Exemplos de OKRs

Para o tema Cybersecurity da camada New Technology, os OKRs devem focar em fortalecer a infraestrutura de segurança da informação, conscientizar sobre práticas de segurança, e responder de forma proativa a ameaças emergentes.

Seguem os exemplos de OKRs para este tema:

Objetivo 1: Reforçar as defesas contra ameaças cibernéticas.

· KR1: Implementar um novo sistema de detecção e resposta a incidentes (EDR) que reduza o tempo de detecção de ameaças de dias para horas até o final do próximo trimestre.

· KR2: Aumentar a cobertura de testes de penetração e avaliações de vulnerabilidade em 50% dos sistemas críticos de TI.

· KR3: Alcançar zero violações de dados em sistemas críticos através de aprimoramentos na infraestrutura de segurança cibernética até o final do ano.

Objetivo 2: Cultivar uma cultura de segurança cibernética em toda a organização.

· KR1: Realizar treinamentos trimestrais de conscientização em segurança cibernética para 100% dos funcionários.

· KR2: Reduzir o número de incidentes de segurança causados por erro humano em 30% através de campanhas de conscientização.

· KR3: Estabelecer um programa de embaixadores de segurança cibernética em todos os departamentos até o segundo semestre.

Objetivo 3: Assegurar a conformidade regulatória e mitigar riscos legais.

· KR1: Alcançar 100% de conformidade com a GDPR e outras regulamentações relevantes de privacidade de dados.

· KR2: Realizar revisões de conformidade em todas as operações de dados, resultando em zero não conformidades nas próximas auditorias externas.

· KR3: Desenvolver e implementar uma política de gerenciamento de riscos cibernéticos que seja revisada e atualizada semestralmente.

Objetivo 4: Melhorar a resposta a incidentes e a recuperação de desastres.

· KR1: Reduzir o tempo médio de resposta a incidentes de segurança cibernética para menos de 15 minutos após a detecção.

· KR2: Realizar exercícios de simulação de ataque cibernético trimestrais, melhorando a eficácia da resposta em 20%.

· KR3: Atualizar e testar o plano de recuperação de desastres anualmente,

garantindo a restauração dos serviços críticos em menos de 4 horas após um incidente.

Objetivo 5: Avançar na proteção proativa com o uso de tecnologias emergentes.

· KR1: Integrar soluções de inteligência artificial em 30% dos nossos processos de monitoramento de segurança para prever e neutralizar ameaças proativamente.

· KR2: Implementar blockchain para aumentar a segurança nas transações e armazenamento de dados sensíveis em 2 projetos-piloto.

· KR3: Estabelecer um laboratório de inovação em segurança cibernética que teste novas tecnologias e produza pelo menos 3 protótipos até o final do ano.

Estes OKRs são essenciais para assegurar que a equipe de Cybersecurity esteja focada em proteger a infraestrutura da empresa contra a crescente paisagem de ameaças cibernéticas, mantendo a confidencialidade, integridade e disponibilidade dos ativos de dados e contribuindo para a resiliência organizacional.