# PADRÕES PARA NOTIFICAÇÃO DE INCIDENTES DE SEGURANÇA AO CTIR GOV

## 1. Objetivo

Definir padrões e esclarecer os procedimentos relacionados ao processo de notificação de incidentes de segurança em redes de computadores da Administração Pública Federal (APF) ao Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR Gov).

## 2. Referências

2.1. Norma Complementar nº 05 /IN01/DSIC/GSIPR, de 14/Ago/09, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da APF.

2.2. Norma Complementar nº 08 /IN01/DSIC/GSIPR, de 19/Ago/10, que disciplina o gerenciamento de incidentes de segurança em redes de computadores realizado pelas ETIR dos órgãos e entidades da APF.

## 3. Introdução

3.1. O CTIR Gov integra o Departamento de Segurança de Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSIPR) e tem como finalidade o atendimento aos incidentes em redes de computadores pertencentes à APF. Além disso, atua como centro de coordenação entre as partes envolvidas, acompanhando as ações de tratamento e resposta aos incidentes de segurança.

3.2. A comunidade atendida pelo CTIR Gov é composta por todos os órgãos e entidades da Administração Pública Federal direta e indireta. Em caráter excepcional e de forma colaborativa, o atendimento será estendido aos órgãos dos Estados, Municípios e Distrito Federal, pertencentes aos domínios “gov.br”, “jus.br”, “leg.br”, “mil.br” e outros sob a responsabilidade da APF.

3.3. Conforme estabelecem o item 10.6 da NC nº 05 e o item 6 da NC nº 08, as equipes de tratamento e resposta a incidentes em redes computacionais dos órgãos e entidades da APF deverão comunicar de imediato ao CTIR Gov a ocorrência dos incidentes de segurança nas redes de computadores, contribuindo para as soluções integradas para a comunidade atendida e para a geração de estatísticas, de acordo com os padrões e procedimentos definidos neste documento.

## 4. Procedimentos para Notificação

4.1. A comunicação entre órgãos e instituições da APF e o CTIR Gov deve ocorrer por meio das ETIR ou por pessoas com essa atribuição, de forma centralizada, preferencialmente por meio de *e-mail* institucional relacionado a incidentes de segurança, como sugestão: **abuse@orgao.gov.br**. Deve-se fazer constar no assunto da notificação o “nome do órgão” e o “tipo do incidente”.

4.2. O ponto único de contato para as notificações de incidentes de segurança ao CTIR Gov é o endereço eletrônico: **ctir@ctir.gov.br**.
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
O CTIR Gov atende ainda pelo telefone INOC-DBA: **10954*810.**

4.3. 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**.

4.4. Para a composição das notificações, deve ser observado o que se segue:
**Assunto**: fazer constar o "nome do órgão" e o "tipo do incidente".

**Destinatário**: ctir@ctir.gov.br.

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

**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.

**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.

4.5. Dentre os diversos tipos de incidentes de segurança possíveis de serem notificados, destacam-se:
4.5.1 abuso de sítios (desfiguração, injeção de links/código - s*pamdexing*, erros de código, *cross site scripting*, abuso de fórum ou livros de visita, etc.);
4.5.2 inclusão remota de arquivos (*remote file inclusion - RFI*) em servidores web;
4.5.3 uso abusivo de servidores de *e-mail*;
4.5.4 hospedagem ou redirecionamento de artefatos ou código malicioso;
4.5.5 ataques de negação de serviço;
4.5.6 uso ou acesso não autorizado a sistemas ou dados;
4.5.7 varredura de portas;
4.5.8 comprometimento de computadores ou redes;
4.5.9 desrespeito à política de segurança ou uso inadequado dos recursos de Tecnologia da Informação (TI);
4.5.10 ataques de engenharia social - *phishing*;
4.5.11 cópia e distribuição não autorizada de material protegido por direitos autorais;
4.5.12 uso abusivo ou indevido de redes sociais para difamação, calúnia, ameaças ou fraudes.

4.6. 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.

4.7. O CTIR Gov provê os seguintes serviços à APF: tratamento de incidentes; análise de artefatos maliciosos; coordenação nas respostas a incidentes; distribuição de alertas e recomendações; estatísticas relativas a incidentes; notificação automática de incidentes; apoio à capacitação por meio de reuniões, *workshops*, colóquios, oficinas, palestras e exercícios de segurança da informação e segurança cibernética.

4.8. Considera-se incidente de segurança qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores. O processo de tratamento de incidentes realizado pelo CTIR Gov desdobra-se em:

4.8.1 **Notificação do Incidente**: o recebimento de notificações de incidentes permite ao CTIR Gov atuar como ponto central para coordenação de soluções dos problemas decorrentes, por meio da coleta de atividades e incidentes reportados, análise das informações e correlação decorrente no âmbito da organização informante ou da comunidade da APF.
As informações podem ser utilizadas também para determinar tendências e padrões de atividades de ataques e para recomendar estratégias de prevenção adequadas para toda a APF.

4.8.2 **Análise de Incidentes**: esta atividade consiste em examinar todas as informações disponíveis sobre o incidente, incluindo artefatos e outras evidências relacionadas ao evento. O propósito da análise é identificar o escopo do incidente, sua extensão, sua natureza e prejuízos causados, além de propor estratégias de contenção e recuperação.

4.8.3 **Suporte à Recuperação de Incidentes**: neste caso, o CTIR Gov auxilia no processo de recuperação. Esse auxílio pode ser prestado por telefone, *e-mail*, fax ou pela indicação de documentos que possam auxiliar no processo de recuperação. Essa atividade pode envolver o auxílio na interpretação dos dados coletados e na recomendação de estratégias de contenção e recuperação.

4.8.4 **Coordenação na Resposta a Incidentes**: nesta atividade, o CTIR Gov coordena as ações entre os envolvidos em um incidente, o que pode incluir redes e outros centros de tratamento (CSIRTs) externos ao seu âmbito de atuação. O processo de coordenação envolve a coleta de informações de contato, a notificação dos responsáveis pelas redes, computadores ou sistemas que possam estar envolvidos ou comprometidos e a geração de indicadores e estatísticas relativas aos incidentes. O CTIR Gov age como um facilitador no processo de recuperação dos incidentes e na troca de informações entre as partes envolvidas.

4.8.5 **Distribuição de Alertas, Recomendações e Estatísticas**: esta atividade consiste em disseminar informações relativas a novos ataques ou tendências de ataques observadas pelo CTIR Gov, por outros centros de tratamento ou por empresas especializadas. Esses alertas, em geral, são produzidos pelo próprio CTIR Gov, baseados nas notificações recebidas ou em incidentes tratados, ou são redistribuições de alertas emitidos por outros Centros com responsabilidade nacional. O CTIR Gov, ao redistribuir alertas, pode acrescentar recomendações específicas para seu público alvo.

4.8.6 **Cooperação com outras Equipes de Tratamento de Incidentes**: o CTIR Gov, por meio da Coordenação-Geral, atua na implementação de cooperação com outras Equipes de Tratamento de Incidente da APF, bem como com outros CSIRTs, públicos e privados, nacionais e internacionais, visando à cooperação técnica e à ajuda mútua no tratamento de incidentes de segurança.

## 5. Outras Considerações

5.1. O CTIR Gov não realiza procedimentos de investigação criminal. As atividades do Centro restringem-se a detecção, análise, resposta e tratamento de incidentes de segurança nas redes de computadores da APF. Eventuais desdobramentos relacionados aos incidentes são encaminhados às autoridades policiais competentes.

5.2. Todas as notificações ou mensagens recebidas pelo CTIR Gov recebem o tratamento adequado após o processo de triagem e análise. As ações desencadeadas pelas notificações têm como objetivo sanar os incidentes relatados ou restabelecer eventuais serviços comprometidos às condições normais de funcionamento.

5.3. Na maioria dos casos, o recebimento das notificações é informado aos requisitantes e, durante o tratamento do incidente, todos os envolvidos são notificados sobre as ações a serem adotadas. O não recebimento de um retorno sobre um incidente reportado não significa que tal incidente não foi tratado ou solucionado. Em alguns casos torna-se inviável relatar todos os procedimentos realizados aos requisitantes.

5.4. O CTIR Gov controla as notificações recebidas ou enviadas atribuindo um número de identificação ao campo "Assunto" no formato [CTIR Gov BR #XXXXX]. É de fundamental importância que esse número **seja referenciado em todas as interações ocorridas ao longo do tratamento do incidente**.

5.5. Conforme estabelece o item 8.5 da NC nº 08 /IN01/DSIC/GSIPR, havendo indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, as ETIR de órgãos da APF devem, além de comunicar ao CTIR Gov, acionar as autoridades policiais competentes para a adoção dos procedimentos legais necessários. Ademais, deve observar os procedimentos para preservação das evidências, exigindo consulta às orientações sobre cadeia de custódia, e priorizar a continuidade dos serviços da ETIR e da missão institucional da organização.

Brasília, DF, 30 de agosto de 2012.

Equipe do CTIR Gov