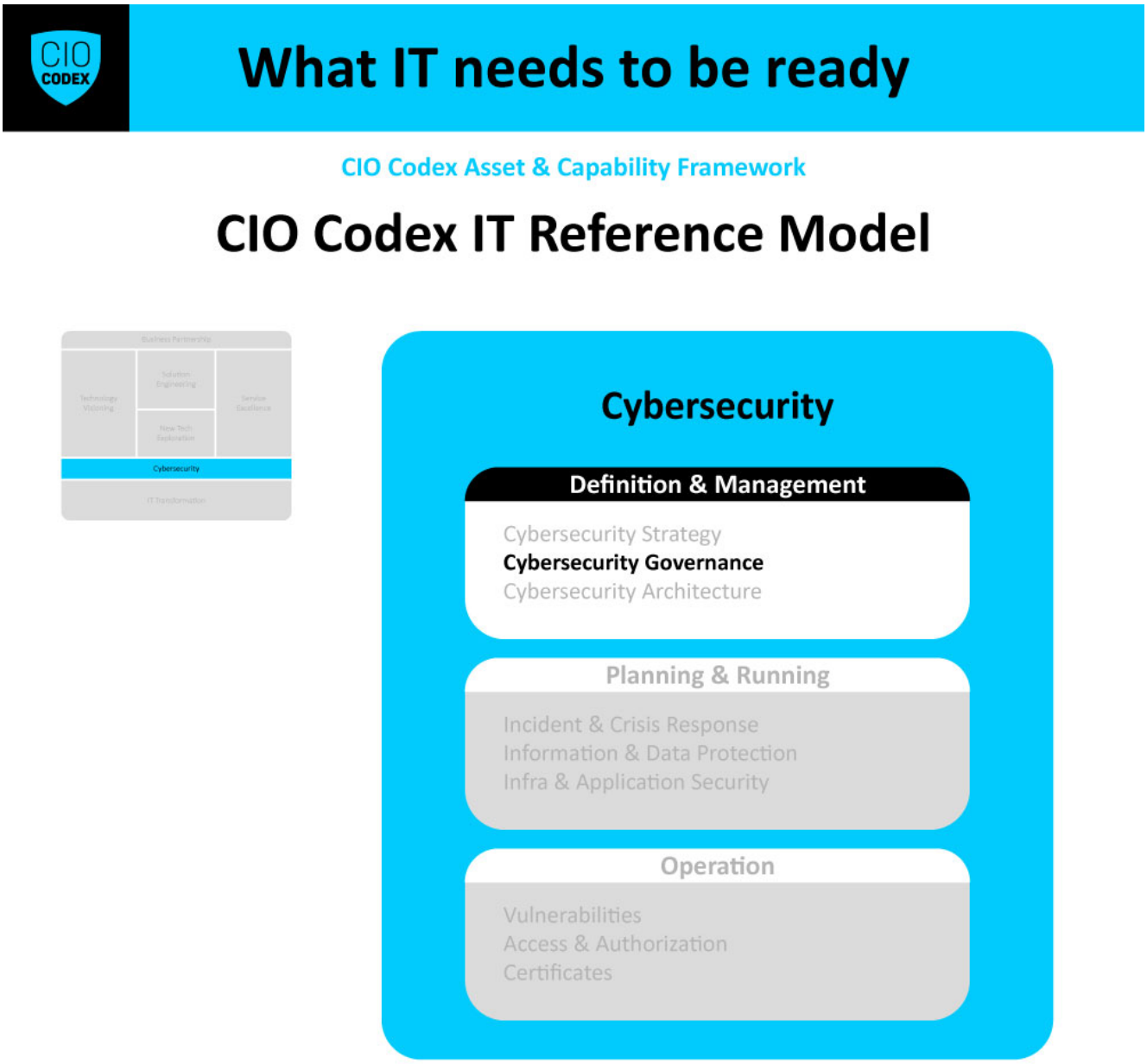

A Cybersecurity Governance, inserida na macro capability Definition & Management e englobada na camada Cybersecurity do CIO Codex Capability Framework, desempenha um papel crucial na manutenção de uma postura de segurança robusta e atualizada nas organizações.

Este domínio é essencial para enfrentar os desafios em constante evolução no campo das ameaças cibernéticas, assegurando uma gestão eficaz de todos os níveis de risco e proteção dos ativos de informação de forma eficiente e resiliente.

Os conceitos fundamentais que norteiam a Cybersecurity Governance incluem a própria governança de segurança cibernética, a conformidade regulatória e o controle de segurança.

A governança de segurança cibernética é compreendida como um conjunto de práticas e estruturas organizacionais que garantem a alinhamento da segurança cibernética com os objetivos estratégicos da empresa.

Já a conformidade regulatória implica no cumprimento de leis e normas pertinentes à segurança cibernética, resguardando a organização contra implicações legais.

Por fim, o controle de segurança engloba medidas técnicas e organizacionais implementadas para a proteção de ativos de informação e mitigação de riscos de segurança.

Características fundamentais da Cybersecurity Governance incluem o desenvolvimento de políticas de segurança, o monitoramento de conformidade, a avaliação de riscos de segurança, a realização de auditorias, a gestão de incidentes de segurança e a promoção de educação e conscientização sobre segurança cibernética.

Estes elementos colaboram para a criação de um framework de segurança cibernética robusto, que não apenas estabelece diretrizes e padrões para toda a organização, mas também assegura que estas sejam seguidas de acordo com as regulamentações aplicáveis.

O propósito central da Cybersecurity Governance é assegurar que as políticas, procedimentos e controles de segurança estejam alinhados às regulamentações e padrões da indústria, monitorando continuamente o cumprimento das políticas de segurança e avaliando de forma constante os riscos de segurança.

Através deste processo, a organização mantém uma postura de segurança eficaz e atualizada, essencial para a proteção de seus ativos digitais.

Os objetivos dentro do contexto do CIO Codex Capability Framework para a Cybersecurity Governance incluem o aumento da eficiência operacional através do estabelecimento de processos e procedimentos de governança, a garantia de conformidade regulatória para minimizar riscos legais, a promoção da inovação em práticas de segurança cibernética e a contribuição para a vantagem competitiva da organização, fortalecendo a confiança dos clientes e parceiros de negócios.

No âmbito tecnológico, a Cybersecurity Governance impacta significativamente várias dimensões. Na infraestrutura, define requisitos de segurança para a TI, assegurando proteção contra ameaças cibernéticas.

Na arquitetura, influencia a concepção de sistemas e aplicativos, integrando medidas de segurança desde o início. Nos sistemas, estabelece políticas de segurança abrangentes, que incluem aspectos como autenticação, autorização e criptografia.

Além disso, a governança de segurança cibernética determina a estrutura para tomada

de decisões e responsabilidades, garantindo a conformidade e eficácia das medidas de segurança.

Em resumo, a Cybersecurity Governance é uma capability vital para assegurar a resiliência e a eficácia das estratégias de segurança cibernética nas organizações.

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

A capacidade de gerir proativamente os riscos cibernéticos e manter a continuidade operacional diante de desafios na segurança digital é um diferencial competitivo fundamental, reforçando a reputação e a resiliência organizacional no cenário empresarial contemporâneo.

Conceitos e Características

A Cybersecurity Governance desempenha um papel crítico na manutenção de uma postura de segurança atualizada e eficaz.

Ela permite que as organizações enfrentem os desafios em constante evolução das ameaças cibernéticas, garantindo que todos os níveis de risco sejam devidamente gerenciados e que os ativos de informação estejam protegidos de maneira sólida e eficiente.

Conceitos

- Governança de Segurança Cibernética: Refere-se ao conjunto de práticas e estruturas organizacionais que asseguram que a segurança cibernética esteja alinhada com os objetivos estratégicos da organização.
- Conformidade Regulatória: Envolve o cumprimento das leis e regulamentos relacionados à segurança cibernética, garantindo que a organização esteja em conformidade com as obrigações legais.
- Controle de Segurança: São medidas técnicas e organizacionais implementadas para proteger ativos de informação e mitigar riscos de segurança.

Características

- Desenvolvimento de Políticas de Segurança: Criação de políticas de segurança abrangentes que estabelecem diretrizes e padrões de segurança para toda a organização.
- Monitoramento de Conformidade: Acompanhamento constante para garantir que todas as políticas e procedimentos de segurança sejam seguidos de acordo com as regulamentações aplicáveis.
- Avaliação de Riscos de Segurança: Identificação e análise contínua dos riscos de segurança cibernética para tomar medidas preventivas e corretivas.
- Auditoria de Segurança: Realização de auditorias internas e externas para avaliar a eficácia dos controles de segurança e conformidade.
- Gestão de Incidentes de Segurança: Preparação e resposta a incidentes de segurança cibernética, minimizando danos e impactos.
- Educação e Conscientização: Promover a conscientização sobre segurança cibernética em toda a organização, capacitando os colaboradores a agir de maneira segura.

Propósito e Objetivos

A Cybersecurity Governance é uma capability essencial que tem um papel fundamental na governança da segurança cibernética dentro de uma organização.

Seu propósito principal é garantir que as políticas, procedimentos e controles de segurança estejam em conformidade com as regulamentações e padrões da indústria.

Isso inclui o monitoramento contínuo do cumprimento das políticas de segurança e a avaliação constante dos riscos de segurança para manter uma postura de segurança eficaz e atualizada.

Objetivos

Dentro do contexto do CIO Codex Capability Framework, os objetivos da Cybersecurity Governance são:

- Eficiência Operacional: Estabelecer processos e procedimentos de governança de segurança que otimizem a eficiência operacional,

minimizando interrupções nos negócios devido a incidentes de segurança cibernética.
- Conformidade Regulatória: Garantir que a organização cumpra todas as regulamentações relevantes relacionadas à segurança cibernética, minimizando o risco de penalidades legais.
- Inovação: Promover a inovação em práticas de segurança cibernética, adotando as melhores práticas e abordagens mais recentes para proteger ativos digitais.
- 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 Governance influencia significativamente várias dimensões da tecnologia:

- Infraestrutura: Define requisitos de segurança para a infraestrutura de TI, garantindo que os componentes de rede e sistemas críticos estejam protegidos contra ameaças cibernéticas.
- Arquitetura: Orienta a arquitetura de sistemas e aplicativos, incorporando medidas de segurança desde a concepção.
- Sistemas: Define políticas de segurança para sistemas e aplicativos, incluindo autenticação, autorização e criptografia.
- Cybersecurity: A governança de segurança cibernética estabelece a estrutura de tomada de decisões e responsabilidades para garantir a conformidade e a eficácia das medidas de segurança.
- Modelo Operacional: Estabelece processos de governança para monitorar e avaliar o cumprimento das políticas de segurança, bem como a gestão de riscos cibernéticos em curso.

Roadmap de Implementação

A Cybersecurity Governance é uma capability essencial no contexto da cibersegurança que desempenha um papel crítico na manutenção de uma postura de segurança atualizada e eficaz.

Sua implementação adequada permite que as organizações enfrentem os desafios em constante evolução das ameaças cibernéticas, garantindo que todos os níveis de risco sejam devidamente gerenciados e que os ativos de informação estejam protegidos de maneira sólida e eficiente.

- Compreensão dos Princípios de Governança: O primeiro passo na implementação da Cybersecurity Governance é garantir que todos os envolvidos na organização compreendam os princípios fundamentais da governança de segurança cibernética. Isso envolve a educação dos líderes e das equipes de TI sobre a importância da governança e seu impacto na segurança.
- Avaliação do Estado Atual: Realize uma avaliação detalhada do estado atual da governança de segurança cibernética na organização. Identifique pontos fortes e áreas de melhoria para orientar o desenvolvimento da estratégia de governança.
- Definição de Estrutura de Governança: Estabeleça uma estrutura de governança clara que inclua papéis, responsabilidades e tomada de decisões relacionadas à segurança cibernética. Isso pode envolver a criação de comitês de segurança cibernética e a designação de proprietários de processos de governança.
- Desenvolvimento de Políticas e Procedimentos: Crie políticas de segurança cibernética abrangentes que estabeleçam diretrizes e padrões claros para toda a organização. Além disso, defina procedimentos para garantir o cumprimento dessas políticas.
- Implementação de Controles de Governança: Implemente controles de governança que permitam a monitorização e conformidade contínuas. Isso pode incluir sistemas de monitoramento de conformidade e avaliações regulares.
- Treinamento e Conscientização: Eduque e treine os funcionários sobre as políticas e práticas de governança de segurança cibernética. Certifique-se de que todos os colaboradores compreendam suas responsabilidades em

relação à governança.

- Avaliação de Riscos e Auditorias: Realize avaliações regulares de riscos de segurança cibernética e auditorias internas para avaliar a eficácia dos controles de governança. Use os resultados para fazer melhorias contínuas.
- Melhoria Contínua: Estabeleça um ciclo de melhoria contínua da governança de segurança cibernética. Isso envolve a revisão regular das políticas, procedimentos e controles para garantir que permaneçam eficazes em um ambiente em constante evolução.
- Conformidade Regulatória: Garanta que a governança de segurança cibernética esteja em conformidade com todas as regulamentações e padrões relevantes. Mantenha-se atualizado sobre as mudanças nas exigências regulatórias.
- Comunicação e Transparência: Promova uma cultura de comunicação aberta e transparente em relação à governança de segurança cibernética. Mantenha todas as partes interessadas informadas sobre o progresso e os desafios.
- Alocação de Recursos: Certifique-se de que recursos adequados, como pessoal, tecnologia e orçamento, estejam disponíveis para implementar e manter a governança de segurança cibernética.

A implementação eficaz da Cybersecurity Governance é essencial para manter uma postura de segurança sólida e eficiente em um cenário de ameaças cibernéticas em constante evolução.

Ao seguir esse roadmap estratégico, a organização estará mais bem preparada para enfrentar ameaças cibernéticas, proteger seus ativos de informação e cumprir regulamentações relevantes, garantindo, assim, a integridade e a confidencialidade de seus dados e sistemas.

Melhores Práticas de Mercado

Dentro do contexto do CIO Codex Capability Framework, a Cybersecurity Governance é uma capability fundamental para manter a segurança cibernética em organizações.

As melhores práticas de mercado a seguir destacam abordagens essenciais para garantir a eficácia dessa capability:

- Governança Alinhada com Objetivos de Negócios: A governança de segurança cibernética deve ser alinhada com os objetivos estratégicos da organização. Isso assegura que as decisões relacionadas à segurança estejam em harmonia com as metas empresariais.
- Políticas de Segurança Claras: Desenvolver políticas de segurança abrangentes que estabeleçam diretrizes e padrões claros para toda a organização. Essas políticas devem abordar aspectos como acesso a dados, gestão de senhas e uso de dispositivos pessoais.
- Monitoramento de Conformidade Contínuo: Realizar monitoramento constante para garantir que todas as políticas e procedimentos de segurança sejam seguidos de acordo com as regulamentações aplicáveis. Isso envolve auditorias regulares e revisões internas.
- Avaliação Contínua de Riscos de Segurança: Identificar e analisar riscos de segurança cibernética de forma contínua. Isso permite tomar medidas preventivas e corretivas de forma proativa para mitigar ameaças em evolução.
- Auditorias de Segurança Regulares: Realizar auditorias internas e externas para avaliar a eficácia dos controles de segurança e garantir a conformidade com regulamentações e padrões da indústria.
- Gestão Eficaz de Incidentes de Segurança: Ter em vigor planos de resposta a incidentes de segurança cibernética, permitindo uma ação imediata em caso de violações de segurança. Isso minimiza danos e impactos.
- Promoção da Educação e Conscientização: Criar programas de conscientização sobre segurança cibernética em toda a organização. Isso capacita os colaboradores a reconhecer ameaças e a agir de maneira segura.
- Comitê de Segurança Cibernética: Estabelecer um comitê de segurança cibernética composto por membros-chave da organização. Esse comitê é responsável por tomar decisões estratégicas relacionadas à segurança.
- Benchmarking e Melhoria Contínua: Realizar benchmarking com outras organizações e setores para identificar melhores práticas e tendências emergentes em segurança cibernética. A organização deve buscar continuamente melhorias em suas práticas de segurança.
- Transparência e Comunicação: Manter comunicações claras e transparentes em relação às políticas e procedimentos de segurança cibernética. Isso promove a compreensão e o comprometimento de todos

os envolvidos.
- Automatização de Controles de Segurança: Utilizar ferramentas de automação para monitorar e reforçar os controles de segurança. Isso ajuda a identificar ameaças em tempo real e a agir de forma mais rápida.

A Cybersecurity Governance é essencial para garantir que todas as áreas de risco sejam gerenciadas e que os ativos de informação estejam protegidos de forma sólida e eficaz.

Ao seguir essas melhores práticas, as organizações podem fortalecer sua postura de segurança cibernética, minimizar riscos e demonstrar compromisso com a proteção de dados e sistemas.

Desafios Atuais

A Cybersecurity Governance desempenha um papel crítico na manutenção de uma postura de segurança atualizada e eficaz, alinhando a segurança cibernética com os objetivos estratégicos da organização.

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, como definido pelo CIO Codex Capability Framework.

Abaixo os principais desafios:

- Rápida Evolução das Ameaças Cibernéticas: As ameaças cibernéticas estão em constante mutação, tornando desafiador para as organizações acompanharem e se defenderem contra as últimas táticas e técnicas dos adversários cibernéticos.
- Complexidade das Regulamentações: As regulamentações de segurança cibernética estão se tornando mais complexas e variadas, tornando difícil para as organizações entender e cumprir todas as obrigações regulatórias.
- Gestão de Conformidade: Garantir o cumprimento contínuo das regulamentações é um desafio, pois exige monitoramento constante e conformidade com requisitos variados.
- Escassez de Recursos Qualificados: A falta de profissionais de segurança

cibernética qualificados é um obstáculo para as organizações que buscam implementar uma governança eficaz.

- Gestão de Riscos Cibernéticos: Identificar, avaliar e gerenciar riscos cibernéticos de maneira eficaz é um desafio, especialmente em organizações com ativos digitais extensos e diversificados.
- Resposta a Incidentes: Ter uma estratégia eficaz de resposta a incidentes cibernéticos é essencial, mas muitas organizações ainda não possuem planos de resposta bem definidos.
- Cultura de Segurança: Promover uma cultura de segurança cibernética em toda a organização é um desafio, pois requer educação, conscientização e mudança de comportamento dos funcionários.
- Orçamento Limitado: Restrições orçamentárias podem dificultar o investimento em tecnologias e recursos necessários para uma governança sólida de segurança cibernética.
- Fornecedores e Terceiros: Garantir que fornecedores e terceiros cumpram os padrões de segurança cibernética é crítico, mas muitas vezes é um desafio monitorar e garantir o cumprimento.
- Adoção de Tecnologias Emergentes: A rápida adoção de tecnologias emergentes, como IoT e IA, traz novos desafios de segurança que precisam ser abordados na governança de segurança cibernética.

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

Com ameaças em constante evolução, regulamentações complexas, falta de recursos e a necessidade de uma cultura de segurança sólida, a Cybersecurity Governance é crucial para garantir que as organizações estejam preparadas para enfrentar os desafios da segurança cibernética.

A capability de desenvolver e implementar políticas de segurança, monitorar a conformidade, avaliar riscos e responder a incidentes de maneira eficaz é fundamental para proteger os ativos de informação e manter a confiança dos clientes, parceiros e stakeholders.

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

Tendências para o Futuro

A Cybersecurity Governance é uma parte essencial da macro capability Definition & Management e desempenha um papel fundamental na garantia de que a segurança cibernética esteja alinhada com os objetivos estratégicos de uma organização.

Ao considerar as tendências futuras dentro deste contexto, é possível vislumbrar como essa capability evoluirá para enfrentar os desafios em constante evolução das ameaças cibernéticas e o cenário regulatório em mutação.

As expectativas do mercado apontam para várias tendências que moldarão o futuro da Cybersecurity Governance:

- Conformidade Multinacional: Com o aumento das regulamentações de privacidade de dados em todo o mundo, a Cybersecurity Governance terá que lidar com a complexidade de conformidade multinacional, adaptando-se às diferentes leis de proteção de dados em várias jurisdições.
- Ênfase na Responsabilidade Executiva: Espera-se que as organizações atribuam maior responsabilidade aos executivos de alto nível, como o Chief Information Security Officer (CISO), na governança de segurança cibernética, tornando-os diretamente responsáveis pela estratégia e conformidade.
- Automatização de Auditorias e Relatórios: A automação desempenhará um papel crucial na geração de relatórios de conformidade e auditorias de segurança, economizando tempo e recursos.
- Inteligência Artificial e Machine Learning em Governança: IA e Machine Learning serão usados para melhorar a identificação de riscos, avaliação de conformidade e detecção de ameaças, tornando a governança mais proativa e eficaz.
- Padrões de Governança de Segurança Cibernética: A criação de padrões globalmente reconhecidos para governança de segurança cibernética se tornará uma necessidade, proporcionando diretrizes claras para as organizações.
- Ênfase na Privacidade: A privacidade dos dados será uma consideração crítica na governança, à medida que as regulamentações de privacidade se tornarem mais rigorosas e as preocupações dos consumidores aumentarem.
- Auditorias Contínuas em Tempo Real: A capacidade de conduzir

auditorias de segurança cibernética em tempo real, em vez de auditorias pontuais, será uma tendência, permitindo uma resposta mais rápida a ameaças emergentes.
- Governança Distribuída: Com a crescente adoção de ambientes de trabalho remoto e tecnologias descentralizadas, a governança de segurança cibernética se adaptará para abranger sistemas distribuídos.
- Maior Integração com a Estratégia de Negócios: A governança de segurança cibernética se alinhará ainda mais com os objetivos estratégicos de negócios, incorporando considerações de segurança em todas as iniciativas empresariais.
- Treinamento de Conscientização de Segurança Ampliado: A conscientização de segurança será expandida para abranger não apenas funcionários, mas também parceiros de negócios e fornecedores, fortalecendo a postura geral de segurança.

Essas tendências futuras destacam a crescente importância da Cybersecurity Governance e a necessidade de adaptação contínua para enfrentar os desafios cibernéticos emergentes.

À medida que as ameaças e regulamentações evoluem, a governança de segurança cibernética deve permanecer ágil e eficaz para proteger os ativos digitais de uma organização de maneira sólida e eficiente.

KPIs Usuais

A capacidade de Cybersecurity Governance desempenha um papel crítico na garantia da segurança cibernética de uma organização.

Para avaliar e gerenciar eficazmente essa capability, é fundamental monitorar os KPIs apropriados.

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

- Taxa de Conformidade Regulatória (Regulatory Compliance Rate): Mede a conformidade da organização com leis e regulamentações relacionadas à segurança cibernética, garantindo o cumprimento das obrigações legais.

- Avaliação de Riscos de Segurança (Security Risk Assessment): Avalia a identificação e análise contínua dos riscos de segurança cibernética, permitindo a tomada de medidas preventivas e corretivas.
- Taxa de Cumprimento de Políticas de Segurança (Security Policy Compliance Rate): Indica o grau de conformidade com as políticas de segurança cibernética estabelecidas pela organização.
- Taxa de Auditorias de Segurança (Security Audit Rate): Mede a frequência das auditorias internas e externas para avaliar a eficácia dos controles de segurança e conformidade.
- Tempo Médio de Resposta a Incidentes de Segurança (Mean Time to Respond to Security Incidents): Calcula o tempo médio necessário para responder a incidentes de segurança cibernética, minimizando danos e impactos.
- Taxa de Atualização de Políticas de Segurança (Security Policy Update Rate): Avalia a frequência com que as políticas de segurança cibernética são revisadas e atualizadas para refletir as mudanças nas ameaças cibernéticas.
- Avaliação de Maturidade em Governança de Segurança (Security Governance Maturity Assessment): Mede o nível de maturidade da organização em termos de práticas e estruturas de governança de segurança cibernética.
- Taxa de Implementação de Controles de Segurança (Security Control Implementation Rate): Avalia a rapidez e eficácia na implementação de medidas técnicas e organizacionais para proteger ativos de informação.
- 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.
- Avaliação da Conscientização em Segurança Cibernética (Cybersecurity Awareness Assessment): Avalia o nível de conscientização dos colaboradores sobre segurança cibernética e suas responsabilidades na organização.
- Taxa de Implementação de Melhores Práticas (Best Practices Implementation Rate): Mede a adoção de melhores práticas reconhecidas na área de segurança cibernética.
- Tempo Médio de Atualização de Softwares e Patches (Mean Time to Software and Patch Updates): Calcula o tempo médio necessário para atualizar software e aplicar patches de segurança.

- Taxa de Resposta a Solicitações de Conformidade (Compliance Request Response Rate): Avalia a eficácia na resposta a solicitações de conformidade de reguladores e órgãos regulamentadores.
- Taxa de Redução de Incidentes de Segurança (Security Incident Reduction Rate): Mede a eficácia das estratégias de governança de segurança cibernética na redução do número de incidentes ao longo do tempo.
- Avaliação da Eficácia das Políticas de Segurança (Effectiveness Assessment of Security Policies): Avalia quão eficazes são as políticas de segurança cibernética em proteger os ativos de informação.

Esses KPIs são essenciais para avaliar a eficácia da Cybersecurity Governance, garantindo que as políticas, procedimentos e controles de segurança estejam alinhados com os objetivos estratégicos da organização, mantendo a conformidade regulatória e protegendo os ativos de informação contra ameaças cibernéticas em constante evolução.

Exemplos de OKRs

A capability de Cybersecurity Governance na macro capability Definition & Management da camada Cybersecurity é de extrema importância, pois está dedicada à governança da segurança cibernética.

Ela assegura que as políticas, procedimentos e controles de segurança estejam em conformidade com as regulamentações e padrões da indústria.

Além disso, inclui o monitoramento do cumprimento das políticas de segurança e a avaliação contínua dos riscos de segurança para garantir uma postura de segurança eficaz e atualizada.

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

Alinhamento com Regulamentações e Padrões de Segurança

Objetivo: Garantir que a organização esteja em conformidade com todas as regulamentações e padrões de segurança cibernética relevantes.

- KR1: Realizar uma avaliação de conformidade com as regulamentações de segurança aplicáveis.
- KR2: Implementar políticas e controles que estejam alinhados com os padrões de segurança reconhecidos.
- KR3: Manter atualizações regulares para refletir as mudanças nas regulamentações.

Monitoramento do Cumprimento das Políticas de Segurança

Objetivo: Monitorar e garantir o cumprimento das políticas de segurança cibernética estabelecidas.

- KR1: Implementar ferramentas de monitoramento de conformidade para políticas de segurança.
- KR2: Realizar auditorias regulares para avaliar o cumprimento das políticas.
- KR3: Manter registros precisos de incidentes de não conformidade e ações corretivas.

Avaliação Contínua de Riscos de Segurança

Objetivo: Realizar avaliações contínuas dos riscos de segurança cibernética e ajustar as medidas de segurança conforme necessário.

- KR1: Realizar avaliações de risco periódicas em todas as áreas críticas.
- KR2: Identificar ameaças emergentes e avaliar seu impacto potencial.
- KR3: Atualizar planos de mitigação de riscos com base nas descobertas das avaliações.

Melhoria Contínua da Postura de Segurança

Objetivo: Garantir que a postura de segurança da organização seja continuamente aprimorada e atualizada.

- KR1: Implementar um programa de treinamento em segurança cibernética para a equipe.
- KR2: Realizar testes de penetração regulares para identificar

vulnerabilidades.
- KR3: Implementar controles adicionais com base nas melhores práticas da indústria.

Resposta Efetiva a Incidentes de Segurança

Objetivo: Garantir uma resposta rápida e eficaz a incidentes de segurança cibernética.

- KR1: Desenvolver um plano de resposta a incidentes detalhado.
- KR2: Realizar simulações de incidentes para treinar a equipe de resposta.
- KR3: Reduzir o tempo médio de resposta a incidentes de segurança.

Através desses OKRs, a capability de Cybersecurity Governance desempenha um papel fundamental na garantia de que a organização mantenha uma postura de segurança cibernética forte e esteja em conformidade com as regulamentações e padrões relevantes.

Ela permite a governança eficaz das políticas de segurança, a avaliação contínua de riscos e a resposta adequada a incidentes, contribuindo para a proteção dos ativos e dados da organização.

Critérios para Avaliação de Maturidade

A capability Cybersecurity Governance, inserida na macro capability Definition & Management e na camada Cybersecurity, desempenha um papel crítico na governança da segurança cibernética de uma organização.

A avaliação da maturidade dessa capability é fundamental para assegurar que políticas, procedimentos e controles de segurança estejam em conformidade com regulamentações e padrões da indústria.

Abaixo estão os critérios de avaliação de maturidade em cinco níveis: Inexistente, Inicial, Definido, Gerenciado e Otimizado, inspirados no modelo CMMI.

Nível de Maturidade Inexistente

- Não há governança formal de segurança cibernética na organização.
- Não existem políticas ou procedimentos de segurança cibernética documentados.
- Não há monitoramento do cumprimento de políticas de segurança cibernética.
- A organização não está ciente dos riscos de segurança cibernética.
- Não há plano de ação para correção de vulnerabilidades identificadas.

Nível de Maturidade Inicial

- Iniciativas iniciais de governança de segurança cibernética estão sendo exploradas.
- Políticas de segurança cibernética estão sendo desenvolvidas, mas não estão formalizadas.
- Existe um monitoramento limitado do cumprimento das políticas de segurança.
- Alguma conscientização sobre riscos de segurança cibernética é promovida.
- Iniciativas reativas estão sendo tomadas para abordar vulnerabilidades conhecidas.

Nível de Maturidade Definido

- Uma estrutura formal de governança de segurança cibernética está em vigor.
- Políticas de segurança cibernética são documentadas e comunicadas.
- O monitoramento do cumprimento das políticas é regular e documentado.
- Uma abordagem proativa para avaliação de riscos de segurança cibernética é adotada.
- Planos de ação são desenvolvidos para mitigar riscos identificados.

Nível de Maturidade Gerenciado

- A governança de segurança cibernética é eficaz e adaptativa.

- As políticas de segurança cibernética são periodicamente revisadas e aprimoradas.
- O monitoramento do cumprimento das políticas é automatizado e em tempo real.
- Uma abordagem de gestão de riscos de segurança cibernética é implementada.
- Planos de ação são monitorados e executados de forma consistente.

Nível de Maturidade Otimizado

- A governança de segurança cibernética é altamente otimizada e inovadora.
- As políticas de segurança cibernética são ágeis e adaptáveis a ameaças em constante evolução.
- Monitoramento em tempo real e resposta automática a ameaças são implementados.
- A organização é líder em práticas de gestão de riscos de segurança cibernética.
- Planos de ação são revisados continuamente para otimização da segurança.

Esses critérios de maturidade são fundamentais para avaliar a eficácia da governança de segurança cibernética em uma organização.

À medida que a maturidade aumenta, a capacidade de garantir conformidade, promover a segurança e gerenciar riscos cibernéticos de forma eficiente e eficaz é aprimorada, fortalecendo a postura de segurança da organização.

Convergência com Frameworks de Mercado

A capability Cybersecurity Governance, pertencente à macro capability Definition & Management e integrada na camada Cybersecurity, é crucial para assegurar que as políticas, procedimentos e controles de segurança estejam em conformidade com

regulamentações e padrões da indústria.

Esta capability envolve o monitoramento do cumprimento das políticas de segurança e a avaliação contínua dos riscos de segurança, garantindo uma postura de segurança eficaz e atualizada.

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 destaca a governança de TI, incluindo a segurança cibernética. A Cybersecurity Governance é essencial para cumprir com os padrões do COBIT, assegurando que a governança da segurança cibernética esteja alinhada com os objetivos organizacionais e os processos de governança.

ITIL

- Nível de Convergência: Médio
- Racional: O ITIL enfoca a gestão de serviços de TI, incluindo aspectos de segurança. A Cybersecurity Governance complementa o ITIL ao integrar práticas de segurança nos processos de gestão de serviços e no gerenciamento de riscos associados.

SAFe

- Nível de Convergência: Médio
- Racional: O SAFe concentra-se em agilidade e desenvolvimento de software. Embora a governança de segurança cibernética não seja um foco direto, ela suporta o SAFe ao garantir a segurança nos ciclos de desenvolvimento e entrega.

PMI

- Nível de Convergência: Médio
- Racional: O PMI aborda amplamente a gestão de projetos, onde a governança de segurança cibernética pode desempenhar um papel importante na minimização de riscos relacionados à segurança em projetos de TI.

CMMI

- Nível de Convergência: Médio
- Racional: O CMMI visa a maturidade e a melhoria dos processos. A Cybersecurity Governance auxilia no alcance de uma maturidade maior em segurança, influenciando positivamente a avaliação de riscos e a gestão de processos de TI.

TOGAF

- Nível de Convergência: Alto
- Racional: O TOGAF foca na arquitetura empresarial, onde a governança de segurança cibernética é crucial. A Cybersecurity Governance assegura que a segurança seja uma parte integrante da arquitetura de TI e dos processos de tomada de decisão.

DevOps SRE

- Nível de Convergência: Médio
- Racional: Em DevOps e SRE, a segurança é frequentemente integrada ao ciclo de vida do desenvolvimento. A governança de segurança cibernética reforça esta 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 Governance está fortemente alinhada ao NIST, ao estabelecer um framework para a implementação de controles de segurança eficazes e gerenciamento de riscos.

Six Sigma

- Nível de Convergência: Baixo
- Racional: O Six Sigma concentra-se na melhoria da qualidade e redução de defeitos. A Cybersecurity Governance, embora não seja um foco direto do Six Sigma, pode contribuir para a melhoria da qualidade através da redução de riscos e vulnerabilidades de segurança.

Lean IT

- Nível de Convergência: Baixo
- Racional: Lean IT enfatiza a eficiência operacional, enquanto a Cybersecurity Governance se concentra mais na segurança. Apesar disso, uma governança de segurança eficaz pode contribuir para a eficiência ao prevenir interrupções e perdas relacionadas à segurança.

A Cybersecurity Governance é fundamental no contexto atual, onde as ameaças cibernéticas são uma realidade constante.

Ela não apenas fortalece a segurança da informação e dos sistemas de uma organização, mas também assegura que as práticas de segurança estejam em sintonia com os objetivos estratégicos e operacionais.

KPIs relevantes para esta capability incluem a taxa de conformidade com as políticas de segurança, 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 Governance Framework

O desenvolvimento de um framework de governança de segurança cibernética é essencial para estabelecer as diretrizes, políticas e procedimentos que orientarão todas as atividades de segurança dentro da organização.

Este processo envolve a análise dos requisitos regulatórios, a identificação das melhores práticas do setor e a integração desses elementos em um conjunto coeso de políticas que abrangem todos os aspectos da segurança cibernética.

O framework deve definir claramente as responsabilidades, as estruturas de comunicação e os mecanismos de controle necessários para garantir que as políticas de segurança sejam implementadas de maneira eficaz.

Além disso, deve considerar a flexibilidade para se adaptar a novas ameaças e mudanças no ambiente de negócios.

A criação de um framework robusto proporciona uma base sólida para todas as iniciativas de segurança subsequentes, garantindo a conformidade regulatória e a proteção dos ativos de informação da organização.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Conduct Regulatory Analysis	Realizar análise dos requisitos regulatórios aplicáveis.	Regulamentos, melhores práticas	Relatório de análise regulatória	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity

2	Identify Best Practices	Identificar as melhores práticas de governança de segurança cibernética no setor.	Relatório de análise regulatória	Lista de melhores práticas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
3	Develop Policy Framework	Desenvolver o framework de políticas de segurança baseado nas análises realizadas.	Lista de melhores práticas	Framework de políticas de segurança	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
4	Define Roles and Responsibilities	Definir os papéis e responsabilidades dentro do framework de governança.	Framework de políticas	Estrutura de papéis definida	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
5	Establish Communication Mechanisms	Estabelecer mecanismos de comunicação para assegurar a implementação do framework.	Estrutura de papéis definida	Mecanismos de comunicação	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Plan Governance Activities

O planejamento das atividades de governança de segurança cibernética é fundamental para garantir que todas as iniciativas e ações de segurança estejam alinhadas com o framework de governança estabelecido e com os objetivos estratégicos da organização.

Este processo envolve a definição de um plano detalhado que inclui a priorização das atividades, a alocação de recursos, a definição de metas e indicadores de desempenho, e a identificação de responsabilidades específicas para cada atividade.

O plano deve considerar tanto as atividades rotineiras quanto as ações corretivas e preventivas necessárias para manter a conformidade e a eficácia das políticas de segurança.

Além disso, é essencial incorporar a flexibilidade para responder a incidentes e novas ameaças de forma eficiente.

O planejamento eficaz das atividades de governança permite uma gestão proativa da segurança cibernética, assegurando que os riscos sejam mitigados e que a organização mantenha uma postura de segurança robusta.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Identify Governance Priorities	Identificar as prioridades de governança de segurança cibernética.	Framework de governança	Lista de prioridades	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity

2	Allocate Resources	Alocar recursos necessários para as atividades de governança.	Lista de prioridades	Plano de alocação de recursos	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
3	Define Performance Metrics	Definir métricas de desempenho para avaliar a eficácia das atividades de governança.	Plano de alocação de recursos	Lista de métricas de desempenho	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
4	Assign Responsibilities	Designar responsabilidades específicas para cada atividade planejada.	Lista de métricas de desempenho	Plano de responsabilidades	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
5	Develop Action Plan	Desenvolver um plano de ação detalhado para a implementação das atividades de governança.	Plano de responsabilidades	Plano de ação	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Implement Governance Practices

A implementação das práticas de governança de segurança cibernética é crucial para assegurar que as políticas e procedimentos estabelecidos sejam seguidos de maneira eficaz.

Este processo envolve a execução das atividades planejadas, a aplicação das políticas de segurança, a configuração dos controles necessários e a realização de treinamentos para garantir que todos os colaboradores compreendam e cumpram as diretrizes de segurança.

A implementação deve ser monitorada continuamente para identificar e resolver quaisquer desvios ou problemas que possam surgir.

Além disso, é importante documentar todas as atividades e ações realizadas para manter um registro claro de conformidade e facilitar auditorias futuras.

A implementação bem-sucedida das práticas de governança fortalece a postura de segurança da organização, garantindo que os riscos cibernéticos sejam mitigados e que a conformidade com as regulamentações seja mantida.

- PDCA focus: Do
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Execute Action Plan	Executar o plano de ação detalhado para implementar as práticas de governança.	Plano de ação	Ações executadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
2	Apply Security Policies	Aplicar políticas de segurança em toda a organização.	Ações executadas	Políticas aplicadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: Architecture & Technology Visioning; Recommender: Solution Engineering & Development; Executer: Cybersecurity

3	Configure Security Controls	Configurar controles de segurança necessários para proteger os ativos de informação.	Políticas aplicadas	Controles configurados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
4	Conduct Security Training	Realizar treinamentos de segurança para capacitar os colaboradores.	Controles configurados	Colaboradores treinados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: Cybersecurity
5	Document Governance Activities	Documentar todas as atividades de governança realizadas para manter registros claros.	Colaboradores treinados	Documentação completa	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Monitor Governance Compliance

O monitoramento da conformidade com as práticas de governança de segurança é um processo contínuo e essencial para garantir que todas as políticas e procedimentos sejam seguidos conforme planejado.

Este processo envolve a utilização de ferramentas de monitoramento, auditorias internas e externas, e a análise de relatórios de conformidade para identificar desvios e áreas de melhoria.

Através do monitoramento contínuo, é possível detectar rapidamente quaisquer não

conformidades ou violações, permitindo ações corretivas imediatas.

Além disso, este processo fornece insights valiosos sobre a eficácia das políticas de segurança e a maturidade da governança de segurança na organização.

Manter uma conformidade rigorosa não só garante a proteção dos ativos de informação, mas também demonstra o compromisso da organização com a segurança cibernética para clientes, parceiros e reguladores.

- PDCA focus: Check
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Implement Monitoring Tools	Implementar ferramentas de monitoramento para acompanhar a conformidade de segurança.	Ferramentas de monitoramento	Ferramentas implementadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Infrastructure & Operation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Infrastructure & Operation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
2	Conduct Internal Audits	Realizar auditorias internas para verificar a conformidade com as políticas de segurança.	Ferramentas implementadas	Relatórios de auditoria	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity

3	Analyze Compliance Data	Analisar os dados de conformidade para identificar não conformidades e áreas de melhoria.	Relatórios de auditoria	Relatórios de análise	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
4	Report Compliance Status	Relatar o status de conformidade e os resultados das auditorias à alta gestão.	Relatórios de análise	Relatórios de conformidade	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
5	Take Corrective Actions	Implementar ações corretivas para resolver as não conformidades identificadas.	Relatórios de conformidade	Ações corretivas implementadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity

Improve Governance Processes

A melhoria contínua dos processos de governança de segurança cibernética é vital para manter a eficácia e a relevância das políticas e controles de segurança.

Este processo envolve a análise dos feedbacks recebidos, a realização de avaliações de desempenho e a implementação de melhorias baseadas nas lições aprendidas e nas melhores práticas do setor.

A melhoria contínua permite que a organização responda de forma proativa a novas ameaças e mudanças no ambiente de negócios, ajustando suas práticas de governança

para enfrentar desafios emergentes.

Além disso, este processo promove uma cultura de excelência em segurança cibernética, incentivando a inovação e a adoção de tecnologias avançadas para fortalecer as defesas de segurança.

Através da melhoria contínua, a organização pode assegurar que suas práticas de governança de segurança estejam sempre alinhadas com os objetivos estratégicos e regulatórios.

- PDCA focus: Act
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Gather Feedback	Coletar feedback sobre as práticas de governança de segurança de todas as partes interessadas.	Relatórios de conformidade, auditorias	Feedback coletado	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: All areas; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
2	Conduct Performance Reviews	Realizar avaliações de desempenho das práticas de governança de segurança.	Feedback coletado	Relatórios de desempenho	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity

3	Identify Improvement Opportunities	Identificar oportunidades de melhoria com base nas avaliações e feedbacks.	Relatórios de desempenho	Lista de oportunidades de melhoria	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity
4	Implement Improvements	Implementar as melhorias identificadas nos processos de governança.	Lista de oportunidades de melhoria	Melhorias implementadas	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: Cybersecurity
5	Review Improvement Outcomes	Revisar os resultados das melhorias implementadas e ajustar conforme necessário.	Melhorias implementadas	Relatório de resultados	Responsible: Cybersecurity; Accountable: Cybersecurity; Consulted: IT Governance & Transformation; Informed: All areas	Decider: Cybersecurity; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: Cybersecurity