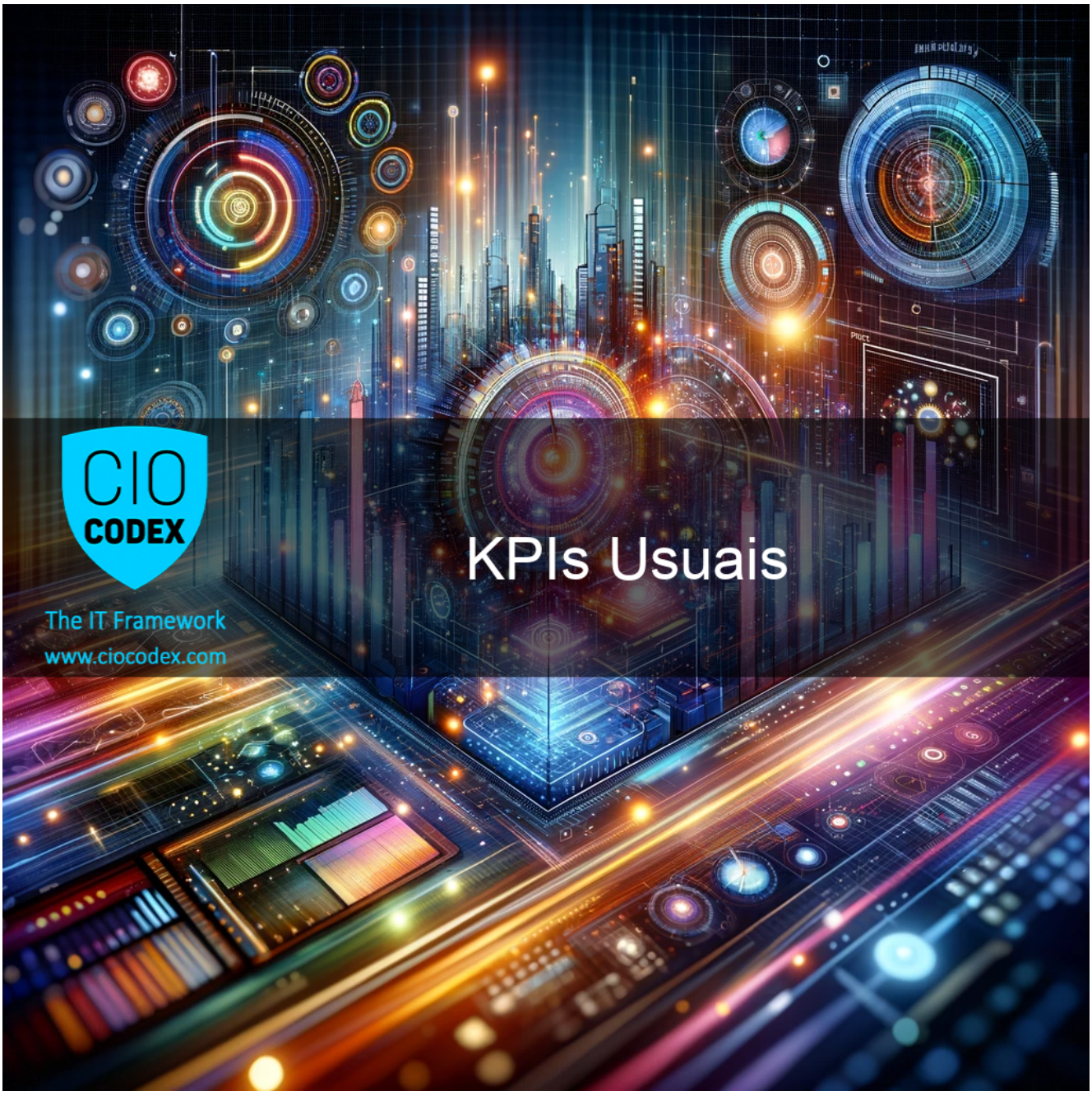
# KPIs Usuais




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.

;

;