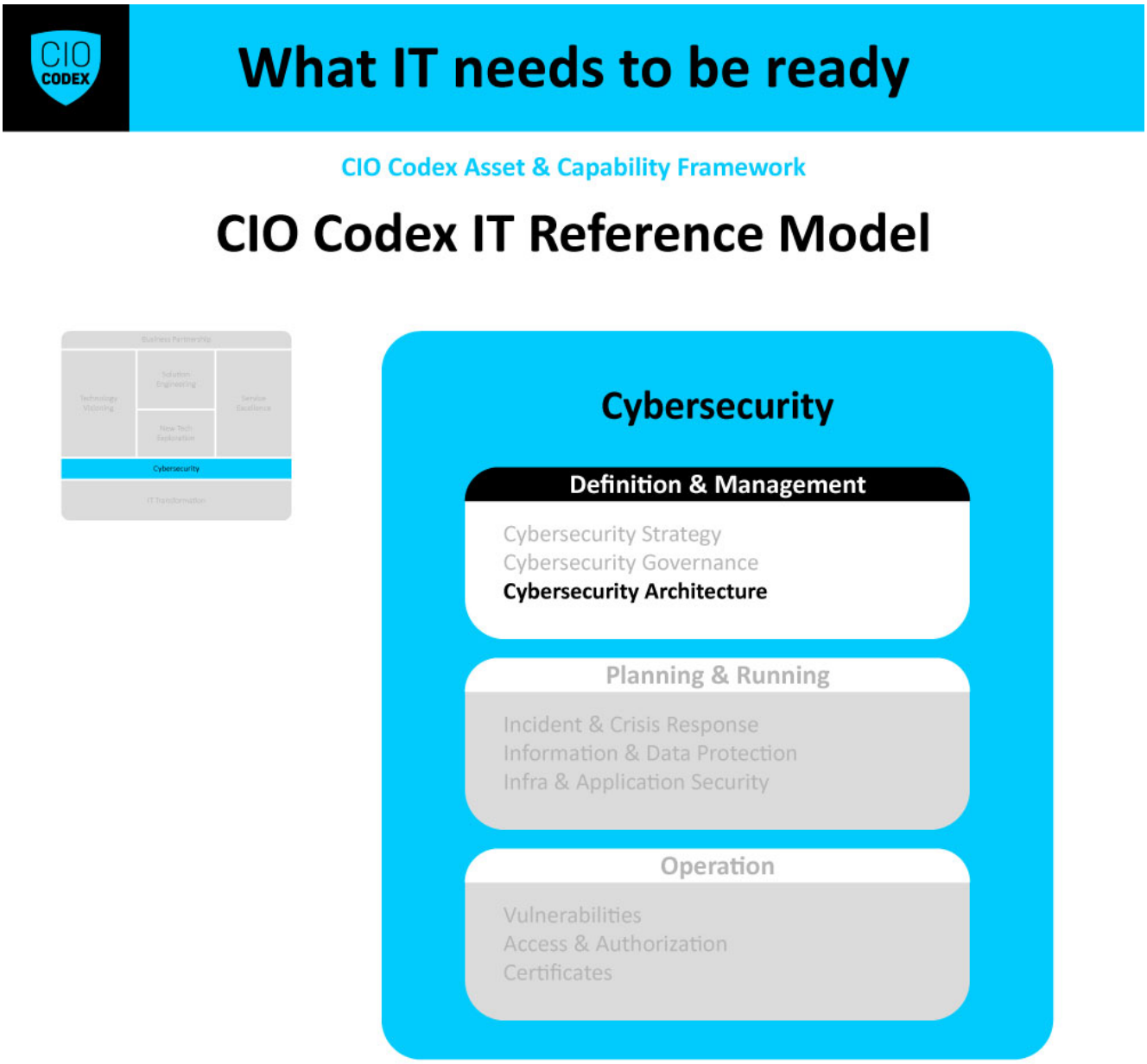


A Cybersecurity Architecture, integrante da macro capability Definition & Management e situada na camada Cybersecurity do CIO Codex Capability Framework, representa um pilar vital para a segurança cibernética eficiente nas organizações.

Esta capability é crucial para garantir que a segurança seja intrínseca em todos os aspectos das operações de TI, oferecendo uma abordagem proativa e resiliente na construção de defesas contra as ameaças cibernéticas dinâmicas e em evolução.

No contexto desta capability, os conceitos-chave abrangem a Arquitetura de Segurança, que se refere ao design estrutural dos sistemas de segurança, abrangendo infraestrutura tecnológica, políticas, procedimentos e modelos de controle.

A Integração de Tecnologias de Segurança é essencial, pois envolve a harmonização de soluções de segurança, como firewalls, antivírus e sistemas de detecção de intrusões, em uma estrutura coesa.

Além disso, os Modelos de Controle de Acesso são fundamentais para determinar quem pode acessar quais recursos e em quais circunstâncias.

As características da Cybersecurity Architecture incluem o Design Seguro, que envolve a incorporação de medidas de segurança desde o início do desenvolvimento de soluções de TI.

A Análise de Vulnerabilidades é uma prática contínua de identificação e avaliação de pontos fracos na arquitetura de segurança.

Os Padrões de Segurança, que definem diretrizes e melhores práticas, guiam a implementação consistente de segurança em toda a organização.

A Resiliência é uma característica chave, assegurando que a arquitetura seja capaz de resistir e recuperar-se de ataques ou eventos adversos.

A Avaliação de Impacto analisa os efeitos potenciais de incidentes de segurança nas operações organizacionais.

Por fim, a Adoção de Princípios de Zero Trust, que implementa uma abordagem de segurança baseada na negação automática de confiança até que seja verificada.

O propósito principal da Cybersecurity Architecture é o desenvolvimento e manutenção de uma arquitetura de segurança robusta, que contribui significativamente para a eficiência operacional, inovação e vantagem competitiva.

Esta capability é crítica para proteger os ativos digitais da organização, incluindo redes, sistemas e dados sensíveis.

Os objetivos desta capability no âmbito do CIO Codex Capability Framework incluem assegurar a eficiência operacional por meio do design e implementação de soluções de segurança que se integrem sem problemas com a infraestrutura existente.

A inovação em segurança cibernética é perseguida através da adoção de tecnologias e abordagens avançadas.

Além disso, demonstrar uma arquitetura de segurança robusta contribui para a vantagem competitiva, atraindo clientes e parceiros que confiam na capacidade da organização de proteger seus dados e operações.

No espectro tecnológico, a Cybersecurity Architecture influencia vários aspectos.

Na infraestrutura, ela define requisitos de segurança, assegurando a proteção contra

ameaças cibernéticas.

Na arquitetura, influencia o design de sistemas e aplicativos, incorporando medidas de segurança desde a concepção.

Nos sistemas, estabelece políticas que guiam o desenvolvimento seguro de sistemas e aplicativos.

A estratégia de segurança cibernética define as estruturas técnicas e controles necessários para a proteção dos ativos tecnológicos.

Por fim, no Modelo Operacional, a Cybersecurity Architecture assegura que a segurança seja uma consideração central em todas as iniciativas de TI, influenciando processos operacionais para monitorar e manter a postura de segurança.

Em resumo, a Cybersecurity Architecture é uma capability essencial que fornece a estrutura para uma abordagem de segurança cibernética integrada e eficaz nas organizações.

Ela não só garante a proteção contra ameaças digitais, mas também reforça a posição da organização no mercado, transmitindo confiança e segurança aos stakeholders.

A capacidade de integrar proativamente a segurança em todas as operações de TI e manter a continuidade operacional diante de desafios na segurança digital é um diferencial competitivo fundamental no cenário empresarial contemporâneo.

# Conceitos e Características

A Cybersecurity Architecture é um alicerce fundamental para uma postura de segurança cibernética eficaz, garantindo que a segurança seja incorporada em todos os aspectos das operações de TI.

Sua abordagem proativa e foco na construção de defesas robustas protege a organização contra ameaças cibernéticas em constante evolução.

**Conceitos**

- Arquitetura de Segurança: Refere-se ao design estrutural de sistemas de segurança que compreendem a infraestrutura tecnológica, políticas, procedimentos e modelos de controle.
- Integração de Tecnologias de Segurança: Envolve a incorporação

harmoniosa de soluções tecnológicas de segurança, como firewalls, antivírus, sistemas de detecção de intrusões, em uma arquitetura coesa.
- Modelos de Controle de Acesso: Definição de políticas e regras que determinam quem tem permissão para acessar quais recursos e sob quais condições.

**Características**

- Design Seguro: Desenvolvimento de uma arquitetura que incorpora medidas de segurança desde o início, garantindo que a segurança seja intrínseca a todas as soluções de TI.
- Análise de Vulnerabilidades: Identificação e avaliação contínua de pontos fracos na arquitetura de segurança, com ações corretivas imediatas.
- Padrões de Segurança: Definição de diretrizes e melhores práticas de segurança para orientar a implementação consistente em toda a organização.
- Resiliência: Garantia de que a arquitetura seja capaz de resistir e se recuperar de ataques cibernéticos ou eventos adversos.
- Avaliação de Impacto: Análise dos efeitos potenciais de incidentes de segurança na operação da organização.
- Adoção de Princípios de Zero Trust: Implementação de uma abordagem de segurança em que a confiança é negada automaticamente até que seja verificada, em vez de confiar implicitamente em qualquer usuário ou dispositivo.

# Propósito e Objetivos

A Cybersecurity Architecture é uma capability de extrema importância, pois tem como propósito central a criação e manutenção de uma arquitetura de segurança robusta.

Nesse contexto, sua relevância para o negócio é inegável, pois contribui de forma significativa para a eficiência operacional, inovação e vantagem competitiva.

Esta capability desempenha um papel crítico na proteção dos ativos digitais da organização, incluindo redes, sistemas e dados sensíveis.

**Objetivos**

Dentro do contexto do CIO Codex Capability Framework, os objetivos da Cybersecurity Architecture são claramente definidos:

- Eficiência Operacional: A principal meta é garantir a eficiência operacional, projetando e implementando soluções de segurança que minimizem o impacto nas operações de TI da organização. Isso envolve a criação de arquiteturas de segurança que se integrem harmoniosamente com a infraestrutura existente, sem comprometer a eficiência.
- Inovação: A Cybersecurity Architecture busca promover a inovação em segurança cibernética, adotando abordagens e tecnologias de ponta para proteger contra ameaças em constante evolução. Isso inclui a identificação e avaliação contínua de novas soluções de segurança e a integração de controles avançados.
- Vantagem Competitiva: A capacidade de demonstrar uma arquitetura de segurança sólida pode se traduzir em vantagem competitiva. Isso atrai clientes e parceiros de negócios que confiam na capacidade da organização de proteger seus dados e operações.

**Impacto na Tecnologia**

A Cybersecurity Architecture influencia diversos aspectos da tecnologia:

- Infraestrutura: Define requisitos de segurança para a infraestrutura de TI, garantindo que os ativos de hardware sejam protegidos contra ameaças cibernéticas.
- Arquitetura: Projeta a arquitetura de segurança, incorporando medidas que protegem sistemas e aplicativos.
- Sistemas: Define políticas de segurança que orientam o desenvolvimento de sistemas e aplicativos seguros.
- Cybersecurity: A arquitetura de segurança cibernética define as estruturas técnicas e controles necessários para proteger ativos tecnológicos contra ameaças.
- Modelo Operacional: Garante que a segurança seja uma consideração central em todas as iniciativas de TI, influenciando processos operacionais para monitorar e manter a postura de segurança.

# Roadmap de Implementação

A Cybersecurity Architecture desempenha um papel fundamental no cenário de segurança cibernética, fornecendo uma base sólida para proteger a organização contra ameaças em constante evolução.

Para implementar essa capability de maneira eficaz, é essencial seguir um roadmap bem definido, considerando os seguintes pontos-chave dentro do contexto do CIO Codex Capability Framework:

- Compreensão dos Princípios de Arquitetura de Segurança: O primeiro passo na implementação da Cybersecurity Architecture é garantir que todos os envolvidos compreendam os princípios fundamentais da arquitetura de segurança. Isso envolve educar líderes e equipes de TI sobre a importância de incorporar medidas de segurança desde o início do design de sistemas e aplicativos.
- Avaliação da Arquitetura Existente: Realize uma avaliação abrangente da arquitetura de segurança atual da organização. Identifique suas principais vulnerabilidades e deficiências, bem como seus pontos fortes. Isso servirá como base para futuras melhorias.
- Definição de Princípios de Design Seguro: Estabeleça princípios claros de design seguro que orientarão o desenvolvimento de sistemas e aplicativos. Isso inclui a consideração de medidas de segurança, como autenticação, autorização e criptografia desde o início do processo de design.
- Integração de Tecnologias de Segurança: Garanta a integração harmoniosa de tecnologias de segurança, como firewalls, antivírus, sistemas de detecção de intrusões, na arquitetura geral de TI. Isso exige uma análise cuidadosa para garantir que essas tecnologias trabalhem em conjunto de maneira eficaz.
- Desenvolvimento de Padrões de Segurança: Defina diretrizes e melhores práticas de segurança que devem ser seguidas em toda a organização. Isso promove a consistência na implementação de medidas de segurança em todos os projetos.
- Avaliação de Vulnerabilidades Contínua: Estabeleça um processo de avaliação contínua de vulnerabilidades na arquitetura de segurança. Isso

inclui a identificação regular de pontos fracos e a aplicação de ações corretivas imediatas.

- Resiliência e Recuperação: Desenvolva estratégias para garantir que a arquitetura seja resiliente e capaz de se recuperar de ataques cibernéticos ou eventos adversos. Isso pode envolver a implementação de redundância e planos de continuidade de negócios.
- Controle de Acesso e Políticas de Segurança: Defina políticas rigorosas de controle de acesso e regras que determinem quem tem permissão para acessar recursos e dados sensíveis. Isso inclui a implementação de modelos de controle de acesso sólidos.
- Monitoramento e Análise de Impacto: Estabeleça sistemas de monitoramento contínuo da segurança e realize análises de impacto para entender as consequências potenciais de incidentes de segurança na operação da organização.
- Adoção de Princípios de Zero Trust: Implemente uma abordagem de "Zero Trust" que nega automaticamente a confiança até que seja verificada. Isso ajuda a fortalecer a postura de segurança, evitando confiança implícita em qualquer usuário ou dispositivo.
- Comunicação e Conscientização: Promova uma cultura de comunicação aberta e conscientização em segurança cibernética em toda a organização. Isso envolve treinar colaboradores e mantê-los informados sobre práticas seguras.
- Documentação e Revisão Contínua: Mantenha uma documentação completa de todos os aspectos da arquitetura de segurança e revise-a regularmente para garantir que esteja alinhada com as necessidades em constante mudança da organização.

A implementação bem-sucedida da Cybersecurity Architecture é um investimento crítico para proteger os ativos digitais da organização.

Ela não apenas fortalece a segurança cibernética, mas também contribui para a eficiência operacional, inovação e vantagem competitiva.

Ao seguir esse roadmap, a organização estará mais preparada para enfrentar ameaças cibernéticas e proteger seus sistemas, dados e reputação.

# Melhores Práticas de Mercado

Dentro do âmbito do CIO Codex Capability Framework, a Cybersecurity Architecture representa uma capability fundamental para assegurar que a segurança seja incorporada de maneira intrínseca em todos os aspectos das operações de TI.

Para uma implementação bem-sucedida dessa capability, é crucial adotar as melhores práticas de mercado.

A seguir, as principais melhores práticas que são amplamente reconhecidas no setor de segurança cibernética:

- Design Seguro desde o Início: Uma abordagem proativa e eficaz começa com o desenvolvimento de uma arquitetura de segurança que incorpora medidas de segurança desde o início. Isso garante que a segurança seja intrínseca a todas as soluções de TI, reduzindo a necessidade de correções pós-implantação e economizando recursos no longo prazo.
- Integração de Tecnologias de Segurança: A integração harmoniosa de diversas soluções tecnológicas de segurança é essencial. Isso inclui firewalls, antivírus, sistemas de detecção de intrusões e outros controles de segurança. Uma arquitetura coesa garante uma defesa sólida e eficiente contra ameaças cibernéticas.
- Modelos de Controle de Acesso Claros: Definir políticas e regras rigorosas de controle de acesso é fundamental para determinar quem tem permissão para acessar quais recursos e sob quais condições. Isso ajuda a evitar acessos não autorizados e a proteger informações sensíveis.
- Análise Contínua de Vulnerabilidades: Identificar e avaliar continuamente pontos fracos na arquitetura de segurança é uma prática essencial. Ações corretivas imediatas podem ser tomadas para mitigar ameaças assim que forem identificadas.
- Definição de Padrões de Segurança: Estabelecer diretrizes e melhores práticas de segurança é crucial para orientar a implementação consistente em toda a organização. Isso garante que todas as partes da infraestrutura sigam as mesmas normas elevadas de segurança.
- Resiliência como Prioridade: Garantir que a arquitetura seja capaz de resistir e se recuperar de ataques cibernéticos ou eventos adversos é uma abordagem crítica. A resiliência minimiza o impacto de incidentes de segurança e reduz o tempo de inatividade.

- Avaliação de Impacto de Segurança: Uma análise cuidadosa dos efeitos potenciais de incidentes de segurança na operação da organização é uma prática preventiva essencial. Isso permite que a organização esteja preparada para lidar com as consequências de violações de segurança.
- Adoção de Princípios de Zero Trust: A implementação de uma abordagem de segurança baseada no princípio de "confiança zero" é cada vez mais relevante. Nesse modelo, a confiança é negada automaticamente até que seja verificada, em vez de confiar implicitamente em qualquer usuário ou dispositivo.
- Aprimoramento Contínuo: A busca por melhorias contínuas é fundamental na segurança cibernética. Isso envolve a identificação e avaliação constantes de novas soluções de segurança e a integração de controles avançados para lidar com ameaças emergentes.
- Transparência e Comunicação Eficiente: Manter comunicações claras e transparentes sobre políticas e procedimentos de segurança é crucial. Isso promove a compreensão e o comprometimento de todos os envolvidos, desde a equipe de TI até os líderes de negócios.

A Cybersecurity Architecture desempenha um papel crítico na proteção dos ativos digitais da organização.

Adotar essas melhores práticas de mercado permite que as organizações fortaleçam suas defesas cibernéticas, enfrentem ameaças em constante evolução e mantenham a integridade de suas operações de TI.

# Desafios Atuais

A Cybersecurity Architecture desempenha um papel crucial na construção de defesas robustas contra ameaças cibernéticas em constante evolução, integrando medidas de segurança em todos os aspectos das operações de TI.

No entanto, ao adotar e integrar essa capability em seus processos de negócios e operações de TI, as organizações enfrentam uma série de desafios atuais no mercado, de acordo com as melhores práticas do setor.

Abaixo os principais desafios:

- Complexidade da Arquitetura de Segurança: Projetar e manter uma arquitetura de segurança robusta é desafiador devido à complexidade das infraestruturas de TI modernas e à diversidade de ameaças cibernéticas.
- Integração de Tecnologias de Segurança: Incorporar tecnologias de segurança, como firewalls e sistemas de detecção de intrusões, de forma coesa na arquitetura é um desafio, pois exige garantir a compatibilidade e a eficácia dessas soluções.
- Gerenciamento de Políticas de Segurança: Definir e gerenciar políticas de segurança consistentes em toda a arquitetura é complexo, pois diferentes partes da organização podem ter requisitos distintos.
- Avaliação Contínua de Vulnerabilidades: Identificar e remediar vulnerabilidades na arquitetura de segurança requer uma análise constante, pois novas ameaças e fraquezas surgem regularmente.
- Mudança Cultural: Promover uma cultura organizacional que priorize a segurança cibernética é desafiador, pois exige uma mudança de mentalidade e comportamento de todos os funcionários.
- Conformidade com Regulamentações: Garantir que a arquitetura esteja em conformidade com regulamentações de segurança cibernética é um desafio, pois as leis estão em constante evolução.
- Escassez de Talentos em Segurança: A falta de profissionais qualificados em segurança cibernética dificulta a implementação e o gerenciamento eficaz da arquitetura.
- Ameaças Emergentes: Lidar com ameaças cibernéticas emergentes, como ataques de ransomware sofisticados, requer atualização constante da arquitetura de segurança.
- Escopo Global: Organizações com presença global enfrentam o desafio de aplicar consistentemente a arquitetura de segurança em todas as regiões, considerando as nuances locais.
- Investimentos Suficientes: Alocar recursos financeiros adequados para desenvolver e manter uma arquitetura de segurança de alto nível é uma preocupação constante.

Esses desafios refletem a natureza dinâmica e complexa da segurança cibernética nos dias de hoje.

Com ameaças em constante evolução, requisitos regulatórios mutáveis e a necessidade de mudanças culturais, a Cybersecurity Architecture é fundamental para enfrentar esses desafios e proteger os ativos digitais da organização.

A capability de projetar uma arquitetura segura desde o início, avaliar vulnerabilidades continuamente, garantir a conformidade e promover uma cultura de segurança é essencial para manter uma postura eficaz contra ameaças cibernéticas.

Investir na arquitetura de segurança cibernética não é apenas uma resposta aos desafios atuais, mas também um passo fundamental para enfrentar as ameaças em constante evolução no futuro.

# Tendências para o Futuro

A Cybersecurity Architecture desempenha um papel crucial na defesa das organizações contra as ameaças cibernéticas em constante evolução.

Sua abordagem proativa na construção de defesas sólidas é fundamental para a segurança cibernética.

Considerando as expectativas do mercado e as grandes tendências, as seguintes tendências futuras que moldarão o desenvolvimento da Cybersecurity Architecture:

- Arquiteturas de Segurança Adaptativas: A evolução das ameaças exigirá arquiteturas de segurança mais adaptativas, capazes de se ajustar em tempo real para responder a ataques em constante mutação.
- Zero Trust Architecture (ZTA): A adoção de abordagens de Zero Trust, onde a confiança é negada até que seja verificada, ganhará destaque na Cybersecurity Architecture para proteger contra ameaças internas e externas.
- Inteligência Artificial para Defesa: O uso de IA e machine learning será amplamente adotado para melhorar a detecção precoce de ameaças, permitindo respostas mais rápidas e eficazes.
- Segurança na Nuvem (Cloud Security): Com a migração contínua para ambientes de nuvem, a Cybersecurity Architecture se concentrará na integração eficaz de medidas de segurança em ambientes em nuvem.
- Privacidade por Design: A integração da privacidade desde a concepção (Privacy by Design) será uma prioridade, alinhando-se com regulamentações de privacidade de dados cada vez mais rigorosas.
- Segurança de IoT (Internet of Things): Com a proliferação de dispositivos IoT, a Cybersecurity Architecture se expandirá para incluir estratégias

específicas para proteger esses dispositivos e suas interações.
- Orquestração de Segurança: A automação e orquestração de tarefas de segurança serão implementadas para otimizar a resposta a incidentes e reduzir a carga de trabalho dos profissionais de segurança.
- Arquitetura Resiliente: A resiliência se tornará um pilar fundamental na arquitetura de segurança, com a capacidade de se recuperar rapidamente de ataques cibernéticos sendo essencial.
- Colaboração com Ecossistemas de Segurança: A colaboração entre organizações para compartilhar informações sobre ameaças e melhores práticas de segurança se tornará mais comum para fortalecer as defesas cibernéticas.
- Governança de Segurança Reforçada: Uma governança robusta de segurança será incorporada à Cybersecurity Architecture para garantir a conformidade e a eficácia das medidas de segurança.

Essas tendências refletem a crescente complexidade do cenário de segurança cibernética e a necessidade contínua de adaptação e inovação na Cybersecurity Architecture.

À medida que as ameaças evoluem, essa capability continuará a desempenhar um papel crítico na proteção dos ativos digitais das organizações e na garantia de operações seguras e eficientes.

# KPIs Usuais

A Cybersecurity Architecture desempenha um papel essencial na proteção das operações de TI e na garantia da segurança cibernética de uma organização.

A avaliação de seu desempenho é fundamental para garantir que as defesas contra ameaças cibernéticas sejam sólidas e eficazes.

Abaixo, uma lista dos principais KPIs usuais no contexto do CIO Codex Capability Framework, que ajudam a medir o desempenho da Cybersecurity Architecture:

- Taxa de Conformidade com Padrões de Segurança (Security Standards Compliance Rate): Mede o grau de conformidade da arquitetura de segurança com os padrões reconhecidos da indústria, como ISO 27001.

- Tempo Médio de Detecção de Vulnerabilidades (Mean Time to Detect Vulnerabilities): Calcula o tempo médio necessário para identificar vulnerabilidades na arquitetura de segurança e iniciar ações corretivas.
- Taxa de Implementação de Controles de Acesso (Access Control Implementation Rate): Avalia a eficácia na implementação de políticas de controle de acesso para proteger recursos críticos.
- Avaliação de Resiliência Cibernética (Cyber Resilience Assessment): Mede a capacidade da arquitetura de segurança de se recuperar de ataques cibernéticos ou eventos adversos.
- Taxa de Atualização de Arquitetura (Architecture Update Rate): Avalia a frequência com que a arquitetura de segurança é revisada e atualizada para enfrentar ameaças em evolução.
- Taxa de Aderência a Princípios de Zero Trust (Zero Trust Principles Adherence Rate): Indica o quão bem a arquitetura incorpora a abordagem de Zero Trust, onde a confiança é negada até que seja verificada.
- Avaliação de Eficácia de Modelos de Controle (Control Model Effectiveness Assessment): Mede a eficácia dos modelos de controle de acesso implementados na arquitetura de segurança.
- Tempo Médio de Recuperação Após Incidente (Mean Time to Recovery After Incident): Calcula o tempo médio necessário para recuperar a funcionalidade total após um incidente de segurança.
- Taxa de Implementação de Criptografia (Encryption Implementation Rate): Avalia a implementação de criptografia para proteger dados sensíveis na arquitetura de segurança.
- Avaliação de Conformidade de Terceiros (Third-Party Compliance Assessment): Mede a conformidade de parceiros e fornecedores com os padrões de segurança estabelecidos na arquitetura.
- Taxa de Redução de Vulnerabilidades (Vulnerability Reduction Rate): Indica o sucesso das ações corretivas na redução do número de vulnerabilidades identificadas.
- Avaliação de Impacto de Incidentes (Incident Impact Assessment): Mede o impacto potencial de incidentes de segurança na operação da organização.
- Taxa de Adoção de Novas Tecnologias de Segurança (Adoption Rate of New Security Technologies): Avalia a rapidez com que a arquitetura incorpora tecnologias de segurança inovadoras.
- Avaliação de Conformidade Regulatória (Regulatory Compliance

Assessment): Mede a conformidade da arquitetura com regulamentos e leis de segurança cibernética.
- Taxa de Realização de Testes de Penetração (Penetration Testing Execution Rate): Avalia a frequência com que testes de penetração são realizados para identificar vulnerabilidades.

Esses KPIs ajudam a garantir que a Cybersecurity Architecture seja proativa na proteção contra ameaças cibernéticas em constante evolução.

A medição regular desses indicadores é crucial para manter uma arquitetura de segurança sólida e eficaz que protege os ativos digitais da organização.

# Exemplos de OKRs

A capability de Cybersecurity Architecture na macro capability Definition & Management da camada Cybersecurity é de suma importância, uma vez que se concentra na criação e manutenção de uma arquitetura de segurança robusta.

Essa capability envolve o design e a implementação de soluções de segurança que protegem as redes, sistemas e dados da organização.

Além disso, inclui a integração de tecnologias de segurança, a definição de modelos de controle de acesso e a garantia de que a segurança é uma consideração central em todas as iniciativas de TI.

A seguir, são apresentados exemplos de Objetivos e Resultados-Chave (OKRs) relacionados a esta capability:

**Design e Implementação de Soluções de Segurança**

**Objetivo: Desenvolver e implementar soluções de segurança eficazes para proteger os ativos de TI da organização.**

- KR1: Realizar uma avaliação abrangente das necessidades de segurança da organização.
- KR2: Projetar e implementar uma arquitetura de segurança que abranja todos os sistemas críticos.
- KR3: Implementar soluções de segurança de próxima geração para proteção contra ameaças avançadas.

**Integração de Tecnologias de Segurança**

**Objetivo: Garantir que as tecnologias de segurança sejam integradas de maneira eficaz e coordenada.**

- KR1: Integrar sistemas de detecção de intrusões e prevenção de ameaças em toda a infraestrutura de TI.
- KR2: Implementar soluções de gerenciamento unificado de ameaças para monitoramento contínuo.
- KR3: Garantir a compatibilidade e interoperabilidade de todas as tecnologias de segurança.

**Definição de Modelos de Controle de Acesso**

**Objetivo: Estabelecer modelos de controle de acesso que limitem o acesso não autorizado aos sistemas e dados.**

- KR1: Implementar políticas de controle de acesso baseadas em funções (RBAC) para sistemas críticos.
- KR2: Configurar autenticação multifator em todas as contas de usuário privilegiadas.
- KR3: Monitorar e revisar regularmente as políticas de controle de acesso para ajustes.

**Segurança como Consideração Central**

**Objetivo: Garantir que a segurança seja incorporada em todas as iniciativas de TI desde o início.**

- KR1: Realizar avaliações de segurança de projetos de TI antes da implementação.
- KR2: Integrar revisões de segurança em todos os processos de desenvolvimento de software.
- KR3: prover treinamento de conscientização em segurança para toda a equipe de TI.

**Avaliação Contínua e Melhoria da Arquitetura de Segurança**

**Objetivo: Avaliar continuamente a eficácia da arquitetura de segurança e realizar melhorias conforme necessário.**

- KR1: Realizar testes de penetração regulares para identificar vulnerabilidades.
- KR2: Realizar auditorias de segurança para avaliar o cumprimento das políticas.
- KR3: Implementar atualizações de segurança em resposta a novas ameaças.

Através desses OKRs, a capability de Cybersecurity Architecture desempenha um papel crucial na proteção dos ativos de TI da organização, garantindo que as soluções de segurança sejam eficazes, as tecnologias sejam integradas de forma coordenada e que a segurança seja uma consideração central em todas as iniciativas de TI.

Isso contribui para a defesa contra ameaças cibernéticas e a manutenção de um ambiente de TI seguro.

# Critérios para Avaliação de Maturidade

A capability Cybersecurity Architecture, inserida na macro capability Definition & Management e na camada Cybersecurity, desempenha um papel crucial na criação e manutenção de uma arquitetura de segurança sólida.

Esta capability abrange o design e a implementação de soluções de segurança que protegem as redes, sistemas e dados da organização.

Para avaliar sua maturidade, seguem critérios inspirados no modelo CMMI, considerando cinco níveis de maturidade: Inexistente, Inicial, Definido, Gerenciado e Otimizado.

**Nível de Maturidade Inexistente**

- Não há considerações específicas de segurança cibernética na arquitetura de TI.

- Ausência de políticas ou diretrizes para a integração de tecnologias de segurança.
- A segurança não é incorporada na definição de modelos de controle de acesso.
- Não existe uma estratégia para garantir que a segurança seja uma consideração central em iniciativas de TI.
- Falta de conscientização sobre a importância da arquitetura de segurança.

**Nível de Maturidade Inicial**

- Iniciativas iniciais de incorporação de segurança cibernética na arquitetura de TI.
- Documentação de políticas de segurança, mas não totalmente integradas na arquitetura.
- Algumas tecnologias de segurança são consideradas, mas não de forma abrangente.
- Controles de acesso são definidos de maneira limitada.
- A segurança é considerada em projetos selecionados de TI.

**Nível de Maturidade Definido**

- Uma estratégia formal de segurança cibernética está definida na arquitetura de TI.
- Políticas de segurança cibernética são documentadas e incorporadas na arquitetura.
- Tecnologias de segurança são integradas de forma planejada.
- Modelos de controle de acesso são bem definidos e implementados.
- A segurança é uma consideração central em todas as iniciativas de TI.

**Nível de Maturidade Gerenciado**

- A arquitetura de segurança cibernética é eficaz e adaptativa.
- Políticas de segurança cibernética são revisadas e aprimoradas

regularmente.
- Monitoramento em tempo real de ameaças é implementado.
- Uma abordagem de gestão de riscos de segurança cibernética é adotada.
- A equipe de arquitetura de segurança mantém-se atualizada com as ameaças cibernéticas.

**Nível de Maturidade Otimizado**

- A arquitetura de segurança cibernética é altamente otimizada e inovadora.
- Políticas de segurança cibernética são ágeis e adaptáveis às ameaças em constante evolução.
- Monitoramento e resposta automática a ameaças são implementados de forma eficaz.
- A organização é líder em práticas de gestão de riscos de segurança cibernética.
- A arquitetura de segurança cibernética é uma parte integral da cultura organizacional.

A avaliação de maturidade da capability Cybersecurity Architecture é essencial para garantir que a arquitetura de segurança seja robusta, adaptativa e alinhada com as ameaças cibernéticas em constante evolução.

À medida que a maturidade aumenta, a capacidade de proteger as redes, sistemas e dados da organização é aprimorada, fortalecendo a postura de segurança global da organização.

# Convergência com Frameworks de Mercado

A capability Cybersecurity Architecture, pertencente à macro capability Definition & Management e integrada na camada Cybersecurity, é fundamental para a criação e manutenção de uma arquitetura de segurança robusta em organizações.

Esta capability abarca o design e implementação de soluções de segurança para

proteger redes, sistemas e dados, incluindo a integração de tecnologias de segurança, definição de modelos de controle de acesso e a garantia de que a segurança é uma consideração central em todas as iniciativas de TI.

A seguir, é analisada a convergência desta capability em relação a um conjunto dez frameworks de mercado reconhecidos e bem estabelecidos em suas respectivas áreas de expertise:

**COBIT**

- Nível de Convergência: Alto
- Racional: O COBIT enfatiza a governança de TI e contempla diretrizes para a gestão de segurança da informação. A Cybersecurity Architecture está alinhada com este framework, fornecendo a estrutura necessária para implementar as práticas de segurança recomendadas pelo COBIT.

**ITIL**

- Nível de Convergência: Médio
- Racional: Enquanto o ITIL foca na gestão de serviços de TI, a Cybersecurity Architecture complementa este framework, incorporando considerações de segurança nos serviços de TI, especialmente no que tange à gestão de riscos e continuidade dos serviços.

**SAFe**

- Nível de Convergência: Médio
- Racional: O SAFe, voltado para agilidade e desenvolvimento de software, se beneficia da Cybersecurity Architecture ao garantir que as práticas de segurança estejam integradas nos processos de desenvolvimento de software e de entrega de produtos.

**PMI**

- Nível de Convergência: Médio

- Racional: Em projetos gerenciados sob as diretrizes do PMI, a Cybersecurity Architecture ajuda a identificar e mitigar riscos relacionados à segurança em projetos de TI, contribuindo para a gestão eficaz do projeto.

**CMMI**

- Nível de Convergência: Médio
- Racional: O CMMI visa a maturidade e melhoria dos processos de TI. A Cybersecurity Architecture apoia este objetivo ao garantir que as práticas de segurança sejam integradas e evoluam com os processos de TI.

**TOGAF**

- Nível de Convergência: Alto
- Racional: O TOGAF se concentra na arquitetura empresarial, onde a Cybersecurity Architecture é crucial para garantir que a segurança seja integrada na arquitetura de TI e nos processos de tomada de decisão.

**DevOps SRE**

- Nível de Convergência: Médio
- Racional: A Cybersecurity Architecture é relevante em contextos DevOps e SRE, fornecendo uma estrutura de segurança que pode ser integrada nas operações e no desenvolvimento, apoiando práticas seguras e eficientes.

**NIST**

- Nível de Convergência: Alto
- Racional: As diretrizes do NIST para a segurança cibernética estão alinhadas com a Cybersecurity Architecture, especialmente na implementação de controles de segurança robustos e na gestão de riscos.

**Six Sigma**

- Nível de Convergência: Baixo
- Racional: Embora o Six Sigma se concentre na melhoria da qualidade e na redução de defeitos, a Cybersecurity Architecture pode contribuir indiretamente ao reduzir riscos e vulnerabilidades de segurança, melhorando assim a qualidade dos processos de TI.

**Lean IT**

- Nível de Convergência: Baixo
- Racional: Lean IT prioriza a eficiência operacional. A Cybersecurity Architecture, ao garantir a segurança e a integridade dos sistemas de TI, pode contribuir para a eficiência ao prevenir interrupções e perdas relacionadas à segurança.

A Cybersecurity Architecture é essencial no atual cenário de ameaças cibernéticas, não apenas para proteger ativos de TI, mas também para apoiar a agilidade e a inovação nos negócios.

KPIs relevantes incluem o tempo de resposta a incidentes de segurança, a taxa de sucesso na prevenção de ataques e a conformidade com padrões de segurança.

Esta capability desempenha um papel vital na garantia da resiliência e segurança contínuas em um ambiente de TI dinâmico e em constante evolução.

# Processos e Atividades

**Develop Security Architecture Plans**

O desenvolvimento de planos detalhados para a arquitetura de segurança é um passo crucial para garantir que a segurança seja incorporada em todas as fases do desenvolvimento e operações de TI.

Este processo envolve a criação de documentos que descrevem as estratégias,

tecnologias e métodos que serão utilizados para proteger os ativos de TI.

O plano deve considerar as ameaças atuais e emergentes, as vulnerabilidades potenciais e as melhores práticas do setor.

Além disso, o plano deve alinhar-se com os objetivos estratégicos da organização, garantindo que as medidas de segurança apoiem as metas de negócios.

O plano detalhado deve incluir a definição de padrões de segurança, a identificação de tecnologias de segurança necessárias, e a integração dessas tecnologias na infraestrutura existente.

Este processo é essencial para estabelecer uma base sólida para a implementação eficaz da arquitetura de segurança.

- PDCA focus: Plan
- Periodicidade: Anual

| # | Nome da Atividade | Descrição | Inputs | Outputs | RACI | DARE |
|---|---|---|---|---|---|---|
| 1 | Conduct Threat Analysis | Realizar uma análise de ameaças para identificar possíveis riscos de segurança. | Dados de ameaças, relatórios de segurança | Relatório de análise de ameaças | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity |
| 2 | Define Security Standards | Definir padrões de segurança que serão seguidos na arquitetura. | Relatório de análise de ameaças | Documentação de padrões de segurança | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Architecture & Technology Visioning; Informed: All areas | Decider: Cybersecurity; Advisor: Architecture & Technology Visioning; Recommender: Solution Engineering & Development; Executer: Cybersecurity |

| | | | | | | |
|---|---|---|---|---|---|---|
| 3 | Identify Security Technologies | Identificar as tecnologias de segurança necessárias para proteger a infraestrutura de TI. | Documentação de padrões de segurança | Lista de tecnologias de segurança | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Data, AI & New Technology; Executer: Cybersecurity |
| 4 | Develop Integration Plan | Desenvolver um plano de integração para incorporar as tecnologias de segurança na infraestrutura existente. | Lista de tecnologias de segurança | Plano de integração | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Architecture & Technology Visioning; Informed: All areas | Decider: Cybersecurity; Advisor: Architecture & Technology Visioning; Recommender: Solution Engineering & Development; Executer: Cybersecurity |
| 5 | Document Security Architecture | Documentar todos os componentes da arquitetura de segurança, incluindo padrões, tecnologias e integrações planejadas. | Plano de integração | Documentação de arquitetura | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity |

### Identify Security Requirements

A identificação dos requisitos de segurança é uma etapa fundamental para garantir que todas as necessidades de proteção da organização sejam consideradas e abordadas adequadamente.

Este processo envolve a análise dos requisitos regulatórios, das políticas internas e das necessidades específicas de segurança dos diversos sistemas e aplicações.

Os requisitos de segurança devem ser definidos de maneira a garantir a

confidencialidade, integridade e disponibilidade dos dados e sistemas.

Além disso, é importante envolver as partes interessadas para assegurar que os requisitos de segurança estejam alinhados com os objetivos de negócios e as expectativas dos usuários.

A definição clara e precisa dos requisitos de segurança é essencial para orientar o desenvolvimento, a implementação e a manutenção das medidas de segurança na organização.

- PDCA focus: Plan
- Periodicidade: Ad-hoc

| # | Nome da Atividade | Descrição | Inputs | Outputs | RACI | DARE |
|---|---|---|---|---|---|---|
| 1 | Review Regulatory Requirements | Revisar os requisitos regulatórios aplicáveis à segurança cibernética. | Regulamentos, políticas internas | Relatório de requisitos regulatórios | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity |
| 2 | Conduct Risk Assessment | Realizar uma avaliação de riscos para identificar ameaças e vulnerabilidades. | Relatório de requisitos regulatórios | Relatório de avaliação de riscos | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas | Decider: Cybersecurity; Advisor: Architecture & Technology Visioning; Recommender: Solution Engineering & Development; Executer: Cybersecurity |

| | | | | | | |
|---|---|---|---|---|---|---|
| 3 | Identify Business Needs | Identificar as necessidades de negócios relacionadas à segurança. | Relatório de avaliação de riscos | Lista de necessidades de negócios | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity |
| 4 | Define Security Controls | Definir os controles de segurança necessários para atender aos requisitos identificados. | Lista de necessidades de negócios | Lista de controles de segurança | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Architecture & Technology Visioning; Informed: All areas | Decider: Cybersecurity; Advisor: Architecture & Technology Visioning; Recommender: Solution Engineering & Development; Executer: Cybersecurity |
| 5 | Document Security Requirements | Documentar todos os requisitos de segurança definidos para referência futura. | Lista de controles de segurança | Documentação de requisitos | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity |

### Implement Security Architecture

A implementação da arquitetura de segurança conforme planejado é essencial para garantir que todos os componentes e controles de segurança sejam configurados e operem de maneira eficaz.

Este processo envolve a instalação e configuração das tecnologias de segurança identificadas, a aplicação dos padrões de segurança definidos e a integração dessas tecnologias na infraestrutura de TI existente.

A implementação deve ser realizada de forma coordenada e supervisionada para evitar

interrupções nos serviços e garantir que todas as medidas de segurança sejam aplicadas corretamente.

Além disso, é importante realizar testes rigorosos para verificar a eficácia dos controles implementados e fazer ajustes conforme necessário.

A implementação bem-sucedida da arquitetura de segurança fortalece a postura de segurança da organização, protegendo seus ativos contra ameaças cibernéticas.

- PDCA focus: Do
- Periodicidade: Contínua

| # | Nome da Atividade | Descrição | Inputs | Outputs | RACI | DARE |
|---|---|---|---|---|---|---|
| 1 | Install Security Technologies | Instalar as tecnologias de segurança conforme identificado nos planos. | Plano de integração, tecnologias de segurança | Tecnologias instaladas | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity |
| 2 | Configure Security Controls | Configurar os controles de segurança para proteger a infraestrutura de TI. | Tecnologias instaladas | Controles configurados | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Architecture & Technology Visioning; Informed: All areas | Decider: Cybersecurity; Advisor: Architecture & Technology Visioning; Recommender: Solution Engineering & Development; Executer: Cybersecurity |

| | | | | | | |
|---|---|---|---|---|---|---|
| 3 | Apply Security Policies | Aplicar as políticas de segurança em toda a organização. | Controles configurados | Políticas aplicadas | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity |
| 4 | Perform Security Testing | Realizar testes de segurança para verificar a eficácia dos controles implementados. | Políticas aplicadas | Relatórios de testes | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity |
| 5 | Document Implementation | Documentar todas as atividades de implementação para referência futura. | Relatórios de testes | Documentação completa | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity |

### Monitor Architecture Performance

O monitoramento contínuo do desempenho da arquitetura de segurança é essencial para garantir que todas as medidas de segurança estejam funcionando conforme esperado e que a organização esteja protegida contra ameaças emergentes.

Este processo envolve o uso de ferramentas de monitoramento, a análise de logs de segurança e a realização de auditorias regulares para avaliar a eficácia dos controles de segurança implementados.

O monitoramento deve ser proativo, permitindo a detecção precoce de anomalias e a resposta rápida a incidentes de segurança.

Além disso, o monitoramento contínuo fornece insights valiosos sobre o desempenho da arquitetura de segurança e ajuda a identificar áreas de melhoria.

Manter um processo de monitoramento rigoroso é crucial para a manutenção de uma postura de segurança robusta e a proteção contínua dos ativos de TI da organização.

- PDCA focus: Check
- Periodicidade: Contínua

| # | Nome da Atividade | Descrição | Inputs | Outputs | RACI | DARE |
|---|---|---|---|---|---|---|
| 1 | Deploy Monitoring Tools | Implantar ferramentas de monitoramento para acompanhar a arquitetura de segurança. | Ferramentas de monitoramento | Ferramentas implantadas | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity |
| 2 | Analyze Security Logs | Analisar logs de segurança para identificar anomalias e possíveis ameaças. | Ferramentas implantadas | Relatórios de análise de logs | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity |
| 3 | Conduct Security Audits | Realizar auditorias de segurança para avaliar a conformidade e a eficácia dos controles. | Relatórios de análise de logs | Relatórios de auditoria | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | Report Security Metrics | Relatar métricas de segurança à alta gestão para revisão e tomada de decisão. | Relatórios de auditoria | Relatórios de métricas | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity |
| 5 | Implement Improvements | Implementar melhorias com base nos resultados do monitoramento e auditorias. | Relatórios de métricas | Melhorias implementadas | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity |

**Review and Optimize Architecture**

A revisão e otimização contínua da arquitetura de segurança é essencial para garantir que a organização esteja sempre preparada para enfrentar novas ameaças cibernéticas e desafios operacionais.

Este processo envolve a análise dos resultados do monitoramento e auditorias, a avaliação das tendências de segurança emergentes e a implementação de melhorias para fortalecer a arquitetura de segurança.

A revisão deve ser sistemática e abrangente, considerando feedbacks de todas as partes interessadas e ajustando os controles e práticas de segurança conforme necessário.

Otimizar a arquitetura de segurança permite à organização manter uma postura de segurança proativa e adaptável, garantindo a proteção eficaz dos ativos de TI e o suporte contínuo aos objetivos de negócios.

- PDCA focus: Act
- Periodicidade: Contínua

| # | Nome da Atividade | Descrição | Inputs | Outputs | RACI | DARE |
|---|---|---|---|---|---|---|
| 1 | Review Monitoring Results | Revisar os resultados do monitoramento e auditorias para identificar áreas de melhoria. | Relatórios de monitoramento | Relatório de revisão | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity |
| 2 | Assess Emerging Threats | Avaliar ameaças emergentes e ajustar a arquitetura de segurança conforme necessário. | Relatório de revisão | Avaliação de ameaças | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Architecture & Technology Visioning; Informed: All areas | Decider: Cybersecurity; Advisor: Architecture & Technology Visioning; Recommender: Solution Engineering & Development; Executer: Cybersecurity |
| 3 | Implement Security Enhancements | Implementar melhorias de segurança baseadas na avaliação de ameaças e resultados do monitoramento. | Avaliação de ameaças | Melhorias de segurança implementadas | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | Document Changes | Documentar todas as mudanças e melhorias realizadas na arquitetura de segurança. | Melhorias de segurança implementadas | Documentação atualizada | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity |
| 5 | Communicate Updates | Comunicar as atualizações de segurança a todas as partes interessadas e treinar conforme necessário. | Documentação atualizada | Comunicação das atualizações | Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas | Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity |