Integrações e Interdependências com Outras Áreas

Cada uma dessas áreas tem um papel crítico na proteção dos ativos digitais da empresa e na sustentação de operações de TI seguras.

A área de Cybersecurity é vital para liderar a estratégia de segurança, mas sua eficácia depende de uma colaboração estreita com todas as outras áreas de TI, garantindo que práticas de segurança sejam integradas em todos os aspectos da tecnologia empresarial.

Com Architecture & Technology Visioning

· Incorporação de Segurança: A área de Cybersecurity trabalha em estreita colaboração com os arquitetos de tecnologia para incorporar requisitos de segurança nas fases iniciais do design arquitetônico, assegurando que a segurança seja um componente intrínseco e não um adendo.

· Frameworks de Segurança: Define e implementa frameworks de segurança que suportam a visão arquitetônica, garantindo que as iniciativas de tecnologia estejam alinhadas com os padrões de segurança.

Com Solution Engineering & Development

· Segurança no Ciclo de Vida de Desenvolvimento: Assegura que as práticas de segurança estejam embutidas em todas as etapas do ciclo de vida de desenvolvimento de soluções, desde a concepção até a implementação e além.

· Práticas de DevSecOps: Integra a segurança dentro das práticas de DevOps para criar um ambiente de DevSecOps, onde a segurança é uma parte contínua e automática do processo de desenvolvimento.

Com IT Infrastructure & Operation

· Defesa da Infraestrutura: Colabora na definição e implementação de controles de segurança robustos para a proteção da infraestrutura de TI contra ameaças externas e internas.

· Monitoramento e Resposta a Incidentes: Trabalha junto à operação de TI para estabelecer sistemas de monitoramento de segurança proativos e um plano de resposta a incidentes eficiente.

Com Data, AI & New Technology

· Proteção de Dados e Inteligência Artificial: Atua para garantir a segurança de dados, especialmente em contextos de grande volume e uso de AI, estabelecendo práticas de segurança que protegem a privacidade e a integridade dos dados.

· Gestão de Riscos de Novas Tecnologias: Avalia e gerencia os riscos associados à adoção de novas tecnologias, colaborando para implementar medidas de segurança que acompanhem o ritmo da inovação.

Com IT Governance & Transformation

· Política de Segurança e Compliance: Trabalha junto com a governança de TI para desenvolver e manter políticas de segurança, além de assegurar o cumprimento de requisitos regulatórios e de compliance.

· Cultura de Segurança e Capacitação: Fomenta uma cultura organizacional de segurança e colabora em programas de treinamento para promover a conscientização sobre segurança em todos os níveis da organização.