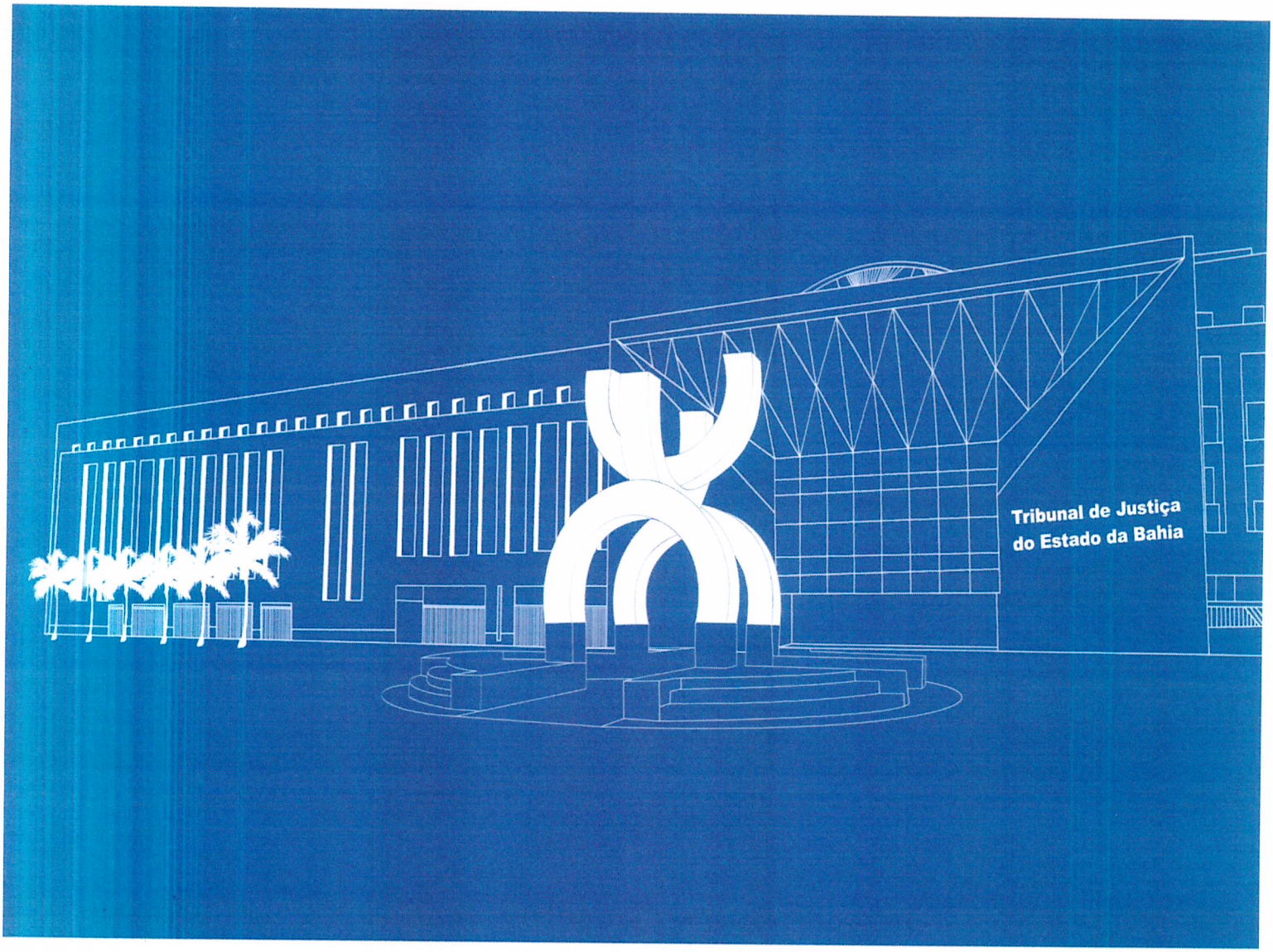

Protocolo de Investigação para Ilícitos Cibernéticos (PIIC-TJBA)

SUUMCUIQUE TRIBUERE

PODER JUDICIÁRIO
DO ESTADO DA BAHIA

Tribunal de Justiça do Estado da Bahia

Presidente

Desembargador Nilson Soares Castelo Branco

1ª Vice-Presidente

Desembargadora Gardênia Pereira Duarte

2ª Vice-Presidente

Desembargadora Márcia Borges Faria

Corregedor Geral de Justiça

Desembargador José Edivaldo Rocha Rotondano

Corregedor das Comarcas do Interior

Desembargador Edmilson Jatahy Fonseca Júnior

Secretário Geral da Presidência

Franco Bahia Karaoglan Mendes Borges Lima

Secretário de Tecnologia da Informação e Modernização

Ricardo Neri Franco

1. Objetivo e referências legais e normativas

O protocolo de investigação para ilícitos cibernéticos (PIIC-TJBA) do Tribunal de Justiça do Estado da Bahia é um documento complementar ao protocolo de gerenciamento de crises cibernéticas do Tribunal de Justiça do Estado da Bahia (PPINC-TJBA), que por sua vez é um complemento à Política de Segurança da Informação (PSI), instituída por meio do Decreto n.º 474, de 16 de agosto de 2019, **ANEXO VIII - NORMA DE GERENCIAMENTO DE INCIDENTES DE SEGURANÇA.**

Este Protocolo está alinhado à Resolução n.º 396 de 7 de junho de 2021, do Conselho Nacional de Justiça (CNJ) e tem por objetivo gerir ações para salvaguardar as evidências coletadas em investigações de incidente cibernético no ambiente computacional do TJBA.

2. Termos e definições

Incidente de segurança da informação: Qualquer evento que fuja da situação normal de utilização dos Sistemas de Informação, podendo ser uma violação ou uma ameaça de violação da Política de Segurança da Informação.

Autenticidade: Garante que a informação é verídica ou original.

Backup: É a cópia de segurança de um conjunto qualquer de dados.

Crise cibernética: É um cenário declarado quando o tratamento de determinado incidente cibernético não foi suficiente para solucioná-lo no tempo adequado, gerando uma situação fora do controle.

Ilícito: É o ato causador de prejuízo, seja patrimonial ou físico, ao Tribunal de Justiça do Estado da Bahia ou a terceiros.

Item de Configuração (IC): Qualquer componente tecnológico ou documental que faça parte de um serviço de TIC.

Sistemas de informação: Sistemas implantados ou em fase de implantação, destinados ao atendimento das atividades da instituição.

3. Escopo

3.1. Gerir ações para salvaguardar as evidências coletadas quando da investigação de um incidente cibernético no ambiente computacional do TJBA.

3.2. Determinar quais evidências serão disponibilizadas, em que momento e para qual agente externo/interno será entregue.

4. Requisitos informáticos

4.1. Para coletar as evidências necessárias para comprovação de um ilícito cibernético, alguns elementos devem ser previamente configurados ou tratados, sendo eles:

- Informações operacionais dos Itens de Configuração devidamente atualizados: horário e data de hosts (desktops, servidores, notebooks do TJBA, e outros hosts em que sejam aplicáveis tais configurações);
- Registro de logs de eventos;
- Informações mínimas de um log de evento (tipo do evento, usuário autenticado, data/hora, IP, porta de origem, descritivo da porta de origem);
- Usuário administrador que consiga realizar as devidas configurações.

4.2. Dispositivos tecnológicos que não sejam passíveis de aplicar as configurações do item 4.1, devem ser categorizados e geridos de forma diferenciada para que se consiga um mínimo de auditoria.

4.3. Sistemas computacionais, redes e demais ambientes tecnológicos devem ser monitorados de tal forma que o TJBA consiga obter informações suficientes para um processo de auditoria. Alguns controles que podem ser implementados: política de senha, estabelecimento de perfis de usuários e níveis de acesso, alteração de arquivos sistêmicos ou de uso departamental.

5. Processo de coleta de evidências computacionais

5.1. O processo de coleta de evidências computacionais deve ser estruturado de tal maneira que o TJBA consiga estabelecer um conjunto de atividades que atendam aos requisitos deste protocolo.

5.2. A responsável pelo processo de coleta de evidências computacionais será a Equipe de Tratamento e Resposta a Incidentes (ETIR) que deverá: a) preservar todas as evidências encontradas, b) preservar as mídias envolvidas no ilícito cibernético, c) manter os dados voláteis detectados, d) gerir e manter todos os eventos citados neste protocolo.

5.3. No caso da impossibilidade de preservar as evidências, visando retornar o serviço crítico de TIC ou sistemas à normalidade, a ETIR deverá fazer cópia de segurança do arquivo afetados pelo incidente cibernético. Um componente importante nesse procedimento são os arquivos de logs (quando aplicáveis), que devem ser preservados em sua totalidade.

5.4. Um relatório de coleta de evidências computacionais deve ser criado, buscando registrar todas as ações realizadas, o contexto do ilícito, o time envolvido no processo e as informações de todas as evidências encontradas. Esse artefato deverá ser produzido pela ETIR com a supervisão de um superior hierárquico.

5.5. Os materiais físicos envolvidos no processo de coleta de evidências devem ser isolados e devidamente armazenados, preferencialmente lacrados e inacessíveis para agentes não autorizados e entregues à autoridade competente.

6. Comunicação do ilícito cibernético

6.1. Uma das principais ações do processo de ilícito cibernético é a comunicação para os envolvidos.

6.2. Deverá ser criado um canal de comunicação oficial do TJBA e específico para esta finalidade.

6.3. Este canal de comunicação deverá ter um processo bem estruturado e monitorado pela equipe ETIR.

6.4. Quando um incidente cibernético for detectado e este for de abrangência relevante, os órgãos competentes serão devidamente comunicados.

6.5. O comitê de crise cibernética deverá ser acionado, assim que um incidente cibernético for detectado e declarado no TJBA.

6.6. A comunicação feita para os envolvidos no processo de investigação de ilícito cibernético deverá constar no relatório final, juntamente com todas as evidências encontradas.

6.7. A comunicação será realizada apenas para o público envolvido, não cabendo disseminar informações para públicos não interessados.

7. Ações contínuas pós-ilícito cibernético

7.1. Após o processo de ilícito cibernético ter sido encerrado, ações contínuas deverão ser realizadas para melhoria do ambiente organizacional e computacional.

7.2. As bases de conhecimento deverão ser atualizadas, fazendo constar o ocorrido do ilícito e as ações realizadas.

7.3. Caberá ao TJBA avaliar se o ambiente tecnológico pós-ilícito cibernético retornou à operação normal.

7.4. Os membros da equipe de Tratamento e Resposta a Incidentes (ETIR) e do Comitê Gestor de Segurança da Informação deverão realizar reunião formal para declarar o encerramento das ações do processo de investigação de ilícito cibernético.

Salvador, 29 de setembro de 2022

Desembargador NILSON SOARES CASTELO BRANCO

Presidente do Tribunal de Justiça da Bahia