Poder Judiciário

Conselho Nacional de Justiça

ANEXO III – Protocolo – Investigação para ilícitos cibernéticos do Poder Judiciário

Protocolo

Investigação para Ilícitos Cibernéticos do Poder Judiciário

Material de referência com as principais diretrizes necessárias para implantação do protocolo de investigação para Ilícitos Cibernéticos do Poder Judiciário

Sumário

1. Objetivo 3
2. Requisitos para Adequação dos Ativos de Informação 3
3. Procedimento para Coleta e Preservação das Evidências 4
4. Comunicação do Incidente de Segurança 6

Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ)

1. Objetivo

1.1. O Protocolo de Investigação para Ilícitos Cibernéticos (PIILC-PJ) tem por finalidade estabelecer os procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal.

2. Requisitos para Adequação dos Ativos de Informação

2.1. O horário dos ativos de informação deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a Hora Legal Brasileira – HLB, de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).

2.2. Os ativos de informação devem ser configurados de forma a registrar todos os eventos relevantes de Segurança da Informação e Comunicações (SIC), tais como:

a) autenticação, tanto as bem-sucedidas quanto as malsucedidas;
b) acesso a recursos e dados privilegiados; e
c) acesso e alteração nos registros de auditoria.

2.3. Os registros dos eventos previstos no item 2.2 devem incluir as seguintes informações:

a) identificação inequívoca do usuário que acessou o recurso;
b) natureza do evento, como, por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha etc.;
c) data, hora e fuso horário, observando-se a HLB; e
d) endereço IP (*Internet Protocol*), porta de origem da conexão, identificador do ativo de informação, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento.

2.4. Os ativos de informação que não propiciem os registros dos eventos listados no item 2.2 devem ser mapeados e documentados quanto ao tipo e formato de registros de auditoria permitidos e armazenados.

2.5. Os sistemas e as redes de comunicação de dados devem ser monitorados, registrando-se, minimamente, os seguintes eventos de segurança, sem prejuízo de outros considerados relevantes:

a) utilização de usuários, perfis e grupos privilegiados;
b) inicialização, suspensão e reinicialização de serviços;
c) acoplamento e desacoplamento de dispositivos de *hardware*, com especial atenção para mídias removíveis;
d) modificações da lista de membros de grupos privilegiados;
e) modificações de política de senhas, como, por exemplo, tamanho, expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico etc.;
f) acesso ou modificação de arquivos ou sistemas considerados críticos; e
g) eventos obtidos por meio de quaisquer mecanismos de segurança existentes.

2.6. Os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (*logs*) em formato que possibilite a completa identificação dos fluxos de dados.

2.7. Os registros devem ser armazenados pelo período mínimo de seis meses, sem prejuízo de outros prazos previstos em normativos específicos.

2.8. Recomenda-se que os ativos de informação sejam configurados de forma a armazenar seus registros de auditoria não apenas localmente, mas também remotamente, por meio do uso de tecnologia aplicável.

3. Procedimento para Coleta e Preservação das Evidências

3.1. A ETIR, sob a supervisão de seu responsável, durante o processo de tratamento do incidente penalmente relevante, deverá, sem prejuízo de outras ações, coletar e preservar:

a) as mídias de armazenamento dos dispositivos afetados ou as suas respectivas imagens forenses;
b) os dados voláteis armazenados nos dispositivos computacionais, como a memória principal (memória RAM); e
c) todos os registros de eventos citados neste documento.

3.2. Nos casos de inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados ou das suas respectivas imagens forenses, em razão da necessidade de pronto restabelecimento do serviço afetado, a ETIR, sob a supervisão do seu responsável, deverá coletar e armazenar cópia dos arquivos afetados pelo incidente, tais como: *logs*, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original e os "metadados" desses arquivos, como data, hora de criação e permissões.

3.3. O agente responsável pela ETIR deverá fazer constar em relatório a eventual impossibilidade de preservação das mídias afetadas e listar todos os procedimentos adotados.

3.4. As ações de restabelecimento do serviço não devem comprometer a coleta e a preservação da integridade das evidências.

3.5. Para a preservação dos arquivos coletados, deve-se:

a) gerar arquivo que contenha a lista dos resumos criptográficos de todos os arquivos coletados;
b) gravar os arquivos coletados, acompanhados do arquivo com a lista dos resumos criptográficos descritos na alínea *a* deste subitem; e
c) gerar resumo criptográfico do arquivo a que se refere *a* deste subitem.

3.6. Todo material coletado deverá ser lacrado e custodiado pelo agente responsável pela ETIR, o qual deverá preencher Termo de Custódia dos Ativos de Informação relacionados ao incidente de segurança penalmente relevante.

3.7. O material coletado ficará à disposição da autoridade responsável pelo órgão do Poder Judiciário competente.

4. Comunicação do Incidente de Segurança

4.1. Assim que tomar conhecimento de Incidente de Segurança em Redes Computacionais penalmente relevante, deverá o responsável pelo órgão do Poder Judiciário afetado comunicá-lo de imediato ao órgão de polícia judiciária com atribuição para apurar os fatos.

4.2. Considerado o incidente uma Crise Cibernética, o Comitê de Crise deverá ser acionado, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas.

4.3. Após a conclusão do processo de coleta e preservação das evidências do incidente penalmente relevante, o responsável pela ETIR deverá elaborar Relatório de Comunicação de Incidente de Segurança em Redes Computacionais, descrevendo detalhadamente os eventos verificados.

4.4. O Relatório de Comunicação de Incidente de Segurança em Redes Computacionais deverá conter as seguintes informações, sem prejuízo de outras julgadas relevantes:

a) nome do responsável pela preservação dos dados do incidente, com informações de contato;
b) nome do agente responsável pela ETIR e informações de contato;
c) órgão comunicante com sua localização e informações de contato;
d) número de controle da ocorrência;
e) relato sobre o incidente que descreva o que ocorreu, como foi detectado e quais dados foram coletados e preservados;
f) descrição das atividades de tratamento e resposta ao incidente e todas as providências tomadas pela ETIR, incluindo as ações de preservação e coleta, a metodologia e as ferramentas utilizadas e o local de armazenamento das informações preservadas;
g) resumo criptográfico dos arquivos coletados;
h) Termo de Custódia dos Ativos de Informação Relacionados ao Incidente de Segurança;
i) número de lacre de material físico preservado, se houver; e
j) justificativa sobre a eventual inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados, diante da impossibilidade de mantê-las.

4.5. O Relatório de Comunicação de Incidente de Segurança em Redes Computacionais deverá ser acondicionado em envelope lacrado e rubricado pelo agente responsável pela ETIR, protocolado e encaminhado formalmente à autoridade responsável pelo órgão do Poder Judiciário afetado.

4.6. Deverá constar no documento formal de encaminhamento a que se refere o item 4.5, apenas a informação de que se trata de comunicação de evento relacionado à segurança da informação, sem a descrição dos fatos.

4.7. Recebida a Comunicação de Incidente de Segurança em Redes Computacionais, a autoridade responsável pelo órgão do Poder Judiciário deverá encaminhá-la formalmente ao Ministério Público e ao órgão de polícia judiciária com atribuição para apurar os fatos, juntamente com o todo o material previsto neste protocolo, para fins de instrução da notícia crime.