



Exemplos de OKRs



Os Objetivos e Resultados-Chave (OKRs) são essenciais para direcionar e medir o sucesso das iniciativas de Cybersecurity em uma organização.

Eles ajudam a estabelecer metas claras e mensuráveis, alinhadas com os objetivos

estratégicos mais amplos e mantenha o foco em objetivos estratégicos cruciais, promovendo a segurança robusta, a eficiência operacional e o alinhamento com as metas gerais da organização.

Aqui estão alguns exemplos de OKRs para a área de Cybersecurity:

Objetivo: Reforçar as Defesas Contra Ameaças Cibernéticas

- KR1: Reduzir o tempo médio de detecção de incidentes de segurança (MTTD) em 30% no próximo trimestre.
- KR2: Aumentar a taxa de detecção de ameaças avançadas em 40% até o final do semestre.
- KR3: Implementar com sucesso duas novas tecnologias de segurança avançada nos próximos seis meses.

Objetivo: Melhorar a Conformidade e o Gerenciamento de Riscos

- KR1: Alcançar 100% de conformidade nas próximas auditorias de segurança cibernética.
- KR2: Realizar avaliações trimestrais de risco e reduzir os riscos identificados em 25%.
- KR3: Implementar um novo sistema de gestão de riscos até o final do ano.

Objetivo: Aumentar a Conscientização e Capacitação em Segurança Cibernética

- KR1: Treinar 90% dos funcionários em práticas de segurança cibernética até o final do próximo trimestre.
- KR2: Reduzir os incidentes de segurança relacionados ao erro humano em 50% nos próximos seis meses.

- KR3: Realizar simulados mensais de phishing e melhorar a taxa de detecção em 40%.

Objetivo: Aprimorar a Resposta a Incidentes e Recuperação de Desastres

- KR1: Desenvolver e testar um novo plano de resposta a incidentes em 3 meses.
- KR2: Reduzir o tempo médio de resposta a incidentes (MTTR) em 35% até o final do ano.
- KR3: Realizar dois exercícios completos de recuperação de desastres nos próximos seis meses.

Objetivo: Fortalecer a Segurança em Ambientes de Nuvem e IoT

- KR1: Implementar medidas de segurança aprimoradas para a infraestrutura de nuvem, reduzindo as vulnerabilidades em 50%.
- KR2: Realizar uma auditoria de segurança em todos os dispositivos IoT conectados e mitigar todos os riscos identificados.
- KR3: Desenvolver e implementar uma política específica de segurança para IoT até o final do próximo semestre.



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.



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