Áreas de gestão

A Gestão de Vulnerabilidades e Ameaças é uma prática básica em termos de Segurança da Informação, visto que uma das atuações mais intuitivas na área seria exatamente a identificação de ameaças, a eliminação de vulnerabilidades e o uso de controles para mitigar ameaças residuais.

- **I. A priorização de iniciativas de mitigação ou remediação é parte da gestão.**
- **II. A busca por ameaças mais específicas e avançadas é algo a ser considerado por Órgãos Setoriais com maior nível de Maturidade.**

A área de Monitoramento e Operações envolve a parte operacional da implementação de controles e detecção/eliminação/mitigação de ameaças.

A avaliação da qualidade das operações é uma atividade relevante, uma vez que não há uma ferramenta única capaz de mitigar todas as possibilidades e certamente nenhuma ferramenta é capaz de eliminar todas as ameaças.

O processo de monitoramento poderá começar como sendo pontual, para então passar para ocasional/periódico e chegar enfim ao estado desejado, que é o monitoramento contínuo.

A Infraestrutura e Rede contêm frequentemente os ativos mais valiosos em termos de tecnologia da informação e comunicação e, portanto, necessitam de proteção adequada, especialmente se o Órgão Setorial possuir um data center ou similar.

A segurança da rede envolve a proteção de ambientes virtualizados como IaaS e outras formas de acesso remoto.

O controle de Identidades e Acessos é, muitas vezes, um dos objetivos mais claros e imediatos de Segurança da Informação e permeia todas as demais áreas, direta ou indiretamente.

Nuvem precisa ser tratada de forma diferenciada em termos de Segurança da Informação, uma vez que existem diversas formas de contratação e uso, impactando na implementação e operação dos controles de segurança.

A contratação e/ou uso da nuvem traz consigo questões não técnicas, especialmente questões de caráter legal/regulatório, que precisam ser levadas em consideração.

Os Endpoints e Dispositivos Móveis são um elemento de extrema relevância em qualquer arquitetura ou infraestrutura de tecnologia da informação e comunicação.

A questão do BYOD (Bring Your Own Device) é um desafio a ser tratado, considerando-se por um lado a sua conveniência e baixo custo, e por outro lado os riscos de se ter dados do Órgão Setorial em equipamentos e ambientes fora do seu controle direto.

A segurança das Aplicações trata tanto da segurança em termos de desenvolvimento quanto de execução, incluindo a proteção dos Dados que utilizam. Os Dados propriamente ditos são geralmente os ativos mais valiosos a serem protegidos e medidas devem ser tomadas para sua proteção, para fins de inserção/atualização/exibição/eliminação, processamento, armazenamento e transmissão/transferência.

Revision #2
Created 2025-11-14 16:55:03 UTC by Arthur
Updated 2026-01-23 13:36:37 UTC by Loyd Hiroki Kozawa