**TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE**
**COMISSÃO PERMANENTE DE SEGURANÇA DA INFORMAÇÃO**

# ATA DE REUNIÃO Nº 2/2024/CPSI

## 1. Identificação da reunião

| Data | Horário | Local | Responsável |
|---|---|---|---|
| 17/05/2024 | 9h às 10h | Reunião remota | Marcos Flávio Nascimento Maia |

## 2. Objetivo

Informes da CPSI e próximas demandas

## 3. Itens da pauta

| Item | Descrição |
|---|---|
| 1. | Apresentação do Plano de Trabalho de Segurança da Informação |
| 2. | Treinamento de Segurança da Informação |
| 3. | Múltiplo Fator de Autenticação - SEI 3749/2024 |
| 4. | 3º Evento de Cybersegurança |

## 4. Participantes

| Nome | Setor de atuação |
|---|---|
| Alexandre Márcio Cavalcanti Machado | SSI/COINF |
| Arlley Andrade de Souza | 1ª Zona Eleitoral |
| Augusto César Macedo Brandão de Araújo | ASSINT (AUSENTE - Licença médica) |
| Carlos Magno do Rozário Câmara | COINF |
| Daniel César Gurgel Coelho Ponte | SRI/COINF/STIE |
| Denilson Bastos da Silva | SSI/COINF/STIE (AUSENTE - Férias) |

| | |
|---|---|
| Edwin Aldrin Salviano de Brito | NSI/PRES |
| Francisco de Assis Paiva Leal | SSI/COINF/STIE |
| Gabriela Domitildes da Silva Xavier | NSI/PRES |
| Helder Jean Brito da Silva | SSI/COINF/STIE |
| Isaac Bruno Gomes Leandro | AJCRE |
| Janaína Helena Ataíde Targino | SJDP/CGI/SJ (AUSENTE) |
| José Wendell de Morais Silva | SBDS/COSIS/STIE |
| Karla Ramos Donida | SEGEAT/CODES/SGP |
| Leonardo Dantas de Oliveira | SRI/COINF/STIE |
| Marcos Flávio Nascimento Maia | STIE |
| Maria Ruth Bezerra Maia de Hollanda | AGE/PRES |
| Nelson de Queiroz Oliveira | SEPOF/COFIN/SAOF |
| Osmar Fernandes de Oliveira Junior | COSIS/STIE |
| Sara Angélica Oliveira Cardoso | ASCOM/PRES |
| Thiago Fernandes Silva Dutra | SBDS/COSIS/STIE |
| Walquíria Gomes Cortez Cordeiro | GAPDG |

**5. Itens de Discussão**

| Item | Descrição | Responsável |
|---|---|---|
| 1. | Apresentação do Plano de Trabalho de Segurança da Informação<br>• Marcos Maia apresentou o plano aos presentes, esclarecendo que já havia sido validado em reunião do COGESTIC em 08.02.2024.<br>• Esclarecido que se trata de Plano que contempla ações com prazos, responsáveis e situação, objetivando a garantia de cumprimento de todas as exigências constantes nas normas abaixo relacionadas:<br>◦ Resolução CNJ nº 396/2021 - ENSEC-PJ<br>◦ Resolução TSE nº 23644/2021 - PSI JE<br>◦ Resolução TRE-RN nº 110/2023 - PSI JERN<br>• Aprovado o conteúdo do plano por todos os participantes e definido que será encaminhado à Administração para apreciação e instituição formal. | Marcos Maia |

| | | |
|---|---|---|
| 2. | Treinamento de Segurança da Informação<br><br>• Aprovada a realização de um treinamento sobre "Engenharia Social" com tema em segurança da informação no 2º semestre paara todos os servidores utilizando a ferramente KnowBe4 | Todos os participantes |
| 3. | Múltiplo Fator de Autenticação (MFA) - SEI 3749/2024<br><br>• Apresentado por Marcos o teor da Portaria 140/2024-CNJ encaminhada por meio do Ofício-Circular 32/2024 - CNJ (SEI 3749/2024)<br>• A portaria determina que os órgãos do Poder Judiciário implementem de método de autenticação do tipo Múltiplo Fator de Autenticação (MFA) como requisito funcional para acesso a sistemas judiciais sensíveis.<br>• Restou definido que a COINF e COSIS farão análise de viabilidade de implementação do MFA nos sistemas do TRE/RN que se enquadram na classificação de sistemas judiciais sensíveis, de acordo com o art. 2º da Portaria em questão.<br>• O prazo estabelecido pelo CNJ para a implementação do MFA é de 90 dias após a publicação da norma (a partir de 24.04.2024). | Todos os participantes |
| 4. | 3º Evento de Cybersegurança<br><br>• Definido que será realizado no dia 14.06.2024, em formato híbrido<br>• Programação:<br>◦ 09:15 - Abertura DG e STIE<br>◦ 09:25 - Palestra sobre LGPD (Dra. Anna Raves - advogada)<br>◦ 10:00 - Quiz sobre palestra LGPD<br>◦ 10:10 - Palestra sobre Cibersegurança (Profª. UFRN)<br>◦ 10:45 - Café e sorteio de brindes<br>◦ 11:00 - Palestra sobre Segurança do Sistema Eleitoral Eletrônico (Rodrigo Carneiro - SERVIN TSE)<br>◦ 12:00 - Encerramento | Marcos Maia<br>Carlos Magno |

**6. Pendências**

| Item | Pendência | Data limite | Responsável |
|---|---|---|---|
| 1. | Estudo de viabilidade de implementação do MFA nos sistemas sensíveis do TRE/RN | 07/06/2024 | COINF / COSIS |
| 2. | Memorando encaminhando o PTS à Diretoria-Geral | 22/05/2024 | GAPSTIE |
| 3. | Memorando solicitando autorização para realização do 3º Evento de Cybersegurança | 31/05/2024 | CPSI |

**7. Observações**

Sem observações.

**8. Fechamento da Ata**

| Data | Secretário(a) |
|---|---|
| 17/05/2024 | Dina Márcia de V. Maranhão da Câmara |

**ANEXO(S)**

Plano de Trabalho de Segurança da Informação (0042844)

Documento assinado eletronicamente por **Maria Ruth Bezerra Maia de Hollanda**, **Membro da Comissão Permanente de Segurança da Informação**, em 27/03/2025, às 15:43, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Marcos Flavio Nascimento Maia**, **Presidente da Comissão Permanente de Segurança da Informação**, em 28/03/2025, às 11:45, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Alexandre Marcio Cavalcanti Machado**, **Membro da Comissão Permanente de Segurança da Informação**, em 28/03/2025, às 11:53, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Carlos Magno do Rozario Camara**, **Presidente da Comissão Permanente de Segurança da Informação**, em 28/03/2025, às 11:54, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Thiago Fernandes Silva Dutra**, **Membro da Comissão Permanente de Segurança da Informação**, em 28/03/2025, às 11:54, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Helder Jean Brito da Silva**, **Membro da Comissão Permanente de Segurança da Informação**, em 28/03/2025, às 12:00, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Francisco de Assis Paiva Leal**, **Membro da Comissão Permanente de Segurança da Informação**, em 28/03/2025, às 12:20, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-rn.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=0041405&crc=6AA82E18 informando, caso não preenchido, o código verificador **0041405** e o código CRC **6AA82E18**.

# PLANO DE TRABALHO DE SEGURANÇA DA INFORMAÇÃO

**Implantação da Resolução 396 CNJ; Resolução 23.644 TSE e dos Protocolos e Manuais elencados na Portaria nº 162/2021-CNJ;**

**SSI**

SEÇÃO DE SEGURANÇA DA INFORMAÇÃO

**CPSI**

COMISSÃO PERMANENTE DE SEGURANÇA DA INFORMAÇÃO

**NATAL - TRE/RN**

Tribunal Regional Eleitoral-RN

Tribunal Regional Eleitoral-RN

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE

# PLANO DE TRABALHO DE SEGURANÇA DA INFORMAÇÃO

**Secretaria de Tecnologia da Informação e Eleições**
**Coordenadoria de Infraestrutura Tecnológica**
**Seção de Segurança da Informação**

**Natal | 2024**

# INTRODUÇÃO

O Conselho Nacional de Justiça (CNJ), através da Portaria nº 162 de 10/06/2021 aprovou os Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

Os protocolos e manuais aprovados por este ato deverão ser implementados por todos os órgãos do Poder Judiciário, com exceção do Supremo Tribunal Federal.

A norma contém os seguintes protocolos (Anexos I, II e III):

I – Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ);

II – Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ); e

III – Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ).

A norma contém os seguintes manuais (Anexos IV, V, VI e VII):

I – Proteção de Infraestruturas Críticas de TIC;

II – Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital;

III – Gestão de Identidades; e

IV – Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário.

# IDENTIFICAÇÃO

Identificação do Plano:

| NOME |
|---|
| Plano de Trabalho de Segurança da Informação para Implementação dos Protocolos e Manuais aprovados na Portaria nº 162/2021-CNJ no âmbito do TRE/RN |
| **PÚBLICO-ALVO** |
| TRE RN |

| UNIDADE ADMINISTRATIVA |
|---|
| Presidência |
| **UNIDADE SOLICITANTE** |
| Secretaria de Tecnologia da Informação e Eleições (STIE) |

| HISTÓRICO DE REGISTRO | | | |
|---|---|---|---|
| **DATA** | **RESPONSÁVEL** | **DESCRIÇÃO** | **VERSÃO** |
| 04/10/2023 | Seção de Segurança da Informação/COINF/STIE e Coordenadoria de Infraestrutura Tecnológica/STIE | Elaboração de documento | 2.0 |

# JUSTIFICATIVA

Necessidade de implementação dos Protocolos e Manuais aprovados pelo Conselho Nacional de Justiça (CNJ) através da Portaria nº 162 de 10/06/2021, criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), no âmbito do Poder Judiciário, com revisão a cada dois anos.

# OBJETIVOS

O Plano de Trabalho de Segurança da Informação visa a implementação dos Protocolos e Manuais aprovados pelo Conselho Nacional de Justiça (CNJ) através da Portaria nº 162 de 10/06/2021, criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte (TRE/RN).

# ALINHAMENTO ESTRATÉGICO

O Plano de Trabalho de Segurança da Informação está alinhado quanto ao:

**Plano Estratégico da Justiça Eleitoral do RN 2021-2026 (PEJERN):**

- Fortalecimento da segurança da informação – Objetivo Estratégico AC3
  - Promover o fortalecimento contínuo da segurança da informação no âmbito institucional – Iniciativa AC3.1;
  - Fortalecer a segurança cibernética assegurando o alinhamento às diretrizes do Poder Judiciário – Iniciativa AC3.2;
  - Aprimorar a infraestrutura tecnológica e os serviços em nuvem – Iniciativa AC3.3;
  - Fortalecer a gestão de riscos de incidentes de TIC – Iniciativa AC3.4 ;
  - Implementar mecanismos voltados à proteção de dados pessoais – Iniciativa AC3.5.

# BENEFÍCIOS ESPERADOS

Este plano tem como resultados pretendidos:

- ☐ Formalizar este plano de trabalho de segurança da informação ao TRE/RN;
- ☐ Estabelecer objetivos, princípios e diretrizes de Segurança da Informação, no âmbito do TRE/RN, alinhados às recomendações constantes das normas que trata sobre o tema;

- ☐ Regulamentar as normas que dispõe sobre a Estrutura de Gestão da Segurança da Informação, no âmbito do TRE/RN;
- ☐ Sensibilizar e conscientizar os servidores sobre a Segurança da Informação;
- ☐ Aprimorar a capacidade do Poder Judiciário, no âmbito do TRE/RN, de coordenar pessoas, desenvolver recursos e aperfeiçoar processos, visando minimizar danos e agilizar o restabelecimento da condição de normalidade em caso de ocorrência de ataques cibernéticos de grande impacto.

# PRIORIZAÇÃO DAS AÇÕES

Este plano está adstrito a propor à administração do TRE/RN um conjunto inicial de ações estruturantes que visam a implementação dos Protocolos e Manuais aprovados pelo Conselho Nacional de Justiça (CNJ) através da Portaria nº 162 de 10/06/2021, criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

A Segurança da Informação é um tema que envolve diferentes aspectos de uma organização, desde os locais onde a informação é guardada até recursos humanos e tecnológicos.

Abrange processos de trabalho, relação com fornecedores e prestadores de serviço, uso adequado das ferramentas e serviços de tecnologia da informação, cuidados com o ambiente de trabalho e publicação de normas que regulamentem o tema.

Diante dessas várias linhas de ação possíveis, a CPSI, Seção de Segurança da Informação/COINF/STIE junto com a Coordenadoria de Infraestrutura Tecnológica/STI dirigiu os esforços para ações voltadas à estruturação da gestão da Segurança da Informação, com a classificação dessas necessidades, resultando na seleção de um reduzido conjunto de ações prioritárias, formado por ações estruturantes e por ações de conformidade, consideradas passíveis de execução no espaço de tempo de dois anos a partir de sua propositura.

Nele constam as ações, essas categorizadas como estratégicas, vinculados às diretrizes prioritárias definidas no plano de gestão dos dirigentes do Tribunal, alinhadas ao plano estratégico, passando a compor o portfólio institucional do biênio respectivo.

## AÇÕES RECOMENDADAS

Recomenda-se à Presidência do Tribunal Regional Eleitoral do Rio Grande do Norte a implementação de ações de conformidade, ações de sensibilização e conscientização.

# ACOMPANHAMENTO DAS AÇÕES

Todas as ações serão acompanhadas pela estrutura de pessoal do Sistema de Gestão da Segurança da Informação.

O Sistema de Gestão de Segurança da Informação (SGSI) do TRE/RN inclui estratégias, planos, políticas, medidas, controles, e diversos instrumentos usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação. Estabelecido, inicialmente, junto à estrutura de Governança Corporativa de Tecnologia da Informação e Comunicação, por meio da Resolução TRE/RN n. 12/2014, consolida-se como o conjunto de instrumentos estratégicos fundamentais para que a organização possa integrar a segurança da informação às suas políticas e objetivos estratégicos.

Seu objetivo é instituir diretrizes estratégicas, responsabilidades e competências visando à estruturação da segurança da informação; promover ações necessárias à implementação e à manutenção da segurança da informação; combater atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação e a imagem da instituição; e promover a conscientização e a capacitação de recursos humanos em segurança da informação.

No TRE/RN, a estrutura de pessoal do Sistema de Gestão da Segurança da Informação é composta pela Comissão Permanente de Segurança da Informação (CPSI), instituída por meio da Resolução TRE/RN n.º 008/2009, a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR), instituída por meio da Portaria n.º 423/2017, o Gestor de Segurança da Informação, designado através da Portaria DG n.º 45/2017 e, pela Seção de Suporte e Segurança da Informação (SSI), vinculada à Coordenadoria de Infraestrutura Tecnológica/STIE, criada após reestruturação estabelecida pela Resolução TRE/RN n.º 19/2019.

# CRONOGRAMA

| CNJ | | | | | |
|---|---|---|---|---|---|
| **RESOLUÇÃO 396** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 10 | .Elaboração da Política de Riscos de SI e Mapeamento do processo que Gestão de Riscos de SI | SSI | dez/24 | .Portaria n.º 183/2020 - GP - Institui o processo de Gestão de Riscos da Segurança da Informação, no âmbito da Justiça Eleitoral do Rio Grande do Norte<br>ver inciso:<br>11.1 Anexo V | Em andamento |
| 10 | .estabelecer um Sistema de Gestão em Segurança da Informação baseado em riscos | estrutura de Governança Corporativa de Tecnologia da Informação e Comunicação | dez/23 | .Resolução TRE/RN n. 12/2014, no Portal de Transparência em: https://www.tre-rn.jus.br/transparencia-e-prestacao-de-contas/governanca-e-gestao-de-tic/sistema-de-gestao-da-seguranca-da-informacao | Finalizada |
| 10 | .revisar, bianualmente, a estrutura de pessoal do Sistema de Gestão da Segurança da Informação | estrutura de Governança Corporativa de Tecnologia da Informação e Comunicação | dez/25 | .Resolução TRE/RN n. 12/2014, no Portal de Transparência em: https://www.tre-rn.jus.br/transparencia-e-prestacao-de-contas/governanca-e-gestao-de-tic/sistema-de-gestao-da-seguranca-da-informacao | Ação Contínua |
| Art. 11, I. III e XI | .elaborar Plano de Resposta a Incidentes de Segurança Cibernética | SSI | dez/24 | ver incisos:<br>- 2.1.4 Anexo I<br>- 7.5.2 Anexo I<br>- 7.5.3 Anexo I<br>- 7.5.4 Anexo I<br>- 7.5.5 Anexo I | Em andamento |

| CNJ | | | | | |
|---|---|---|---|---|---|
| **RESOLUÇÃO 396** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| Art. 11, I. III e XI | Revisar Plano de Continuidade de Serviços Essenciais de TIC | COINF e COSIS | jun/23 | .Portaria n.º177/2019-GP - Institui a Gestão da Continuidade de Serviços Essenciais de Tecnologia da Informação e Comunicação - TIC<br><br>.Portaria n.º 191/2019 - GP - Institui os processos de Gerenciamento dos Acordos de Nível de Serviços Essenciais de TIC e de Monitoramento e Aferição dos Acordos de Nível de Serviços Essenciais de TIC, no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte<br><br>ver incisos:<br>- 2.1 Anexo I<br>- 5.3 Anexo II<br>- 26.1 Anexo V | Finalizada |
| Art. 11, II<br>Art. 19, V | Revisar a norma que institui a ETIR, de acordo com a ENSEC_PJ e PSI do TSE | Agente Responsável pela ETIR | dez/23 | .Portaria n.º423/2017-GP - Institui a Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais (ETIR)<br><br>.Portaria n.º 127/2020 - GP - Altera a Portaria n.º 423/2017-GP, que institui a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) no âmbito do TRE-RN | Finalizada |
| Art. 11, II<br>Art. 19, V | .publicar Portaria com nova composição e atribuições da ETIR | PRES | dez/23 | | Finalizada |

| CNJ | | | | | |
|---|---|---|---|---|---|
| **RESOLUÇÃO 396** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| Art. 11, IV | .concluir aquisição, treinamento e implementação da solução de Controle de Ativos e Patches | COINF | dez/23 | [IVANTI] [Gestão de Patches e Ativos]<br><br>[Contrato nº 54/2022] [SYSTEM MANAGER TECNOLOGIA LTDA]<br><br>[PAE] [2584/2022] (planejamento)<br><br>[PAE] [11836/2022] (seleção do fornecedor) e (gestão do contrato)<br><br>ver incisos:<br>- 3.2.2 Anexo I<br>- 2.8 Anexo III<br>- 32.1 Anexo V<br>- 34.4.f Anexo V | Finalizada |
| Art. 11, V | .dar continuidade a participação de servidor do Tribunal em grupo Nacional de SI do TSE e incluir servidor da SSI em grupos acadêmicos ou fóruns abertos que discutam Cibersegurança | SSI | | | Ação Contínua |
| Art. 11, VI | .revisar Processo de Gerenciamento de Cópias de Segurança (backup) e de Restauração de Dados de forma a providenciar a realização de cópias de segurança atualizadas e segregadas de forma automática em local protegido, em formato que permita a investigação de incidentes | SRI | jun/23 | Portaria n.º 183/2020 - GP -processo de Gerenciamento de Cópias de Segurança (backup) e de Restauração de Dados | Finalizada |
| Art. 11, VI | .revisar a Política de Backup (Portaria n.º 130/2017) | SRI | dez/22 | ver inciso:<br>- 7.2 Anexo IV<br>- nova norma aguardando publicação | Finalizada |
| Art. 11, VI | .validar a implantação da nova Solução de Backup | SRI | jun/23 | | Finalizada |

| CNJ | | | | | |
|---|---|---|---|---|---|
| **RESOLUÇÃO 396** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| Art. 11, VII | .instituir a Política de Gestão de Ativos contendo requisitos específicos de segurança relativos aos ativos, incluindo ambientes centralizados, endpoints, equipamentos intermediários ou finais conectados em rede ou a algum sistema de comunicação, inclusive computadores portáteis e telefones celulares (Implantação do IVANTI) | COINF | dez/24 | TSE: Portaria nº 458 de 13 de julho de 2021 - Institui norma de gestão de ativos, relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral<br><br>TRE/RN: Portaria n.º 195/2019 - GP - Institui o processo de Gerenciamento de Configuração e Ativos de TIC, no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte<br><br>Solução adquirida: [IVANTI]<br><br>Empresa fornecedora: [SYSTEM MANAGER TECNOLOGIA LTDA]<br><br>[PAE] [2584/2022] (planejamento)<br><br>[PAE] [11836/2022] (seleção do fornecedor) e (gestão do contrato) | Em andamento |
| Art. 11, VII | .concluir a aquisição, treinamento e implementação da solução de Controle de Ativos e Patches | COINF | dez/23 | [Implantada]<br><br>Solução adquirida: [IVANTI]<br><br>Empresa fornecedora: [SYSTEM MANAGER TECNOLOGIA LTDA]<br><br>[PAE] [2584/2022] (planejamento)<br><br>[PAE] [11836/2022] (seleção do fornecedor) e (gestão do contrato) | Finalizada |
| Art. 11, VIII | .desenvolvimento de norma com especificação de requisitos específicos de segurança cibernética relacionados com o trabalho remoto | COGESTIC | dez/24 | | Não iniciada |

| CNJ | | | | | |
|---|---|---|---|---|---|
| **RESOLUÇÃO 396** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| Art. 11, VIII | .revisar norma específica de segurança cibernética para o trabalho remoto | | dez/24 | (Portaria n.º 78/2022-GP (Extranet e VPN) | Não iniciada |
| Art. 11, VIII | .concluir aquisição, treinamento e implementação da solução de VDI | COINF | jun/23 | | Finalizada |
| Art. 11, IX | .concluir a aquisição e implantar o uso de tokens que possibilitarão o uso do múltiplo fator de autenticação em novas soluções internas e externas | SRI/SSI | dez/23 | | Finalizada |
| Art. 11, X | .implantar a realização de testes de conformidade em segurança cibernética com uso de ferramentas de monitoramento como por exemplo, TENABLE.SC, TENABLE.AD e Endpoint | SRI/SSI | jun/23 | | Finalizada |
| Art. 19, I | .aprovar Plano de Trabalho de Segurança da informação (anexo ao PDTIC) | COGESTIC | dez/23 | | Finalizada |
| Art. 19, II | .revisar a Política de Segurança da Informação do TRE/RN (Resolução n.º 20/2019) | SSI e GAPSTIE | dez/23 | Normas de referência<br>CNJ - ENSEC-PJ<br><br>TSE - PSI (Res. TSE n.º 23.644/2021) | Finalizada |
| Art. 19, III<br>Art. 31 | .aprovar o Plano de Contratações e Soluções de TIC 2024 (anexo ao PDTIC 2024) | COGESTIC | dez/23 | | Finalizada |
| Art. 19, IV | .aprovar o Plano de Capacitação de TIC 2024 (anexo ao PDTIC) com ações de treinamento voltadas para SI e ferramentas de SI adquiridas pelo TRE | COGESTIC | dez/23 | | Finalizada |

| CNJ | | | | | |
|---|---|---|---|---|---|
| **RESOLUÇÃO 396** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| Art. 19, IV | .aplicação e uso da Plataforma de Educação e Conscientização em Segurança da Informação, com simulação de Phishings | SSI | dez/23 | **[KNOWBE4]**<br>[Plataforma de Conscientização em SI]<br>[Contrato nº 46/2022]<br>[QUALITEK TECNOLOGIA]<br><br>[PAE] [2585/2022] (planejamento)<br><br>[PAE] [2359/2022] (consulta sobre interesse em participar da contratação de solução para conscientização e capacitação em Cibersegurança)<br><br>[PAE] [6498/2022] (adesão a ARP TRE-ES nº 04/2022) e (seleção do fornecedor)<br><br>[PAE] [10424/2022] (gestão do contrato)<br><br>ver incisos:<br>- 3.2.2 Anexo I<br>- 5.1 Anexo IV<br>- 5.2 Anexo IV<br>- 6.1 Anexo IV<br>- 0.2 Anexo V | Finalizada |
| Art. 19, IV | Elaboração de projeto de evento institucional sobre Segurança da Informação e Cibernética | CPSI | mar/23 | [em andamento]<br>Plano de Ação da CPSI | Finalizada |
| Art. 20 | .revisar os componentes da Comissão Permanente de Segurança da Informação (CPSI) | PRES | jun/23 | | Finalizada |
| Art. 26 | .aprovar Plano de Trabalho de Segurança da Informação para implementação dos protocolos e manuais aprovados na Portaria CNJ n.º 162/2021 | STIE | dez/23 | | Finalizada |
| Art. 26 | .adotar e seguir o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ) | SSI | ago/23 | | Finalizada |
| Art. 26 | .adotar e seguir o Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ) | SSI | ago/23 | | Finalizada |
| Art. 26 | .adotar e seguir o Protocolo de Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ) | SSI | ago/23 | | Finalizada |

| CNJ | | | | | |
|---|---|---|---|---|---|
| **RESOLUÇÃO 396** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| Art. 28, I | elaborar norma de Gestão de Ativos | SSI | jun/23 | | Finalizada |
| Art. 28, I | .elaborar norma de Controle de Acesso | SRI | jun/23 | Na ENSEC PJ, determina a política de Gestão de Usuários que inclua:<br>Gerenciamento de Identidades<br>Gerenciamento de Acessos<br>Gerenciamento de Privilégios<br><br>Revisão da Portaria 45/2018 - GP - Acesso a serviços e sistemas<br>Revisão da Portaria 78/2022-GP - Acesso remoto - Extranet e VPN<br>Revisão da Portaria 219/2017 - GP - Acesso à Internet<br>Revisão da Portaria 99/2015-GP - Acesso à rede sem fio | Finalizada |
| Art. 28, II | .revisar a Política de Segurança da Informação e incluir ações de controle e restrição de acesso | SSI e GAPSTIE | dez/23 | | Finalizada |
| Art. 28, III | .incluir no plano de capacitação treinamentos na área de Segurança da Informação com certificação internacional | COGESTIC | dez/24 | | Não iniciada |
| Art. 28, IV | .estabelecer requisitos de segurança cibernética nas contratações | COGESTIC | dez/23 | | Finalizada |
| Art. 28, IV | .incluir contratações específicas de Segurança da Informação no Plano de Contratações de TIC | COGESTIC | dez/23 | | Finalizada |
| Art. 28, V | .ampliar o número de soluções que utilizam o certificado digital ou mecanismos de múltiplos fatores de autenticação | COINF e COSIS | dez/23 | **[WAF]**<br>**[F5 BIGFIX]**<br>[Solução de Firewall Camada 7 para proteção Aplicações WEB (WAF - Web Application Firewall)<br>[NTSEC SOLUÇÕES EM TELEINFORMÁTICA]<br>[PAE] [7596/2022] (planejamento)<br><br>[PAE] [6524/2022] (adesão a ARP TRE-PA nº 91/2022) e (seleção do fornecedor) | Finalizada |

| CNJ | | | | | |
|---|---|---|---|---|---|
| **RESOLUÇÃO 396** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| Art. 29 | .aprovar normativo de gestão de acessos e permissões | COGESTIC | dez/24 | | Não iniciada |
| Art. 29 | .concluir treinamento e implementação da solução de Cofre de Senhas | COINF e COSIS | jun/23 | **[*BEYOUNDTRUST*]**<br><br>Empresa fornecedora: [*SEVEN SECURE* TECNOLOGIA DA INFORMAÇÃO LTDA]<br><br>[PAE] [2586/2022] (Planejamento)<br><br>[PAE] [4956/2022] (Adesão ARP TSE 02/2022) | Finalizada |
| Art. 30 | .adesão à PCESC-PJ (Portaria CNJ 162/2021 - VII) ( aprovar Plano de Trabalho de Segurança da informação) | COGESTIC | dez/22 | | Finalizada |
| Art.36 | .revisar o Plano de Continuidade de Serviços Essenciais | STIE | jun/23 | - Portaria n.º177/2019-GP - Institui a Gestão da Continuidade de Serviços Essenciais de Tecnologia da Informação e Comunicação - TIC<br><br>- Portaria n.º 191/2019 - GP - Institui os processos de Gerenciamento dos Acordos de Nível de Serviços Essenciais de TIC e de Monitoramento e Aferição dos Acordos de Nível de Serviços Essenciais de TIC, no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte | Finalizada |
| Art.37 | .elaborar Plano de Gestão de Riscos de TIC, alinhado ao Plano Institucional de Gestão de Riscos | STIE | jun/24 | | Não iniciada |
| | | | | | Não iniciada |

| TSE | | | | | |
|---|---|---|---|---|---|
| **RESOLUÇÃO 23.644** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| Art.9º, I | .revisar a Política de Segurança da Informação do TRE/RN (Resolução n.º 20/2019) | SSI e GAPSTIE | jun/23 | Revisada | Finalizada |
| Art.9º, I | .revisar a Política de Segurança da Informação do TRE/RN (Resolução n.º 20/2019) | SSI e GAPSTIE | jun/23 | Revisada | Finalizada |
| Art.9º, II, a | .elaborar minuta de norma com regramento e processo relacionado à Gestão de Ativos | SSI e GAPSTIE | jun/23 | | Finalizada |
| Art.9º, II, b | .elaborar minuta de norma com regramento e processo relacionado à Controle de Acesso Físico e Lógico | SRI e NS | jun/23 | | Finalizada |
| Art.9º, II, c | .Elaborar minuta de norma com regramento e processo relacionado à Gestão de Riscos de Segurança da Informação | SSI e GAPSTIE | dez/23 | | Finalizada |
| Art.9º, II, d | .elaborar minuta de norma com regramento e processo relacionado à Uso Aceitável de Recursos de TI | SRI | dez/23 | | Finalizada |
| Art.9º, II, e | .elaborar minuta de norma com regramento e processo relacionado à Geração e Restauração de Cópias de Segurança (backup) | SRI | dez/23 | | Finalizada |
| Art.9º, II, e | .revisar a Portaria n.º 130/2017 - GP, que instituiu a Política de Backup | SRI | dez/23 | | Finalizada |
| Art.9º, II, f | .revisar a Portaria n.º 177/2019-GP, que instituiu a gestão da continuidade de serviços essenciais de TIC, no TRE/RN | COINF e COSIS | jun/23 | | Finalizada |
| Art.9º, II, f | .revisar o Plano de Continuidade de Serviços Essenciais de TI | COINF e COSIS | dez/23 | Revisado | Finalizada |
| Art.9º, II, g | .Elaborar processo relacionado à Gestão de Incidentes de Segurança da Informação | SSI | jun/23 | | Finalizada |
| Art.9º, II, h | .elaborar minuta de norma relacionado à Gestão de Vulnerabilidades e Padrões de Configuração Segura | SSI | dez/23 | | Finalizada |
| Art.9º, II, i | .elaborar minuta de norma com regramento à Gestão e Monitoramento de Registros de Atividade (logs) | SSI | dez/23 | | Finalizada |
| Art.9º, II, j | .elaborar minuta de norma com regramento e processo relacionado ao desenvolvimento seguro de sistemas | COSIS | jun/23 | | Finalizada |

# PLANO DE TRABALHO DE SEGURANÇA DA INFORMAÇÃO

IMPLEMENTAÇÃO DA RESOLUÇÃO 396 CNJ; RESOLUÇÃO 23.644 TSE E DOS PROTOCOLOS E MANUAIS APROVADOS NA PORTARIA Nº 162/2021-CNJ.

| TSE | | | | | |
|---|---|---|---|---|---|
| **RESOLUÇÃO 23.644** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| Art.9º, II, j | .revisar a Portaria n.º 187/2019-GP, que institui a gestão do desenvolvimento, sustentação e implantação de sistemas no âmbito do TRE/RN | COSIS | dez/2 | | Não iniciada |
| Art.9º, III | .criar base de conhecimento específica de segurança da informação | SSI | dez/24 | | Em andamento |
| Art.10 | .revisar a Resolução TRE/RN nº 008/2009 - Institui a Comissão Permanente de Segurança da Informação | GAPSTIE | jun/23 | | Finalizada |
| Art.10, § 2º | .providenciar a assinatura do Termo de Sigilo de todos os servidores que compõem a CPSI | Presidente da CPSI | jun/24 | | Não iniciada |
| Art.13 | .revisar a Portaria n.º 045/2017 DG - Designa o Gestor de Segurança da Informação | GAPSTIE e GABPRES | dez/24 | | Não iniciada |
| Art.14 | .revisar a norma que institui a ETIR, de acordo com a ENSEC_PJ e PSI do TSE | CPSI | jun/23 | [Revisada]<br><br>.Portaria n.º423/2017-GP - Institui a Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais (ETIR)<br><br>.Portaria n.º 127/2020 - GP - Altera a Portaria n.º 423/2017-GP, que institui a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) no âmbito do TRE-RN | Finalizada |
| Art.14, § 1º \| | ..elaborar o Plano de Gestão e Resposta a Incidentes Cibernéticos | ETIR | jun/23 | | Finalizada |
| Art.22 | .Revisar a Política de Segurança da Informação do TRE/RN (Resolução n.º 20/2019) a luz da PSI do TSE (Res. 23644/2021) | SSI e GAPSTIE | jun/23 | [Revisada] | Finalizada |
| Art.27 | .dar ciência e exigir cumprimento da PSI junto aos celebrantes de contratos e convênios | gestores de contrato de TIC | | | Ação Contínua |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **PROTOCOLO DE INCIDENTES CIBERNÉTICOS DO PODER JUDICIÁRIO - PPINC-PJ (ANEXO I)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 2.1.1 | .identificar os Serviços Essenciais de TICma | STIE | ago/23 | .instituído a Gestão da Continuidade dos Serviços Essenciais de TIC no âmbito do TRE-RN, através da Portaria nº 177/2019 - GP<br><br>.Revisar o Mapeamento do processo de Gerenciamento de Continuidade de Serviços Essenciais de TIC | Finalizada |
| 2.1.3 | .consolidar o uso das ferramentas de Cibersegurança adquiridas pelo TRE de acordo com a indicação de criticidade estabelecida pelo grupo nacional de segurança | STIE | jun/23 | | Finalizada |
| 2.1.4 | .elaborar o Plano de Gestão e Resposta a Incidentes Cibernéticos | SSI e ETIR | ago/23 | | Finalizada |
| 2.1.4 | .elaborar o Plano de Comunicação de Cibersegurança | DG e STIE | dez/24 | | Não iniciada |
| 2.1.4 | .elaborar o Plano de Mitigação | SSI | dez/24 | | Não iniciada |
| 2.1.5 | .elaborar o Plano de Restauração | ETIR | jun/25 | | Não iniciada |
| 3.2.1 | .criar a Base de Conhecimento de Defesa | ETIR | jun/24 | | Não iniciada |

# CRONOGRAMA

| **PORTARIA Nº 162/2021-CNJ** | | | | | |
|---|---|---|---|---|---|
| **PROTOCOLO DE INCIDENTES CIBERNÉTICOS DO PODER JUDICIÁRIO - PPINC-PJ (ANEXO I)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 3.2.2 | .capacitar as equipes técnicas sobre segurança cibernética | EJE e STIE | jun/22 | Ação contínua de capacitação e ações de conscientização<br><br>**[CIBER JE]**<br>**[Repasse tecnológico da solução]**<br><br>**1.[TREND]**<br>[Antivírus] [Contrato de aquisição de unidades de subscrições de Solução de Segurança para Servidores]<br><br>[Contrato nº 46/2022]<br>[DFTI - Comércio e Serviços de Informática Ltda]<br><br>[PAE] [1397/2022] (planejamento)<br><br>[PAE] [2865/2022] (seleção do fornecedor)<br><br>[PAE] [4107/2022] (gestão do contrato)<br><br>**2.[KNOWBE4]**<br>[Plataforma de Conscientização em SI]<br><br>[Contrato nº 46/2022]<br>[QUALITEK TECNOLOGIA]<br><br>[PAE] [2585/2022] (planejamento)<br><br>[PAE] [2359/2022] | Finalizada |

| | | | | | |
|---|---|---|---|---|---|
| | | | | (consulta sobre interesse em participar da contratação de solução para conscientização e capacitação em Cibersegurança)<br><br>[PAE] [6498/2022] (adesão a ARP TRE-ES nº 04/2022) e (seleção do fornecedor)<br><br>[PAE] [10424/2022] (gestão do contrato)<br><br>**3.[IVANTI]**<br>[Gestão de Patches e Ativos]<br><br>[Contrato nº 54/2022] [SYSTEM MANAGER TECNOLOGIA LTDA]<br><br>[PAE] [2584/2022] (planejamento)<br><br>[PAE] [11836/2022] (seleção do fornecedor) e (gestão do contrato)<br><br>**4.[TENABLE AD]**<br>[Solução de Auditoria e Segurança para o AD (Active Directory)<br>[Contrato de solução unificada de Auditoria de Segurança no Active Directory]<br>[Contrato nº 55/2022]<br>[SERVIX Informática Ltda]<br><br>[PAE] [7595/2022] (planejamento)<br><br>[PAE] [3786/2022] (consulta sobre interesse em participar da contratação de solução para conscientização e capacitação em Cibersegurança) e (seleção do fornecedor)<br><br>**5.[BEYOUNDTRUST]**<br>[Solução de Gerenciamento de Acessos Privilegiados para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos)]<br><br>[Contrato nº 33/2022] [SEVEN SECURE TECNOLOGIA DA INFORMAÇÃO LTDA] | |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **PROTOCOLO DE INCIDENTES CIBERNÉTICOS DO PODER JUDICIÁRIO - PPINC-PJ (ANEXO I)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 3.2.2 | .disseminar a cultura sobre segurança cibernética | EJE e STIE | jun/22 | Ação contínua de capacitação e ações de conscientização<br><br>**[KNOWBE4] [Plataforma de Conscientização em SI] :**<br><br>.Criação de campanhas de PHISHING<br>.Criação de treinamentos sobre Segurança da Informação | Finalizada |
| 3.2.4 | .revisar indicadores de Segurança da Informação | SSI | dez/24 | | Não iniciada |
| 3.2.5 | .incluir no Plano de Capacitação institucional, ações voltadas para segurança cibernética | EJE e STIE | dez/22 | Ação contínua de capacitação e ações de conscientização | Finalizada |
| 3.2.5 | .revisar, periodicamente, os instrumentos de formação, capacitação e conscientização, utilizados dentro da organização | EJE e STIE | Ação Contínua | Ação contínua de capacitação e ações de conscientização | Finalizada |
| 3.2.6 | .implementar soluções automatizadas de segurança cibernética, visando medições confiáveis, escaláveis e contínuas | STIE | Ação Contínua | Ação contínua (Plano de Contratações) | Finalizada |
| 3.2.6 | .priorizar as soluções automatizadas de segurança cibernética a serem adquiridas | STIE | dez/22 | [PAE 9236/2021] Estratégia Nacional de Cibersegurança | Finalizada |
| 3.2.7 | .elaborar o Plano de Resiliência | ETIR | dez/24 | | Não iniciada |
| 4.1 | .mapear o processo de Gestão de Incidentes de Segurança | SSI | jun/23 | | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **PROTOCOLO DE INCIDENTES CIBERNÉTICOS DO PODER JUDICIÁRIO - PPINC-PJ (ANEXO I)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 5.1 | .instituir a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) | STIE | dez/22 | | Finalizada |
| 6.1 | .publicar no sítio eletrônico do órgão o funcionamento da ETIR, regulado por documento formal de constituição, devendo constar, no mínimo, os seguintes pontos:<br>a) definição da missão;<br>b) público-alvo;<br>c) modelo de implementação;<br>d) nível de autonomia;<br>e) designação de integrantes;<br>f) canal de comunicação de incidentes de segurança; e<br>g) serviços prestados. | ETIR | jul/22 | Revisar ETIR | Finalizada |
| 7.2 | .instituir a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) | ETIR | dez/22 | Revisar ETIR | Finalizada |
| 7.5.1 | .elaborar o Plano de Gestão e Resposta a Incidentes Cibernéticos | SSI e ETIR | ago/23 | ver incisos:<br>- 2.1.4 Anexo I<br>- 7.5.2 Anexo I<br>- 7.5.3 Anexo I<br>- 7.5.4 Anexo I<br>- 7.5.5 Anexo I<br>- 3.5.1 Anexo V | Finalizada |
| 7.5.2 | .elaborar o Plano de Gestão e Resposta a Incidentes Cibernéticos | SSI e ETIR | ago/23 | ver incisos:<br>- 2.1.4 Anexo I<br>- 7.5.2 Anexo I<br>- 7.5.3 Anexo I<br>- 7.5.4 Anexo I<br>- 7.5.5 Anexo I<br>- 3.5.1 Anexo V | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **PROTOCOLO DE INCIDENTES CIBERNÉTICOS DO PODER JUDICIÁRIO - PPINC-PJ (ANEXO I)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 7.5.3 | .elaborar o Plano de Gestão e Resposta a Incidentes Cibernéticos | SSI e ETIR | ago/23 | ver incisos:<br>- 2.1.4 Anexo I<br>- 7.5.2 Anexo I<br>- 7.5.3 Anexo I<br>- 7.5.4 Anexo I<br>- 7.5.5 Anexo I<br>- 3.5.1 Anexo V | Finalizada |
| 7.5.4 | .elaborar o Plano de Gestão e Resposta a Incidentes Cibernéticos | SSI e ETIR | ago/23 | ver incisos:<br>- 2.1.4 Anexo I<br>- 7.5.2 Anexo I<br>- 7.5.3 Anexo I<br>- 7.5.4 Anexo I<br>- 7.5.5 Anexo I<br>- 3.5.1 Anexo V | Finalizada |
| 7.5.5 | .elaborar o Plano de Gestão e Resposta a Incidentes Cibernéticos | SSI e ETIR | ago/23 | ver incisos:<br>- 2.1.4 Anexo I<br>- 7.5.2 Anexo I<br>- 7.5.3 Anexo I<br>- 7.5.4 Anexo I<br>- 7.5.5 Anexo I<br>- 3.5.1 Anexo V | Finalizada |
| 7.5.6 | .participar dos grupos locais e nacionais de identificação e resposta a ataques cibernéticos do Poder Judiciário | .participar dos grupos locais e nacionais de identificação e resposta a ataques cibernéticos do Poder Judiciário | jul/23 | GRUPO NACIONAL DE SEGURANÇA, GRUPOS DE SEGURANÇA CIBERNÉTICA JE E JF WHATSAPP | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **PROTOCOLO DE GERENCIAMENTO DE CRISES CIBERNÉTICAS DO PODER JUDICIÁRIO - PGCRC-PJ (ANEXO II)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 4.1 | .aprovar o Plano de Trabalho de Segurança da Informação e Proteção de Dados com cronograma de atividades em protocolo específico de Segurança Cibernética | COGESTIC | ago/23 | | Finalizada |
| 4.2 | .definir a Sala de Situação | STIE e DG | dez/24 | | Não iniciada |
| 4.2 | .criar um Comitê de Crises Cibernéticas | STIE e DG | dez/24 | | Não iniciada |
| 4.3 | .elaborar o Plano de Gestão e Resposta a Incidentes Cibernéticos | SSI e ETIR | dez/24 | o Plano de Gestão de Incidentes Cibernéticos onde deverá possuir, no mínimo:<br>- as categorias de incidentes a que os ativos críticos estão sujeitos<br>- a indicação do procedimento de resposta específico a ser aplicado em caso de ocorrência do incidente<br>- a severidade do incidente<br><br>ver incisos:<br>- 2.1.4 Anexo I<br>- 7.5.1 Anexo I<br>- 7.5.2 Anexo I<br>- 7.5.3 Anexo I<br>- 7.5.4 Anexo I<br>- 7.5.5 Anexo I<br>- 3.5.1 Anexo V | Não iniciada |
| 5.1 | .implementar o Plano de Comunicação de Cibersegurança | DG e STIE | dez/24 | | Não iniciada |
| 5.3 | .elaborar o Plano de Continuidade dos Serviços Essenciais de TIC (Plano de Contingência) | COINF e COSIS | jun/23 | | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **PROTOCOLO DE GERENCIAMENTO DE CRISES CIBERNÉTICAS DO PODER JUDICIÁRIO - PGCRC-PJ (ANEXO II)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 5.4 | .designar o responsável pela Chefia do Comitê de Crise, profissional indicado pelo Presidente do respectivo órgão do Poder Judiciário, com autoridade e autonomia para tomar decisões sobre conteúdo de comunicação a serem divulgados, bem como delegar atribuições, estabelecer metas e prazos de ações | PRES | dez/24 | | Não iniciada |
| 5.9 | .criar protocolo de comunicação de incidentes graves | DG e STIE | dez/24 | | Não iniciada |
| 6.4 | .elaborar o Relatório de Comunicação de Incidente de Segurança Cibernética, que contenha a descrição e o detalhamento da crise e o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados | Comitê de Crise Cibernética | sob demanda | | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **PROTOCOLO DE INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS DO PODER JUDICIÁRIO - PIILC-PJ (ANEXO III)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 1.1 | .estabelecer os procedimentos básicos para coleta e preservação de evidências | ETIR | ago/23 | | Finalizada |
| 1.1 | .estabelecer os procedimentos básicos para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal | PRES, DG e STIE | dez/24 | | Não iniciada |
| 2.1 | .sincronizar o relógio interno dos ativos de tecnologia da informação, conforme a Hora Legal Brasileira (HLB), de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON), de forma a garantir as configurações de:<br>- data<br>- hora<br>- fuso horário | SRI | jun/22 | | Finalizada |
| 2.3 | .mapear o processo de Gerenciamento e Monitoramento de Logs | SRI | dez/24 | | Não iniciada |
| 2.5 | .aquisição de solução de *WAF (Web Application Firewall)* para atender a necessidade de proteção do perímetro das aplicações do TRE/RN, do ambiente de Rede do Tribunal<br>[F5 BIGFIX]<br>Solução de Firewall Camada 7 para proteção Aplicações WEB (WAF - Web Application Firewall)<br>[NTSEC SOLUÇÕES EM TELEINFORMÁTICA] | STIE | ago/23 | [PAE] [7596/2022] (planejamento)<br><br>[PAE] [6524/2022] (adesão a ARP TRE-PA nº 91/2022) e (seleção do fornecedor) | Finalizada |

# CRONOGRAMA

| **PORTARIA Nº 162/2021-CNJ** | | | | | |
|---|---|---|---|---|---|
| **PROTOCOLO DE INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS DO PODER JUDICIÁRIO - PIILC-PJ (ANEXO III)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 2.5 | .aquisição de solução de Gerenciamento de Acessos Privilegiados (Cofre de Senhas) para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos) | STIE | dez/22 | Solução adquirida: **[*BEYOUNDTRUST*]**<br><br>Empresa fornecedora: [*SEVEN SECURE* TECNOLOGIA DA INFORMAÇÃO LTDA]<br><br>[PAE] [2586/2022] (Planejamento)<br><br>[PAE] [4956/2022] (Adesão ARP TSE 02/2022) | Finalizada |
| 2.5 | .implantação da solução de *WAF (Web Application Firewall)* | SRI | jun/24 | | Finalizada |
| 2.5 | .implantação da solução de Gerenciamento de Acessos Privilegiados (Cofre de Senhas) para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos) | SRI | jun/23 | [Implantada]<br><br>**[*BEYOUNDTRUST*]**<br><br>Empresa fornecedora: [*SEVEN SECURE* TECNOLOGIA DA INFORMAÇÃO LTDA]<br><br>[PAE] [2586/2022] (Planejamento)<br><br>[PAE] [4956/2022] (Adesão ARP TSE 02/2022) | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **PROTOCOLO DE INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS DO PODER JUDICIÁRIO - PIILC-PJ (ANEXO III)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 2.8 | Implantar ferramenta de Gestão de Patches e Ativos | SRI e SSI | jun/23 | [Implantada]<br><br>Solução adquirida:<br>**[IVANTI]**<br><br>Empresa fornecedora:<br>[SYSTEM MANAGER TECNOLOGIA LTDA]<br><br>[PAE] [2584/2022] (planejamento)<br><br>[PAE] [11836/2022] (seleção do fornecedor) e (gestão do contrato) | Finalizada |
| 3.1 | .estabelecer os procedimentos básicos para coleta e preservação de evidências durante o processo de tratamento do incidente penalmente relevante, onde deverá, sem prejuízo de outras ações, coletar e preservar:<br>a) as mídias de armazenamento dos dispositivos afetados ou as suas respectivas imagens forenses;<br>b) os dados voláteis armazenados nos dispositivos computacionais, como a memória principal (memória RAM); e<br>c) todos os registros de eventos citados neste documento | ETIR | ago/23 | ver inciso:<br>- 1.1 Anexo III | Finalizada |
| 3.2 | .estabelecer os procedimentos básicos para coleta e preservação de evidências 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, 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 | ETIR | ago/23 | ver incisos:<br>- 1.1 Anexo III<br>- 2.3 Anexo III | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **PROTOCOLO DE INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS DO PODER JUDICIÁRIO - PIILC-PJ (ANEXO III)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 3.5 | .estabelecer nos procedimentos básicos de preservação de evidências ações que visem preservar os arquivos coletados, devendo-se:<br>a) gerar arquivo que contenha a lista dos resumos criptográficos de todos os arquivos coletados<br>b) gravar os arquivos coletados, acompanhados do arquivo com a lista dos resumos criptográficos descritos na alínea a deste subitem; e<br>c) gerar resumo criptográfico do arquivo a que se refere a deste subitem" | ETIR | ago/23 | ver inciso:<br>- 1.1 Anexo III | Finalizada |
| 3.6 | .estabelecer os procedimentos básicos para coleta de evidências durante o processo de tratamento do incidente penalmente relevante, onde todo material coletado deverá ser lacrado e custodiado pelo agente responsável pela ETIR, o qual deverá preencher Termo de Custódia dos Ativos de Informação | ETIR | ago/23 | | Finalizada |
| 3.7 | .estabelecer os procedimentos básicos para coleta de evidências onde o material coletado deverá ficar à disposição da autoridade responsável pelo órgão do Poder Judiciário competente | ETIR | ago/23 | | Finalizada |
| 4.1 | .estabelecer os procedimentos básicos para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal | PRES, DG e STIE | dez/24 | | Não iniciada |
| 4.3 | .estabelecer os procedimentos básicos para elaboração do Relatório de Comunicação de Incidente de Segurança Cibernética, descrevendo detalhadamente os eventos verificados, após a conclusão do processo de coleta e preservação das evidências do incidente penalmente relevante | ETIR | dez/24 | | Em andamento |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **PROTOCOLO DE INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS DO PODER JUDICIÁRIO - PIILC-PJ (ANEXO III)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 4.4 | .estabelecer os procedimentos básicos para a elaboração do Relatório de Comunicação de Incidente de Segurança Cibernética, descrevendo detalhadamente os eventos verificados, após a conclusão do processo de coleta e preservação das evidências do incidente penalmente relevante, contendo as seguintes informações, sem prejuízo de outras julgadas relevantes:<br>a) nome do responsável pela preservação dos dados do incidente, com informações<br>de contato;<br>b) nome do agente responsável pela ETIR e informações de contato;<br>c) órgão comunicante com sua localização e informações de contato;<br>d) número de controle da ocorrência;<br>e) relato sobre o incidente que descreva o que ocorreu, como foi detectado e quais<br>dados foram coletados e preservados;<br>f) descrição das atividades de tratamento e resposta ao incidente e todas as<br>providências tomadas pela ETIR, incluindo as ações de preservação e coleta, a<br>metodologia e as ferramentas utilizadas e o local de armazenamento das informações<br>preservadas;<br>g) resumo criptográfico dos arquivos coletados;<br>h) Termo de Custódia dos Ativos de Informação Relacionados ao Incidente de<br>Segurança;<br>i) número de lacre de material físico preservado, se houver; e<br>j) justificativa sobre a eventual inviabilidade de preservação das mídias de<br>armazenamento dos dispositivos afetados, diante da impossibilidade de mantê-las. | ETIR | dez/24 | | Em andamento |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **PROTOCOLO DE INVESTIGAÇÃO PARA ILÍCITOS CIBERNÉTICOS DO PODER JUDICIÁRIO - PIILC-PJ (ANEXO III)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 4.5 | .estabelecer os procedimentos básicos para a elaboração do Relatório de Comunicação de Incidente de Segurança Cibernética, onde 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 | ETIR | dez/24 | | Em andamento |
| 4.7 | .estabelecer os procedimentos básicos para o encaminhamento formal, pela autoridade responsável pelo órgão do Poder Judiciário, a Comunicação de Incidente de Segurança em Redes Computacionais 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 | PRES | sob demanda | | Não iniciada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS DE TIC (ANEXO IV)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 1.2 | .adotar o Juízo 100% Digital visando viabilizar a execução de todos os atos processuais exclusivamente por meio eletrônico e remoto | DG e STIE | jun/23 | Balcão Virtual | Finalizada |
| 1.3 | .implantar no órgão os padrões mínimos visando a proteção de sua infraestrutura tecnológica | COINF e SSI | jun/23 | adquirir e implantar ferramentas definidas como prioridade 1 pelo grupo nacional de segurança | Finalizada |
| 1.3 | .elaborar norma que trata sobre a Implantação e Gestão de Sistemas com foco na Segurança da Informação | COINF e COSIS | jul/23 | | Finalizada |
| 1.3 | .seguir as orientações organizacionais sobre a sua aplicação e observar a lista de controles mínimos exigidos para implantação dos padrões mínimos visando a proteção de sua infraestrutura tecnológica | COINF e SSI | jun/23 | adquirir e implantar ferramentas definidas como prioridade 1 pelo grupo nacional de segurança | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS DE TIC (ANEXO IV)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 5.1 | Implementar ferramentas de Cyber segurança definidas como prioridade 1 pelo grupo nacional de SI | COINF e COSIS | jun/23 | **[CIBER JE]**<br>**[Contratado e implantado]**<br><br>**1.[TREND]**<br>[Antivírus] [Contrato de aquisição de unidades de subscrições de Solução de Segurança para Servidores]<br><br>[Contrato nº 46/2022]<br>[DFTI - Comércio e Serviços de Informática Ltda]<br><br>[PAE] [1397/2022]<br>(planejamento)<br><br>[PAE] [2865/2022]<br>(seleção do fornecedor)<br><br>[PAE] [4107/2022]<br>(gestão do contrato)<br><br>**2.[KNOWBE4]**<br>[Plataforma de Conscientização em SI]<br><br>[Contrato nº 46/2022]<br>[QUALITEK TECNOLOGIA]<br><br>[PAE] [2585/2022]<br>(planejamento)<br><br>[PAE] [2359/2022]<br>(consulta sobre interesse em participar da contratação de solução para conscientização e capacitação em | Finalizada |

| | | | | | |
|---|---|---|---|---|---|
| | | | | Cibersegurança)<br><br>[PAE] [6498/2022] (adesão a ARP TRE-ES nº 04/2022) e (seleção do fornecedor)<br><br>[PAE] [10424/2022] (gestão do contrato)<br><br>**3.[IVANTI]**<br>[Gestão de Patches e Ativos]<br><br>[Contrato nº 54/2022] [SYSTEM MANAGER TECNOLOGIA LTDA]<br><br>[PAE] [2584/2022] (planejamento)<br><br>[PAE] [11836/2022] (seleção do fornecedor) e (gestão do contrato)<br><br>**4.[TENABLE AD]**<br>[Solução de Auditoria e Segurança para o AD (Active Directory)<br>[Contrato de solução unificada de Auditoria de Segurança no Active Directory]<br><br>[Contrato nº 55/2022] [SERVIX Informática Ltda]<br><br>[PAE] [7595/2022] (planejamento)<br><br>[PAE] [3786/2022] (consulta sobre interesse em participar da contratação de solução para conscientização e capacitação em Cibersegurança) e (seleção do fornecedor)<br><br>**5.[BEYOUNDTRUST]**<br>[Solução de Gerenciamento de Acessos Privilegiados para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos)]<br><br>[Contrato nº 33/2022] [SEVEN SECURE TECNOLOGIA DA INFORMAÇÃO LTDA]<br><br>**[Contratado e não implantado]** | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | **6.[Oracle Database Vault]** [Oracle Advanced Security (TDE+Data Redaction)] Ferramentas de segurança Oracle [AX4B SISTEMAS DE INFORMÁTICA LTDA]<br><br>**[Em processo de contratação]**<br><br>**7.[F5 BIGFIX]** [Solução de Firewall Camada 7 para proteção Aplicações WEB (WAF - Web Application Firewall) [NTSEC SOLUÇÕES EM TELEINFORMÁTICA]<br><br>**[Participe]**<br><br>**8.[Segurança Cibernética] [Prestação de serviços especializados de segurança cibernética para a Justiça Eleitoral]**<br><br>**9.[SIEM] [Gerenciamento de Logs e Eventos]**<br><br>**10.[Gestão de Riscos e LGPD]**<br><br>**11.[Monitoramento de Rede & Theat Intel]**<br><br>[PAE] [3978/2023]<br><br>ver inciso:<br>- 3.2.2 Anexo I | |

# CRONOGRAMA

| **PORTARIA Nº 162/2021-CNJ** | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS DE TIC (ANEXO IV)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 5.2 | .dar ciência sobre as orientações e os controles recomendados a todos os membros do órgão, sejam eles magistrados ou magistradas, servidores ou servidoras, colaboradores ou colaboradoras, fornecedores, prestadores ou prestadoras de serviços, estagiários ou estagiárias que, oficialmente, executem atividades relacionadas ao órgão | STIE | jul/22 | Dar conhecimento da política de segurança da informação do TSE, TRE e outras normas de segurança | Finalizada |
| 5.2 | .promover a divulgação da Política de Segurança da Informação, bem como ações para disseminar a cultura em segurança da informação | CPSI divulgar a PSI após a revisão | | Ação contínua de capacitação e ações de conscientização<br><br>**[Informativos mensais]**<br><br>**[KNOWBE4] [Plataforma de Conscientização em SI]** :<br><br>.Criação de campanhas de PHISHING<br>.Criação de treinamentos sobre Segurança da Informação<br><br>ver inciso:<br>- 3.2.2 Anexo I | Ação Contínua |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS DE TIC (ANEXO IV)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 5.2 | Implantar a solução de Plataforma de Educação e Conscientização em Segurança da Informação, com simulação de Phishings | NEAD e STIE | jun/23 | **[CIBER JE]**<br>**[Contratado e implantado]**<br><br>**[KNOWBE4]**<br>**[Plataforma de Conscientização em SI]**<br><br>[Contrato nº 46/2022]<br>[QUALITEK TECNOLOGIA]<br><br>[PAE] [2585/2022] (planejamento)<br><br>[PAE] [2359/2022] (consulta sobre interesse em participar da contratação de solução para conscientização e capacitação em Cibersegurança)<br><br>[PAE] [6498/2022] (adesão a ARP TRE-ES nº 04/2022) e (seleção do fornecedor)<br><br>[PAE] [10424/2022] (gestão do contrato)<br><br>ver incisos:<br>- 3.2.2 Anexo I<br>- 5.1 Anexo IV | Finalizada |

# CRONOGRAMA

| **PORTARIA Nº 162/2021-CNJ** | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS DE TIC (ANEXO IV)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 5.3 | .criar a base mínima para a proteção de infraestruturas críticas de TI | STIE | jun/23 | Estabelecer a estrutura mínima de proteção e monitoramento para *hardware* e *software* (soluções com criticidade 1) | Finalizada |
| 6.1 | .instituir a nova Política de Segurança da Informação (PSI) no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte, observando como princípios norteadores a Eficiência, Ética, Impessoalidade, Legalidade, Moralidade e Publicidade | CPSI revisar PSI | jul/23 | [Instituída] TRE-RN Resolução n.º 20, de 11 de setembro de 2019 | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS DE TIC (ANEXO IV)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 6.1 | .promover a divulgação da Política de Segurança da Informação, bem como ações para disseminar a cultura em segurança da informação | CPSI divulgar após aprovação | | TRE-RN Resolução n.º 20, de 11 de setembro de 2019<br><br>[CIBER JE]<br>[Contratado e implantado]<br><br>KNOWBE4]<br>[Plataforma de Conscientização em SI]<br><br>[Contrato nº 46/2022]<br>[QUALITEK TECNOLOGIA]<br><br>[PAE] [2585/2022]<br>(planejamento)<br><br>[PAE] [2359/2022]<br>(consulta sobre interesse em participar da contratação de solução para conscientização e capacitação em Cibersegurança)<br><br>[PAE] [6498/2022]<br>(adesão a ARP TRE-ES nº 04/2022) e (seleção do fornecedor)<br><br>[PAE] [10424/2022]<br>(gestão do contrato)<br><br>ver incisos:<br>- 3.2.2 Anexo I<br>- 5.1 Anexo IV | Ação Contínua |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS DE TIC (ANEXO IV)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 7.1 | .implementar as soluções indicadas pelo grupo nacional de segurança cibernética como prioridade 1 para manter uma estrutura mínima de SI compatível com os outros TREs | STIE | jun/23 | | Finalizada |
| 7.2 | .Implementar solução de E-mail com proteção de dados e backup | SRI | dez/22 | ver Inciso:<br>- 5.3 Anexo IV | Finalizada |
| 7.2 | .implementar Solução de Backup | | dez/21 | | Finalizada |
| 7.3 | .implementar Solução de Endpoint | SSI | dez/23 | **[CIBER JE]**<br>**[Contratado e implantado]**<br><br>1.[TREND]<br>[Antivírus] [Contrato de aquisição de unidades de subscrições de Solução de Segurança para Servidores]<br><br>[Contrato nº 46/2022]<br>[DFTI - Comércio e Serviços de Informática Ltda]<br><br>[PAE] [1397/2022]<br>(planejamento)<br><br>[PAE] [2865/2022]<br>(seleção do fornecedor)<br><br>[PAE] [4107/2022]<br>(gestão do contrato)<br><br>ver inciso:<br>- 3.2.2 Anexo I<br>- 5.1 Anexo IV | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS DE TIC (ANEXO IV)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 7.4 | .direcionar e priorizar os esforços de segurança da informação a serem operacionalizados, conforme a sugestão de ordem de implantação, pela classificação por grupos, observando a sua aplicabilidade e aderência sempre validadas\adequadas para o contexto da organização | STIE | jun/22 | Criar lista de prioridades na implantação de soluções de cibersegurança (soluções com criticidade 1) | Finalizada |
| 7.6 | .estruturar a Gestão da Segurança da Informação, no âmbito do TRE/RN | STIE | jun/22 | Resolução TRE/RN n. 12/2014 | Finalizada |
| 7.7 | .aplicar checklists, periodicamente (anualmente, pelo menos), buscando a adequação do TRE/RN ao atendimento dos requisitos mínimos estabelecidos pelo grupo nacional de segurança direcionado pelo TSE, que esses checklists tenham níveis de atendimento/maturidade, possibilitando a melhoria contínua da segurança digital de cada órgão | SSI | Ação Contínua | | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL (ANEXO V)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 0.1 | .aprovar no plano de segurança um manual de referência para PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL, em conformidade com o Comitê Gestor de Segurança Cibernética do Poder Judiciário (CGSCPJ) | STIE | jul/23 | | Finalizada |
| 0.2 | .orientar quanto a aplicação das melhores práticas de Segurança da informação | DG, STIE e EJE | dez/22 Ação contínua | [Ação contínua de capacitação e ações de conscientização]<br><br>[Informativos mensais]<br><br>[KNOWBE4] [Plataforma de Conscientização em SI] :<br><br>.Criação de campanhas de PHISHING<br>.Criação de treinamentos sobre Segurança da Informação<br><br>ver inciso:<br>- 3.2.2 Anexo I | Finalizada |
| 3.1 | .revisar o Sistema de Gerenciamento de Segurança da Informação (SGSI) | CPSI | dez/24 | | Não iniciada |
| 4.1 | .revisar o Sistema de Gerenciamento de Segurança da Informação (SGSI) | CPSI | dez/24 | | Não iniciada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL (ANEXO V)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 5.1 | .mapear o processo de Gestão de Riscos de Segurança da Informação | SSI | jun/23 | [Mapeado]<br><br>Portal da Transparência: https://www.tre-rn.jus.br/transparencia-e-prestacao-de-contas/governanca-e-gestao-de-tic/processos/processos | Finalizada |
| 7.1 | .elaborar o Programa de Auditoria de sistema de gestão da segurança da informação | AUDI | dez/24 | | Não iniciada |
| 11.1 | .elaborar Política de Gestão de Riscos institucional | AGE | dez/24 | | Finalizada |
| 11.4 | .revisar o Processo de Gestão de Riscos de Segurança da Informação, observando-se as diretrizes fornecidas pela Associação Brasileira de Normas Técnicas (ABNT) | SSI | jun/23 | | Finalizada |
| 12.1 | .elaborar a Política Gestão de Riscos de Segurança da Informação, observando-se os seguintes princípios:<br>a) Proteção dos valores organizacionais;<br>b) Melhoria contínua da organização;<br>c) Visão sistêmica;<br>d) Qualidade e tempestividade das informações;<br>e) Abordagem explícita da incerteza;<br>f) Transparência;<br>g) Dinamismo e interatividade;<br>h) Alinhamento à gestão de riscos corporativos;<br>i) Integração. | CPSI | jun/24 | | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL (ANEXO V)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 13.1 | .Mapear o processo de Gestão de Riscos de Segurança da Informação, observando-se as seguintes diretrizes:<br>a) Ser parte integrante dos processos organizacionais de Tecnologia da Informação e Comunicação (TIC);<br>b) Ser parte da tomada de decisões;<br>c) Ser sistemático, estruturado e oportuno;<br>d) Ser baseado nas melhores informações disponíveis;<br>e) Considerar fatores humanos e culturais;<br>f) Ser transparente e inclusivo;<br>g) Ser dinâmico, interativo e capaz de reagir às mudanças tempestivamente;<br>h) Contribuir para a melhoria contínua da organização. | SSI | jun/23 revisado | [Mapeado]<br><br>Portal da Transparência: https://www.tre-rn.jus.br/transparencia-e-prestacao-de-contas/governanca-e-gestao-de-tic/processos/processos | Finalizada |
| 14.1 | .elaborar a Política de Gestão de Riscos de Segurança da Informação, observando-se como objetivos:<br>a) apoiar as unidades organizacionais no que tange aos riscos de segurança da informação em tecnologia da informação da organização;<br>b) aprimorar o processo de tomada de decisão, com o propósito de incorporar a visão de riscos em conformidade com as melhores práticas;<br>c) melhorar a alocação de recursos;<br>d) aprimorar os controles internos;<br>e) alinhar a tolerância a risco à estratégia adotada;<br>f) resguardar a Administração Superior e os demais gestores da organização quanto à tomada de decisão e à prestação de contas;<br>g) identificar, avaliar e reagir às oportunidades e ameaças; e<br>h) melhorar a eficiência operacional por meio do gerenciamento de riscos proativos | CPSI | jun/24 | | Finalizada |
| 15.1 | .estabelecer uma estrutura de gestão de riscos de segurança da informação identificando pelo menos:<br>a) a unidade dirigente de TIC do órgão; e<br>b) os gestores de riscos | CPSI | dez/24 | | Não iniciada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL (ANEXO V)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 15.2 | .elaborar a Política de Gestão de Riscos de Segurança da Informação e definir como gestores de riscos, em seus respectivos âmbitos e escopos de atuação, os titulares das unidades responsáveis pelos serviços | CPSI | dez/24 | | Não iniciada |
| 15.4 | .elaborar a Política de Gestão de Riscos de Segurança da Informação e definir a gestão de riscos de segurança da informação de forma que seja de responsabilidade compartilhada de magistrados e magistradas, servidores e servidoras, estagiários e estagiárias, e prestadores e prestadoras de serviço, embora determinem-se papéis e responsabilidades específicas | CPSI | dez/24 | | Não iniciada |
| 16.1 | .aprovar a Política de Gestão de Riscos de Segurança da Informação e decidir sobre prioridades de atuação | Comitê de Governança de Tecnologia da Informação | dez/24 | | Não iniciada |
| 17.1 | .revisar a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral, observando-se que compete à unidade dirigente de TIC do órgão:<br>I. disseminar a política de gestão de riscos de segurança da informação em suas unidades subordinadas;<br>II. monitorar, avaliar, revisar e propor alterações na política de gestão de riscos de segurança da informação;<br>III. monitorar o tratamento dos riscos; e<br>IV. analisar e encaminhar o Relatório de Riscos de Segurança da Informação não tratados ao CGSI" | STIE | jul/23 | Revisada | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL (ANEXO V)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 18.1 | .revisar Bienalmente a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral, observando-se que compete à unidade responsável pela Gestão de Segurança da Informação de TIC do TRE/RN as seguintes competências:<br>I. propor as atualizações necessárias à presente política;<br>II. monitorar o processo de gestão de riscos de segurança da informação | CPSI | jul/25 | | Finalizada |
| 19.1 | .determinar aos gestores de risco as seguintes competências:<br>I. realizar a escolha dos processos de trabalho que devam ter os riscos gerenciados e tratados, tendo em vista a dimensão dos prejuízos que possam causar | DG e STIE | dez/24 | | Não iniciada |
| 21.1.I | .estabelecimento de inventário de sistemas, serviços e ativos de Tecnologia da Informação e Comunicação do órgão que serão submetidos, periodicamente, à análise de segurança, buscando-se identificar vulnerabilidades técnicas que possam vir a comprometer os dados, os objetivos de negócio e/ou afetar a imagem institucional do órgão | SSI | jun/23 | implementação das ferramentas de análise de vulnerabilidades (tenable) e de inventário Ivanti) | Finalizada |
| 22.2 | .indicar servidor da SSI para participar de grupo nacional de segurança da informação | SSI | jun/22 | | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL (ANEXO V)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 26.1 | .revisar o Plano de Continuidade de Serviços Essenciais de TIC | STIE, COINF e COSIS | jun/23 | Revisado | Finalizada |
| 32.1 | .implantar solução de Gestão de Patches e Ativos | COINF | jun/23 | [Implantada]<br><br>Solução adquirida:<br><br>**[IVANTI]**<br>[Gestão de Patches e Ativos]<br><br>[Contrato nº 54/2022]<br>[SYSTEM MANAGER TECNOLOGIA LTDA]<br><br>[PAE] [2584/2022] (planejamento)<br><br>[PAE] [11836/2022] (seleção do fornecedor) e (gestão do contrato)<br><br>ver incisos:<br>- 2.8 Anexo III<br>- 5.1 Anexo IV | Finalizada |
| 34.1.a | .implantar a solução de Hiper Convergência e Alta Disponibilidade com site de backup em local divergente do datacenter principal | SRI | dez/22 | | Finalizada |

# CRONOGRAMA

| **PORTARIA Nº 162/2021-CNJ** | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL (ANEXO V)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 34.1.b | .implantar a solução de Endpoint | SRI | jun/23 | [CIBER JE]<br>[Contratado e implantado]<br><br>solução adquirida:<br>**[TREND]**<br>[Antivírus] [Contrato de aquisição de unidades de subscrições de Solução de Segurança para Servidores]<br><br>[Contrato nº 46/2022]<br>[DFTI - Comércio e Serviços de Informática Ltda]<br><br>[PAE] [1397/2022] (planejamento)<br><br>[PAE] [2865/2022] (seleção do fornecedor)<br><br>[PAE] [4107/2022] (gestão do contrato) | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL (ANEXO V)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 34.4.f | .implantar as soluções de:<br>- Endpoint<br>- Gestão de Patches e Ativos<br>- Solução de Auditoria e Segurança para o *AD (Active Directory)*<br>- Solução de Gerenciamento de Acessos Privilegiados para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos) | SSI, SRI e SMI | jun/23 | [CIBER JE]<br>[Contratado e implantado]<br><br>**1.[TREND]**<br>[Antivírus] [Contrato de aquisição de unidades de subscrições de Solução de Segurança para Servidores]<br><br>[Contrato nº 46/2022]<br>[DFTI - Comércio e Serviços de Informática Ltda]<br><br>[PAE] [1397/2022] (planejamento)<br><br>[PAE] [2865/2022] (seleção do fornecedor)<br><br>[PAE] [4107/2022] (gestão do contrato)<br><br>**2.[IVANTI]**<br>[Gestão de Patches e Ativos]<br><br>[Contrato nº 54/2022]<br>[SYSTEM MANAGER TECNOLOGIA LTDA]<br><br>[PAE] [2584/2022] (planejamento)<br><br>[PAE] [11836/2022] (seleção do fornecedor) e (gestão do contrato) | Finalizada |

| | | | | | |
|---|---|---|---|---|---|
| | | | | **3.[TENABLE AD]**<br>[Solução de Auditoria e Segurança para o AD (Active Directory)<br>[Contrato de solução unificada de Auditoria de Segurança no Active Directory]<br><br>[Contrato nº 55/2022]<br>[SERVIX Informática Ltda]<br><br>[PAE] [7595/2022] (planejamento)<br><br>[PAE] [3786/2022] (consulta sobre interesse em participar da contratação de solução para conscientização e capacitação em Cibersegurança) e (seleção do fornecedor)<br><br>**4.[BEYOUNDTRUST]**<br>[Solução de Gerenciamento de Acessos Privilegiados para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos)]<br><br>[Contrato nº 33/2022]<br>[SEVEN SECURE TECNOLOGIA DA INFORMAÇÃO LTDA]<br><br>ver incisos: | |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS E CONFIANÇA DIGITAL (ANEXO V)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 34.1.h | ,implementar rotinas de monitoramento com a ferramenta utilizada para a análise de vulnerabilidades (*TENABLE.SC*) | SSI | dez/22 | [Implementada] | Finalizada |
| 34.1.i | ,implementar rotinas de monitoramento com as ferramentas utilizadas para a análise de vulnerabilidades (*TENABLE.SC*), Auditoria e Segurança para o *AD (Active Directory)* (*TENABLE.AD*) e *Endpoint* (*TREND*) | SSI e SRI | dez/23 | [Implementada]<br><br>TENABLE.SC<br>TREND | Finalizada |
| 34.1.f | .mapear o processo de Gerenciamento de Vulnerabilidades | SSI | jun/23 | [Mapeado] | Finalizada |

# CRONOGRAMA

| **PORTARIA Nº 162/2021-CNJ** | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - GESTÃO DE IDENTIDADE E DE CONTROLE DE ACESSOS (ANEXO VI)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 1.1 | .aprovar a criação de Manual de Referência - Gestão de Identidade e de Controle de Acessos | STIE | dez/24 | | Não iniciada |
| 1.2 | .implantar a solução de Gerenciamento de Acessos Privilegiados | COINF e COSIS | jun/23 | [implantada]<br><br>**[BEYOUNDTRUST]**<br>[Solução de Gerenciamento de Acessos Privilegiados para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos)]<br><br>[Contrato nº 33/2022]<br>[SEVEN SECURE TECNOLOGIA DA INFORMAÇÃO LTDA] | Finalizada |
| 1.3 | .definir na Política de Gestão de Identidades e de Controle de Acessos as responsabilidades dos titulares de contas individuais quanto à proteção de suas contas e ao uso adequado de suas autorizações, bem como aos operadores responsáveis pelo Gerenciamento de Identidade e Acesso para sistemas de informação | SSI e SRI | jun/22 | política de acesso | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - GESTÃO DE IDENTIDADE E DE CONTROLE DE ACESSOS (ANEXO VI)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 1.1 | .aprovar a criação de Manual de Referência - Gestão de Identidade e de Controle de Acessos | STIE | dez/24 | | Não iniciada |
| 1.2 | .implantar a solução de Gerenciamento de Acessos Privilegiados | COINF e COSIS | jun/23 | [implantada]<br><br>**[BEYOUNDTRUST]**<br>[Solução de Gerenciamento de Acessos Privilegiados para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos)]<br><br>[Contrato nº 33/2022]<br>[SEVEN SECURE TECNOLOGIA DA INFORMAÇÃO LTDA] | Finalizada |
| 1.3 | .definir na Política de Gestão de Identidades e de Controle de Acessos as responsabilidades dos titulares de contas individuais quanto à proteção de suas contas e ao uso adequado de suas autorizações, bem como aos operadores responsáveis pelo Gerenciamento de Identidade e Acesso para sistemas de informação | SSI e SRI | jun/22 | política de acesso | Finalizada |
| 2.1.1 | .adotar as diretrizes de práticas recomendadas para segurança cibernética do *Center for Internet Security Critical Security Controls for Effective Cyber Defense20* | STIE | dez/24 | | Não iniciada |
| 2.3.1 | .especificar os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização | STIE | Ação Contínua | Revisar, bianualmente, a estrutura de pessoal do Sistema de Gestão da Segurança da Informação | Ação Contínua |
| 3.1 | .dar publicidade a Política de Gestão de Identidades e de Controle de Acessos | STIE | ago/23 | | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - GESTÃO DE IDENTIDADE E DE CONTROLE DE ACESSOS (ANEXO VI)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 3.2 | .estabelecer, em normativo próprio, o regramento do órgão, considerando as boas práticas de segurança da informação e em observância às seguintes diretrizes:<br>-definição de padrão de identidade do órgão, que contemple, no mínimo, os critérios para padronização de nome de usuário e de conta de e-mail<br>-consideração do princípio de privilégio mínimo e de segregação de funções, visando a evitar acessos indevidos e reduzir os riscos de vazamento de informações;<br>-estabelecimento de processo e de responsáveis por solicitação, gerenciamento e revogação de contas de acesso, preferencialmente de forma automática<br>- utilização de login único para acesso a serviços de diretório corporativo e para acesso aos sistemas, com o objetivo de uniformizar e garantir a experiência única de interação e evitar a criação de contas e autorizações locais<br>-adoção de modelo de controle de acesso, preferencialmente utilizando controle de acesso baseado em funções (RBAC) em que as credenciais recebam os privilégios de acesso conforme os papéis e as responsabilidades executadas pelos usuários<br>-criação de processos de verificação de identidade nas interações entre sistemas, internos ou externos, com vinculação das credenciais aos usuários e às suas autorizações<br>-registro de trilhas de auditoria que vise ao registro dos acessos a sistema de informação, quais operações foram realizadas e em qual período<br>-definição de requisitos de tamanho, reutilização, critérios de complexidade e período de expiração de senhas<br>-empenho pela adoção de múltiplo fator de autenticação<br>-busca pela unificação de plataformas de autenticação, autorização e autenticação (AAA)<br>-estabelecimento de regras quanto ao acesso remoto e forma de disponibilização de sistemas e serviços na internet<br>-gestão de credenciais privilegiadas e restrição ao uso de credenciais genéricas e de uso compartilhado | STIE | jun/22 | política de acesso | Finalizada |

| | | | | | |
|---|---|---|---|---|---|
| | -rastreabilidade de acessos e ações executadas por administradores de TI<br>-utilização de mecanismos seguros de criptografia para o armazenamento e trânsito de credenciais de acesso<br>-segregação de redes conforme o grupo dos serviços, sistemas ou usuários<br>-controle do acesso físico aos ativos de tecnologia da informação e comunicação (TIC)<br>-implementação de controles de acesso proporcionais à classificação da informação<br>-monitoração dos acessos e tentativas de acesso para identificação de ataques | | | | |

# CRONOGRAMA

| **PORTARIA Nº 162/2021-CNJ** | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - GESTÃO DE IDENTIDADE E DE CONTROLE DE ACESSOS (ANEXO VI)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 4.1 | .adotar o método de criação de conta, em um repositório central, com autenticação federada | COINF e COSIS | dez/23 | | Finalizada |
| 4.2 | . remover ou limitar o uso de contas compartilhadas | COINF e COSIS | jun/23 | | Finalizada |
| 4.4 | .limitar o uso de privilégios em contas com autorizações privilegiadas e desencorajar ou vetar o uso direto de contas compartilhadas com privilégios | COINF e COSIS | jun/23 | | Finalizada |
| 6.1 | .revisar a norma de controle de acessos aos sistemas informatizados | SRI | jul/23 | | Finalizada |
| 6.1 | .aquisição de solução de Gerenciamento de Acessos Privilegiados (Cofre de Senhas) para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos) | STIE | dez/22 | Solução adquirida: **[*BEYOUNDTRUST*]**<br><br>Empresa fornecedora: [*SEVEN SECURE* TECNOLOGIA DA INFORMAÇÃO LTDA]<br><br>[PAE] [2586/2022] (Planejamento)<br><br>[PAE] [4956/2022] (Adesão ARP TSE 02/2022) | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - GESTÃO DE IDENTIDADE E DE CONTROLE DE ACESSOS (ANEXO VI)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 6.1 | .implantação da solução de Gerenciamento de Acessos Privilegiados (Cofre de Senhas) para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos) | SRI | dez/22 | [Implantada]<br><br>**[*BEYOUNDTRUST*]**<br><br>Empresa fornecedora: [*SEVEN SECURE* TECNOLOGIA DA INFORMAÇÃO LTDA]<br><br>[PAE] [2586/2022] (Planejamento)<br><br>[PAE] [4956/2022] (Adesão ARP TSE 02/2022) | Finalizada |
| 6.2 | .instituir regras para a gestão de identidade e de controle de acessos físico e lógico ao ambiente cibernético do TRE/RN | COGESTIC | jul/23 | conjunto de normas adaptada para o TRE/RN | Finalizada |
| 6.2 | .dar ciência às unidades envolvidas na concessão de autorizações da política de autorização da norma que trata sobre o controle de acesso aos sistemas informatizados | COGESTIC | jul/23 | conjunto de normas adaptada para o TRE/RN | Finalizada |
| 6.3.2.1 | .exigir que as funções de aprovador administrativo e de aprovador técnico não sejam exercidas pela mesma pessoa ou, quando for o caso, que o custodiante de dados não desempenhe nenhuma dessas funções | COINF e COSIS | jul/23 | conjunto de normas adaptada para o TRE/RN | Finalizada |
| 6.3.4.1 | .projetar e implantar soluções para possibilitar sistemas e aplicativos com remoção das autorizações e contas de uma pessoa nos momentos apropriados | COINF e COSIS | junho/22 | script e cadastro com data determinada | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - GESTÃO DE IDENTIDADE E DE CONTROLE DE ACESSOS (ANEXO VI)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 7.1 | .garantir na Política de Gestão de Identidades e de Controle de Acessos que os usuários devam:<br>-criar senhas que estejam em conformidade com os critérios de senhas seguras estabelecidos pelo órgão<br>-não compartilhar senhas relacionadas a algum sistema corporativo com qualquer outra pessoa<br>-não reutilizar senhas relacionadas a qualquer sistema corporativo em contas pessoais<br>-alterar imediatamente as senhas e notificar o gestor do sistema apropriado e/ou área de segurança da informação se houver motivos para acreditar que uma senha foi divulgada, acessada ou utilizada indevidamente por uma pessoa não autorizada<br>-utilizar os privilégios associados a uma conta apenas para a finalidade para a qual foram autorizados e nada mais<br>-valer-se de contas e autorizações privilegiadas apenas quando tal privilégio for necessário para completar uma função<br>-fazer logoff ou utilizar bloqueio de tela que exija autenticação ao deixar um dispositivo sem supervisão | STIE | jul/23 | conjunto de normas adaptada para o TRE/RN e cofre de senhas | Finalizada |
| 8.4 | .aplicar periodicamente *checklists* ou listas de autoverificação implementadas pela organização (no mínimo com periodicidade anual)<br>.estabelecer os níveis de maturidade nessa avaliação | STIE | mar/23 | Realizar pesquisas para monitorar o nível de maturidade em SI dos usuários do TRE/RN | Finalizada |
| 8.4 | .aplicar periodicamente (no mínimo com periodicidade anual) *checklists* ou listas de autoverificação implementadas pela organização | STIE | mar/23 | Realizar pesquisas para monitorar o nível de maturidade em SI dos usuários do TRE/RN | Finalizada |
| 8.4 | .estabelecer os níveis de maturidade na avaliação realizada através de *checklists* ou listas de autoverificação implementadas pela organização, de forma a possibilitar a melhoria contínua de normativos, processos e iniciativas em segurança cibernética da organização | STIE | mar/23 | Realizar pesquisas para monitorar o nível de maturidade em SI dos usuários do TRE/RN | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - POLÍTICA DE EDUCAÇÃO E CULTURA EM SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO (ANEXO VII)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 0.1 | .estabelecer as diretrizes necessárias consubstanciadas em ações permanentes de capacitação, de educação, de engenharia social e de formação de cultura especializada | EJE e STIE | jun/23 | | Finalizada |
| 0.1 | .implantar a solução de Plataforma de Educação e Conscientização em Segurança da Informação, com simulação de Phishings | NEAD e STIE | jun/23 | **[Implantada]**<br><br>**.[KNOWBE4]**<br>[Plataforma de Conscientização em SI]<br>[Contrato nº 46/2022]<br>[QUALITEK TECNOLOGIA]<br><br>[PAE] [2585/2022] (planejamento)<br><br>[PAE] [2359/2022] (consulta sobre interesse em participar da contratação de solução para conscientização e capacitação em Cibersegurança)<br><br>[PAE] [6498/2022] (adesão a ARP TRE-ES nº 04/2022) e (seleção do fornecedor)<br><br>[PAE] [10424/2022] (gestão do contrato)<br><br>ver incisos:<br>- 3.2.2 Anexo I<br>- 5.1 Anexo IV<br>- 5.2 Anexo IV<br>- 6.1 Anexo IV<br>- 0.2 Anexo V | Finalizada |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - POLÍTICA DE EDUCAÇÃO E CULTURA EM SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO (ANEXO VII)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 0.2 | .tratar o tema de formação de cultura e de educação em segurança cibernética de forma equânime, uniforme e articulada com todos os órgão do Poder Judiciário e em conformidade com os mais atualizados paradigmas, procedimentos e padrões nacionais e internacionais | STIE | jun/22 | Integrante em grupos nacionais ou regionais que tratam de SI | Finalizada |
| 0.3 | .incentivar a troca de experiências e conhecimentos, com participação de servidores do TRE/RN em fóruns multisetoriais e treinamentos ofertados por outros órgãos, na área de Segurança Cibernética | NEAD, STIE e SSI | Ação contínua | entrar em algum fórum local e nacional de SI | Ação Contínua |
| 0.4 | .desenvolver ações educacionais, no órgão, observando a diversidade e a multiplicidade de opções de cursos; programas de treinamento; modalidades de aquisição e disseminação de conhecimentos; formação técnica e gerencial; e plataformas tecnológicas educacionais presentes no mercado educacional contemporâneo | NEAD e STIE | Ação contínua | Realizar ações periódicas de conscientização em cibersegurança e capacitações | Ação Contínua |
| 1.2.1.a | .incluir no plano de capacitação e de contração ações voltadas para melhoria da Segurança Cibernética | NEAD e STIE | dez/22 | | Finalizada |
| 1.2.1.d | .dar ciência à todo usuário da Política de Segurança da Informação | NEAD e STIE | jul/22 | repetir após revisão | Finalizada |
| 1.2.1.e | .assegurar que novos conhecimentos atinentes ao tema da segurança cibernética sejam permanentemente ofertados aos profissionais das áreas de Tecnologia da Informação e Comunicação e de Segurança da Informação, técnico, gerencial, entre outros aplicáveis | NEAD e STIE | Ação contínua | incluir ações Segurança cibernética nos planos de capacitação | Ação Contínua |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - POLÍTICA DE EDUCAÇÃO E CULTURA EM SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO (ANEXO VII)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 2.1.1 | .desenvolver ações de capacitação, formação, reciclagem, fomento e conscientização em segurança cibernética, podendo incluir, entre outras:<br>a) programas de formação;<br>b) programas de reciclagem;<br>c) programas de extensão educacional;<br>d) programas de pesquisa e fomento de natureza técnica, acadêmica e científica;<br>e) elaboração de artigos, materiais e publicações de natureza técnica, acadêmica e<br>científica;<br>f) programas de intercâmbio, imersão e cooperação educacional;<br>g) ações periódicas de capacitação;<br>h) cursos em plataformas do tipo *MOOC – Massive Open Online Courses*;<br>i) programas de certificação especializada;<br>j) palestras, congressos, seminários e afins;<br>k) concursos, competições e premiações; e<br>l) *workshops* | EJE, NEAD e STIE | Ação contínua | criar plano de capacitação de ciber segurança para os servidores da SSI, SRI,SDS e SBDS | Ação Contínua |
| 3.3.1 | .incluir nos planejamentos anuais, através das áreas de Comunicação Social e Institucional do órgão, programas de divulgação, conscientização, informação e esclarecimentos aos seus públicos-alvo, tanto internos como externos, referentes a temas de Segurança Cibernética | ASCOM, DG e STIE | Ação contínua | Realizar ações de conscientização de SI e combate a desinformação público externo ASCOM | Ação Contínua |
| 4.1.a | .garantir que os programas de formação, capacitação e reciclagem devem propiciar que o órgão possua:<br>a) profissionais de Tecnologia da Informação e Comunicação e de Segurança da Informação em seus quadros, qualificados em segurança cibernética em nível de graduação, pós-graduação ou de certificações especializadas | EJE, NEAD e STIE | Ação contínua | criar plano de capacitação de ciber segurança para os servidores da SSI, SRI,SDS e SBDS | Ação Contínua |

# CRONOGRAMA

| PORTARIA Nº 162/2021-CNJ | | | | | |
|---|---|---|---|---|---|
| **MANUAL DE REFERÊNCIA - POLÍTICA DE EDUCAÇÃO E CULTURA EM SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO (ANEXO VII)** | | | | | |
| **Artigo/ Inciso** | **Ação** | **Responsável** | **Prazo** | **Observações/ Evidências** | **Situação** |
| 4.1.b | .garantir que os programas de formação, capacitação e reciclagem devem propiciar que o órgão possua:<br>b) todos os usuários internos com educação básica e cultura em segurança cibernética | NEAD e STIE | dez/23 | curso básico de SI e cursos com ferramenta de conscientização | Finalizada |
| 4.2 | .apresentar ao CNJ, no início do ano seguinte, relatório que comprove a efetividade das ações realizadas no exercício anterior e o respectivo desempenho dos usuários e profissionais treinados | DG e STIE | início de cada ano | Encaminhar ao CNJ relatório com principais ações de SI desenvolvidos no ano | Ação Contínua |

# CONSIDERAÇÕES FINAIS

Considerando os benefícios decorrentes das ações aqui propostas, bem como a proteção do conjunto de dados e informações corporativas, buscando garantir a sua disponibilidade, integridade e confiabilidade e o cumprimento da Política de Segurança da Informação e Comunicação vigente, manifesta-se a expectativa de que a Administração deste Tribunal acolha este Plano de Trabalho em Segurança da Informação, reconheça o seu caráter estratégico e, consequentemente, priorize a implementação das ações no âmbito do Tribunal Regional Eleitoral do Rio Grande do Norte (TRE/RN).