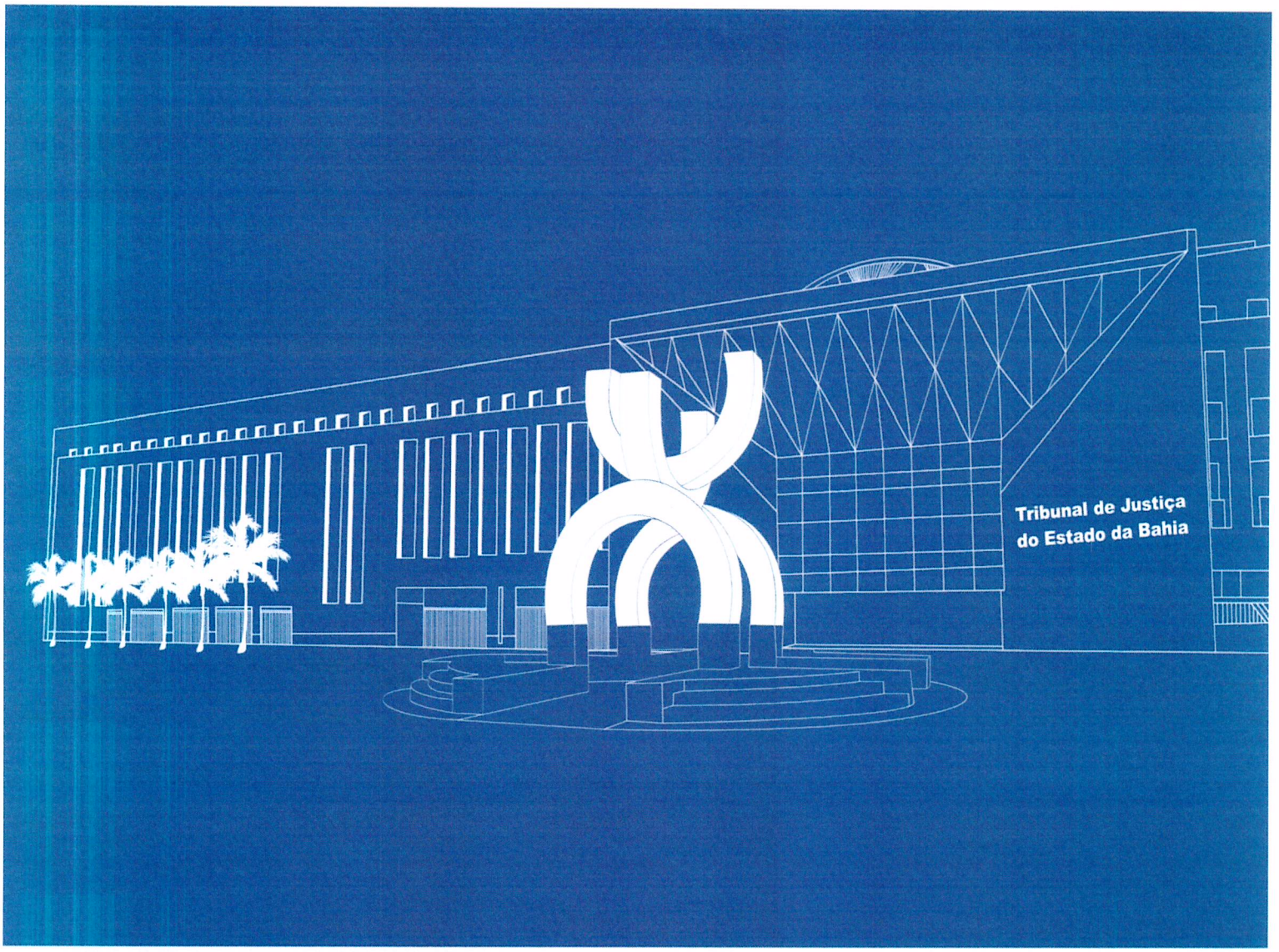

Protocolo de gerenciamento de crises cibernéticas (PGCRC-TJBA)

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 gerenciamento de crise cibernética (PGCRC-TJBA) do Tribunal de Justiça do Estado da Bahia é um documento complementar ao Protocolo de Prevenção de Incidentes Cibernéticos do Tribunal de Justiça do Estado da Bahia (PPINC-TJBA), que por sua vez é um complemento da política de segurança da informação - PSI, instituída pelo Decreto Judiciário n.º 474, de 16 de agosto de 2019, constante do **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 tempestivas quando ficar evidente que um incidente de segurança cibernética não será tratado/mitigado de forma rápida.

2. Termos e definições

Para fins deste protocolo define-se:

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.

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

3. Escopo

3.1. Gerir ações tempestivas quando ficar evidente que um incidente de segurança cibernética não será tratado/mitigado de forma adequada, estabelecendo-se um ambiente de crise, que pode trazer severos impactos

negativos para o TJBA.

3.2 Determinar um ambiente de crise tecnológica no TJBA, se um incidente de segurança cibernética não foi resolvido e não exista perspectiva de ser resolvido em curto espaço de tempo.

4. Identificar uma crise cibernética

4.1. Uma das primeiras atividades em um processo de crise cibernética é a identificação. O processo de gerenciamento de incidentes de segurança é composto de atividades para avaliar o cenário encontrado no TJBA e determinar uma resposta inicial para um evento danoso na área de segurança da informação.

4.1.2. O processo de gerenciamento de crise inicia-se quando:

a) Um impacto severo nos serviços críticos de TIC ou sistemas for detectado, a ponto de não ser capaz de aplicar uma solução de contorno em até vinte e quatro horas;

b) Caracterizar-se dano financeiro ou institucional, impactando negativamente o TJBA;

c) Evidenciar-se que as ações de resposta ao incidente cibernético provavelmente irão se prolongar por médio e longo prazo;

d) O incidente impactar severamente a atividade finalística do TJBA;

e) O incidente cibernético impactar a sociedade de uma maneira geral;

f) O incidente cibernético, ocorrido no ambiente computacional do TJBA, causar impactos negativos em outras esferas governamentais.

5. Gestão de crises

5.1. O protocolo de gerenciamento de crise cibernética no âmbito do Tribunal de Justiça do Estado da Bahia estrutura-se com base nas fases estabelecidas pela resolução em referência no item 1 deste artefato, quais sejam: pré-crise (planejamento); execução (investigação e solução) e melhoria contínua de serviço (pós-crise).

5.2. Fase 1 (Pré-crise): é uma fase fundamental em que o TJBA precisa se estruturar para atuar em possível ambiente de crise. Para isso alguns componentes devem ter sido previamente criados, sendo eles: a) base de conhecimento estabelecida, b) políticas e procedimentos institucionais implementados para apoiar o tratamento de incidentes, c) ambiente computacional monitorado adequadamente, d) auditórias cíclicas em sistemas e serviços críticos de TIC; e) processo de gestão de riscos ativo.

As atividades recomendas nessa fase são:

a) Identificar quais são os ativos críticos no ambiente tecnológico do TJBA;
b) Analisar o protocolo cibernético de prevenção a incidente cibernético;
c) Verificar o processo de gerenciamento de riscos e seus respectivos planos de respostas e monitoramento;
d) Identificar as categorias de incidentes cibernéticos para uma análise mais detalhada e precisa;
e) Promover a realização de simulação de testes de invasão e avaliar continuamente a efetividade dos planos criados;
f) Criar plano de crise que possa conduzir o TJBA em um ambiente adverso.
g) Estabelecer um comitê de crise cibernética em um processo de sala de crise.

5.3. Fase 2 - investigação e solução (execução): é a fase pós-planejamento, na qual uma das primeiras ações é criar um canal de comunicação entre os atores envolvidos no ambiente de crise. As seguintes atividades fazem parte dessa etapa:

a) A equipe ETIR deve determinar se o TJBA está em um ambiente de crise cibernética;
b) Em uma sala de crise criada, o comitê de crise deve se reunir para realizar as devidas tratativas iniciais;
c) Os responsáveis pelo comitê de crise devem acionar os respectivos planos de apoio, entre os quais: Plano de Continuidade de Negócio (PCN), Plano de Continuidade de Serviço de TIC (PCSTI), Plano de Contingência;
d) O comitê de crise deverá minimamente:

- Ter uma visão clara do ambiente de crise;
- Possuir suporte do processo de gerenciamento de riscos;
- Analisar as informações da área de monitoramento e eventos de TIC;
- Verificar as informações oriundas do processo de gerenciamento de incidentes cibernéticos;
- Considerar os incidentes graves no processo de análise;
- Avaliar a necessidade de suspender ou desativar os serviços críticos de TIC ou sistemas que foram impactados;
- Convocar especialistas para apoiar as ações;
- Definir as prioridades nas atividades;
- Evocar um plano de retorno das atividades críticas;
- Realizar reuniões regulares até que a crise seja dissipada.

5.3. Fase 3 - melhoria contínua de serviço (pós-crise): é a fase pós-crise, na qual análises deverão ser realizadas para verificar as ações tomadas e seus efeitos positivos. Algumas ações centrais deverão ser realizadas, como:

- Analisar a causa-raiz do incidente cibernético;
- Verificar a efetividade das ações realizadas pelo comitê de crise e atores envolvidos;
- Criar um relatório pós-crise para efeito de registro e inserção na base de conhecimento;
- Comunicar os envolvidos e as áreas impactadas de que a crise foi dissipada e os serviços de TIC ou sistemas foram reestabelecidos;
- Registrar o tempo em que os sistemas/serviços críticos de TIC ficaram indisponíveis;
- Resguardar e dispor as evidências encontradas, a exemplo de logs e outros itens relevantes.

6. Ações contínuas pós-crise

6.1. Após o momento de crise ter sido resolvido com as ações efetivas do TJBA, é relevante manter o impulso das ações pós-crise tratando devidamente relatórios e evidências.

6.2. Ações pós-crise que podem ser verificadas: a) melhorar o processo de

prevenção de incidentes cibernéticos, b) melhorar o processo de gerenciamento de crise cibernética, c) ampliar e melhorar as ferramentas tecnológicas de proteção ao ambiente computacional; d) identificar possíveis gaps no processo de gerenciamento de riscos; e) analisar a eficácia do processo de gerenciamento de incidentes graves; f) fomentar treinamentos técnicos acerca da temática de tratamento de crises.

6.3. Caberá ao TJBA avaliar se o ambiente tecnológico pós-crise retornou à operação normal anterior ao momento da crise e comunicar aos envolvidos os resultados encontrados. Por operação normal entende-se: condições pactuadas em acordos de níveis de serviços.

6.4. Analisar o comportamento tecnológico do serviço de monitoramento de serviços críticos de TIC e sistemas computacionais.

Salvador, 29 de setembro de 2022

Desembargador NILSON SOARES CASTELO BRANCO
Presidente do Tribunal de Justiça da Bahia