CSIN

Coordenadoria de Segurança da Informação

12.05.2023

Bom dia!

ENSEC-PJ

Res. CNJ 396/2021 - Institui a Estratégia Nacional de Segurança Cibernética do PJ

RES. CNJ nº 396/2021
ENSEC-PJ

Art. 1º

Instituir a **Estratégia Nacional** de **Segurança da Informação** e **Cibernética** do Poder Judiciário...

Art. 4º

A **visão** da ENSEC-PJ consiste em **alcançar a excelência em segurança cibernética** no Poder Judiciário.

RES. CNJ nº 396/2021
ENSEC-PJ

Art. 6º São objetivos da ENSEC-PJ:

I – tornar o Judiciário **mais seguro e inclusivo no ambiente digital;**

II – aumentar a resiliência às ameaças cibernéticas;

III – estabelecer governança de segurança cibernética e fortalecer a gestão e coordenação integrada de ações de segurança cibernética nos órgãos do Poder Judiciário; e

IV – permitir a **manutenção e a continuidade dos serviços**, ou o seu restabelecimento em menor tempo possível.

RES. CNJ nº 396/2021

*Art. 20

Cada órgão do Poder Judiciário, com exceção do STF, deverá constituir Comitê de **Governança** de **Segurança da Informação** (CGSI) , ao qual caberá:

I – **assessorar** a **alta administração** do órgão do Poder Judiciário em **todas as questões** relacionadas à **segurança da informação**;

II – propor alterações na política de segurança da informação e **deliberar sobre** assuntos a ela relacionados, incluindo atividades de **priorização de ações e gestão de riscos de segurança**;

III – propor **normas internas** relativas à segurança da informação;

IV – **constituir grupos de trabalho para tratar de temas** e propor **soluções específicas** sobre segurança da informação; e

V – **consolidar e analisar os resultados** dos trabalhos **de auditoria** sobre a gestão da segurança da informação.

*** Art. 3º Port. SGP/CSIN 382/2023**

RES. CNJ nº 396/2021
ENSEC-PJ

Art. 21

Cada órgão do Poder Judiciário, com exceção do STF, deverá constituir estrutura de **segurança da informação, subordinada diretamente à alta administração** do órgão e **desvinculada** da área de **TIC.**

Port. CNJ 162

Protocolos, Manuais e Glossário

Port. CNJ 162

- Art. 1º Aprovar os Anexos I, II e III desta Portaria, que contêm os seguintes protocolos:
  - Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ)
  - Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCC-PJ)
  - Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ)

Port. CNJ 162

- Art. 2º Aprovar os Anexos IV, V, VI e VII desta Portaria, que contêm os seguintes Manuais:
  - IV - Proteção de Infraestruturas Críticas de TIC;
  - V - Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital;
  - VI - Gestão de Identidades; e
  - VII - Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário.
- Art. 3º Aprovar o glossário de termos técnicos, constantes do Anexo VIII ...

2.
Estratégia

Portarias CSIN/TRT 971, 972, 973, 974, 3358 e 3359

Implementações

- Protocolo de Investigação de Ilícitos Cibernéticos (Port. 971)
- Protocolo de Prevenção de Incidentes Cibernéticos (Port. 973)
- Protocolo de Gerenciamento de Crises Cibernéticas (Port. 974)
- Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética - ETIR (Port. 972)
- Disciplina a Adoção dos Manuais da ENSEC-PJ (Port. 3358)
- Diretrizes para Gestão de Incidentes de Segurança da Informação (Port. 3359)

Port. 3358/22

- Proteção de infraestruturas críticas de TIC (**153***) - **CIS v8**
- Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital (**46***)
- Gestão de Identidade e Controle de Acessos (**23***)
- Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário (**04***)

*** medidas de segurança**

Port. 3358/22

- **Capítulo VI -** Da evolução da maturidade na adoção dos manuais

Grau de Implementação	Escala	Pontos
Não Implementado	**0% a 24,9%**	**0,00**
Implementado em menor parte	**25% a 49,9%**	**0,25**
Implementado parcialmente	**50% a 74,9%**	**0,50**
Implementado em maior parte	**75% a 99,9%**	**0,75**
Implementado totalmente	**100%**	**1,00**

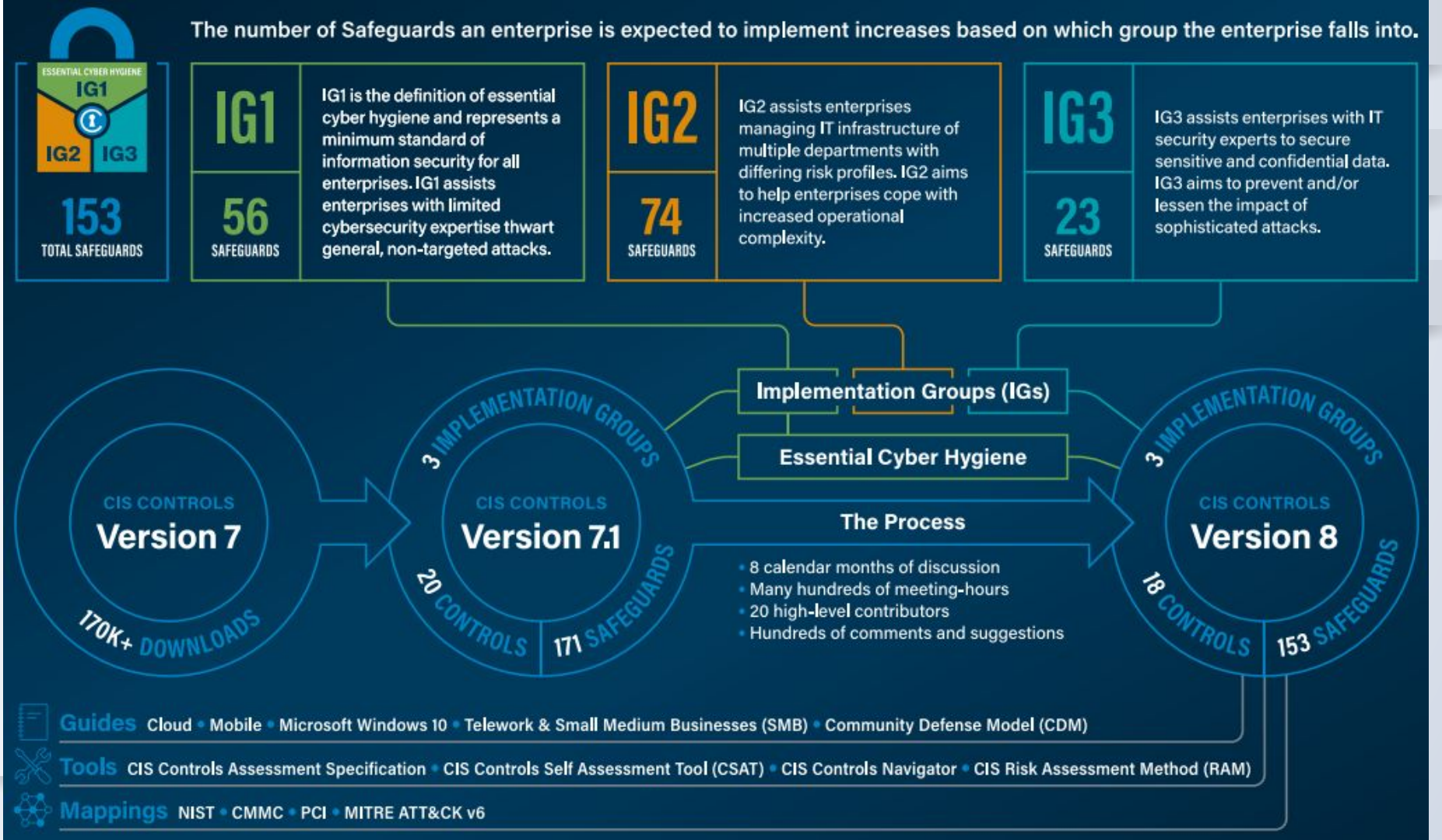
CIS – CONTROLS

Center for Internet Security - Critical Security Controls for Effective Cyber Defense

CIS Controls

É um conjunto **prescritivo**, **priorizado** e simplificado de práticas recomendadas para **fortalecer** a **postura** de **segurança cibernética**.

Foco nas **etapas mais importantes** para defesa contra **ataques cibernéticos reais**.


The number of Safeguards an enterprise is expected to implement increases based on which group the enterprise falls into.
ESSENTIAL CYBER HYGIENE
IG1
IG2
IG3
153
TOTAL SAFEGUARDS
IG1
56
SAFEGUARDS
IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.
IG2
74
SAFEGUARDS
IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.
IG3
23
SAFEGUARDS
IG3 assists enterprises with IT security experts to secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.
Implementation Groups (IGs)
Essential Cyber Hygiene
CIS CONTROLS
Version 7
170K+ DOWNLOADS
3 IMPLEMENTATION GROUPS
CIS CONTROLS
Version 7.1
20 CONTROLS
171 SAFEGUARDS
The Process
8 calendar months of discussion
Many hundreds of meeting-hours
20 high-level contributors
Hundreds of comments and suggestions
3 IMPLEMENTATION GROUPS
CIS CONTROLS
Version 8
18 CONTROLS
153 SAFEGUARDS
Guides Cloud • Mobile • Microsoft Windows 10 • Telework & Small Medium Businesses (SMB) • Community Defense Model (CDM)
Tools CIS Controls Assessment Specification • CIS Controls Self Assessment Tool (CSAT) • CIS Controls Navigator • CIS Risk Assessment Method (RAM)
Mappings NIST • CMMC • PCI • MITRE ATT&CK v6

CIS Critical Security Controls

Versão 8

01 - Inventário e controle de ativos corporativos

02 - Inventário e controle de ativos de software

03 - Proteção de dados

04 - Configuração segura de ativos corporativos e software

05 - Gestão de Contas

06 - Gestão do controle de acesso

07 - Gestão contínua de vulnerabilidades

08 - Gestão de registros de auditoria

09 - Proteção de e-mail e navegador Web

10 - Defesas contra de malware

11 - Recuperação de dados

12 - Gestão da infraestrutura de rede

13 - Monitoramento e defesa de Rede

14 - Conscientização sobre segurança e treinamento de competências

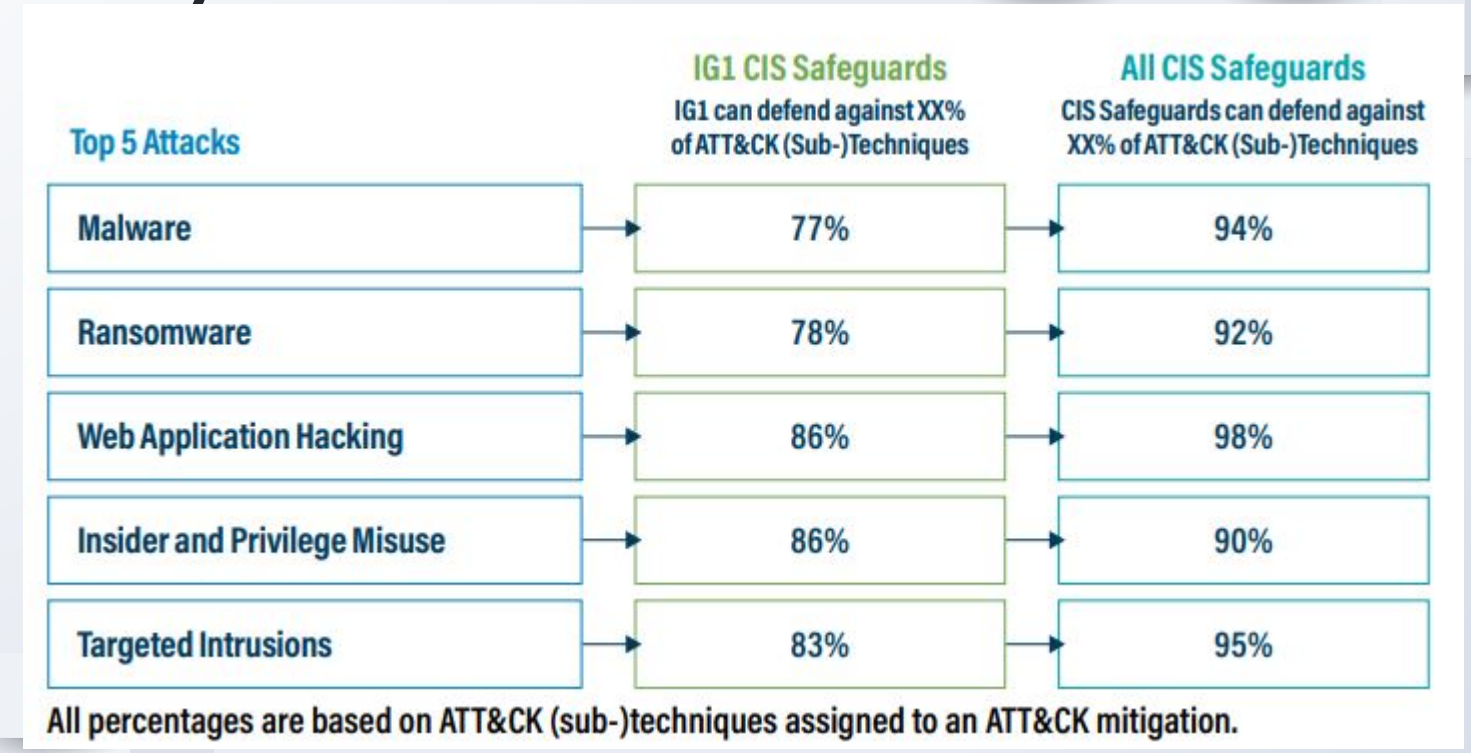
15 - Gestão de provedor de serviços

16 - Segurança de aplicações

17 - Gestão de respostas e incidentes

18 - Testes de invasão

CIS - CDM
Community Defense Model



3.

Status dos Planos

Protocolos de Segurança Cibernética
Adoção dos Manuais da ENSEC-PJ
Recomendações de Auditoria

Plano para Implementação de Protocolos de Segurança Cibernética

82%

Plano de Adoção de Manuais de Referência da ENSEC-PJ

93%

Maturidade nos MANUAIS

Portaria CNJ 162/2021 e Port. TRT18 3358/2022

Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital

63,7%

Gestão de Identidade e Controle de Acessos

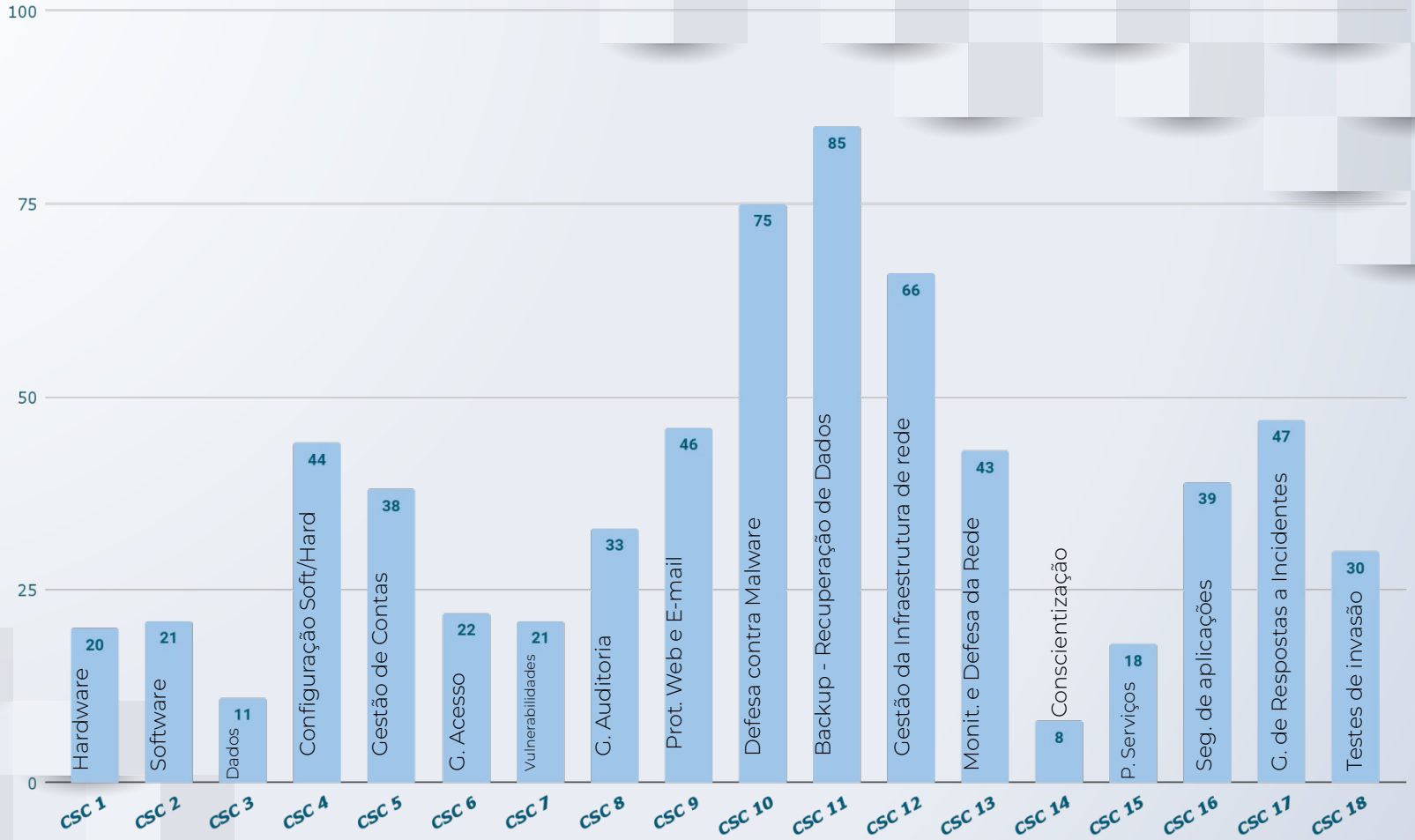
50%

Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário

43,8%

Proteção de Infraestruturas Críticas de TIC

CIS v8



36%

Proteção de Infraestrutura Crítica de TIC

Linha de Base e de Plano de Metas

Doc.051 PA-14287/2022

	Linha de Base - 2022	Meta 2023	Meta 2024	Meta 2025/2026
Grau de Implementação do Manual de Referência Anexo IV Port CNJ 162/2021 - medidas de segurança para **proteção de infraestruturas críticas de TIC**	**36%**	**53%**	**70%**	**87%**
Grau de Implementação do Manual de Referência Anexo V Port CNJ 162/2021 - **Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital**	**63,7%**	**75,4%**	**79,9%**	**92,5%**
Grau de Implementação do Manual de Referência Anexo VI Port CNJ 162/2021 - **Gestão de Identidade e Controle de Acessos**	**50%**	**62%**	**81%**	**93%**
Grau de Implementação do Manual de Referência Anexo VII Port CNJ 162/2021 - **Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário**	**43,8%**	**62,5%**	**75,0%**	**81,3%**

4.
Filas PDTIC 2023

Ação - fila Infra/Servidores de Aplicação	Unidade Solicitante	Prazo	Pontuação
2023.NS22 - Estabelecer e manter o inventário detalhado de ativos corporativos - IG1 escopo servidores de aplicação	Segurança da Informação	Prazo: 05/23 - 06/23	415
2021.NS22 - Estabelecer processos de Gerenciamento de Capacidade e Disponibilidade ****PA 8791/2017 Auditoria de Conformidade na área de STIC do TRT18ª, conforme previsão constante do Plano Anual de Auditorias para o ano de 2017, considerando a necessidade de atender a exigência disposta nos artigos 14 e 17, § 2º, da Resolução nº 171, de 1º de março de 2013, do CNJ.** **Esse item foi solicitado em questionários do IGOV-TIC para melhoria da nota e faz parte do PA 2247/2023 Plano de ação para os achados de Auditoria do CSJT 15152/2020.**	Infraestrutura de TIC	De: 03/23 - 08/23 Para: 07/23 - 12/23	1269
2023.NS09 - Implantar o Processo de Gerenciamento de Evento ****PA 6746/2018 Ação Coordenada do Conselho Nacional de Justiça sobre "Governança, Gestão, Riscos e Controle de Tecnologia da Informação e Comunicação".** ****PA 2247/2023 Plano de ação para os achados de Auditoria do CSJT 15152/2020, para implantação desse projeto até 06/24.**	Infraestrutura de TIC	De: 09/23 - 02/24 Para: 01/24 - 06/24 Backlog, próximo da fila	338

Ação - fila Infra/Redes	Unidade Solicitante	Prazo	Pontuação
2021.NS41 - Implantar links de dados nas Varas de Trabalho no interior (Rede JT)	Infraestrutura de TIC	Prazo: 03/23 - 04/23	1484
2023.NS21-Estabelecer e manter o inventário detalhado de ativos corporativos - IG1 escopo redes	Segurança da Informação	Prazo: 05/23 - 06/23	415
2021.NS19 - Implantar os controles da matriz de riscos originados do Plano de Gestão de Riscos de TIC com escopo em Redes para o PCSTIC	Infraestrutura de TIC	De: 05/23 - 08/23 Para: 07/23 - 10/23	1476
2021.NS26 - Implementar IPv6 para viabilizar sistema autônomo e link redundante ** item para melhoria da nota no IGOV-TIC 2023	Infraestrutura de TIC	De: 09/23 - 12/23 Para: 11/23 - 02/24	1392

Ação - fila Infra/Voz e Vídeo	Unidade Solicitante	Prazo	Pontuação
2023.NS20-Estabelecer e manter o inventário detalhado de ativos corporativos - IG1 escopo voz e vídeo	Segurança da Informação	Prazo: 05/23 - 06/23	415
2023.NS07 - Contratar módulo de call center e realizar estudo para migração do núcleo de gerência para nuvem	Infraestrutura de TIC	De: 05/23 - 08/23 Para: 07/23 - 10/23	392

Obrigado!

Perguntas?

Contatos:

- #5822
- segurança.informação@trt18.jus.br
- vinicius.elias@trt18.jus.br