TAXONOMIA ATÉ 31 DEZ 2025	TAXONOMIA A PARTIR DE 01 JAN 2026	DESCRIÇÃO	EXEMPLOS DE TERMOS ASSOCIADOS
Vazamento de Dados	**Conteúdo Abusivo (Abusive Content)**	Envio ou divulgação de Informações não solicitadas ou informações nocivas ou pessoais.	Doxxing, Deepfake, Spam, Sexual, Violence, Spamdexing, Harmful Speech, Disinformation, Misinformation, Malinformation
Código Malicioso	**Código Malicioso (Malware)**	Programa, ou parte de um programa de computador, projetado especificamente para atentar contra a segurança de um sistema computacional, normalmente por meio de exploração de alguma vulnerabilidade de sistema.	Exploit, Keylogger, Spyware, Vírus, Rootkit, Screenlogger, Wiper, Trojan, Worm, Dialler, Remote Access Tool (RAT), Adware, Scareware, Rogueware
Scan	**Obtenção de Informações (Information Gathering)**	Tentativas de obtenção e reunião de informações sobre tecnologias, redes e sistemas, como escaneamento e enumeração.	Scanning, Sniffing, fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, …), port scanning, wiretapping
Abuso de Sítio Web Abuso no Serviço de E-mail (SMTP)	**Intrusões (Intrusion or Intrusion Attempts)**	Tentativas ou acesso a redes e sistemas no contexto uma ação maliciosa, bem como seus impactos mais visíveis (desfiguração de sítios, vazamento de dados, etc...).	Exploit, Login attempts, Brute force, Attack signature, Credential stuffing, Privileged, Unprivileged, Account compromise, Bot, Botnet, Exploitation, Backdoor, Command & Control, Defacement, Espionage
Vulnerabilidade DRDoS	**Indisponibilidade (Not Availability)**	Inclui ações diversas para negação de serviços, indisponibilidade e outras formas de sabotagem de redes e sistemas.	Dos, DDos, DRDos, Flood, Negação de Serviço, Sabotage, indisponibilidade Parcial, Indisponibilidade Total Sabotagem Cibernética
Página Falsa Phishing	**Engenharia Social (Social Engineering)**	Técnica por meio da qual um ator de ameaça, utilizando manipulação psicológica, procura persuadir uma pessoa a executar determinadas ações. É considerada uma prática de má-fé para tentar explorar a boa-fé ou abusar da ingenuidade e da confiança das pessoas.	Social Engineering, Phishing, Vishing, Spear Phishing, Smishing, Spoofing, Masquerade, Whaling, Phishing Site, Disfarce, Clickbait, Ataque Sybil, Deepfake, Fake News
Software Vulnerável Vulnerabilidade de Criptografia Vulnerabilidade DRDoS	**Vulnerabilidades (Vulnerability)**	Condição que, quando explorada por um ator de ameaça, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha.	Open for abuse, zero day, vulnerability, exposição remota desnecessária de ativos, erros de configuração, Server-Side Request Forgery (SSRF), Cross Site Request Forgery – CSRF, Cross Site Scripting XSS, SQL Injection, Bypass
Código Malicioso	**Ransomware**	Tipo de malware, que, por meio de criptografia, impede o acesso a dados computacionais. Para recuperar o acesso, exige-se pagamento de um valor de resgate.	Ransomware, Ransomware as a Service (RaaS), Extorsão Múltipla, cryptpolocker
	Outros (Other)	Evidências relacionadas a incidentes ainda não agrupadas ou categorizadas. Compartilhamento de IOCs , Técnicas, Táticas e Procedimentos (TTPs) e outras informações relacionadas a Ameaças.	