INAGE,IP

Instituto Nacional de Governo Electrónico, Instituto Público

DIVISÃO DE SEGURANÇA CIBERNÉTICA

Taxonomia do CSIRT.GOV

Maputo, Julho de 2025

Classificação de Incidentes

Classe de Incidente	Tipo de Incidente	Descrição do Tipo de Incidente
Conteúdo Abusivo	***SPAM***	• Envio de email não solicitado de mensagens de *email* em massa com mesmo conteúdo; • Mensagens com links maliciosos visando roubo de dados pessoais; • Mensagens com anexos maliciosos ou links que instalam software malicioso; • Mensagens não autorizadas originadas de contas comprometidas internas.
	Direitos de autor	Distribuição ou compartilhamento não autorizado de conteúdo protegido por direitos autorais.
	Exploração Sexual Infantil, racismo, incitação à violência ou tumulto.	Distribuição ou partilha de conteúdos ilegais, como material de exploração sexual infantil, racismo, xenofobia, tumultos, entre outros.
Fraude	**Uso indevido ou não autorizado de recursos**	Utilização de recursos de uma instituição para fins diferentes daqueles para quais foram afectos.
	Falsa representação	Uso não autorizado do nome de uma instituição.
Segurança da Informação	**Acesso não autorizado**	Interceptação de informação ou acesso não autorizado a um determinado conjunto de informações.
	Modificação ou Remoção não autorizada	Alteração ou eliminação não autorizada de um determinado conjunto de informações
Intrusão	**Exploração de vulnerabilidade**	Uso não autorizado de ferramentas para explorar vulnerabilidades específicas do sistema.
		Manipulação não autorizada ou leitura de informações contidas em um banco de dados usando a técnica de injeção de SQL.
		Ataque realizado com o uso de técnicas de *cross-site scripting.*
		Inclusão não autorizada de arquivos em um sistema sob ataque com o uso de técnicas de inclusão de arquivos.

		Acesso não autorizado a um sistema ou componente, através de *bypass do* sistema de controle de acesso.
	Compromisso de Conta	Acesso não autorizado a um sistema ou componente usando credenciais de acesso roubadas.
Tentativa de Intrusão	**Tentativa de Exploração de vulnerabilidade**	Uso malsucedido de uma ferramenta para explorar uma vulnerabilidade específica de um determinado sistema.
		Tentativa malsucedida de manipular ou ler informações de um banco de dados usando a técnica de injeção de SQL.
		Tentativas malsucedidas de executar ataques usando técnicas de *cross-site scripting*.
		Tentativa malsucedida de incluir arquivos em determinado sistema usando técnicas de inclusão de arquivos.
		Tentativa de acesso não autorizado a um sistema ou componente, através de *bypass* de mecanismos de controle de acesso.
	Tentativa de login	Tentativa malsucedida de Login usando ataques de força bruta para obter acesso a determinado sistema.
		Tentativa malsucedida de aquisição de credenciais de acesso, violando mecanismos de criptografia de chaves.
		Tentativa malsucedida de login usando ataque de dicionário.
Recolha de Informação de Segurança	***Scanning***	Varredura de sistema procurando por portas ou serviços abertos;
		Varredura de uma rede com a finalidade de identificar os sistemas ativos na rede.
		Transferência de zonas DNS;
	Sniffing	Interceptação lógica ou física de comunicações.
	Phishing	Envio de mensagens de e-mail em massa com objectivo de coletar dados para fins de *phishing*.
		Hospedagem de sites para fins de phishing.
	Engenharia Social	Colecta de informações pessoais usando meios não técnicos, por exemplo, mentiras, truques, subornos ou ameaças).

Disponibilidade	**DoS/DDoS**	Uso de ferramentas especialmente projetado para explorar vulnerabilidades e afectar o funcionamento normal de um serviço específico (esgotar recursos de rede, capacidade de processamento, sessões, etc.).
		Envio em massa de solicitações (pacotes de rede, e-mails, etc.) para um serviço específico, visando afectar seu funcionamento normal.
	Sabotagem	Atividades lógicas e físicas que visem causar danos à informação ou impedir sua transmissão entre sistemas.
	Configuração incorrecta	Configuração incorrecta de software que resulta em problemas de disponibilidade de serviço, p. ex. um servidor DNS com a DNSSEC KSK da zona raiz, desactualizada.
Código malicioso	**Infecção**	Sistema ou aplicação infectada com código malicioso, permitindo acesso remoto, monitoramento de actividades do sistema e coleta de informações
	Distribuição	Código malicioso anexado a uma mensagem de e-mail ou contendo uma hiperligação para URL ou IP mal-intencionado.
	Command & Control (C&C)	Sistema usado como um ponto de comando e controlo.
	Conexão maliciosa	Sistema tentando obter acesso a uma porta normalmente vinculada a um tipo específico de código malicioso.
Outro	**Sem tipo**	Todos os incidentes que não se encaixam num dos tipos especificados devem ser colocados nesta classe, ou o incidente não é classificado.
	Indeterminada	A classificação do incidente é desconhecida /indeterminada.

Aprovado por

_____

Inalda Ernesto

(Directora de Divisão de Segurança Cibernética)