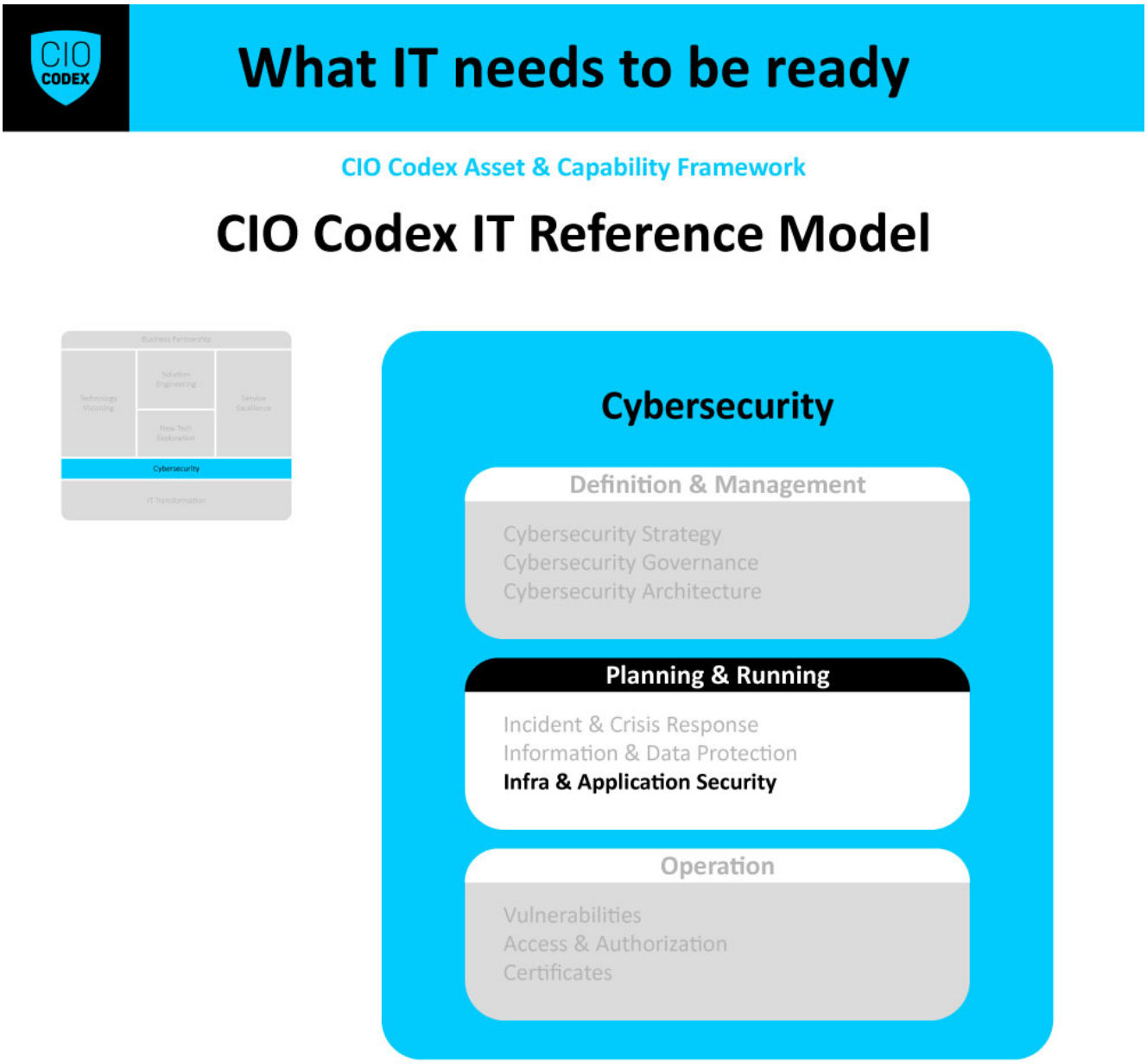

A capability de Infrastructure & Application Security, inserida na macro capability Planning & Running e pertencente à camada Cybersecurity do CIO Codex Capability Framework, é de suma importância para assegurar a integridade e a disponibilidade dos sistemas e aplicações de uma organização, protegendo-os contra vulnerabilidades e ameaças internas e externas.

Essa função é vital para manter as operações da organização seguras e eficientes, diante do cenário de ameaças cibernéticas em constante evolução.

Dentro dos conceitos principais, a Segurança da Infraestrutura de TI abrange as práticas e tecnologias aplicadas para salvaguardar servidores, redes, sistemas operacionais e outros componentes da infraestrutura de TI.

Já a Segurança de Aplicações se concentra em medidas de segurança implementadas no desenvolvimento e operação de softwares para reduzir riscos de vulnerabilidades e ataques.

O uso de Firewalls, dispositivos ou softwares que controlam o tráfego de rede com base em regras de segurança, também é um componente crucial desta capability.

As características distintivas incluem Sistemas de Detecção e Prevenção de Intrusões (IDS/IPS) para monitoramento e ação contra atividades suspeitas, a Criptografia para a proteção de dados em trânsito e em repouso, e o Desenvolvimento Seguro que integra práticas de segurança desde o início do ciclo de vida do desenvolvimento de software.

A Auditoria de Segurança é fundamental para monitorar a infraestrutura e as aplicações, enquanto a Gestão de Identidade e Acesso assegura que apenas indivíduos autorizados tenham acesso aos dados e sistemas críticos.

O propósito principal da Infrastructure & Application Security é garantir que a infraestrutura de TI e as aplicações estejam protegidas contra ameaças cibernéticas, mantendo a integridade, confidencialidade e disponibilidade dos sistemas críticos da organização.

Esta capability desempenha um papel crucial na manutenção da operação contínua e na redução de riscos relacionados à segurança da informação.

Os objetivos definidos dentro do contexto do CIO Codex Capability Framework incluem garantir a eficiência operacional através da implementação de medidas de segurança que se integrem às operações de TI sem comprometê-las, promover a inovação ao incorporar práticas de segurança no desenvolvimento de aplicações, e oferecer uma vantagem competitiva, uma vez que sistemas confiáveis e seguros são um diferencial importante para clientes e parceiros de negócios.

No que diz respeito ao impacto tecnológico, a Infrastructure & Application Security afeta várias dimensões da tecnologia.

Na Infraestrutura, implementa firewalls e sistemas IDS/IPS para proteger contra-ataques cibernéticos. Na Arquitetura, define e implementa modelos de segurança que se integram à arquitetura de sistemas.

Nos Sistemas, aplica práticas de segurança no desenvolvimento de aplicações.

Em Cybersecurity, inclui medidas para proteger servidores, redes e sistemas. E no Modelo Operacional, define políticas de segurança e procedimentos de resposta a incidentes.

Em resumo, a Infrastructure & Application Security é uma capability essencial que fornece às organizações as ferramentas e processos necessários para a proteção eficaz de infraestruturas de TI e aplicações.

Esta capability 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 Infrastructure & Application Security visa a garantir a integridade e a disponibilidade dos sistemas e aplicações, protegendo-os contra vulnerabilidades e ameaças tanto internas quanto externas.

Isso é essencial para manter a operação segura e eficiente da organização.

Conceitos

- Segurança da Infraestrutura de TI: Refere-se às práticas e tecnologias para proteger servidores, redes, sistemas operacionais e outros componentes da infraestrutura contra ameaças.
- Segurança de Aplicações: Envolve a implementação de medidas de segurança no desenvolvimento e na operação de software para mitigar riscos de vulnerabilidades e ataques.
- Firewall: Um dispositivo ou software que controla o tráfego de rede, permitindo ou bloqueando com base em regras de segurança predefinidas.

Características

- Sistemas de Detecção e Prevenção de Intrusões (IDS/IPS): Implementação de tecnologias que monitoram o tráfego de rede em busca de atividades suspeitas e tomam medidas para bloquear ou alertar sobre possíveis ataques.
- Criptografia: Uso de algoritmos criptográficos para proteger dados em

trânsito e em repouso, garantindo que apenas destinatários autorizados possam acessá-los.
- Desenvolvimento Seguro: Integração de práticas de segurança desde o início do ciclo de vida do desenvolvimento de software, identificando e corrigindo vulnerabilidades desde o início.
- Auditoria de Segurança: Monitoramento constante da infraestrutura e das aplicações para identificar e remediar possíveis brechas de segurança.
- Gestão de Identidade e Acesso: Controle rigoroso de quem tem acesso a sistemas e dados, garantindo que apenas pessoas autorizadas possam acessar recursos críticos.

Propósito e Objetivos

A Infrastructure & Application Security é uma capability fundamental que visa proteger a infraestrutura de TI e as aplicações contra ameaças cibernéticas.

Seu propósito principal é garantir que a organização esteja preparada para enfrentar ataques, mantendo a integridade, confidencialidade e disponibilidade de seus sistemas críticos.

Esta capability desempenha um papel crucial na manutenção da operação contínua e na redução de riscos relacionados à segurança da informação.

Objetivos

Dentro do contexto do CIO Codex Capability Framework, a Infrastructure & Application Security tem os seguintes objetivos bem definidos:

- Eficiência Operacional: Contribui para a eficiência operacional por meio da implementação de medidas de segurança que não prejudicam a produtividade das operações de TI. Isso permite que a organização funcione de forma suave e segura.
- Inovação: Promove a inovação ao incorporar práticas de segurança no desenvolvimento de aplicações, permitindo a adoção de novas tecnologias com segurança.
- Vantagem Competitiva: Oferece uma vantagem competitiva, uma vez que

a confiabilidade e a segurança dos sistemas são diferenciais importantes para clientes e parceiros.

Impacto na Tecnologia

A Infrastructure & Application Security tem um impacto significativo em várias dimensões da tecnologia:

- Infraestrutura: Implementa firewalls, sistemas de detecção e prevenção de intrusões (IDS/IPS) e outras soluções para proteger a infraestrutura de TI contra ataques cibernéticos.
- Arquitetura: Define e implementa modelos de segurança que se integram à arquitetura de sistemas, garantindo que os componentes críticos sejam adequadamente protegidos.
- Sistemas: Aplica práticas de segurança no desenvolvimento de aplicações, como análises de segurança de código e testes de penetração, para garantir que as aplicações sejam resistentes a ataques.
- Cybersecurity: A segurança da infraestrutura e das aplicações inclui medidas para proteger servidores, redes e sistemas contra ameaças.
- Modelo Operacional: Define políticas de segurança, procedimentos de resposta a incidentes e realiza treinamentos para garantir a eficácia da segurança cibernética em toda a organização.

Roadmap de Implementação

A capability de Infrastructure & Application Security desempenha um papel crucial na proteção dos sistemas e aplicações contra ameaças internas e externas.

A implementação eficaz desta capability é essencial para garantir a integridade e a disponibilidade dos recursos de TI.

Neste contexto, um roadmap de implementação, considerando os princípios do CIO Codex Capability Framework:

- Avaliação de Riscos: Inicie o processo de implementação realizando uma avaliação abrangente de riscos de segurança da infraestrutura e das

aplicações. Identifique ameaças potenciais, vulnerabilidades e ativos críticos que precisam ser protegidos.

- Definição de Políticas de Segurança: Desenvolva políticas de segurança claras e abrangentes que estabeleçam diretrizes para a proteção da infraestrutura e das aplicações. Essas políticas devem abordar questões como acesso, autenticação, criptografia e auditoria.
- Implementação de Firewall e IDS/IPS: Implemente soluções de firewall para controlar o tráfego de rede e sistemas de Detecção e Prevenção de Intrusões (IDS/IPS) para monitorar atividades suspeitas e tomar medidas preventivas.
- Integração de Criptografia: Integre a criptografia em sistemas e comunicações críticas, garantindo a confidencialidade dos dados em trânsito e em repouso.
- Desenvolvimento Seguro: Adote práticas de desenvolvimento seguro desde o início do ciclo de vida do software. Realize análises de segurança de código, testes de penetração e revisões de segurança de aplicativos.
- Gestão de Identidade e Acesso: Implemente um rigoroso controle de identidade e acesso para garantir que apenas pessoas autorizadas tenham permissão para acessar sistemas e dados sensíveis.
- Monitoramento Contínuo: Estabeleça sistemas de monitoramento contínuo para auditoria de segurança, identificando e respondendo a atividades suspeitas ou violações de segurança em tempo real.
- Treinamento e Conscientização: Promova a conscientização sobre segurança entre os funcionários e forneça treinamento regular sobre as políticas e procedimentos de segurança.
- Resposta a Incidentes: Desenvolva planos de resposta a incidentes que definam procedimentos claros para lidar com violações de segurança. Treine equipes para responder de forma eficaz a incidentes.
- Testes de Vulnerabilidade: Realize testes regulares de vulnerabilidade e avaliações de segurança para identificar e remediar possíveis vulnerabilidades na infraestrutura e nas aplicações.
- Conformidade com Regulamentações: Assegure-se de que todas as práticas de segurança estejam em conformidade com regulamentações relevantes, como o GDPR, LGPD e outras normas aplicáveis.
- Aprimoramento Contínuo: Estabeleça um ciclo de melhoria contínua, revisando regularmente as políticas e procedimentos de segurança, ajustando-os com base em lições aprendidas e nas mudanças no cenário

de ameaças.

A implementação eficaz da Infrastructure & Application Security não apenas protegerá os sistemas e aplicações da organização, mas também contribuirá para a eficiência operacional, inovação e vantagem competitiva.

Esta capability é um elemento essencial para garantir a operação segura e eficiente da organização, protegendo contra ameaças internas e externas.

Melhores Práticas de Mercado

No contexto do CIO Codex Capability Framework, a capability de Infrastructure & Application Security desempenha um papel crítico na proteção da integridade e disponibilidade dos sistemas e aplicativos de uma organização contra uma variedade de ameaças, tanto internas quanto externas.

Para alcançar um nível eficaz de segurança cibernética, é crucial adotar as melhores práticas de mercado que são amplamente reconhecidas e aplicadas por organizações líderes em todo o mundo.

Abaixo estão as principais melhores práticas dentro dessa capability:

- Avaliação de Vulnerabilidades Regular: Realize avaliações regulares de vulnerabilidades em sistemas, aplicativos e infraestrutura de TI para identificar potenciais pontos fracos. Isso inclui testes de penetração e análises de código.
- Gestão de Patch: Mantenha todos os sistemas e aplicativos atualizados com as correções de segurança mais recentes. Implemente uma rigorosa política de gestão de patch para corrigir vulnerabilidades conhecidas.
- Segmentação de Rede: Isole e segmente as redes para limitar o movimento lateral de invasores em caso de comprometimento. A segmentação ajuda a conter possíveis violações.
- Firewalls Avançados: Utilize firewalls avançados que possam inspecionar o tráfego de rede em nível de aplicação. Isso permite o bloqueio de tráfego malicioso e a aplicação de políticas de segurança granulares.
- Monitoramento de Segurança em Tempo Real: Implemente sistemas de monitoramento de segurança em tempo real que possam detectar

atividades suspeitas ou não autorizadas. A resposta rápida a incidentes é essencial.

- Auditoria de Segurança Contínua: Realize auditorias regulares de segurança para garantir que as políticas e controles de segurança estejam sendo seguidos e que os sistemas estejam em conformidade com os padrões de segurança.
- Proteção de Aplicativos: Adote tecnologias de proteção de aplicativos, como Web Application Firewalls (WAFs), para proteger contra-ataques específicos a aplicativos, como SQL Injection e Cross-Site Scripting (XSS).
- Gestão de Identidade e Acesso (IAM): Implemente uma robusta solução de IAM para garantir que apenas usuários autorizados tenham acesso aos sistemas e aplicativos. Isso inclui autenticação multifatorial e controle de acesso baseado em função.
- Treinamento e Conscientização em Segurança: Realize treinamentos regulares de conscientização em segurança para todos os funcionários, a fim de aumentar a conscientização sobre ameaças cibernéticas e boas práticas de segurança.
- Resposta a Incidentes: Desenvolva um plano de resposta a incidentes detalhado e teste-o regularmente. A capacidade de responder de forma eficaz a incidentes pode reduzir significativamente o impacto de uma violação de segurança.
- Revisões de Código Seguro: Realize revisões de código seguro durante o desenvolvimento de software para identificar e corrigir vulnerabilidades desde o início do ciclo de vida do aplicativo.

Adotar essas melhores práticas de mercado dentro da capability de Infrastructure & Application Security é fundamental para fortalecer a postura de segurança cibernética de uma organização, garantindo que sistemas e aplicativos permaneçam protegidos contra ameaças em constante evolução.

Além disso, ajuda a garantir a operação segura e eficiente de toda a infraestrutura de TI.

Desafios Atuais

A Capability de Infrastructure & Application Security desempenha um papel vital na garantia da integridade e disponibilidade dos sistemas e aplicações, protegendo-os contra ameaças internas e externas.

No entanto, a adoção e integração dessa capability nos processos de negócios e operações de TI das organizações enfrentam diversos desafios atuais de mercado.

Abaixo, os principais desafios considerados as melhores práticas do mercado:

- Ameaças Cibernéticas em Evolução: O cenário de ameaças cibernéticas está em constante evolução, com hackers desenvolvendo novas técnicas e ataques mais sofisticados. As organizações devem se manter atualizadas para enfrentar essas ameaças em constante mutação.
- Complexidade da Infraestrutura: A infraestrutura de TI moderna é complexa, incluindo servidores, redes, dispositivos móveis, nuvem e muito mais. Garantir a segurança em todas essas frentes é um desafio significativo.
- Desenvolvimento Rápido de Aplicações: A demanda por desenvolvimento ágil de aplicações muitas vezes coloca a segurança em segundo plano. Equilibrar velocidade e segurança é um desafio constante.
- Escassez de Profissionais de Segurança: Há uma escassez de profissionais de segurança qualificados, o que torna difícil para as organizações recrutarem e manterem talentos nessa área crítica.
- Conformidade Regulatória: As regulamentações de segurança de dados estão se tornando mais rigorosas. As organizações enfrentam o desafio de se manterem em conformidade com as leis de privacidade e proteção de dados.
- Proteção de Dados em Ambientes de Nuvem: Migrar para a nuvem cria desafios de segurança adicionais, pois os dados podem estar fora do controle direto da organização.
- Gestão de Identidade e Acesso: Controlar quem tem acesso a sistemas e dados é crítico, mas pode ser complexo em organizações com muitos funcionários e sistemas.
- Integração de Segurança no Desenvolvimento: Incorporar segurança desde o início do ciclo de vida do desenvolvimento de software é essencial, mas muitas organizações ainda lutam com essa integração.

- Ataques Internos: As organizações enfrentam desafios na prevenção de ameaças internas, incluindo vazamentos de dados causados por funcionários mal-intencionados.
- Gerenciamento de Incidentes de Segurança: Ter um plano de resposta a incidentes eficaz é crucial. As organizações precisam estar preparadas para agir rapidamente em caso de violação de segurança.

Esses desafios refletem a importância crítica da Capability de Infrastructure & Application Security no atual ambiente de negócios, onde a segurança de infraestrutura e aplicações é fundamental para a continuidade dos negócios e a proteção dos ativos de informações da organização.

A capacidade de enfrentar esses desafios requer a implementação de tecnologias de segurança avançadas, como sistemas de detecção e prevenção de intrusões (IDS/IPS), criptografia, desenvolvimento seguro de aplicações e gerenciamento de identidade e acesso.

Além disso, investir na formação e retenção de talentos de segurança cibernética é essencial para enfrentar as ameaças em constante evolução.

Tendências para o Futuro

A Capability de Infrastructure & Application Security desempenha um papel crítico na proteção dos sistemas e aplicações contra ameaças cibernéticas, garantindo a integridade e a disponibilidade dos recursos de TI.

O cenário de segurança cibernética está em constante evolução, e é fundamental antecipar as tendências que moldarão o futuro dessa capability.

Neste contexto, as principais tendências futuras no âmbito do CIO Codex Capability Framework:

- Inteligência Artificial (IA) na Segurança: A IA será amplamente utilizada para melhorar a detecção e a prevenção de ameaças. Algoritmos de IA serão capazes de identificar padrões de comportamento suspeito e ataques em tempo real, tornando a segurança mais eficaz.
- Segurança de DevOps: Com a crescente adoção de práticas DevOps, a segurança será integrada ao ciclo de vida de desenvolvimento de software

desde o início. Isso incluirá a automação de testes de segurança e a verificação contínua de código para vulnerabilidades.

- Zero Trust Architecture: A abordagem Zero Trust continuará a ganhar destaque, onde a confiança não é concedida com base na localização ou na rede do usuário, mas em sua autenticação e validação contínua.
- Proteção de Dados em Nuvem: Com a migração contínua para ambientes em nuvem, a segurança de dados na nuvem será aprimorada. Tecnologias de criptografia e gerenciamento de identidade desempenharão um papel crucial.
- Segurança em IoT (Internet das Coisas): Com o aumento da conectividade de dispositivos IoT, a segurança desses dispositivos se tornará vital. Medidas para proteger a integridade e a confidencialidade dos dados gerados por dispositivos IoT serão implementadas.
- Autenticação Multifatorial Avançada: A autenticação multifatorial evoluirá com métodos mais avançados, como reconhecimento biométrico e autenticação por comportamento, para garantir que apenas usuários autorizados acessem sistemas e aplicativos.
- Resposta a Incidentes Autônoma: A automação na resposta a incidentes ganhará destaque, permitindo ação imediata para conter ameaças, isolar sistemas comprometidos e mitigar danos.
- Blockchain para Auditoria de Segurança: A tecnologia blockchain será usada para criar registros imutáveis de auditorias de segurança, permitindo uma trilha de auditoria confiável e à prova de adulterações.
- Segurança em Dispositivos Móveis: Com o uso crescente de dispositivos móveis no ambiente corporativo, a segurança móvel se tornará mais complexa e necessária, com foco em proteger dados corporativos em dispositivos pessoais.
- Treinamento em Conscientização em Segurança: Investimentos contínuos em treinamento de conscientização em segurança cibernética garantirão que os colaboradores estejam preparados para identificar e responder a ameaças.

Essas tendências representam as expectativas do mercado em relação à evolução da Capability de Infrastructure & Application Security.

À medida que as organizações enfrentam ameaças cada vez mais sofisticadas, aprimorar a segurança da infraestrutura e das aplicações se tornará uma prioridade estratégica para manter a operação segura e eficiente.

KPIs Usuais

A capacidade de Infrastructure & Application Security desempenha um papel vital na proteção da integridade e disponibilidade dos sistemas e aplicações de uma organização contra ameaças internas e externas.

Medir o desempenho dessa capability é crucial para garantir a segurança da infraestrutura de TI e a confiabilidade das aplicações.

Abaixo, uma lista dos principais KPIs usuais no contexto do CIO Codex Capability Framework, que ajudam a avaliar o desempenho da Infrastructure & Application Security:

- Taxa de Conformidade com Padrões de Segurança (Security Standards Compliance Rate): Mede o grau de conformidade da organização com padrões de segurança, como ISO 27001, NIST, ou outros relevantes para a indústria.
- Taxa de Vulnerabilidades Identificadas (Identified Vulnerabilities Rate): Avalia a frequência com que vulnerabilidades de segurança são identificadas em sistemas e aplicações.
- Tempo Médio de Resposta a Incidentes de Segurança (Mean Time to Respond to Security Incidents): Calcula o tempo médio necessário para a equipe de segurança responder a incidentes de segurança após sua detecção.
- Taxa de Ataques de Negociação (Distributed Denial of Service – DDoS Attack Rate): Indica a frequência de ataques DDoS direcionados à infraestrutura de TI da organização.
- Taxa de Uso de Criptografia (Encryption Usage Rate): Avalia o percentual de tráfego de rede e dados em repouso que é criptografado para proteção contra acessos não autorizados.
- Taxa de Auditorias de Segurança Realizadas (Security Audits Conducted Rate): Mede a regularidade das auditorias de segurança para garantir a conformidade com políticas e padrões de segurança.
- Tempo Médio de Resolução de Vulnerabilidades (Mean Time to Resolve Vulnerabilities): Calcula o tempo médio necessário para corrigir vulnerabilidades de segurança após sua identificação.

- Taxa de Aplicativos com Análise de Segurança de Código (Applications with Code Security Analysis Rate): Avalia a porcentagem de aplicações que passaram por análise de segurança de código.
- Taxa de Identificação de Ameaças Internas (Internal Threat Detection Rate): Indica a eficácia na detecção de ameaças internas, como comportamentos suspeitos de funcionários.
- Taxa de Testes de Penetração (Penetration Testing Rate): Mede a frequência com que são realizados testes de penetração para avaliar a resistência de sistemas e aplicações a ataques.
- Taxa de Aplicações com Autenticação Multifatorial (Applications with Multifactor Authentication Rate): Avalia a porcentagem de aplicações que utilizam autenticação multifatorial para acesso.
- Taxa de Resposta a Incidentes de Segurança (Security Incident Response Rate): Indica a eficácia na resposta a incidentes de segurança, incluindo a contenção e mitigação de impactos.
- Taxa de Treinamento em Segurança de Aplicações (Application Security Training Rate): Avalia a porcentagem de desenvolvedores e equipes de TI que receberam treinamento em segurança de aplicações.
- Taxa de Acesso Não Autorizado a Sistemas (Unauthorized System Access Rate): Mede a frequência de tentativas de acesso não autorizado a sistemas protegidos.
- Taxa de Cumprimento de Políticas de Segurança (Security Policy Compliance Rate): Avalia o grau de conformidade dos funcionários e equipes com as políticas de segurança da organização.

Esses KPIs são fundamentais para avaliar a eficácia da Infrastructure & Application Security na proteção da infraestrutura de TI e das aplicações críticas da organização.

A medição constante desses indicadores permite identificar áreas de melhoria e manter a segurança da informação em um nível elevado, garantindo a operação segura e eficiente da organização.

Exemplos de OKRs

A capability de Infrastructure & Application Security na macro capability Planning & Running da camada Cybersecurity desempenha um papel crucial na proteção de

infraestruturas de TI e aplicações contra ameaças cibernéticas.

Essa capability envolve a implementação de medidas de segurança robustas para prevenir ataques e garantir a integridade dos sistemas.

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

Implementação de Firewalls e IDS/IPS

Objetivo: Reforçar a segurança da infraestrutura de TI com medidas de prevenção de ataques.

- KR1: Configurar firewalls em todos os pontos de entrada da rede.
- KR2: Implementar sistemas de Detecção e Prevenção de Intrusões (IDS/IPS).
- KR3: Realizar análises regulares de tráfego para identificar atividades suspeitas.

Aplicação de Criptografia em Comunicações

Objetivo: Garantir a confidencialidade das comunicações de dados.

- KR1: Criptografar todas as comunicações sensíveis, incluindo e-mails e transmissões de dados.
- KR2: Implementar protocolos de criptografia fortes em todas as transferências de dados.
- KR3: Manter chaves de criptografia seguras e atualizadas.

Práticas de Segurança no Desenvolvimento de Aplicações

Objetivo: Integrar a segurança desde o início do ciclo de vida do desenvolvimento de software.

- KR1: Realizar avaliações de segurança de código em todas as etapas do desenvolvimento.
- KR2: Estabelecer diretrizes de segurança para o desenvolvimento de aplicações.
- KR3: prover treinamento em segurança para os desenvolvedores.

Monitoramento Contínuo de Segurança

Objetivo: Identificar e responder rapidamente a ameaças de segurança.

- KR1: Implementar sistemas de monitoramento de segurança em tempo real.
- KR2: Configurar alertas para atividades suspeitas ou violações de política.
- KR3: Ter equipes de resposta a incidentes prontas para ação imediata.

Testes de Penetração Regulares

Objetivo: Avaliar a resistência da infraestrutura e aplicações a ataques simulados.

- KR1: Realizar testes de penetração internos e externos trimestralmente.
- KR2: Corrigir imediatamente as vulnerabilidades identificadas nos testes.
- KR3: Documentar e analisar os resultados dos testes para melhorar a segurança.

Através desses OKRs, a capability de Infrastructure & Application Security visa salvaguardar a infraestrutura tecnológica essencial e as aplicações críticas contra vulnerabilidades e ameaças externas e internas.

Isso é fundamental para manter a continuidade das operações, proteger dados sensíveis e garantir a confiança dos stakeholders.

Critérios para Avaliação de Maturidade

A capability Infrastructure & Application Security, inserida na macro capability Planning & Running e na camada Cybersecurity, desempenha um papel crucial na proteção de infraestruturas de TI e aplicações contra ameaças cibernéticas.

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 medidas de segurança implementadas para proteger infraestruturas e aplicações.
- Ausência de consciência sobre ameaças cibernéticas.
- Falta de firewalls e sistemas de detecção de intrusões.
- Não há práticas de segurança no desenvolvimento de aplicações.
- Ausência de políticas de criptografia.

Nível de Maturidade Inicial

- Alguns esforços iniciais para proteção, mas não abrangentes.
- Consciência limitada sobre ameaças cibernéticas.
- Implementação de firewalls básicos.
- Práticas de segurança adotadas em algumas aplicações.
- Criptografia parcialmente aplicada em dados sensíveis.

Nível de Maturidade Definido

- Processos formalizados e documentados de segurança.
- Consciência crescente sobre ameaças cibernéticas.
- Firewalls e sistemas de detecção de intrusões bem estabelecidos.
- Práticas de segurança incorporadas no desenvolvimento de aplicações.
- Políticas de criptografia claramente definidas.

Nível de Maturidade Gerenciado

- Processos de segurança eficazes e adaptáveis.
- Conscientização disseminada sobre ameaças cibernéticas.
- Monitoramento ativo de firewalls e sistemas de detecção de intrusões.
- Práticas de segurança avançadas em todas as aplicações.
- Uso consistente e eficaz da criptografia.

Nível de Maturidade Otimizado

- Processos de segurança altamente otimizados e inovadores.
- Conscientização e treinamento contínuos sobre ameaças cibernéticas.
- Monitoramento em tempo real de todos os sistemas de segurança.
- Práticas avançadas de segurança em desenvolvimento e operações.
- Criptografia avançada e atualizada em conformidade com as melhores práticas.

A avaliação de maturidade da capability Infrastructure & Application Security é fundamental para garantir que a organização esteja preparada para prevenir ataques cibernéticos e proteger sua infraestrutura e aplicações críticas.

À medida que a maturidade aumenta, a segurança da organização se torna mais resiliente contra ameaças internas e externas.

Convergência com Frameworks de Mercado

A capability Infrastructure & Application Security, inserida na macro capability Planning & Running e pertencente à camada Cybersecurity, é crucial para a proteção das infraestruturas de TI e aplicações.

Esta capability engloba a implementação de medidas de segurança robustas para prevenir ataques cibernéticos, garantindo a integridade dos sistemas através do uso de firewalls, sistemas de detecção e prevenção de intrusões, criptografia e práticas de segurança no desenvolvimento de aplicações.

O foco é proteger a infraestrutura tecnológica essencial e as aplicações críticas contra vulnerabilidades e ameaças externas e internas.

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 oferece um framework de governança de TI que

abrange gestão de riscos e segurança da informação. A Infrastructure & Application Security alinha-se aos princípios do COBIT para a proteção eficaz das informações e infraestruturas tecnológicas.

ITIL

- Nível de Convergência: Médio
- Racional: O ITIL proporciona diretrizes para a gestão de serviços de TI, abrangendo aspectos de segurança em seus processos. A capability se integra ao ITIL ao garantir que os serviços de TI estejam protegidos contra ameaças de segurança.

SAFe

- Nível de Convergência: Médio
- Racional: O SAFe, como um framework de desenvolvimento ágil, inclui práticas de segurança em seus processos, alinhando-se à Infrastructure & Application Security na implementação de medidas de segurança durante a entrega contínua.

PMI

- Nível de Convergência: Médio
- Racional: A metodologia do PMI para a gestão de projetos pode incorporar a Infrastructure & Application Security para assegurar que os projetos de TI sejam protegidos contra riscos de segurança.

CMMI

- Nível de Convergência: Médio
- Racional: O CMMI, focado na maturidade dos processos, pode se beneficiar da Infrastructure & Application Security ao integrar práticas de segurança nos processos de desenvolvimento e gestão.

TOGAF

- Nível de Convergência: Médio
- Racional: No TOGAF, que aborda a arquitetura empresarial, a capability contribui para a inclusão de considerações de segurança na arquitetura de TI, fortalecendo a proteção de infraestruturas e aplicações.

DevOps SRE

- Nível de Convergência: Médio
- Racional: Em ambientes DevOps SRE, onde a inovação rápida e a entrega contínua são fundamentais, a Infrastructure & Application Security é essencial para manter a segurança dos processos de desenvolvimento e operação.

NIST

- Nível de Convergência: Alto
- Racional: O NIST fornece diretrizes detalhadas para a segurança cibernética. A capability alinha-se ao NIST na implementação de soluções de segurança para proteger as infraestruturas e aplicações de TI.

Six Sigma

- Nível de Convergência: Baixo
- Racional: O Six Sigma se concentra na melhoria da qualidade e eficiência dos processos. A Infrastructure & Application Security, embora menos alinhada, contribui para a minimização de riscos e falhas de segurança nos processos.

Lean IT

- Nível de Convergência: Baixo

- Racional: Lean IT, com seu foco na eficiência operacional, tem uma convergência limitada com a Infrastructure & Application Security. No entanto, a segurança robusta pode ajudar a eliminar desperdícios e melhorar a eficiência operacional.

A capability Infrastructure & Application Security desempenha um papel vital na proteção contra ameaças cibernéticas, garantindo a segurança dos dados e sistemas críticos.

Os KPIs relevantes podem incluir a frequência de violações de segurança, o tempo de resposta a incidentes e a eficácia das medidas de segurança implementadas.

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

Processos e Atividades

Develop Security Plans

O desenvolvimento de planos detalhados para segurança de infraestrutura e aplicações é um processo crítico que envolve a criação de uma estrutura abrangente para proteger os ativos de TI da organização.

Este processo começa com a avaliação dos riscos e vulnerabilidades para identificar áreas críticas que necessitam de proteção.

Em seguida, são definidos os objetivos de segurança alinhados aos requisitos de negócios e regulatórios.

O plano de segurança deve incluir a implementação de políticas de segurança, procedimentos operacionais e a designação de papéis e responsabilidades.

Além disso, deve estabelecer os mecanismos de monitoramento e resposta a incidentes, garantindo que a organização esteja preparada para lidar com ameaças e violações de segurança.

A documentação detalhada dos planos de segurança é essencial para assegurar que todos os envolvidos compreendam suas funções e as medidas necessárias para manter a segurança da infraestrutura e das aplicações.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Conduct Risk Assessment	Realizar uma avaliação de riscos para identificar ameaças e vulnerabilidades.	Dados de risco, análise de ameaças	Relatório de avaliação 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 avaliação 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 Security Policies	Desenvolver políticas de segurança para proteção da infraestrutura e das aplicações.	Objetivos de segurança definidos	Políticas de segurança	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

4	Assign Roles and Responsibilities	Atribuir papéis e responsabilidades para a equipe de segurança de TI.	Políticas de segurança	Documento de papéis e responsabilidades	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
5	Document Security Plan	Documentar o plano de segurança de forma detalhada e acessível.	Documento de papéis e responsabilidades	Plano de segurança	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 para infraestrutura e aplicações é um processo fundamental que assegura que todas as necessidades de proteção sejam compreendidas e atendidas. Este processo envolve a análise dos requisitos regulatórios, as políticas internas e as melhores práticas do setor para determinar as medidas de segurança necessárias. Os requisitos de segurança devem abranger controle de acesso, criptografia, auditoria de segurança, e muito mais. A identificação precisa desses requisitos permite o desenvolvimento de planos de segurança robustos e a implementação de soluções eficazes. A colaboração entre diferentes áreas da TI e do negócio é crucial para garantir que todos os aspectos sejam considerados e que os requisitos sejam adequadamente incorporados aos planos de segurança.

PDCA focus: Plan

Periodicidade: Semestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE

1	Analyze Regulatory Requirements	Analisar requisitos regulatórios e de compliance para segurança de TI.	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	Identify Business Needs	Identificar as necessidades de negócios relacionadas à segurança de TI.	Relatório de requisitos regulatórios	Relatório de necessidades de negócios	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Define Security Controls	Definir os controles de segurança necessários para atender aos requisitos identificados.	Relatório de necessidades de negócios	Lista de controles 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 Compliance Procedures	Desenvolver procedimentos de compliance para garantir a conformidade com os requisitos.	Lista de controles de segurança	Procedimentos de compliance	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

5	Document Requirements	Documentar todos os requisitos de segurança de forma clara e acessível.	Procedimentos de compliance	Documentação de requisitos	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity

Implement Security Solutions

A implementação das soluções de segurança conforme planejado é crucial para garantir que as medidas de proteção sejam efetivamente aplicadas e mantidas.

Este processo envolve a execução dos procedimentos definidos nos planos de segurança, incluindo a configuração de firewalls, a implementação de criptografia, a configuração de sistemas de detecção e prevenção de intrusões (IDS/IPS) e a utilização de ferramentas de auditoria de segurança.

A coordenação entre as várias áreas de TI é fundamental para assegurar que as soluções sejam integradas de forma eficaz e que os sistemas estejam protegidos em todos os níveis.

A formação contínua da equipe e a validação das soluções implementadas através de testes regulares garantem a eficácia das medidas de segurança.

- PDCA focus: Do
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE

1	Configure Firewalls	Configurar firewalls para controlar o tráfego de rede e proteger contra acessos não autorizados.	Lista de controles de segurança	Firewalls configurados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
2	Implement Encryption	Implementar criptografia para proteger dados sensíveis durante o armazenamento e a transmissão.	Lista de controles de segurança	Dados criptografados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
3	Deploy IDS/IPS	Implementar sistemas de detecção e prevenção de intrusões (IDS/IPS) para monitorar o tráfego de rede.	Lista de controles de segurança	IDS/IPS implementados	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	Setup Audit Tools	Configurar ferramentas de auditoria de segurança para monitorar e registrar atividades suspeitas.	Lista de controles de segurança	Ferramentas de auditoria configuradas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Solution Engineering & Development; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity

5	Validate Implementation	Validar a implementação das soluções de segurança através de testes e auditorias.	Ferramentas de auditoria configuradas	Implementação validada	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Monitor Security Performance

O monitoramento contínuo do desempenho das soluções de segurança 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 de firewalls, criptografia e sistemas de detecção e prevenção de intrusões (IDS/IPS). 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 Optimize Security Processes

A revisão e otimização contínua dos processos de segurança 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