NOTIFICAÇÃO CTIR.BR

PROCEDIMENTOS PARA A NOTIFICAÇÃO

1. A comunicação entre órgãos e instituições da APF e o CTIR Gov deve ocorrer por meio das ETIR, de forma centralizada, preferencialmente por meio de e-mail institucional relacionado a incidentes de segurança. No caso do TRT4 será utilizado o e-mail do Escritório de Segurança da Informação (posteriormente, poderá ser implementada nova conta específica abuse@orgao.gov.br, como sugerido nos padrões do CTIR).

2. O ponto único de contato para as notificações de incidentes de segurança ao CTIR Gov é o endereço eletrônico: ctir@ctir.gov.br.

   2.1. Para comunicação através de um canal seguro, deverá ser utilizada a seguinte chave PGP:

   PGP Key ID: 0xAFBEDFCF

   Fingerprint: 1E57 8A38 4834 6F1B 76BB 98C4 953E EB94 AFBE DFCF

   2.2. O CTIR Gov atende ainda pelo telefone INOC-DBA: 10954*810.

3. As questões gerenciais ou relacionadas à Coordenação-Geral de Tratamento de Incidentes de Rede (CGTIR) serão tratadas por meio do correio eletrônico: cgtir@planalto.gov.br.

4. A notificação deverá conter os seguintes dados:

   4.1. Assunto: fazer constar o “nome do órgão” e o “tipo do incidente”.

   4.2. Destinatário: ctir@ctir.gov.br.

   4.3. CC: eventualmente, podem ser copiados outros envolvidos no incidente.

   4.4. Corpo da Notificação: descrever sucintamente o incidente ocorrido, atentando para a correção das informações, tais como: organizações, pessoas ou serviços de rede envolvidos; time zone; registros de log; cronologia dos acontecimentos; ações adotadas; outros detalhes técnicos e incidentes correlacionados.

   4.5. Anexos: Deverão ser anexadas as informações que facilitem a análise e a resposta ao incidente, tais como: logs de servidores e/ou serviços, cabeçalho de mensagens, código malicioso, etc.

5. No caso de recebimento de uma notificação ou resposta do CTIR, nas

Comunicações que se seguirem deve sempre ser referenciado no campo “Assunto” o número de identificação fornecido no formato [CTIR Gov BR #XXXXX].

6. Principais tipos de incidentes de segurança possíveis de serem notificados:

6.1. abuso de sítios (desfiguração, injeção de links/código - spamdexing, erros de erros de código, cross site scripting, abuso de fórum ou livros de visita, etc.);

6.2. inclusão remota de arquivos (remote file inclusion - RFI) em servidores web;

6.3. uso abusivo de servidores de e-mail;

6.4. hospedagem ou redirecionamento de artefatos ou código malicioso;

6.5. ataques de negação de serviço;

6.6. uso ou acesso não autorizado a sistemas ou dados;

6.7. varredura de portas;

6.8. comprometimento de computadores ou redes;

6.9. desrespeito à política de segurança ou uso inadequado dos recursos de Tecnologia

6.10. ataques de engenharia social - phishing; (no caso de phishing recebido por e-mail, solicita-se que, além do texto da mensagem, sejam enviados os cabeçalhos completos para que se proceda, dentre outras coisas, à notificação do servidor de e-mail comprometido).

6.11. cópia e distribuição não autorizada de material protegido por direitos autorais;

6.12. uso abusivo ou indevido de redes sociais para difamação, calúnia, ameaças ou fraudes.