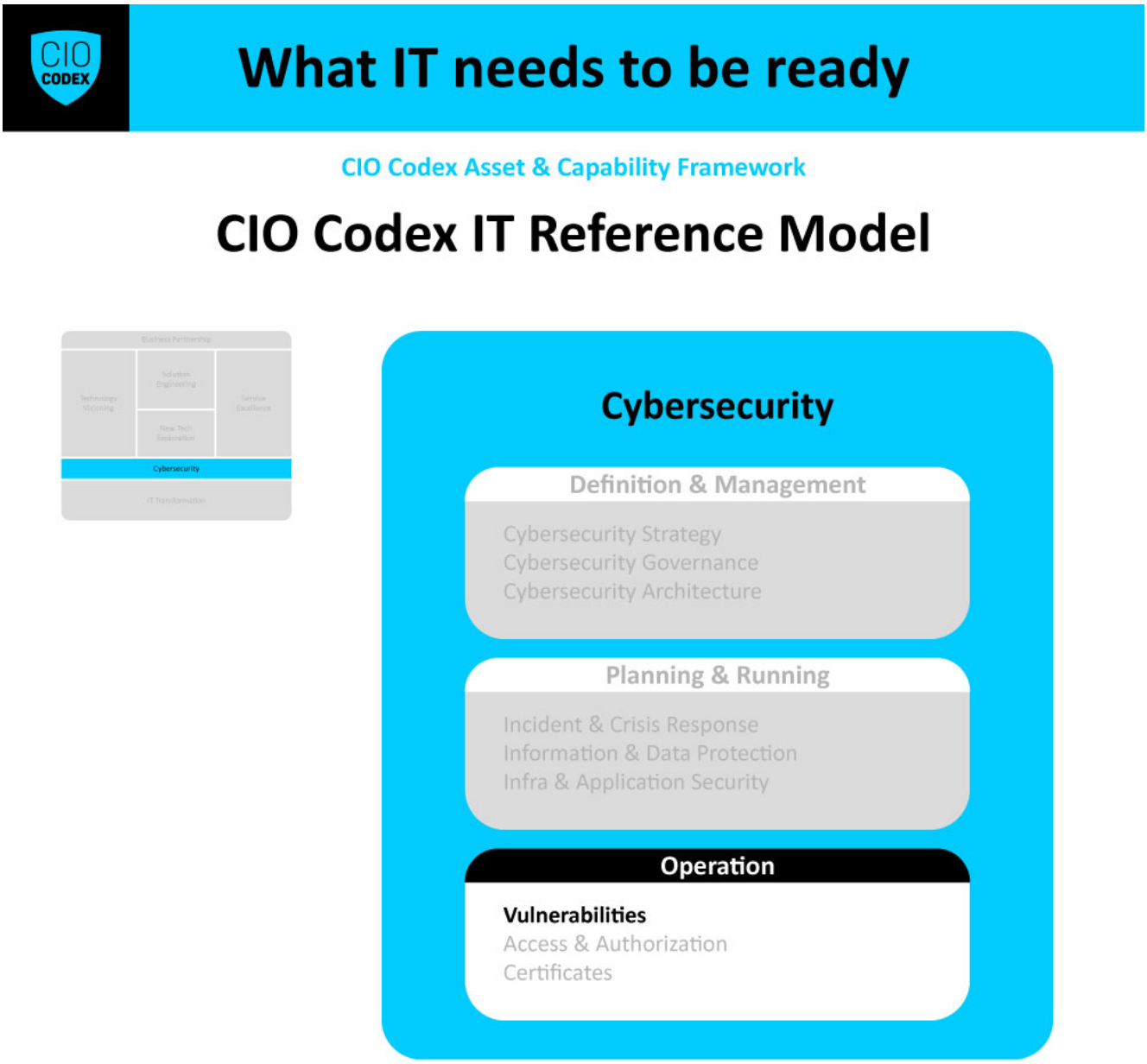

A capability de Vulnerabilities Management, integrada à macro capability Operation e à camada Cybersecurity no CIO Codex Capability Framework, é fundamental para a proteção contra-ataques cibernéticos.

Essa função garante que vulnerabilidades sejam identificadas e tratadas eficazmente, protegendo a infraestrutura de TI e os dados organizacionais contra ameaças dinâmicas e em constante mudança.

No contexto de conceitos fundamentais, Vulnerabilidades de Segurança referem-se a falhas ou fraquezas nos sistemas de TI que podem ser exploradas por atacantes para comprometer a segurança.

Estas podem incluir desde erros de configuração e software desatualizado até códigos maliciosos.

A Avaliação de Risco envolve classificar vulnerabilidades com base em sua severidade e impacto potencial nos sistemas e dados da organização, enquanto a Remediação abrange as ações corretivas, como aplicação de patches, reconfigurações e atualizações de segurança.

Entre as características mais marcantes da Vulnerabilities Management estão a Varredura Automatizada para identificar vulnerabilidades, a Priorização de Vulnerabilidades com base em avaliações de risco, e o Monitoramento Contínuo do ambiente de TI para detectar novas vulnerabilidades assim que emergem.

Uma abordagem colaborativa entre equipes de segurança cibernética, desenvolvimento de software e operações de TI é essencial para garantir uma resposta eficaz.

Além disso, a manutenção de Relatórios e Documentação detalhados é crucial para o registro das vulnerabilidades identificadas e das ações de remediação tomadas.

O propósito principal da Vulnerabilities Management é salvaguardar os ativos de TI contra ameaças cibernéticas, assegurando a integridade e a segurança dos sistemas.

Contribui significativamente para a eficiência operacional, proteção da reputação e dos dados da organização.

Os objetivos no âmbito do CIO Codex Capability Framework incluem a melhoria da eficiência operacional através da automatização do processo de identificação de vulnerabilidades e da priorização de correções, promovendo a inovação ao incorporar práticas de segurança no ciclo de vida de desenvolvimento dos sistemas e oferecendo vantagem competitiva ao demonstrar um compromisso sólido com a segurança cibernética.

O impacto dessa capability nas dimensões tecnológicas é vasto.

Na Infraestrutura, envolve a implementação de ferramentas de varredura de vulnerabilidades que monitoram a infraestrutura de TI em busca de ameaças.

Na Arquitetura, orienta a implementação de modelos de segurança que se integram à arquitetura de sistemas. Nos Sistemas, realiza avaliações de segurança para identificar e classificar vulnerabilidades.

Em Cybersecurity, envolve a identificação, avaliação e correção de pontos fracos que possam ser explorados por atacantes.

E no Modelo Operacional, estabelece processos para priorização e correção de

vulnerabilidades, assegurando uma abordagem organizada e eficaz para mitigar ameaças.

Em suma, a Vulnerabilities Management é uma capability essencial que fornece às organizações as ferramentas e processos necessários para a proteção eficaz contra vulnerabilidades de segurança.

Essa função é crucial para garantir a segurança dos sistemas e dados da organização, contribuindo significativamente para a eficiência operacional, inovação e vantagem competitiva em um ambiente de negócios onde a segurança cibernética é um fator crítico para o sucesso e a confiança.

Conceitos e Características

A capability de Vulnerabilities Management é essencial para prevenir ataques cibernéticos, garantindo que as vulnerabilidades sejam identificadas e abordadas de forma eficaz, protegendo assim a infraestrutura de TI e os dados da organização contra ameaças em constante evolução.

Conceitos

- Vulnerabilidades de Segurança: São falhas ou fraquezas nos sistemas de TI que podem ser exploradas por atacantes para comprometer a segurança. Podem incluir erros de configuração, software desatualizado ou códigos maliciosos.
- Avaliação de Risco: Envolve a classificação das vulnerabilidades com base em sua gravidade e no potencial impacto nos sistemas e nos dados da organização.
- Remediação: Refere-se às ações tomadas para corrigir ou mitigar as vulnerabilidades identificadas, incluindo a aplicação de patches, reconfigurações ou atualizações de segurança.

Características

- Varredura Automatizada: A capability utiliza ferramentas automatizadas para identificar vulnerabilidades nos sistemas, realizando verificações

regulares em busca de ameaças potenciais.
- Priorização de Vulnerabilidades: Com base na avaliação de risco, as vulnerabilidades são classificadas em ordem de importância, permitindo que a equipe concentre seus esforços nas mais críticas.
- Monitoramento Contínuo: A capacidade de monitorar constantemente o ambiente de TI em busca de novas vulnerabilidades à medida que surgem.
- Colaboração: Uma abordagem colaborativa envolvendo equipes de segurança cibernética, desenvolvimento de software e operações de TI para garantir uma resposta eficaz às vulnerabilidades.
- Relatórios e Documentação: Manutenção de registros detalhados das vulnerabilidades identificadas, das ações de remediação tomadas e dos planos de mitigação.

Propósito e Objetivos

A Vulnerabilities Management é uma capability essencial que desempenha um papel crítico na identificação, avaliação e remediação de vulnerabilidades nos sistemas de TI.

Seu propósito fundamental é salvaguardar os ativos de Tecnologia da Informação contra ameaças cibernéticas, assegurando a integridade e a segurança dos sistemas.

Ela contribui significativamente para o negócio, tanto em termos de eficiência operacional quanto na proteção da reputação e dos dados da organização.

Objetivos

Dentro do contexto do CIO Codex Capability Framework, a Vulnerabilities Management busca atingir os seguintes objetivos:

- Eficiência Operacional: Esta capability contribui para a eficiência operacional ao automatizar processos de identificação de vulnerabilidades e priorização de correções. Isso permite que a organização reaja rapidamente a ameaças potenciais, reduzindo o tempo de exposição a riscos.
- Inovação: Promove a inovação ao incorporar práticas de segurança desde

o início do ciclo de vida de desenvolvimento de sistemas. Isso permite que novas tecnologias sejam adotadas com segurança, impulsionando a transformação digital.
- Vantagem Competitiva: Garante uma vantagem competitiva ao demonstrar compromisso com a segurança cibernética, ganhando a confiança de clientes e parceiros. A organização se destaca como um ambiente seguro para a realização de negócios.

Impacto na Tecnologia

A Vulnerabilities Management influencia várias dimensões da tecnologia:

- Infraestrutura: Implementa ferramentas de varredura de vulnerabilidades que monitoram continuamente a infraestrutura de TI em busca de possíveis ameaças.
- Arquitetura: Define modelos de segurança que orientam a arquitetura de sistemas, garantindo que as melhores práticas sejam seguidas desde o início.
- Sistemas: Realiza avaliações de segurança em sistemas existentes, identificando e classificando vulnerabilidades com base no risco.
- Cybersecurity: Gerenciar vulnerabilidades envolve a identificação, avaliação e correção de pontos fracos que podem ser explorados por atacantes.
- Modelo Operacional: Estabelece processos para a priorização e correção de vulnerabilidades, garantindo uma abordagem organizada e eficaz para mitigar ameaças.

Roadmap de Implementação

A capability de Vulnerabilities Management desempenha um papel crucial na proteção da infraestrutura de TI e dos dados da organização contra ameaças cibernéticas em constante evolução.

Para garantir uma implementação bem-sucedida dessa capability, é essencial seguir um roadmap estratégico que leve em consideração os princípios do CIO Codex

Capability Framework, a seguir, as principais etapas desse roadmap:

- Avaliação Inicial: Realize uma avaliação abrangente da infraestrutura de TI e das aplicações existentes para identificar possíveis vulnerabilidades. Isso envolve a revisão de sistemas, redes e configurações para identificar pontos fracos.
- Priorização de Vulnerabilidades: Classifique as vulnerabilidades identificadas com base na gravidade e no potencial impacto nos sistemas e dados da organização. Isso permitirá focar nos problemas mais críticos primeiros.
- Seleção de Ferramentas: Escolha ferramentas de gerenciamento de vulnerabilidades adequadas às necessidades da organização. Essas ferramentas automatizarão a identificação e o monitoramento contínuo de vulnerabilidades.
- Varreduras e Análises: Inicie varreduras regulares de vulnerabilidades em toda a infraestrutura de TI e nas aplicações. As varreduras devem ser acompanhadas por análises detalhadas para confirmar a existência e a gravidade das vulnerabilidades.
- Desenvolvimento de Políticas: Elabore políticas de gerenciamento de vulnerabilidades que definam procedimentos claros para a identificação, avaliação e remediação de vulnerabilidades.
- Equipe de Resposta a Vulnerabilidades: Crie uma equipe dedicada para lidar com a gestão de vulnerabilidades, incluindo representantes das áreas de segurança cibernética, desenvolvimento de software e operações de TI.
- Implementação de Patches e Correções: Desenvolva um processo ágil para aplicar patches de segurança e correções de vulnerabilidades de forma rápida e eficaz, minimizando o tempo de exposição a riscos.
- Monitoramento Contínuo: Estabeleça sistemas de monitoramento contínuo para identificar novas vulnerabilidades à medida que surgem e garantir que as correções sejam aplicadas de forma oportuna.
- Relatórios e Documentação: Mantenha registros detalhados de todas as vulnerabilidades identificadas, das ações de remediação tomadas e dos planos de mitigação. Isso é essencial para auditorias e relatórios regulatórios.
- Treinamento e Conscientização: Promova a conscientização sobre segurança cibernética entre os funcionários e forneça treinamento

regular sobre as políticas e procedimentos de gerenciamento de vulnerabilidades.
- Aprimoramento Contínuo: Estabeleça um ciclo de melhoria contínua, revisando regularmente as políticas e procedimentos de gerenciamento de vulnerabilidades com base nas lições aprendidas e nas mudanças no cenário de ameaças.
- Conformidade Regulatória: Assegure-se de que todas as práticas de gerenciamento de vulnerabilidades estejam em conformidade com as regulamentações aplicáveis, como GDPR, LGPD e outras normas de segurança.

A implementação eficaz da Vulnerabilities Management não apenas protegerá a organização contra ameaças cibernéticas, mas também contribuirá para a eficiência operacional, inovação e vantagem competitiva.

Esta capability é um pilar fundamental da cibersegurança, garantindo a integridade e a segurança dos sistemas e dados da organização.

Melhores Práticas de Mercado

No contexto do CIO Codex Capability Framework, a capability de Vulnerabilities Management desempenha um papel crítico na proteção dos sistemas de TI e dados da organização contra ameaças cibernéticas, garantindo que as vulnerabilidades sejam identificadas e tratadas de maneira eficaz.

Para alcançar um nível efetivo de gerenciamento de vulnerabilidades, é essencial adotar as melhores práticas de mercado que são amplamente reconhecidas e implementadas por organizações líderes em todo o mundo.

Abaixo estão as principais melhores práticas dentro dessa capability:

- Varreduras e Avaliações Regulares: Realize varreduras automáticas e avaliações regulares de vulnerabilidades em todos os sistemas e aplicativos para identificar potenciais pontos fracos. Isso inclui varreduras de rede, análises de código e testes de penetração.
- Priorização Baseada em Risco: Classifique as vulnerabilidades identificadas com base em sua gravidade e no potencial impacto nos

sistemas e dados da organização. Concentre-se nas vulnerabilidades mais críticas e que representam maior risco.

- Automação de Fluxo de Trabalho: Implemente fluxos de trabalho de automação para o tratamento de vulnerabilidades, incluindo a atribuição de tarefas, a aplicação de patches e a comunicação eficaz entre equipes de segurança e TI.
- Monitoramento Contínuo: Mantenha o monitoramento contínuo do ambiente de TI em busca de novas vulnerabilidades à medida que surgem. Isso garante uma resposta ágil a ameaças emergentes.
- Integração com Desenvolvimento Seguro: Integre práticas de gerenciamento de vulnerabilidades ao ciclo de vida de desenvolvimento de software, identificando e corrigindo vulnerabilidades desde o início.
- Comunicação Efetiva: Estabeleça uma comunicação eficaz entre as equipes de segurança cibernética, desenvolvimento de software e operações de TI para garantir uma resposta coordenada a vulnerabilidades.
- Testes de Controle de Segurança: Realize testes de controle de segurança para verificar a eficácia das correções e das medidas de remediação aplicadas às vulnerabilidades.
- Avaliação de Terceiros: Avalie regularmente fornecedores e parceiros quanto às práticas de gerenciamento de vulnerabilidades, garantindo que terceiros não representem um risco para a organização.
- Treinamento e Conscientização: Forneça treinamento e conscientização em segurança cibernética para todos os funcionários, a fim de promover a cultura de segurança e a colaboração na identificação de vulnerabilidades.
- Documentação e Relatórios: Mantenha registros detalhados das vulnerabilidades identificadas, das ações de remediação tomadas e dos planos de mitigação. Isso é essencial para a auditoria e conformidade.
- Avaliação Pós-Incidente: Após incidentes de segurança, avalie as vulnerabilidades exploradas e as medidas de remediação adotadas para evitar futuros ataques semelhantes.

A adoção dessas melhores práticas de mercado dentro da capability de Vulnerabilities Management é crucial para fortalecer a postura de segurança cibernética de uma organização, garantindo que sistemas e dados permaneçam protegidos contra ameaças em constante evolução.

Além disso, contribui para a eficiência operacional e a proteção da reputação da organização no mercado.

Desafios Atuais

A Capability de Vulnerabilities Management desempenha um papel crítico na prevenção de ataques cibernéticos, identificando e tratando vulnerabilidades de segurança nos sistemas de TI.

No entanto, ao adotar e integrar essa capability em seus processos de negócios e operações de TI, as organizações enfrentam diversos desafios atuais de mercado.

A seguir, os principais desafios com base nas melhores práticas do mercado:

- Complexidade das Vulnerabilidades: A crescente complexidade das vulnerabilidades de segurança, incluindo ameaças de dia zero, torna a identificação e mitigação mais desafiadoras.
- Volume de Dados: A quantidade massiva de dados gerados pelas ferramentas de varredura de vulnerabilidades pode sobrecarregar as equipes de segurança, tornando difícil a priorização e tratamento adequado das vulnerabilidades.
- Priorização Eficiente: A necessidade de priorizar as vulnerabilidades com base em sua gravidade e no impacto potencial é um desafio constante, garantindo que as mais críticas sejam tratadas primeiro.
- Atualizações e Patches: Garantir a aplicação oportuna de atualizações e patches de segurança é um desafio, especialmente em ambientes complexos e altamente regulamentados.
- Integração com DevOps: A integração da segurança de vulnerabilidades nos processos DevOps é essencial para o desenvolvimento seguro, mas requer coordenação e colaboração eficazes.
- Falsos Positivos: Lidar com falsos positivos nas ferramentas de varredura de vulnerabilidades consome tempo e recursos preciosos da equipe de segurança.
- Educação e Conscientização: A falta de conscientização e treinamento em segurança cibernética entre os funcionários pode levar a erros que introduzem novas vulnerabilidades.

- Ciclo de Vida de Aplicações: Gerenciar vulnerabilidades em aplicações legadas e em constante evolução requer diferentes abordagens e recursos.
- Integração de Diversas Fontes de Dados: Consolidar dados de várias fontes, como scanners de vulnerabilidades, sistemas de registro de incidentes e feeds de ameaças, é um desafio de integração.
- Escassez de Profissionais de Segurança: A escassez de profissionais de segurança qualificados dificulta a construção e manutenção de equipes de Vulnerabilities Management eficazes.

Esses desafios destacam a importância da Capability de Vulnerabilities Management em um mundo cibernético em constante evolução.

Superá-los requer a implementação de processos automatizados de identificação de vulnerabilidades, uma abordagem colaborativa entre equipes de segurança, desenvolvimento e operações, além de educação contínua em segurança cibernética para todos os membros da organização.

A capability de gerenciar vulnerabilidades com eficácia é essencial para garantir a integridade e a segurança dos sistemas de TI, protegendo assim os ativos de informação críticos da organização contra ameaças em constante evolução.

Tendências para o Futuro

A Capability de Vulnerabilities Management, inserida na macro capability de Operation e na camada de Cybersecurity, desempenha um papel crucial na prevenção de ataques cibernéticos, identificando e mitigando vulnerabilidades nos sistemas de TI.

Neste contexto, é essencial antecipar as tendências futuras que moldarão o desenvolvimento dessa capability, de acordo com as expectativas do mercado e as necessidades de segurança cibernética.

A seguir, as principais tendências para o futuro:

- Inteligência Artificial na Identificação de Vulnerabilidades: A utilização de algoritmos de IA avançados será amplamente adotada para identificar vulnerabilidades de forma mais precisa e rápida, permitindo uma resposta mais eficiente a ameaças emergentes.

- Automatização na Remediação de Vulnerabilidades: A automação será aplicada não apenas na identificação, mas também na remediação de vulnerabilidades de baixa complexidade, acelerando a correção de falhas comuns.
- Análise de Comportamento para Identificação de Ameaças: Soluções de análise de comportamento serão empregadas para detectar atividades anômalas nos sistemas, permitindo a identificação de ameaças que evitam detecção por métodos tradicionais.
- Zero Trust em Vulnerabilities Management: A abordagem Zero Trust será aplicada à Vulnerabilities Management, garantindo que a confiança seja constantemente verificada e não presumida, mesmo dentro da rede corporativa.
- Integração com DevSecOps: A integração entre Vulnerabilities Management e práticas DevSecOps será aprofundada, assegurando que as vulnerabilidades sejam tratadas desde o desenvolvimento inicial, evitando problemas no futuro.
- Priorização Inteligente de Vulnerabilidades: Técnicas avançadas de análise de risco serão aplicadas para priorizar vulnerabilidades com base em seu potencial impacto nos negócios, permitindo que as equipes concentrem seus esforços nas mais críticas.
- Automatização na Análise de Vulnerabilidades de Código: Ferramentas de análise estática e dinâmica de código serão aprimoradas com automação avançada, identificando vulnerabilidades de código de forma mais precisa.
- Orquestração de Resposta a Incidentes: A orquestração na resposta a incidentes relacionados a vulnerabilidades será mais comum, permitindo uma ação coordenada e rápida em cenários de ameaça.
- Segurança em Nuvem e Containerization: A segurança de ambientes em nuvem e de contêineres será incorporada às práticas de Vulnerabilities Management, refletindo a evolução das infraestruturas tecnológicas.
- Avaliação Contínua de Fornecedores: A avaliação contínua das vulnerabilidades associadas a fornecedores será uma tendência, garantindo que terceiros não introduzam riscos na cadeia de suprimentos de TI.

Essas tendências refletem as expectativas do mercado em relação à evolução da Capability de Vulnerabilities Management.

À medida que as ameaças cibernéticas continuam a se sofisticar, a capacidade de identificar e mitigar vulnerabilidades de forma proativa se torna fundamental para proteger a infraestrutura de TI e os dados da organização.

KPIs Usuais

A capability de Vulnerabilities Management é um pilar fundamental da camada de Cybersecurity no contexto da macro capability Operation.

Sua importância reside na identificação, avaliação e remediação de vulnerabilidades de segurança nos sistemas de TI, contribuindo para a proteção da infraestrutura e dos dados da organização contra ameaças cibernéticas.

Para mensurar o sucesso dessa capability, é necessário acompanhar uma série de KPIs usuais que fornecem insights valiosos sobre a eficácia das operações de gerenciamento de vulnerabilidades.

Abaixo, uma lista dos principais KPIs usualmente utilizados no mercado dentro do contexto do CIO Codex Capability Framework:

- Taxa de Identificação de Vulnerabilidades (Vulnerability Identification Rate): Mede a eficácia da capacidade em identificar vulnerabilidades nos sistemas de TI da organização ao longo do tempo.
- Taxa de Classificação de Risco (Risk Classification Rate): Avalia a capacidade de classificar as vulnerabilidades com base em sua gravidade e no potencial impacto nos sistemas e dados.
- Tempo Médio de Resposta a Vulnerabilidades (Mean Time to Remediate Vulnerabilities): Calcula o tempo médio necessário para a equipe de segurança remediação de vulnerabilidades após a identificação.
- Taxa de Cumprimento de Políticas de Segurança (Security Policy Compliance Rate): Avalia a conformidade com as políticas de segurança da organização relacionadas a vulnerabilidades.
- Taxa de Vulnerabilidades Críticas Remediadas (Critical Vulnerabilities Remediated Rate): Indica a frequência com que as vulnerabilidades críticas são corrigidas em relação ao total identificado.
- Taxa de Varreduras de Vulnerabilidade Concluídas (Completed Vulnerability Scans Rate): Mede a regularidade das varreduras de

vulnerabilidades realizadas nos sistemas de TI.

- Taxa de Atualização de Patches (Patch Update Rate): Avalia a rapidez com que as atualizações de segurança são aplicadas após sua disponibilização.
- Taxa de Vulnerabilidades Recorrentes (Recurring Vulnerabilities Rate): Indica a frequência com que as mesmas vulnerabilidades reaparecem após a remediação.
- Taxa de Adoção de Melhores Práticas (Best Practices Adoption Rate): Avalia a implementação de melhores práticas de segurança recomendadas pela indústria.
- Tempo Médio de Avaliação de Risco (Mean Time for Risk Assessment): Calcula o tempo médio necessário para avaliar o risco de vulnerabilidades após sua identificação.
- Taxa de Vulnerabilidades Não Corrigidas (Unresolved Vulnerabilities Rate): Indica a porcentagem de vulnerabilidades identificadas que permanecem não corrigidas.
- Taxa de Relatórios de Vulnerabilidades (Vulnerability Reporting Rate): Mede a frequência com que relatórios de vulnerabilidades são gerados e compartilhados com as partes interessadas.
- Taxa de Colaboração Interdepartamental (Interdepartmental Collaboration Rate): Avalia a colaboração entre equipes de segurança cibernética, desenvolvimento de software e operações de TI para lidar com vulnerabilidades.
- Taxa de Cumprimento de SLAs de Remediação (Remediation SLA Compliance Rate): Indica a conformidade com os acordos de nível de serviço (SLAs) estabelecidos para a remediação de vulnerabilidades.
- Taxa de Treinamento em Gerenciamento de Vulnerabilidades (Vulnerability Management Training Rate): Avalia a porcentagem de membros da equipe que receberam treinamento em gerenciamento de vulnerabilidades.

Esses KPIs desempenham um papel fundamental na avaliação do desempenho da Vulnerabilities Management.

Eles fornecem uma visão abrangente das operações de segurança cibernética, ajudando as organizações a identificarem áreas de melhoria, priorizar a remediação de vulnerabilidades críticas e manter a integridade de seus sistemas de TI e dados.

A medição constante desses indicadores é essencial para manter um ambiente seguro

em um mundo digital em constante evolução.

Exemplos de OKRs

A capability de Vulnerabilities Management na macro capability Operation da camada Cybersecurity desempenha um papel fundamental na identificação, avaliação e remediação de vulnerabilidades nos sistemas de TI.

Essa capability envolve a constante varredura e análise dos sistemas para descobrir falhas de segurança, classificá-las com base no risco que representam e implementar as correções necessárias.

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

Identificação Contínua de Vulnerabilidades

Objetivo: Garantir que todas as vulnerabilidades sejam identificadas e documentadas.

- KR1: Realizar varreduras regulares de vulnerabilidades em todos os sistemas.
- KR2: Utilizar ferramentas de verificação de segurança atualizadas.
- KR3: Manter um registro centralizado de todas as vulnerabilidades identificadas.

Avaliação de Riscos e Priorização de Correções

Objetivo: Priorizar as correções com base no risco e na criticidade.

- KR1: Classificar as vulnerabilidades de acordo com o seu impacto potencial.
- KR2: Estabelecer critérios de priorização claros.
- KR3: Garantir que as vulnerabilidades críticas sejam corrigidas imediatamente.

Implementação de Correções e Patches

Objetivo: Assegurar que as correções sejam aplicadas de forma eficaz.

- KR1: Implementar correções de segurança de acordo com os procedimentos padrão.
- KR2: Realizar testes de regressão após a aplicação das correções.
- KR3: Monitorar para garantir que as correções tenham sido aplicadas em todos os sistemas afetados.

Acompanhamento e Verificação de Correções

Objetivo: Certificar-se de que as correções tenham sido eficazes.

- KR1: Verificar se as vulnerabilidades foram corrigidas com sucesso.
- KR2: Monitorar o ambiente para garantir que as vulnerabilidades não ressurgiram.
- KR3: Realizar auditorias de conformidade regularmente.

Relatórios e Comunicação

Objetivo: Manter as partes interessadas informadas sobre o status das vulnerabilidades.

- KR1: Gerar relatórios regulares de status de vulnerabilidades.
- KR2: Comunicar vulnerabilidades críticas aos responsáveis pela tomada de decisão.
- KR3: prover orientações de mitigação para vulnerabilidades não corrigidas.

Através desses OKRs, a capability de Vulnerabilities Management visa prevenir ataques cibernéticos, garantir a integridade dos sistemas de TI e reduzir os riscos de segurança.

A abordagem sistemática e proativa para identificar e remediar vulnerabilidades é essencial para manter um ambiente de TI seguro e resiliente.

Critérios para Avaliação de Maturidade

A capability Vulnerabilities Management, inserida na macro capability Operation e na camada Cybersecurity, desempenha um papel crítico na identificação, avaliação e remediação de vulnerabilidades nos sistemas de TI.

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 processos para identificar vulnerabilidades.
- Ausência de varreduras de segurança nos sistemas.
- Falta de classificação de vulnerabilidades com base no risco.
- Não há correções implementadas para falhas de segurança.
- Inexistência de registros de vulnerabilidades.

Nível de Maturidade Inicial

- Alguns esforços iniciais para identificar vulnerabilidades, mas sem processos definidos.
- Varreduras esporádicas de segurança.
- Classificação limitada das vulnerabilidades quanto ao risco.
- Implementação de correções de forma reativa.
- Registros rudimentares de vulnerabilidades.

Nível de Maturidade Definido

- Processos formalizados para identificação de vulnerabilidades.
- Varreduras de segurança regulares e documentadas.
- Classificação das vulnerabilidades com base no risco estabelecida.
- Implementação de correções planejadas e controladas.
- Registros abrangentes de vulnerabilidades e ações corretivas.

Nível de Maturidade Gerenciado

- Processos de identificação de vulnerabilidades eficazes e eficientes.
- Varreduras de segurança automatizadas e monitoradas.
- Classificação precisa e dinâmica das vulnerabilidades.
- Implementação de correções proativa e monitoramento contínuo.
- Análise de tendências e relatórios de vulnerabilidades.

Nível de Maturidade Otimizado

- Processos de identificação de vulnerabilidades altamente otimizados e integrados.
- Varreduras de segurança em tempo real e resposta automática a ameaças.
- Classificação dinâmica e adaptativa das vulnerabilidades com base em inteligência de ameaças.
- Implementação de correções em tempo real e análise de impacto mínima.
- Inteligência de vulnerabilidades utilizada para aprimorar a postura de segurança.

A avaliação de maturidade da capability Vulnerabilities Management é essencial para garantir que a organização seja capaz de identificar e remediar vulnerabilidades de forma eficaz, reduzindo o risco de ataques cibernéticos e garantindo a integridade dos sistemas de TI.

À medida que a maturidade aumenta, a capacidade de resposta às vulnerabilidades se torna mais ágil e eficiente.

Convergência com Frameworks de Mercado

A capability Vulnerabilities Management, integrada à macro capability Operation e situada na camada Cybersecurity, é crucial para a identificação, avaliação e remediação de vulnerabilidades nos sistemas de TI.

Esta capability engloba a constante varredura e análise dos sistemas para descobrir falhas de segurança, classificando-as com base no risco e implementando correções necessárias, sendo essencial para prevenir ataques cibernéticos e garantir a integridade dos sistemas.

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, incluindo a gestão de riscos e segurança da informação. A Vulnerabilities Management alinha-se com o COBIT na identificação e mitigação de riscos de segurança, fortalecendo as práticas de governança de TI.

ITIL

- Nível de Convergência: Médio
- Racional: O ITIL fornece um framework de gestão de serviços de TI, abordando aspectos de segurança em seus processos. A capability integra-se ao ITIL ao garantir a identificação e remediação de vulnerabilidades, contribuindo para a melhoria contínua dos serviços de TI.

SAFe

- Nível de Convergência: Médio
- Racional: O SAFe, como um framework de desenvolvimento ágil, inclui práticas de segurança em seus processos. A Vulnerabilities Management complementa o SAFe ao assegurar que as práticas de segurança sejam integradas nas fases de planejamento e desenvolvimento.

PMI

- Nível de Convergência: Médio
- Racional: A metodologia do PMI para a gestão de projetos pode integrar a Vulnerabilities Management para garantir que os projetos de TI incorporem práticas eficazes de identificação e remediação de vulnerabilidades.

CMMI

- Nível de Convergência: Médio
- Racional: O CMMI, focado na maturidade dos processos, se beneficia da Vulnerabilities Management para incorporar práticas de segurança robustas nos processos de desenvolvimento e gestão.

TOGAF

- Nível de Convergência: Médio
- Racional: O TOGAF, que lida com a arquitetura empresarial, se alinha com a Vulnerabilities Management ao incluir considerações de segurança na arquitetura de TI, promovendo a proteção contra vulnerabilidades.

DevOps SRE

- Nível de Convergência: Médio
- Racional: Em DevOps SRE, a rapidez e a entrega contínua são essenciais. A Vulnerabilities Management é crucial para manter a segurança dos processos de desenvolvimento e operação.

NIST

- Nível de Convergência: Alto
- Racional: O NIST fornece diretrizes detalhadas para segurança cibernética. A capability alinha-se ao NIST ao adotar práticas rigorosas para a identificação e remediação de vulnerabilidades, assegurando a segurança dos sistemas de TI.

Six Sigma

- Nível de Convergência: Baixo
- Racional: O Six Sigma foca na melhoria da qualidade e eficiência dos processos. Embora a Vulnerabilities Management tenha uma convergência limitada, contribui para a minimização de riscos e falhas de segurança nos processos.

Lean IT

- Nível de Convergência: Baixo
- Racional: Lean IT, com seu foco em eficiência operacional, tem uma convergência limitada com a Vulnerabilities Management. Contudo, práticas de segurança eficazes podem ajudar a eliminar desperdícios e melhorar a eficiência.

A capability Vulnerabilities Management desempenha um papel crítico na proteção contra ameaças cibernéticas, mantendo a segurança dos dados e sistemas críticos.

KPIs relevantes podem incluir a frequência de descoberta de vulnerabilidades, tempo médio para remediação e eficácia das medidas de segurança implementadas.

Esta capability é fundamental para manter a resiliência cibernética em um ambiente de ameaças em constante evolução.

Processos e Atividades

Develop Vulnerability Management Plans

O desenvolvimento de planos detalhados para a gestão de vulnerabilidades é um processo essencial para garantir que a organização esteja preparada para identificar, avaliar e mitigar vulnerabilidades de segurança.

Este processo envolve a criação de um framework abrangente que define as políticas, procedimentos e responsabilidades para a gestão de vulnerabilidades.

Começa com a análise dos riscos e a identificação das vulnerabilidades potenciais nos sistemas de TI.

Em seguida, são definidos os objetivos de segurança, as estratégias de mitigação e as prioridades de remediação.

O plano também deve incluir a integração de ferramentas automatizadas para varredura de vulnerabilidades, bem como a definição de um cronograma para avaliações regulares.

A documentação completa do plano garante que todos os stakeholders estejam cientes de suas responsabilidades e das medidas a serem adotadas para proteger a infraestrutura de TI contra ameaças cibernéticas.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Conduct Risk Analysis	Realizar uma análise de riscos para identificar vulnerabilidades potenciais.	Dados de risco, análise de ameaças	Relatório de análise de riscos	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 Objectives	Definir objetivos de segurança alinhados aos requisitos de negócios e regulatórios.	Relatório de análise de riscos	Objetivos de segurança definidos	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Architecture & Technology Visioning; Informed: All areas	Decider: Cybersecurity; Advisor: Architecture & Technology Visioning; Recommender: Solution Engineering & Development; Executer: Cybersecurity

3	Develop Mitigation Strategies	Desenvolver estratégias de mitigação para lidar com as vulnerabilidades identificadas.	Objetivos de segurança definidos	Estratégias de mitigação	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
4	Establish Priorities	Estabelecer prioridades de remediação com base na gravidade das vulnerabilidades.	Estratégias de mitigação	Prioridades estabelecidas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
5	Document Vulnerability Plan	Documentar o plano de gestão de vulnerabilidades de forma detalhada.	Prioridades estabelecidas	Plano de gestão de vulnerabilidades	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Identify Vulnerability Scenarios

A identificação dos cenários de vulnerabilidades é um processo fundamental para entender os diferentes tipos de ameaças que podem afetar a infraestrutura de TI da organização.

Este processo envolve a utilização de ferramentas automatizadas de varredura de vulnerabilidades, além da análise manual de especialistas em segurança cibernética.

Os cenários de vulnerabilidades devem ser classificados com base em sua gravidade e no potencial impacto nos sistemas e dados da organização.

A identificação precisa desses cenários permite a criação de estratégias de mitigação

eficazes e a priorização dos esforços de remediação.

A colaboração entre as equipes de TI e de segurança cibernética é crucial para garantir que todas as possíveis vulnerabilidades sejam identificadas e abordadas de forma adequada.

- PDCA focus: Plan
- Periodicidade: Semestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Conduct Automated Scans	Realizar varreduras automatizadas para identificar vulnerabilidades nos sistemas de TI.	Ferramentas de varredura, dados de sistema	Relatórios de varredura	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
2	Perform Manual Analysis	Executar análise manual de especialistas para identificar vulnerabilidades não detectadas automaticamente.	Relatórios de varredura	Relatórios de análise manual	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Classify Vulnerabilities	Classificar as vulnerabilidades com base em sua gravidade e impacto potencial.	Relatórios de análise manual	Vulnerabilidades classificadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity

4	Document Vulnerability Scenarios	Documentar os cenários de vulnerabilidades identificados de forma detalhada.	Vulnerabilidades classificadas	Documentação de cenários	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
5	Review Scenarios with Stakeholders	Revisar os cenários de vulnerabilidades com as partes interessadas para validação e priorização.	Documentação de cenários	Cenários revisados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Execute Vulnerability Assessments

A execução das avaliações de vulnerabilidades conforme planejado é crucial para identificar as fraquezas nos sistemas de TI e implementar medidas corretivas antes que possam ser exploradas por atacantes.

Este processo envolve a realização de varreduras regulares e detalhadas nos sistemas, a aplicação de testes de penetração para identificar vulnerabilidades em profundidade e a análise dos resultados para definir as ações de remediação.

A colaboração entre as equipes de segurança cibernética, desenvolvimento de software e operações de TI é fundamental para garantir que todas as áreas críticas sejam avaliadas e protegidas.

A documentação e o relatório detalhado das avaliações realizadas são essenciais para manter um histórico das vulnerabilidades identificadas e das ações tomadas para mitigá-las.

- PDCA focus: Do
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Perform Regular Scans	Realizar varreduras regulares de vulnerabilidades nos sistemas de TI.	Ferramentas de varredura, dados de sistema	Relatórios de varredura	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
2	Conduct Penetration Testing	Realizar testes de penetração para identificar vulnerabilidades em profundidade.	Relatórios de varredura	Relatórios de testes de penetração	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Analyze Assessment Results	Analisar os resultados das avaliações de vulnerabilidades para definir ações corretivas.	Relatórios de testes de penetração	Relatórios de análise	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity

4	Implement Remediation Actions	Implementar ações de remediação para corrigir as vulnerabilidades identificadas.	Relatórios de análise	Ações de remediação implementadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
5	Document and Report Findings	Documentar e relatar os resultados das avaliações e as ações de remediação para as partes interessadas.	Ações de remediação implementadas	Relatórios de avaliação	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Monitor Vulnerability Management Performance

O monitoramento contínuo do desempenho da gestão de vulnerabilidades é essencial para garantir a eficácia das medidas implementadas e identificar áreas que necessitam de ajuste.

Este processo envolve a coleta e análise de dados sobre a performance dos controles de segurança, incluindo a eficácia das varreduras automatizadas e dos testes de penetração.

As auditorias regulares e a análise de logs são componentes chave deste processo.

O feedback obtido através do monitoramento permite ajustes e melhorias contínuas, assegurando que a organização esteja sempre protegida contra novas ameaças.

A comunicação regular dos resultados do monitoramento para as partes interessadas é crucial para manter a transparência e a confiança.

- PDCA focus: Check
- Periodicidade: Mensal

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Collect Performance Data	Coletar dados de desempenho das soluções de segurança implementadas.	Logs de segurança, relatórios de auditoria	Dados de desempenho coletados	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	Analyze Security Metrics	Analisar as métricas de segurança para avaliar a eficácia das soluções implementadas.	Dados de desempenho coletados	Relatórios de análise de métricas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Conduct Security Audits	Realizar auditorias de segurança para identificar possíveis vulnerabilidades e não conformidades.	Relatórios de análise de métricas	Relatórios de auditoria	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

4	Generate Improvement Reports	Gerar relatórios de melhoria com base na análise de desempenho e auditorias realizadas.	Relatórios de auditoria	Relatórios de melhoria	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
5	Report Findings	Relatar as descobertas e recomendações de melhoria para a alta gestão e partes interessadas.	Relatórios de melhoria	Relatórios de descobertas	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 Improve Vulnerability Management Practices

A revisão e otimização contínua das práticas de gestão de vulnerabilidades são fundamentais para manter a eficácia das medidas de proteção e se adaptar a novas ameaças.

Este processo envolve a análise dos resultados do monitoramento e das auditorias para identificar áreas de melhoria.

As lições aprendidas são integradas aos procedimentos existentes e novos controles de segurança são desenvolvidos conforme necessário.

O processo inclui também a atualização das políticas e procedimentos de segurança, a realização de treinamentos regulares e a validação das práticas de segurança através de testes contínuos.

A melhoria contínua assegura que a organização esteja sempre preparada para proteger sua infraestrutura e aplicações contra ameaças emergentes.

- PDCA focus: Act
- Periodicidade: Trimestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Analyze Audit Findings	Analisar as descobertas das auditorias e monitoramento de desempenho.	Relatórios de auditoria	Análise de descobertas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
2	Identify Improvement Areas	Identificar áreas de melhoria nos processos de segurança com base na análise.	Análise de descobertas	Lista de áreas de melhoria	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Update Security Procedures	Atualizar os procedimentos de segurança para incorporar as melhorias identificadas.	Lista de áreas de melhoria	Procedimentos atualizados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Data, AI & New Technology; Executer: Cybersecurity

4	Conduct Training Sessions	Realizar sessões de treinamento para assegurar que a equipe esteja familiarizada com os procedimentos atualizados.	Procedimentos atualizados	Sessões de treinamento realizadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
5	Validate Security Practices	Validar as práticas de segurança através de testes e auditorias contínuas.	Procedimentos atualizados	Práticas validadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity