Critérios para Avaliação de Maturidade

A capability Cybersecurity Governance, inserida na macro capability Definition & Management e na camada Cybersecurity, desempenha um papel crítico na governança da segurança cibernética de uma organização.

A avaliação da maturidade dessa capability é fundamental para assegurar que políticas, procedimentos e controles de segurança estejam em conformidade com regulamentações e padrões da indústria.

Abaixo estão os critérios de avaliação de maturidade em cinco níveis: Inexistente, Inicial, Definido, Gerenciado e Otimizado, inspirados no modelo CMMI.

Nível de Maturidade Inexistente

· Não há governança formal de segurança cibernética na organização.

· Não existem políticas ou procedimentos de segurança cibernética documentados.

· Não há monitoramento do cumprimento de políticas de segurança cibernética.

· A organização não está ciente dos riscos de segurança cibernética.

· Não há plano de ação para correção de vulnerabilidades identificadas.

Nível de Maturidade Inicial

· Iniciativas iniciais de governança de segurança cibernética estão sendo exploradas.

· Políticas de segurança cibernética estão sendo desenvolvidas, mas não estão formalizadas.

· Existe um monitoramento limitado do cumprimento das políticas de segurança.

· Alguma conscientização sobre riscos de segurança cibernética é promovida.

· Iniciativas reativas estão sendo tomadas para abordar vulnerabilidades conhecidas.

Nível de Maturidade Definido

· Uma estrutura formal de governança de segurança cibernética está em vigor.

· Políticas de segurança cibernética são documentadas e comunicadas.

· O monitoramento do cumprimento das políticas é regular e documentado.

· Uma abordagem proativa para avaliação de riscos de segurança cibernética é adotada.

· Planos de ação são desenvolvidos para mitigar riscos identificados.

Nível de Maturidade Gerenciado

· A governança de segurança cibernética é eficaz e adaptativa.

· As políticas de segurança cibernética são periodicamente revisadas e aprimoradas.

· O monitoramento do cumprimento das políticas é automatizado e em tempo real.

· Uma abordagem de gestão de riscos de segurança cibernética é implementada.

· Planos de ação são monitorados e executados de forma consistente.

Nível de Maturidade Otimizado

· A governança de segurança cibernética é altamente otimizada e inovadora.

· As políticas de segurança cibernética são ágeis e adaptáveis a ameaças em constante evolução.

· Monitoramento em tempo real e resposta automática a ameaças são implementados.

· A organização é líder em práticas de gestão de riscos de segurança cibernética.

· Planos de ação são revisados continuamente para otimização da segurança.

Esses critérios de maturidade são fundamentais para avaliar a eficácia da governança de segurança cibernética em uma organização.

À medida que a maturidade aumenta, a capacidade de garantir conformidade, promover a segurança e gerenciar riscos cibernéticos de forma eficiente e eficaz é aprimorada, fortalecendo a postura de segurança da organização.

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.