PROTOCOLO

PREVENÇÃO DE INCIDENTES CIBERNÉTICOS

SUMÁRIO

1. HISTÓRICO DE ELABORAÇÃO/REVISÃO 2

2. SIGLAS 2

3. INTRODUÇÃO 3

4. FUNÇÕES BÁSICAS e PRINCÍPIOS 3

5. MEDIDAS DE PREVENÇÃO 7

IDENTIFICAR 7

PROTEGER 9

DETECTAR 15

RESPONDER 16

RECUPERAR 16

6. PLANO DE AÇÃO PARA IMPLEMENTAÇÃO INTEGRAL DO PROTOCOLO PPINC-PJ 18

7. REFERÊNCIAS 21

1. HISTÓRICO DE ELABORAÇÃO/REVISÃO

Versão	Data	Descrição da ação / alteração	Responsável
1	13/08/2023	Versão inicial	Gestor de Segurança da Informação
2	30/07/2024	Versão 2 – Atualização várias ações/procedimentos	Gestor de Segurança da Informação
3	22/01/2025	Atualização de procedimentos	Gestor de Segurança da Informação
4	13/08/2025	Atualização de informações	Gestor de Segurança da Informação

2. SIGLAS

SIGLA	DESCRIÇÃO
ENSEC	Estratégia Nacional de Segurança Cibernética do Poder Judiciário
ETIR	Equipe de Tratamento e Resposta a Incidentes de Redes
HTTPS	*Hypertext Transfer Protocol Secure*
LGPD	Lei Geral de Proteção de Dados, Lei n.º 13.709/2018
LOGs	Conjunto de registros de eventos
PSI	Política de Segurança da Informação da Justiça Eleitoral, Resolução TSE n.º 23.655/2021
SSL	*Secure Sockets Layer*
TIC	Tecnologia da Informação e Comunicação
TLS	*Transport Layer Security*
ZE	Zonas Eleitorais

3. INTRODUÇÃO

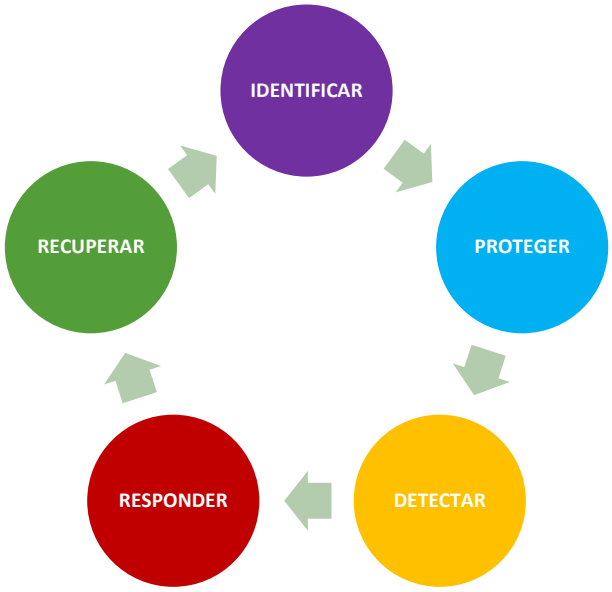
3.1. Diante do aumento constante das ameaças de ataques hackers direcionados à infraestrutura digital dos tribunais brasileiros e levando em consideração a crescente atuação da Justiça no ambiente virtual, o Conselho Nacional de Justiça (CNJ) deu origem à Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), estabelecida através da Resolução nº 396/2021.

3.2. Com o intuito de aderir integralmente a essa Resolução e à Portaria nº 162 CNJ de 10/06/2021, que endossou os Protocolos e Manuais desenvolvidos pela ENSEC-PJ, a Secretaria de Tecnologia da Informação e Comunicação (STIC) juntamente com o Gestor de Segurança da Informação do Tribunal, iniciaram um trabalho, onde resultante desse esforço é o Protocolo de Prevenção de Incidentes Cibernéticos (PPINC).

3.3. O PPINC engloba um conjunto abrangente de diretrizes, cujo foco central é a prevenção de incidentes cibernéticos em todos os níveis, com divisões funcionais estrategicamente alinhadas à gestão global de riscos. Seu propósito primordial é embasar decisões apropriadas para confrontar as ameaças emergentes e aprimorar a administração de práticas e metodologias já estabelecidas conforme as melhores práticas do mercado.

4. FUNÇÕES BÁSICAS e PRINCÍPIOS

4.1. São funções básicas do **Protocolo de Prevenção de Incidentes Cibernéticos** as relacionadas a seguir:



IDENTIFICAR - Compreensão institucional visando à gestão de riscos iminentes e/ou potenciais provenientes de ataques cibernéticos direcionados a sistemas, indivíduos, recursos, informações e ativos.

PROTEGER - Criação e aplicação de medidas de proteção para garantir a segurança de informações, incluindo dados pessoais e ativos de informação, além da garantia de continuidade na prestação de serviços essenciais.

DETECTAR - Elaboração e execução de ações voltadas para identificação de incidentes de segurança cibernética, abrangendo detecção de anomalias e ocorrências relevantes.

RESPONDER - Formulação e execução de ações adequadas para a aplicação de medidas em resposta a incidentes cibernéticos identificados. Isso engloba elaboração de planos de reação, comunicação, avaliação, redução de impacto e aprimoramentos.

RECUPERAR - Elaboração, execução e atualização dos planos de resiliência e recuperação de capacidades ou serviços afetados.

4.2. Para o desenvolvimento de um sistema de segurança cibernética eficiente e eficaz é necessário minimamente atender aos seguintes princípios fundamentais:

4.2.1. **Base de conhecimento de defesa:** Construção de uma base de informações e conhecimentos de ataques reais, fornecida por outras ETIRs, visando absorção contínua de conhecimento prático para à construção de defesas e ações cada vez mais céleres, efientes e eficazes.

4.2.2. **Priorização:** Mapear sistemas e informações críticas e com maior risco para o negócio do Tribunal, com o objetivo de proteção contra as ameaças e visando redução de riscos.

4.2.3. **Instrumentos de medição e métricas:** Estabelecimento de indicadores compartilhados, utilizando terminologia que facilite a compreensão de todas as partes envolvidas, permitindo a rápida implementação das correções necessárias.

4.2.4. **Diagnóstico contínuo:** Avaliação contínua para verificar e validar a eficácia das medidas de segurança em vigor, auxiliando na determinação de prioridades e orientando os próximos passos a serem empreendidos.

4.2.5. **Formação, capacitação e conscientização:** Procedimentos educacionais contínuos por meio da integração de atividades de capacitação nos planos, abrangendo a divulgação, o treinamento, a conscientização e a orientação de todos os envolvidos na promoção da cultura de segurança cibernética do Tribunal.

4.2.6. **Automação:** Priorização de investimentos em soluções com automação, aprendizado de máquina, Inteligência Artificial e análise preditiva, para possibilitar a implementação de procedimentos, análises a ações confiáveis, mensuráveis e constantes com a menor intervenção humana possível.

4.2.7. Resiliência: A resiliência no tratamento e resposta a incidentes cibernéticos não se trata apenas de tecnologia, mas também de processos, pessoas e coordenação, ou seja, é necessário estar preparado para lidar com incidentes cibernéticos de forma eficaz, minimizando seus impactos e garantindo a continuidade das operações críticas do Tribunal.

4.3. Adicionalmente, este Protocolo também busca orientar-se pelas diretrizes recomendadas de segurança cibernética e suas aplicações práticas, conforme delineadas nas seguintes dimensões de visão geral:

4.3.1. **Preparação** – resposta metódica, envolvendo planejamento sobre como responder e notificar cada incidente de segurança, bem como processos de educação e de formação.

4.3.2. **Identificação** – trata-se da aptidão dos entes para diferenciar as irregularidades em redes de dados e identificar o mau funcionamento dos sistemas críticos, em razão de ataques cibernéticos em curso.

4.3.3. **Contenção** – Visa a garantir que o incidente não cause mais danos. A prioridade é isolar o que foi afetado, manter a produção e, acima de tudo, garantir que as ações não comprometam, ainda mais, a segurança ou as operações críticas. As equipes devem seguir o Protocolo de Gerenciamento de Crises Cibernéticas.

4.3.4. **Erradicação** – Consiste na remoção da ameaça, garantindo a retomada dos serviços essenciais. Na medida do possível, devem-se preservar evidências a serem utilizadas na investigação de crime cibernético.

4.3.5. **Recuperação** – execução do plano de restauração de operações, priorizando sistemas críticos ou sua execução em modo analógico até que se restabeleça a confiança em seu desempenho.

4.3.6. **Lições aprendidas** – registro dos impactos imediatos de um incidente, assim como as melhorias em longo prazo da segurança cibernética do órgão.

5. MEDIDAS DE PREVENÇÃO

5.1. IDENTIFICAR

ATIVIDADE: IDENTIFICAR OS ATIVOS DE INFORMAÇÃO CRÍTICOS Entende-se por ativos de informação os meios de armazenamento, transmissão e processamento de informação, sistemas de informação e locais onde se encontram esses meios e as pessoas que a eles têm acesso. A atividade consiste em enumerar todos os ativos de informação mais impactantes em caso de incidentes cibernéticos, gerando uma espécie de catálogo de ativos da informação, com responsáveis pelos mesmos. Para esta atividade, recomenda-se:	
Recomendações	**Responsáveis** (por observar a recomendação)
Observar orientações da Portaria PR 69/2023 – Institui a ETIR.	- ETIR
Observar orientações da Resolução 7882/2021 do TRE-DF – Sistema de Gestão de Riscos Institucionais	- Unidades STIC - Todas as unidades TRE-DF
Observar as melhores práticas sobre o Gerenciamento da Continuidade de Serviços de TIC (CIS Controls V.8 e ISO 27001 e 27002)	- STIC/COIE - SESOP/SETEL - ETIR
Observar a PSI, instituída pela Resolução TSE 23.644/2021	- Todos os usuários do TRE-DF
Observar a Resolução 396/2021 do CNJ	- Unidades STIC - Todos os usuários do TRE-DF

ATIVIDADE: INVENTÁRIO E CONTROLE DE ATIVOS DE HARDWARE A atividade consiste em enumerar todos os ativos de hardware, gerando uma espécie de catálogo de ativos de hardware, com responsáveis pelos mesmos. Em caso de incidentes cibernéticos será possível identificar se os ativos mais críticos, de maior risco foram impactados, permitindo uma ação direcionada para tratar os mesmos. Para esta atividade, recomenda-se:	
Recomendações	**Responsáveis**
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP
Observar orientações da Portaria PR 69/2023 – Institui a ETIR.	- Unidades da STIC - ETIR
Observar as orientações na PARTIC – Política de Acesso aos Recursos de TIC – Portaria PR 122/2022	- Unidades da STIC - Todos os usuários do TRE-DF

ATIVIDADE: INVENTÁRIO E CONTROLE DE ATIVOS DE SOFTWARE A atividade consiste em enumerar todos os ativos de software mais impactantes em caso de incidentes cibernéticos, gerando uma espécie de catálogo de ativos de software, com responsáveis pelos mesmos. Para esta atividade, recomenda-se:	
Recomendações	**Responsáveis**
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP
Observar as orientações na PARTIC – Política de Acesso aos Recursos de TIC – Portaria PR 183/2024	- Unidades da STIC - Todos os usuários do TRE-DF
Observar orientações da Portaria PR 69/2023 – Institui a ETIR.	- Unidades da STIC - ETIR

5.2. PROTEGER

5.2.1. Esta função está ligada aos esforços relacionados ao gerenciamento de identidade e controle de acesso, conscientização e treinamento, segurança de dados, processos e procedimentos de proteção da informação.

ATIVIDADE: MONITORAMENTO E CONTROLE DE CONTAS

Conta de usuário pode ser entendida como identificador único de usuário em sistemas de computadores. A atividade consiste em administrar contas de usuário, zelando para que os acessos à rede sejam imediatamente revogados quando ocorrer o desligamento do respectivo usuário proprietário da conta de usuário, permitindo auditoria nos acessos aos sistemas.

Para esta atividade, recomenda-se:

Recomendações	Responsáveis
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP
Observar orientações da Portaria PR 69/2023 – Institui a ETIR.	- Unidades da STIC - ETIR
Observar as orientações na PARTIC – Política de Acesso aos Recursos de TIC – Portaria PR 183/2024	- Unidades da STIC - Todos os usuários do TRE-DF
Observar a necessidade de fazer de forma mais efetiva o Gerenciamento de Contas de Usuários, Terceirizados, Estagiários, Requisitados, Juízes e Servidores Aposentados.	- Unidades da STIC - Unidade responsável pelos contratos do Tribunal - Unidade gestora de contratos de estágio - Fiscais de contratos de terceiros - Unidade gestora de informações de servidores requisitados - Unidade gestora de dados de magistrados - Unidade gestora dos dados dos servidores aposentados

ATIVIDADE: PROGRAMA DE CONSCIENTIZAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

Um programa eficaz de orientação e conscientização de usuários em segurança da informação e cibersegurança requer uma abordagem abrangente e bem planejada. É um esforço contínuo, e a cultura de segurança deve ser incorporada às práticas diárias de todos na organização.

Para esta atividade, recomenda-se:

Recomendações	Responsáveis
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP - Todos usuários de TIC
Publicar mensalmente matéria sobre a PSI, no portal de intranet ou outros meios de comunicação.	- STIC e ASCOM - Gestor de Segurança da Informação
Realizar campanhas de conscientização com treinamentos na plataforma de capacitação de usuários em cibersegurança.	- STIC - ASCOM - Gestor de Segurança da Informação
Oferecer cursos on-line obrigatório com orientações básicas sobre o tema na plataforma de capacitação de usuários em cibersegurança.	- STIC - ASCOM - Gestor de Segurança da Informação

ATIVIDADE: SEGURANÇA DE APLICAÇÕES DE SOFTWARE (ACESSOS, PRIVILÉGIOS, DESENVOLVIMENTO SEGURO)

Autorização é o processo que ocorre após a autenticação e tem a função de diferenciar os privilégios atribuídos ao usuário que foi autenticado. Os atributos de autorização normalmente são definidos em grupos mantidos em uma base de dados centralizada, sendo que cada usuário herda as características do grupo ao qual ele pertence. Portanto, autorização é o direito ou permissão de acesso a um recurso de um sistema. Direito de Acesso é privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo.

Desenvolvimento seguro é um conjunto de práticas, integradas em todos os estágios de desenvolvimento e manutenção de software, visando a fortalecer a segurança e a conformidade e propicia benefícios na qualidade das aplicações, na redução de riscos, e permite implementar o monitoramento de vulnerabilidades nos códigos desenvolvidos

Para esta atividade, recomenda-se:

Recomendações	Responsáveis
Observar orientações da Portaria PR	- Unidades da STIC

69/2023 – Institui a ETIR.	- ETIR
Observar as orientações na PARTIC – Política de Acesso aos Recursos de TIC – Portaria PR 183/2024	- Unidades da STIC - Todos os usuários do TRE-DF
Necessidade de implementar o processo de Gerenciamento de Mudanças	- STIC/COIE - COIE/SESOP
Necessidade de implementar o processo de Gerenciamento de Continuidade de Serviços de TIC	- STIC/COIE - COIE/SESOP
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP - Todos usuários de TIC
Necessidade de implementar o processo de Gerenciamento de Configuração de Ativos de Serviço, no âmbito da STIC	- STIC/COIE - COIE/SESOP

ATIVIDADE: DEFESA DE PERÍMETRO

A segurança de perímetro, dentro do contexto do ITIL, envolve o estabelecimento de controles de acesso, firewalls, sistemas de detecção de intrusões e outras medidas para proteger os ativos de TI contra ameaças externas. Também está relacionada à identificação e controle dos pontos de entrada e saída da rede, bem como à implementação de mecanismos de segurança, além dos já mencionados firewalls, como sistemas de prevenção de intrusões (IPS), autenticação forte e políticas de controle de acesso, ou seja, a limitação e controle de portas, protocolos e serviços, que objetiva restringir o tráfego não essencial e os serviços não utilizados.

Para esta atividade, recomenda-se:

Recomendações	Responsáveis
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP - Todos usuários de TIC
Observar as orientações na PARTIC – Política de Acesso aos Recursos de TIC – Portaria PR 183/2024	- Unidades da STIC - Todos os usuários do TRE-DF
Necessidade de implementar o processo de Gerenciamento de Mudanças	- STIC/COIE - COIE/SESOP

ATIVIDADE: PROTEÇÃO DE DADOS

Segurança de dados consiste na adoção de medidas de segurança da informação aptas a proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas.

A LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Para esta atividade, recomenda-se:

Recomendações	Responsáveis
Observar a Portaria Conjunta nº 30/2022 do TR-DF, Portaria Conjunta nº 30/2020, Portaria Conjunta nº 31/2020 (DPO, Política de Privacidade de dados e institui o CCPDP)	- Unidades STI - Ouvidoria - Todas unidades da STIC -Todos os usuários do TRE-DF
Observar as orientações na PARTIC – Política de Acesso aos Recursos de TIC – Portaria PR 122/2022	- Unidades da STIC - Todos os usuários do TRE-DF
Observar a Portaria Presidência nº 69/2021, que institui a Política de Backup no TRE-DF	- Unidades STIC - Responsáveis pelos sistemas e serviços disponibilizados aos usuários
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP - Todos usuários de TIC

ATIVIDADE: USO CONTROLADO E DISTRIBUIÇÃO DE PRIVILÉGIOS ADMINISTRATIVOS

Direito de Acesso é privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo.

Para esta atividade, recomenda-se:

Recomendações	Responsáveis
Observar as orientações na PARTIC – Política de Acesso aos Recursos de TIC – Portaria PR 183/2024	- Unidades da STIC - Todos os usuários do TRE-DF
Necessidade de implementar o processo de Gerenciamento de Configuração de Ativos de Serviço, no âmbito da STIC	- STIC/COIE - COIE/SESOP
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP - Todos usuários de TIC

ATIVIDADE: CONFIGURAÇÃO SEGURA DE HARDWARE E SOFTWARE EM DISPOSITIVOS MÓVEIS, LAPTOPS, ESTAÇÕES DE TRABALHO E EQUIPAMENTOS SERVIDORES

Esta ação consiste em configurar corretamente hardware e software, a fim de aumentar a segurança do ambiente computacional do Tribunal.

Para esta atividade, recomenda-se:

Recomendações	Responsáveis
Observar as orientações na PARTIC – Política de Acesso aos Recursos de TIC – Portaria PR 183/2024	- Unidades da STIC - Todos os usuários do TRE-DF
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP - Todos usuários de TIC

ATIVIDADE: PROTEÇÕES DE E-MAIL E NAVEGADOR DA WEB (WEBMAIL), ANTISPAM NO TSE (P/ E-MAIL)

Esta ação consiste em configurar corretamente serviço de e-mail, a fim de aumentar a segurança do ambiente computacional do Tribunal.

Para esta atividade, recomenda-se:

Recomendações	Responsáveis
Observar as orientações na PARTIC – Política de Acesso aos Recursos de TIC – Portaria PR 183/2024	- Unidades da STIC - Todos os usuários do TRE-DF
Observar a necessidade de fazer de forma mais efetiva o Gerenciamento de Contas de Usuários, Terceirizados, Estagiários, Requisitados, Juízes e Servidores Aposentados.	- Todas as unidades do TRE-DF
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP - Todos usuários de TIC

ATIVIDADE: DEFESAS CONTRA MALWARE

Esta ação consiste em implementar e manter atualizado recursos que permitem defesa contra software malicioso, a fim de aumentar a segurança do ambiente computacional do . TRE-DF

Para esta atividade, recomenda-se:

Recomendações	Responsáveis

Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP - Todos usuários de TIC
Observar orientações da Portaria PR 69/2023 – Institui a ETIR.	- Unidades da STIC - ETIR
Observar as orientações na PARTIC – Política de Acesso aos Recursos de TIC – Portaria PR 183/2024	- Unidades da STIC - Todos os usuários do TRE-DF
Observar a necessidade de definir orientações para realização segura dos acessos externos a rede interna do Tribunal	- STIC/COIE - Gestor de Segurança da Informação
Estabelecer campanhas e treinamentos direcionados para conscientização contra softwares e agentes maliciosos	- STIC - ASCOM - Gestor de Segurança da Informação

ATIVIDADE: LIMITAÇÃO E CONTROLE DE PORTAS, PROTOCOLOS E SERVIÇOS DE REDE

Esta ação consiste em limitar e controlar portas, protocolos e serviços de rede, a fim de aumentar a segurança do ambiente computacional do Tribunal.

Para esta atividade, recomenda-se:

Recomendações	Responsáveis
Observar orientações da Portaria PR 69/2023 – Institui a ETIR.	- Unidades da STIC - ETIR
Observar as orientações na PARTIC – Política de Acesso aos Recursos de TIC – Portaria PR 183/2024	- Unidades da STIC - Todos os usuários do TRE-DF
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP - Todos usuários de TIC

ATIVIDADE: CONFIGURAÇÃO SEGURA DE DISPOSITIVOS DE REDE (FIREWALLS, ROTEADORES, SWITCHES, ACCESS POINT ETC.)

Esta ação consiste em configurar corretamente dispositivos de rede, a fim de aumentar a segurança do ambiente computacional do Tribunal.

Para esta atividade, recomenda-se:

Recomendações	Responsáveis
Observar orientações da Portaria PR 69/2023 – Institui a ETIR.	- Unidades da STIC - ETIR
Observar as orientações na PARTIC –	- Unidades da STIC

Política de Acesso aos Recursos de TIC – Portaria PR 183/2024	- Todos os usuários do TRE-DF
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP - Todos usuários de TIC

5.3. DETECTAR

5.3.1. Esta função está ligada aos esforços no monitoramento contínuo de segurança, processos de detecção de anomalias e eventos.

ATIVIDADE: GERENCIAMENTO CONTÍNUO DE VULNERABILIDADES

Esta ação consiste em gerenciar continuamente vulnerabilidades, a fim de aumentar a segurança do ambiente computacional do TRE-DF.

Para esta atividade, recomenda-se:

Recomendações	Responsáveis
Observar orientações da Portaria PR 69/2023 – Institui a ETIR.	- Unidades da STIC - ETIR
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP - Todos usuários de TIC
Observar as orientações na PARTIC – Política de Acesso aos Recursos de TIC – Portaria PR 183/2024	- Unidades da STIC - Todos os usuários do TRE-DF

ATIVIDADE: MANUTENÇÃO, MONITORAMENTO E ANÁLISE DE LOGS DE AUDITORIA

Logs ou registros de auditoria são registros de eventos relevantes em um dispositivo ou sistema computacional. Esta ação consiste em gerenciar LOGs, a fim de aumentarem a segurança do ambiente computacional do TRE-DF.

Para esta atividade, recomenda-se:

Recomendações	Responsáveis
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP - Todos usuários de TIC
Observar as orientações na PARTIC – Política de Acesso aos Recursos de TIC – Portaria PR 183/2024	- Unidades da STIC - Todos os usuários do TRE-DF

ATIVIDADE: MONITORAMENTO DO SISTEMA DE ANTIVÍRUS Para esta atividade, recomenda-se:	
Recomendações	**Responsáveis**
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP - Todos usuários de TIC
Observar as orientações na PARTIC – Política de Acesso aos Recursos de TIC – Portaria PR 183/2024	- Unidades da STIC - Todos os usuários do TRE-DF

5.4. RESPONDER

5.4.1. Esta função está ligada aos planos de resposta, de comunicações, de análise, de mitigação e de melhorias.

ATIVIDADE: MANTER BASE DE DADOS SOBRE OS INCIDENTES Esta ação consiste em manter base de dados que possa auxiliar nas execuções das atividades ligadas à segurança da informação, a fim de aumentar a segurança do ambiente computacional do TRE-DF. Para esta atividade, recomenda-se:	
Recomendações	**Responsáveis**
Observar orientações da Portaria PR 69/2023 – Institui a ETIR.	- Unidades da STIC - ETIR
Estabelecer com base na metodologia de gestão de riscos, os riscos relacionados à Tecnologia da Informação e Comunicação	- Unidades STIC
Implementar o processo de Gerenciamento de Continuidade de Serviços de TIC	- STIC/COIE - COIE/SESOP
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP - Todos usuários de TIC
Implementar o processo de Gerenciamento de Problemas	- STIC/COIE - COIE/SESOP

5.5. RECUPERAR

5.5.1. Esta função está ligada aos planos de resiliência e de restauração de capacidades ou serviços.

ATIVIDADE: RESPOSTA E GERENCIAMENTO DE INCIDENTES CIBERNÉTICOS Esta ação consiste em gerenciar riscos relacionados a incidentes cibernéticos e executar respostas para restabelecer o ambiente computacional, a fim de garantir a continuidade de negócio do TRE-DF. Para esta atividade, recomenda-se:	
Recomendações	**Responsáveis**
Observar as orientações da Portaria PR 69/2023 – Institui a ETIR.	- Unidades da STIC - ETIR - Comitê de Gestão de Crises
Estabelecer com base na metodologia de gestão de riscos, os riscos relacionados à Tecnologia da Informação e Comunicação	- Unidades STIC
Implementar o processo de Gerenciamento de Continuidade de Serviços de TIC	- STIC/COIE - Gestor de Segurança da Informação
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP - Todos usuários de TIC

ATIVIDADE: CAPACIDADES DE RECUPERAÇÃO DE DADOS – BACKUP E RESTORE Backup ou cópia de segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Para esta atividade, recomenda-se:	
Recomendações	**Responsáveis**
Observar as orientações da Portaria PR 122/2021 – Institui a ETIR.	- Unidades da STIC - ETIR - Comitê de Gestão de Crises
Estabelecer com base na metodologia de gestão de riscos, os riscos relacionados à Tecnologia da Informação e Comunicação	- Unidades STIC
Observar a Portaria Presidência nº 69/2021, **que regulamenta a Política de Backup no TRE-DF,** procedimentos de backup e recuperação de dados	- Unidades STIC - Gestores de sistemas e serviços
Implementar o processo de Gerenciamento de Continuidade de Serviços de TIC,	- STIC/COIE - COIE/SESOP - Gestor de Segurança de Informação
Observar as orientações na PSI, instituída pela Resolução TSE 23.644/2021	- Unidades da STIC - COIE/SESOP - Todos usuários de TIC
Implementar o processo de Gerenciamento	- STIC/COIE

de Mudanças	- COIE/SESOP

6. PLANO DE AÇÃO PARA IMPLEMENTAÇÃO INTEGRAL DO PPINC-PJ

6.1. Visando atender ao PPINC-PJ definido no Anexo I da Portaria nº 162/2021 do CNJ, foram definidas algumas ações e procedimentos, conforme tabela abaixo.

	Identificar
	Ação/Procedimento
1	**Os ativos críticos foram definidos?**
2	**Os riscos associados aos ativos críticos foram levantados e definidos?**
3	**Os riscos críticos são tratados e monitorados?**
4	**Os sistemas críticos foram identificados?**
5	**Os serviços críticos foram identificados?**
6	**As vulnerabilidades nos ativos críticos são identificadas?**
7	**As vulnerabilidades nos ativos críticos são tratadas?**
8	**Existe inventário atualizado de ativos de TI (hardware, software e dados sensíveis)?**
	Proteger
9	**Os dados são classificados?**
10	**Os dados sensíveis de acordo com a LGPD são identificados?**
11	**Existe controle de acesso aos dados baseado na necessidade de conhecimento do usuário?**
12	**Os acessos aos dados são registrados?**
13	**Cópias de segurança dos dados são realizadas?**
14	**Os ativos corporativos são atualizados constantemente?**
15	**Os ativos corporativos são inventáriados?**
16	**Os acessos externos são criptografados?**
17	**Os acessos externos utilizam duplo fator de autenticação?**
18	**Controles de acesso são implementados?**
19	**Controles de acesso são monitorados e auditados?**
20	**Políticas de senhas são implementadas e monitoradas?**
21	**Ativos para proteção e gestão da segurança da informação como firewalls de rede e de aplicação foram implementados e estão operacionais?**
22	**Solução de antimalware foi implementada e está operacional?**
23	**Solução de proteção para banco de dados foi implementada e está operacional?**
24	**Solução de proteção de acessos de usuários com privilégio foi implementada e está operacional?**

25	Todas as contas com privilégio são geridas pela solução de proteção de acessos, de credenciais (cofre de senhas)?
26	Existe solução de duplo fator de autenticação implementada e operacional?
27	A solução de proteção de acessos e de credenciais com privilégio utiliza o duplo fator de autenticação?
28	Solução de consciêntização em segurança cibernética foi implementada e está operacional?
	Detectar
29	Os serviços críticos são monitorados?
30	Os ativos críticos são monitorados?
31	Os dados são monitorados?
32	Existem alertas configurados nas ferramentas utilizadas para monitoração do ambiente?
33	Os eventos e alertas gerados pelas ferramentas de apoio a gestão da segurança da informação são analisados diáriamente?
34	Os eventos e alertas gerados pelas ferramentas de apoio a gestão da segurança da informação são analisados semanalmente ou quinzenalmente?
35	Os eventos e alertas gerados pelas ferramentas de apoio a gestão da segurança da informação são armazenados?
36	Solução para consolidação e análise de logs foi implementa e está operacional?
	Responder
37	Exite plano de gestão de incidentes cibernéticos formalizado?
38	Existe plano de comunicação de incidentes cibernéticos formalizado?
39	Existe plano de mitigação e análise de incidentes cibernéticos formalizado?
40	Os procedimentos e responsabilidades estão claros e bem definidos no plano de resposta a incidentes cibernéticos?
	Recuperar
41	Existe plano formalizado para recuperação do ambiente em caso de incidente de segurança cibernética?
42	Os planos para apoio a gestão de incidentes de segurança cibernética são atualizados e gerenciados
43	Existe política de backup formalizada e em prática na instituição?
44	Os backups são testados de forma regular, pelo menos 02 vezes ao ano?
45	Existe infraestrutura disponível para recuperação de serviço em caso de necessidade?
	Princípios Críticos
46	A equipe de Tratamento e Resposta a Incidentes interage ou coopera com outras equipes de ETIR de outras organizações?
47	A equipe de Tratamento e Resposta a Incidentes fez alguma capacitação específica na área de segurança cibernética?

48	A quantidade de integrantes da ETIR é suficiente para tratar de todas as responsabilidades de sua competência?
49	Existe trilha específica de capacitação para equipe da ETIR?
50	A trilha de capacitação está em andamento pela equipe da ETIR?
51	Foram definidas métricas para medição da eficácia das medidas de segurança da informação dentro da organização?
52	As métricas definidas para medição da eficácia das medidas de segurança são testadas e validadas continuamente?
53	Campanhas formais de consciêntização em segurança cibernética são realizadas contínuamente?
54	O nível de conhecimento sobre segurança cibernética da instituíção é medido regularmente?
55	A organização tem buscado investir em soluções automatizadas de segurança cibernética?
56	A organização possui processo formalizado e instituído para orientar a recuperação e o reestabelecimento dos serviços afetados?
57	A gestão de incidentes de segurança cibernética é realizada por meio de processo definido e constituído formalmente?
58	As fases de detecção, triagem, análise e resposta aos incidentes de segurança cibernética estão definidos e constituídos formalmente?
	Boas práticas da ETIR
59	Existe ETIR formalmente instituída na organização?
60	A ETIR está vinculada no organograma institucional à Secretaria de Tecnologia da Informação?
61	A ETIR está vinculada no organograma institucional à Diretoria Geral?
62	O funcionamento da ETIR está definido em documento formal da instituíção, publicado em sítio eletrônico do órgão?
63	No documento de constituíção da ETIR estão definidas a missão, público-alvo, modelo de implementação, autonomia, integrantes, canal de comunicação e serviços?
64	As funções de preparação, identificação, contenção, erradicação, recuperação e lições aprendidas estão definidas e os procedimentos estabelecidos em documento específico da organização?
65	A ETIR possui ações e procedimentos definidos para responder e notificar os incidentes de segurança?
66	A Organização possui normativo com a indentificação da cadeia de comando em situação de crise?
67	A Organização possui normativo ou procedimento definido para capacitar e educar usuários em segurança cibernética?
68	A Organização possui normativo ou procedimento definido para capacitar e educar os responsáveis segurança cibernética?
69	A equipe da ETIR está devidamente capacitada para identificar um possível ataque cibernético em curso?

70	A equipe da ETIR possui o ferramental necessário para identificar um possível ataque cibernético em curso?
71	A equipe da ETIR possui os acessos, permissões e capacidade necessárias para identificar um possível ataque cibernético em curso?
72	Existe na organização processo mapeado, implementado e formalmente publicado para diagnóstico e triágem de incidentes cibernéticos?
73	Existe na organização processo mapeado, implementado e formalmente publicado para avaliação do impacto de incidentes cibernéticos?
74	Existe na organização processo mapeado, implementado e formalmente publicado para restauração e recuperação do ambiente em caso de incidente cibernético?
75	Existe na organização processo mapeado, implementado e formalmente publicado para contenção e erradicação de incidente cibernético?

6.2. Para consecução, implementação e execução das ações e procedimentos definidos, foi estabelecido o seguinte cronograma:

Status	Nível de Conformidade	Prazo para atendimento	Medições	Observações
Atual	**37,84%**		**37,84%**	**Medição inicial – Mai/2023**
1ª Evolução	58,56%	Set/2024	**64,29%**	**Análise em Jul/2024**
2ª Evolução	79,28%	Jun/2025	**79,72%**	**Análise em Jan/2025**
3ª Evolução	100%	Dez/2025		

7. REFERÊNCIAS

- DECRETO Nº 10.222, de 5 DE FEVEREIRO DE 2020, que aprovou a Estratégia Nacional de Segurança Cibernética, E-Ciber.
- Decreto nº 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação.
- Lei nº 12.527, de 18 de novembro de 2011.
- Lei nº 12.965, de 23 de abril de 2014.
- Lei nº 13.709, de 14 de agosto de 2018.
- Portaria CNJ nº 162, de 10 de junho de 2021.
- Portaria CNJ nº 46, de 10 de fevereiro de 2022.
- Portaria nº 93, de 26 de setembro de 2019, do Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República, a qual aprova o Glossário de Segurança da Informação.

- Relatório TCU: TC 001.873/2020-2 - levantamento objetivando conhecer a macroestrutura de governança e gestão de segurança da informação e de segurança cibernética na Administração Pública Federal (APF).
- Resolução CNJ nº 396, de 07 de junho de 2021.
- Resolução CNJ nº 370/2021, de 28 de janeiro de 2021.