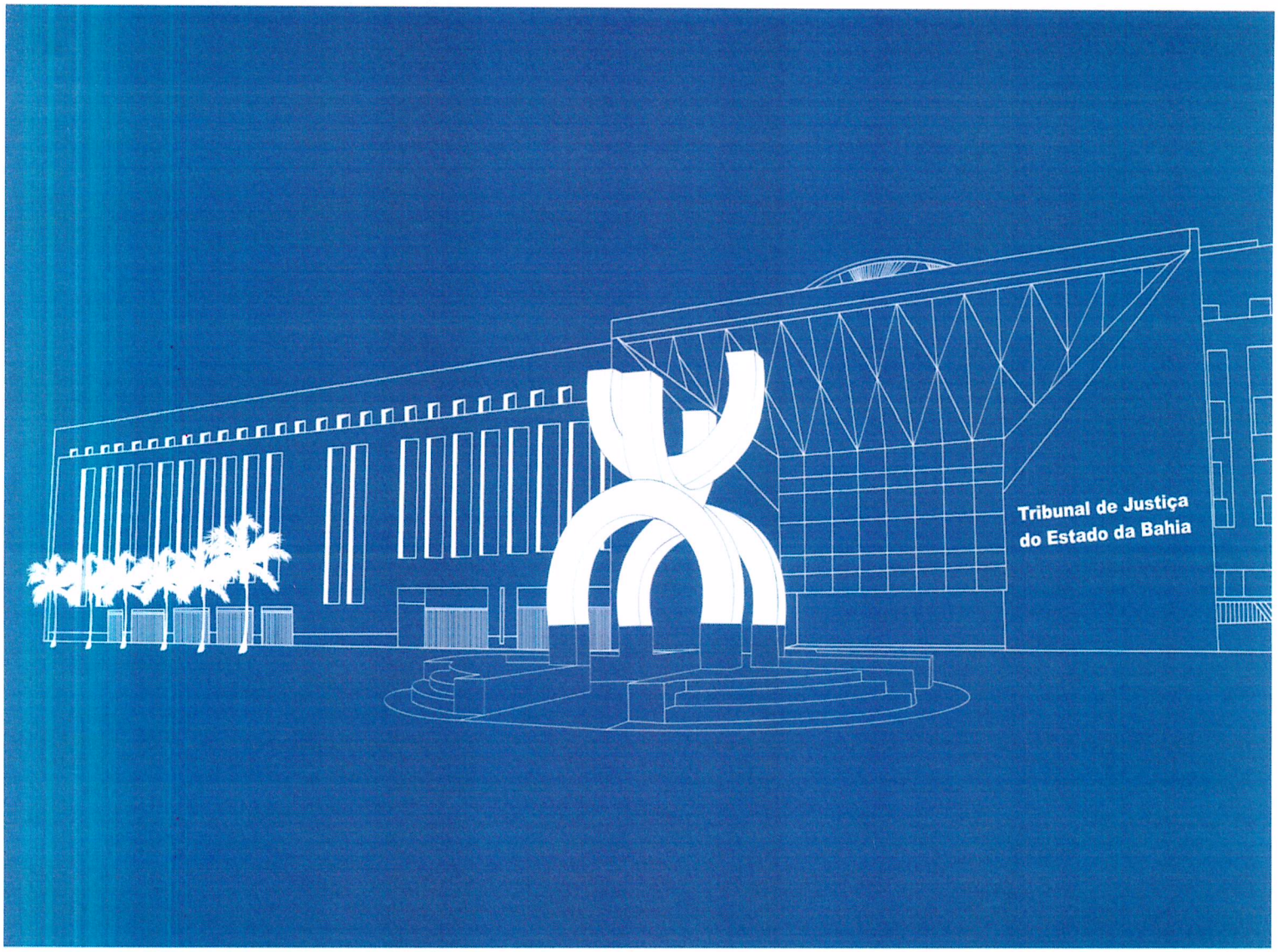

Protocolo de Prevenção de Incidentes Cibernéticos (PPINC-TJBA)

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 prevenção de incidentes cibernéticos do Tribunal de Justiça da Bahia (PPINC-TJBA) 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 atender aos incidentes de segurança cibernética no ambiente organizacional do TJBA.

2. Termos e definições

Confidencialidade: É a garantia de que as informações só serão acessíveis a partes autorizadas.

Disponibilidade: Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

Integridade: Salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

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.

3. Escopo

3.1. Este protocolo visa atender aos incidentes de segurança cibernética no ambiente organizacional do TJBA.

3.2. O protocolo de prevenção a incidentes cibernéticos do TJBA aborda um conjunto de direcionamentos para a prevenção a incidentes cibernéticos, com tratativas em alto nível, dando suporte às áreas estratégicas, táticas e operacionais do Órgão.

3.3. Os direcionamentos serão estruturados em processos que demonstram a gestão do risco tecnológico, entendendo que adaptações e ajustes poderão ocorrer visando acomodar a realidade organizacional do Tribunal de Justiça do Estado da Bahia.

4. Benefícios

4.1. Este protocolo de prevenção de incidentes cibernéticos busca trazer os seguintes benefícios:

a) Fortalecer as iniciativas de tratativas de incidentes cibernéticos;

b) Elevar o nível de segurança cibernética do ambiente tecnológico;

c) Adotar práticas e requisitos de segurança cibernética.

5. Processos de tratamento

5.1. O Protocolo de Prevenção a Incidentes Cibernéticos do TJBA possui os seguintes processos: identificar, proteger, detectar, responder e recuperar.

5.1.2. **Identificar:** compreender a estrutura organizacional para gerenciar o risco tecnológico contra-ataques cibernéticos a sistemas computacionais, pessoas envolvidas, ativos organizacionais e recursos de TIC – Tecnologia da Informação e Comunicação. O primeiro procedimento relevante é a identificação do incidente cibernético, sem o qual o TJBA não consegue atuar de maneira assertiva. O incidente de segurança cibernético deve ser registrado em uma ferramenta tecnológica para sua respectiva gestão.

5.1.3. **Proteger:** executar ações que busquem garantir a proteção de dados, de ativos da informação, bem como a prestação de serviços críticos, inclusive os serviços prestados remotamente por servidores públicos ou prestadores de serviços. Outros processos de TIC podem apoiar na execução da proteção de dados sendo alguns deles: gerenciamento de identidade, gestão de continuidade de serviço de TI (GCSTI) e gerenciamento de acesso.

5.1.4. **Detectar:** executar atividades de identificação/detecção de eventos de segurança cibernética. As ações de detecção geralmente passam por ferramentas e soluções tecnológicas implementadas e configuradas conforme as necessidades do TJBA. Um fator importante é criar as categorias de eventos de incidentes de segurança cibernéticos detectados, sejam elas: informacional, alerta ou crítico.

5.1.5. **Responder:** estabelecer um plano de resposta a incidentes de segurança cibernética de acordo com o cenário encontrado no TJBA, buscando atender as necessidades organizacionais. Outros planos podem ser criados e

serem complementares, sendo eles: a) plano de comunicação, b) plano de análise das informações coletadas, c) plano de melhorias de serviço de TIC (PMSTIC) e; d) plano de mitigação de riscos atrelados a TIC.

5.1.6. **Recuperar:** criar os planos de recuperação de incidentes cibernéticos e de restauração de quaisquer capacidades ou serviços de TIC – Tecnologia da Informação e Comunicação - que foram impactados negativamente em razão de incidentes de segurança cibernética ocorridos.

5.2. A gestão de incidentes de segurança da informação relaciona-se com a política de segurança da informação do TJBA, mencionada no item 2 deste artefato, que possui o seguinte fluxo de tratamento genérico: triagem, investigação, contenção, análise, recuperação.

6. Direcionadores

6.1. O protocolo de prevenção a incidentes cibernéticos criado no âmbito do Tribunal de Justiça do Estado da Bahia aborda um conjunto de direcionadores.

6.2. Os direcionadores podem ser adaptados de acordo com a realidade organizacional do Tribunal de Justiça do Estado da Bahia, sendo eles:

6.2.1. Criar uma base de conhecimento: consiste em criar um repositório para o uso e compartilhamento de informações e conhecimento de ataques cibernéticos reais que comprometeram os sistemas computacionais. O objetivo é fomentar o aprendizado contínuo e a disseminação de conteúdo relacionado aos aspectos de segurança da informação no ambiente organizacional do TJBA.

6.2.2. Estabelecer mecanismos de medição: definir os instrumentos e as métricas para otimizar a compreensão do contexto de incidente cibernético de todos os atores envolvidos do sistema de segurança da informação. Seu objetivo é medir o que está sendo gerenciado e estabelecer métricas coletáveis e auditáveis.

6.2.3. Criar práticas de monitoração: trata-se de um processo de trabalho contínuo de monitoramento e análise para coletar, medir e validar se as ações de segurança da informação estão gerando os resultados esperados pelo TJBA.

6.2.4. Realizar a Melhoria de Serviço Continuada (MSC): executar melhorias

cíclicas nos sistemas de segurança da informação e comunicação e nos processos de tratamento a incidentes cibernéticos. A melhoria de serviço continuada (MSC) pode percorrer a busca por automações com base em ferramentas tecnológicas. Uma ferramenta importante nesse item é o uso do ciclo **PDCA (Planejar/Fazer/Checar/Agir)** para melhorar políticas, processos e procedimentos de gerenciamento de incidentes cibernéticos e relacionados.

6.2.5. Fomentar a capacitação: incluir planos de treinamentos periódicos (minimamente anuais), que contemplem a formação de todos os atores envolvidos em atividades diretas ou indiretas, ligadas ao processo de segurança cibernética no ambiente do TJBA.

6.2.6. Estabelecer um PCN e PCSTI: criar um Plano de Continuidade de Negócio (PCN), em consonância com o Plano de Continuidade de Serviço de TI (PCSTI).

6.2.7. Criar processos de auditorias: possuir ferramentas e soluções que sejam capazes de realizar e consolidar os registros de auditorias em diversas fontes de ativos, principalmente os relacionados com os serviços críticos de TIC.

6.2.8. Manter processos de cópia de segurança: providenciar a realização de cópia de segurança de sistemas computacionais e serviços de TIC, de forma automática e em local protegido.

6.2.9. Adotar práticas de gestão de acessos externos: elaborar processos e procedimentos específicos que sejam aplicados a acessos externos, inclusive abordando equipamentos de notebook, telefones celulares e outros possíveis dispositivos portáteis.

7. Equipe ETIR

7.1. Criar uma Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) que deverá atuar no ambiente tecnológico e organizacional do TJBA.

7.2. Caberá ao TJBA avaliar o posicionamento hierárquico que a equipe ETIR ocupará em seu organograma institucional.

7.3. A ETIR terá autonomia em suas atuações, participando de decisões táticas e operacionais, principalmente em assuntos relacionados com os procedimentos a serem executados para as tratativas de um incidente

cibernético. Sua autonomia será gerida pelo Comitê Gestor de Segurança da Informação.

7.4. A ETIR atuará diretamente ou colaborará com as atividades que envolvam segurança da informação relacionadas ao ambiente tecnológico.

7.5. A ETIR será composta por servidores da Secretaria de Tecnologia da Informação do TJBA, que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e à resposta a incidentes de segurança da informação, as quais são prioritárias.

7.6. O funcionamento da ETIR se dará da seguinte forma:

7.6.1. Será regulado por documento formal do TJBA, publicado no sítio do órgão, contendo minimante os seguintes pontos:

a) Objetivo;
b) Definição da missão;
c) Responsabilidades
d) Público-alvo;
e) Nível de autonomia;
f) Designação de integrantes;
g) Canal de comunicação de incidentes de segurança da informação; e
h) Serviços prestados.

7.7. Enquanto não efetivado o art. 21 da Resolução CNJ nº 396/2021, a ETIR estará temporariamente subordinada ao Comitê Gestor de Segurança da Informação.

8. Boas práticas de segurança cibernética

8.1. Guiando-se pelas boas práticas de mercado, o processo de prevenção a incidentes de segurança cibernética contempla os processos de:

- Preparação;
- Identificação;
- Contenção;
- Erradicação;
- Recuperação; e
- Lições aprendidas.

8.1.1. **Preparação:** é o processo de criar e treinar equipe para atuar na resposta a incidentes de segurança cibernética.

8.1.2. **Identificação:** trata-se do processo de identificar os incidentes de segurança e analisar os eventos relacionados. Podem ser utilizadas ferramentas tecnológicas para apoiar o processo de diagnóstico e otimizar os resultados esperados.

8.1.3. **Contenção:** tem como prioridade isolar o ambiente de TIC afetado, buscando manter o ambiente de produção/operacional e garantir que as ações não comprometam a segurança da informação ou as operações críticas. O principal objetivo é não comprometer o ambiente que ainda não foi impactado negativamente.

8.1.4. **Erradicação:** composta de ações para remover/retirar/erradicar a ameaça do ambiente tecnológico do TJBA. Neste processo são aplicadas soluções e realizados procedimentos técnicos que visem reconstruir o sistema ou o serviço de TI impactado. O principal objetivo é a remoção da ameaça e o refazimento do item ou serviço de TIC impactado.

8.1.5. **Recuperação:** consiste em publicar o plano de recuperação em fases para restauração das operações de TI, com foco nos sistemas críticos. O objetivo é recuperar o mais rápido possível os sistemas e serviços de TIC que são vitais para o TJBA.

8.1.6 **Lições aprendidas:** Trata-se da criação de um Registro de Lições Aprendidas e o estabelecimento de um processo contínuo para capturar os impactos imediatos de um incidente de segurança cibernética. A principal ideia é o de armazenamento de registros das ações executadas para a recuperação dos sistemas e serviços críticos de TIC, para uma possível reutilização em momento oportuno.

8.2. Criar um canal de comunicação assertivo e claro entre os envolvidos para potencializar a gestão do processo de incidentes de segurança cibernética. Esse canal de comunicação deve ser executado e monitorado com métricas próprias, no sentido de atender os interesses do TJBA.

8.2. Estabelecer, publicar e atualizar lista de sistemas e serviços críticos de TIC, a qual deverá conter os componentes/sistemas/serviços considerados vitais para o negócio do TJBA.

Salvador, 29 de setembro de 2022

Desembargador NILSON SOARES CASTELO BRANCO

Presidente do Tribunal de Justiça da Bahia