PROTOCOLO PARA INVESTIGAÇÃO DE ILÍCITOS CIBERNÉTICOS (PIILC-PJ)

1. OBJETIVOS

1.1. 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.

1.2. Promover adequação e alinhamento às regulamentações, normas e melhores práticas relacionadas à segurança cibernética.

1.3. Definir requisitos para adequação dos ativos de tecnologia da informação no que tange à configuração e ao registro de informações de auditoria.

2. CONSIDERAÇÕES IMPORTANTES

2.1. Este protocolo é parte do conjunto de Protocolos de Segurança Cibernética, definido pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), do qual também fazem parte o Protocolo de Prevenção de Incidentes Cibernéticos e o Protocolo de Gerenciamento de Crises Cibernéticas.

2.2. As ações e medidas elencadas neste protocolo são complementares às políticas, aos processos, às práticas e aos procedimentos relacionados à segurança da informação já formalizados e estabelecidos no âmbito do TRT.

3. GLOSSÁRIO

3.1. Os conceitos utilizados neste protocolo têm como embasamento a definição constante no Anexo VIII da Portaria CNJ nº 162/2021.

4. DA ADEQUAÇÃO DOS ATIVOS TECNOLÓGICOS EM RELAÇÃO AO REGISTRO DE INFORMAÇÕES

4.1. Os ativos tecnológicos do Tribunal (ex.: estações de trabalho, servidores, serviços, sistemas, dentre outros) devem:

4.1.1. Ser configurados de acordo com a Hora Legal Brasileira (HLB), de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).

4.1.2. Ser configurados de forma a registrar eventos relevantes de segurança da informação, bem como de informações que possibilitem a depuração de incidentes e de problemas.

4.1.3. Registrar, sempre que possível, as seguintes informações:

4.1.3.1. identificação inequívoca do usuário que acessou o recurso;

4.1.3.2. natureza do evento, como, por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha etc.;

4.1.3.3. data, hora e fuso horário, observando-se a HLB; e

4.1.3.4. endereço IP (*Internet Protocol*), porta de origem da conexão, identificador do ativo de informação e demais informações que possibilitem identificar a origem do evento.

4.2. Os registros devem ser armazenados pelo período mínimo de 6 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos.

4.3. O armazenamento dos registros de auditoria deve ser realizado remotamente (e não apenas localmente), por meio do uso de tecnologia aplicável, para, ao menos, os ativos tecnológicos considerados críticos.

5. PROCEDIMENTOS PARA COLETA E PRESERVAÇÃO DE EVIDÊNCIAS

5.1. Confirmada a ocorrência de um incidente, deve ser avaliada a necessidade de ativação do Protocolo de Gerenciamento de Crises Cibernéticas.

5.2. A investigação do ilícito cibernético deve ser realizada de acordo com as normas estabelecidas na Política de Segurança da Informação vigente, especificamente no tocante ao assunto de gestão de incidentes de segurança da informação e à Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação.

5.3. Os incidentes de segurança cibernética devem ser registrados em Relatório de Incidente de Segurança da Informação, que contém os dados de identificação de quem o preencheu, data e hora da ocorrência, informações sobre o incidente, como ele foi tratado, oportunidades de melhoria e lições aprendidas.

5.4. Caso seja necessária a coleta de evidências, ela deverá ser realizada de acordo com a prática forense digital, de forma a garantir a devida confidencialidade, integridade e autenticidade das informações coletadas.

5.5. Se o incidente de segurança envolver a suspeita de crime, os órgãos competentes devem ser acionados, nos termos da legislação vigente.

6. CONSIDERAÇÕES FINAIS

6.1. Na ocorrência de indícios de ilícitos criminais durante o tratamento de incidentes cibernéticos, além das ações elencadas ou referenciadas neste protocolo, deverão ser observadas eventuais solicitações e orientações dos órgãos competentes que forem acionados.

6.2. Este documento deve ser revisado anualmente ou quando houver alteração significativa que enseje sua pronta alteração.