



# 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.



### **CIO Codex**

Com o advento da era digital, a Tecnologia da Informação assumiu um papel de destaque dentro das estratégias corporativas das empresas dos mais diversos portes e setores de atuação. O CIO Codex Framework foi concebido com o propósito de oferecer uma visão integrada dos conceitos de uma área de tecnologia pronta para a era digital.



## The IT framework

O conteúdo apresentado neste website, incluindo o framework, é protegido por direitos autorais e é de propriedade exclusiva do CIO Codex. Isso inclui, mas não se limita a, textos, gráficos, marcas, logotipos, imagens, vídeos e demais materiais disponíveis no site. Qualquer reprodução, distribuição, ou utilização não autorizada desse conteúdo é estritamente proibida e sujeita às penalidades previstas na legislação aplicável