TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO
Diretoria-Geral

Anexo da IN DG nº 03/2023 - Norma de Gestão de Incidentes de Segurança da Informação

Tabela **1— CATEGORIAS DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO		
Categoria	**Tipo**	**Descrição / Exemplos**
Código malicioso	Vírus	Programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Podem ser propagados por e-mail, scripts, macro ou telefone celular
	Worm	Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador
	Bot ou botnet	Programa semelhante ao *worm*, mas que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente
	Rootkit	Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido
	Trojan (Cavalo de Troia)	Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário
	Spyware	Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros
Coleta de Informações	*Scanning* (Varredura)	Ataques que enviam pedidos a um sistema para descobrir pontos fracos ou vulnerabilidades e executam testes para recolher informações sobre hosts, serviços e contas. Exemplos: *fingerd*, consultas DNS, ICMP, SMTP, etc.
	Sniffing	Observação e registro do tráfego de rede (escutas)
	Engenharia social	Coleta de informações a partir do ser humano com ou sem o uso da tecnologia (por exemplo , mentiras, truques, subornos ou ameaças)
Intrusão	Exploração de vulnerabilidades	Uma tentativa de comprometer um sistema ou interromper qualquer serviço , explorando vulnerabilidades do sistema (por exemplo, *buffer overflow* , *backdoors* , *cross side scripts*, etc).
	Tentativas de *login*	Várias tentativas de *login* (*cracking* de senhas, força bruta)
	Ataque com assinatura desconhecida	Tentativa usando um *exploit* desconhecido
	Conta privilegiada comprometida	Comprometimento do funcionamento normal de um sistema ou aplicação (serviço). Pode ser causado remotamente por uma vulnerabilidade conhecida ou nova, mas também por acesso local não autorizado
	Conta não privilegiada comprometida	
	Aplicação comprometida	
Disponibilidade	DoS (*Denial of Service*)	Tipo de ataque no qual um sistema é bombardeado com tantos pacotes que ficam lentos e em alguns casos podem até travar. Exemplos de um DoS remoto são *Syn flood*, *ping flood*, etc. No entanto, a disponibilidade pode ser afetada também por ações locais (destruição, rompimento de fornecimento de energia, etc.).
	DdoS (*Distributed DoS*)	
	Sabotagem	
Segurança da Informação	Acesso não autorizado	A segurança da informação pode ser ameaçada por uma conta de usuário válida ou aplicação comprometida que permitam acesso não autorizado à informação. Há, ainda, ataques que interceptam e acessam informações durante a transmissão dos dados pela rede.
	Modificação não autorizada	
Fraude	Uso não autorizado dos recursos	Uso de recursos para fins não autorizados, incluindo *ventures* com fins lucrativos (por exemplo, o uso de e-mail para participar na cadeia de lucro ilegais ou esquemas de pirâmide)
	Direitos autorais (*copyright*)	Vender ou instalar cópias de software ou outros materiais protegidos por direitos autorais sem a devida licença

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO		
Categoria	**Tipo**	**Descrição / Exemplos**
	Masquerade	Tipos de ataques em que uma entidade ilegítima assume a identidade do outro , a fim de obter benefícios
Outros		Todos os incidentes não categorizados em um dos tipos anteriores devem ser classificados nesta classe. Quando o número de incidentes nesta categoria aumentar, será o momento de rever esta tabela de classificações.

(fonte: TRE-SP)

TABELAS 2, 3 E 4 - PRIORIZAÇÃO DE INCIDENTES

Para que seja estabelecida a priorização dos incidentes de Segurança da Informação devem ser considerados:

a) O Impacto no Negócio

A ETIR deve levar em conta o impacto negativo que o incidente pode causar nos negócios do Tribunal, incluindo os impactos futuros que podem atingir o órgão. A tabela abaixo traz os níveis de impacto no negócio.

Tabela 2

Categoria	Definição
Nenhum	Não afeta a capacidade da organização de fornecer todos os serviços a todos os usuários.
Baixo	Efeito mínimo; a organização ainda pode fornecer todos os serviços essenciais para todos os usuários, mas perdeu eficiência.
Médio	A organização perdeu a capacidade de fornecer um serviço crítico a um subconjunto de usuários do sistema.
Alto	A organização não é mais capaz de fornecer alguns serviços essenciais a nenhum usuário.

(fonte: Secretaria de Governo Digital do Ministério da Economia)

b) O Impacto em Dados e Informações

Deve ser avaliado o impacto do incidente na confidencialidade, integridade e disponibilidade dos dados e informações e sua repercussão na esfera do Tribunal, de entes parceiros e titulares de dados.

As categorias de impacto aos dados e informações estão previstas na seguinte tabela.

Tabela 3

Categoria	Definição
Nenhum	Nenhuma informação relevante foi exposta, alterada, excluída ou de alguma maneira comprometida.
Violação de privacidade	Informações confidenciais de identificação pessoal (DP) de contribuintes, funcionários, beneficiários etc. foram acessadas ou expostas.
Violação Proprietária	Informações proprietárias não classificadas, como informações de infraestrutura crítica protegida (PCII), foram acessadas ou expostas.
Perda de Integridade	Informações confidenciais ou proprietárias foram alteradas ou excluídas.

(fonte: Secretaria de Governo Digital do Ministério da Economia)

c) Recuperabilidade

É preciso, ainda, estabelecer o nível de impacto do incidente nos recursos e o tempo necessário para a recuperação. Nesta etapa identificam-se e avaliam-se os recursos e a importância, para o Tribunal, da recuperação do incidente. As categorias de recuperabilidade estão elencadas dessa forma:

Tabela 4

Categoria	Definição
Regular	O tempo de recuperação é previsível com os recursos existentes.
Suplementado	O tempo de recuperação é previsível com recursos adicionais.
Estendido	O tempo de recuperação é imprevisível; recursos adicionais e ajuda externa são necessários.
Não Recuperável	A recuperação do incidente não é possível (por exemplo, dados confidenciais expostos e postados publicamente); lançar investigação.

(fonte: Secretaria de Governo Digital do Ministério da Economia)

****