Critérios para Avaliação de Maturidade

Para avaliar a maturidade do tema Cybersecurity na camada New Technology, os seguintes critérios inspirados no modelo CMMI podem ser aplicados para cada nível de maturidade:

Nível de Maturidade: Inexistente

· Ausência de Políticas de Segurança: Falta de políticas formais de segurança cibernética.

· Desconhecimento das Ameaças: Desconhecimento geral sobre ameaças cibernéticas e melhores práticas de segurança.

· Falta de Treinamento em Segurança: Ausência de treinamento em segurança para os funcionários.

· Sem Gestão de Incidentes: Não há processo definido para gestão de incidentes de segurança.

· Falta de Ferramentas de Segurança: Ausência de ferramentas e tecnologias de segurança implementadas.

Nível de Maturidade: Inicial

· Reconhecimento da Importância: Reconhecimento inicial da importância da segurança cibernética.

· Medidas de Segurança Básicas: Implementação de algumas medidas básicas de segurança, como antivírus e firewalls.

· Conscientização Inicial: Realização de campanhas iniciais de conscientização sobre segurança para funcionários.

· Resposta Ad Hoc a Incidentes: Respostas ad hoc a incidentes de segurança sem um plano formal.

· Análise de Vulnerabilidade Pontual: Realização de análises de vulnerabilidade esporádicas.

Nível de Maturidade: Definido

· Políticas de Segurança Definidas: Desenvolvimento e implementação de políticas formais de segurança cibernética.

· Treinamento e Conscientização Regulares: Programa regular de treinamento e conscientização em segurança cibernética para todos os funcionários.

· Gestão de Incidentes Estruturada: Processo estruturado para a gestão de incidentes de segurança.

· Avaliação e Gerenciamento de Riscos: Implementação de um processo de avaliação e gerenciamento de riscos de segurança.

· Auditorias de Segurança: Realização periódica de auditorias de segurança e testes de penetração.

Nível de Maturidade: Gerenciado

· Monitoramento Contínuo: Implementação de monitoramento contínuo de segurança e sistemas de detecção de intrusões.

· Resposta a Incidentes e Recuperação: Existência de um plano de resposta a incidentes e recuperação de desastres bem definido.

· Melhoria Contínua em Segurança: Uso de feedback de incidentes e auditorias para melhoria contínua das práticas de segurança.

· Conformidade com Normas: Adesão e conformidade com normas e regulamentações de segurança relevantes.

· Integração de Segurança no Desenvolvimento: Práticas de segurança integradas no ciclo de vida de desenvolvimento de software (DevSecOps).

Nível de Maturidade: Otimizado

· Cultura de Segurança Avançada: Cultura organizacional que prioriza a segurança cibernética em todas as operações.

· Liderança em Cybersecurity: Reconhecimento como líder em práticas de segurança cibernética.

· Inovação em Segurança: Inovação contínua em tecnologias e práticas de segurança.

· Adaptação Proativa: Capacidade de adaptação rápida a novas ameaças e mudanças no cenário de segurança.

· Benchmarking e Melhores Práticas: Engajamento em benchmarking e contribuição ativa para o avanço das melhores práticas de segurança no setor.

Esses critérios permitem à organização avaliar seu nível atual de maturidade em Cybersecurity, identificar áreas para melhoria e desenvolver uma estratégia para fortalecer sua postura de segurança em um ambiente tecnológico 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.