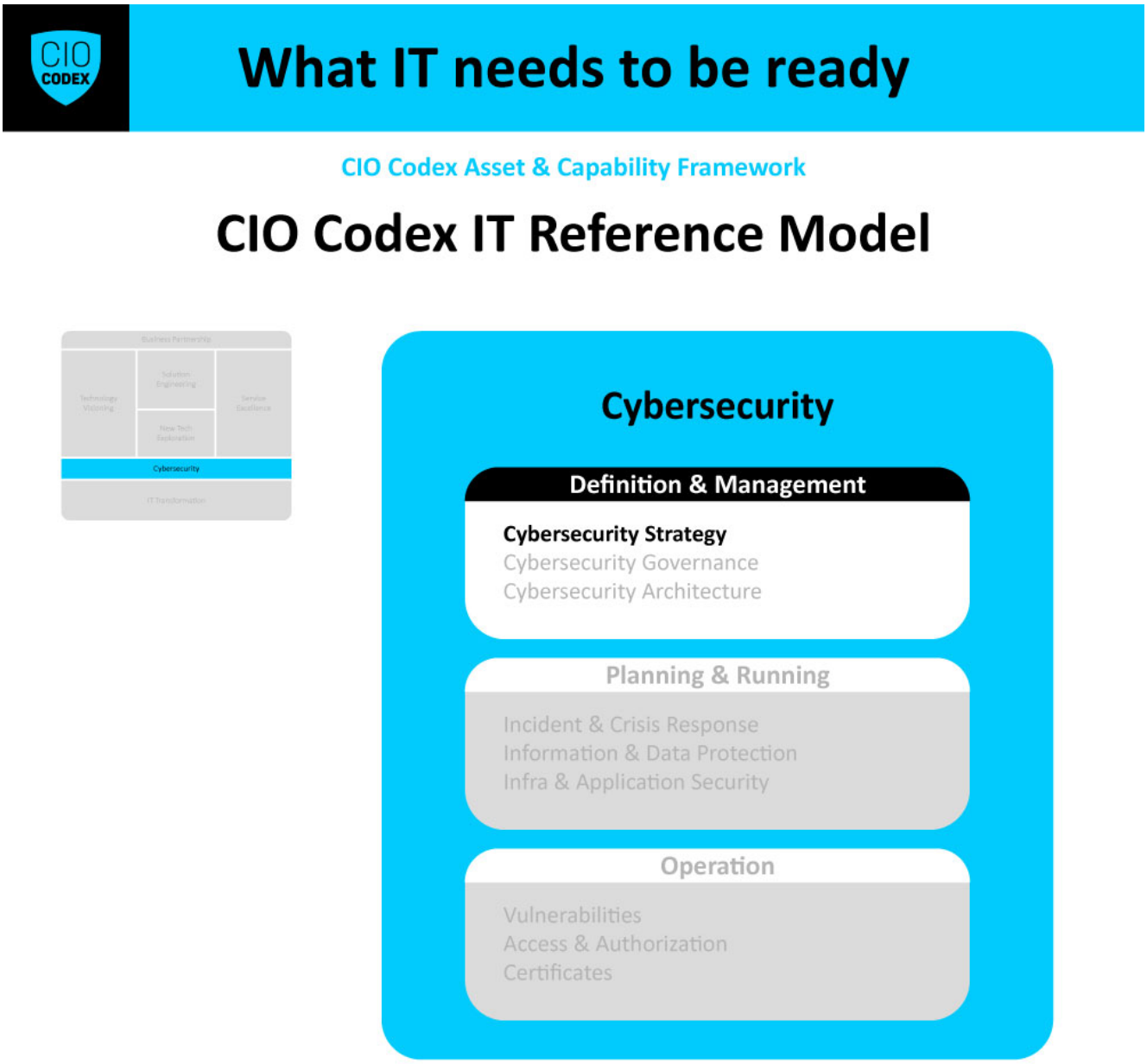

A Cybersecurity Strategy, incorporada na macro capability Definition & Management e na camada Cybersecurity do CIO Codex Capability Framework, representa uma face fundamental na proteção de informações e sistemas em organizações.

Este domínio estratégico é essencial para salvaguardar a integridade, confidencialidade e disponibilidade dos dados e sistemas da organização.

Alinhando estrategicamente as práticas de segurança cibernética com os objetivos de negócios, a Cybersecurity Strategy estabelece um ambiente seguro, fomentando a confiança entre clientes, parceiros e stakeholders, e mantendo a continuidade das operações frente às ameaças cibernéticas em constante evolução.

Na esfera da Cybersecurity Strategy, conceitos-chave como a própria estratégia de segurança cibernética, o alinhamento com os objetivos de negócios e a priorização de riscos são fundamentais. Estes conceitos abrangem o planejamento e a execução de ações focadas na proteção dos ativos digitais da organização.

A estratégia de segurança cibernética, desenvolvida em sinergia com as metas organizacionais, assegura que a segurança esteja integrada em todas as operações de negócios, enquanto a priorização de riscos envolve identificar e classificar ameaças potenciais, possibilitando o uso eficiente dos recursos de segurança.

Dentro deste escopo, a Cybersecurity Strategy se caracteriza pela avaliação contínua de vulnerabilidades, definição de diretrizes de segurança, alocação adequada de recursos, gestão eficiente de incidentes de segurança, conscientização e treinamento contínuos dos colaboradores, e auditorias regulares para verificar a conformidade com políticas e regulamentações pertinentes.

Estas ações são projetadas para estabelecer um framework robusto de segurança cibernética, integrando e reforçando todas as facetas da infraestrutura de TI e práticas organizacionais.

O propósito central da Cybersecurity Strategy é desenvolver e implementar uma estratégia de segurança cibernética holística, promovendo o alinhamento entre iniciativas de segurança e os objetivos de negócio da organização.

Isso envolve a definição de prioridades, o estabelecimento de diretrizes de segurança e a garantia de alocação apropriada de recursos para a proteção contra ameaças cibernéticas.

Este enfoque estratégico não só melhora a postura de segurança da organização, mas também contribui para sua resiliência e adaptabilidade em face a ameaças em evolução.

Os objetivos dentro do CIO Codex Capability Framework são claros: aprimorar a eficiência operacional através do desenvolvimento e implementação de políticas e práticas de segurança cibernética eficazes, fomentar a inovação em segurança cibernética, adotando tecnologias e abordagens avançadas e reforçar a vantagem competitiva da organização, demonstrando um compromisso robusto com a segurança cibernética, o que por sua vez aumenta a confiança dos clientes e parceiros de negócios.

No que diz respeito ao impacto tecnológico, a Cybersecurity Strategy afeta múltiplas dimensões. Na infraestrutura, estabelece requisitos de segurança essenciais, garantindo a proteção contra ameaças cibernéticas. Na arquitetura, influencia o design dos sistemas, integrando considerações de segurança desde o início.

Nos sistemas, estabelece políticas abrangentes que cobrem aspectos como autenticação, autorização, criptografia e monitoramento. E no modelo operacional, delineia processos e procedimentos para gerenciamento eficiente de incidentes cibernéticos, assegurando uma resposta rápida e eficaz às ameaças em tempo real.

Portanto, a Cybersecurity Strategy é um componente crucial para a segurança e a estabilidade operacional das organizações no cenário digital atual.

Através da implementação efetiva de uma estratégia de segurança cibernética, as organizações não só protegem seus ativos digitais contra ameaças externas, mas também reforçam sua posição no mercado, transmitindo confiança e segurança a clientes e parceiros de negócios.

A capacidade de responder proativamente a ameaças emergentes e manter a continuidade das operações diante de desafios cibernéticos é um diferencial competitivo crucial, que reforça a reputação e a resiliência da organização no cenário empresarial contemporâneo.

Conceitos e Características

A Cybersecurity Strategy é essencial para proteger a integridade, confidencialidade e disponibilidade dos dados e sistemas da organização.

Ao alinhar estrategicamente a segurança cibernética com os objetivos de negócios, ela cria um ambiente seguro que promove a confiança dos clientes, parceiros e stakeholders, mantendo a continuidade das operações mesmo diante de ameaças cibernéticas em constante evolução.

Conceitos

- Estratégia de Segurança Cibernética: Refere-se ao plano de ação deliberado e orientado pelos objetivos de negócios para proteger os ativos digitais da organização contra ameaças cibernéticas.
- Alinhamento com Objetivos de Negócios: A estratégia de segurança cibernética é desenvolvida em estreita colaboração com as metas e objetivos da organização, garantindo que a segurança esteja integrada nas operações de negócios.
- Priorização de Riscos: Identificação e classificação das ameaças

cibernéticas potenciais com base em sua probabilidade e impacto, permitindo a alocação eficaz de recursos de segurança.

Características

- Avaliação de Vulnerabilidades: Realização de análises regulares para identificar vulnerabilidades nos sistemas e aplicativos da organização.
- Definição de Diretrizes de Segurança: Estabelecimento de políticas, padrões e diretrizes de segurança cibernética para orientar as práticas e comportamentos dos colaboradores.
- Alocação de Recursos: Garantia de que recursos adequados, como pessoal, tecnologia e orçamento, estejam disponíveis para implementar e manter a estratégia de segurança.
- Gestão de Incidentes: Desenvolvimento de processos para detectar, responder e mitigar incidentes de segurança cibernética de forma eficiente.
- Conscientização e Treinamento: Educação contínua dos colaboradores sobre as melhores práticas de segurança cibernética e a importância de sua contribuição para a segurança da organização.
- Auditoria e Conformidade: Verificação regular da conformidade com as políticas de segurança e regulamentações aplicáveis.

Propósito e Objetivos

A Cybersecurity Strategy desempenha um papel fundamental na defesa das organizações contra as crescentes ameaças cibernéticas.

Seu propósito central é o desenvolvimento e a implementação de uma estratégia de segurança cibernética abrangente.

Isso envolve alinhar as iniciativas de segurança com os objetivos de negócio da organização, definindo prioridades, estabelecendo diretrizes de segurança e garantindo a alocação adequada de recursos para proteger contra ameaças cibernéticas.

Objetivos

Dentro do contexto do CIO Codex Capability Framework, os objetivos dessa capability incluem:

- Eficiência Operacional: Desenvolver e implementar políticas, procedimentos e práticas de segurança cibernética que melhorem a eficiência operacional, minimizando o impacto de incidentes cibernéticos na continuidade dos negócios.
- Inovação: Promover a inovação em segurança cibernética, adotando tecnologias e abordagens avançadas para proteger proativamente contra ameaças emergentes.
- Vantagem Competitiva: Contribuir para a vantagem competitiva da organização, demonstrando um compromisso sólido com a segurança cibernética, o que aumenta a confiança dos clientes e parceiros de negócios.

Impacto na Tecnologia

A Cybersecurity Strategy tem um impacto profundo em várias dimensões da tecnologia:

- Infraestrutura: Define requisitos de segurança para a infraestrutura de TI, incluindo redes, servidores e armazenamento, garantindo que estejam protegidos contra ameaças cibernéticas.
- Arquitetura: Influencia a arquitetura de TI, exigindo a incorporação de medidas de segurança desde a concepção de sistemas e aplicativos.
- Sistemas: Define políticas de segurança para sistemas e aplicativos, abrangendo autenticação, autorização, criptografia e monitoramento.
- Cybersecurity: A estratégia de segurança cibernética define a direção e as prioridades para proteger ativos tecnológicos, considerando ameaças e riscos.
- Modelo Operacional: Estabelece processos e procedimentos para a gestão de incidentes cibernéticos, garantindo uma resposta eficaz às ameaças em tempo real.

Roadmap de Implementação

A implementação bem-sucedida da capability Cybersecurity Strategy é de extrema importância para garantir a proteção dos ativos digitais e a continuidade das operações da organização.

Dentro do contexto do CIO Codex Capability Framework, as principais etapas para a implementação eficaz dessa capability:

- Alinhamento com Objetivos de Negócios: O primeiro passo é estabelecer um alinhamento claro entre a estratégia de segurança cibernética e os objetivos de negócios da organização. Isso envolve entender como a segurança cibernética pode contribuir para a realização desses objetivos.
- Avaliação de Riscos: Realize uma avaliação abrangente dos riscos cibernéticos que a organização enfrenta. Isso inclui a identificação de ameaças, vulnerabilidades e os possíveis impactos dessas ameaças nos ativos digitais e nas operações.
- Definição de Metas e Métricas: Estabeleça metas claras e mensuráveis para a estratégia de segurança cibernética. Determine as métricas-chave que serão usadas para avaliar o progresso e o desempenho da segurança cibernética.
- Desenvolvimento de Políticas de Segurança: Crie políticas de segurança cibernética abrangentes que abordem todos os aspectos da proteção cibernética, desde o acesso de usuários até a proteção de dados sensíveis.
- Implementação de Controles de Segurança: Identifique e implemente controles de segurança adequados para mitigar os riscos identificados. Isso pode incluir medidas como firewalls, sistemas de detecção de intrusões e autenticação multifator.
- Treinamento e Conscientização: Eduque e treine os funcionários sobre as políticas e práticas de segurança cibernética. Certifique-se de que todos os colaboradores compreendam sua responsabilidade na proteção cibernética.
- Monitoramento Contínuo: Estabeleça sistemas de monitoramento contínuo para detectar atividades suspeitas ou ameaças em tempo real. Isso permite uma resposta rápida a incidentes de segurança.
- Gestão de Incidentes: Desenvolva procedimentos de gestão de incidentes cibernéticos que definam como lidar com violações de segurança, desde a

detecção até a resposta e recuperação.

- Revisão e Melhoria Contínua: Realize revisões regulares da estratégia de segurança cibernética para garantir sua eficácia contínua. Faça ajustes conforme necessário com base nas ameaças em evolução e nas mudanças nos objetivos de negócios.
- Auditorias e Conformidade: Conduza auditorias regulares para garantir que a estratégia de segurança cibernética esteja alinhada com regulamentações e padrões relevantes.
- Comunicação e Conscientização: Mantenha uma comunicação eficaz sobre a segurança cibernética em toda a organização. Promova uma cultura de segurança cibernética conscientizando os funcionários e partes interessadas.

A implementação dessas etapas é essencial para garantir que a Cybersecurity Strategy atinja seus objetivos de proteger os ativos digitais da organização, manter a confiabilidade dos serviços e minimizar os riscos cibernéticos.

Ao seguir esse roadmap estratégico, a organização estará mais bem preparada para enfrentar ameaças cibernéticas em constante evolução e proteger seus interesses críticos.

Melhores Práticas de Mercado

A Cybersecurity Strategy é crucial para proteger os ativos digitais da organização.

As melhores práticas de mercado enfatizam o alinhamento estratégico, avaliação de riscos, políticas claras, conscientização, gestão de incidentes eficaz, tecnologias avançadas, auditoria, testes, gestão de identidade, monitoramento contínuo e inteligência de ameaças.

Melhores Práticas de Mercado para Cybersecurity Strategy:

- Alinhamento com Objetivos de Negócios: A principal prática de mercado é alinhar estrategicamente a segurança cibernética com os objetivos de negócios da organização. Isso envolve a compreensão das metas empresariais e a incorporação da segurança desde o início do planejamento de projetos.

- Avaliação de Riscos e Priorização: Realize avaliações regulares de riscos para identificar ameaças potenciais e vulnerabilidades. Priorize os riscos com base na probabilidade e no impacto, concentrando recursos onde são mais necessários.
- Desenvolvimento de Políticas e Diretrizes: Estabeleça políticas e diretrizes claras de segurança cibernética que definam expectativas e padrões de comportamento para funcionários e colaboradores.
- Investimento em Conscientização e Treinamento: Eduque continuamente a equipe sobre as melhores práticas de segurança cibernética e a importância da sua contribuição para a segurança organizacional.
- Gestão de Incidentes: Desenvolva processos robustos para a detecção, resposta e mitigação de incidentes cibernéticos. Isso inclui planos de comunicação eficazes e equipes de resposta bem treinadas.
- Implementação de Tecnologias Avançadas: Adote tecnologias de segurança avançadas, como detecção de ameaças em tempo real, análise de comportamento de usuário e automação de segurança.
- Auditoria e Conformidade: Realize auditorias regulares para garantir a conformidade com regulamentações de segurança e padrões da indústria.
- Testes e Simulações: Realize testes regulares de segurança e simulações de ataques para avaliar a eficácia dos controles de segurança existentes.
- Gestão de Identidade e Acesso: Implemente sistemas de gestão de identidade e acesso (IAM) robustos para garantir que apenas usuários autorizados tenham acesso a sistemas e dados sensíveis.
- Monitoramento Contínuo: Estabeleça uma vigilância constante de ameaças e anomalias no ambiente de TI para detectar ameaças em estágio inicial.
- Inteligência de Ameaças: Utilize fontes de inteligência de ameaças para estar ciente das tendências e táticas de ataque atuais.

Essas práticas visam aumentar a eficiência operacional, promover a inovação em segurança cibernética e manter a vantagem competitiva, garantindo um ambiente seguro e protegido contra ameaças em constante evolução.

A Cybersecurity Strategy impacta a infraestrutura, arquitetura, sistemas, segurança cibernética e modelo operacional de TI, garantindo a proteção dos ativos digitais em um cenário cibernético desafiador.

Desafios Atuais

A Cybersecurity Strategy é uma capability fundamental para proteger a integridade, confidencialidade e disponibilidade dos dados e sistemas de uma organização no cenário de ameaças cibernéticas em constante evolução.

No entanto, ao adotar e integrar essa capability em seus processos de negócios e operações de TI, as organizações enfrentam uma série de desafios atuais no mercado, conforme definido pelo CIO Codex Capability Framework.

Abaixo os principais desafios:

- Evolução das Ameaças Cibernéticas: As ameaças cibernéticas estão em constante evolução, com adversários usando táticas cada vez mais sofisticadas. Isso exige uma estratégia dinâmica para enfrentar ameaças em evolução.
- Escassez de Talentos em Cibersegurança: A demanda por profissionais de cibersegurança qualificados supera a oferta, tornando difícil para as organizações encontrarem e reter talentos adequados.
- Complexidade Tecnológica: A crescente complexidade das infraestruturas de TI, incluindo nuvens públicas, privadas e sistemas legados, torna desafiador proteger todos os pontos de entrada possíveis.
- Privacidade de Dados e Regulamentações: Regulamentações rigorosas de privacidade de dados, como o GDPR, impõem desafios adicionais para garantir a conformidade e proteger os dados dos clientes.
- Ameaças Internas: A ameaça interna representa um desafio, pois funcionários podem inadvertidamente ou intencionalmente comprometer a segurança cibernética da organização.
- Cibersegurança em Nuvem: A migração para a nuvem requer uma abordagem de segurança diferente, o que pode ser um desafio na criação de estratégias abrangentes.
- Orçamento Limitado: Restrições orçamentárias podem limitar a capacidade de investir em tecnologias e treinamento necessários para fortalecer a cibersegurança.
- Gerenciamento de Riscos: Avaliar e priorizar riscos cibernéticos de forma eficaz é um desafio, especialmente em organizações com muitos ativos digitais.
- Educação da Força de Trabalho: A conscientização e treinamento

contínuos dos funcionários são essenciais, mas podem ser difíceis de implementar de maneira eficaz.
- Cibersegurança de Terceiros: À medida que as organizações dependem de terceiros para serviços e soluções, garantir que esses parceiros atendam aos padrões de segurança torna-se um desafio crítico.

Esses desafios refletem a complexidade e a dinâmica do cenário de cibersegurança atual.

Com ameaças em constante evolução, escassez de talentos, regulamentações rigorosas e a necessidade de proteger uma variedade de ambientes tecnológicos, a Cybersecurity Strategy é mais crucial do que nunca.

Enfrentar esses desafios exige uma abordagem estratégica e uma compreensão profunda das melhores práticas de segurança cibernética.

A capability de desenvolver e implementar uma estratégia de segurança cibernética alinhada aos objetivos de negócios e adaptada às ameaças emergentes é fundamental para proteger os ativos digitais e manter a confiança dos clientes, parceiros e stakeholders.

Investir na Cybersecurity Strategy não é apenas uma resposta aos desafios atuais, mas também uma preparação para um futuro em constante evolução no cenário de cibersegurança.

Tendências para o Futuro

A Cybersecurity Strategy, dentro do contexto do CIO Codex Capability Framework, desempenha um papel crucial na proteção da integridade, confidencialidade e disponibilidade dos dados e sistemas de uma organização.

Para garantir sua eficácia contínua, é imperativo considerar as tendências futuras que moldarão essa capability.

As expectativas do mercado apontam para diversas tendências que impactarão a estratégia de segurança cibernética:

- IA e Machine Learning em Defesa Cibernética: O uso crescente de Inteligência Artificial (IA) e Machine Learning permitirá a detecção e resposta automatizada a ameaças cibernéticas em tempo real,

melhorando a eficiência da estratégia de segurança.

- Zero Trust Architecture (ZTA): A ZTA ganhará destaque, onde a confiança não é automaticamente concedida a dispositivos ou usuários, mesmo dentro da rede interna, tornando a segurança mais granular e adaptável.
- 5G e IoT: Com a expansão da tecnologia 5G e a proliferação da Internet das Coisas (IoT), a superfície de ataque aumentará, exigindo estratégias de segurança cibernética mais robustas e abrangentes.
- Segurança de Cloud: Com a migração contínua para ambientes de nuvem, a segurança cibernética se concentrará mais na proteção de dados e aplicativos na nuvem.
- Criptomoedas e Ransomware: O aumento no uso de criptomoedas facilitará o pagamento de resgates em ataques de ransomware, tornando esses ataques ainda mais lucrativos e preocupantes.
- Legislação de Proteção de Dados: Novas regulamentações de proteção de dados, inspiradas no GDPR, continuarão a surgir, exigindo que as organizações fortaleçam suas estratégias de privacidade e segurança.
- Cibersegurança Quântica: A computação quântica poderá quebrar algoritmos de criptografia convencionais, impulsionando o desenvolvimento de soluções de segurança pós-quântica.
- Colaboração entre Empresas: Empresas colaborarão mais estreitamente para compartilhar informações sobre ameaças e fortalecer suas defesas coletivas contra ataques cibernéticos.
- Treinamento de Conscientização de Segurança: A conscientização de segurança será uma prioridade, com foco em educar todos os funcionários sobre melhores práticas e ameaças emergentes.
- IA Ética em Segurança Cibernética: A ética em IA será integrada à estratégia de segurança cibernética, garantindo a tomada de decisões responsáveis e justas em resposta a ameaças.

Essas tendências futuras refletem a crescente complexidade e sofisticação das ameaças cibernéticas e a necessidade de uma estratégia de segurança cibernética ágil e adaptável.

A Cybersecurity Strategy deve evoluir continuamente para enfrentar esses desafios e proteger os ativos digitais de uma organização de maneira eficaz e proativa.

KPIs Usuais

A capacidade de Cybersecurity Strategy desempenha um papel vital na proteção dos ativos digitais de uma organização, garantindo a integridade, confidencialidade e disponibilidade dos dados e sistemas.

Para avaliar eficazmente essa capability, é fundamental acompanhar os KPIs adequados.

Abaixo estão os principais KPIs usuais no contexto do CIO Codex Capability Framework:

- Taxa de Detecção de Ameaças Cibernéticas (Cyber Threat Detection Rate): Mede a eficácia na detecção precoce de ameaças cibernéticas, indicando a capacidade de identificar incidentes em estágios iniciais.
- Taxa de Resposta a Incidentes (Incident Response Rate): Avalia a rapidez e eficácia da resposta a incidentes de segurança cibernética, incluindo a mitigação de ameaças e a recuperação de sistemas afetados.
- Nível de Conformidade com Políticas de Segurança (Security Policy Compliance Level): Indica o grau de conformidade das operações de TI com as políticas de segurança cibernética estabelecidas.
- Tempo Médio de Correção de Vulnerabilidades (Mean Time to Remediate Vulnerabilities): Calcula o tempo médio necessário para corrigir vulnerabilidades identificadas em sistemas e aplicativos.
- Taxa de Treinamento em Segurança Cibernética (Cybersecurity Training Rate): Mede a participação dos colaboradores em programas de treinamento em segurança cibernética, refletindo a conscientização e educação da equipe.
- Avaliação de Vulnerabilidades Ativas (Active Vulnerability Assessment): Avalia a frequência e eficácia das análises regulares de vulnerabilidades nos ativos de TI.
- Taxa de Adoção de Tecnologias de Segurança Emergentes (Adoption of Emerging Security Technologies): Avalia a implementação de tecnologias avançadas de segurança cibernética para proteção proativa contra ameaças emergentes.
- Tempo Médio de Detecção de Ameaças Internas (Mean Time to Detect Insider Threats): Calcula o tempo médio necessário para detectar ameaças internas, como comportamento suspeito de colaboradores.

- Taxa de Auditoria de Segurança (Security Audit Rate): Mede a frequência das auditorias de segurança cibernética para garantir a conformidade com regulamentações e padrões.
- Avaliação da Maturidade em Segurança Cibernética (Cybersecurity Maturity Assessment): Avalia o nível de maturidade da organização em termos de práticas e políticas de segurança cibernética.
- Taxa de Cumprimento de Planos de Ação (Action Plan Compliance Rate): Indica o grau de conformidade com os planos de ação para abordar vulnerabilidades e ameaças identificadas.
- Tempo Médio de Recuperação de Incidentes (Mean Time to Recover from Incidents): Calcula o tempo médio necessário para recuperar completamente os sistemas após um incidente de segurança cibernética.
- Avaliação da Conscientização da Alta Administração (Executive Awareness Assessment): Avalia o nível de conscientização da alta administração em relação aos riscos e desafios de segurança cibernética.
- Taxa de Incidentes Cibernéticos por Colaborador (Cyber Incidents per Employee Rate): Mede a frequência de incidentes cibernéticos por colaborador, identificando áreas de risco.
- Taxa de Redução de Incidentes Cibernéticos (Cyber Incident Reduction Rate): Avalia a eficácia das estratégias de segurança cibernética na redução do número de incidentes ao longo do tempo.

Esses KPIs desempenham um papel crítico na avaliação e melhoria contínua da Cybersecurity Strategy, permitindo que as organizações protejam seus ativos digitais, garantam a conformidade com regulamentações e padrões, e promovam uma cultura de segurança cibernética em toda a organização.

Exemplos de OKRs

A capability de Cybersecurity Strategy na macro capability Definition & Management da camada Cybersecurity é de extrema importância, pois envolve o desenvolvimento e a implementação de uma estratégia de segurança cibernética abrangente.

Esta capability se concentra em alinhar as iniciativas de segurança com os objetivos de negócio da organização, definindo prioridades, estabelecendo diretrizes de segurança e garantindo a alocação adequada de recursos para proteger contra ameaças

cibernéticas.

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

Desenvolvimento da Estratégia de Segurança Cibernética

Objetivo: Desenvolver uma estratégia de segurança cibernética que esteja alinhada com os objetivos de negócio.

- KR1: Realizar uma avaliação abrangente de riscos cibernéticos e vulnerabilidades.
- KR2: Definir objetivos de segurança cibernética que suportem os objetivos de negócio.
- KR3: Estabelecer um plano estratégico de segurança cibernética de longo prazo.

Definição de Diretrizes e Políticas de Segurança

Objetivo: Estabelecer diretrizes e políticas de segurança para orientar as práticas de segurança cibernética.

- KR1: Desenvolver políticas de segurança abrangentes que abordem ameaças cibernéticas específicas.
- KR2: Implementar diretrizes de segurança para funcionários e partes interessadas.
- KR3: Garantir a conformidade com regulamentações de segurança cibernética relevantes.

Priorização de Investimentos em Segurança

Objetivo: Priorizar e alocar recursos financeiros e de pessoal para iniciativas de segurança cibernética.

- KR1: Identificar áreas de maior risco que requerem investimento imediato.
- KR2: Estabelecer um orçamento dedicado à segurança cibernética.
- KR3: Avaliar a eficácia dos investimentos em segurança cibernética.

Treinamento e Conscientização em Segurança

Objetivo: Garantir que a equipe esteja bem-informada e treinada em práticas de segurança cibernética.

- KR1: Oferecer treinamento em segurança cibernética para todos os funcionários.
- KR2: Realizar exercícios regulares de conscientização sobre segurança.
- KR3: Monitorar a conformidade dos funcionários com as políticas de segurança.

Monitoramento e Resposta a Incidentes

Objetivo: Implementar sistemas de monitoramento para detectar e responder a ameaças cibernéticas em tempo real.

- KR1: Implementar ferramentas de monitoramento de segurança cibernética.
- KR2: Desenvolver procedimentos de resposta a incidentes.
- KR3: Reduzir o tempo médio de resposta a incidentes de segurança.

Esses OKRs destacam a importância crítica da capability de Cybersecurity Strategy.

Ao desenvolver uma estratégia sólida, definir diretrizes de segurança, priorizar investimentos, treinar a equipe e implementar sistemas de monitoramento, esta capability desempenha um papel fundamental na proteção da organização contra ameaças cibernéticas.

Ela garante que a segurança cibernética seja tratada como uma parte integral da estratégia de negócios, contribuindo para a resiliência e a segurança da organização.

Critérios para Avaliação de Maturidade

A capability Cybersecurity Strategy, inserida na macro capability Definition & Management e na camada Cybersecurity, desempenha um papel crucial no desenvolvimento e implementação de uma estratégia de segurança cibernética

abrangente.

Para avaliar a maturidade dessa capability, segue um modelo inspirado no CMMI, composto por cinco níveis: Inexistente, Inicial, Definido, Gerenciado e Otimizado.

Nível de Maturidade Inexistente

- Não há uma estratégia formal de segurança cibernética na organização.
- Não existem diretrizes para alinhar a segurança cibernética aos objetivos de negócio.
- Não há definição de prioridades em termos de segurança cibernética.
- Não há alocação de recursos específicos para proteção contra ameaças cibernéticas.
- A organização não possui políticas de segurança cibernética.

Nível de Maturidade Inicial

- Uma estratégia de segurança cibernética inicial está em desenvolvimento.
- As diretrizes para alinhar a segurança cibernética aos objetivos de negócio começam a ser definidas.
- Prioridades em termos de segurança cibernética estão sendo estabelecidas.
- Recursos estão sendo alocados de forma limitada para proteção contra ameaças cibernéticas.
- Políticas de segurança cibernética estão sendo criadas, mas ainda não estão totalmente implementadas.

Nível de Maturidade Definido

- Uma estratégia de segurança cibernética formal e documentada está em vigor.
- As diretrizes de segurança cibernética estão claramente definidas e alinhadas com os objetivos de negócio.
- Prioridades de segurança cibernética são bem compreendidas e comunicadas.
- Recursos são alocados de forma consistente para proteção contra

ameaças cibernéticas.
- Políticas de segurança cibernética são implementadas e periodicamente revisadas para conformidade.

Nível de Maturidade Gerenciado

- A estratégia de segurança cibernética é eficaz e periodicamente revisada para ajustes.
- As diretrizes de segurança cibernética são monitoradas e atualizadas regularmente.
- Prioridades de segurança cibernética são dinâmicas e adaptáveis a novas ameaças.
- Recursos são gerenciados eficazmente para proteção contínua contra ameaças cibernéticas.
- Auditorias regulares garantem a conformidade com as políticas de segurança cibernética.

Nível de Maturidade Otimizado

- A estratégia de segurança cibernética é altamente otimizada, aproveitando tecnologias avançadas.
- As diretrizes de segurança cibernética são dinâmicas e baseadas em análises de risco contínuas.
- Prioridades de segurança cibernética são ágeis e adaptáveis a cenários em constante evolução.
- Recursos são alocados de forma inteligente e eficiente para proteção contra ameaças cibernéticas.
- A organização está constantemente atualizada com as melhores práticas de segurança cibernética e antecipa ameaças emergentes.

Esses critérios de maturidade são essenciais para avaliar o desenvolvimento e implementação eficazes da estratégia de segurança cibernética.

À medida que a organização progride nos níveis de maturidade, sua capacidade de proteger-se contra ameaças cibernéticas e alinhar a segurança com os objetivos de

negócio é aprimorada, garantindo a resiliência e a segurança das operações.

Convergência com Frameworks de Mercado

A capability Cybersecurity Strategy, integrante da macro capability Definition & Management e localizada na camada Cybersecurity, é vital para o desenvolvimento e a implementação de uma estratégia de segurança cibernética abrangente.

Esta capability concentra-se em harmonizar as iniciativas de segurança com os objetivos de negócio da organização, estabelecendo prioridades, diretrizes de segurança e garantindo a alocação apropriada de recursos para a proteção contra ameaças cibernéticas.

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 segurança da informação. A Cybersecurity Strategy é fundamental para atender aos padrões do COBIT, pois garante que as políticas de segurança estejam em alinhamento com os objetivos organizacionais e os processos de governança.

ITIL

- Nível de Convergência: Alto
- Racional: O ITIL ressalta a importância da gestão de serviços de TI, incluindo a segurança. A Cybersecurity Strategy apoia o ITIL ao assegurar que as práticas de segurança estejam integradas aos processos de gestão de serviços, aumentando a resiliência dos serviços de TI.

SAFe

- Nível de Convergência: Médio
- Racional: Embora o SAFe se concentre em metodologias ágeis para o desenvolvimento de software, uma estratégia de cibersegurança robusta complementa o SAFe ao reforçar a segurança nos ciclos de desenvolvimento e entrega.

PMI

- Nível de Convergência: Médio
- Racional: O PMI aborda a gestão de projetos, onde a segurança pode ser um aspecto crítico. Uma estratégia de cibersegurança eficaz pode melhorar a segurança dos projetos de TI, alinhando-se aos padrões de gestão do PMI.

CMMI

- Nível de Convergência: Médio
- Racional: O CMMI visa a melhoria dos processos. Uma estratégia de cibersegurança eficaz contribui para a maturidade dos processos, especialmente na gestão de riscos e na segurança de informações.

TOGAF

- Nível de Convergência: Alto
- Racional: O TOGAF se foca na arquitetura empresarial, onde a segurança é um componente crucial. A Cybersecurity Strategy assegura que as considerações de segurança estejam incorporadas na arquitetura de TI, promovendo alinhamento estratégico e operacional.

DevOps SRE

- Nível de Convergência: Médio
- Racional: Em DevOps e SRE, a segurança é frequentemente integrada ao ciclo de vida do desenvolvimento. Uma estratégia de cibersegurança robusta fortalece essa integração, promovendo práticas seguras de desenvolvimento e operações.

NIST

- Nível de Convergência: Alto
- Racional: O NIST fornece diretrizes detalhadas para a segurança cibernética. A Cybersecurity Strategy está fortemente alinhada com o NIST ao estabelecer um framework para a implementação de controles de segurança eficazes e gerenciamento de riscos.

Six Sigma

- Nível de Convergência: Baixo
- Racional: Embora o Six Sigma foque na melhoria da qualidade e na redução de defeitos, uma estratégia de cibersegurança pode contribuir indiretamente para esses objetivos, ao reduzir riscos e vulnerabilidades que podem impactar a qualidade e a eficiência dos processos.

Lean IT

- Nível de Convergência: Baixo
- Racional: Lean IT enfoca a eficiência operacional, enquanto a Cybersecurity Strategy se concentra mais na segurança. No entanto, pode haver uma convergência indireta, uma vez que uma boa estratégia de segurança pode prevenir interrupções e perdas, contribuindo assim para a eficiência operacional.

A Cybersecurity Strategy é fundamental na era digital, pois não apenas fortalece a segurança das informações e sistemas de uma organização, mas também assegura que as práticas de segurança estejam em sintonia com os objetivos estratégicos e

operacionais da organização.

KPIs relevantes para esta capability incluem a taxa de incidentes de segurança resolvidos, o tempo de resposta a incidentes de segurança e a eficácia das medidas preventivas implementadas.

A estratégia de cibersegurança eficazmente implementada e gerida não apenas eleva a maturidade da organização em termos de segurança, mas também apoia a sua resiliência operacional e a capacidade de resposta a ameaças emergentes.

Processos e Atividades

Develop Cybersecurity Strategy

O desenvolvimento de uma estratégia de segurança cibernética é um processo fundamental para alinhar as práticas de segurança com os objetivos estratégicos da organização.

Esse processo envolve a análise detalhada do ambiente de ameaças cibernéticas, a identificação de vulnerabilidades e a definição de um plano abrangente que inclua políticas, procedimentos e controles de segurança.

O objetivo é criar uma abordagem estruturada e proativa para proteger os ativos digitais da organização, minimizando os riscos e garantindo a continuidade dos negócios.

A estratégia deve considerar as tecnologias emergentes, tendências de mercado e regulamentos de conformidade.

Além disso, é crucial garantir que a estratégia seja comunicada e compreendida por todos os níveis da organização, promovendo uma cultura de segurança robusta e colaborativa.

O desenvolvimento de uma estratégia de segurança cibernética bem fundamentada proporciona uma base sólida para todas as iniciativas de segurança subsequentes, permitindo uma resposta eficaz às ameaças e incidentes.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Conduct Threat Analysis	Realizar análise detalhada do ambiente de ameaças cibernéticas.	Dados de ameaças, histórico de incidentes	Relatório de análise de ameaças	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
2	Identify Vulnerabilities	Identificar vulnerabilidades nos sistemas e aplicativos da organização.	Relatório de análise de ameaças	Lista de vulnerabilidades	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: IT Infrastructure & Operation; Executer: Cybersecurity
3	Define Security Policies	Definir políticas, procedimentos e controles de segurança cibernética.	Lista de vulnerabilidades	Políticas de segurança	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: Architecture & Technology Visioning; Recommender: IT Governance & Transformation; Executer: Cybersecurity

4	Develop Resource Plan	Desenvolver um plano de alocação de recursos para implementar a estratégia.	Políticas de segurança	Plano de recursos	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
5	Communicate Strategy	Comunicar a estratégia de segurança cibernética a todos os níveis da organização.	Plano de recursos	Estratégia comunicada	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity

Identify Cybersecurity Objectives

A definição dos objetivos de segurança cibernética é um processo crítico que estabelece as metas específicas que a organização pretende alcançar em termos de proteção de seus ativos digitais.

Este processo envolve a consulta a stakeholders, a análise dos requisitos de negócios e a avaliação das ameaças e vulnerabilidades identificadas para definir objetivos claros e mensuráveis.

Esses objetivos devem ser alinhados com a estratégia geral de negócios da organização e considerar os aspectos de confidencialidade, integridade e disponibilidade dos dados e sistemas.

Além disso, é essencial priorizar os objetivos com base na criticidade dos ativos e no impacto potencial das ameaças, garantindo que os recursos sejam alocados de maneira eficaz para mitigar os riscos mais significativos.

A definição precisa dos objetivos de segurança cibernética fornece uma base sólida para a implementação de controles de segurança e para a medição contínua do desempenho e da eficácia das iniciativas de segurança.

- PDCA focus: Plan

- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Stakeholder Consultation	Realizar consultas com stakeholders para entender os requisitos de segurança.	Requisitos de negócios, feedback de stakeholders	Dados coletados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
2	Analyze Business Requirements	Analisar os requisitos de negócios para alinhar os objetivos de segurança cibernética.	Dados coletados, requisitos de negócios	Relatório de análise	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: Architecture & Technology Visioning; Recommender: IT Governance & Transformation; Executer: Cybersecurity
3	Evaluate Threats and Vulnerabilities	Avaliar ameaças e vulnerabilidades para identificar áreas críticas de foco.	Relatório de análise, lista de vulnerabilidades	Áreas críticas identificadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity

4	Define Security Objectives	Definir objetivos de segurança cibernética claros e mensuráveis.	Áreas críticas identificadas	Objetivos de segurança	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
5	Prioritize Objectives	Priorizar os objetivos de segurança cibernética com base na criticidade dos ativos.	Objetivos de segurança	Objetivos priorizados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity

Implement Cybersecurity Initiatives

A implementação das iniciativas de segurança cibernética é um processo vital para transformar as estratégias e objetivos de segurança em ações concretas e medidas de proteção eficazes.

Esse processo envolve a execução de projetos e programas específicos destinados a fortalecer a postura de segurança da organização.

As atividades incluem a instalação de ferramentas de segurança, a configuração de sistemas de monitoramento, a realização de treinamentos e a implementação de políticas e procedimentos definidos na estratégia.

A implementação deve ser cuidadosamente planejada e gerenciada para garantir que todos os componentes necessários estejam integrados de forma coesa e que os recursos sejam utilizados de maneira eficiente.

Além disso, é essencial monitorar continuamente o progresso das iniciativas e ajustar as abordagens conforme necessário para abordar novas ameaças e vulnerabilidades.

A execução eficaz deste processo assegura que a organização esteja equipada para prevenir, detectar e responder a incidentes de segurança cibernética de forma

proativa e resiliente.

- PDCA focus: Do
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Develop Implementation Plan	Desenvolver um plano detalhado para a implementação das iniciativas de segurança.	Estratégia de segurança, objetivos priorizados	Plano de implementação	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Data, AI & New Technology; Executer: Cybersecurity
2	Install Security Tools	Instalar e configurar ferramentas de segurança cibernética.	Plano de implementação	Ferramentas de segurança instaladas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: Architecture & Technology Visioning; Recommender: Solution Engineering & Development; Executer: Cybersecurity
3	Configure Monitoring Systems	Configurar sistemas de monitoramento para detectar e responder a incidentes.	Ferramentas de segurança instaladas	Sistemas de monitoramento configurados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Data, AI & New Technology; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity

4	Conduct Security Training	Realizar treinamentos de segurança para os colaboradores.	Sistemas de monitoramento configurados	Colaboradores treinados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Data, AI & New Technology; Executer: Cybersecurity
5	Implement Policies and Procedures	Implementar políticas e procedimentos de segurança definidos na estratégia.	Colaboradores treinados	Políticas e procedimentos implementados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: Architecture & Technology Visioning; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Monitor Cybersecurity Performance

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

Este processo envolve o uso de ferramentas e sistemas de monitoramento para acompanhar a atividade da rede, identificar padrões suspeitos e responder a incidentes de segurança em tempo real.

Através da coleta e análise de dados de segurança, é possível detectar vulnerabilidades e brechas antes que elas possam ser exploradas.

Além disso, o monitoramento contínuo fornece insights valiosos sobre a eficácia das políticas e controles de segurança, permitindo ajustes e melhorias contínuas.

Este processo não apenas ajuda a manter a integridade e a disponibilidade dos sistemas e dados, mas também demonstra o compromisso da organização com a segurança cibernética aos stakeholders.

- PDCA focus: Check
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Set Up Monitoring Tools	Configurar e calibrar ferramentas de monitoramento para acompanhar a atividade da rede.	Ferramentas de monitoramento	Ferramentas configuradas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: Solution Engineering & Development; Recommender: Data, AI & New Technology; Executer: Cybersecurity
2	Monitor Network Activity	Monitorar a atividade da rede para identificar padrões suspeitos.	Ferramentas configuradas	Relatórios de atividade	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Data, AI & New Technology; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
3	Detect Security Incidents	Detectar e responder a incidentes de segurança em tempo real.	Relatórios de atividade	Incidentes detectados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: Architecture & Technology Visioning; Recommender: Solution Engineering & Development; Executer: Cybersecurity

4	Analyze Security Data	Analisar dados de segurança para identificar vulnerabilidades e brechas.	Incidentes detectados	Relatório de análise	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: Data, AI & New Technology; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
5	Report Security Metrics	Relatar métricas de segurança e insights para a alta gestão e stakeholders.	Relatório de análise	Relatórios de métricas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: Architecture & Technology Visioning; Recommender: Data, AI & New Technology; Executer: Cybersecurity

Review and Update Cybersecurity Strategy

A revisão e atualização da estratégia de segurança cibernética é um processo essencial para garantir que as políticas e controles de segurança da organização permaneçam eficazes e relevantes diante das mudanças no cenário de ameaças e nos objetivos de negócios.

Este processo envolve a análise dos dados coletados durante o monitoramento contínuo, a realização de auditorias e a consulta a stakeholders para identificar áreas de melhoria e ajustar a estratégia conforme necessário.

A revisão periódica permite que a organização incorpore novas tecnologias, melhore processos existentes e responda a novas ameaças de forma proativa.

Além disso, a atualização regular da estratégia demonstra o compromisso contínuo da organização com a segurança cibernética, fortalecendo a confiança dos clientes, parceiros e stakeholders.

Este processo é fundamental para manter a resiliência e a eficácia das defesas de segurança cibernética da organização.

- PDCA focus: Act
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Conduct Strategy Review	Realizar uma revisão detalhada da estratégia de segurança cibernética.	Relatórios de métricas, feedback de stakeholders	Relatório de revisão	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
2	Identify Improvement Areas	Identificar áreas de melhoria com base nos resultados da revisão de desempenho.	Relatório de revisão	Lista de áreas de melhoria	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
3	Update Security Policies	Atualizar políticas, procedimentos e controles de segurança conforme necessário.	Lista de áreas de melhoria	Políticas atualizadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: Architecture & Technology Visioning; Recommender: IT Governance & Transformation; Executer: Cybersecurity

4	Communicate Updates	Comunicar as atualizações de políticas e procedimentos a todos os colaboradores.	Políticas atualizadas	Estratégia comunicada	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
5	Validate Effectiveness	Validar a eficácia das atualizações implementadas através de testes e auditorias.	Estratégia comunicada	Relatório de validação	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity