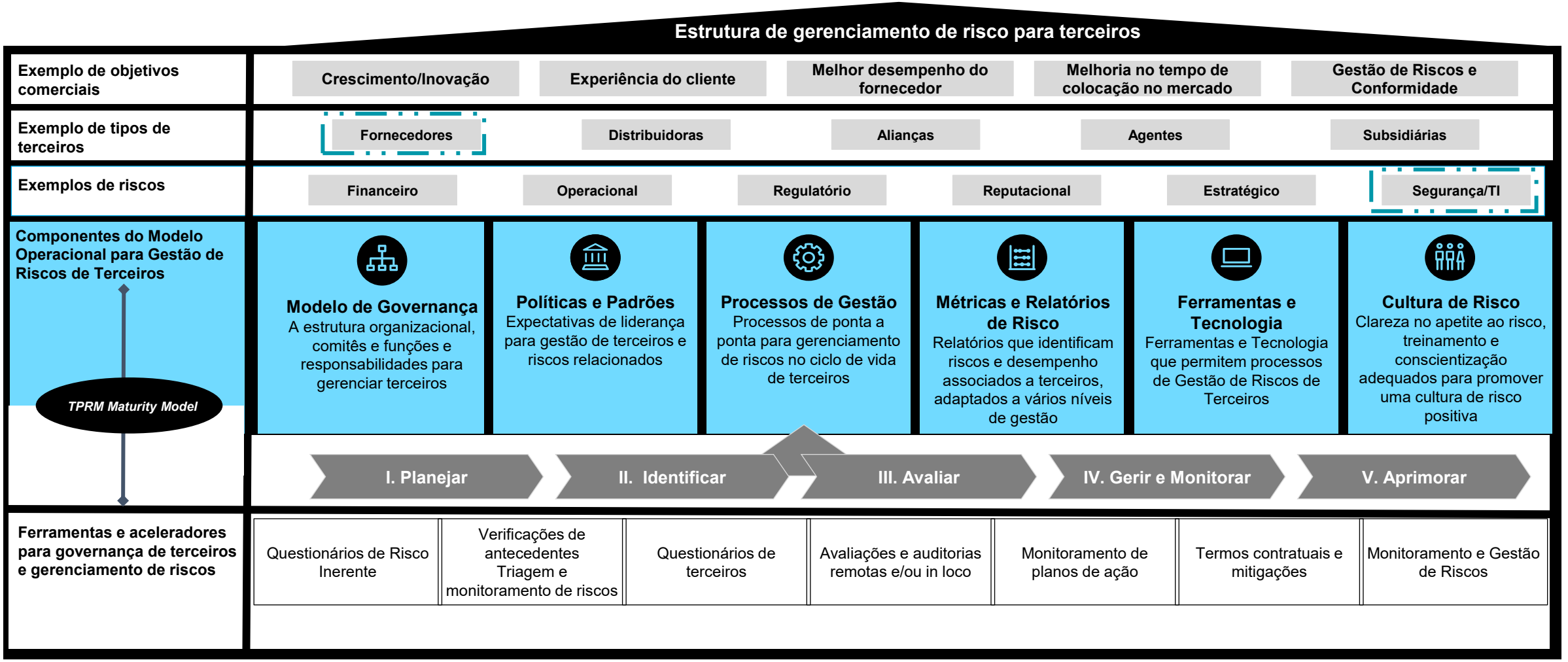


Gestão de Terceiros

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Gestão de Terceiros

A seguir apresentamos uma abordagem integrada para gerenciar relacionamentos com terceiros, considerando os objetivos de negócio das Instituição, bem como as categorias de relacionamento com terceiros e seus domínios de risco, utilizando tecnologias focadas em otimizar e impulsionar a gestão de riscos.



Avaliação de Segurança em Terceiros

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Avaliação de Segurança em Terceiros

FEBRABAN

De acordo com o CIS Controls, é necessário **desenvolver um processo para avaliar os provedores de serviços que mantêm dados sensíveis, ou são responsáveis por plataformas ou processos de TI críticos** de uma empresa, para garantir que esses provedores estejam protegendo essas plataformas e dados de forma adequada.

Principais controles:

Inventário de Fornecedores

Estabeleça e mantenha um inventário de provedores de serviço. O inventário deve listar todos os provedores de serviços conhecidos, incluir classificações e designar um contato corporativo para cada provedor de serviços.

Política de gestão de provedores de serviços

Estabeleça e mantenha uma política de gestão de provedores de serviços. Certifique-se de que a política trate da classificação, inventário, avaliação, monitoramento e descomissionamento de prestadores de serviços.

Classificar provedores de serviços

Certifique-se de que os contratos do provedor de serviços incluem requisitos de segurança, tais como: notificação e resposta de incidente ou de violação de dados, criptografia de dados e compromissos de descarte de dados.

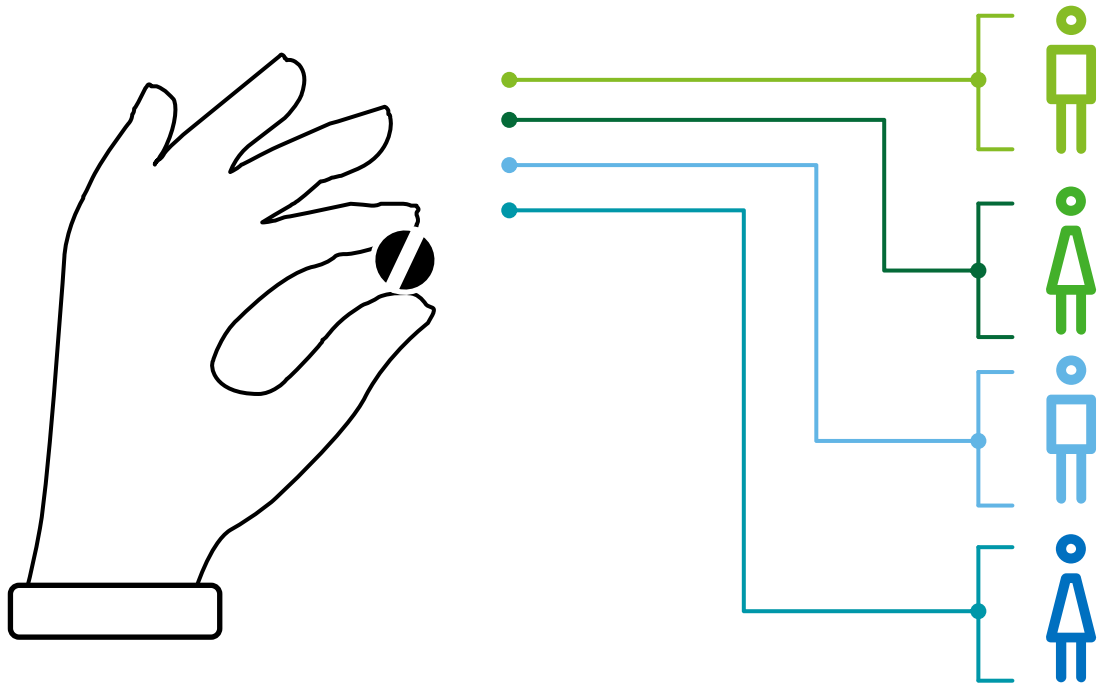
Monitorar provedores de serviços

Monitore os provedores de serviços de acordo com a política de gestão de provedores de serviços da empresa. O monitoramento pode incluir reavaliação periódica da conformidade do provedor de serviços.

Avaliação de Segurança em Terceiros

FEBRABAN

Objetivo: Fornecer informações sob a ótica de segurança da informação para a tomada de decisão na contratação ou continuação do serviço, bem como apoiar na metodologia de cálculo de risco e na definição de controles a serem aplicados durante esse processo.



Principais Pontos de Preocupação

Fornecedores realizam e suportam processos e atividades importantes às Instituições.

As Instituições possuem conexões diretas com diversos fornecedores que, nem sempre, possuem o mesmo nível de segurança interno.

Fornecedores são alvos de fraudadores para o roubo de informações e tentativas de intrusão.

Risco relacionado a quarteirização de serviços, avaliar possíveis vulnerabilidades no processo de contratação de uma empresa externa pela empresa que presta serviços terceirizados.

Quais os benefícios?

01 Visibilidade, mensuração e mitigação de riscos de segurança causados pelos fornecedores, evitando possíveis impactos à Instituição.

02 Conformidade com leis, regulamentos e padrões de segurança.

Quais as partes interessadas?

Gestores de Contrato

Times técnicos e/ou de projetos envolvidos

Riscos Corporativos, Compliance e Controles Internos

Avaliação de Segurança em Terceiros

FEBRABAN

Métodos e Técnicas: Avaliação de Segurança da Informação:

Avaliação dos principais controles de segurança da informação, baseados nos modelos de operação adotados pela Organização, por exemplo: Gestão e Governança de Riscos Cibernéticos; Normas e Políticas de Segurança; Controle de Acesso, entre outros. **Envio dos questionários e interação fornecedores**.

Questionários (self assessment)

Avaliação da postura de segurança de fornecedores, por meio de informações na internet, como por exemplo: Segurança de Aplicações Web (site não impõe encriptação HTTPS,; Segurança da Rede; Cadência dos patche; Segurança de Endpoint (browser ou sistema operacional desatualizado).

Ferramentas

Visita técnica ao fornecedor para validação dos controles, políticas e estrutura de segurança da informação.

Visitas Técnicas

Avaliação de Segurança em Terceiros

Métodos e Técnicas: Coleta de informações – Avaliação de Terceiros

Dados Públicos

- Coleta de informações em fontes públicas para identificação de possíveis riscos derivados do relacionamento com esse terceiro, bem como Sócios.
- Análise Jurídica, Financeira, Cadastral, Reputacional, Relacionamento com o poder público e outros quesitos selecionados pelo cliente.

Dados do Terceiro

- Coleta de informações disponibilizadas pelo terceiro à serem analisadas preliminarmente ao início do relacionamento.
- Envio de questionamentos sobre situações que possam agravar ou atenuar o risco do relacionamento.
- Obtenção de documentação suporte à tomada de decisão.

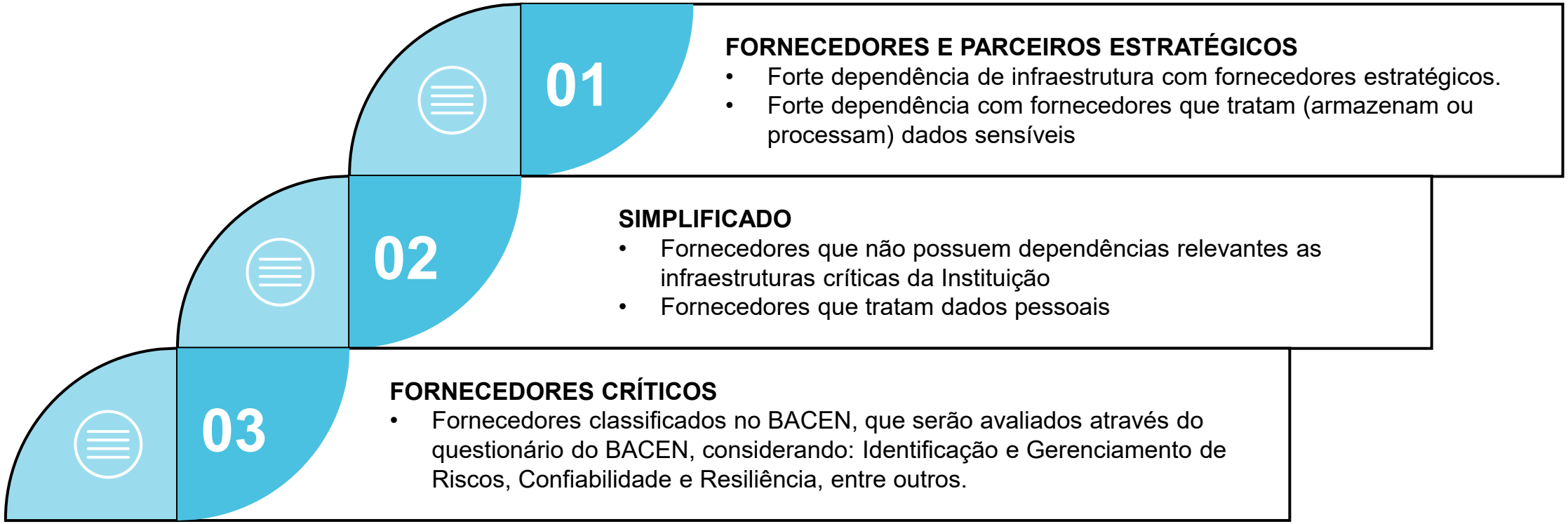
Dados do Relacionamento

- Coleta de informações sobre o tipo de relacionamento que esse terceiro terá com a Instituição.
- Análise de situações que possam agravar ou atenuar o risco do relacionamento, de acordo com as diretrizes de riscos da Instituição.

Avaliação de Segurança em Terceiros

FEBRABAN

Questionários: Abordagens utilizadas



Avaliação de Segurança em Terceiros

FEBRABAN

Clique no ícone ao lado para acessar um template de questionário.

Questionários: Exemplos de tópicos de avaliações de terceiros – segurança da informação

Temas		Abordagens
Política de Proteção de Dados	Política de Segurança de Rede	QUESTIONÁRIOS
Política de uso aceitável	Controle de acesso	
Revisão de Segurança Física	Proteção Contra Malware	DOCUMENTAÇÃO
Incidente de segurança	Política de Segurança de Software	
Política de criptografia	Política de Continuidade de Serviço	ENTREVISTAS
Vulnerabilidade	Política de Continuidade de Serviço	
SDLC	Treinamento	AUDITORIA INTERNA
Cloud Security	Classificação da Informação	

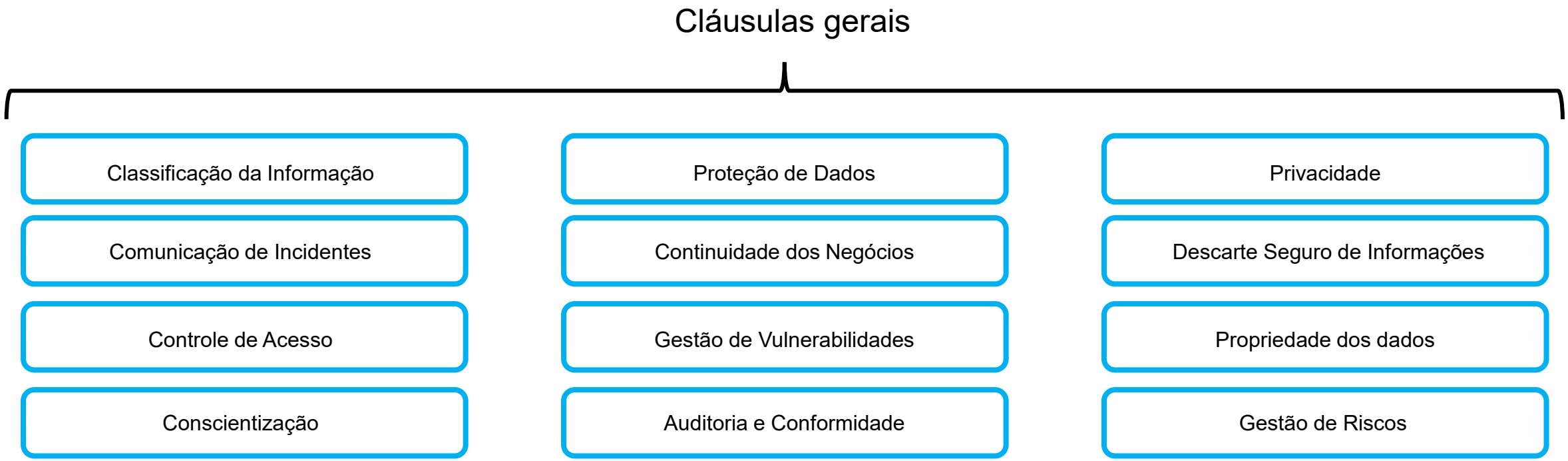
Exemplo ilustrativo

Controle/Requisito	Descrição	Recomendação
Controle de Acesso	A empresa possui uma política de Gestão de Acessos definida? Descreva como os acessos são concedidos, se existem aprovações, segregação de perfil de acordo com o cargo e função do colaborador. Comente também sobre a existência de um processo de revisão periódica de acessos e de revogação de privilégios de usuários por desligamento ou transferência.	Obrigatória
Controle de Acesso	A empresa possui controles de acesso à rede, aplicações de negócios e demais ativos de modo a restringir o acesso a pessoas autorizadas?	Obrigatória
Gestão de Vulnerabilidades	Possui uma Política de Gerenciamento de Vulnerabilidades e atualização de patches? Descreva o processo e comente sobre as técnicas e ferramentas que apoiam o processo.	Obrigatória
Gestão de Vulnerabilidades	A empresa realiza periodicamente: testes de verificação de vulnerabilidades nos seus ativos e testes de invasão (pentests) interno e externo? São elaborados relatórios gerenciais com indicadores para os planos de ação?	Obrigatória
Gestão de Incidentes	A empresa possui estrutura (processos, pessoas e tecnologias) para suportar o gerenciamento de incidentes de segurança? Descreva a estrutura e responsabilidades.	Obrigatória
Gestão de Incidentes	A empresa possui processo de aplicação de correções emergenciais? Descreva o processo, a existência do registro e aprovação dos owners.	Obrigatória
Proteção de Dados	A empresa possui medidas de prevenção, detecção e tratamento contra vazamento de informações? Descreva-as. Existe processo formal para comunicar a divulgação não autorizada a um grupo responsável por lidar com violações de confidencialidade?	Obrigatória
Proteção de Dados	A empresa utiliza soluções criptográficas? Se sim, quais? Foram estabelecidas diretrizes de uso destas tecnologias de criptografia? Descreva.	Obrigatória
Inteligência em Ameaças	Descreva quais as fontes externas confiáveis que proveem dados de ameaças.(agências do governo, informações públicas, consultores confiáveis e informações compartilhadas em fóruns)	Obrigatória
Gestão de ativos de software e hardware	A empresa possui medidas de segurança para o gerenciamento do ciclo de vida do hardware (avaliação, aquisição, manutenção e descarte)? Adicionalmente, comente a existência de processo de revisão, atualização do inventário dos ativos e hardening antes do uso.	Obrigatória
Gestão de ativos de software e hardware	A empresa possui medidas de segurança adotadas nos seus equipamentos de escritório (impressoras, fax, scanners e multifuncionais), para conter acessos indevidos, programas ou softwares desnecessários, além do descarte seguro? Descreva.	Obrigatória

Observação: De acordo com o Artigo 12º da resolução 4893: Na avaliação da relevância do serviço a ser contratado, mencionada no inciso I do caput, a instituição contratante deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado.

Avaliação de Segurança em Terceiros

Aplicando segurança da informação em contratos com provedores:



Observação: De acordo com o Artigo 48º da Lei Geral de Proteção de Dados (LGPD), no juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

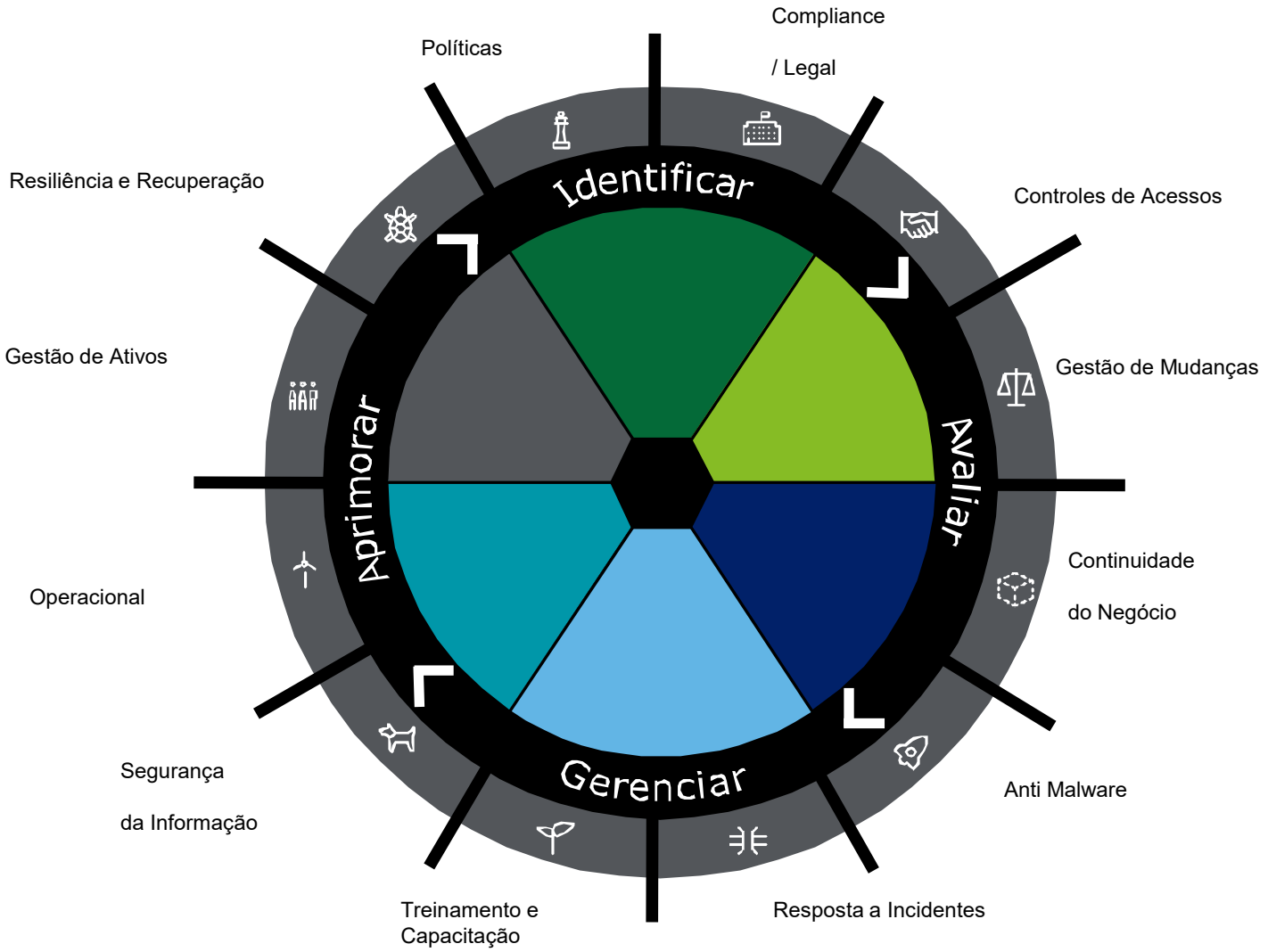
Gestão de Riscos de Terceiros

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Identificação dos Riscos

FEBRABAN

Quais são os riscos?



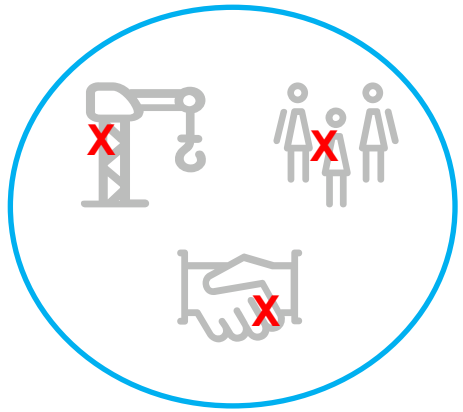
Gestão de Riscos de Terceiros

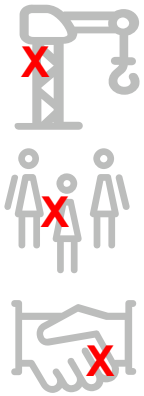
Questionário: Cada questão possui uma classificação de risco, baseada na metodologia de riscos corporativos (Vulnerabilidade X impacto).

Identificação dos riscos

Análise de Vulnerabilidade **e impacto de materialização de riscos**

Fornecedores





Vulnerabilidade	Impacto
Alto	Muito alto
Baixo	Médio
Baixo	Muito baixo

Risco que necessita tratamento

Gestão de Riscos de Terceiros

Termos e Definições:

- **Risco**
- Ameaça
- Probabilidade
- Impacto
- Severidade

O risco é o efeito da incerteza.

Exemplo:

Potencial exposição em caso de vazamento de dados devido à ausência de criptografia.

Gestão de Riscos de Terceiros

Termos e Definições:

- Risco
- **Ameaça**
- Probabilidade
- Impacto
- Severidade

Tentativa deliberada e não autorizada de acessar ou manipular informações, ou tornar um sistema inacessível, não íntegro, ou indisponível

Exemplo:

Ameaças Internas: prestadores de serviços e funcionários.
Ameaças Externas: malwares, engenharia social e hackers.

Gestão de Riscos de Terceiros

Termos e Definições:

- Risco
- Ameaça
- Probabilidade
- Impacto
- Severidade

Representa a possibilidade de que um determinado evento ocorra.

Exemplo:

Existe uma alta probabilidade de um hacker explorar vulnerabilidades conhecidas.

Gestão de Riscos de Terceiros

Termos e Definições:

- Risco
- Ameaça
- Probabilidade
- Impacto
- Severidade

Impacto é a consequência de um incidente que afeta os objetivos Estratégicos da Instituição

Exemplo:

Indisponibilidade e/ou comprometimento de aplicações e servidores.

Gestão de Riscos de Terceiros

Termos e Definições:

Risco

Ameaça

Probabilidade

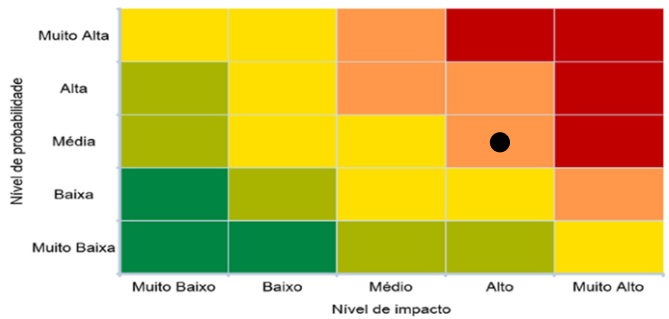
Impacto

Severidade

É o resultado da ponderação de um risco em relação ao seu impacto e probabilidade. É um sinalizador da importância e relevância do risco para a Instituição..

Exemplo:

Quando a probabilidade é média e o impacto é alto a severidade é alta.



Gestão de Riscos de Terceiros

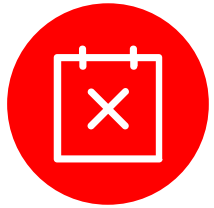
A partir da avaliação dos controles (de acordo com os questionários previamente elaborados), torna-se necessário **definir o nível de implementação de cada um dos controles**, conforme os níveis apresentados a seguir:

Implementado

O controle foi desenvolvido e implementado de acordo com os requisitos utilizados na avaliação.

Parcialmente implementado

O controle foi desenvolvido, mas não implementado de acordo com os requisitos utilizados na avaliação. Ele pode ser incompleto, mal implementado ou não funcionar conforme o esperado.



Não implementado

O controle não foi desenvolvido nem implementado.

Observação: O nível de implementação do controle pode ser utilizado para balizar a definição do nível de vulnerabilidade.

Gestão de Riscos de Terceiros

Todos os riscos identificados devem ser avaliados quanto a sua vulnerabilidade de ocorrência e potencial impacto. O resultado do cruzamento da vulnerabilidade e impacto nos fornece a severidade do risco, que sinaliza a sua prioridade. A seguir são apresentados alguns exemplos de como determinar o nível de severidade do risco:

Exemplo

R01 - Quando a vulnerabilidade é média e o impacto é alto

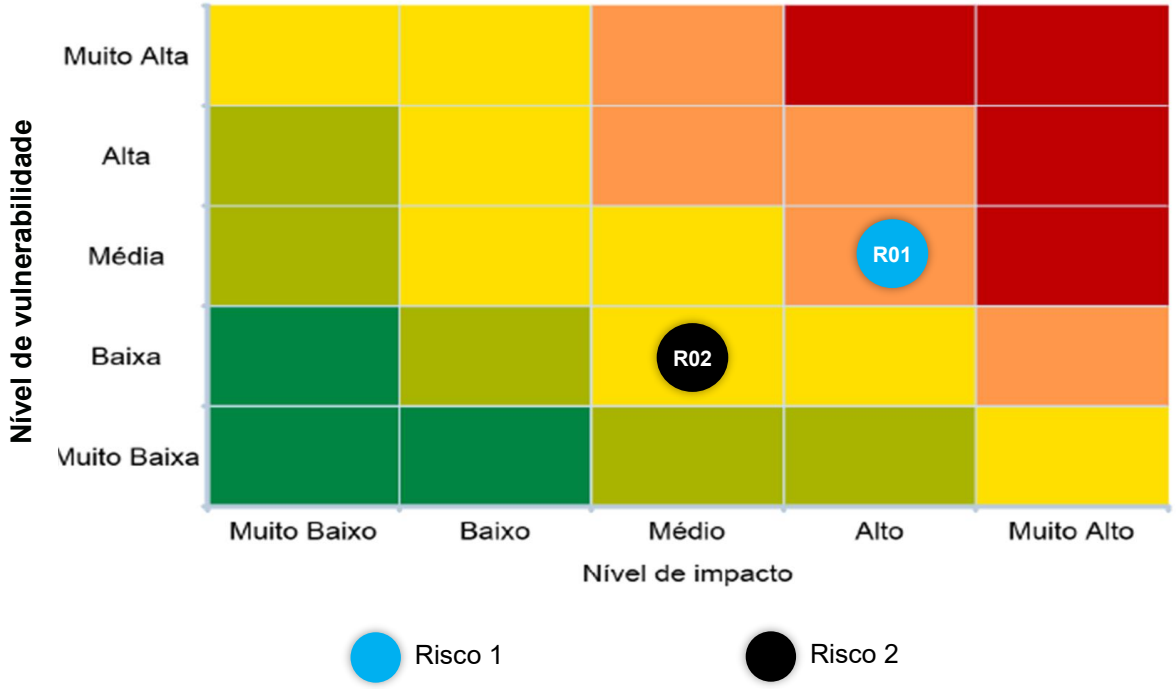
R01 Falha na entrega dos produtos e serviços em decorrência de erros em processamentos manuais.

Severidade: Alta

R01 - Quando a vulnerabilidade é baixa e o impacto é médio

R02 Falha na entrega dos produtos e serviços em decorrência de erros em processamentos manuais.

Severidade: Média



Gestão de Riscos de Terceiros

FEBRABAN

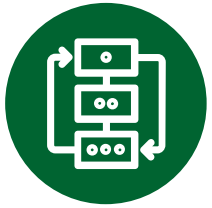
Todos os riscos relevantes identificados devem ter uma ou mais ações associadas, que em conjunto definem a resposta ao risco, exemplos:

Evitar

Não iniciar ou descontinuar uma atividade que dá origem ao risco

Reduzir

Desenvolver ações para reduzir a probabilidade e/ou o impacto dos riscos



Transferir

Compartilhamento do risco com outra(s) parte(s)

Aceitar

Retenção do risco por uma escolha consciente

Observar

Monitorar o risco para acompanhamento de sua evolução

Pesquisar

Reunir informações adicionais sobre o risco

Explorar

(apenas para oportunidades)

Assumir ou aumentar a exposição a um risco

Gestão de Riscos de Terceiros

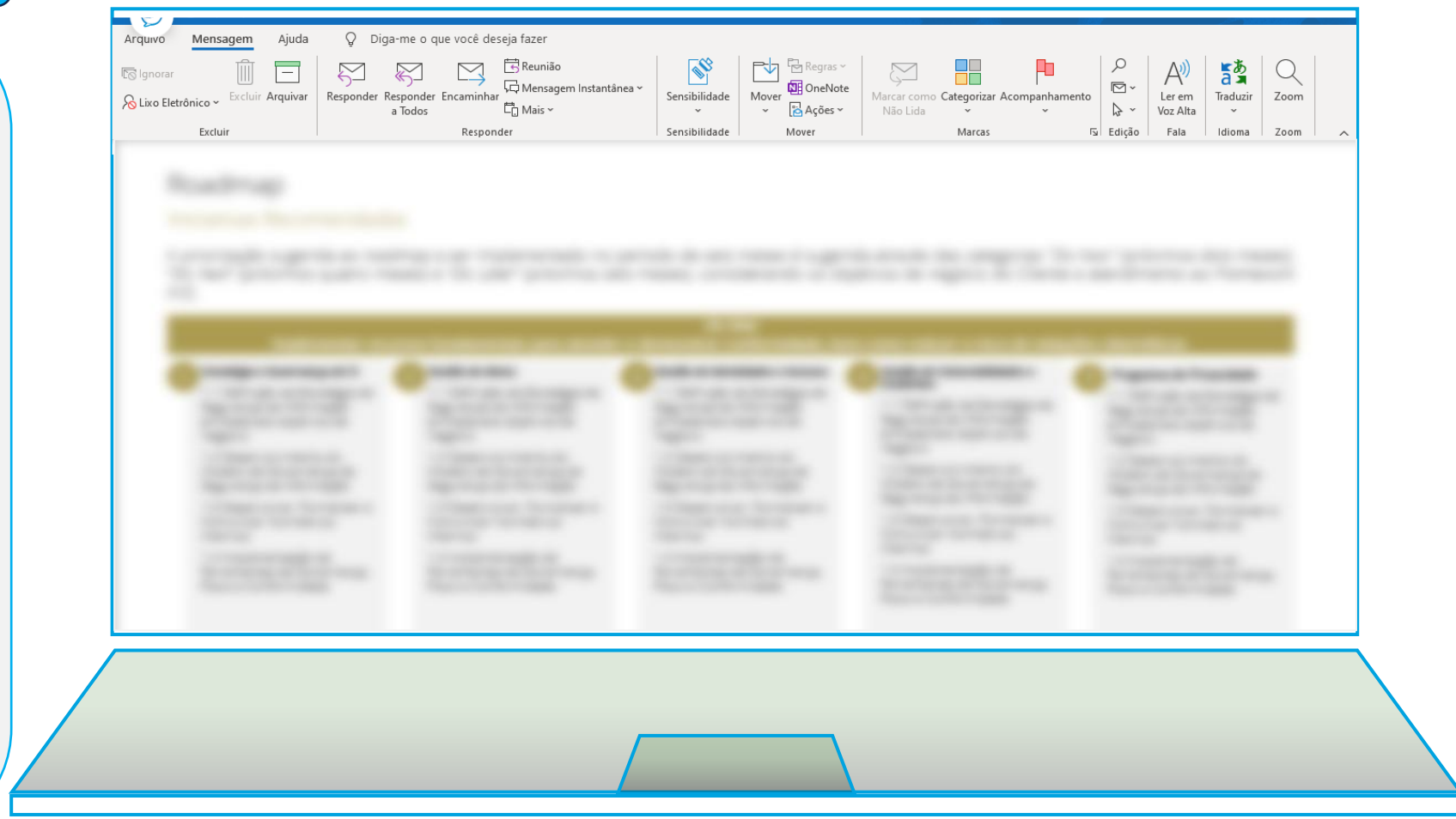
FEBRABAN

Reporte e acompanhamento dos Riscos:

REPORTE DOS RISCOS

FORNECEDORES

- Os riscos podem ser reportados aos gestor do contrato e ao fornecedor;
- **Fornecedores avaliados com risco “alto” ou “muito alto”, recebem recomendações referentes aos gaps identificados na avaliação. À partir dessas recomendações, são elaborados planos de ação**, que devem ser executados e reportados para que seja feita uma nova avaliação;
- Para os demais (classificados como risco “baixo” e “médio”), são enviados relatórios dos gaps, riscos, ameaças e recomendações.



Considerações Finais

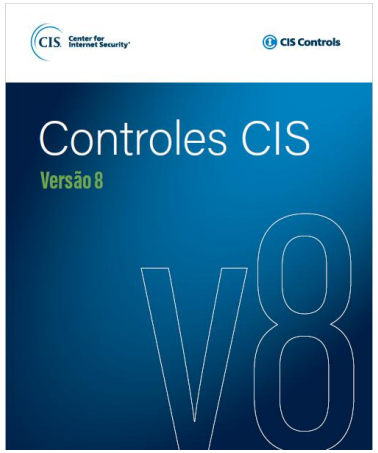
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Frameworks e Normas de Referência

FEBRABAN

Para apoiar no entendimento e implementação de toda a metodologia apresentada neste material, a seguir são apresentados as normas e frameworks de referência no tema:

Frameworks Padrão Utilizados



NIST
National Institute of Standards and Technology

Conformidade: Requisitos de conformidade mais exigentes, permitindo estimar o nível de conformidade com ABNT NBR ISO, PCI-DSS, NIST, entre outros

Relembrando os principais conceitos

Agora que aprendemos sobre as atividades relacionadas a Gestão de Provedor de Serviços, relembre os principais termos e conceitos apresentados neste material:

Inventário de Fornecedores: Estabeleça e mantenha um inventário de provedores de serviço. O inventário deve listar todos os provedores de serviços conhecidos, incluir classificações e designar um contato corporativo para cada provedor de serviços.

Política de gestão de provedores de serviços: Estabeleça e mantenha uma política de gestão de provedores de serviços. Certifique-se de que a política trate da classificação, inventário, avaliação, monitoramento e descomissionamento de prestadores de serviços.

Classificar provedores de serviços: Certifique-se de que os contratos do provedor de serviços incluem requisitos de segurança, tais como: notificação e resposta de incidente ou de violação de dados, criptografia de dados e compromissos de descarte de dados.

Monitorar provedores de serviços: Monitore os provedores de serviços de acordo com a política de gestão de provedores de serviços da empresa. O monitoramento pode incluir reavaliação periódica da conformidade do provedor de serviços.

Módulo: Gestão de Registros e Auditoria

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Requisitos – Gestão de Registros e Auditoria

FEBRABAN

Este material foi elaborado de acordo com as diretrizes do PCI DSS e CIS Controls, bem como foram considerados os requisitos de segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

CIS Controls

- 8.1 Estabelecer e manter um processo de gestão de log de auditoria
- 8.2 Coletar logs de auditoria
- 8.3 Garantir o armazenamento adequado do registro de auditoria
- 8.4 Padronizar a sincronização de tempo
- 8.5 Coletar logs de auditoria detalhados
- 8.6 Coletar logs de auditoria de consulta dns
- 8.7 Coletar logs de auditoria de requisição de url
- 8.8 Coletar logs de auditoria de linha de comando
- 8.9 Centralizar os logs de auditoria
- 8.10 Reter os logs de auditoria
- 8.11 Conduzir revisões de log de auditoria
- 8.12 Colete logs do provedor de serviços

PCI DSS

- 10.1 Processos e mecanismos para registrar e monitorar todos os acessos aos componentes de sistema e aos dados do titular do cartão são definidos e documentados.
- 10.2 Os registros de auditoria são implementados para apoiar a detecção de anomalias e atividades suspeitas, e a análise forense de eventos.
- 10.3 Os registros de auditoria são protegidos contra destruição e modificações não autorizadas.
- 10.4 Os registros de auditoria são revisados para identificar anomalias ou atividades suspeitas.
- 10.5 O histórico do registro de auditoria é mantido e disponível para análise.
- 10.6 Os mecanismos de sincronização de tempo suportam configurações de tempo consistentes em todos os sistemas.
- 10.7 Falhas de sistemas críticos de controle de segurança são detectadas, relatadas e respondidas prontamente."

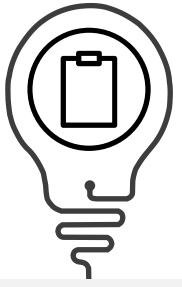
ISO 27002

- 5.33 Proteção de registros
- 5.35 Revisão independente da segurança da informação
- 5.36 Conformidade com políticas, regras e padrões para segurança da informação
- 8.15 Registro
- 8.16 Atividades de monitoramento
- 8.17 Sincronização de relógio
- 8.34 Proteção de sistemas de informação durante testes de auditoria

NIST CSF

- GV. OC-03: Os requisitos legais, regulamentares e contratuais relativos à segurança cibernética - incluindo obrigações de privacidade e liberdades civis - são compreendidos e gerenciados
- GV. OV-02: A estratégia de gerenciamento de riscos de segurança cibernética é revisada e ajustada para garantir a cobertura dos requisitos e riscos organizacionais
- D.IM-01: Melhorias são identificadas a partir de avaliações
- ID.IM-02: As melhorias são identificadas a partir de testes e exercícios de segurança, incluindo aqueles feitos em coordenação com fornecedores e terceiros relevantes
- PR.PS-04: Registros de log são gerados e disponibilizados para monitoramento contínuo

ISO27701



- 5.7.2 Auditoria interna
- 6. 9.4.1 Registros de eventos (logs)
- 6.9.7 Considerações quanto à auditoria de sistemas de informação
- 6.15.1 Compliance com requisitos legais e contratuais
- 6.15.2.1 Análise crítica independente da segurança da informação
- 7.2.8 Registros relativos ao tratamento de DP
- 7.5.3 Registros de transferência de DP

Sumário

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Sumário

Contexto

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Casos reais

Risco Iminente

Estee Lauder tem 440 milhões de registros de e-mail e logs expostos

https://www.cisoadvisor.com.br/estee-lauder-tem-440-milhoes-de-registros-de-e-mail-e-logs-expostos/

Um dos maiores vazamentos de dados da história envolve a empresa de crédito norte-americana Equifax. (Getty Images/Reprodução)

https://www.tecmundo.com.br/seguranca/282594-7-maiores-vazamentos-dados-historia.htm

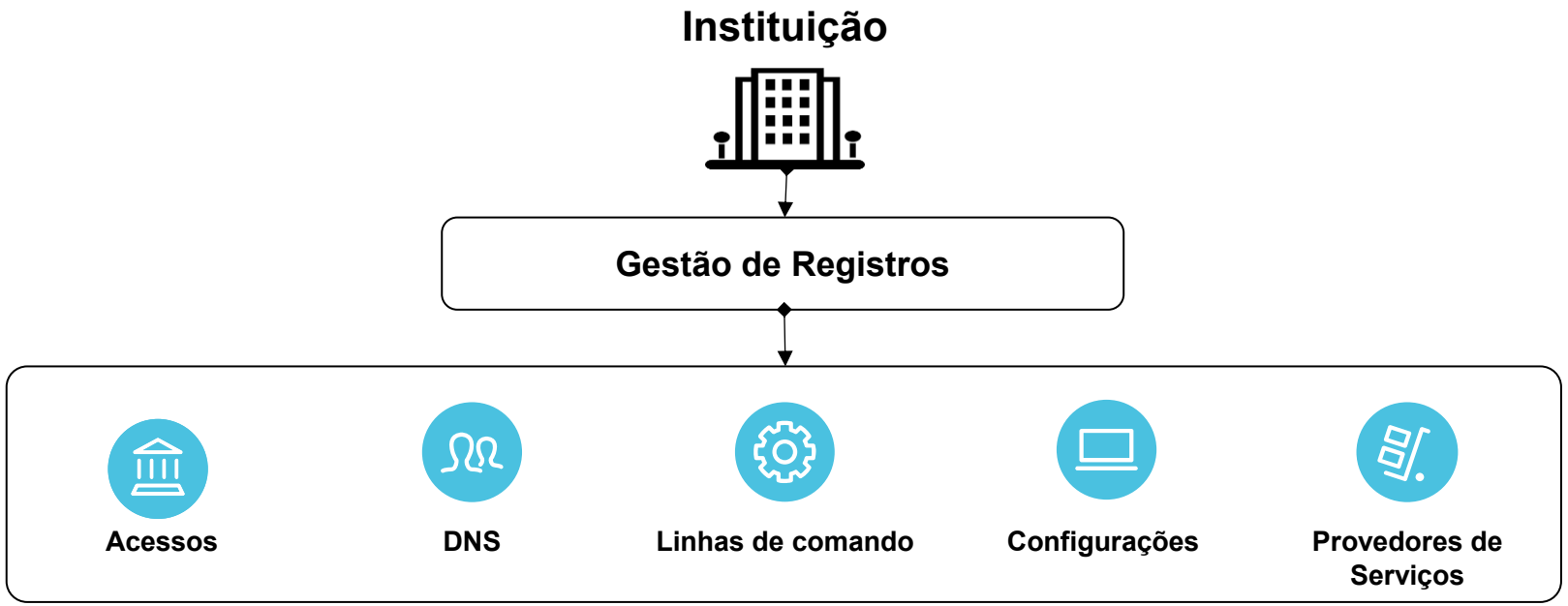
Cibercrime

2,7 bilhões de registros em vazamento na dark web

https://www.cisoadvisor.com.br/27-bilhoes-de-registros-em-vazamento-na-dark-web/

Introdução

Segundo a ISO27001, **os registros (log) de eventos das atividades do usuário** (exceções, falhas e eventos de segurança da informação) **devem produzidos, mantidos e analisados** criticamente, a intervalos regulares, tais como: identificação dos usuários (IDs), atividades do sistema, log-in e log-off, arquivos acessados ou alterados, endereços de rede e protocolos, entre outros.



Os registros de log também são essenciais para a resposta a incidentes. Após a detecção de um ataque, a análise de log pode ajudar as empresas a compreender a extensão de um ataque. Os registros de log completos podem mostrar, por exemplo, **quando e como o ataque ocorreu, quais informações foram acessadas e se os dados foram extraídos**. A retenção de logs também é crítica no caso de acompanhamento de uma investigação ser necessária ou se um ataque permanecer não detectado por um longo período de tempo.

Benefícios

- Contribui com a resposta a incidentes
- Preservar o valor da marca e a reputação
- Aprimorar a relação de confiança com clientes e parceiros
- Mitigar riscos financeiros, operacionais e legais

Boas Práticas
Gestão de Registros

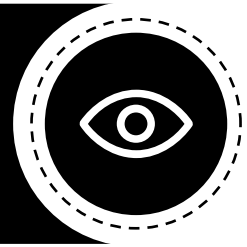
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Procedimentos e Ferramentas

A seguir é apresentado alguns procedimentos e ferramentas que devem ser considerados na Gestão dos Registros:

A maioria dos ativos e softwares corporativos oferecem recursos de log. **O log deve ser ativado, com os logs enviados para servidores de log centralizados**, tais como: Firewalls, proxy e sistemas de acesso remoto (VPN - Virtual Private Network; dial-up, entre outros) devem ser configurados e habilitados.

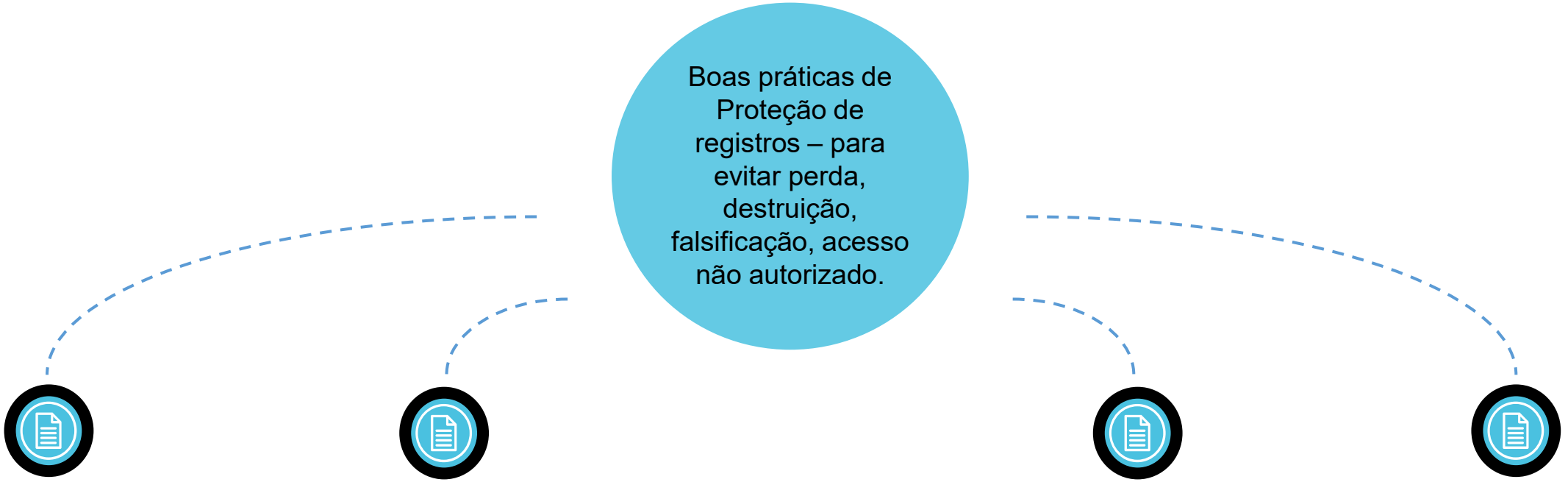
A retenção de dados de log também é importante no caso de uma investigação de incidente ser necessária. **É importante definir uma política de retenção e eliminação**, bem como **determinar por quanto tempo os registros/logs devem ser armazenados** (de acordo com os requisitos legais e regulamentares).



Além disso, todos os ativos corporativos devem ser configurados para criar logs de controle de acesso quando um usuário tenta acessar recursos sem os privilégios apropriados. Para avaliar se tal log está em vigor, **a empresa deve verificar periodicamente seus logs e compará-los com o inventário de ativos corporativos, a fim de garantir que cada ativo gerenciado ativamente conectado à rede está gerando logs periodicamente**.

Boas Práticas de Gestão de Registros

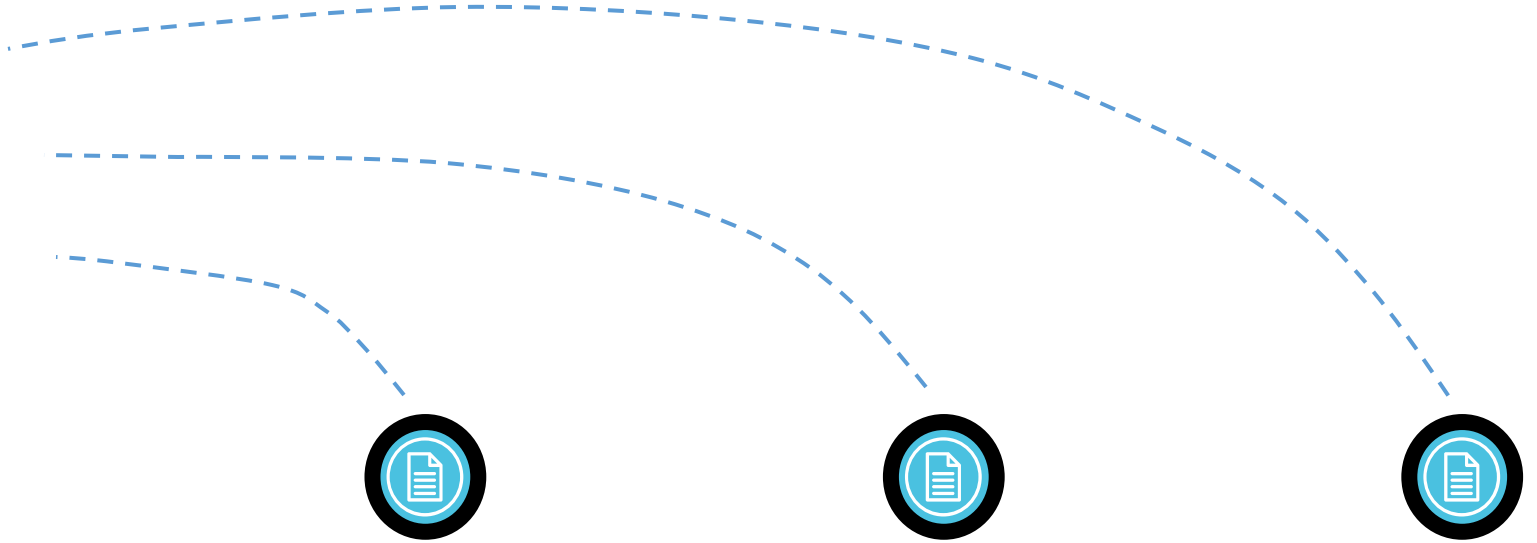
FEBRABAN



Boas Práticas de Gestão de Registros

FEBRABAN

Boas práticas de Proteção de registros – para evitar perda, destruição, falsificação, acesso não autorizado.



Categorizar os registros (sistêmicos, transação de negócios, registros pessoais, legais) e detalhar os tempos de retenção, formato de armazenamento (físico ou digital).

Sistemas de armazenamento de dados devem ser selecionados seguindo requisitos de registros com determinados frames e formatos.

Estabelecer controles de acesso aos registros no período de tempo definido, visando proteger de perdas devido a mudanças tecnológicas.

Boas Práticas de Gestão de Registros

Para gerar evidência, recordação de eventos, manter a integridade da informação de logs e prevenir acessos sem autorização é de **extrema importância que o registro dos logs seja protegido, armazenado e documentado e analisado.**

Detalhamento de Logs devem conter, se aplicável:

- IDs de usuários
- Origem/atividades de sistema
- Datas, horários e detalhes relevantes
- Identidade de aparelho e sistema e localização
- Endereços de rede e protocolos (DNS, roteamento, IPs)
- Documentos acessados e o tipo de acesso
- Tipo do evento
- Criação, modificação ou exclusão de documentos
- Transições executadas por usuários e aplicações

Medidas de Proteção de Logs

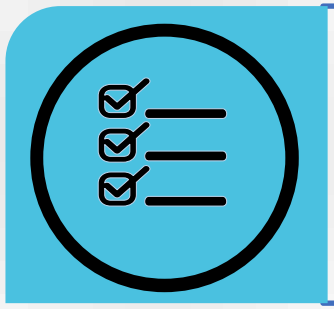
- Usuários não devem ter permissão para apagar ou desativar logs de suas próprias atividades.

- Alguns controles devem ser aplicados focando em alterações sem autorização e operacionais, como:
  - alteração das mensagens que forem registradas;
  - Realizar cópias de segurança (backups);
  - documentos de log serem deletados ou editados;
  - aplicação se necessário, de criptografia hashing, ou documentos de leitura apenas;
  - controle de acesso, entre outros.

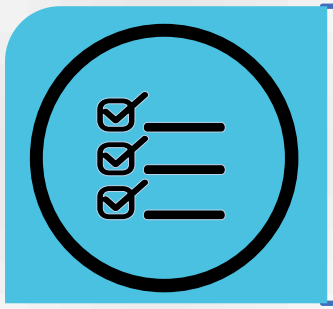
Monitoramento dos Registros de Atividades

As redes, sistemas e aplicações devem ser monitorados visando identificar comportamentos alterados e suas devidas ações consequentes.

Quais os registros relevantes a serem coletados para garantir um bom monitoramento de atividades e os cuidados com devidos registros?

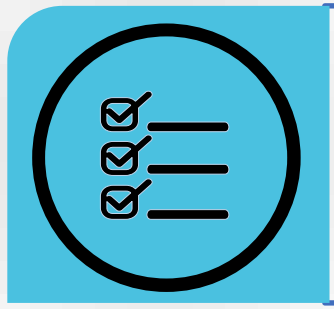


A organização deve **estabelecer um padrão de comportamento** e verificar por diferenças para **identificar anomalias**, ao estabelecer esse padrão, é importante revisar a utilização de sistemas em períodos normais e períodos de turbulência, e horários comuns de acesso, localização comum e frequência de acesso de determinados grupos.



Deve-se registrar:

- Tráfego de redes, sistemas e aplicações (e os acessos realizados à estes)
- Acesso à sistemas de nível administrativo ou crítico
- Os logs de ferramentas de segurança e de eventos (relacionados à sistemas e atividades da rede)
- O uso de recursos (CPU, memória, hard disks) e sua performance)



Através destes registros deve ser possível identificar:

- Atividades tipicamente associadas à malware ou tráfego de origem maliciosa
- Conhecer características comuns de ataques
- Comportamento incomum de sistema ou sobrecargas
- Acessos não autorizados à informações de sistema
- Tentativas bem sucedidas e mal sucedidas em acessos à recursos protegidos

Sincronização de Relógios

Os relógios dos sistemas de processamento de informação **devem estar todos sincronizados** para possibilitar **fontes confiáveis** e correspondência relacionada, permitindo investigações exatas em caso de incidente.

Requisitos para a sincronização e precisão devem ser aplicados e implementados.

Um horário padrão de referência deve ser utilizado na organização para todos os sistemas, incluindo gerenciamento de construção de sistemas, sistemas de entrada e saída e outros que podem ser utilizados para auxiliar em investigações.

Um relógio atômico nacional ou de sistema de posicionamento global deve ser utilizado como referência para os sistemas de Log.

Protocolo de horário de rede (NTP) ou protocolo de precisão de tempo (PTP) devem ser utilizados para manter os sistemas sincronizados.

A sincronização de horários pode ser dificultada em caso de uso de múltiplos serviços em nuvem ou ao utilizar serviços em nuvem e on-premise. Nestes casos o relógio de cada um dos serviços deve ser monitorado e a diferença deve ser registrada visando mitigar riscos devido à discrepância.

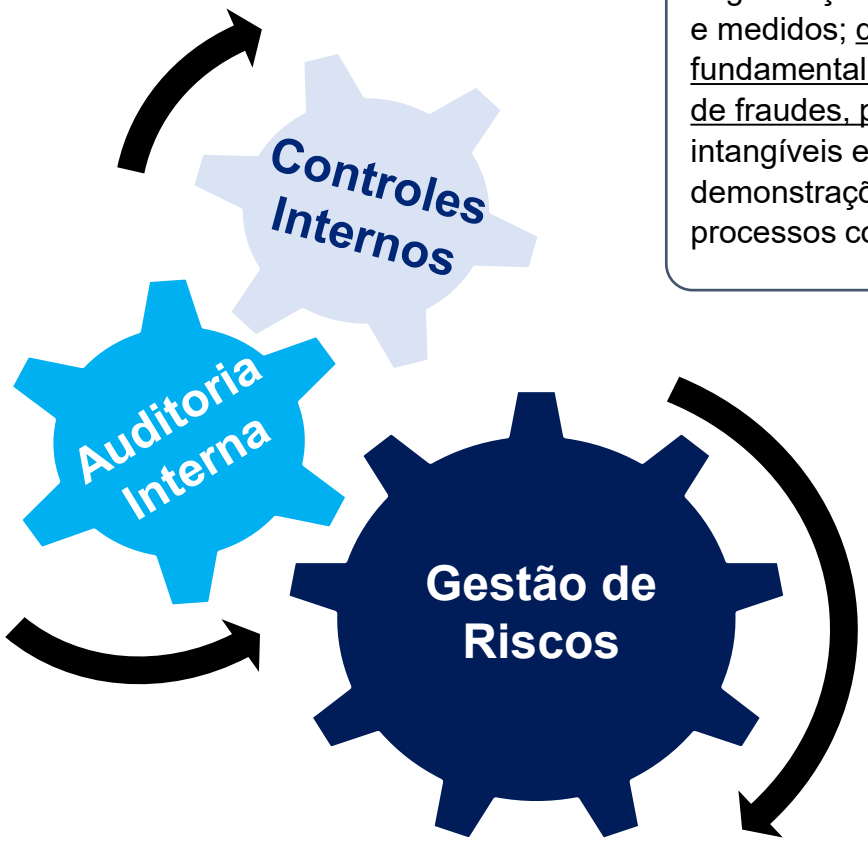
Introdução a Auditoria

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Introdução

Governança Corporativa é o conjunto de políticas, funções, responsabilidades e processos que orientam e controlam as ações adotadas pela Organização para atingir seus objetivos de negócio, resultando em sinergia e alinhamento:

Auditoria Interna é função independente e de aconselhamento à Alta Administração, destinada a agregar valor e melhorar as operações da Organização, por meio do aprimoramento dos instrumentos destinados à gestão de riscos, controles e processos de governança. Seu escopo de atuação é amplo, e contribui para a confiabilidade dos relatórios técnicos, financeiros, salvaguarda dos ativos e conformidade com leis e regulamentos internos ("*compliance*").



Controles Internos atua na gestão das práticas pelas quais os recursos da Organização são dirigidos, monitorados e medidos; desempenha papel fundamental na prevenção e detecção de fraudes, proteção dos ativos físicos e intangíveis e garantia na confiança das demonstrações financeiras e seus processos correlatos.

Gestão de Riscos tem como objetivo a identificação de eventos que poderiam comprometer as estratégias da Organização na consecução dos seus objetivos de negócio; atua no gerenciamento destes eventos, de modo a contribuir para o alinhamento às diretrizes de apetite ao risco.

Fatores de Risco

FEBRABAN

A auditoria de TI/SI está focada nos maiores riscos para a organização, nas áreas de risco mais impactantes à estratégia de negócios da Instituição.

DevSecOps confiança em riscos e controles

O desenvolvimento continuo (DevSecOps) exige uma nova **abordagem para mitigar os riscos** de TI e levará os auditores a repensar riscos e controles históricos para SOX e riscos operacionais em um mundo DevSecOps.

Privacidade de dados

Falhas ou violações na gestão de dados atraíram atenção significativa do regulador e de cliente, bem como resultaram em uma pressão maior para melhorar os procedimentos e políticas de governança de dados.

IT Transformation

Investir energia no estabelecimento de controles internos, ainda em fase de implementação ou transformação de sistema, pode economizar tempo e evitar a necessidade de remediação.

Riscos digitais e tecnologias cognitivas

A automação de tarefas rotineiras está ganhando força nos dias atuais, contudo muitas empresas não pensaram no **aumento dos riscos de segurança, privacidade, bem como no aumento da suscetibilidade de hackers cibernéticos**.

Assegurar

A auditoria fornece garantia baseada em riscos sobre controles internos da organização, incluindo a utilização de ferramentas e tecnologia para otimizações.

Comunicar

A Auditoria é proativa, transparente, relevante e valiosa para a organização, aconselhando sobre a capacidade de gerenciar efetivamente os riscos de forma ampla

Antecipar

A Auditoria antecipa e alinha esforços a riscos emergentes, estratégias e objetivos operacionais
da organização

Risco de dados, classificação & proteção

Muitas organizações lutam para implementar e impor com sucesso **estruturas de governança de dados**, pois dependem de novos modelos de infraestrutura, com dados e sistemas de armazenamento fragmentados.

Cyber identity & access management

Com a mudança para uma força de trabalho remota, muitos departamentos de TI são **incapazes de acompanhar a crescente necessidade de direitos de acesso.**

Cyber network & endpoint protection

O comprometimento de um único endpoint dentro de um ambiente considerando como **crítico pode comprometer a segurança de toda uma organização**.

Enterprise business & technology resiliency

A escala de **mudanças globais e organizacionais**, agravada pelas deficiências na gestão da continuidade de negócios, está **aumentando a exposição das organizações aos riscos de interrupção operacional**.

Auditoria em Segurança da Informação

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

27001: Sistema de Gestão de Segurança da Inf.

Sistema de Gestão de Segurança da Informação (SGSI):

Selecionando o escopo para Auditoria

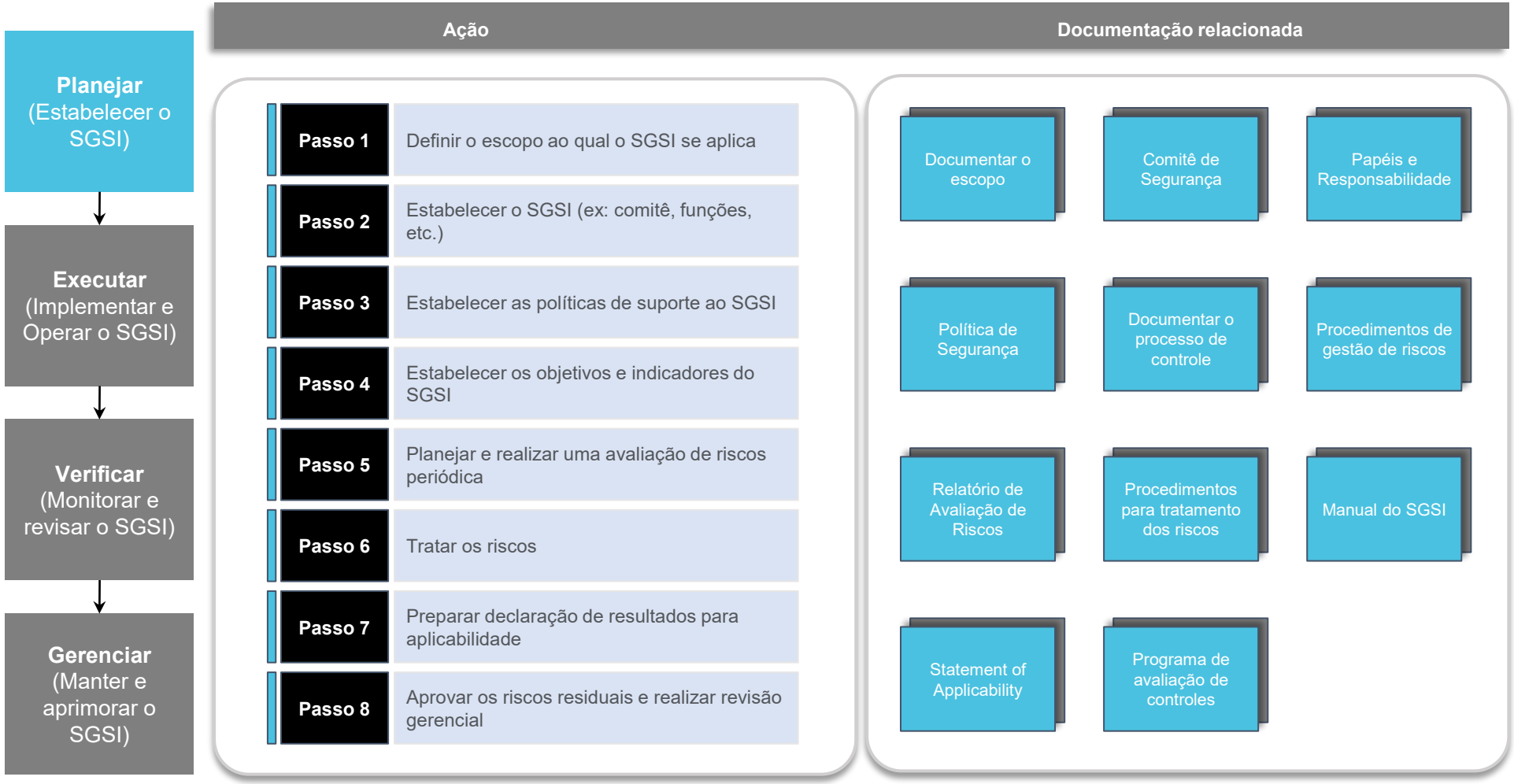
- ✓ Pessoas
- ✓ Ativos Físicos
- ✓ Ativos Intangíveis
- ✓ Hardware
- ✓ Software
- ✓ Ativos de Informação
- ✓ Serviços

- Um escopo explicitamente detalhado descreve o que será avaliado pela norma.
- A organização que está dentro do escopo deve apresentar uma separação física e/ou lógica de terceiros e de outras organizações dentro de um grupo maior.
- O escopo identificado para o SGSI precisa levar em conta as interfaces, pontos de contato e interdependências com as outras partes da organização.
- Alguns limites têm que ser identificados na organização:
  - ✓ Características do negócio;
  - ✓ Ativos (qualquer ativo de valor);
  - ✓ Redes e comunicação (mapas de redes);
  - ✓ Dados; e
  - ✓ Localizações geográficas.
- A norma exige explicitamente que seja identificado o que está fora do escopo do SGSI e justificativa da sua exclusão.

Planejar – Segurança da Informação

FEBRABAN

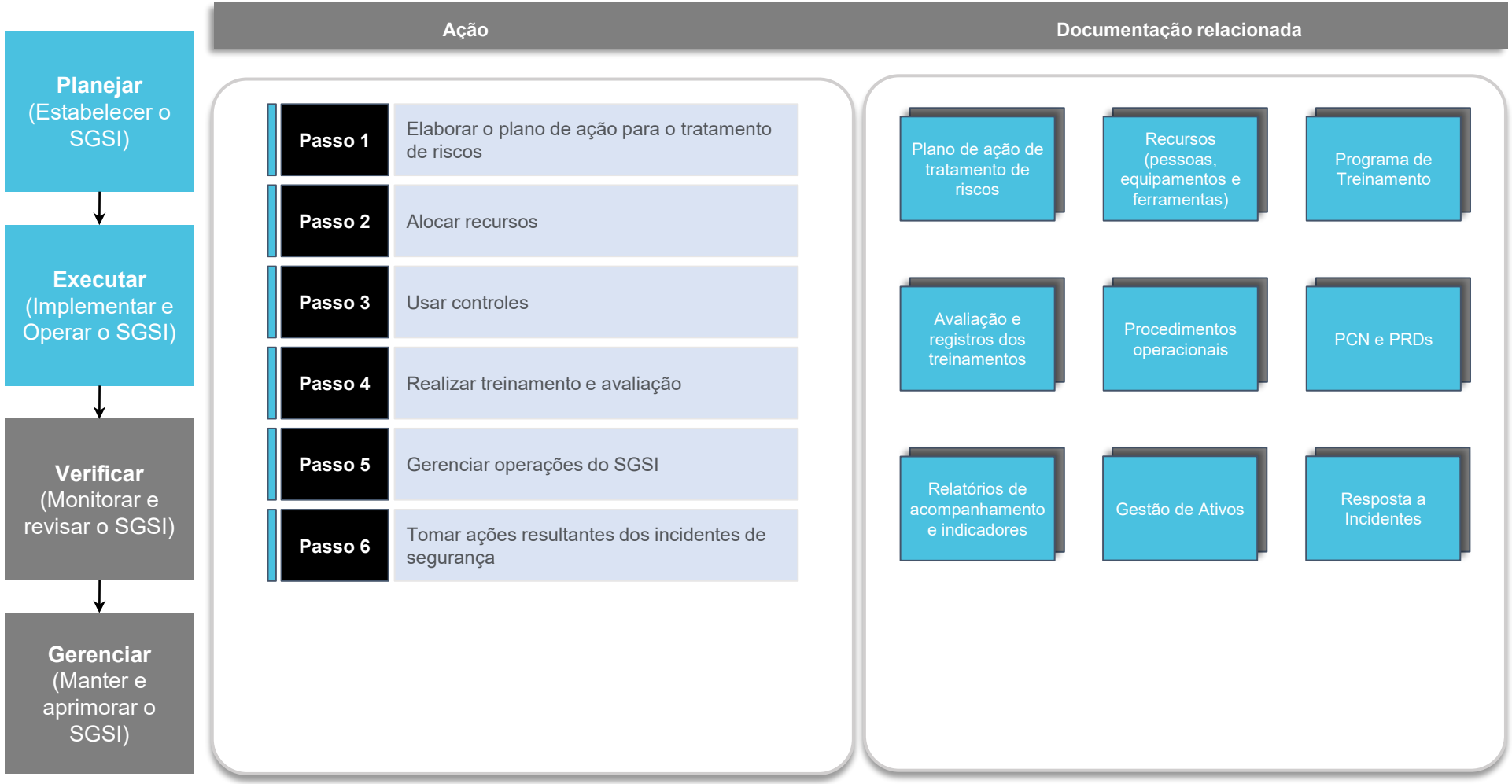
Estrutura para estabelecer um Sistema de Gestão de Segurança da Informação (SGSI):



Executar – Segurança da Informação

FEBRABAN

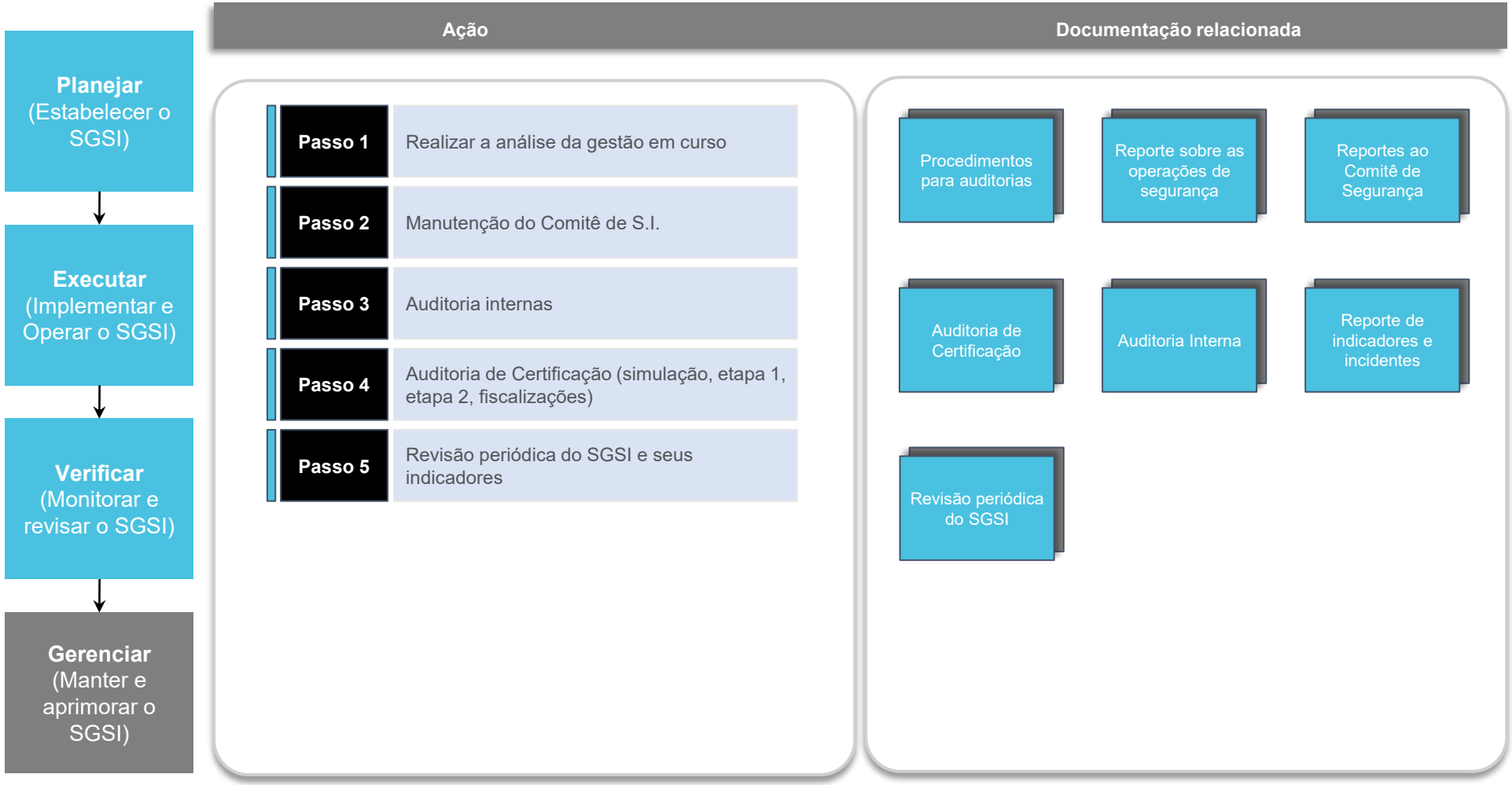
Estrutura para estabelecer um Sistema de Gestão de Segurança da Informação (SGSI):



Verificar – Segurança da Informação

FEBRABAN

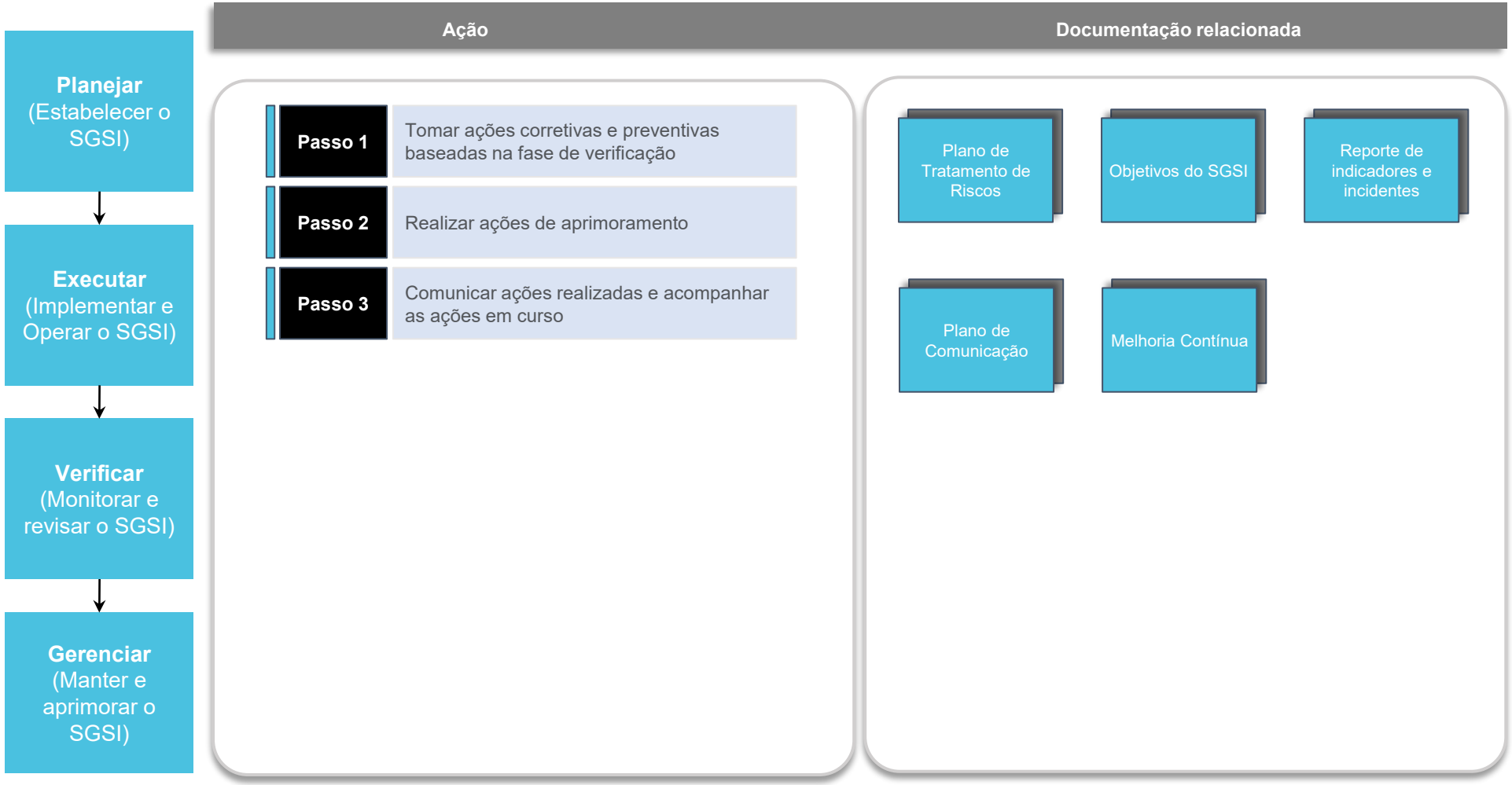
Estrutura para estabelecer um Sistema de Gestão de Segurança da Informação (SGSI):



Gerenciar – Segurança da Informação

FEBRABAN

Estrutura para estabelecer um Sistema de Gestão de Segurança da Informação (SGSI):



Abordagem Auditoria

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Abordagem - Auditoria

FEBRABAN

A seguir são apresentadas as fases e abordagem para orquestração da auditoria:

Planejar

- Alinhar expectativas da auditoria;
- Comunicar os objetivos da auditoria as partes envolvidos (*reunião de abertura*);
- Detalhar escopo a ser auditado;
- Solicitar documentação à área a ser auditada (ex. Evidência de implementação de técnicas de criptografia, Certificados digitais, etc);
- Programar reuniões de acompanhamento.

Executar

- Conduzir entrevistas com os responsáveis para entendimento do processo;
- Analisar as documentações internas do processo (políticas, procedimentos);
- Realizar teste de efetividade com o objetivo de validação dos controles ou identificação de eventuais deficiências.

Documentar

- Documentar o cenário atual e observações;
- Definição de conformidades e não conformidades;
- Preparar as recomendações e oportunidades de aprimoramento;
- Produção de atas.

Reportar

- Consolidar os resultados identificados;
- Preparar relatório de auditoria interna;
- Realizar reunião de apresentação do resultado da auditoria;
- Emitir o relatório detalhado, contendo o objetivo e escopo do trabalho, descrição dos pontos identificados, e recomendações;
- Apresentação dos resultados e encerramento.

Produtos

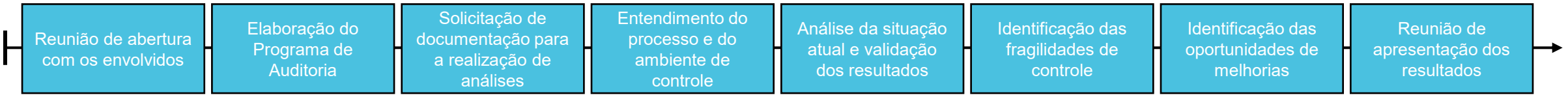
• Cronograma • Reunião de Abertura	• Matriz de controles • Matriz de riscos • Matriz de aplicabilidade	• Documentações • Atas	• Relatório

Considerações Gerais - Auditoria

FEBRABAN

Atributos da Área de Auditoria	Principais Atividades
• Possuir linha de reporte clara e **independente**, comunicando-se diretamente com o Comitê de Auditoria e Alta Administração. • Possuir **autonomia** para obtenção e análise de informações e execução dos trabalhos. • Estar **alinhada** às diretrizes estratégicas e ao modelo de Governança Corporativa. • Contribuir para aderência das atividades às expectativas dos gestores, padrões éticos, políticas internas e regulamentações (“***compliance***”). • Atuar de modo **complementar** às atividades de Gestão de Riscos e Controles Internos, buscando sinergias. • **Propor melhorias** nos processos, controles e aprimoramento dos instrumentos destinados à gestão de risco e Governança Corporativa.	• Elaborar plano de auditoria alinhado às **diretrizes estratégicas**, riscos e processos relevantes e **prioridades** dos gestores. • Auxiliar na **identificação e avaliação** dos principais riscos, suas origens e estratégias de mitigação. • Revisar os **controles** relacionados aos principais processos de negócio. • Executar **testes de auditoria**, avaliando aspectos de gestão, tecnologia, controles internos e “*compliance*”. • Validar os aspectos identificados com as áreas auditadas e **propor ações** para mitigação dos riscos. • Conduzir **“follow-up” dos planos de ação** e realizar trabalhos especiais. • **Priorizar o reporte** dos resultados às áreas auditadas e ao Comitê de Auditoria.

Fluxo de trabalho



Boas Práticas em Auditoria

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Boas Práticas - Auditoria

FEBRABAN

O programa de **segurança da informação** da organização e sua implementação, incluindo pessoas, processos e tecnologias **deve ser revisada de forma independente e com intervalos planejados** ou quando houver mudança significativa.

A organização deve possuir processos para **conduzir revisões independentes**. Planejar e contemplar avaliação para melhorias e necessidade de **mudanças pela segurança da informação,** incluindo suas políticas e controles

As **revisões devem ser feitas por pessoas fora da área com competência apropriada** e não podendo estar em linha de autoridade para **garantir a independência da avaliação**.

Os resultados das revisões independentes **devem ser reportadas** para o gerenciamento que iniciou as revisões e se apropriado, para maior gerenciamento.

Caso a revisão conclua que o gerenciamento e a implementação da **segurança da informação seja inadequada**, o gerenciamento deve **iniciar ações de correção**

Boas Práticas - Testes em Sistemas

Testes de auditoria em sistemas operacionais devem ser planejados e acordados, visando minimizar o impacto da auditoria e outras atividades em sistemas operacionais e processos de negócios.

Recomendações:

- O escopo dos testes técnicos da auditoria devem ser acordado e controlado.
- Os testes de auditoria devem ser limitados ao acesso somente para leitura de software e dado.
- Verificar os requisitos de segurança dos aparelhos utilizados para acesso ao sistema.
- Permitir acesso além de ‘apenas leitura” apenas para cópias isoladas de documentos do sistema, e deletá-los ao finalizar uso.
- Monitoramento e logging de todos os acessos para fins da auditoria e teste.
- Aplicar testes de auditora que podem afetar a disponibilidade de sistema fora do horário de trabalho.

Considerações Finais

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Frameworks e Normas de Referência

Para apoiar no entendimento e implementação de toda a metodologia apresentada neste material, a seguir são apresentados as normas e frameworks de referência no tema:

Frameworks Padrão Utilizados

ISO 27017 International Organization for Standardization

PCI DSS COMPLIANT

CIS Center for Internet Security®

NIST 800-53 Revision 5 Security Controls

Conformidade: Dado o uso extensivo de padrões amplamente aceitos pela indústria, a Gestão dos Registros e Práticas de Auditoria deve ser alinhada com alguns dos requisitos de conformidade mais exigentes, permitindo estimar o nível de conformidade com PCI-DSS, ISO, Bacen 4.893, NIST, entre outros.

Relembrando os principais conceitos

Agora que aprendemos sobre as atividades relacionadas a Gestão de Registros e Práticas de Auditoria, relembre os principais termos e conceitos apresentados neste material:

Proteção e boas práticas de registros: para evitar perda, destruição, falsificação, acesso não autorizado é de extrema importância a proteção e apropriada documentação de registros seguindo as políticas da empresa e seu armazenamento protegido e devidamente categorizado.

Boas práticas de registros em compliance: Aplicação devida de compliance seguindo normas, regras e boas práticas organizacionais devem ser revisados regularmente para garantir que a segurança da informação seja implementada e operada em concordância..
Gerentes, serviços, produtos ou outros detentores de informação devem identificar como revisar os requisitos de segurança da informação e outras regulamentações.

Proteção em processos de auditoria: Em processos de auditoria, como testes, avaliações, análises e outros procedimentos intra ao sistema é de extrema importância a proteção de dados e documentos que serão disponibilizados ao processo. Todos os acessos devem ser analisados e verificados, e de preferência os documentos devem ser mantidos como forma de “apenas leitura” para evitar vulnerabilidades.

Módulo: Boas Práticas de Segurança - Fábricas de Cartões

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

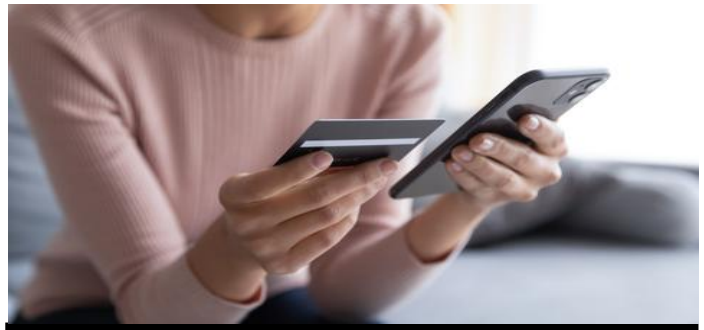
Sumário

Contexto

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Principais Riscos e Ameaças

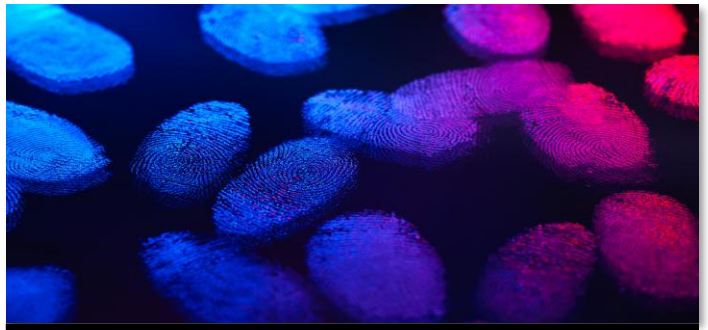
Roubo de dados e cartões mantidos ou gerenciados por terceiros



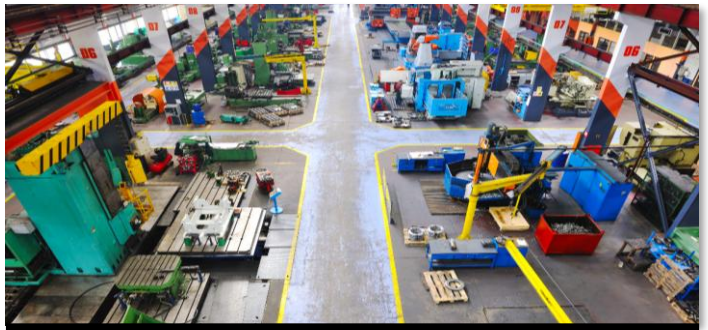
Ações relacionadas a fraudes e crimes cibernéticos

Vazamento e exposição de informações sensíveis (titulares de cartões)

Alta complexidade para implementação dos padrões de segurança



Regulamentações e fatores externos



Indisponibilidade de sistemas e serviços críticos, levando a perdas

Introdução

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

PCI - DSS

Payment Card Industry
Padrão de Segurança de Dados

O Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS) **foi desenvolvido para aprimorar a segurança dos dados de contas de cartões de pagamento** e facilitar a ampla adoção de medidas de segurança de dados consistentes no mundo todo. O PCI DSS **fornece os requisitos técnicos e operacionais projetados para proteger os dados**. Embora especificamente projetado para se concentrar em ambientes com dados de conta de cartão de pagamento, o PCI DSS **também pode ser usado para proteger contra ameaças e proteger outros elementos no ecossistema de pagamento**.

Requisitos de Segurança e Proteção dos Dados

- Segurança em redes
- Criptografia
- Proteção de sistemas
- **Segurança física**
- Configurações seguras
- Gestão de vulnerabilidades
- Desenvolvimento seguro
- Testes de segurança
- Proteção de dados
- Proteção de sistemas
- Controle de acesso
- Políticas e procedimentos

Processo de Certificação

Para obter a certificação é necessário atender os requisitos da PCI Compliance Assessment (Avaliação de Conformidade PCI) e **contratar uma empresa ou um responsável autorizado** (*Qualified Security Assessors*) **para emissão de conformidade dos controles**. A certificação PCI DSS é um padrão de mercado que visa proteger as transações financeiras com cartões de crédito e débito contra fraudes e roubo de dados.

Para obter a certificação, as empresas precisam cumprir uma série de requisitos, como:

- ✓ Instalar firewalls
- ✓ Software antimalware
- ✓ Software antivírus
- ✓ Implementar criptografia
- ✓ Controle de acesso
- ✓ Monitoramento continuo
- ✓ Testes de segurança
- ✓ Gestão de vulnerabilidades

O processo para obter a certificação PCI DSS, ou *Payment Card Industry Data Security Standard*, envolve uma série de etapas, como:

- Avaliar controles de segurança destinados a produção de cartões (fábricas);
- Adequar a organização às exigências da certificação;
- Contratar uma consultoria especializada para implementar as configurações necessárias;
- Realizar uma auditoria para verificar se todos os requisitos foram atendido.

Obs.: O Relatório de Cumprimento (ROC) é o modelo de relatório que o auditor utiliza para realizar as avaliações nos fornecedores. Ele serve como uma declaração dos resultados da avaliação do fornecedor do cartão em relação ao cumprimento com o PCI.

Visão Geral

O que faz uma fábrica de cartão?

Uma fábrica de cartão de crédito é uma empresa que **produz, imprime ou personaliza cartões**, utilizando máquinas modernas e profissionais especializados.

A fabricação de um cartão envolve várias etapas, como:

- Produção da placa
- Personalização da placa com impressão
- Corte dos cartões
- Finalizações
- Testes
- Distribuição e entrega dos cartões

Qual a importância das medidas de segurança física no processo de fabricação e personalização de cartões?

Mitigar riscos associados à **entradas não autorizadas ao local, possíveis vulnerabilidades visando golpes e fraudes**, proteção e retenção de informações e itens sigilosos.

É fundamental estar atento à forte implementação de **medidas de proteção nas fábricas de cartões pelo alto nível de sensibilidade das informações** pessoais.

Elementos de segurança física em fábricas e personalizadoras de cartões:

Monitoramento

Controle de acesso

Barreiras físicas

Controles Detectivos

Boas Práticas de Segurança

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Controles Físicos

FEBRABAN

Segundo o PCI, as **áreas e instalações em que há produção de cartão, componentes ou dados são armazenados ou processados, são chamados de áreas de alta segurança (HSA)**, tornando-se assim fundamental a proteção destas áreas por meio da implementação e gestão de controles físicos rígidos:

Não deve ser possível exibir atividades na HSA (área de alta segurança) **a partir do exterior do edifício**, através da utilização de vidro **opaco ou não transparente**.

Toda a HSA (área de alta segurança) deve ser **coberta por CCTV** (Circuito Fechado de Televisão) e **monitoramento humano**.

Todos os pontos de acesso (por exemplo, dutos elétricos, janelas e poços de ventilação) **devem ter barreiras físicas**.

Paredes e tetos devem ser construídas em torno da HSA (área de alta segurança) **visando a prevenção de acesso através de tetos falsos ou pisos elevados**.

As portas não devem abrir diretamente para o exterior do edifício, apenas em situações de emergência.

Todas as portas e portões devem possuir equipamento com fecho automático ou **dispositivos de bloqueio e alarmes sonoros** que soam se a porta ou **porta permanece aberta** durante **mais de 30 segundos**.

Saídas de emergência devem estar equipadas com alarmes sonoros locais e monitorado 24 horas por dia e também deve exibir um sinal indicando “porta de saída de emergência com alarme.”

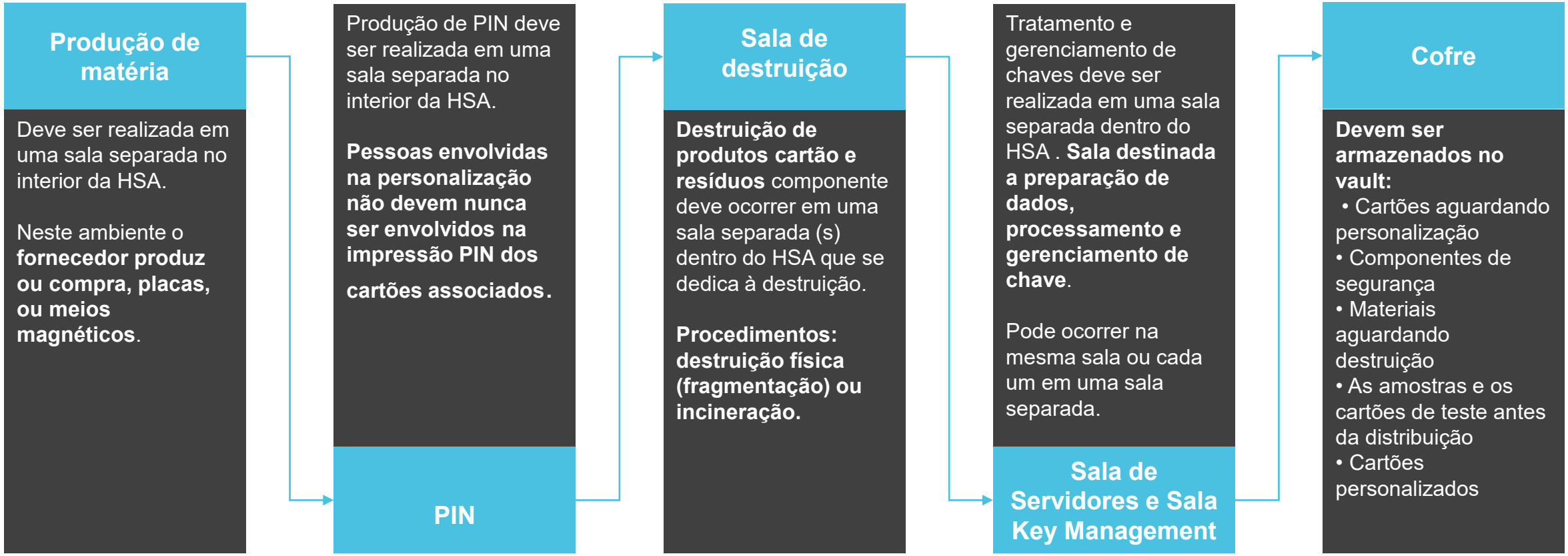
Todas as portas devem estar equipados com um sistema de acesso de **leitor de cartão** conectado a um **computador que grava todos os registros/movimentos**.

Link – Material de Apoio

Segmentação e Controle de Acesso em Salas

FEBRABAN

Dentro do HSA (área de alta segurança), podem **existir os seguintes salas/ambientes segmentados**:



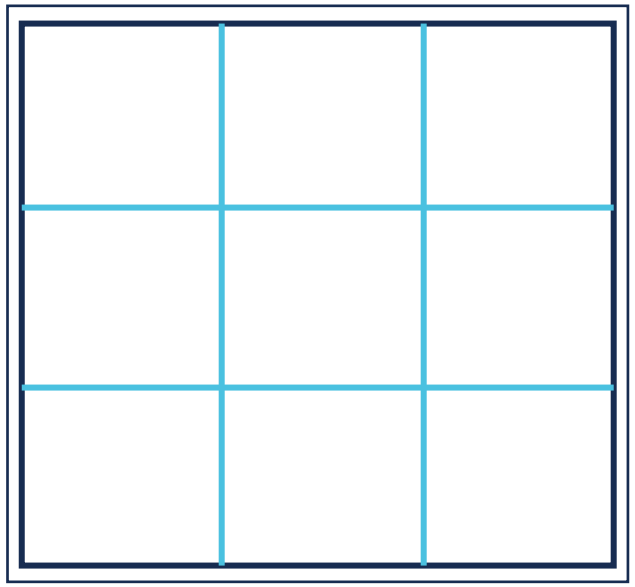
Segmentação e Controle de Acesso em Salas

FEBRABAN

Se a HSA contém **portas corta-fogo que operam normalmente fechadas** ou pode ser fechada manualmente.

Estas portas estão sujeitos aos mesmos controles de acesso como qualquer outra porta que dá acesso a uma sala/quarto.

Os ambientes devem possuir **barreiras físicas**, **controles** de temperatura, umidade, **detectores** de fumaça e calor, assim como detectores de presença e movimento.



Salas separadas dentro do HSA devem cumprir todos os requisitos de segurança física.

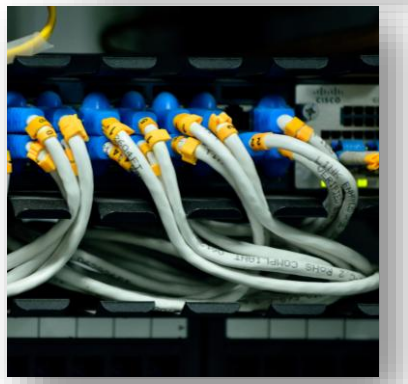
Destruição de produtos cartão e resíduos componente **deve ocorrer em uma sala separada** (s) dentro do HSA que se dedica à destruição.

Sempre que qualquer sala dentro do HSA é ocupado, ele deve conter um mínimo de dois funcionários autorizados. Este deve ser executada pelo sistema de controle de acesso.

WC's são **proibidos** (exceto quando exigido por lei local) e **devem ser isoladas**. Quando usados, o modo de **entrada e saída deve ser monitorado câmera**.

Controle de Acesso (Pessoa-a-pessoa)

- Mecanismos de controle de acesso devem ser implementados (barreiras físicas, catracas, controles de ingresso aos ambientes) e gerenciados por meios lógicos, assegurando conformidade com as exigências de controle de acesso de pessoas.
- A ativação do dispositivo de acesso deve ser controlado por um leitor de cartões que impõe uma função *antipass-back* (controle para evitar que os usuários possam entrar ou sair mais de uma vez consecutivamente).
- Os leitores de cartão devem operar permanentemente conectados a um computador que centraliza o registro de qualquer ativação de leitura.
- O status do acesso deve mudar apenas quando a pessoa tenha concluído com êxito o ciclo de acesso.



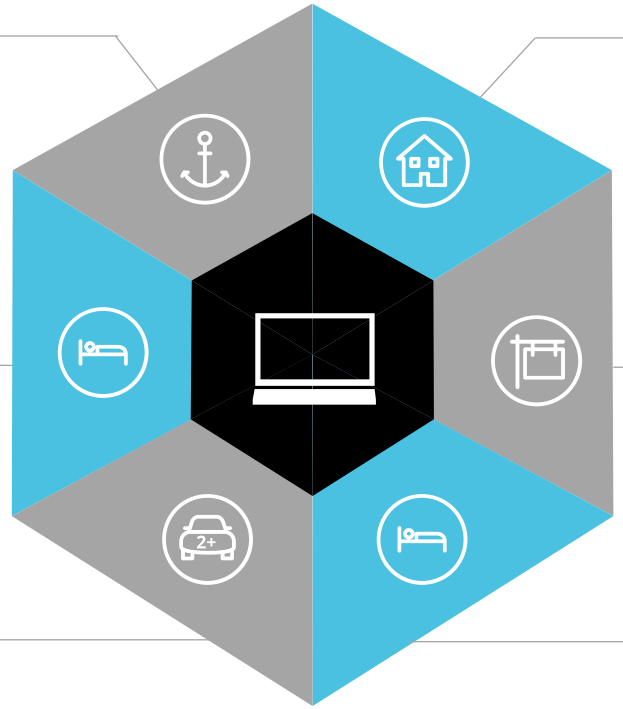
Boas Práticas de Segurança

Abaixo estão relacionadas algumas boas práticas de segurança:

A designação de um responsável por todas as questões de segurança. Além disso, torna-se necessário produzir relatórios de segurança relatando incidentes, ameaças, problemas, entre outros (de preferência mensalmente).

Garantir que os indivíduos realizem ou gerenciem tarefas que exijam acesso aos componentes do cartão e dados, tenham um contrato de trabalho definido com o fornecedor.

Assegurar que o **treinamento de segurança contemple a obrigação dos funcionários de relatar qualquer violação** de procedimento de segurança estabelecido observada.



Disponibilizar uma cópia do manual de segurança interna para todos os funcionários contendo:

- HSAs;
- Requisitos de segurança e diretrizes;
- Procedimentos que os funcionários devem seguir enquanto trabalham na instalação.

A realização de sessões de capacitação obrigatórias pelo menos anualmente. Estas sessões devem incluir a compreensão das políticas de segurança da empresa e responsabilidades dos funcionários e sua adesão às políticas de segurança.

Exibir cartazes e avisos relacionados com a segurança em locais-chave dentro das instalações do fornecedor.

Notificação e Documentação

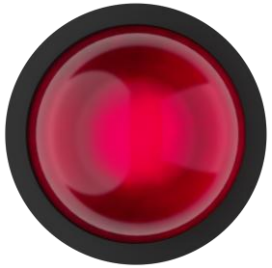
O f**ornecedor** deve **notificar sobre quaisquer mudanças de pessoal que afetem diretamente a segurança dos cartões** e componentes relacionados, incluindo mas não limitados a alta administração e funcionários das empresas, gerente de Segurança e trabalhadores autorizados a receber ou assinar para quaisquer componentes de cartões.

Deve ser realizada a documentação dos seguintes tópicos:

A guarda de **responsabilidades, procedimentos e atividades por posição/perfil**

A interação entre gestão de processos de produção, contratados de guarda ou de monitoramento de serviços, a polícia e outros serviços de emergência

Controle de acesso em todos os pontos de entrada e de saída das instalações, por data e hora de ativação



Os procedimentos de ativação de alarme, resposta a alarmes, incluindo a notificação para a aplicação da lei em casos de acesso não autorizado às instalações

A atividade diária e relatório de incidente imediato, assim como potenciais ameaças

Os procedimentos devem ser revistos, validados e, se necessário, atualizado anualmente.

Considerações Finais

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Frameworks e Normas de Referência

Para apoiar no entendimento e implementação de toda a metodologia apresentada neste material, a seguir são apresentados as normas e frameworks de referência no tema:

Frameworks Padrão Utilizados

Conformidade: Requisitos de conformidade mais exigentes, permitindo estimar o nível de conformidade com o PCI-DSS.

Relembrando os principais conceitos

Agora que aprendemos sobre as práticas de Segurança em Fábricas de Cartões, relembre os principais termos e conceitos apresentados neste material:

- **PCI-DSS:** O Padrão de Segurança de Dados da Payment Card Industry (PCI DSS) foi desenvolvido para aprimorar a segurança dos dados de contas de cartões de pagamento e facilitar a ampla adoção de medidas de segurança de dados consistentes no mundo todo.

- **Segmentação e Controle de Acesso em Salas:** Dentro do HSA (área de alta segurança), podem existir os seguintes salas/ambientes segmentados, tais como: produção de matéria, PIN, sala de destruição, sala de servidores e key management e sala de cofre.

- **Controle de Acesso (Pessoa-a-pessoa):** Mecanismos de controle de acesso devem ser implementados (barreiras físicas, catracas, controles de ingresso aos ambientes) e gerenciados por meios lógicos, assegurando conformidade com as exigências de controle de acesso de pessoas.

- **Notificação e Documentação:** O fornecedor deve notificar sobre quaisquer mudanças de pessoal que afetem diretamente a segurança de produtos de cartões e componentes relacionados, incluindo mas não limitados a alta administração e funcionários das empresas, gerente de Segurança e trabalhadores autorizados a receber ou assinar para quaisquer componentes de cartões.

Módulo: Inteligência Artificial

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Requisitos – Inteligência Artificial

FEBRABAN

Este material foi elaborado de acordo com as diretrizes da ISO e NIST, bem como foram considerado os requisitos de segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

ISO 23894

- Princípios da Gestão de Riscos em IA
- Framework
- Processo de Gestão de Risco

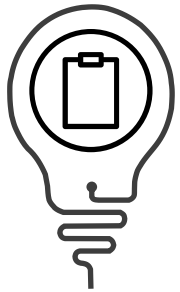
PL 2.338/2023

- Marco Regulatório da IA no Brasil
  - Senado aprovou o Projeto de Lei 2.338/2023
  - Passará para a Câmara dos Deputados

NIST CSF

- ID.AM-08: Sistemas, hardware, software, serviços e dados são gerenciados ao longo de seus ciclos de vida.
- PR.DS: A confidencialidade, integridade e disponibilidade dos dados são protegidas.
- DE.CM-01: Redes e serviços de rede são monitorados para encontrar eventos potencialmente adversos.
- DE.AE-02: Eventos potencialmente adversos são analisados para entender melhor as atividades associadas.
- DE.AE-03: Informações são correlacionadas de múltiplas fontes.
- RS.AN-03: Análises são realizadas para estabelecer o que ocorreu durante um incidente e a causa raiz do incidente.

NIST AI RMF



1. Framing Risk
2. Audience
3. AI Risks and Trustworthiness
4. Effectiveness of the AI RMF
5. AI RMF Core
6. AI RMF Profiles

Sumário

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Sumário

Introdução e contexto

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Introdução e contexto

A inteligência artificial é um ramo da ciência da computação, que visa o desenvolvimento de sistemas capazes de realizar tarefas que normalmente exigem inteligência humana. Esses sistemas são projetados para simular algumas características do pensamento humano, como aprendizado, raciocínio, resolução de problemas, reconhecimento de padrões, dentre outros.

História da Inteligência Artificial (IA)

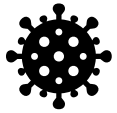
1940	“máquinas que imitam a inteligência humana”	Regras lógicas em algoritmos específicos para solucionar problemas

Os algoritmos de Redes Neurais Artificias (RNA), Computação Evolutiva (algoritmos genéticos) e Lógica Fuzzy fizeram parte das técnicas de implementação da IA. O Machine Learning (Aprendizagem de Máquina), atualmente muito associado ao Big Data e ao Analytics, foi defendido por T. Mitchell em 1997 e surgiu dos sistemas baseados em conhecimento da IA clássica. O grande desafio é desenvolver sistemas capazes de aprender:

- Por si mesmos, através de experiências e comportamentos passados (aprendizagem não supervisionada)
- Por meio de entrada de mapas de dados (aprendizagem supervisionada)

Introdução

Principais conceitos em Inteligência Artificial

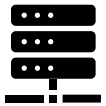


Machine Learning

Machine learning (ML) ou aprendizado de máquina, é uma área da inteligência artificial (IA) que permite que sistemas aprendam e melhorem de forma autônoma. O ML usa algoritmos para analisar grandes quantidades de dados, identificar padrões e correlações, e tomar decisões com base nessas análises.

Visão computacional

A visão computacional é uma área de pesquisa que combina inteligência artificial, aprendizado de máquina, processamento de imagens e outras técnicas, para ensinar máquinas a realizarem interpretação de imagem e informações visuais



NLP

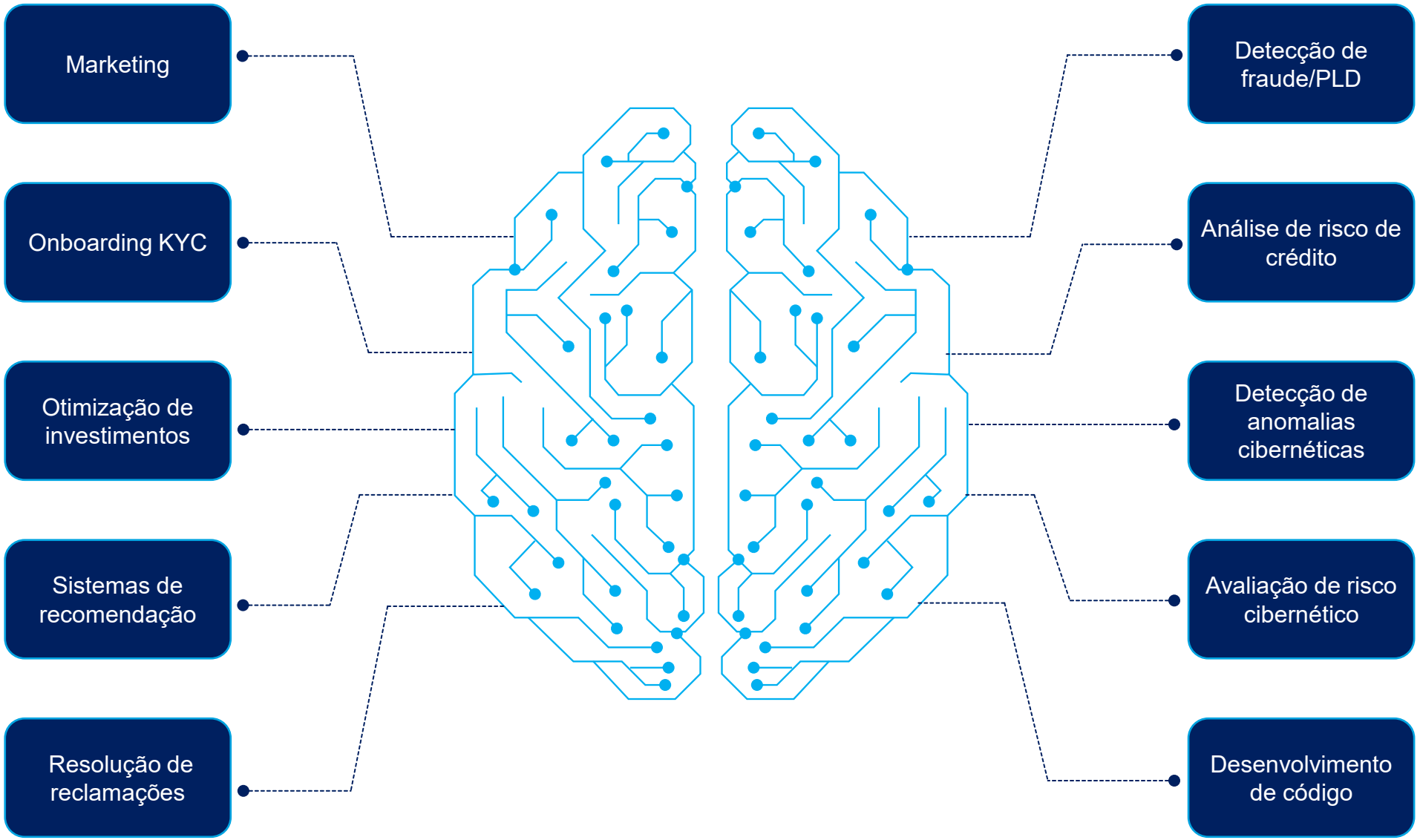
Natural Language Processing (Processamento de Linguagem Natural) é uma área da Inteligência Artificial (IA) que permite que os dispositivos tecnológicos compreendam a linguagem humana e respondam às suas demandas, traduzindo informações verbais ou escritas para formatos digitais

Sistemas Inteligentes

Sistemas inteligentes são plataformas tecnológicas que simulam a capacidade racional do ser humano de resolução de problemas e tomada de decisões.

Principais usos das aplicações de IA pelos bancos

FEBRABAN



Casos Reais

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Casos Reais

Exame

Deepfakes superam ataques cibernéticos como principal uso malicioso de IA, aponta DeepMind

O uso de inteligência artificial (IA) para criar deepfakes que imitam políticos e celebridades é mais prevalente do que o uso da IA para...

25 de jun. de 2024

Forbes Brasil

IA foi utilizada em mais de 50% dos ataques recentes contra empresas brasileiras

Com textos melhores, credenciais forjadas e imagens ou vozes geradas por deepfake, criminosos estão sobrecarregando as equipes de TI.

2 de mai. de 2024

Especialistas apontam IA como arma para proteger sistemas de hackers sofisticados

A inteligência artificial (IA) está reformulando o campo da cibersegurança, com avanços importantes na detecção de ameaças e na proteção de...

25 de jun. de 2024

Principais Riscos

Os riscos existentes relacionados à inteligência artificial podem ocorrer durante o ciclo de vida da IA (design, desenvolvimento, implantação, operação, treinamento ou descomissionamento). Em muitos casos os riscos relacionados à IA podem envolver comportamento humano. Os casos de vulnerabilidades podem envolver modelos ou sistemas arquitetônicos, mecanismos de treinamento ou arquivamento, tipos de dados usados, níveis de modelo de acesso ou disponibilidade, e aplicações ou contextos de casos de uso.

Confabulação
Produção de informações errôneas ou de falso conteúdo

Conteúdo de ódio, ilegal ou perigoso
Produção de conteúdo violento, explícito ou com condutas ilegais

Data Privacy
Impactos causados por vazamento, uso não autorizado ou corrompimento de dados sensíveis

Preconceitos prejudiciais
Podem ser causados por errônea performance devido à dados não representativos de grupos sociais, questões históricas e discriminação

Configurações Humanas-IA
Podem gerar defeitos ou informações incorretas de configuração

Integridade da informação
Pode ser afetada ou corrompida por informações incorretas ou opiniões

Propriedade Intelectual
Compartilhamento, plágio ou apropriação de conteúdo sem autorização e busca de fontes e origem de material

Conteúdo abusive, obceno ou explícito
Envolvendo casos de imagens compartilhadas sem autorização

Segurança da Informação
Exposição à vulnerabilidades e possíveis ameaças cibernéticas

Gestão de Risco em IA

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

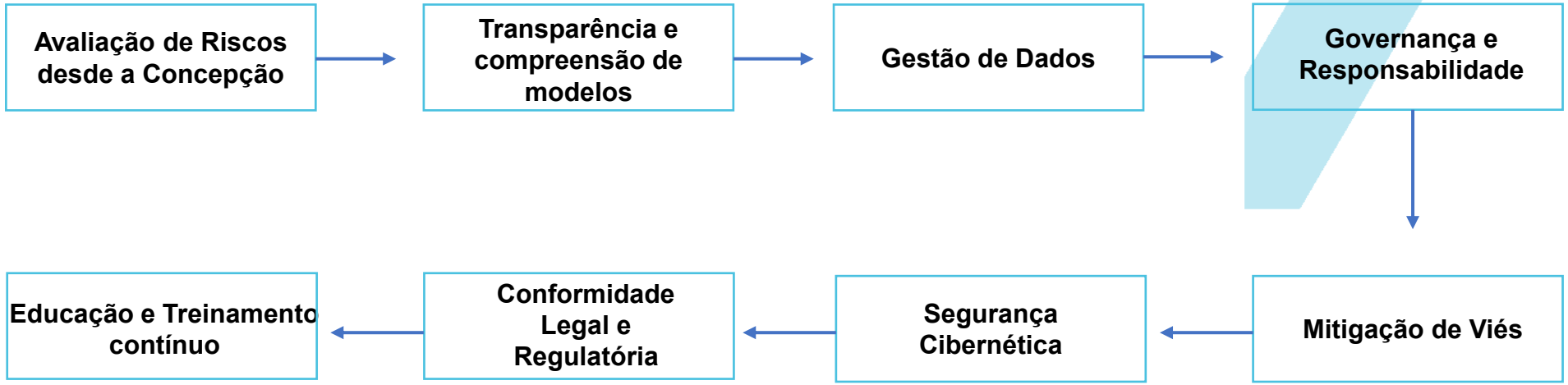
Gestão de Risco em IA

Gestão de Riscos

Definir uma estratégia de uso de IA inclui determinar a integridade dos sistemas de IA contra atores mal-intencionados e a capacidade de defesa contra ameaças cibernéticas.

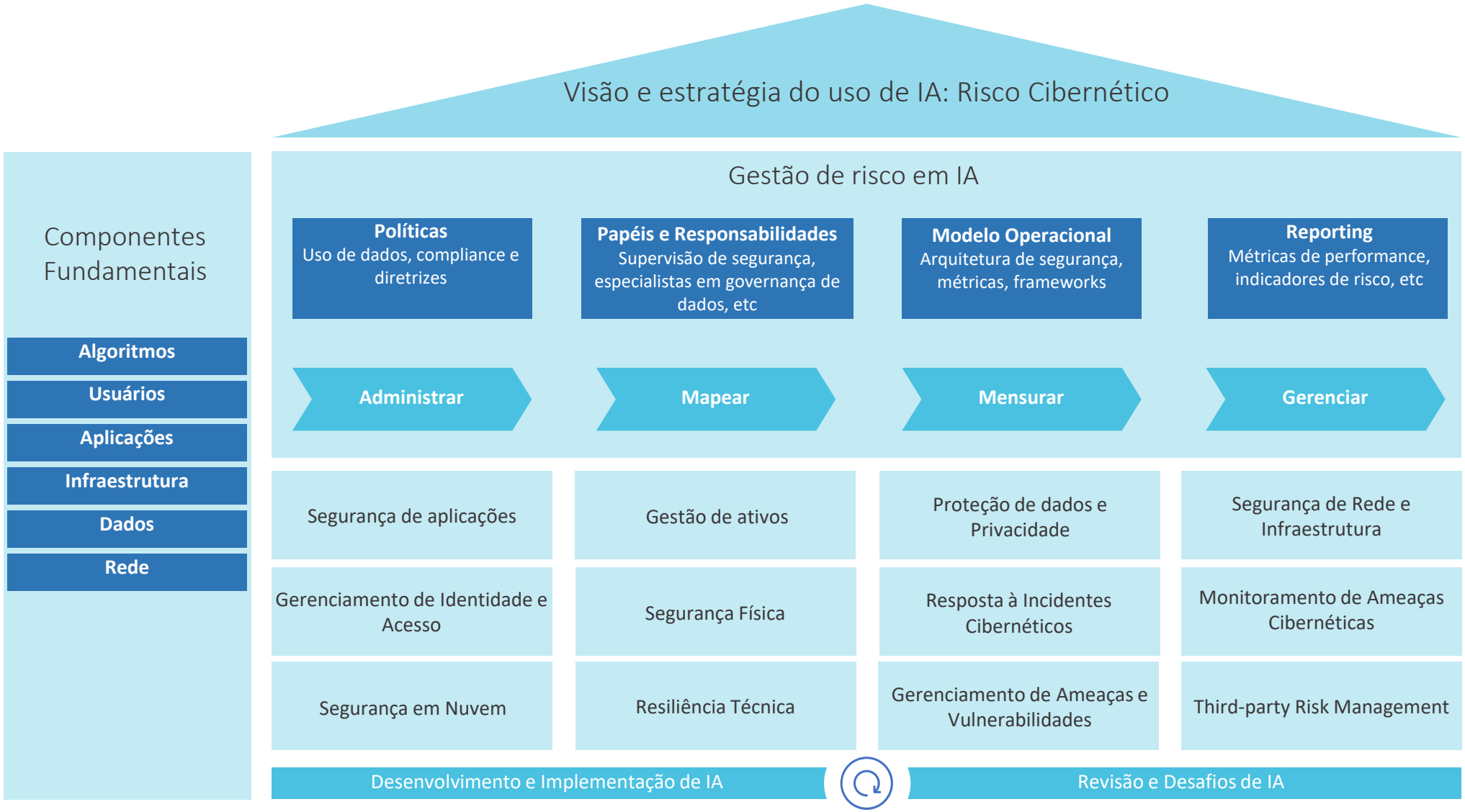
A estratégia de IA deve promover a implementação segura e protegida de IA e de produtos GenAI, incluindo ferramentas de desenvolvimento e suporte à equipe de desenvolvimento.

Etapas de Gestão de Riscos



Gestão de Risco em IA

FEBRABAN



Cibersegurança no desenvolvimento de GenAI

FEBRABAN

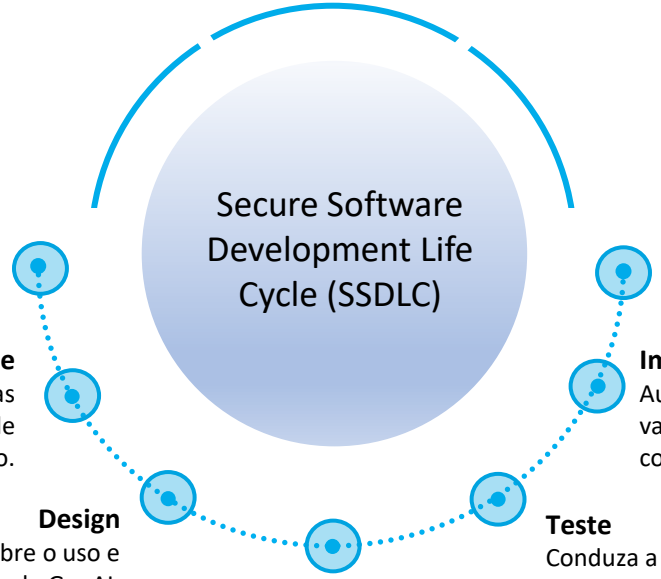
GOVERNANÇA

- **Políticas de Uso Aceitável da Ferramenta GenAI**
- **Requisitos fundamentais**
- **Conselho de Governança GenAI**

PESSOAS

- **Treinamento GenAI focado em desenvolvedores**
- **Cultura colaborativa e consciente de segurança**
- **Foco na experiência do usuário e do desenvolvedor**

PROCESSO



Concepção
Acompanhe os atributos do projeto e o perfil de risco e alinhe-o aos requisitos da política.

Análise
Obter aprovação para uso de ferramentas GenAI e implantar plataforma de desenvolvimento seguro.

Design
Prover orientação e treinamento sobre o uso e controles de ferramentas de GenAI.

Desenvolvimento
Habilitar a abordagem AI-fast shift-left para identificar e corrigindo vulnerabilidades com visibilidade para metas de conformidade.

Teste
Conduza a priorização de vulnerabilidades com base em riscos e fornecer mitigações.

Implantação
Automatize as proteções de segurança para validar os requisitos de segurança e a conformidade dos testes de segurança.

Manutenção
Conduza varreduras contínuas em busca de possíveis "secrets" ou exposição de CI por meio da GenAI e monitore continuamente os GAPs do programa de segurança.

Princípios Fundamentais

Pessoas

O "fator humano" é decisivo para a segurança da IA. O treinamento é vital para ajudar os membros da equipe a entenderem os riscos, as melhores práticas e a lógica por trás dos controles.

Os treinamentos devem incluir diretrizes sobre dados permitidos nas ferramentas GenAI para proteger a propriedade intelectual e cumprir as regulamentações de dados.

Um ponto importante é que de acordo com o relatório da Snyk, mais da metade dos usuários de IA encontraram vulnerabilidades nos códigos gerados por estas Inteligências Artificiais. Além disso, observa-se que muitos desenvolvedores que usam GenAI confiam por muitas vezes, mais nos códigos gerados por IA do que em seus próprios códigos gerados "manualmente". Sendo assim, há chances de um desenvolvedor replicar um código vulnerável em suas instituições, e para mitigar esse ponto é importante fornecer orientações claras sobre as políticas de uso de ferramentas de IA para codificação.

Princípios Fundamentais

Processo

As organizações devem considerar como atualizar seus processos e políticas, de forma a acomodar o uso crescente de ferramentas de GenAI no desenvolvimento, sem comprometer a segurança da empresa.

As ferramentas GenAI permitem um ritmo rápido de desenvolvimento, o que pode afetar significativamente a eficácia dos processos de segurança de aplicativos (AppSec) existentes. Além de processos e políticas que governam o uso do GenAI, deve-se considerar as seguintes recomendações para escalar componentes-chave do programa de AppSec, para atender à demanda aumentada pelo desenvolvimento com GenAI:

- Comunicação
- Orientação sobre falsos positivos
- Priorização de vulnerabilidades

Princípios Fundamentais

Governança

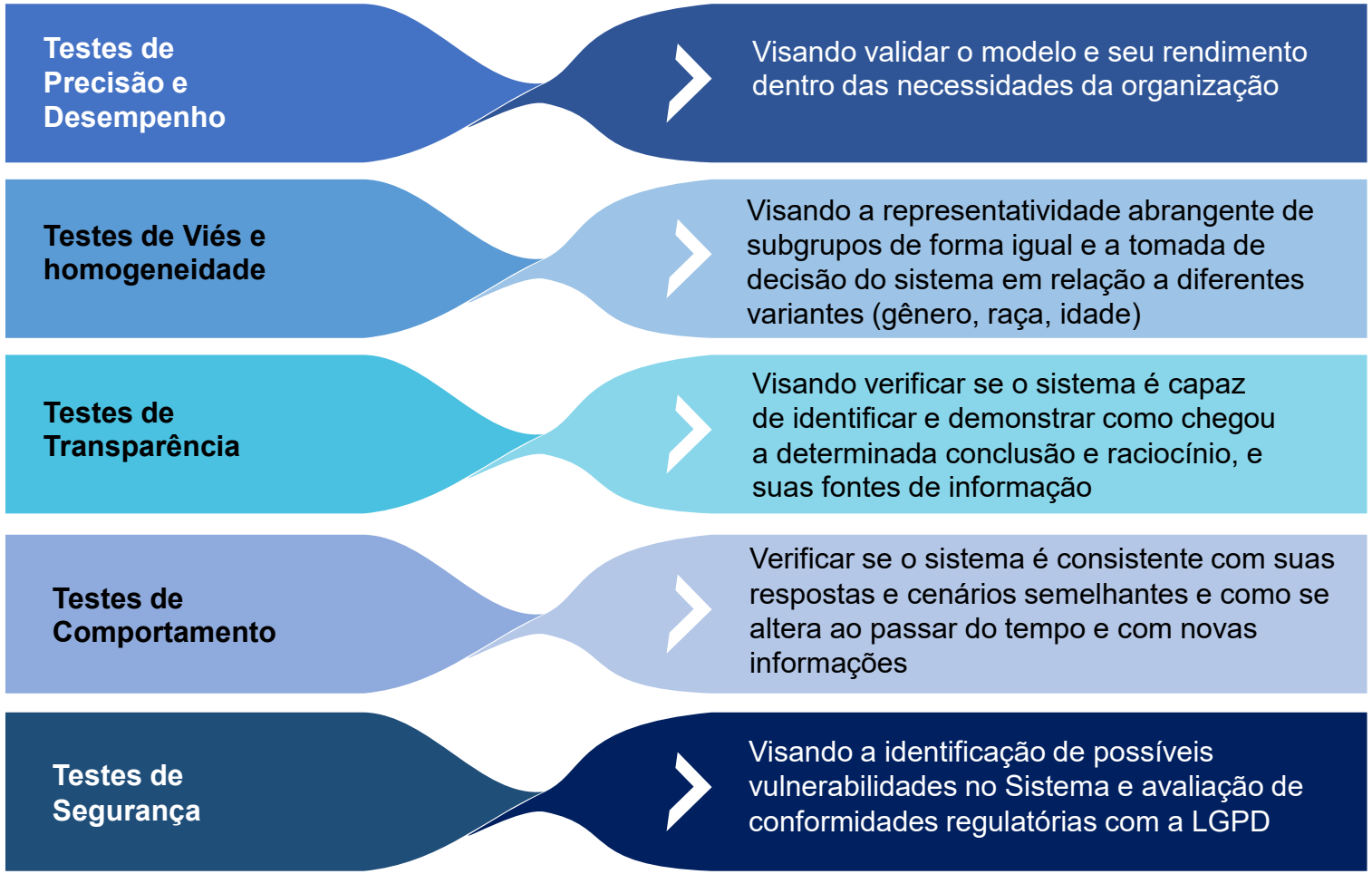
A governança eficaz é essencial no campo de mudanças rápidas envolvendo GenAI. Essa governança envolve validação rigorosa de segurança, implementação de políticas de segurança preparadas para IA e instalação de ferramentas de segurança antes de implantar o GenAI para desenvolvimento.

As organizações devem estabelecer políticas programáticas para evitar a aceitação precipitada e acrítica de código gerado por IA e garantir que o código gerado passe por revisão. As políticas internas sobre o uso de ferramentas GenAI para desenvolvimento devem abordar:

- Definição clara de casos de uso aceitáveis
- Seleção e uso de dados
- Privacidade e segurança de dados
- Requisitos de conformidade
- Atualizações regulares

Aplicação de Testes em Sistemas Inteligentes

Testar sistemas de inteligência artificial (IA) é uma tarefa fundamental para garantir que estes funcionem corretamente, de forma ética, segura e eficaz. Alguns possíveis testes a serem aplicados são:

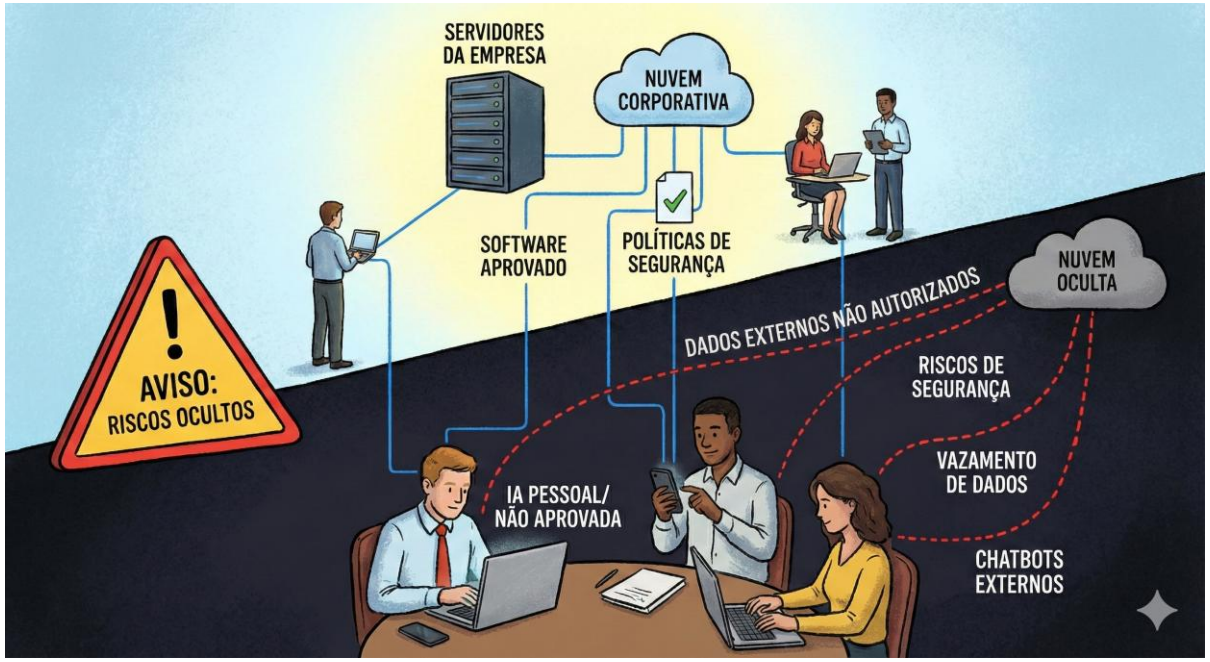


Vazamento de Dados e Shadow AI

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Vazamento de Dados e Shadow AI

A adoção acelerada da inteligência artificial trouxe ganhos de produtividade, mas também novos riscos. Um dos mais críticos é o **vazamento de dados por meio de ferramentas de IA**. Quando colaboradores inserem informações sensíveis em sistemas externos, como chatbots ou geradores de código, esses dados podem ser armazenados e usados para treinar modelos, sem controle da organização. Em casos extremos, se o provedor da IA sofrer um ataque, essas informações podem ser roubadas. **Isso compromete segredos corporativos, dados pessoais e propriedade intelectual, gerando impactos financeiros e regulatórios severos.**



O que é Shadow AI?

Shadow AI refere-se ao uso de ferramentas de inteligência artificial sem aprovação ou supervisão da área de TI. Esse fenômeno cresce rapidamente, impulsionado pela busca por eficiência e inovação, mas representa um risco invisível para as organizações. Quando colaboradores utilizam IA sem governança, a empresa perde controle sobre dados, compliance e segurança, criando brechas para vazamentos e violações regulatórias.

Olhar atento!

De acordo com a pesquisa Gartner 2025 sobre Inovações em Cibersegurança e Gestão de Riscos em IA, **lidar com os riscos de Shadow AI é um grande desafio para as organizações**. Os dados revelam um cenário preocupante:

- 69% das empresas suspeitam ou têm evidências de que colaboradores utilizam ferramentas públicas de GenAI proibidas.
- 79% acreditam que há mau uso de soluções públicas de GenAI aprovadas.

Recomendações

Segundo as melhores práticas de segurança em IA, é recomendado implementar um plano de comunicação abrangente para garantir que todos os colaboradores compreendam as diretrizes básicas para interagir com IA de forma segura. Algumas orientações norteadoras incluem:

- Compartilhar apenas dados classificados como públicos com ferramentas de IA não autorizadas. Nunca envie informações confidenciais, proprietárias ou reguladas para serviços GenAI sem aprovação.
- Utilizar configurações fornecidas pelo fornecedor para desativar a reutilização de dados em qualquer interação com IA não autorizada.
- Validar sempre as respostas da IA antes de compartilhar ou tomar decisões com base nelas.

Fonte: https://www.gartner.com/en/documents/6567002

Desenvolvimento Seguro com IA

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Desenvolvimento de Segurança com IA

O desenvolvimento de Segurança com a IA se trata da aplicação de técnicas de Inteligência Artificial (IA) visando a robustez e melhora da segurança cibernética e proteção de sistemas e dados contra ameaças emergentes. Aqui estão os principais aspectos do Desenvolvimento de Segurança com IA:

Detecção e Respostas de Ameaças	A IA pode ser treinada para identificar comportamentos anômalos e suspeitos dentro das redes ou sistemas. Em alguns casos, a IA pode não apenas detectar um ataque, mas também tomar medidas imediatas para mitigar a ameaça. Além disso, os Sistemas Inteligentes podem ser usados para analisar grandes volumes de logs e eventos gerados por sistemas de segurança, buscando comportamentos fora do padrão.
Prevenção de Ameaças	Sistemas de IA podem aprimorar a autenticação de usuários, detectando comportamentos anômalos e aprimorando os processos de verificação de identidade, além de analisar comportamento de código através de Machine Learning sendo capaz de identificar e bloquear malwares antes que eles causem danos; A IA pode ser usada para prever ataques cibernéticos com base em padrões históricos e dados atuais.
Fortalecimento de Criptografia	Os algoritmos de IA podem ser aplicados para melhorar e fortalecer os métodos de criptografia, criando sistemas mais robustos para proteger dados sensíveis.
Análise de Vulnerabilidades	A IA pode ser utilizada para realizar testes de penetração automatizados para checar por possíveis vulnerabilidades no sistema, além de serem ser aplicados para analisar automaticamente grandes bases de código buscando falhas.
Aprimoramento de SIEM	Pode-se utilizar a IA para realizar uma análise mais inteligente de grandes volumes de dados de segurança em tempo real e priorizando alertas e possíveis vulnerabilidades, além de analisar o comportamento de usuários dentro do sistema observando comportamentos incomuns.
Resposta de Incidentes	A IA pode automatizar a resposta a incidentes de segurança tomando decisões rápidas para mitigar danos e ameaças, além de atuar diretamente no processo pós incidente, ao analisar o sistema e buscar a causa raiz ou vulnerabilidade de origem de ataque e elaborar relatórios.

Boas Práticas

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Boas práticas relacionadas à Inteligência Artificial

FEBRABAN

Data Privacy

- Alinhar o desenvolvimento da IA com o uso de leis e regulamentações aplicáveis.
- Estabelecer políticas de transparência e processos de documentação das fontes de informação e histórico de treinamento.
- Conduzir monitoramento periódico de conteúdo gerado por IA em busca de riscos de privacidade e possíveis exposições ou vulnerabilidades de dados

Conteúdo abusivo, obceno ou explícito

- Estabelecer políticas e mecanismos de prevenção aos sistemas IA, de produzir conteúdo que viole leis e regulamentações
- Produzir filtros de conteúdo e atualizá-los constantemente com auxílio de machine learning

Boas práticas relacionadas à Inteligência Artificial

FEBRABAN

Configurações Humanas-IA

- Estabelecer políticas e procedimentos de revisão pós resposta de incidentes e ameaças para identificar falhas
- Estabelecer processos de verificação para conferir se os indivíduos que atuam no Sistema de IA, demonstram possuir as habilidades e treinamentos necessários
- Definir usos e políticas que contemple a intervenção humana no ciclo de vida do Sistema IA (chatbots, processos de tomadas de decisão), incluindo critérios que impeçam a IA de resolver

Segurança da Informação

- Estabelecer práticas de identificação mínima necessárias a serem realizadas pelo sistema IA em casos de incidentes, como por exemplo: ID do sistema, título, fonte, data do incidente, data do relatório, descrição, impacto
- Implementar planos contínuos de testes para identificação de vulnerabilidades e potenciais manipulações ou má conduta
- Definir o perfil de ameaças existentes no cenário à IA, contemplando ameaças emergentes, vulnerabilidades atuais, a possibilidade de ocorrência, assim como seu possível impacto à organização

Boas práticas relacionadas à Inteligência Artificial

FEBRABAN

Integridade da informação

- Considerar os seguintes pontos ao atualizar ou definir riscos de IA: abusos ou impactos à integridade da informação; dependências entre IA e outros sistemas de dados; ameaças à Segurança pública ou à leis e direitos fundamentais; impactos psicológicos; uso malicioso.
- Definir as responsabilidades organizacionais de forma periódica e a avaliação do conteúdo e monitoramento de incidentes em sistemas de IA.
- Reavaliar o limite de tolerâncias de riscos da organização

Preconceitos prejudiciais

- Manter uma hierarquia atualizada de riscos identificados e esperados, voltados ao uso de modelos de IA.
- Determinar e documentar o contexto de uso do Sistema de IA esperado e aceitável em colaboração com especialistas socio-culturais (valores ligados à organização, ambiente operacional e padrões de uso observados, potenciais impactos negativos e positivos individuais, Segurança pública e expectativas sociais e democráticas)
- Manter um monitoramento constante dos possíveis impactos causados pelo Sistema de IA, verificando se está devidamente equilibrado entre diferentes sub grupos

Considerações Finais

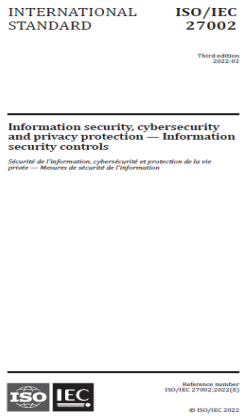
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Frameworks e normas de referência

FEBRABAN

Para apoiar no entendimento e implementação de toda a metodologia apresentada neste material, a seguir são apresentados as normas e frameworks de referência no tema:

Frameworks Padrão Utilizados


INTERNATIONAL STANDARD

ISO/IEC 27002

Third edition 2022-02

Information security, cybersecurity and privacy protection — Information security controls

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

ISO IEC

Reference number ISO/IEC 27002:2022(E)

© ISO/IEC 2022


NORMA BRASILEIRA

ABNT NBR ISO 22300

Primeira edição 07.01.2022

Segurança e resiliência — Vocabulário

Security and resilience — Vocabulary

ABNT

International Organization for Standardization

ISO

22301

Conformidade: Dado o uso extensivo de padrões amplamente aceitos pela indústria, a continuidade dos negócios deve ser alinhada com alguns dos requisitos de conformidade mais exigentes, permitindo estimar o nível de conformidade com NIST, ISO, Bacen 4.893, DRI, entre outros.

Relembrando os principais conceitos

Agora que aprendemos sobre as atividades relacionadas ao processo de gestão de continuidade de negócios, relembre os principais termos e conceitos apresentados neste material:

Machine learning (ML) ou aprendizado de máquina: é uma área da inteligência artificial (IA) que permite que sistemas aprendam e melhorem de forma autônoma que faz uso de algoritmos para analisar grandes quantidades de dados, identificar padrões e correlações, e tomar decisões com base nessas análises.

Gestão de Riscos de IA: Envolve uma sequência de etapas necessárias para estabelecer um desenvolvimento seguro dentro do ciclo de vida da IA . O processo de gestão de riscos de IA engloba desde sua implantação e escopo, desenvolvimento de modelo, gestão de dados, governança, conformidades legais e melhorias, treinamento contínuo e em alguns casos o desligamento.

Testes em Sistemas de Treinamento: A aplicação de treinamentos em sistemas de IA é fundamental para garantir o funcionamento correto e seguro destes sistemas e suas devidas aplicações, alguns testes de alta relevância são os testes comportamentais, testes de transparência e testes de segurança. A aplicação destes testes deve ser realizada de forma periódica e com relatórios robustos.

Módulo: Proteção de APIs

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Requisitos – Proteção de APIs

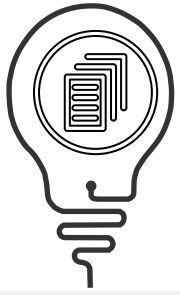
Este material foi elaborado com base nas diretrizes da OWASP, considerando também os requisitos de segurança da informação pertinentes ao tema. Os controles principais estão listados a seguir, organizados conforme normas e frameworks consolidados, em ordem de priorização, de acordo com a visão da Deloitte:

CIS Controls

Controles

- **Controle 2**: Inventário e controle de ativos de software
- **Controle 3**: Proteção de dados
- **Controle 6**: Gestão de controle de acesso
- **Controle 16**: Segurança de aplicação de software
- **Controle 18**: Teste de intrusão (Pentest)

PCI DSS



Requisitos

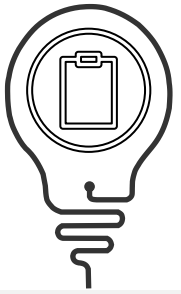
- **Requisito 4**: Proteger os dados com criptografia forte durante a transmissão em redes abertas e públicas
- **Requisito 6**: Desenvolver e manter sistemas e softwares seguros
- **Requisito 8**: Identificar os usuários e autenticar o acesso aos componentes do sistema
- **Requisito 10**: Registrar e monitorar todos os acessos aos componentes do sistema e aos dados do portador do cartão
- **Requisito 11**: Testar regularmente a segurança de sistemas e redes

ISO 27002:2022

Controles

- **5.9** Inventário de informações e outros ativos associados
- **5.15** Controle de acesso
- **5.16** Gestão de identidade
- **8.16** Monitoramento de atividades
- **8.24** Uso de criptografia
- **8.25** Ciclo de vida de desenvolvimento seguro
- **8.28** Codificação segura
- **8.29** Testes de segurança no desenvolvimento e aceitação
- **8.31** Separação entre ambientes de desenvolvimento, teste e produção

NIST CSF



Subcategorias

- **PR.PS-06**: Práticas seguras de desenvolvimento de software são integradas
- **ID.IM-02**: Testes e exercícios de segurança
- **ID.AM-02**: Inventários de software, serviços e sistemas gerenciados pela organização
- **PR.AA-01**: Identidades e credenciais de usuários, serviços e dispositivos autorizados
- **PR.AA-05**: Permissões de acesso, direitos e autorizações são definidas incorporando os princípios de privilégio mínimo e separação de funções
- **PR.DS**: Confidencialidade, integridade e disponibilidade dos dados em repouso, em trânsito
- **PR.IR-01**: Ambientes são protegidos contra acesso lógico e uso não autorizado
- **DE.CM-01**: Monitoramento contínuo de redes

Sumário

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Sumário

Contextualização

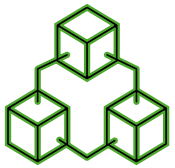
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Função de uma API

As APIs são mecanismos que permitem a comunicação e interação entre diferentes softwares, viabilizando a troca de dados e funcionalidades. **Elas funcionam como alicerces digitais**, possibilitando que empresas ofereçam serviços a desenvolvedores e parceiros externos.

Além de orquestrar a comunicação entre aplicações, as APIs desempenham papéis estratégicos, como melhorar a experiência do usuário, ampliar o alcance dos negócios e impulsionar a inovação tecnológica de ponta a ponta.

No entanto, à medida que se tornam mais presentes e abrangentes, as APIs também passam a **representar desafios crescentes à segurança**. Isso ocorre porque praticamente toda aplicação ou serviço web disponível hoje é, de alguma forma, alimentado por APIs, o que amplia a superfície de exposição a possíveis vulnerabilidades.



No **setor financeiro brasileiro**, é possível destacar o uso de APIs para interação ao Open Finance, que representa um ecossistema que permite o compartilhamento de dados entre instituições financeiras. Esse ecossistema é sustentado por uma documentação robusta, que abrange desde especificações técnicas até diretrizes de segurança.

Tipos de APIs

APIs privadas (também chamadas de APIs internas) são comumente utilizadas por desenvolvedores e prestadores de serviço dentro da própria empresa. Frequentemente associadas a iniciativas de arquitetura orientada a serviços (SOA), essas APIs têm como objetivo simplificar o desenvolvimento interno, permitindo que diferentes departamentos ou unidades de negócio acessem dados entre si de forma eficiente e eficaz.

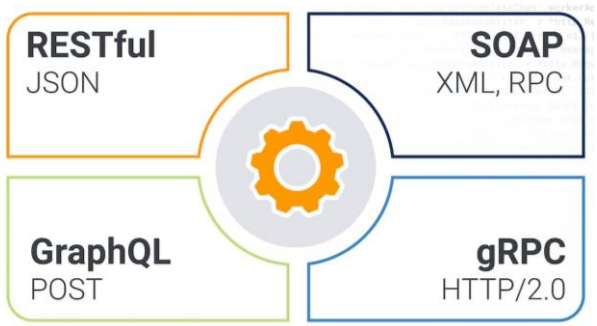
X

APIs públicas (ou externas) podem ser acessadas por parceiros, clientes ou até pelo público em geral, dependendo do nível de abertura definido. Por serem voltadas aos usuários externos, essas APIs exigem um controle mais rigoroso, incluindo autenticação (se aplicável), monitoramento de uso e, principalmente, uma documentação clara e completa, que facilite a integração por desenvolvedores que não fazem parte da organização.

API WEB:

Uma API Web é uma interface programável que permite a comunicação entre sistemas por meio da Web. Ela consiste em um ou mais endpoints (pontos de acesso) expostos publicamente, que seguem um modelo de troca de mensagens no formato solicitação-resposta — geralmente utilizando JSON ou XML. Essas APIs são disponibilizadas por meio de servidores Web, com o protocolo HTTP sendo o mais comum para transporte das mensagens.

Os quatro principais tipos de APIs da Web vistos hoje, são:



APIs, ou interfaces de programação de aplicações, são uma parte fundamental do desenvolvimento moderno da Web, a partir desta responsabilidade a segurança é fundamental. Alguns dos aspectos mais relevantes envolvendo a segurança de API da WEB são a autenticação, a autorização e a validação de entrada, fazendo com que os dados sejam verificados antes de serem processados.

Identificação de riscos e ameaças

Implementação de abordagem sistemática para identificar e corrigir vulnerabilidades comuns de API, incluindo as do OWASP API Top 10.

Assim como em qualquer aplicação ou sistema de software, o monitoramento e a manutenção em tempo real são essenciais para manter a segurança de API.

É de grande importância que organizações adotem padrões de segurança como as recomendações de segurança de API do Open Web Application Security Project (OWASP). A lista Top 10 de Segurança de API do OWASP, por exemplo, oferece uma estrutura para entender e mitigar as ameaças de segurança de API mais críticas e comuns, como autenticação quebrada, atribuição em massa e falsificação de solicitação do lado do servidor.

Outras fontes de referência e atualização de ameaças e informações podem ser fundamentais neste processo, como o MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK), a General Data Protection Regulation (GDPR), e o International Organization for Standardization (ISO).

OWASP Top 10 API

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

1 - API1:2023 - Broken Object Level Authorization

As APIs tendem a expor endpoints que manipulam identificadores de objetos, criando uma ampla superfície de ataque para problemas de Controle de Acesso em Nível de Objeto. Verificações de autorização em nível de objeto devem ser consideradas em todas as funções que acessam uma fonte de dados usando um ID do usuário.

Impactos:
O acesso não autorizado a objetos de outros usuários pode resultar na divulgação de dados a partes não autorizadas, perda de dados ou manipulação de dados.

Exemplo de caso:
Uma plataforma de e-commerce exibe lojas parceiras hospedadas. Ao inspecionar as requisições no navegador, um atacante identifica os endpoints da API e seu modelo. Usando outro endpoint, ele acessa toda a lista de lojas e, com um script simples, altera os nomes exibidos. Além disso, consegue acessar dados de vendas diretamente pela URL, explorando falhas de autorização e exposição indevida de dados.

Recomendações:
- Implementar um mecanismo de autorização adequado que se baseie nas políticas e hierarquia do usuário.
- Utilizar o mecanismo de autorização para verificar se o usuário logado tem acesso para realizar a ação solicitada no registro em cada função que usa uma entrada do cliente para acessar um registro no banco de dados.
- Preferir o uso de valores aleatórios e imprevisíveis como GUIDs para os IDs dos registros.
- Escrever testes para avaliar a vulnerabilidade do mecanismo de autorização. Não implementar alterações que façam os testes falharem.

2 - API2:2023 - Broken Authentication

Mecanismos de autenticação são frequentemente implementados incorretamente, permitindo que invasores comprometam tokens de autenticação ou explorem falhas de implementação para assumir a identidade de outros usuários, temporária ou permanentemente. Comprometer a capacidade de um sistema de identificar o cliente/usuário compromete a segurança geral da API.

Impactos:
Os atacantes podem obter controle total das contas de outros usuários no sistema, ler seus dados pessoais e realizar ações sensíveis em seu nome. É improvável que os sistemas consigam distinguir as ações dos atacantes das ações legítimas dos usuários.

Exemplo de caso:
Uma plataforma permite que usuários atualizem o e-mail da conta via API, sem exigir confirmação de identidade como a senha atual. Se um atacante obtiver o token de autenticação da vítima, ele pode alterar o e-mail cadastrado e iniciar o processo de redefinição de senha, assumindo o controle total da conta.

Recomendações:
- Certificar de conhecer todos os possíveis fluxos para autenticar-se na API.
- Utilizar padrões de autenticação, geração de tokens ou armazenamento de senhas.
- Exigir nova autenticação para operações sensíveis (por exemplo, alterar o endereço de e-mail do proprietário da conta).
- Onde possível, implementar autenticação multifator.
- Implementar mecanismos contra *bruteforce* para mitigar ataques de dicionário e ataques de força bruta em seus pontos finais de autenticação. Esse mecanismo deve ser mais rigoroso do que os mecanismos regulares de limitação de taxa em suas APIs.
- Implementar mecanismos de bloqueio de conta/*captcha* para prevenir ataques de força bruta contra usuários específicos. Implementar verificações de senhas fracas.
- Não usar as chaves de API para autenticação de usuários, mas sim para autenticação de clientes API.

3 - API3:2023 - Broken Object Property Level Authorization

Ausência ou a validação inadequada da autorização no nível da propriedade do objeto. Isso leva à exposição ou manipulação de informações por terceiros não autorizados.

Impactos:
O acesso não autorizado a propriedades de objetos privados pode resultar em divulgação de dados, perda de dados ou corrupção de dados. Em certas circunstâncias, o acesso não autorizado a propriedades de objetos pode levar à elevação de privilégios ou à tomada parcial/total de conta.

Exemplo de caso:
Em uma plataforma de aluguel, anfitriões podem aprovar reservas feitas por hóspedes. Um anfitrião malicioso percebe que ao enviar uma requisição legítima consegue incluir uma propriedade oculta com o valor total da estadia e alterá-lo sem ter permissão. Como a API não valida se ele pode modificar essa informação, o hóspede é cobrado indevidamente, evidenciando uma falha de autorização a nível de propriedade do objeto.

Recomendações:
- Ao expor um objeto usando API, sempre certificar de que o usuário tenha acesso às propriedades do objeto que você expõe.
- Evitar usar métodos genéricos como to_json() e to_string(). Em vez disso, selecionar especificamente as propriedades do objeto que deseja retornar.
- Se possível, evitar usar funções que automaticamente vinculam a entrada de um cliente a variáveis de código, objetos internos ou propriedades de objetos ("Atribuição em Massa").
- Permitir alterações apenas nas propriedades do objeto que devem ser atualizadas pelo cliente.
- Implementar um mecanismo de validação de resposta baseado em esquema como uma camada extra de segurança. Como parte desse mecanismo, definir e aplicar os dados retornados por todos os métodos da API.
- Manter as estruturas de dados retornadas ao mínimo necessário, de acordo com os requisitos funcionais e de negócios para o ponto de extremidade.

4 - API4:2023 - Unrestricted Resource Consumption

Atender solicitações de API consome recursos como largura de banda, CPU, memória e armazenamento. Serviços externos integrados via API, como envio de e-mails, SMS, chamadas ou validação biométrica, também geram custos por requisição. Ataques que exploram essas funcionalidades podem causar indisponibilidade do sistema ou aumentar significativamente os custos operacionais.

Impactos:
A exploração pode levar a um DoS devido à escassez de recursos, mas também pode resultar em aumento dos custos operacionais, como aqueles relacionados à infraestrutura, devido à maior demanda por CPU, aumentando as necessidades de armazenamento na nuvem, etc.

Exemplo de caso:
Uma plataforma de tradução oferece uma API que aceita textos de qualquer tamanho. Sem limites definidos, um usuário malicioso envia milhares de requisições com documentos extensos em paralelo. Como cada requisição consome processamento intensivo, os custos com infraestrutura aumentam drasticamente, evidenciando a falta de controle sobre o consumo de recursos.

Recomendações:

- Usar uma solução que facilita a limitação de memória, CPU, número de reinicializações, descritores de arquivos e processos, como Contêineres / código serverless (por exemplo, Lambdas).
- Definir um tamanho máximo de dados em todos os parâmetros e cargas úteis de entrada, como comprimento máximo para strings, número máximo de elementos em arrays e tamanho máximo de upload de arquivo (independentemente de estar armazenado localmente ou em armazenamento em nuvem).
- Implementar um limite sobre com que frequência um cliente pode interagir com a API dentro de um intervalo de tempo definido (limitação de taxa).
- Configurar limites de gastos para todos os fornecedores de serviços/integrations de API. Quando configurar limites de gastos não for possível, configurar alertas de cobrança em vez disso.

5 - API5:2023 - Broken Function Level Authorization	Políticas complexas de controle de acesso com diferentes hierarquias, grupos e funções, além de uma separação pouco clara entre funções administrativas e regulares, tendem a levar a falhas de autorização. Ao explorar esses problemas, invasores podem obter acesso aos recursos e/ou funções administrativas de outros usuários.

Impactos:
Essas falhas permitem que atacantes acessem funcionalidades não autorizadas. Funções administrativas são alvos-chave para esse tipo de ataque e podem levar à divulgação de dados, perda de dados ou corrupção de dados. No fim das contas, isso pode levar à interrupção do serviço.

Exemplo de caso:
Uma API contém um endpoint que deve ser exposto apenas aos administradores - GET /api/admin/v1/users/all. Este endpoint retorna os detalhes de todos os usuários do aplicativo e não implementa verificações de autorização em nível de função. Um invasor que aprendeu a estrutura da API faz um palpite e consegue acessar esse endpoint, o que expõe detalhes confidenciais dos usuários do aplicativo.

Recomendações:
- A aplicação deve ter um módulo de autorização consistente e fácil de analisar, que seja invocado de todas as suas funções de negócios. Os mecanismos de aplicação devem negar todo o acesso por padrão, exigindo concessões explícitas para funções específicas de acesso a cada função.
- Revisar seus endpoints de API em relação a falhas de autorização em nível de função, tendo em mente a lógica de negócios do aplicativo e a hierarquia de grupos.
- Certificar de que todos os seus controladores administrativos herdem de um controlador abstrato administrativo que implemente verificações de autorização com base no grupo/função do usuário.
- Certificar de que as funções administrativas dentro de um controlador regular implementem verificações de autorização com base no grupo e na função do usuário.

6 - API6:2023 - Unrestricted Access to Sensitive Business Flows	APIs vulneráveis a esse risco expõem um fluxo de negócios – como a compra de um ingresso ou a publicação de um comentário – sem compensar como a funcionalidade poderia prejudicar os negócios se usada de forma excessiva e automatizada. Isso não se deve necessariamente a bugs de implementação.

Impactos:
De modo geral, não se espera um impacto técnico. A exploração pode prejudicar o negócio de diferentes maneiras, por exemplo: impedir que usuários legítimos comprem um produto ou levar à inflação na economia interna de um jogo.

Exemplo de caso:
Uma companhia aérea permite cancelamentos gratuitos de passagens. Um usuário mal-intencionado reserva a maioria dos assentos de um voo e cancela tudo pouco antes da viagem, forçando a empresa a baixar os preços. Em seguida, ele compra uma passagem muito mais barata, explorando a falta de restrições no consumo de recursos da API.

Recomendações:
O plano de mitigação deve atuar em duas frentes: negócios, identificando fluxos críticos que podem ser explorados em excesso, e engenharia, aplicando mecanismos de proteção adequados. Entre as defesas estão:

- Impressão digital de dispositivos para bloquear clientes suspeitos.
- Usar CAPTCHA ou biometria para validar o acesso humano.
- Analisar o fluxo do usuário para detectar padrões não humanos (por exemplo, o usuário acessou as funções "adicionar ao carrinho" e "concluir compra" em menos de um segundo).
- Considerar bloquear endereços IP de nós de saída do Tor e proxies conhecidos.
- Proteger e limitar o acesso às APIs que são consumidas diretamente por máquinas (como APIs de desenvolvedor e B2B). Elas tendem a ser um alvo fácil para atacantes porque muitas vezes não implementam todos os mecanismos de proteção necessários

7 - API7:2023 - Server Side Request Forgery

Falhas de falsificação de solicitação do lado do servidor (SSRF) podem ocorrer quando uma API busca um recurso remoto sem validar o URI fornecido pelo usuário. Isso permite que um invasor force o aplicativo a enviar uma solicitação criada para um destino inesperado, mesmo quando protegido por um firewall ou VPN.

Impactos:
A exploração bem-sucedida pode levar à enumeração de serviços internos (por exemplo, varredura de portas), divulgação de informações, contorno de firewalls ou outros mecanismos de segurança. Em alguns casos, pode levar a um DoS ou o servidor ser usado como um proxy para esconder atividades maliciosas.

Exemplo de caso:
Uma plataforma de rede social permite que usuários atualizem suas fotos de perfil fornecendo uma URL de imagem. O servidor, ao buscar essa imagem, acaba acessando o endereço informado pelo usuário. Um invasor explora essa funcionalidade enviando URLs internas da própria infraestrutura da empresa, como serviços administrativos ou bancos de dados. Com isso, ele consegue obter informações sensíveis.

Recomendações:

- Isolar o mecanismo de recuperação de recursos na sua rede: geralmente, essas funcionalidades são destinadas a recuperar recursos remotos e não internos.
- Sempre que possível, usar listas de permissão de:
  - Origens remotas das quais os usuários devem baixar recursos (por exemplo, Google Drive, Gravatar, etc.).
  - Esquemas de URL e portas .
  - Tipos de mídia aceitos para uma determinada funcionalidade .
- Desabilitar redirecionamentos HTTP.
- Usar um parser de URL bem testado e mantido para evitar problemas causados por inconsistências na análise de URL.
- Validar e sanar todos os dados de entrada fornecidos pelo cliente.

8 - API8:2023 - Security Misconfiguration

As APIs e os sistemas que as suportam normalmente contêm configurações complexas, destinadas a torná-las mais personalizáveis. Engenheiros de software e DevOps podem ignorar essas configurações ou não seguir as práticas recomendadas de segurança em relação à configuração, abrindo caminho para diferentes tipos de ataques.

Impactos:
Problemas em configuração de segurança não apenas expõem dados sensíveis dos usuários, mas também detalhes do sistema que podem levar a uma comprometimento total do servidor.

Exemplo de caso:
Uma rede social oferece mensagens diretas entre usuários. Para buscar novas mensagens, o site faz a chamada GET /dm/user_updates.json?conversation_id=12345&cursor=GRlFp7. Como a resposta da API não inclui o HTTP Cache-Control, as conversas são armazenadas no cache do navegador. Um invasor com acesso ao dispositivo pode recuperá-las diretamente do sistema de arquivos.

Recomendações:
O ciclo de vida da API deve incluir:

- Projetar um processo *hardening* que leve a uma implantação rápida e fácil de um ambiente devidamente restrito.
- Criar uma tarefa para revisar e atualizar configurações em toda a pilha da API. A revisão deve incluir: arquivos de orquestração, componentes da API e serviços em nuvem.
- Criar um processo automatizado para avaliar continuamente a eficácia da configuração e das configurações em todos os ambientes.
- Garantir que todas as comunicações da API do cliente para o servidor da API e quaisquer componentes a montante/a jusante ocorram através de um canal de comunicação criptografado (TLS), independentemente de ser uma API interna ou voltada para o público.
- Definir e aplicar todos os esquemas de carga útil de resposta da API, incluindo respostas de erro, para evitar que rastreamentos de exceção e outras informações valiosas sejam enviadas de volta aos invasores.

9 - API9:2023 - Improper Inventory Management

As APIs tendem a expor mais endpoints do que os aplicativos web tradicionais, o que torna a documentação adequada e atualizada extremamente importante. Um inventário adequado de hosts e versões de API implantadas também é importante para mitigar problemas como versões de API obsoletas e endpoints de depuração expostos.

Impactos:
Os atacantes podem ter acesso a dados sensíveis ou até mesmo assumir o controle do servidor. Agentes de ameaça podem explorar endpoints obsoletos disponíveis em versões antigas da API para obter acesso a funções administrativas ou explorar vulnerabilidades conhecidas.

Exemplo de caso:
Foi implementado em um app um mecanismo de *rate limit* que impede invasores de usar força bruta para adivinhar tokens de redefinição de senha. Um pesquisador encontrou um host de API beta que executa a mesma API, incluindo o mecanismo de redefinição de senha, mas sem *rate limit*. O pesquisador conseguiu redefinir a senha de qualquer usuário usando força bruta simples para adivinhar o token de 6 dígitos.

Recomendações:
- Catalogar todos os hosts da API e documentar aspectos importantes de cada um deles, focando no ambiente da API (por exemplo, produção, preparação, teste, desenvolvimento), quem deve ter acesso à rede do host e a versão da API.
- Catalogar serviços integrados e documentar aspectos importantes como seu papel no sistema, quais dados são trocados (fluxo de dados) e sua sensibilidade.
- Documentar todos os aspectos da sua API, como autenticação, erros, redirecionamentos, limitação de taxa, política de compartilhamento de recursos de origem cruzada (CORS) e endpoints, incluindo seus parâmetros, solicitações e respostas
- Gerar documentação automaticamente adotando padrões abertos. Incluir a geração de documentação em seu pipeline de CI/CD.
- Disponibilize a documentação da API apenas para aqueles autorizados a usar a API.
- Utilize medidas de proteção externas, como soluções específicas de segurança para APIs, para todas as versões expostas das suas APIs, e não apenas para a versão de produção atual.

10 - API10:2023 - Unsafe Consumption of APIs

Os desenvolvedores tendem a confiar mais nos dados recebidos de APIs de terceiros do que nas informações fornecidas pelos usuários e, portanto, tendem a adotar padrões de segurança mais fracos. Para comprometer as APIs, os invasores buscam serviços de terceiros integrados em vez de tentar comprometer a API alvo diretamente.

Impactos:
O impacto varia de acordo com o que a API de destino faz com os dados extraídos. A exploração bem-sucedida pode levar à exposição de informações sensíveis a atores não autorizados, a muitos tipos de injeções ou à negação de serviço.

Exemplo de caso:
Uma API usava um serviço externo para enriquecer endereços comerciais enviados por usuários. Criminosos usam o serviço de terceiros para armazenar um *payload SQLi* associado a uma empresa criada por eles. Ao consultar esses dados, a API armazenava o conteúdo em um banco SQL vulnerável, executando o código malicioso e exfiltrando dados para servidores dos invasores.

Recomendações:
- Ao avaliar provedores de serviços, avalie sua postura de segurança de API.
- Assegurar de que todas as interações de API ocorram por meio de um canal de comunicação seguro (TLS).
- Validar e sanitizar corretamente os dados recebidos de APIs integradas antes de usá-los.
- Manter uma lista de permissões dos locais bem conhecidos para os quais as APIs integradas podem redirecionar a sua: não seguir redirecionamentos cegamente.

Boas Práticas em Segurança de API

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Ciclo de Vida de Desenvolvimento de Software Seguro (SSDLC)

FEBRABAN

Conceito

O Ciclo de Vida de Desenvolvimento de Software Seguro (SSDLC) é um processo que integra medidas de segurança em todas as fases do desenvolvimento de software. Essa abordagem envolve a **implementação de práticas de segurança** desde o início do desenvolvimento até a manutenção contínua, garantindo que a segurança seja uma parte integral do ciclo de vida do software.

Motivação

Adotar o SSDLC permite reduzir proativamente os riscos de vulnerabilidades, ao integrar a segurança desde o início do desenvolvimento. Isso fortalece a proteção das aplicações, evita retrabalho e melhora a conformidade com normas e regulamentações. Um estudo da IBM, sugere que corrigir um defeito de uma aplicação em produção é 100 vezes mais elevado que corrigi-lo na fase design. Dessa forma, a antecipação de ameaças e a cultura de segurança ajudam a construir softwares mais resilientes e confiáveis.

Implementação

A imagem a seguir representa as principais fases do SSDLC, destacando como práticas de segurança são integradas em cada etapa do desenvolvimento.

Ciclo de Vida de Desenvolvimento de Software Seguro (SSDLC)

FEBRABAN

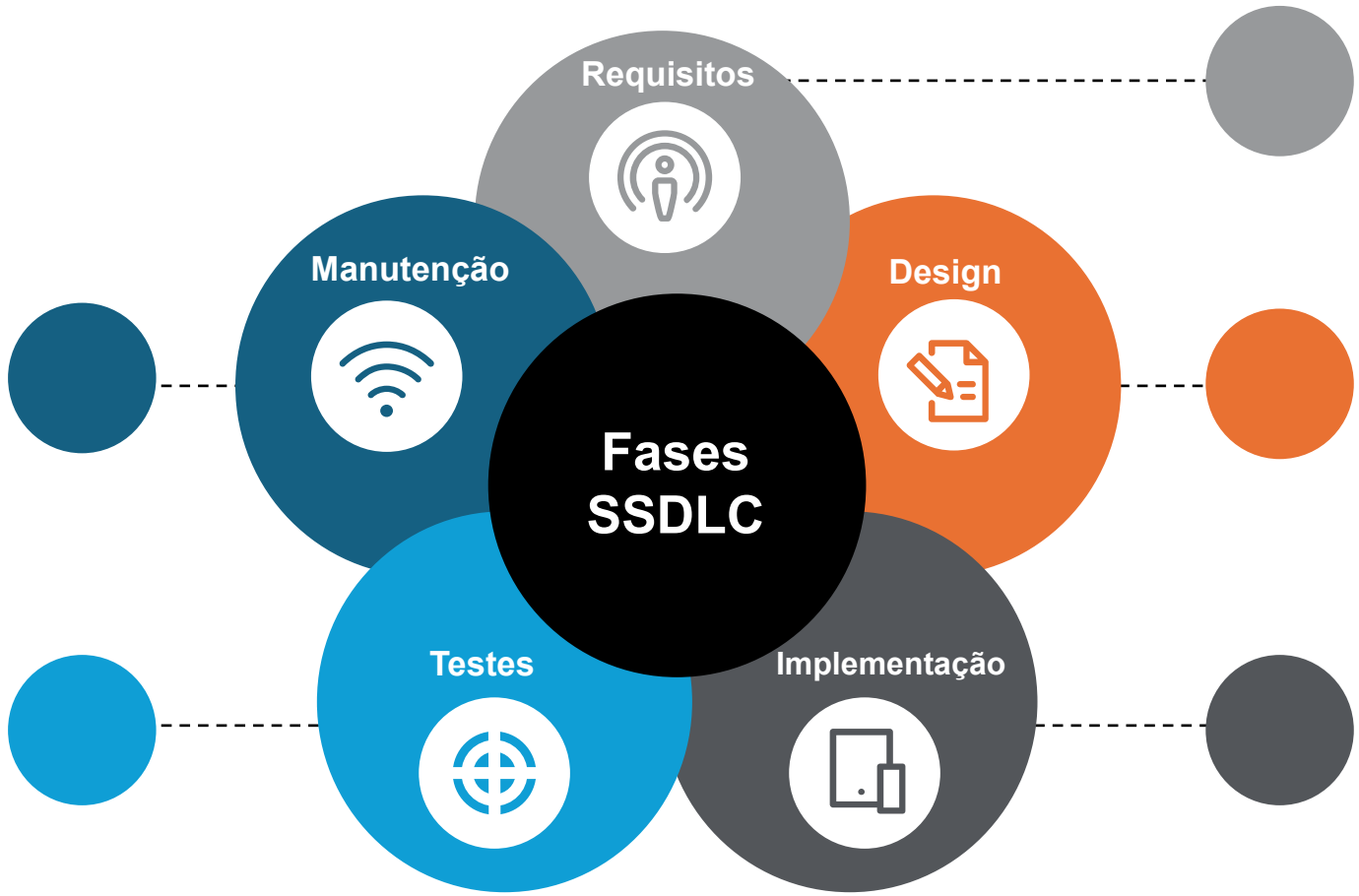
Risk Assessment
Identificar os requisitos de segurança.

Modelagem de Ameaças & Revisão de Design
Aplicar design seguro e modelagem de ameaças recorrentemente, entender as necessidades de arquitetura de software.

Desenvolvimento
Aplicar padrões seguros de codificação e atender aos requisitos de segurança identificados.

Testes de Segurança & Revisão de Código
Realizar testes de segurança com ferramentas automáticas, testes manuais e revisões de códigos.

Security Assessment & Configuração Segura
Aplicar práticas contínuas de segurança durante a manutenção da aplicação, após seu *deploy*.



Testes de Intrusão (Pentest)

Conceito

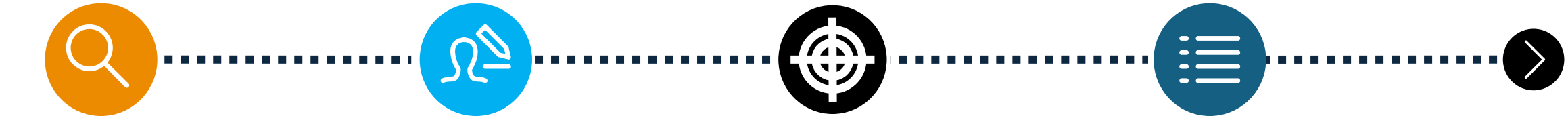
O pentest é uma prática de segurança ofensiva que simula ataques reais para identificar vulnerabilidades em sistemas, aplicações e redes. Seu objetivo é avaliar a eficácia dos controles de segurança e revelar falhas que poderiam ser exploradas por agentes maliciosos.

Motivação

Realizar pentests e outros exercícios de segurança ofensiva regularmente permite antecipar riscos, validar a robustez das defesas e garantir conformidade com normas de segurança. Essa abordagem proativa fortalece a postura de segurança da organização e mitiga o impacto de possíveis incidentes.

Implementação

Sua execução envolve definir escopo, utilizar técnicas manuais e automatizadas, explorar vulnerabilidades de forma controlada e documentar os achados, em linhas gerais é possível segmentar em 5 grandes fases, conforme ilustração abaixo. A execução geralmente é realizada pela equipe interna ou por consultorias especializadas. Além disso, os resultados deve orientar correções e melhorias contínuas nos sistemas avaliados.



Inventário de Software

Conceito

Inventário de software focado em APIs é o processo de identificar, catalogar e manter informações sobre todas as APIs utilizadas na organização. Isso inclui detalhes como endpoints, funcionalidades, proprietários e dependências, permitindo uma visão mais clara das interfaces que conectam sistemas e serviços.

Motivação

Manter um inventário de APIs contribui para agilizar operações, facilitar a manutenção dos sistemas e identificar dependências desatualizadas ou não utilizadas. Essa visibilidade permite decisões mais precisas sobre atualizações, correções e integrações, além de melhorar o controle sobre os ativos tecnológicos da organização.

Implementação

A implementação envolve listar e classificar os endpoints, avaliar riscos, identificar vulnerabilidades e monitorar alterações. As APIs devem ser incluídas nos processos de avaliação de riscos da organização, permitindo ajustes e melhorias contínuas com base nas informações coletadas.

Criptografia Forte

Conceito

Criptografia forte é o uso de algoritmos confiáveis e chaves de tamanho adequado para proteger dados em repouso e em trânsito. Em contextos de autenticação e autorização, ela garante que credenciais, tokens e permissões sejam transmitidos e armazenados de forma segura, evitando exposição indevida e manipulação de informações sensíveis.

Motivação

Adotar criptografia forte reduz riscos de interceptação, acesso não autorizado e manipulação de dados. A prática atende exigências regulatórias e melhora a segurança de credenciais e permissões em sistemas digitais.

Implementação

A implementação envolve o uso de protocolos como TLS para proteger a comunicação, algoritmos de hash seguros (como SHA-256) para armazenar senhas, e criptografia simétrica ou assimétrica para proteger tokens de acesso. É recomendável utilizar bibliotecas atualizadas, rotacionar chaves periodicamente e aplicar controles de acesso baseados em contexto. O uso de padrões como OAuth 2.0 e OpenID Connect, com tokens JWT assinados e criptografados, contribui para uma gestão segura e escalável de autenticação e autorização.

API Gateway

Conceito

API Gateway é um ponto de entrada centralizado que atua como intermediário entre clientes e serviços de backend. Ele recebe requisições, roteia para os serviços corretos, aplica políticas como autenticação e autorização, e retorna as respostas ao cliente, simplificando a comunicação em arquiteturas distribuídas.

Motivação

Utilizar API Gateway ajuda a reduzir a latência, aumentar a segurança e diminuir a complexidade da integração entre sistemas. Ele permite consolidar controles de acesso, monitoramento, limitação de taxa e gerenciamento de erros, contribuindo para maior desempenho e disponibilidade das aplicações.

Implementação

A implementação envolve configurar o gateway para autenticar usuários, autorizar acessos, aplicar políticas de tráfego, registrar logs e monitorar métricas. Pode ser realizado em ambientes locais, em nuvem ou híbridos, utilizando soluções como Kong, Apigee, AWS API Gateway ou NGINX, com suporte a protocolos seguros e integração com sistemas de identidade.

As API Gateways também possuem recursos de limitação de taxa, auxiliando na limitação e frequência com que um cliente pode enviar uma solicitação a um serviço em um determinado intervalo de tempo.

Monitoramento contínuo de APIs

Conceito

Monitoramento contínuo de APIs é o processo de observação em tempo real das chamadas, comportamentos e padrões de uso das interfaces de programação.

Motivação

Com APIs cada vez mais expostas e críticas para integrações, o monitoramento contínuo ajuda a detectar anomalias rapidamente, reduzir o tempo de resposta a incidentes e prevenir interrupções. Além disso, fornece dados valiosos para auditoria, análise de desempenho e melhoria contínua da segurança e disponibilidade dos serviços.

Implementação

A implementação envolve a coleta de métricas (latência, taxa de erro, volume de chamadas), análise de logs, rastreamento de requisições e geração de alertas em tempo real. Existem ferramentas no mercado que podem ser integradas aos gateways de API ou diretamente aos serviços, abaixo se encontra alguns exemplos de ferramentas. É recomendável definir limites de uso, configurar alertas para padrões suspeitos e manter dashboards atualizados para facilitar a resposta rápida a incidentes.

Casos Reais e Tendências

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Casos reais

A seguir, destacamos casos relevantes de violações envolvendo API:

Comprometimento na Uber (2016)

Em 2016, a Uber foi alvo de um ataque que comprometeu as informações pessoais de 57 milhões de usuários e motoristas. O ataque foi possível devido à má configuração de uma API privada da Uber, que expôs credenciais de acesso a um repositório na nuvem, permitindo que os invasores obtivessem acesso a dados armazenados.
O incidente foi agravado pelo fato de que a Uber não revelou a violação imediatamente. Em vez disso, a empresa tentou encobrir o ataque pagando aos hackers para deletarem os dados roubados.

- https://www.uber.com/en-CH/newsroom/2016-data-incident/

API da Equifax (2017)

Em 2017, a empresa sofreu um ataque cibernético que resultou no roubo de informações pessoais de 147 milhões de pessoas, incluindo números de Segurança Social, datas de nascimento, endereços e, em alguns casos, números de cartões de crédito.
A brecha foi explorada através de uma vulnerabilidade conhecida no Apache Struts, um framework de desenvolvimento de aplicativos web usado pela Equifax em uma de suas APIs.

- https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf

Facebook e a Cambridge Analytica (2018)

O incidente expôs as falhas de segurança e privacidade na API do Facebook, que permitiu a coleta massiva de dados pessoais de cerca de 87 milhões de usuários. A API permitia que desenvolvedores de aplicativos acessassem informações não apenas dos usuários que consentiam em usar seus aplicativos, mas também dos amigos desses usuários, sem que eles estivessem cientes disso.

- https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Tendência de ataques

Segundo o relatório **State of the Internet Reports (2025) da Akamai**, foi compartilhado no tópico de **State of Apps and API Security 2025: How AI Is Shifting the Digital Terrain** a grande preocupação e urgência com a Segurança e proteção de APIs, visto que estas tem se tornado um alvo crescente de ataques.

De acordo com o estudo realizado pela Akamai em 2024, apenas 13% das instituições entrevistadas testavam suas APIs diariamente, o que representa uma queda de 37% desde 2023, números alarmantes diante do cenário atual.

É apontado que a rápida adoção de aplicações com inteligência artificial (IA) tem ampliado as superfícies de ataque digitais, sendo as APIs os principais alvos, com 150 bilhões de ataques registrados pela empresa entre janeiro de 2023 e dezembro de 2024.

O relatório mostra que APIs baseadas em Inteligência Artificial, muitas vezes com autenticação inadequada e acessos externos abertos, são ainda mais vulneráveis que as tradicionais, já que os cibercriminosos também têm se beneficiado de tecnologias baseadas em IA para automatizar ataques e contornar barreiras de segurança.
Além disso, a instituição também aponta um aumento significativo nos ataques de DDoS (negação de serviço distribuída) da camada 7 (camada de aplicação) contra aplicações Web e APIs. O volume mensal de ataques passou de pouco mais de 500 bilhões no início de 2023 para mais de 1,1 trilhão em dezembro de 2024 – um aumento de 94%.

https://www.akamai.com/lp/soti/app-api-ai-security-report-2025

https://www.akamai.com/resources/state-of-the-internet/app-api-ai-security-report-2025

Tendência de ataques

Estratégias de ataque em API baseadas em IA

Target estratégico:
Hackers usam IA para mapear APIs e gerar ataques personalizados com código malicioso. Isso exige segurança reforçada e monitoramento constante.

Ataques Volumétricos:
Invasores usam IA para gerar tráfego excessivo e sobrecarregar sistemas, comprometendo a disponibilidade de serviços. Bots automatizados são empregados em ataques DDoS, que simulam acessos em massa para derrubar aplicações e redes.

Ataques Automatizados:
Com o apoio de IA, invasores conseguem automatizar ataques usando bots, reduzindo esforço humano e aumentando a eficiência das ações maliciosas.

Ataques baseados em comportamento:
IA utilizada para analisar padrões de tráfego e comportamento visando criar ataques lentos e discretos, quase que imperceptíveis, sem acionar alarmes.

https://www.akamai.com/resources/state-of-the-internet/app-api-ai-security-report-2025

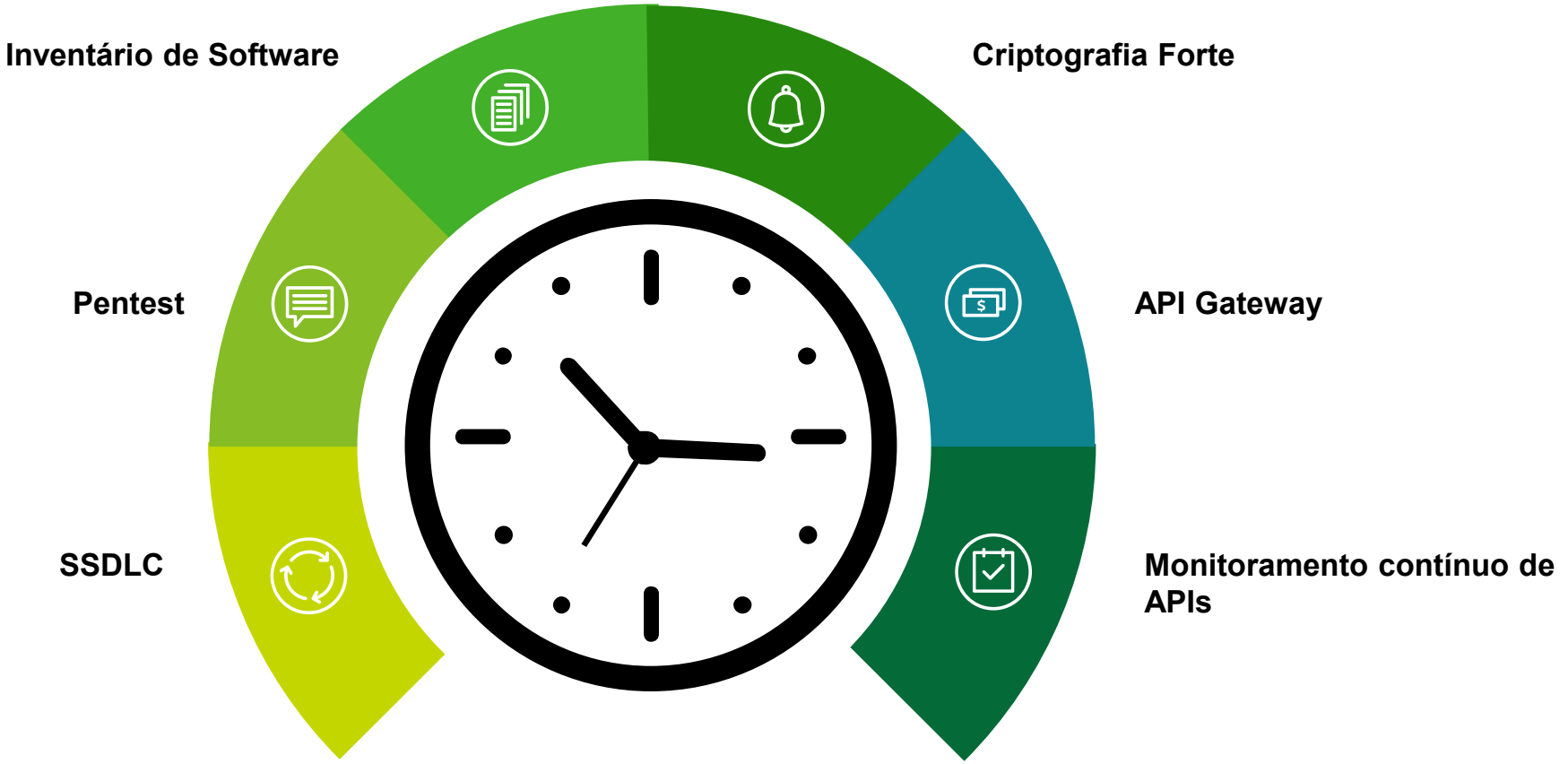
Conclusão

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Conclusão

Ao implementar proteções proativas e em tempo real de APIs, é possível minimizar os riscos de se tornarem alvos vulneráveis de ataques cibernéticos, como parte da proteção de funções.

Relembrando as Boas Práticas em Segurança de API:



Módulo: Zero Trust

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Requisitos – Proteção Zero Trust

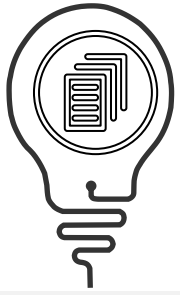
Este material foi elaborado com base nas diretrizes da OWASP, bem como foram considerados os requisitos de segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

CIS Controls

Controles

- **Controle 1**: Inventário e controle de ativos empresariais
- **Controle 2**: Inventário e controle de ativos de software
- **Controle 3**: Proteção de dados
- **Controle 6**: Gestão de controle de acesso
- **Controle 12:** Gerenciamento de infraestrutura de rede
- **Controle 13:** Monitoramento e defesa de rede
- **Controle 14:** Treinamento de habilidades e conscientização em segurança

PCI DSS



Requisitos

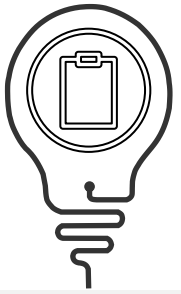
- **Requisito 1**: Implementar e manter controles de segurança de rede
- **Requisito 6**: Desenvolver e manter sistemas e softwares seguros
- **Requisito 3**: Proteger dados de conta armazenados
- **Requisito 8**: Identificar os usuários e autenticar o acesso aos componentes do sistema
- **Requisito 11**: Testar regularmente a segurança de sistemas e redes
- **Requisito 12**: Políticas de Segurança da Informação e Treinamentos

ISO 27002:2022

Controles

- **5.9** Inventário de ativos de informação
- **5.12** Classificação da informação
- **5.15** Controle de acesso (menor privilégio)
- **5.16** Gestão de identidades e credenciais
- **5.18** Acesso a informações e funções
- **8.8** Gestão de vulnerabilidades técnicas
- **8.16** Monitoramento de atividades
- **8.20** Controles de segurança de rede
- **8.22** Segregação de redes
- **8.24** Uso de criptografia
- **8.25** Segurança em ambientes de desenvolvimento e teste
- **8.29** Testes de segurança de aplicações
- **8.31** Separação entre ambientes de desenvolvimento, teste e produção

NIST CSF



Subcategorias

- **GV.PO**: Política de segurança cibernética
- **ID.AM-02**: Inventários de software, serviços e sistemas gerenciados pela organização
- **PR.AA-01**: Identidades e credenciais de usuários, serviços e dispositivos autorizados
- **PR.AA-05**: Princípios de privilégio mínimo e separação de funções
- **PR.AA-02**: As identidades são comprovadas e vinculadas às credenciais com base no contexto das interações
- **PR.DS**: Confidencialidade, integridade e disponibilidade dos dados
- **PR.IR-01**: Ambientes são protegidos contra acesso lógico e uso não autorizado
- **PR.PS-01**: As práticas de gerenciamento de configuração são aplicadas
- **DE.CM-01**: Monitoramento contínuo de redes
- **DE.AE-02**: Eventos são analisados para melhor compreensão das atividades

Sumário

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Sumário

Contextualização

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Modelo Zero Trust

O Zero Trust é um modelo moderno de segurança cibernética baseado no princípio de que nenhuma entidade seja usuário, dispositivo, aplicação ou rede deve ser considerada confiável por padrão.

Diferente das abordagens tradicionais, que protegiam um perímetro definido e permitiam acesso livre a tudo que estivesse dentro dele, o Zero Trust entende que o perímetro não existe mais. Hoje, dados, usuários e aplicações estão distribuídos entre ambientes locais, nuvem, dispositivos móveis e serviços de terceiros, o que exige uma postura de segurança contínua e adaptativa.

O objetivo do Zero Trust é claro: **proteger os dados e serviços críticos em um cenário onde a confiança não pode ser assumida**. Ele serve tanto para aumentar a resiliência contra ataques externos, como ransomware e invasões direcionadas, quanto para mitigar riscos internos, como abuso de credenciais ou acessos indevidos. Além disso, seu uso facilita a conformidade com normas e regulamentações de segurança, como NIST, PCI DSS, ISO 27001 & 27002 e legislações de privacidade de dados.

Em um ambiente onde transações ocorrem em milissegundos, dados sensíveis circulam entre múltiplos sistemas e a superfície de ataque cresce aceleradamente, confiar por padrão é um risco que nenhuma instituição pode assumir. O modelo Zero Trust surge como resposta direta a essa nova realidade, onde o acesso deve ser conquistado, não concedido automaticamente.

Fundamentos do Zero Trust

O modelo Zero Trust vai além da tecnologia, é uma filosofia de segurança que redefine como protegemos dados e acessos. No setor financeiro, ele é essencial para garantir a integridade das informações dos clientes frente às ameaças cibernéticas modernas. Para entender como essa filosofia se aplica na prática, podemos destacar **três princípios fundamentais**:

Verificação Contínua

Todo acesso a dados ou sistemas, mesmo se for de dentro da rede, é tratado como uma nova solicitação. O sistema verifica continuamente a identidade e o contexto do acesso antes de conceder permissão.

Menor Privilégio

Usuários e sistemas recebem apenas o mínimo de acesso necessário para realizar suas tarefas. Isso restringe o movimento de possíveis ataques dentro da rede e ajuda a proteger informações sensíveis.

Microssegmentação

A rede é dividida em pequenas "bolhas" (microssegmentos). Se uma dessas bolhas for comprometida, o ataque não se espalha facilmente para outras partes da rede, contendo o risco.

Lacunas de segurança

A confiança implícita nos modelos tradicionais de segurança pode abrir brechas nos sistemas. Sem Zero Trust, a rede fica mais suscetível a ameaças que podem comprometer dados, operações e conformidade regulatória. São exemplos de lacunas:

Acesso interno indevido

Um modelo de segurança tradicional presume que os usuários e dispositivos dentro da rede são confiáveis. Um funcionário mal-intencionado poderia se mover pela rede, acessando dados confidenciais e sistemas críticos sem grandes barreiras.

Propagação de ransomware

Em uma rede sem microssegmentação, um único dispositivo infectado pode se tornar um ponto de entrada para um ataque de ransomware que se espalha rapidamente por toda a rede, criptografando arquivos e paralisando operações. O Zero Trust, com sua segmentação, isolaria o ataque, minimizando os danos

Movimentação lateral de atacantes

Se um atacante consegue penetrar no perímetro da rede, ele poderia explorar a confiança implícita para se mover lateralmente (de um sistema para outro) e escalar seus privilégios até alcançar os dados mais valiosos. Um modelo Zero Trust previne esse tipo de movimento, exigindo verificação contínua em cada ponto de acesso.

Não conformidade com regulamentações

Sem visibilidade e controle robusto, torna-se difícil atender exigências como a LGPD, pode levar a falhas de conformidade e colocando a instituição em risco legal.

Aplicabilidade do Modelo Zero Trust

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

Aplicabilidade Zero Trust - Identidade e Acesso

Identidade e Acesso

No modelo Zero Trust, o acesso de identidade é o pilar fundamental de segurança da informação.
Em vez de confiar em um perímetro de rede, a identidade se torna o novo perímetro. Isso significa que a segurança não se baseia em **onde** o usuário está (dentro ou fora da rede), mas sim em **quem** ele é.

Objetivo:
Tornar o acesso não autorizado por meio de credenciais roubadas ou vazadas (como senhas) significativamente mais difícil.

Impedir que contas de alto valor, como as de administradores, sejam comprometidas, já que um único fator não é suficiente para o acesso.

Exemplo de caso:
Uma instituição financeira sofreu um ataque de phishing que resultou no roubo das credenciais de um administrador de rede. Sem o MFA, o atacante teria acesso irrestrito a sistemas críticos.

Com o MFA implementado, a tentativa de login do atacante foi bloqueada, pois ele não possuía o segundo fator de autenticação, salvando a instituição de uma possível invasão massiva.

Recomendações:

- Implementar o MFA para todos os usuários, incluindo administradores e fornecedores externos. E escolher métodos de MFA robustos, como aplicativos de autenticação ou chaves de segurança. Evite o uso de SMS, pois essa tecnologia pode ser mais vulnerável.
- Revisar e ajustar regularmente as permissões de acesso dos funcionários.
- Automatizar a remoção de privilégios quando um funcionário muda de cargo ou deixa a empresa.
- Adotar uma ferramenta de Gerenciamento de Acesso Privilegiado (PAM) para automatizar o processo de solicitação e revogação.
- Definir políticas claras sobre o tempo máximo de concessão de privilégios.
- Configurar a expiração de sessões de inatividade para um tempo curto e razoável.
- Exigir a reautenticação para ações críticas, como transferências de grandes valores ou mudanças de dados pessoais.

Aplicabilidade Zero Trust - Inventário Atualizado de Dispositivos

FEBRABAN

Inventário Atualizado de Dispositivos

Não se pode proteger o que não se conhece. Por isso, o inventário de dispositivos é uma etapa necessária para garantir visibilidade e controle sobre todos os ativos conectados à rede sejam eles corporativos, pessoais ou de terceiros.

Objetivo:
Garantir que apenas os dispositivos autorizados (sejam eles da empresa ou pessoais, no modelo BYOD) tenham acesso à rede e sistemas. Isso reduz a superfície de ataque, pois impede que dispositivos desconhecidos ou não auditados se conectem e potencialmente introduzam malware ou outras ameaças.

Exemplo de caso:
Uma instituição com uma política BYOD permite que funcionários usem seus notebooks pessoais. Um novo funcionário tenta se conectar à rede corporativa com seu laptop pessoal, mas o dispositivo não está registrado no inventário. O sistema de segurança, seguindo a política Zero Trust, bloqueia a conexão automaticamente. Esse bloqueio evita que um dispositivo não verificado acesse dados sensíveis, protegendo a rede de roubo de dados.

Recomendações:

- Implementar um sistema de inventário automatizado que registre e monitore todos os dispositivos.
- Criar políticas claras e auditáveis para o uso de dispositivos pessoais (BYOD), definindo requisitos de segurança mínimos antes do acesso.
- Realizar auditorias regulares para garantir que o inventário esteja sempre atualizado e que não existam dispositivos não autorizados na rede.
- Utilizar ferramentas de Network Access Control (NAC) ou MDM (Mobile Device Management) que validem a postura do dispositivo antes de permitir qualquer acesso.
- Definir um conjunto de requisitos de segurança (linha de base) que todos os dispositivos devem atender.
- Integrar as ferramentas de detecção (EDR) com as ferramentas de controle de acesso (NAC/MDM) para uma resposta automatizada e instantânea.
- Ter um plano de resposta a incidentes claro, que inclua a quarentena imediata de dispositivos, permitindo uma ação rápida quando uma ameaça for detectada.

Aplicabilidade Zero Trust - Redes de Comunicação

Redes de Comunicação

No modelo de segurança tradicional, a rede é vista como um castelo com um fosso. Uma vez que o invasor atravessa o perímetro, ele tem liberdade para se mover. O Zero Trust derruba essa ideia, tratando a rede como um ambiente hostil onde cada comunicação precisa ser verificada.

Objetivo:
A microssegmentação divide a rede em zonas menores e isoladas, o que impede que uma ameaça se espalhe rapidamente. Se um invasor conseguir comprometer um sistema, ele ficará confinado àquele segmento, sem poder se mover lateralmente para acessar dados críticos ou infectar outros sistemas.

Exemplo de caso:
Um hacker consegue invadir um servidor de baixo valor em um data center. Usando esse ponto de entrada, ele começa a escanear a rede interna para encontrar outros servidores vulneráveis. A ferramenta de inspeção de tráfego detecta esse comportamento e notifica a equipe de segurança, que isola o servidor imediatamente. Sem essa inspeção, o hacker poderia ter continuado o ataque e comprometido toda a rede.

Recomendações:

- Mapear todas as aplicações e dependências para entender o fluxo de dados e separar os workloads.
- Usar firewalls de última geração ou software-defined networking (SDN) para criar segmentos lógicos e impor políticas rigorosas de tráfego entre eles.
- Revisar as políticas de microssegmentação continuamente para garantir que os limites de segurança estejam sempre atualizados.
- Utilizar um sistema de gerenciamento de acesso que integre dados de identidade, dispositivos e contexto.
- Automatizar as respostas para que, em caso de violação de política, o acesso seja imediatamente restrito ou bloqueado.
- Instalar soluções de inspeção e monitoramento de tráfego dentro da sua rede, em vez de apenas no perímetro.
- Utilizar ferramentas de análise de comportamento de rede que identifiquem atividades anômalas.
- Avaliar a substituição de VPNs por soluções ZTNA, especialmente para acesso de funcionários remotos e terceiros.
- Configurar a ZTNA para garantir que o acesso seja concedido com base em políticas de menor privilégio.

Aplicabilidade Zero Trust - Aplicações e Dados

FEBRABAN

Aplicações e Dados

No modelo de segurança Zero Trust, a proteção mais importante é aquela que foca nos dados e nas aplicações. Afinal, a informação é o ativo mais valioso de uma empresa. A lógica é simples: se o dado está protegido, o negócio está seguro, não importa onde o acesso aconteça.

Objetivo:
As políticas de acesso baseadas em sensibilidade protegem diretamente os dados, ajustando permissões dado o tipo de informação e o contexto do acesso, como quem está acessando, de onde e com qual dispositivo. Isso ajuda a evitar que dados confidenciais sejam acessados ou transferidos para dispositivos não confiáveis.

Exemplo de caso:
Uma funcionária do setor de crédito precisa acessar um relatório com dados de clientes. O sistema Zero Trust permite que ela visualize o documento no navegador do seu notebook corporativo. No entanto, ao tentar fazer o download do relatório para um pendrive ou um serviço de armazenamento pessoal, o sistema bloqueia a ação, impedindo a exfiltração de dados sensíveis para um ambiente não seguro.

Recomendações:

- Criar uma matriz clara de classificação de dados para todos os tipos de informação da organização.
- Utilizar ferramentas de automação para identificar e classificar dados, especialmente em grande escala.
- Integrar a classificação de dados com o sistema de controle de acesso.
- Implementar regras que restrinjam ações como download, impressão ou cópia de dados sensíveis para dispositivos não verificados.
- Revisar e atualizar as políticas de acesso regularmente, com base em novos riscos e mudanças de comportamento dos usuários.
- Registrar todas as atividades de acesso, incluindo quem, o quê, quando e de onde.
- Utilizar ferramentas de SIEM ou UEBA (User and Entity Behavior Analytics) para analisar os dados e identificar comportamentos anômalos.
- Automatizar o processo de alerta para garantir que a equipe de segurança seja notificada instantaneamente em caso de atividade suspeita.
- Implementar uma solução de DLP integrada aos sistemas de e-mail, web e armazenamento de arquivos.

Aplicabilidade Zero Trust - Governança e Cultura

FEBRABAN

Governança e Cultura

A tecnologia é apenas metade da equação para o sucesso do Zero Trust. A outra metade, e talvez a mais crucial, é a Cultura. Sem políticas claras, treinamento contínuo e processos de revisão, a arquitetura de segurança, por mais robusta que seja, terá falhas. A governança garante que o modelo Zero Trust seja sustentável e a cultura faz com que a segurança seja uma responsabilidade de todos.

Objetivo:
Ter em sua organização políticas claras de Zero Trust é o alicerce de toda a sua estratégia. Essas políticas definem as regras, as expectativas e as responsabilidades para todos os usuários, sejam eles funcionários, fornecedores ou parceiros.

Exemplo de caso:
Uma instituição financeira estabeleceu uma política clara de Zero Trust que exige que todos os fornecedores externos passem por uma avaliação de segurança e usem MFA. Um novo parceiro tenta acessar o sistema com credenciais básicas, mas o acesso é negado. A política protegeu a rede de um parceiro potencialmente vulnerável e garantiu que o acesso só fosse concedido após o cumprimento de todos os requisitos de segurança.

Recomendações:

- Elaborar e documentar as políticas de Zero Trust de forma clara e acessível para todos os públicos.
- Obter o apoio da alta gerência para as políticas, garantindo que a segurança seja uma prioridade em toda a organização.
- Comunicar as políticas regularmente a todos os stakeholders, incluindo contratados e fornecedores, e incluí-las em contratos e acordos.
- Implementar um programa de treinamento de segurança obrigatório e contínuo.
- Realizar simulações de phishing regulares para testar a conscientização dos funcionários.
- Manter o treinamento relevante e envolvente, abordando as ameaças mais recentes.
- Estabelecer um cronograma fixo para revisões de acesso (por exemplo, trimestral ou semestral).
- Automatizar o processo de revisão de acesso sempre que possível.
- Exigir que os gerentes de equipe validem e aprovem os acessos de seus subordinados durante as revisões.

Aplicabilidade Zero Trust - Monitoramento e Automação

Monitoramento e Automação

Em um ambiente Zero Trust, o monitoramento e a automação **são o motor que impulsiona a segurança**. Eles garantem que as políticas de confiança não sejam estáticas, mas sim um ciclo contínuo de avaliação e resposta. Sem visibilidade e automação, o modelo Zero Trust seria ineficaz contra ameaças em constante evolução.

Objetivo:
A Resposta Automatizada a Incidentes (SOAR) permite reagir rapidamente a ataques cibernéticos. Ela automatiza ações com base em alertas de ferramentas como SIEM e UEBA, respondendo em tempo real sem depender da intervenção humana. Assim, a equipe de segurança pode focar em ameaças mais complexas.

Exemplo de caso:
A conta de um analista de um banco é usada para tentar fazer login em um servidor de produção às 3 da manhã, algo que nunca aconteceu antes. O SIEM registra a tentativa de login, e o UEBA, ao analisar o histórico do usuário, marca o comportamento como "anômalo". Imediatamente, o sistema emite um alerta de alto risco para a equipe de segurança, indicando uma provável conta comprometida.

Recomendações:

- Investir em uma solução SIEM com recursos de UEBA nativos para uma análise de comportamento mais profunda.
- Definir linhas de base de comportamento “normal” para usuários e dispositivos.
- Treinar as equipes de segurança para interpretar os alertas e investigar os incidentes de forma eficiente.
- Mapear os fluxos de trabalho de resposta a incidentes e automatizá-los com uma solução SOAR.
- Testar os “playbooks” de automação regularmente para garantir que funcionem corretamente.
- Integrar as ferramentas de segurança de detecção com as de resposta para uma comunicação fluida.
- Utilizar a inteligência de ameaças para enriquecer os dados do SIEM, permitindo uma análise mais profunda de atividades suspeitas.
- Implementar uma plataforma de acesso que utilize um motor de risco para pontuar cada sessão.
- Definir gatilhos para reautenticação baseados em mudanças de comportamento, localização ou postura do dispositivo.

Tendências

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

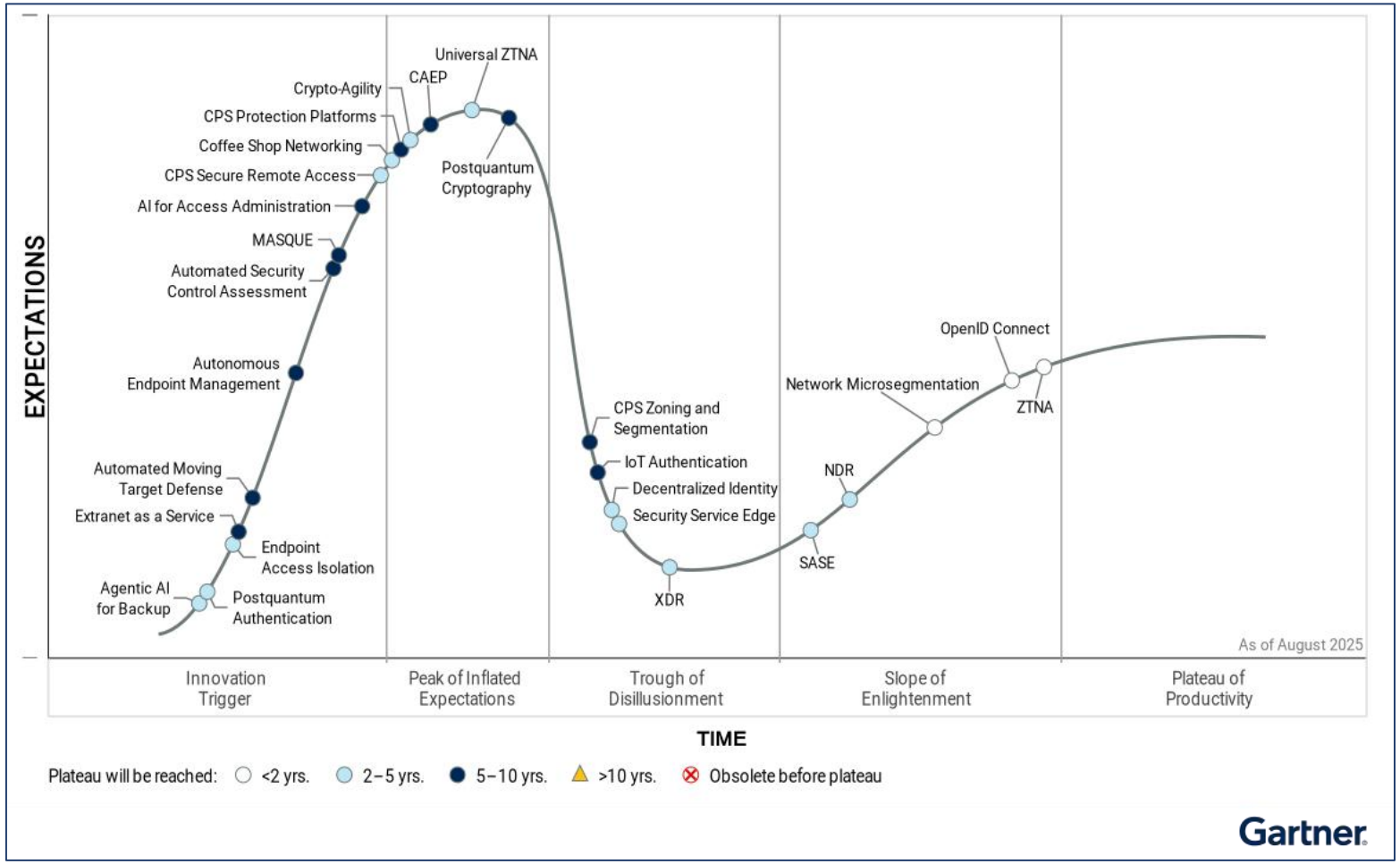
Tendências – Ciclo de Hype

O Zero Trust evoluiu rapidamente de um conceito de segurança de nicho para uma estratégia essencial para organizações que operam em ambientes complexos e distribuídos.

Embora tecnologias centradas em rede — como o acesso à rede de confiança zero (ZTNA), microssegmentação e detecção e resposta de rede (NDR) — continuem sendo pilares importantes, elas estão atingindo a maturidade e devem alcançar o estágio de produtividade nos próximos dois anos.

A seguir, vemos a figura criada pelo Gartner representando o ciclo do Hype envolvendo tecnologias Zero Trust:

Figura 1: Ciclo de Hype envolvendo tecnologias Zero Trust (2025)



Fonte: Hype Cycle for Zero-Trust Technology, 2025 - Gartner

Tendências – Matriz de Prioridade

A Matriz de Prioridade é uma ferramenta estratégica que ajuda líderes a tomar decisões mais conscientes sobre investimentos em tecnologia. Ela esclarece as compensações entre iniciativas de alto impacto e longo prazo e oportunidades de curto prazo, permitindo um planejamento mais equilibrado e alinhado com os objetivos da organização.

Ao relacionar os benefícios potenciais das inovações com sua posição no Ciclo do Hype, essa matriz funciona como um guia para definir onde e quando investir.

Nos próximos dois anos, espera-se que tecnologias como OpenID e microssegmentação de rede se consolidem como práticas comuns, contribuindo para uma experiência de usuário mais fluida e para o fortalecimento das defesas de segurança.

Tabela 1: Matriz de Prioridade envolvendo tecnologias Zero Trust (2025)

Benefit	**Years to Mainstream Adoption**		
	Less Than 2 Years	2 to 5 Years	5 to 10 Years
Transformational		Decentralized Identity SASE	
High	Network Microsegmentation OpenID Connect	Agentic AI for Backup CPS Secure Remote Access Crypto-Agility Postquantum Authentication Security Service Edge Universal ZTNA	AI for Access Administration Autonomous Endpoint Management CAEP CPS Protection Platforms CPS Zoning and Segmentation IoT Authentication Postquantum Cryptography
Moderate	ZTNA	Coffee Shop Networking Endpoint Access Isolation NDR XDR	Automated Moving Target Defense Automated Security Control Assessment
Low			Extranet as a Service MASQUE

Fonte: Hype Cycle for Zero-Trust Technology, 2025 - Gartner

Tendências

Segundo relatório do Gartner até 2027, **40% das grandes organizações** com ZTNA de acesso remoto **estenderão a aplicação** independente de localização, substituindo tecnologias legadas para simplificar as políticas de acesso e reduzir as superfícies de ataque — **acima dos menos de 10% em 2024.**

- Espera-se que o ZTNA universal alcance uma adoção generalizada — ou seja, mais de 40% — até 2027. As organizações precisam analisar fornecedores que evoluíram para oferecer uma abordagem unificada, independentemente da localização física do usuário ou dispositivo — incluindo ambientes locais, abrangendo TI e CPS (tecnologia operacional [TO] e Internet das Coisas [IoT]).

- Existem arquiteturas de Zero Trust que não são ideais para acesso seguro, com implementações complexas que não conseguem satisfazer os requisitos dinâmicos em evolução em uma arquitetura híbrida.

- Os invasores buscarão maneiras de explorar modelos de implantação complexos, ignorando as arquiteturas de Zero Trust existentes para penetrar no serviço de ataque em expansão.

Fonte: Hype Cycle for Zero-Trust Technology, 2025 - Gartner

Conclusão

À medida que as ameaças cibernéticas se tornam mais sofisticadas, as medidas de segurança estáticas se mostram cada vez mais inadequadas, levando as organizações a adotar estratégias de segurança mais adaptáveis e responsivas.

O modelo de Zero Trust se baseia na premissa de que o sistema deve "nunca confiar, sempre verificar". Ele exige a verificação contínua de identidades e direitos de acesso, alinhando-se à necessidade de controles de acesso dinâmicos e baseados em risco, que possam se ajustar em tempo real com base no ambiente de ameaças atual e no comportamento do usuário ou dispositivo.

O aumento do trabalho remoto e da força de trabalho estendida, incluindo contratados e fornecedores terceirizados, expandiu a superfície de ataque, exigindo medidas de segurança mais robustas para gerenciar o acesso e proteger dados confidenciais em ambientes diversos e distribuídos.

Diante desse cenário, a adoção do modelo Zero Trust não é apenas uma tendência, mas uma necessidade estratégica para garantir a resiliência cibernética das organizações no futuro digital

Módulo: Gerenciamento de Acesso Privilegiado (PAM)

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

506

Requisitos – Gerenciamento de Acesso Privilegiado

FEBRABAN

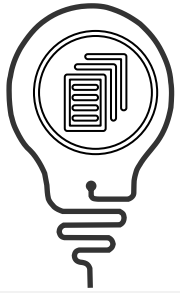
Este material foi elaborado com base nas diretrizes da OWASP, bem como foram considerados os requisitos de segurança da informação relacionados ao tema de acordo com as normas e frameworks apresentado abaixo:

CIS Controls

Controles

- **Controle 5**: Gestão de contas
- **Controle 6**: Gestão de controle de acesso
- **Controle 8:** Gerenciamento de registros e auditoria
- **Controle 13:** Monitoramento e defesa de rede
- **Controle 16:** Segurança de Software

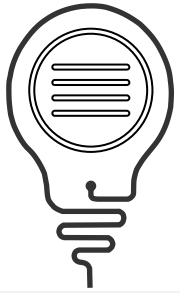
PCI DSS



Requisitos

- **Requisito 7**: Restringir o acesso aos dados do titular do cartão
- **Requisito 8**: Identificar os usuários e autenticar o acesso aos componentes do sistema
- **Requisito 10**: Registrar e monitorar os acessos aos sistemas e dados
- **Requisito 12**: Manter políticas de Segurança da Informação

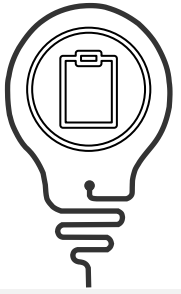
ISO 27002:2022



Controles

- **5.15** Controle de acesso
- **5.16** Gestão de identidades
- **5.17** Informações de autenticação
- **5.18** Direitos de acesso
- **8.2** Direito de acesso privilegiado
- **8.5** Autenticação segura
- **8.15** Registro (Logging)
- **8.16** Monitoramento de atividades
- **8.22** Segregação de redes

NIST CSF



Subcategorias

- **PR.AA-01**: Identidades e credenciais de usuários, serviços e dispositivos autorizados
- **PR.AA-02**: As identidades são comprovadas e vinculadas às credenciais com base no contexto das interações
- **PR.AA-05**: Princípios de privilégio mínimo e separação de funções
- **PR.IR-01**: Ambientes são protegidos contra acesso lógico e uso não autorizado
- **PR.PS-04**: Os logs são gerados e disponibilizados para monitoramento contínuo
- **DE.CM-01**: Monitoramento contínuo de redes

Sumário

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

508

Sumário

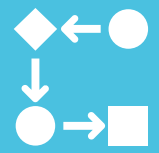
Introdução

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

510

Gerenciamento de Acesso Privilegiado (PAM)

Gerenciamento de Acesso Privilegiado (*Privileged Access Management* - PAM) é um conjunto de práticas, processos e tecnologias voltadas para **controlar, monitorar e proteger contas com privilégios elevados dentro de uma organização**. Essas contas, como administradores de sistemas, bancos de dados ou aplicações críticas, **possuem permissões que podem causar impactos significativos** em caso de uso indevido ou comprometimento.



Funcionamento

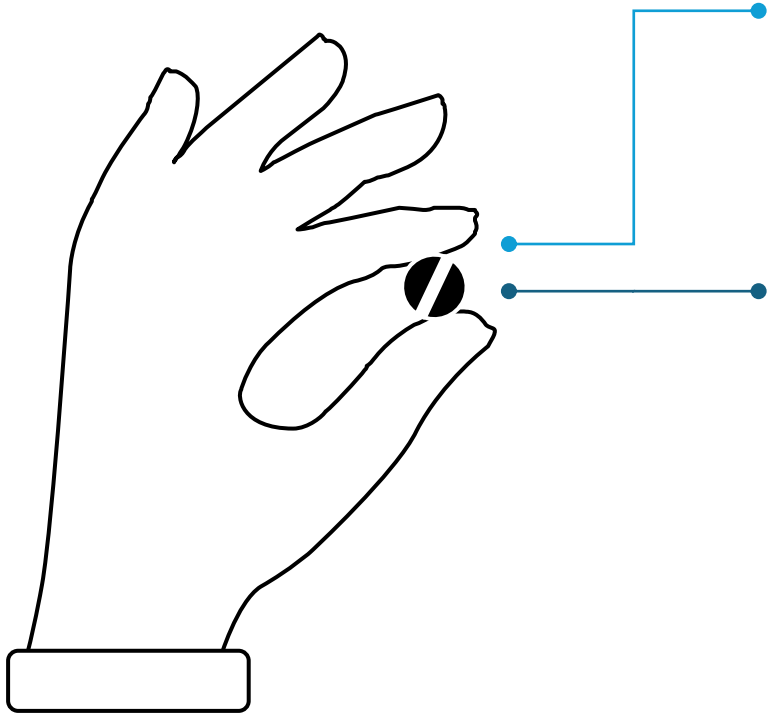
O PAM envolve a **aplicação de controles** como autenticação forte, gestão de senhas privilegiadas, segregação de funções e monitoramento contínuo das atividades realizadas por contas privilegiadas. Soluções PAM geralmente incluem cofres de senhas, sessões monitoradas e alertas em tempo real para detectar comportamentos anômalos, garantindo maior segurança e rastreabilidade.

Objetivo

O propósito primário do PAM é **aplicar o Princípio do Menor Privilégio** e conter a movimentação lateral em caso de invasão. Ele remove direitos administrativos permanentes das estações de trabalho e servidores, garantindo que o privilégio seja concedido apenas sob demanda (Just-in-Time) e com aprovação prévia Além de reforçar a segurança, o PAM é essencial para a conformidade (LGPD, PCI DSS, ISO 27001), pois fornece uma trilha de auditoria inalterável sobre “quem fez o quê” nos sistemas críticos da empresa.

Princípio do Menor Privilégio

Esse princípio consiste em conceder aos usuários, sistemas e processos apenas as permissões estritamente necessárias para executar suas funções. Essa abordagem reduz a superfície de ataque e limita o impacto de incidentes de segurança.



Benefícios

- Minimiza danos em caso de comprometimento de credenciais.
- Reduz riscos de movimentação lateral por invasores.
- Facilita auditoria e conformidade com normas internacionais.

Gerenciamento

O maior desafio é definir quais permissões cada usuário realmente precisa e manter essas regras atualizadas conforme funções mudam. Para isso:

- Crie políticas claras de acesso baseado em função (RBAC).
- Utilize ferramentas para auditar e revisar permissões periodicamente.
- Implemente automação e varreduras contínuas para identificar excessos de privilégios.
- Adote práticas como Just-in-Time Access, concedendo privilégios temporários sob demanda.

Uma conta privilegiada é uma conta de usuário que possui permissões elevadas para acessar sistemas, aplicativos ou dados críticos dentro de uma organização. Essas contas geralmente permitem executar ações administrativas ou sensíveis.

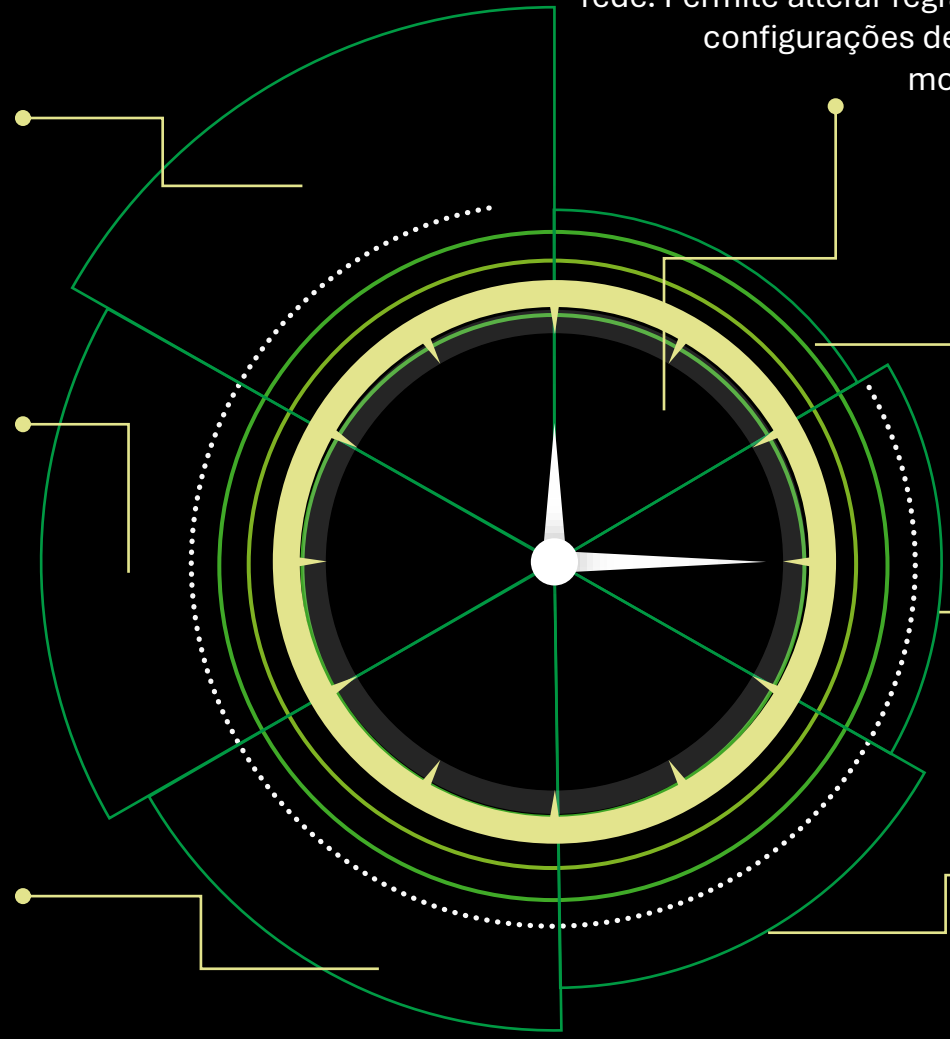
Tipos de Contas Privilegiadas

Conta de Administrador de Rede
Utilizada para gerenciar dispositivos de rede. Permite alterar regras de tráfego, configurações de segurança e monitoramento.

Conta de Emergência
São contas administrativas que só são ativadas em situações críticas, como perda de acesso devido a um ataque cibernético ou falha grave.

Conta de Administrador de Domínio
Possui controle total sobre todos os recursos do domínio, incluindo usuários, grupos e políticas de segurança.

Conta de Usuário Privilegiado
Contas com acesso a determinados recursos com base nas responsabilidades do trabalho, como acesso a determinadas capacidades administrativas.



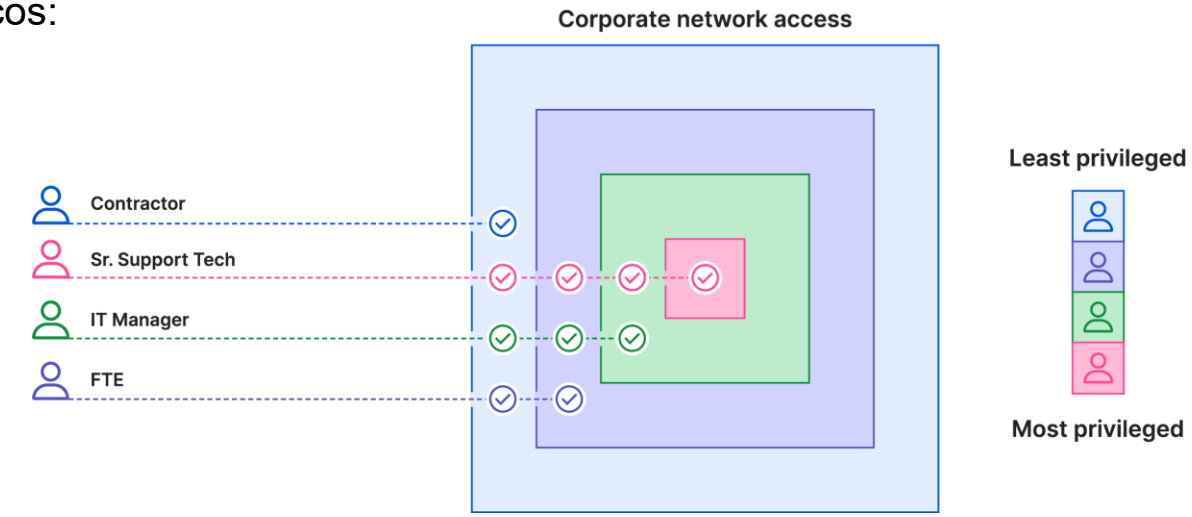
Conta de Administrador Local
Contas com privilégios administrativos em servidores ou estações de trabalho específicos e geralmente são criadas para tarefas de manutenção.

Conta de Serviço
Utilizada por aplicações ou serviços para executar processos automatizados e interagir com o SO com mais segurança.

Conta de Aplicação
Criada para permitir que aplicações interajam com bancos de dados ou outros sistemas. Pode ter privilégios elevados.

Princípio do Menor Privilégio - Cenário

Em uma grande empresa, diferentes perfis precisam acessar recursos da rede corporativa, mas cada um com níveis distintos de privilégio para reduzir riscos:



Contractor (Least Privileged)
Um prestador externo contratado para um projeto pontual só pode acessar um sistema específico para inserir dados, sem acesso à rede interna ou servidores críticos. Isso garante que, mesmo em caso de comprometimento, o impacto seja mínimo.

IT Manager (Intermediate Privilege)
O gerente de TI precisa acessar consoles de administração e relatórios estratégicos, mas não tem acesso irrestrito a cofres de senhas ou código-fonte. Seu privilégio é controlado para equilibrar eficiência e segurança.

FTE (Low Privilege)
Um colaborador interno utiliza aplicações de negócio para executar suas tarefas diárias, mas não possui permissões administrativas. Assim, evita-se que ações acidentais ou maliciosas afetem sistemas críticos.

Sr. Support Tech (Most Privileged)
O técnico de suporte sênior, responsável por manutenção e resolução de incidentes, possui privilégios elevados para aplicar patches e reiniciar serviços. No entanto, esses acessos são monitorados e concedidos sob demanda para evitar abusos.

Boas Práticas e Implementação - PAM

FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

515

Acesso Just-in-Time (JIT) e Just-Enough-Administration (JEA)

Conceito

O Acesso Just-in-Time (JIT) e Just-Enough-Administration (JEA) são práticas que garantem que privilégios administrativos sejam concedidos apenas quando necessários e pelo tempo mínimo possível. O JIT limita a duração do acesso, enquanto o JEA restringe o escopo, permitindo apenas comandos ou funções essenciais. Essa abordagem elimina privilégios permanentes e reduz a superfície de ataque.

Motivação

Contas privilegiadas permanentes são um dos maiores riscos de segurança. Se comprometidas, podem dar controle total ao invasor. Ao aplicar JIT e JEA, mesmo que uma credencial seja exposta, seu impacto é limitado. Também reduzem custos com incidentes e retrabalho, pois cada elevação é registrada e vinculada a uma justificativa.

Implementação

- Adotar políticas: Exigir solicitação formal, dupla aprovação, MFA e tempo máximo para cada elevação (ex.: 30–60 minutos).
- Configurar JIT: Conceder privilégios temporários sob demanda com expiração automática.
- Usar Azure AD PIM: Ativar roles temporárias para administradores em ambientes Windows.
- Integrar com ITSM para vincular elevações a tickets e com SIEM para correlacionar eventos.
- Monitorar sessões: Gravar todas as ações (CLI/GUI), configurar alertas para comandos críticos e encerrar automaticamente ao fim do tempo.

Controle de Acesso por Atividades

Conceito

O controle baseado em atividades combina RBAC (Role-Based Access Control) e ABAC (Attribute-Based Access Control) para garantir que permissões sejam atribuídas conforme tarefas específicas e condições contextuais, como horário, localização e postura do dispositivo.

Motivação

Evita perfis genéricos com privilégios excessivos e assegura que o acesso ocorra apenas em contexto seguro. Essa prática reduz riscos de abuso e simplifica auditorias, pois cada permissão tem justificativa clara e dono definido.

Implementação

- Mapear tarefas críticas: Identificar atividades que exigem privilégios elevados.
- Implementar RBAC: Criar funções específicas para cada processo, evitando perfis genéricos.
- Aplicar ABAC: Configurar políticas condicionais baseadas em atributos (ex.: horário, localização, postura do dispositivo).
- Bloquear acessos fora do contexto: Negar privilégios se dispositivo não estiver em compliance ou fora do horário permitido.

Cofre de Credenciais e Rotação Automática

Conceito

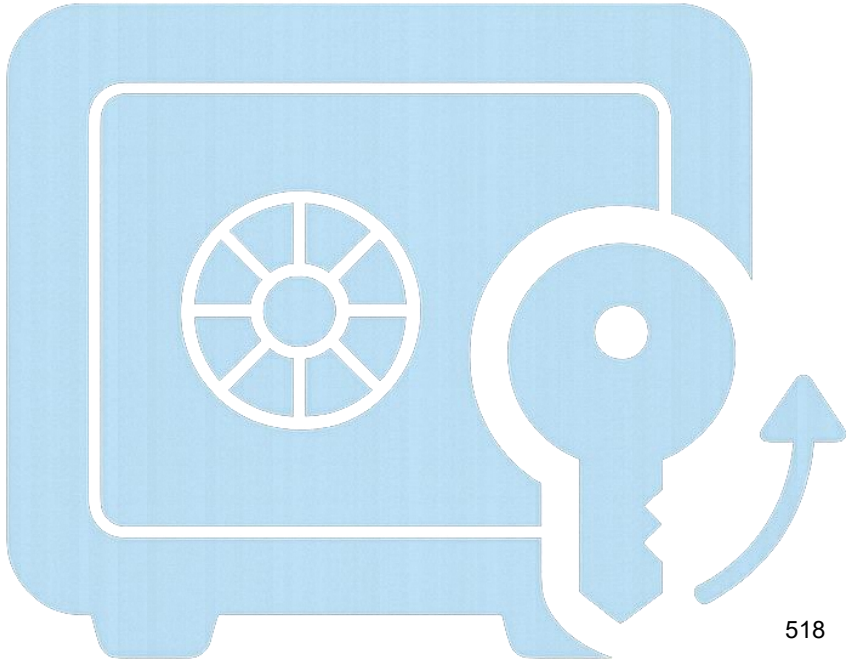
O Cofre de Credenciais e a Rotação Automática são controles que centralizam a guarda de segredos e renovam suas senhas dinamicamente. O Cofre armazena e injeta a credencial no sistema alvo sem revelá-la ao usuário, enquanto a Rotação altera a senha automaticamente após cada uso ou intervalo definido. Essa abordagem elimina senhas estáticas e impede o compartilhamento inseguro de contas administrativas.

Motivação

Credenciais fixas e conhecidas por humanos são o principal vetor de ataques de movimentação lateral. Se uma senha estática é roubada, o atacante mantém o acesso indefinidamente. Ao utilizar cofres com rotação, qualquer senha eventualmente capturada torna-se obsoleta em minutos, neutralizando o ataque e garantindo a rastreabilidade exata de quem acessou cada recurso.

Implementação

- Centralizar segredos: Armazenar senhas, chaves e tokens em cofres seguros.
- Implementar MFA: Exigir autenticação multifator para acessar o cofre.
- Configurar rotação automática: Alterar credenciais após cada uso ou em eventos críticos.
- Segregar contas: Separar contas humanas e contas de serviço no cofre.
- Integrar com DevOps: Injete segredos dinamicamente via Secrets Manager, evitando hard-coded secrets.



Gravação e Análise de Sessões Privilegiadas

Conceito

Registrar todas as ações realizadas em sessões privilegiadas (RDP, SSH, banco de dados) por meio de proxy PAM, com gravação de tela e comandos, alertas para atividades sensíveis e análise pós-evento.

Motivação

Garante evidências forenses, inibe abuso e acelera resposta a incidentes. Atende exigências regulatórias e fortalece auditoria, permitindo correlação com outros eventos de segurança.

Implementação

- Configurar proxy de sessão: Interceptar conexões RDP, SSH e banco de dados via PAM.
- Gravar todas as ações: Capturar tela e comandos executados durante sessões privilegiadas.
- Marcar eventos críticos: Identificar comandos sensíveis (ex.: DROP DATABASE, Add-ADGroupMember Domain Admins).
- Configurar alertas: Disparar notificações em tempo real para atividades suspeitas.
- Bloquear automaticamente: Interromper sessões ao detectar comandos proibidos.
- Integrar com SIEM/SOAR: Enviar logs para correlação e resposta automatizada.
- Criptografar gravações: Armazenar sessões com proteção e política de retenção definida.

Tendências de Mercado

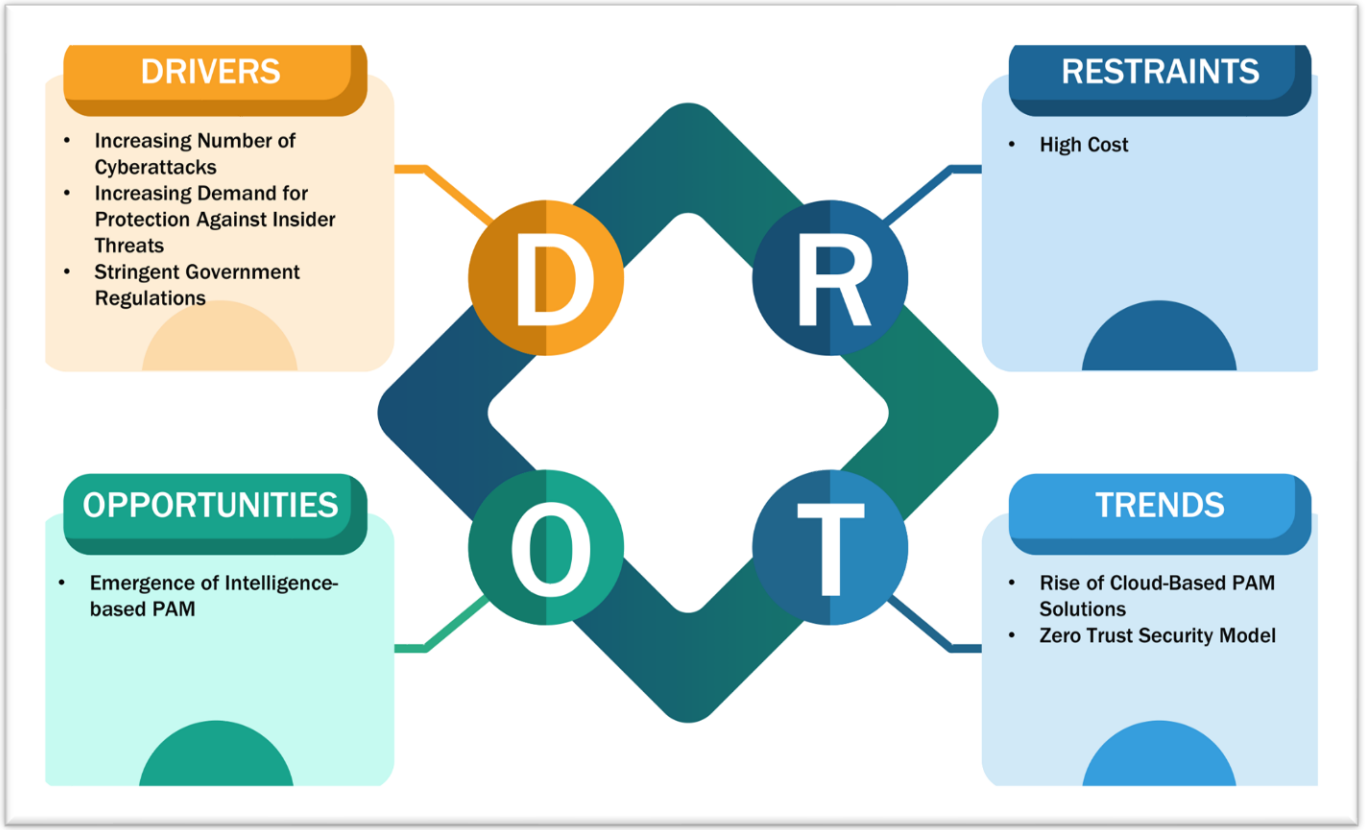
FEBRABAN FEDERAÇÃO BRASILEIRA DE BANCOS

520

Dinâmicas do Mercado de PAM

O mercado de Privileged Access Management (PAM) na América do Sul e Central está em expansão, impulsionado por fatores que moldam sua evolução. A análise DROT (Drivers, Restraints, Opportunities e Trends) permite compreender os elementos que aceleram ou limitam esse crescimento, bem como as oportunidades emergentes e tendências estratégicas. Essa visão é essencial para organizações que buscam fortalecer sua postura de segurança e alinhar investimentos às exigências regulatórias e tecnológicas.

KEY MARKET DYNAMICS



Fonte da imagem EMIS

Fatores que Impulsionam e Limitam o Mercado

Habilitadores (Drivers)

Aumento dos ciberataques

Em 2025, o setor financeiro registrou um custo médio de violação de US$ 5,56 milhões, o segundo maior entre as indústrias[1]. As ameaças cibernéticas são uma preocupação crítica, pois organizações operam em ambientes digitais. O aumento dos ataques reforça a importância da cibersegurança para proteger infraestruturas críticas e evitar acessos não autorizados.

Insider

Pelo segundo ano consecutivo, ataques internos maliciosos registraram o maior custo médio de violação: USD 4,92 milhões[1]. Ameaças internas envolvem riscos cibernéticos originados dentro da organização, geralmente por funcionários ou ex-colaboradores com acesso direto à rede e dados sensíveis. Soluções PAM ajudam a mitigar esses riscos ao monitorar e controlar acessos privilegiados, reduzindo a chance de ataques internos.

Regulamentações rigorosas

Diversas regulamentações do setor e do governo exigem que as empresas sigam controles de segurança rigorosos. Nesse contexto, o gerenciamento de acesso privilegiado é um elemento essencial da estratégia de cibersegurança das organizações.

Restrições (Restraints)

Alto custo de implementação

O gerenciamento de acesso privilegiado é uma medida essencial para controlar credenciais com permissões avançadas. No entanto, o investimento inicial pode ser elevado para muitas empresas, variando conforme fatores como porte da organização e quantidade de endpoints ou servidores acessados.

[1] IBM

Caminhos para Inovação e Adoção

Oportunidades (Opportunities)

PAM baseado em inteligência:

As soluções PAM estão evoluindo com recursos inteligentes, como IA e Machine Learning, para reforçar segurança e controle de acesso. A análise comportamental permite identificar padrões normais, detectar desvios (como acessos incomuns) e acionar alertas ou ações preventivas automaticamente.

Tendências (Trends)

Ascensão das soluções PAM baseadas em nuvem

Com a migração de aplicações e infraestrutura para a nuvem, cresce a demanda por soluções PAM baseadas em cloud, que oferecem plataforma centralizada e segura para controlar acessos privilegiados em ambientes híbridos e multicloud. Entre os benefícios estão escalabilidade, flexibilidade, eficiência de custos, gestão simplificada e segurança aprimorada.

Modelo Zero Trust

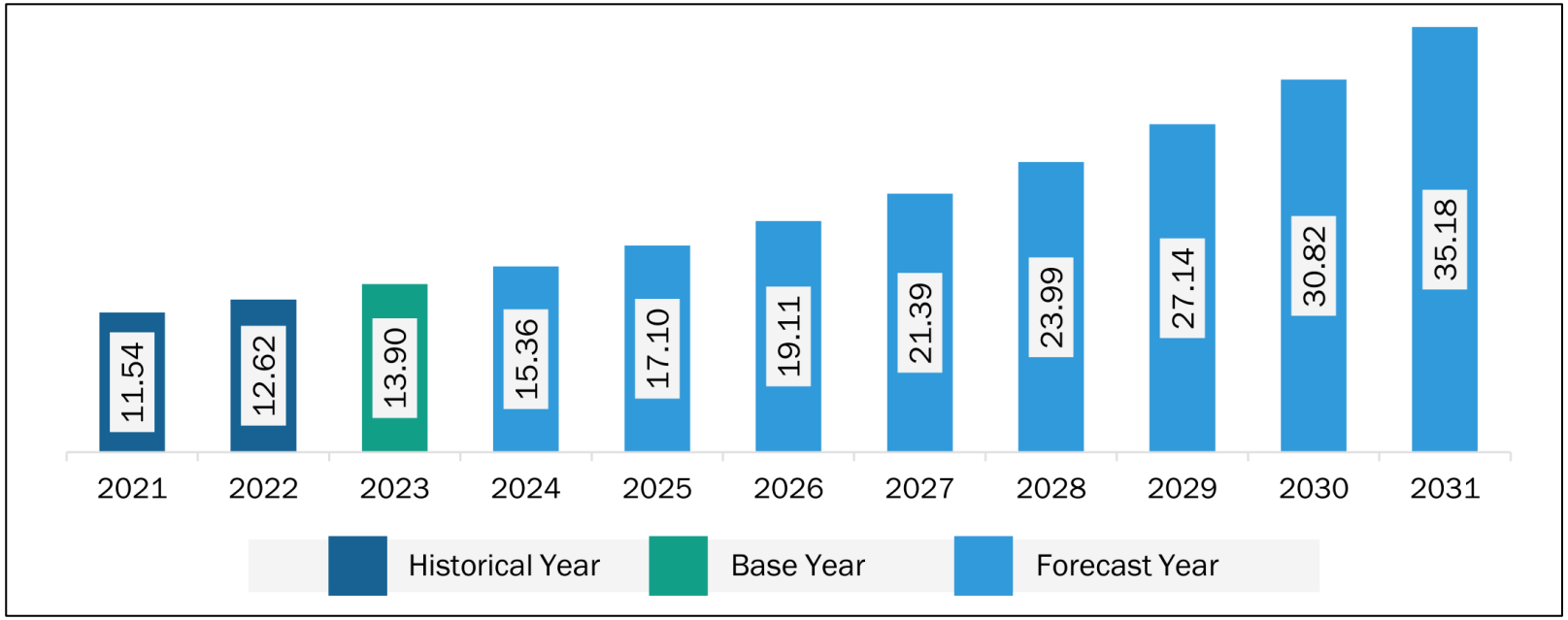
O modelo Zero Trust está transformando o gerenciamento de acesso privilegiado, impondo práticas de segurança mais rigorosas. Seu objetivo é conceder acesso apenas quando necessário e por um motivo específico, garantindo que contas, aplicações ou equipamentos sejam usados sob demanda e por tempo limitado. As soluções modernas de PAM seguem esse princípio, substituindo gradualmente os modelos tradicionais baseados em perímetro.

Crescimento do Mercado de PAM

A lucratividade e a reputação do setor financeiro dependem diretamente da capacidade de proteger clientes e ativos contra ameaças cada vez mais sofisticadas. A complexidade dos processos internos e o aumento contínuo dos ciberataques impulsionam a demanda por soluções que garantam controle rigoroso sobre acessos privilegiados. Nesse cenário, o gerenciamento de acessos privilegiados (PAM) se destaca como um componente estratégico para fortalecer a governança, reduzir riscos e apoiar a recuperação frente a incidentes, incluindo ataques internos.

O gráfico a seguir apresenta a evolução do mercado de soluções PAM na América do Sul e Central para o setor financeiro, com projeções de crescimento até 2031, refletindo a importância crescente dessas ferramentas para instituições financeiras.

MERCADO DE SOLUÇÕES PAM PARA O SETOR FINANCEIRO NA AMÉRICA DO SUL E CENTRAL – RECEITA E PREVISÃO (US$ MILHÕES) [1]



Fonte do gráfico EMIS

Conclusão

À medida que os ataques cibernéticos se tornam mais sofisticados e impactam setores críticos, como demonstrado por incidentes bilionários envolvendo provedores de serviços de tecnologia no Sistema de Pagamentos Brasileiro, fica evidente que controles estáticos não são suficientes para proteger organizações em um cenário dinâmico e interconectado.

Gerenciamento de Acesso Privilegiado surge como um pilar estratégico para reduzir riscos associados a credenciais privilegiadas, que continuam sendo alvo prioritário em campanhas avançadas. Reguladores e seguradoras já exigem sua implementação como requisito de conformidade e cobertura, enquanto a expansão do acesso por terceiros e dispositivos não gerenciados amplia a superfície de ataque, exigindo maior visibilidade e governança.

Mais do que um controle tradicional, **PAM é um habilitador do modelo Zero Trust**, sustentado pela adoção de práticas como Just-in-Time e gestão de identidades de máquinas. Essa abordagem garante que privilégios sejam concedidos apenas quando necessários e pelo tempo estritamente limitado, reduzindo drasticamente riscos de movimentação lateral e comprometimento sistêmico.

Diante desse cenário, evoluir para um PAM moderno que vá além do cofre de credenciais e incorpore detecção de ameaças privilegiadas, gestão de segredos em ambientes cloud, DevOps e RPA não é apenas uma tendência, mas **uma necessidade estratégica para assegurar resiliência cibernética e continuidade operacional no futuro digital.**

Deloitte.