



Critérios para Avaliação de Maturidade



A capability Cybersecurity Strategy, inserida na macro capability Definition & Management e na camada Cybersecurity, desempenha um papel crucial no desenvolvimento e implementação de uma estratégia de segurança cibernética

abrangente.

Para avaliar a maturidade dessa capability, segue um modelo inspirado no CMMI, composto por cinco níveis: Inexistente, Inicial, Definido, Gerenciado e Otimizado.

;

Nível de Maturidade Inexistente

- Não há uma estratégia formal de segurança cibernética na organização.
- Não existem diretrizes para alinhar a segurança cibernética aos objetivos de negócio.
- Não há definição de prioridades em termos de segurança cibernética.
- Não há alocação de recursos específicos para proteção contra ameaças cibernéticas.
- A organização não possui políticas de segurança cibernética.

;

Nível de Maturidade Inicial

- Uma estratégia de segurança cibernética inicial está em desenvolvimento.
- As diretrizes para alinhar a segurança cibernética aos objetivos de negócio começam a ser definidas.
- Prioridades em termos de segurança cibernética estão sendo estabelecidas.
- Recursos estão sendo alocados de forma limitada para proteção contra ameaças cibernéticas.
- Políticas de segurança cibernética estão sendo criadas, mas ainda não estão totalmente implementadas.

;

Nível de Maturidade Definido

- Uma estratégia de segurança cibernética formal e documentada está em vigor.
- As diretrizes de segurança cibernética estão claramente definidas e alinhadas com os objetivos de negócio.
- Prioridades de segurança cibernética são bem compreendidas e comunicadas.
- Recursos são alocados de forma consistente para proteção contra ameaças cibernéticas.
- Políticas de segurança cibernética são implementadas e periodicamente revisadas para conformidade.

;

Nível de Maturidade Gerenciado

- A estratégia de segurança cibernética é eficaz e periodicamente revisada para ajustes.
- As diretrizes de segurança cibernética são monitoradas e atualizadas regularmente.
- Prioridades de segurança cibernética são dinâmicas e adaptáveis a novas ameaças.
- Recursos são gerenciados eficazmente para proteção contínua contra ameaças cibernéticas.
- Auditorias regulares garantem a conformidade com as políticas de segurança cibernética.

;

Nível de Maturidade Otimizado

- A estratégia de segurança cibernética é altamente otimizada, aproveitando tecnologias avançadas.
- As diretrizes de segurança cibernética são dinâmicas e baseadas em análises de risco contínuas.
- Prioridades de segurança cibernética são ágeis e adaptáveis a cenários em constante evolução.
- Recursos são alocados de forma inteligente e eficiente para proteção contra ameaças cibernéticas.
- A organização está constantemente atualizada com as melhores práticas de segurança cibernética e antecipa ameaças emergentes.

;

Esses critérios de maturidade são essenciais para avaliar o desenvolvimento e implementação eficazes da estratégia de segurança cibernética.

À medida que a organização progride nos níveis de maturidade, sua capacidade de proteger-se contra ameaças cibernéticas e alinhar a segurança com os objetivos de negócio é aprimorada, garantindo a resiliência e a segurança das operações.

;



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