Ações de resposta a incidentes envolvendo ataques DoS/DDoS

No cenário atual de ameaças cibernéticas, os ataques de **negação de serviço (DoS) e negação de serviço distribuída (DDoS)** representam um dos principais riscos à disponibilidade de serviços e sistemas conectados à internet. Esses ataques têm como objetivo sobrecarregar servidores, aplicações ou infraestruturas de rede, tornando serviços indisponíveis para usuários legítimos e causando impactos operacionais significativos.

É fundamental que a instituição esteja preparada para **identificar rapidamente sinais de ataque, aplicar medidas de contenção e restabelecer a disponibilidade dos serviços afetados**. Uma resposta estruturada e eficiente reduz o tempo de indisponibilidade, minimiza impactos.

Este material tem como objetivo apresentar, de forma estruturada e prática, as **principais ações de resposta a incidentes envolvendo ataques DoS e DDoS**. Serão abordados conceitos, procedimentos de detecção, estratégias de mitigação, coordenação com provedores e boas práticas para recuperação segura dos serviços.

A capacidade de responder adequadamente a ataques de negação de serviço é um elemento essencial para garantir a **resiliência, continuidade e confiabilidade dos serviços digitais da instituição**.

Como praxe, reforçamos que tais ações estão contidas no escopo de sustentação e administração de redes locais e de serviços disponibilizados localmente pelas CTIs ou responsáveis técnicos pelos ativos envolvidos.