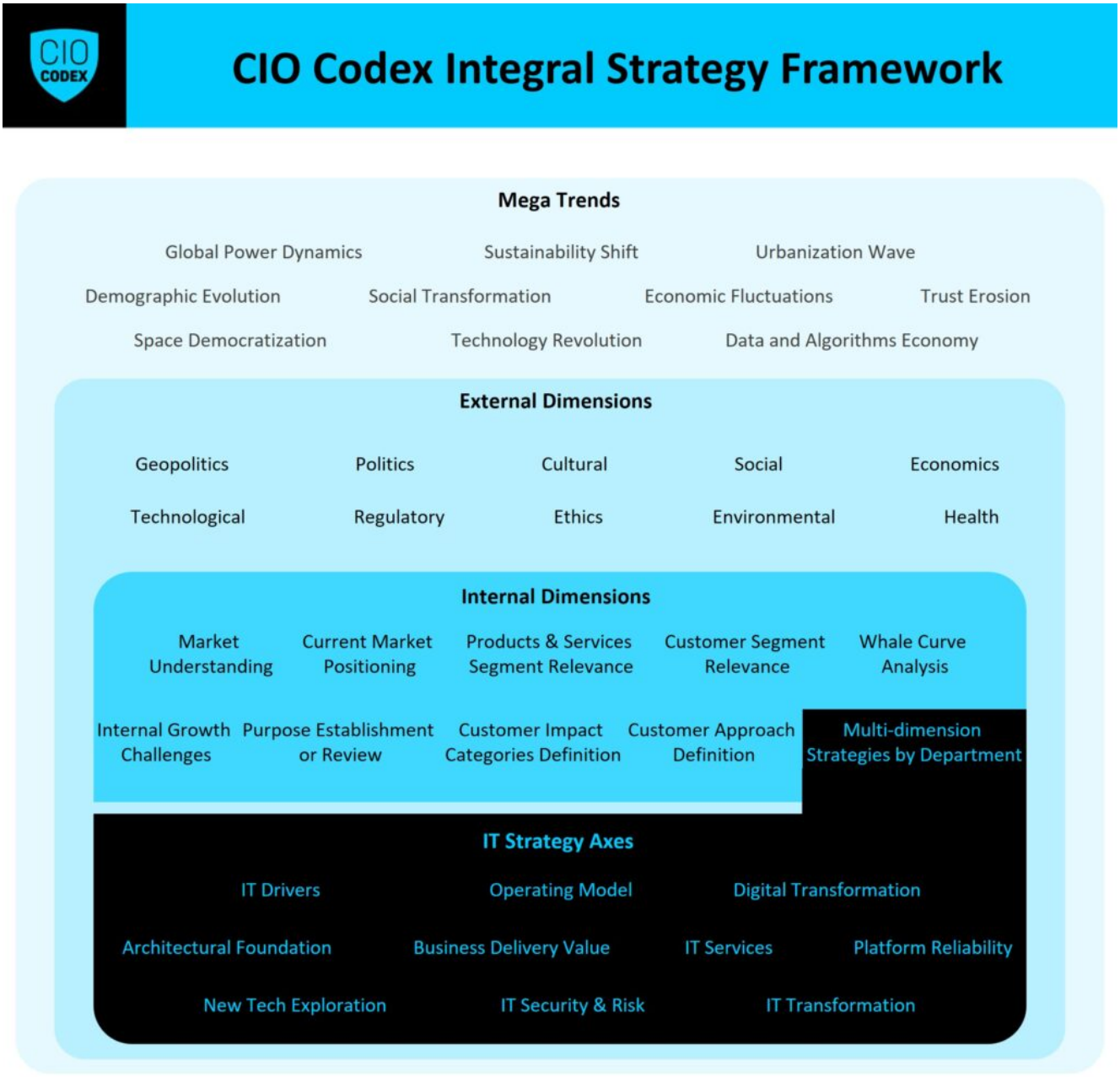
IT Security & Risk



O eixo IT Security & Risk (Segurança e Riscos de TI) na Estratégia Tecnológica é de extrema importância, pois aborda a proteção dos ativos digitais da organização contra ameaças cibernéticas e violações de dados.

Este eixo enfoca o desenvolvimento e a implementação de políticas, práticas e tecnologias de segurança robustas para salvaguardar as informações e a infraestrutura de TI.

Aspectos a Considerar na Elaboração da Estratégia de TI para a Segurança de TI:

- Avaliação de Riscos de Segurança: Realizar avaliações de risco contínuas para identificar vulnerabilidades e ameaças potenciais à infraestrutura de TI e aos dados da organização.
- Desenvolvimento de Políticas de Segurança: Criar e manter políticas de segurança claras e abrangentes que abordem aspectos como controle de acesso, gerenciamento de senhas, proteção de dados e resposta a incidentes.
- Tecnologias de Proteção: Implementar tecnologias avançadas de segurança, como firewalls, sistemas de detecção e prevenção de intrusões, antivírus, criptografia e segurança em nuvem, para proteger contra ameaças cibernéticas.
- Conformidade Regulatória: Garantir que as práticas de segurança de TI estejam em conformidade com regulamentações relevantes, como GDPR, LGPD, HIPAA, entre outras, dependendo da localização e do setor da organização.
- Treinamento e Conscientização: Promover programas de treinamento e conscientização em segurança para os colaboradores, visando reduzir o risco de violações de segurança causadas por erro humano.
- Gestão de Incidentes de Segurança: Desenvolver e manter um plano de resposta a incidentes de segurança, incluindo procedimentos para detecção, contenção, erradicação e recuperação de incidentes, bem como comunicação de incidentes.
- Monitoramento e Análise Contínuos: Estabelecer sistemas de monitoramento e análise contínuos para detectar atividades suspeitas ou maliciosas em tempo real e responder apropriadamente.
- Testes de Segurança: Realizar testes regulares de segurança, como avaliações de vulnerabilidade e testes de penetração, para identificar e corrigir falhas de segurança.

- Gestão de Parceiros e Fornecedores: Avaliar e gerenciar os riscos associados a terceiros, como fornecedores de serviços e parceiros de negócios, garantindo que eles também adotem práticas de segurança adequadas.
- Inovação e Adaptação: Manter-se atualizado com as tendências e inovações em segurança cibernética, adaptando a estratégia de segurança para enfrentar novos desafios e ameaças em um ambiente digital em constante mudança.

Ao desenvolver a estratégia para a Segurança de TI, é crucial adotar uma abordagem holística e proativa, considerando todos os aspectos da segurança da informação e protegendo a organização contra uma variedade de ameaças cibernéticas.

A estratégia de segurança de TI deve ser integrada a todas as facetas da estratégia tecnológica da empresa, garantindo uma proteção abrangente e eficaz.