PODER JUDICIÁRIO FEDERAL
JUSTIÇA DO TRABALHO
Tribunal Regional do Trabalho da 9.ª Região

MARCUS AURELIO LOPES 14/06/2024 TRT9

Vetor: Comitê de Segurança da Informação e Proteção de Dados (CSIPD) (N° 284029)

Ata/Pauta - 07.06.2024 - 1ª Reunião ordinária do Comitê de Segurança da Informação e Proteção de Dados (CSIPD) (ID 10478014)

Agendamento (ID 10478015)

Data: 07/06/2024
Horário: 10:30
Reunião Extraordinária: Não
Convidados:

MARCUS AURELIO LOPES - COORDENADOR - Desembargador(a), indicado(a) pela Presidência do Tribunal - SUPLENTE LUIZ EDUARDO GUNTHER

ANGÉLICA CÂNDIDO NOGARA SLOMP - VICE-COORDENADOR - Encarregado(a) pelo tratamento de dados pessoais - SUPLENTE SIMONE GALAN DE FIGUEIREDO

SANDRO ALENCAR FURTADO - MEMBRO TITULAR - DIRETOR-GERAL - DIRETORIA-GERAL

EDUARDO SILVEIRA ROCHA - MEMBRO TITULAR - SECRETÁRIO - SECRETARIA GERAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES

DANIEL VICENTE THOMAZ - MEMBRO TITULAR - SECRETÁRIO - SECRETARIA DE DESENVOLVIMENTO DE SOLUÇÕES

ALEXANDRE TETSUO YAMAUCHI - MEMBRO TITULAR - SECRETÁRIO - SECRETARIA DE INFRAESTRUTURA E OPERAÇÕES

YONARA YOKO POZZOLO - MEMBRO TITULAR - SECRETÁRIO - SECRETARIA GERAL JUDICIÁRIA

PAULO ROBERTO NUNES - MEMBRO TITULAR - COORDENADOR - COORDENADORIA DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

MARIA ROSICLER CRETELLA - MEMBRO TITULAR - SECRETÁRIO - SECRETARIA GERAL DA PRESIDÊNCIA

ILSE REGINA VIANA RAMOS BACELLAR - MEMBRO TITULAR - ASSESSOR - ASSESSORIA JURÍDICA DA PRESIDÊNCIA

DÉBORA GNATA BALECHE PROENÇA - MEMBRO TITULAR - CHEFE DA DIVISÃO DE OUVIDORIA

MARCUS AURELIO LOPES 14/06/2024 TRT9

Local da reunião: Telepresencial
Participantes:

MARCUS AURELIO LOPES - COORDENADOR - Desembargador(a), indicado(a) pela Presidência do Tribunal

LUIZ EDUARDO GUNTHER - SUPLENTE DO COORDENADOR - Desembargador(a), indicado(a) pela Presidência do Tribunal

ANGÉLICA CÂNDIDO NOGARA SLOMP - VICE-COORDENADOR - Encarregado(a) pelo tratamento de dados pessoais

EDUARDO SILVEIRA ROCHA - MEMBRO TITULAR - SECRETÁRIO - SECRETARIA GERAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES

DANIEL VICENTE THOMAZ - MEMBRO TITULAR - SECRETÁRIO - SECRETARIA DE DESENVOLVIMENTO DE SOLUÇÕES

ALEXANDRE TETSUO YAMAUCHI - MEMBRO TITULAR - SECRETÁRIO - SECRETARIA DE INFRAESTRUTURA E OPERAÇÕES

YONARA YOKO POZZOLO - MEMBRO TITULAR - SECRETÁRIO - SECRETARIA GERAL JUDICIÁRIA

PAULO ROBERTO NUNES - MEMBRO TITULAR - COORDENADOR - COORDENADORIA DE GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

ILSE REGINA VIANA RAMOS BACELLAR - MEMBRO TITULAR - ASSESSOR - ASSESSORIA JURÍDICA DA PRESIDÊNCIA

DÉBORA GNATA BALECHE PROENÇA - MEMBRO TITULAR - CHEFE DA DIVISÃO DE OUVIDORIA

Convidados:

JAIME BRITTO - NÚCLEO DE APOIO AOS COLEGIADOS TEMÁTICOS

DANIEL ADRIANO PINTO DA SILVA - COORDENADOR • COORDENADORIA DE GOVERNANÇA DE TIC

OESLEI TABORDA RIBAS - CHEFE DE SEÇÃO • SEÇÃO DE OPERAÇÃO DA SEGURANÇA DA INFORMAÇÃO

FRANCISCO RIEDI - CHEFE DE SUBSEÇÃO • COORDENADORIA DE GOVERNANÇA DE TIC

ANA ROSA GOSLAR - REPRESENTANTE DO COMITE DE DOCUMENTAÇÃO E MEMÓRIA

Link da reunião gravada: https://drive.google.com/file/d/1wk8bkZmRgNi6idi5gHYkSqT8ttIaAQ3G/view

Itens da reunião (ID 10478023)

Item 1 (ID 10478024)

Nome do item: 1) Abertura e organização dos trabalhos do Comitê
Descrição:

O Sr. Paulo apresentou a forma de acesso ao chat de discussões do espaço e a forma de acesso ao conteúdo dos documentos do Comitê.

- Espaço de discussões: https://mail.google.com/mail/u/0/?tab=rm&ogbl#chat/space/AAAAzc8otzA
- Espaço de documentos: https://drive.google.com/drive/folders/0AIRhMyy-y5mWUk9PVA

O Desembargador Marcus solicitou que o espaço virtual seja utilizado para otimizar as discussões prévias e propostas para as deliberações.

Deliberação:

Nenhuma deliberação sobre esse item, apenas pra ciência dos integrantes do Comitê.

Item 2 (ID 10837596)

Nome do item: 2) Aprovação de políticas e atos de Segurança da Informação
Descrição:

O Sr. Paulo apresentou uma explicação das propostas do item 2.

2.1) Atualização da Política de Segurança da Informação que institui a Política de Segurança da Informação (PSI) e o Sistema de Gestão de Segurança da Informação (SGSI) no âmbito do Tribunal Regional do Trabalho da 9ª Região.

Política de Segurança da Informação (PSI) https://docs.google.com/document/d/1MmDz-auSI9g3TaFMgAwAed7SuoLFXqJ5/edit?usp=drive_link&ouid=108788372426871979913&rtpof=true&sd=true

Sistema de Gestão de Segurança da Informação (SGSI) https://drive.google.com/file/d/1W5UylLKcdOP33P2zKcaTqf_A68VwSvoW/view?usp=drive_link

MARCUS AURELIO LOPES 14/06/2024 TRT9

Descrição: Trata-se da **atualização** da PSI e do SGSI n. 28/2018 aprovada na resolução administrativa 85/2018, considerando os normativos mais recentes.
A **política de segurança da informação (PSI)** é um documento oficial que define regras, práticas e responsabilidades para a proteção de dados e sistemas de informação de uma instituição. Seu objetivo principal é **minimizar os riscos de violações ou perdas de qualquer ativo de TI**, garantindo a confidencialidade, integridade e disponibilidade da informação. Já o **Sistema de Gerenciamento de Segurança da Informação (SGSI)** é um conjunto de processos e procedimentos organizados para proteger a informação de uma organização.

2.2) Atualização da Política de Backup e Retenção de Dados que instituiu a Política de backup e restauração de dados no âmbito do Tribunal Regional do Trabalho da 9ª Região.

https://docs.google.com/document/d/1YewF9T6pXfAsfC0ss0klJBqdOfBy38tz/edit?usp=drive_link&ouid=108788372426871979913&rtpof=true&sd=true

Descrição: Trata-se da **atualização** da política 14/2017 que definiu os procedimentos para backup e restauração de dados da organização, visando garantir a confidencialidade, integridade, disponibilidade e recuperação dos dados em caso de falhas, sinistros ou outros eventos que possam comprometer a operação da organização. A nova política possui **parâmetros mínimos de backup e tempos de retenção** essenciais para instruir a contratação da solução de backup prevista para esse ano.

Sobre esse item, após explanação do Sr. Paulo, o Sr. Eduardo expôs e respondeu detalhes sobre a motivação e importância da aprovação e encaminhamento desta política.

2.3) Atualização do Ato que dispõe sobre a instituição e o funcionamento da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) no âmbito do Tribunal Regional do Trabalho da 9ª Região.

https://docs.google.com/document/d/15HU6IYiBQtCLYWY7MHjDQpovbEr1Uyoc/edit?usp=drive_link&ouid=108788372426871979913&rtpof=true&sd=true

Descrição: Trata-se da **atualização** do ato n. 132, de 30 de setembro de 2021 considerando os normativos mais recentes. A ETIR, CSIRT-TRT9 (sigla usada no TRT da 9ª Região), é composta por especialistas da área de Tecnologia da Informação e tem como missão planejar, coordenar e executar atividades de tratamento e resposta a incidentes em redes computacionais, receber e notificar

qualquer evento adverso à segurança da informação, confirmado ou sob suspeita, relacionado às redes de computadores, preservando os dados, as informações e a infraestrutura do Tribunal Regional do Trabalho da 9ª Região.

Sobre esse item, foi explicado pelo Sr. Paulo o funcionamento da ETIR e destacado o atendimento aos protocolos: "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)." .

2.4) Criação do Subcomitê de Crises Cibernéticas, no âmbito do Tribunal Regional do Trabalho da 9ª Região, conforme item 4.2 da portaria CNJ 162/21 do "Protocolo Gerenciamento de Crises Cibernéticas do Poder Judiciário" com definição da sala de situação.

https://docs.google.com/document/d/1YZwFLKxRwWb91_KFwYGMtWRQWqzYzi-C/edit?usp=drive_link&ouid=108788372426871979913&rtpof=true&sd=true

Descrição: Considerado o incidente como crise cibernética, o Subcomitê de Crise deverá ser acionado, nos termos do Protocolo de Gerenciamento de Incidentes e de Crises Cibernéticas. O gerenciamento de crise se inicia quando: a) ficar caracterizado grave dano material ou de imagem; b) restar evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses; c) o incidente impactar a atividade finalística ou o serviço crítico mantido pela organização; ou d) o incidente atrair grande atenção da mídia e da população em geral.

Sobre esse item , após explanação pelo Sr. Paulo, o Desembargador Marcus questionou sobre a quantidade de pessoas integrantes no Subcomitê de Crises Cibernéticas. Na sequencia o Sr. Eduardo e o Sr. Daniel Thomaz explicaram a importância da participação e representação da Alta Administração neste Subcomitê.

Deliberações:

Sobre o item 2.1) Atualização da Política de Segurança da Informação que institui a Política de Segurança da Informação (PSI) e o Sistema de Gestão de Segurança da Informação (SGSI) no âmbito do Tribunal Regional do Trabalho da 9a Região. Não houve objeções e foi aprovado pelo Comitê para encaminhamento à Presidência.

Sobre o item 2.2) Atualização da Política de Backup e Retenção de Dados que instituiu a Política de backup e restauração de dados no âmbito do Tribunal Regional do Trabalho da 9a Região, o Comitê deliberou pela aprovação da política pelo Comitê e seu encaminhamento à Presidência.

Sobre o item 2.3) Atualização do Ato que dispõe sobre a instituição e o funcionamento da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) no âmbito do Tribunal Regional do Trabalho da 9a Região, a minuta do ato foi aprovada pelo Comitê, que propôs seu encaminhamento à Presidência.

Sobre o item 2.4) Criação do Subcomitê de Crises Cibernéticas, no âmbito do Tribunal Regional do Trabalho da 9a Região, conforme item 4.2 da portaria CNJ 162 /21 do “Protocolo Gerenciamento de Crises Cibernéticas do Poder Judiciário” com definição da sala de situação, o Comitê (CSIPD) deliberou pela aprovação da minuta do ato do Subcomitê de Crises Cibernéticas, que propôs seu encaminhamento à Presidência.

Anexo 2.1: Download: Nova Política de Segurança da Informação.pdf
Anexo 2.2: Download: Nova Política de Backup e Restauração de Dados_16052024.pdf
Anexo 2.3: Download: Novo Ato da ETIR TRT9_jun_2024 .pdf
Anexo 2.4: Download: Novo Ato do Comite de crises cibernéticas.pdf
Anexo 2.1 - SGSI: Download: Macroprocesso - Sistema de Gestão da Segurança da Informação (SGSI) - 2024 (1).pdf

Item 3 (ID 10837610)

Nome do item: 3) Assuntos relacionados à LGPD
Descrição:

A Dra. Angélica e o Sr. Jaime apresentaram as questões referente ao item 3) Assuntos relacionados à LGPD, sendo:

3.1) Vetor nº 315548 Requisição de Serviço - Demanda de Proteção de Dados Pessoais - Solicitações relacionadas à LGPD - e-mail Ouvidoria recebido em 04/03/2024
https://intranet.trt9.jus.br/intranet2/f?p=396:41::::RP,41:P41_CD_TB_PROCESSO,P41_CD_TB_VALOR:315548,10491310

Descrição: Por meio de mensagem eletrônica, enviada em 04 de março de 2024, a Divisão de Ouvidoria encaminhou solicitação, em que requer, mais uma vez, a exclusão do seu nome de consultas através do Google, que aparecem no jus Brasil.

Resumo do Despacho da Dra. ANGÉLICA CÂNDIDO NOGARA SLOMP - Juíza Auxiliar da Presidência, Encarregada de Dados: “6) Considerando que os questionamentos são os mesmos e que não houve alteração no cenário legal, permanece o entendimento já exarado, no sentido de que: a) as informações processuais publicadas na Internet, com o nome da parte, têm origem nos próprios tribunais e ocorrem a partir de determinações contidas em diversos dispositivos legais e normativos dos órgãos de controle; b) a divulgação do nome da parte não viola as disposições da LGPD; c) os mecanismos ou serviços de busca de informações processuais indicados reproduzem informações divulgadas pelos tribunais, ou seja, são públicas; e d) qualquer divergência a respeito do modo a informação é publicada pelos mecanismos ou serviços de busca não pode ser solucionada pela Justiça do Trabalho, porque lhe falta competência material para tanto. 7) Neste contexto, INDEFIRO o requerimento postulado. 8) Não obstante, diante das considerações feitas pela requerente, encaminhe-se para ciência do Comitê de Segurança da Informação e Proteção de Dados (CSIPD), para conhecimento e eventuais ações que considerar cabíveis. 9) Ciência à requerente, à Unidade de Apoio Executivo - UAE do Comitê de Segurança da Informação e Proteção de Dados (CSIPD) e à Ouvidoria. 9) Arquive-

se.”

Despacho completo em https://intranet.trt9.jus.br/intranet2/f?p=396:41::::RP,41:P41_CD_TB_PROCESSO,P41_CD_TB_VALOR:315548,10491310

Após discussões e considerações sobre esse tema, a Sra. Débora, representante da Ouvidoria, questionou sobre o procedimento do envio e resposta dos expedientes similares e recorrentes recepcionados pela Ouvidoria sobre o tema.

Sobre o questionamento da Sra. Débora da Ouvidoria, o Desembargador Marcus e a Dra. Angélica destacaram que todos os expedientes em relação à LGPD sejam sempre demandados para a Dra. Angélica (Encarregada pela Proteção de Dados Pessoais, que atua como coordenadora do GT-LGPD), por intermédio do escritório de privacidade, conforme o fluxo de tratamento já definidos com a Ouvidoria e que o escritório de privacidade também dê ciência prévia ao Desembargador Marcus (Coordenador do Comitê CSIPD) através de sua unidade de Apoio Executivo – UAE do Comitê de Segurança da Informação e Proteção de Dados (CSIPD).

O Comitê concordou com o despacho da Dra. ANGÉLICA CÂNDIDO NOGARA SLOMP - Juíza Auxiliar da Presidência, Encarregada de Dados feito no processo Vetor 315548 e recomendou ao GT-LGDP, que estude e proponha mecanismos de rastreamento de acessos às bases do Tribunal por terceiros.

3.2) Vetor nº 315289 Requisição de Serviço - Demanda de Proteção de Dados Pessoais - Solicitações relacionadas à LGPD - Convênio com a SPC Brasil.

https://intranet.trt9.jus.br/intranet2/f?p=396:41::::RP,41:P41_CD_TB_PROCESSO,P41_CD_TB_VALOR:315289,10477679

Descrição: Assunto: Convênio/termo de cooperação técnica para acesso ao SPC JUD, a fim de que magistrados e servidores possam consultar as informações e funcionalidades do SPC Brasil, mediante cadastro, login e senha.

Despacho da Dra. ANGÉLICA CÂNDIDO NOGARA SLOMP - Juíza Auxiliar da Presidência, Encarregada de Dados: 1) Importante esclarecer que o Comitê Gestor de Proteção de Dados Pessoais teve as as suas atribuições absorvidas pelo Comitê de Segurança da Informação e Proteção de Dados (CSIPD), através do ATO n° 118, de 06 de Setembro de 2022, cujas atribuições, dentre outras é a de "apoiar o Encarregado pelo tratamento de dados pessoais na implantação de Programa de Privacidade dos Dados com base na LGPD" e "realizar estudos internos acerca da Lei Geral de Proteção de Dados e seus impactos no Tribunal, produzindo e apresentando à Presidência relatório detalhado com as ações sugeridas, para direcionamento"; 2) O Art. 41, § 2º, da LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, definem quais são as atribuições do Encarregado de Dados, conforme segue: "*As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.*" 3) Informa-se que a Portaria Presidência nº 21, de 26 de fevereiro de 2024, nomeou a Juíza ANGÉLICA CÂNDIDO

NOGARA SLOMP, como sendo a Juíza Encarregada pelo Tratamento de Dados Pessoais, tendo como suplente a Juíza SIMONE GALAN DE FIGUEIREDO; 4) Diante da complexidade da questão apresentada pela Ordenadoria da Despesa - ODESP, através do seu Despacho nº 62/2024, encaminho o presente requerimento para análise do coordenador do Comitê de Segurança da Informação e Proteção de Dados (CSIPD), Desembargador Marcus Aurélio Lopes, para que convoque reunião extraordinária do colegiado ou acione o Grupo de Trabalho Técnico da LGPD (GT-LGPD), conforme entender mais adequado, para apoio no encaminhamento do caso em tela. 5) Notifique-se a Unidade de Apoio Executivo - UAE do Comitê de Segurança da Informação e Proteção de Dados (CSIPD), a ODESP, a ASSEJUR e Coordenadoria de Conciliação e de Apoio Permanente à Execução de Curitiba."

MARCUS AURELIO LOPES 14/06/2024 TRT9

Após discussões e considerações sobre esse item, o Desembargador Marcus destacou 3 pontos fundamentais: 1) utilidade (necessidade e possibilidade). O que o TRT vai fazer com esses dados? 2) Qual o risco de vazamento de dados sensíveis por quem acessa essa base de dados pelo TRT? 3) Qual a responsabilidade do TRT perante o SPC e donos dos dados sobre os danos decorrentes de possíveis vazamentos? Segundo o Desembargador Marcus, o acesso à essa base de dados do SPC não trará melhorias diretas e impacto significativo em nossa prestação judicial. Por conta do risco alto de mal uso das informações, da dificuldade de treinar todas as pessoas sobre os cuidados com os dados que terão acesso e o risco de vazamento de dados de terceiros, propôs recomendar **não firmar** o Convênio. Segundo a Dra. Angélica, os principais dados que o TRT teria acesso podem ser acessados através de outros convênios que o TRT já possui, concordando com a recomendação do Desembargador Marcus.

3.3) LGPD - Situação dos projetos do Programa de Privacidade - Jaime

Sobre esse item, o Sr. Jaime expôs as dificuldades da implantação dos projetos relacionados à LGPD neste TRT, apesar de estarmos bem pontuados nacionalmente neste tema. Destacou que já existe o grupo de trabalho formalizado junto ao Comitê (GT-LGPD) mas necessita-se melhorar o apoio e suporte à Coordenadora deste grupo, Dra. ANGÉLICA CÂNDIDO NOGARA SLOMP - Juíza Auxiliar da Presidência, Encarregada de Dados.

Desta forma, sugeriu-se a formalização/oficialização da Unidade do Escritório de Privacidade de Dados com a definição das devidas atribuições, competências e responsabilidades.

Deliberações:

Sobre o item 3.1) Vetor no 315548 Requisição de Serviço - Demanda de Proteção de Dados Pessoais - Solicitações relacionadas à LGPD - e-mail Ouvidoria recebido em 04/03/2024

Sobre o questionamento da Sra. Débora da Ouvidoria, foi deliberado que todos os expedientes em relação à LGPD recepcionados pela Ouvidoria sejam sempre demandados para a Dra. Angélica (Encarregada pela Proteção de Dados Pessoais, que atua como coordenadora do GT-LGPD), por intermédio do escritório de privacidade, conforme o fluxo de tratamento já definidos e que o escritório de privacidade também dê ciência prévia ao Desembargador Marcus (Coordenador do Comitê CSIPD) através de sua unidade de Apoio Executivo – UAE do Comitê de Segurança da Informação e Proteção de Dados (CSIPD). Sobre os demais assuntos, o Comitê concordou com o despacho da Dra. ANGÉLICA CÂNDIDO NOGARA SLOMP - Juíza Auxiliar da Presidência, Encarregada de Dados feito no processo Vetor 315548 e recomendou ao GT-LGDP, que estude e proponha mecanismos de rastreamento de acessos às bases do Tribunal por terceiros.

Sobre o item 3.2) Vetor no 315289 Requisição de Serviço - Demanda de Proteção de Dados Pessoais - Solicitações relacionadas à LGPD - Convênio com a SPC Brasil, o Comitê deliberou em recomendar à Presidência **não firmar** o Convênio com o SPC neste momento.

Sobre o item 3.3) LGPD - Situação dos projetos do Programa de Privacidade, o Comitê deliberou pelo encaminhamento à Presidência de proposta de formalização /oficialização da Unidade do Escritório de Privacidade de Dados com a definição das devidas atribuições, competências e responsabilidades.

Anexo 3.3.1: Download: Avaliação Implantação LGPD JT Dez_2023.pdf
Anexo 3.3.2: Download: Lgpd_resumo do plano de implantação.pdf

Item 4 (ID 10837714)

Nome do item: 4) Assuntos Gerais
Descrição:

4.1) Dar conhecimento da Portaria CNJ Presidência nº 140/2024. Implementação do método de autenticação do tipo Múltiplo Fator de Autenticação (MFA) como requisito funcional para acesso a sistemas judiciais sensíveis".
https://drive.google.com/file/d/1mPFAD2kkfsviqXYwFjluB2Cw6RwaGaAB/view?usp=drive_link

O Sr. Paulo expôs e deu conhecimento aos presentes sobre esse item. O Desembargador Marcus expôs sua preocupação sobre a utilização de celular pessoal para uso do Múltiplo Fator de Autenticação (MFA). Desta forma, foi dada a ciência ao Comitê e devido ser uma demanda do CNJ a ser atendida por todos os TRTs, a SGTIC já está coordenando as ações e soluções técnicas para atendimento à essa Portaria.

4.2) Ofício CDOM n. 02/2024

https://drive.google.com/file/d/1FDEdk_ys2YSkUWyjuPHN0TETOqTnF3xu/view?usp=drive_link

“I – orientar quanto aos procedimentos para classificação da informação e dos documentos e disponibilizar instrumentos necessários, de forma a subsidiar o trabalho das unidades do TRT, inclusive promovendo ações de capacitação aplicáveis;

II – auxiliar a unidade de tecnologia da informação responsável pela solução informatizada de gestão de documentos e informações para utilização dos instrumentos mencionados no inciso I deste artigo;”

RESOLUÇÃO ADMINISTRATIVA 45/2018 https://www.trt9.jus.br/basesjuridicas/resolucaoadministrativa.xhtml?id=2363977

O Desembargador Marcus deu ciência sobre a sua participação nas reuniões do Comitê de Documentação e Memória como ouvinte, e da participação como ouvinte, do Coordenador do Comitê de Documentação e Memória nas reuniões do Comitê de Segurança da Informação e Proteção de Dados (CSIPD).

4.3) Fechamento e pré-agendamento da próxima reunião.

O Sr. Paulo informou a sugestão do Desembargador Marcus sobre a data da próxima reunião do Comitê que está pré-agendada para ocorrer dia 25/10 as 10:30h.

Deliberações:

Sobre o item 4.1) Dar conhecimento da Portaria CNJ Presidência nº 140/2024. Implementação do método de autenticação do tipo Múltiplo Fator de Autenticação (MFA) como requisito funcional para acesso a sistemas judiciais sensíveis”, foi dada a ciência ao Comitê e informado que a SGTIC já está coordenando as ações e soluções técnicas para atendimento à essa Portaria.

Sobre o item 4.2) Ofício CDOM n. 02/2024, o Desembargador Marcus deu ciência sobre a participação do Comitê de Documentação e Memória nas reuniões Comitê de Segurança da Informação e Proteção de Dados (CSIPD) e vice-versa.

Sobre o item 4.3) Fechamento e pré-agendamento da próxima reunião, o Comitê tomou ciência sobre a data da próxima reunião, programada para ocorrer dia 25/10 as 10:30h.

Anexo 4.1: Download: SEI_1834303_Portaria_Presidencia_140 (3).pdf
Anexo 4.2: Download: Ofício CDOM 02-2024 - Ao Coordenador do Comitê LGPD (3).pdf

POLÍTICA n° 83, de 16 DE MAIO DE 2024.

*Institui a **Política de Segurança da Informação (PSI) e o Sistema de Gestão de Segurança da Informação (SGSI)** no âmbito do Tribunal Regional do Trabalho da 9ª Região.*

O DESEMBARGADOR DO TRABALHO, PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 9ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO:

- a Resolução nº 396, de 7 de junho de 2021, do Conselho Nacional de Justiça, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

- a Resolução nº 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

- a importância de se estabelecer objetivos, princípios e diretrizes de Segurança da Informação alinhados às recomendações constantes da norma NBR ISO/IEC 27002, que trata da segurança da informação;

- o Ato Presidência n° 118, de 06 de Setembro de 2022, que instituiu o Comitê de Segurança da Informação e Proteção de Dados (CSIPD);

- a Portaria Nº 162, de 10 de junho de 2021, do Conselho Nacional de Justiça, que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;

RESOLVE*, ad referendum* do Tribunal Pleno:

CAPÍTULO I
DAS DISPOSIÇÕES INICIAIS

Art. 1° Instituir a POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) e o SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI) no âmbito do Tribunal Regional do Trabalho da 9ª Região, que é complementada pelas demais normas institucionais internas que fazem referência à Segurança da Informação, a exemplo das seguintes:

I - Backup e restauração de dados;

II - Utilização da Rede de Dados sem Fio;

III - Gestão de Riscos;

IV - Gestão de Ativos de TIC;

V - Identidade Digital e Gerenciamento de Acessos aos recursos de TIC; e

VI - Utilização dos Recursos de TIC.

Art. 2º As diretrizes, normas e procedimentos de segurança da informação de que trata esta política aplicam-se a todos os usuários de informações e de recursos de tecnologia da informação do Tribunal.

Parágrafo único. Todos os usuários, no âmbito de suas atribuições e competências, são corresponsáveis pela segurança da informação e devem, para tanto, zelar pelo correto conhecimento, entendimento e cumprimento das diretrizes, normas, procedimentos e instruções integrantes desta PSI, devendo comunicar à Central de Serviços de TIC do Tribunal Regional do Trabalho da 9ª Região a respeito de qualquer indício de falha, incidente ou irregularidade de que tiver conhecimento.

Art. 3º Para os efeitos da PSI ficam estabelecidas as seguintes **conceituações** principais:

I - ADMINISTRADOR DOS SISTEMAS COMPUTACIONAIS: quaisquer pessoas do quadro funcional ou não, lotadas nas áreas de TIC, que tenham sido autorizadas a conhecer o código de acesso e senha de administração de recurso de Tecnologia da Informação e Comunicação (TIC), seja ele de uso geral, de uso restrito a uma unidade ou grupo de pessoas, ou de uso individual;

II - ÁREA DE TIC: Unidades administrativas do Tribunal responsáveis pelos serviços de TIC do Tribunal, tais como: infraestrutura e operações, desenvolvimento de soluções, governança e gestão de TI e de segurança da informação;

III - CICLO DE VIDA DA INFORMAÇÃO: ciclo que compreende etapas e eventos de produção, recebimento, armazenamento, acesso, uso, alteração, cópia, transporte e descarte da informação;

IV - GESTOR DE SEGURANÇA DA INFORMAÇÃO: pessoa responsável pela coordenação das atividades relacionadas à segurança da informação no âmbito do Tribunal Regional do Trabalho da 9ª Região;

V - INCIDENTE DE SEGURANÇA DA INFORMAÇÃO: qualquer indício de fraude, sabotagem, espionagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer ou ameaçar um ou mais pilares da segurança da informação, a saber, Disponibilidade, Integridade e Confidencialidade;

VI - INFORMAÇÃO: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

VII - PDCA - trata-se de um método iterativo de gestão de quatro etapas: Planejar (do inglês, Plan - P), Fazer (do inglês, Do - D), Checar (do inglês, Check - C) e Agir (do inglês, Act - A) utilizado para o controle e melhoria contínua de processos e produtos.

VIII - PLANO DE SEGURANÇA DA INFORMAÇÃO (PLSI): é um plano estratégico com objetivo de direcionar as ações relativos à segurança da informação que deverão ser implantadas na instituição, considerando os requisitos estabelecidos na Política e no Sistema de gestão de segurança da informação (PSI e SGSI) estabelecidos neste Regional;

IX - RECURSOS DE TIC: equipamentos relacionados à TIC, tais como microcomputadores e dispositivos de armazenamento de dados, softwares, serviços de rede e comunicação de dados, suprimentos e bens de consumo também relacionados à TIC, e dados armazenados em qualquer equipamento;

X - SEGURANÇA DA INFORMAÇÃO: é disciplina que, no âmbito do Tribunal Regional do Trabalho da 9ª Região tem por objetivo garantir a continuidade e eficiência da prestação jurisdicional, salvaguardar as informações, imagem e objetivos institucionais, por meio da preservação das propriedades de confidencialidade, integridade e disponibilidade da informação; Segurança da informação tem um foco mais amplo, cuidando da redução de riscos no transporte de dados por qualquer meio, seja digital ou não;

XI - SEGURANÇA CIBERNÉTICA: é um conjunto de práticas que protege informação armazenada nos computadores e aparelhos de computação e transmitida através das redes de comunicação, incluindo a Internet e telefones celulares. A Segurança Cibernética se aplica a uma parte da segurança da informação com foco na proteção digital, cuidando das ameaças as informações transportadas por meios cibernéticos;XII - SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI): modelo de gestão, composto por um conjunto de políticas ou

normas, que visa estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação; e

XII - USUÁRIOS: magistrados, servidores ocupantes de cargo efetivo ou em comissão, funcionários de empresas prestadoras de serviços terceirizados, consultores, estagiários, advogados, jurisdicionados em geral e outras pessoas que se encontrem a serviço da Justiça do Trabalho, ainda que em caráter temporário.

CAPÍTULO II
DAS DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

Art. 5º São **objetivos** da PSI do Tribunal Regional do Trabalho da 9ª Região:

I - estabelecer princípios de governança e gestão de segurança da informação, definindo diretrizes e normas gerais para a sua efetiva implantação;

II - subsidiar ações para implementação e manutenção de processos de trabalho relacionados com a segurança cibernética;

III - subsidiar ações necessárias para implementação e manutenção de controles para atendimento a requisitos mínimos de segurança da informação nos demais processos de trabalho;

IV - apoiar a manutenção e a continuidade dos serviços críticos do órgão, ou o seu restabelecimento em menor tempo possível.

Parágrafo único. A PSI alinha-se ao objetivo institucional de aprimorar a governança de tic, a proteção de dados e a segurança cibernética.

Art. 6º São **princípios** da Segurança da Informação no Tribunal:

I - O MENOR PRIVILÉGIO: que exige que sejam concedidos aos usuários somente os privilégios necessários ao exercício de suas funções institucionais;

II - O CONTROLE DA RESPONSABILIDADE: que estabelece que as pessoas que estejam em posições de maior responsabilidade e risco devam ser submetidas a controles mais rígidos de segurança da informação;

III - A PROPRIEDADE DA ORGANIZAÇÃO: que garante que informações, sistemas, processos, procedimentos ou métodos específicos criados pelos usuários, no exercício de suas funções, independentemente da forma de sua apresentação ou armazenamento, são de propriedade deste Tribunal e deverão ser adequadamente protegidos e utilizados exclusivamente para fins relacionados às atividades institucionais;

IV - A IDENTIFICAÇÃO DIGITAL: que preconiza que a identificação de qualquer usuário deve ser única, pessoal e intransferível, qualificando-o como

responsável pelas ações realizadas por meio dessa identidade;

V - A TRANSPARÊNCIA: que determina que as informações de interesse público devem permanecer públicas e disponíveis;

VI - A UNIVERSALIDADE: que estabelece que os controles de segurança da informação devam ser aplicados a todos os meios e etapas do ciclo de vida da informação;

VII - O MONITORAMENTO CONTÍNUO: que estabelece que os meios nos quais trafegam as informações devem ser constantemente monitorados e controlados, com o intuito de evitar ameaças à informação;

VIII - O REPOSITÓRIO ADEQUADO: que estabelece que as informações devem ser armazenadas em repositórios ou locais compatíveis com suas características e requisitos de segurança;

IX - A NÃO EXCLUSIVIDADE: que estabelece que não é permitido que apenas um usuário ou administrador de sistemas computacionais do Tribunal possua controle ou acesso exclusivo de um processo de negócio ou recurso imprescindível para a continuidade do negócio.

X - A CONFIDENCIALIDADE: que garante que a informação só́ é acessada por indivíduos, entidades e processos autorizados;

XI - A INTEGRIDADE: que garante que a informação armazenada ou transferida esteja correta e não tenha sofrido adulteração;

XII - A DISPONIBILIDADE: que estabelece que a informação esteja acessível e utilizável sob demanda por uma entidade autorizada;

XIII - A AUTENTICIDADE: que garante que os dados fornecidos são verdadeiros e de que o usuário é legítimo;

XIV - A CRITICIDADE: classificação de acordo com o grau de relevância do ativo de informação em relação a confidencialidade, a integridade e a disponibilidade, observadas as necessidades do negócio e a legislação em vigor;

XV - O NÃO-REPÚDIO OU IRRETRATABILIDADE: que garante que uma pessoa não consiga negar a autoria ou envio de uma informação; e

XVI - A PRIVACIDADE: que garante a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

CAPÍTULO III
DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 7º Esta política é parte integrante do Sistema de Gestão de Segurança da Informação (SGSI), composto, também, pelos processos relacionados ao tema, a exemplo dos seguintes:

I - gerenciamento de riscos de segurança da informação;

II - incidentes de segurança da informação;

III - continuidade de serviços essenciais;

IV - utilização dos recursos de TIC;

V - gerenciamento e controle de ativos de informação;

VI - gestão de backup e retenção de dados;

VII - identidade digital e gerenciamento de acesso;

VIII - gestão, monitoramento e segurança dos Data Centers.

Parágrafo único. O **Sistema de Gestão de Segurança da Informação** é um processo cíclico do tipo "PDCA", de melhoria contínua, e deve ser realizado por meio das etapas de planejamento, execução, monitoramento e melhoria, seguindo as melhores práticas de gestão de segurança da informação vigentes.

Art. 8º Em relação à segurança da informação, cabe à Área de TIC:

I - executar os processos referidos no Art. 7º e outros que os complementem;

II - gerir a infraestrutura de hardware e software necessária à prestação dos serviços corporativos, estabelecendo os procedimentos de segurança e continuidade adequados;

III - registrar ações e eventos que possam ter um impacto na eficácia ou no desempenho do SGSI;

IV - executar ações preventivas e corretivas que impactem positivamente na gestão de segurança da informação;

V - monitorar a utilização dos recursos de tecnologia da informação, com o intuito de detectar infrações a normas, procedimentos e diretrizes que integram a PSI, fornecendo evidências no caso de incidentes de segurança.

Art. 9º Cabe ao GESTOR INSTITUCIONAL DE SEGURANÇA DA INFORMAÇÃO, com apoio da área de TIC:

I – gerir o Sistema de Gestão de Segurança da Informação;

II – propor controles internos fundamentados na gestão de riscos da segurança da informação;

III – apoiar o planejamento e execução de programas, projetos e

processos relativos à segurança da informação;

IV – propor procedimento de tratamento e resposta a incidentes em segurança da informação;

V – observar as normas e os procedimentos específicos aplicáveis em consonância com os princípios e as diretrizes da Resolução CNJ nº 396/2021 e da legislação de regência.

CAPÍTULO IV
DO MONITORAMENTO E MELHORIA

Art. 10. O Gestor de Segurança da Informação dará ciência ao Comitê de Segurança da Informação e Proteção de Dados (CSIPD), dos indicadores e eventos relevantes de segurança da informação, a fim de permitir o acompanhamento do cumprimento desta política.

CAPÍTULO V
DA PRESTAÇÃO DE CONTAS

Art. 11. O Gestor de Segurança da Informação disponibilizará por meio do painel informatizado a relação das políticas ou normas de segurança da informação vigentes, em elaboração, modificadas ou extintas.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 12. O descumprimento desta política, bem como das diretrizes, normas e procedimentos de segurança da informação estabelecidos, poderá acarretar, nos termos da legislação vigente, sanções administrativas, civis e penais, assegurada a ampla defesa.

Art. 13. Os casos omissos e as dúvidas surgidas na aplicação desta política serão dirimidos pela Presidência do Tribunal.

Art. 14. Esta Política entra em vigor na data de sua publicação, revogando-se a Política Nº 28/2018, instituída pela Resolução ADMINISTRATIVA 85/2018, de 26 de novembro de 2018.

CÉLIO HORST WALDRAFF
Desembargador Presidente do TRT da 9ª Região

PODER JUDICIÁRIO
Tribunal Regional do Trabalho da 9ª Região

POLÍTICA Nº 86, DE 16 DE MAIO DE 2024.

*Institui a **Política de backup e restauração de dados** no âmbito do Tribunal Regional do Trabalho da 9ª Região.*

O DESEMBARGADOR DO TRABALHO, PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 9ª REGIÃO, usando de suas atribuições legais e regimentais,

CONSIDERANDO:

- a Política de Segurança da Informação (PSI) do Tribunal Regional do Trabalho da 9ª Região;

- o disposto no Art. 21, inciso "II", alínea "c**"**, da Resolução CNJ 370/2021, sobre a necessidade de constituir e manter estruturas organizacionais adequadas e compatíveis com a relevância e demanda de TIC, considerando, entre outros macroprocessos, o de **Segurança da Informação e Proteção de Dados** e seu processo de **Continuidade de serviços essenciais**;

- o item 12.3 da norma ISO 27.002/2013, que estabelece diretrizes para definição de política de backup (cópias de segurança), com o intuito de proteger o negócio contra perda de dados;

- o Guia Referencial de Segurança da Informação da Justiça do Trabalho, editado pelo Conselho Superior da Justiça do Trabalho (CSJT);

- a necessidade de atender a todos os pilares da Segurança da Informação, a saber, Confidencialidade, Integridade e Disponibilidade;

- a instituição da Política de Gerenciamento de Processos de trabalho no âmbito do Tribunal;

RESOLVE *ad referendum* do Tribunal Pleno

PODER JUDICIÁRIO
Tribunal Regional do Trabalho da 9ª Região

CAPÍTULO I
DAS DISPOSIÇÕES INICIAIS

Art. 1° Instituir a POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS, no âmbito deste Tribunal.

Art. 2º Esta política integra a Política de Segurança da Informação (PSI) do Tribunal Regional do Trabalho da 9ª Região e tem como objetivo assegurar a correta elaboração, aprovação, execução dos planos de backup e dos relatórios de backup e restauração de dados, prevenindo a perda e a indisponibilidade de sistemas e informações produzidos e/ou armazenados nos ativos de Tecnologia de Informação e Comunicação (TIC) do Tribunal.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 3° Para os efeitos deste ato, aplicam-se as seguintes definições e conceitos:

I - AMBIENTE PRIMÁRIO DE BACKUP: local onde é feita a primeira cópia dos arquivos originais, delimitado, precisamente, como sendo o DATACENTER DE BACKUP onde se encontra a biblioteca de fitas magnéticas;

II - ÁREA DE TIC: Unidades administrativas do Tribunal responsáveis pelos serviços de TI do Tribunal como infraestrutura, desenvolvimento e manutenção de soluções da área Judiciária, apoios à governança e à gestão, contratações, projetos e gestão de serviços; desenvolvimento e manutenção de soluções de TIC da área Administrativa; e pela Segurança da Informação, gerenciamento de bancos de dados, servidores web, serviços de rede e gerenciamento de desktops que suportam a infraestrutura de TIC do Tribunal;

III - BACKUP: cópia de segurança de informação para prevenir perda de disponibilidade em caso de perda da informação principal;

IV - BACKUP FULL: backup completo onde são copiados todos os arquivos da fonte que está sendo feito backup. O backup full não depende de outros backup para sua execução ou para restore de dados;

V - BACKUP INCREMENTAL: backup que copia somente os arquivos que foram modificados desde a realização do último backup full ou incremental, sendo assim um backup mais rápido que o backup full que também economiza espaço no armazenamento dos dados; para uma restauração completa ele depende de um backup full e todos os demais incrementais que foram realizados até a data do ponto de restauração desejado;

VI - BACKUP DIÁRIO: backup que é realizado com a frequência mínima de uma vez ao dia;

VII - BACKUP MENSAL: backup que é realizado uma única vez ao mês;

VIII - BACKUP EM FITA: backup que é salvo em mídias magnéticas (fitas) utilizando a tecnologia LTO (Linear Tape-Open);

IX - BACKUP EM DISCO: backup que é armazenado em unidades de disco rígido (*HDD – Hard Disk Drive*), e/ou em unidades de estado sólido (*SSD – Solid State Drive*), e/ou em unidades de memória não volátil expressa (*NVMe – Non-Volatile Memory express*) e/ou em unidades com tecnologia similar a essas;

X - BIBLIOTECA DE FITAS: é um dispositivo de armazenamento que contém uma ou mais unidades de fita, certa quantidade de nichos para guardar cartuchos de fitas magnéticas, um leitor de código de barras para identificar cartuchos de fita e um método automatizado para inserir as fitas na unidade de leitura (um robot). Também conhecida pelas siglas em inglês *tape library* ou simplesmente *library*;

XI - CÓPIA DE SEGURANÇA *OFFSITE*: cópia de backup em mídia armazenada em mídia física localizada fora do ambiente primário de dados de backup. Também podem ser conhecidas como cópias de longa retenção;

XII - CUSTODIANTE DOS ATIVOS DE INFORMAÇÃO: unidade da Área de TIC responsável pela manutenção e operação do sistema de backup;

XIII - DATACENTER: corresponde a um local físico que armazena máquinas de computação e seus equipamentos de hardware relacionados. Ele contém a infraestrutura de computação que os sistemas de TI exigem, como servidores, unidades de armazenamento de dados e equipamentos de rede;

XIV - DATACENTER DE BACKUP: corresponde ao local onde estão armazenadas as cópias dos arquivos do LOCAL PRIMÁRIO DE DADOS, tratando-se de local físico diferente do datacenter primário;

XV - DESDUPLICAÇÃO DE DADOS: trata-se de um conceito que envolve a aplicação de compactação de dados que permite diminuir o volume de dados armazenados eliminando cópias de dados armazenados;

XVI - DONO DA INFORMAÇÃO: proprietário da informação, a saber, o próprio Tribunal Regional do Trabalho da 9ª Região;

XVII - JANELA DE BACKUP: período de tempo compreendido entre o início e o fim de uma operação de backup, sendo um fator importante de avaliação de desempenho da solução de backup instalada;

XVIII - LOCAL PRIMÁRIO DE DADOS: local (ou locais, quando se tratar de conceito de alta disponibilidade de datacenters) onde estão armazenados os dados originais gerados por usuários e/ou aplicações e sistemas;

XIX - RESTAURAÇÃO: processo realizado para colocar disponível uma cópia de segurança de informação anteriormente preservada;

XX - RETENÇÃO DOS DADOS: período de tempo pelo qual os dados copiados são preservados no ambiente de backup; e

XXI – RPO (Ponto Objetivo de Recuperação, do inglês, "Recovery Point Objective"): é a métrica que define o intervalo máximo de tempo para a perda de dados e/ou informações geradas em algum sistema ou serviço desde a última rotina de backup realizada.

CAPÍTULO III
DAS DIRETRIZES GERAIS

Art. 4º As cópias de backup das informações, softwares e sistemas devem ser realizadas e testadas regularmente, de acordo com esta política.

§ 1º O backup de determinado sistema ou serviço deve contemplar todos os arquivos e dados necessários à sua plena restauração, incluindo executáveis, definições de estrutura de banco de dados, entre outros.

§ 2º O backup de sistemas, aplicativos e documentos protegidos por direitos autorais deve observar as restrições de cópia previstas em suas respectivas licenças de uso e sua legislação vigente.

§ 3º As cópias de segurança devem ser geradas, transportadas e armazenadas de forma segura, com controles físicos e lógicos compatíveis com os requisitos de confidencialidade, integridade e disponibilidade das respectivas informações.

§ 4º As cópias do backup de dados devem ser armazenadas em localidade diferente do local primário de dados, a uma distância suficiente para evitar danos ocasionados por eventual desastre no local primário e devem possuir nível apropriado de proteção física e ambiental.

§ 5º De modo a prover redundância e atender à continuidade do negócio em caso de desastre, as mídias de cópia de segurança *offsite* devem ser mantidas fora do ambiente primário de backup, se possível em outra sede, sendo armazenadas em cofres de segurança próprios para esse fim.

§ 6º A Administração deve prover os recursos físicos e humanos necessários para a operação segura e eventual transporte das mídias da cópia de segurança *offsite*.

§ 7º As informações que possuem dados sigilosos devem ter seus backups protegidos por criptografia ou controle de acesso físico e lógico restritos.

§ 8º Os tempos de retenção de backup obedecerão aos parâmetros de temporalidade mínimos estabelecidos na tabela constante no Anexo A e havendo disponibilidade de espaço e recursos, sem impactos orçamentários, tais limites poderão ser dinamicamente ajustados de forma a aproveitar o espaço de armazenamento disponível.

§ 9º Quanto aos dados armazenados em infraestrutura de nuvem que não sejam de aplicações críticas e importantes, para os quais não há políticas próprias de retenção e backup, ficam eles sujeitos aos critérios e parâmetros estabelecidos pela CONTRATADA e pelo TRT9 para tais serviços, obedecendo aos parâmetros e níveis de garantia do serviço definidos contratualmente, os quais serão divulgados pela área de TIC do Tribunal aos seus usuários.

§ 10. Os backups de Registro de Eventos (*Logs*) devem possuir critérios de retenção diferentes dos demais objetos, bem como serem armazenados preferencialmente em mídias menos custosas.

§ 11. Havendo possibilidade técnica e disponibilidade de recursos, será realizada uma operação de cópia dos dados para uma mídia diferente daquela em que os dados foram salvos inicialmente.

§ 12. Visando aumentar a oferta de espaço de armazenamento na infraestrutura de backup otimizando custos financeiros de aquisição, todo e qualquer equipamento de backup em disco adquirido pelo TRT9 deverá fornecer, preferencialmente, a funcionalidade de desduplicação de dados de forma nativa.

CAPÍTULO IV
DOS PAPÉIS E RESPONSABILIDADES

Art. 5º São atribuições do **Custodiante dos ativos de informação**:

I - criar o Plano de Backup de acordo com o Art. 6º;

II - planejar, configurar, executar e monitorar as rotinas de backup;

III - executar testes de restauração de dados salvos no backup.

CAPÍTULO V
DOS PLANOS E RELATÓRIOS

Art. 6º O **Plano de Backup**, a ser elaborado pelo Custodiante dos ativos de informação, deve conter, no mínimo, as seguintes informações:

I – identificação e descrição dos ativos, e da categoria de dado salvo neles, que serão resguardados em backup;

II – volumetria, aproximada, da estrutura de dados que será resguardada em backup;

III – estratégia de emissão de relatórios de execução de backup e/ou de restauração (Ex. periodicidade mensal ou semestral, ou sob demanda etc).

Art. 7º Os períodos de retenção dos dados, bem como as definições relacionadas às mídias de armazenamento das informações e demais parâmetros estão definidos no Anexo A desta política.

Art. 8º O **Relatório de Backup** e o **Relatório de Restauração** devem conter, no mínimo, as seguintes informações:

I – data e hora da execução da rotina de backup e/ou restauração;

II – condição do retorno da execução da rotina de backup e/ou restauração, com os resultados de Sucesso ou Falha, e informações acerca dos resultados obtidos.

Parágrafo único. Consideram-se, também, como **Relatório de Backup** e como o **Relatório de Restauração** os registros de eventos (*logs*) gerados pelas rotinas automatizadas de backup e os processos manuais de restauração realizados pelo software gerenciador de backup.

CAPÍTULO VI
DAS DIRETRIZES ESPECÍFICAS

Art. 9º A criação e a operação dos backups devem observar as seguintes orientações:

I - CRIAÇÃO DE BACKUPS: o backup deverá ser programado, preferencialmente, para execução automática, em horários de menor ou nenhuma utilização dos sistemas e da rede, observando os requisitos do Plano de Backup;

II - OPERAÇÃO DE BACKUPS: o backup deverá ser monitorado pelo Custodiante da Informação.

Parágrafo único. Um relatório (preferencialmente automatizado) deverá ser gerado para as execuções de backup, contendo informações dos registros dos resultados do processo.

Art. 10. Na restauração de dados, por conta de solicitação específica, deverá ser mantido no software gerenciador do backup o registro da informação restaurada, juntamente com as informações relativas à solicitação (número do chamado técnico, solicitação de serviço ou ticket de abertura de chamado), para eventual conferência futura.

CAPÍTULO VII
DA PRESTAÇÃO DE CONTAS

Art. 11. Sempre que solicitado, a área de TIC apresentará aos membros do Comitê de Segurança da Informação e Proteção de Dados (CSIPD) ou aos demais órgãos Colegiados que as requererem, informações acerca do cumprimento da presente política.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 12. Caberá à área de TIC estabelecer os critérios técnicos relacionados aos procedimentos e às configurações de backup e de restauração para cada sistema ou base de dados, em harmonia com o contido nesta política e anexo(s).

Art. 13. O conteúdo do ANEXO A será revisado periodicamente, após parecer de mérito do CSIPD e aprovação direta da Presidência do Tribunal, assegurado o controle documental e de versões.

Art. 14. Compete ao Dono do Processo de Trabalho de Gestão de Backup e Restauração de Dados analisar sobre os casos omissos ou que suscitem dúvidas quanto ao disposto nesta política, cabendo-lhe a decisão de encaminhamento das questões às partes interessadas ou à Alta Administração para deliberação.

Art. 15. Propostas de revisões e atualizações desta política deverão ser encaminhadas para a deliberação do CSIPD.

Art. 16. Em consonância com a Política de Gerenciamento de Processos de trabalho do Tribunal, o dono do Processo de Backup e Restauração de Dados é o(a) titular da área de TIC.

Parágrafo único. O(s) gerente(s) do Processo de Backup e Restauração de Dados será(ão) designado(s) pelo Dono do Processo.

Art. 17. Esta Política entra em vigor na data de sua publicação, revogando-se a Política 14/2017.

CÉLIO HORST WALDRAFF
Desembargador Presidente do TRT da 9ª Região

PODER JUDICIÁRIO
Tribunal Regional do Trabalho da 9ª Região

ANEXO A
TABELA DOS PARÂMETROS MÍNIMOS DE BACKUP E TEMPOS DE RETENÇÃO
(v1, de 16 de maio de 2024) - Política 86/2024

	Categoria do Dado	Descrição	Conteúdo	Parâmetros do Backup Diário		Parâmetros do Backup Mensal	
1	Banco de Dados	Informações contidas em bases de dados dos serviços do Tribunal	Tecnologias Oracle, PostGres, MSSQL, MySQL e Redis e semelhantes a essas.	Armazenamento em disco e/ou em fita	Retenção de 21 dias	Armazenamento em fita	Retenção de 9 meses
2	Máquinas Virtuais	Informações de máquinas virtuais.	VMs (Virtual Machines) do virtualizador VMWare e/ou de outros virtualizadores eventualmente instalados.	Armazenamento em disco e/ou em fita	Retenção de 30 dias	N/A	N/A
3	Servidores Windows e Linux e Aplicações em Geral	Informações dos sistemas operacionais Windows e/ou Linux dos servidores e das aplicações nele contidas que não se enquadram em outra categoria	Servidores de dados diversos, virtualizados ou não, cujos dados de seus sistemas operacionais e dados gerados pelos sistemas e/ou serviços nele instalados precisam ser salvos. Exemplos: dados de cursos e treinamentos da Escola Judicial; dados em arquivos de mídias de áudio e vídeo de sistemas satélites do PJe etc.	Armazenamento em disco e/ou em fita	Retenção de 60 dias	Armazenamento em fita	Retenção de 9 meses
4	Eventos de Rede (Logs)	Informações contidas em diversas fontes de eventos da infraestrutura de rede e armazenados no Elastic Search.	Logs do firewall, Controladores de Domínio, DNS, DHCP dentre outros serviços de rede contendo informações do tipo conexões, acesso a sites e conteúdos na Internet (proxy), acesso VPN, IPS, mudanças nas regras do firewall, autenticação no AD, atribuição de IP, flows de rede etc.	Armazenamento em disco e/ou em fita	Retenção de 60 dias	Armazenamento em fita	Retenção de 12 meses

Observações e Diretrizes Específicas do Anexo

1. N/A = Não Aplicável – Parâmetros não aplicáveis a determinadas categorias de dados.

2. Os prazos definidos neste anexo não conflitam com os critérios mínimos contidos nas orientações de armazenamentos descritas no Guia Referencial de Segurança da Informação da Justiça do Trabalho, versão 2, publicado em fevereiro de 2022.

Disponível em:
https://www.csjt.jus.br/documents/955023/0/Guia_Referencial_de_Seguranca_da_Informacao_da_Justica_do_Trabalho___v2.0.pdf (Acessado em: 16/04/2024)

3. Os tempos de retenção em disco e em fita somente começam a ser contados após a EXCLUSÃO do dado em sua base originária.

    a. O tempo de retenção do dado em sua base originária não é tratado por esse normativo.

4. O Custodiante dos Ativos de Informação definirá tecnicamente, de acordo com a tecnologia envolvida, o melhor método de execução das rotinas de backup (backup full ou backup incremental, e a mídia a ser utilizada) para atendimento dos parâmetros mínimos de retenção para cada categoria de dado.

5. A granularidade temporal na restauração de dados obedece ao tipo de rotina que salvou o dado: granularidade diária, para backup diário, e mensal para as rotinas mensais. Isso implica em:

    a. Dados criados e apagados durante o dia podem não ser salvos no backup diário;

    b. Dados criados e apagados durante um mês podem não ser salvos no backup mensal.

6. Os dados gerados por quaisquer novos equipamentos servidores instalados, passíveis de serem copiados para o backup, devem ser enquadrados em uma das 4 (quatro) categorias descritas no Anexo A.

7. As informações contidas na coluna Conteúdo do Anexo A - Parâmetros de Backup se referem a exemplos de informações em servidores e em aplicações em cada categoria, não se tratando de uma lista exaustiva.

8. Define-se para todas as 4 categorias de dados um **RPO de 24 (vinte e quatro) horas**.

ATO n° 157, de 15 DE MAIO DE 2024.

Dispõe sobre ***a instituição e o funcionamento da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR)*** *no âmbito do Tribunal Regional do Trabalho da 9ª Região.*

O DESEMBARGADOR DO TRABALHO, PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 9ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO:

- o disposto no Parágrafo único do Art. 11, II da Resolução CNJ Nº 396 de 07/06/2021 que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

- a Portaria CNJ Nº 162 de 10/06/2021 e seus anexos que aprovou os Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;

- a Portaria CNJ Nº 172 de 25/05/2022 que instituiu o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ);

- a Política de Segurança da Informação (PSI) e o Sistema de Gestão de Segurança da Informação (SGSI) no âmbito do Tribunal Regional do Trabalho da 9ª Região;

- o Ato Presidência 118/2022 de 06 de setembro de 2022, que instituiu o Comitê de Segurança da Informação e Proteção de Dados (CSIPD) e o Grupo de Trabalho Técnico da LGPD (GT-LGPD) no âmbito do Tribunal Regional do Trabalho da 9a Região.

RESOLVE*, ad referendum* do Tribunal Pleno:

CAPÍTULO I
DAS DISPOSIÇÕES INICIAIS

Art. 1º Instituir e regulamentar o funcionamento da **Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética do TRT9 (ETIR)**, composta por servidores da área de TIC.

Art. 2º A sigla usada no TRT da 9ª Região para referenciar-se a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) é **CSIRT-TRT9**.

CAPÍTULO II
DA MISSÃO

Art. 3° A CSIRT-TRT9 tem como missão planejar, coordenar e executar atividades de tratamento e resposta a incidentes em redes computacionais, receber e notificar qualquer evento adverso à segurança da informação, confirmado ou sob suspeita, relacionado às redes de computadores, preservando os dados, as informações e a infraestrutura do Tribunal Regional do Trabalho da 9ª Região.

CAPÍTULO III
DO PÚBLICO ALVO

Art. 4° O público-alvo é os usuários da rede corporativa de computadores e sistemas do Tribunal Regional do Trabalho da 9ª Região.

CAPÍTULO IV
DO MODELO DE IMPLEMENTAÇÃO

Art. 5° A CSIRT-TRT9 adotará o modelo de implementação utilizando a equipe de Tecnologia da Informação (TIC), e será formada por membros das unidades da Secretaria Geral de Tecnologia da Informação e Comunicações, preferencialmente servidores efetivos, que, além de suas funções regulares, desempenharão as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais.

Art. 6º A CSIRT-TRT9 funcionará como um grupo de trabalho permanente, multidisciplinar, de atuação primordialmente reativa e não exclusiva, que age por demanda.

Parágrafo único: As atividades reativas da CSIRT-TRT9 terão prioridade sobre aquelas designadas pelos supervisores de seus respectivos integrantes.

Art. 7° Neste modelo as funções e serviços de tratamento de incidente deverão ser realizadas, preferencialmente, por administradores de rede ou de sistema ou, ainda, por peritos em segurança.

CAPÍTULO V
DA ESTRUTURA ORGANIZACIONAL E INTEGRANTES

Art. 8° O artigo 5º do Ato 118/2022 passa a ter a seguinte redação:

"Art. 5º O(a) Gestor(a) da COORDENADORIA DE GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO atuará como Gestor Institucional de Segurança da Informação."

Art. 9° A CSIRT-TRT9 é composta pelos integrantes definidos no ANEXO A.

Art. 10. O conteúdo do ANEXO A poderá ser revisado periodicamente, mediante aprovação direta da Presidência do Tribunal, assegurado o controle documental e de versões.

CAPÍTULO VI
DA AUTONOMIA DA CSIRT-TRT9

Art. 11. A CSIRT-TRT9 possuirá autonomia compartilhada, participando do resultado das decisões ao recomendar os procedimentos a serem executados, as medidas de mitigação após a identificação de uma ameaça e debaterá as ações a serem tomadas, seus impactos e a repercussão, caso as recomendações não forem seguidas.

Art. 12. A CSIRT-TRT9 comporá a rede de equipes vinculadas ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ).

Art. 13. A CSIRT-TRT9, através de seu Gestor Institucional de Segurança da Informação, poderá solicitar apoio interno e externo para responder aos incidentes de segurança de maneira adequada e tempestiva.

CAPÍTULO VII
DO CANAL DE COMUNICAÇÃO

Art. 14. O acionamento ou contato com a CSIRT-TRT9 pode ser feito:

- Preferencialmente por meio do endereço de e-mail **csirt@trt9.jus.br, ou** por meio da Central de Serviços, no telefone (41) 3310-7120, **ou** com o registro de incidente específico de segurança da informação diretamente no sistema

de chamados;

- Em caso de impossibilidade de uso dos meios definidos no inciso anterior, por qualquer outro meio disponível.

CAPÍTULO VIII
DOS SERVIÇOS

Art. 15. Os serviços prestados pela CSIRT-TRT9 estão relacionados com o Tratamento e Resposta a incidentes de Segurança Cibernética e compreendem a gestão de incidentes de segurança cibernética, através de processo definido e constituído formalmente, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança.

Parágrafo único. A CSIRT-TRT9 adotará em seus serviços no que couber os protocolos da Portaria CNJ nº 162 de 10/06/2021, ou mais recente que vier a substituí-la:

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

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

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

CAPÍTULO IX
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 16. Os casos omissos e as dúvidas surgidas na aplicação deste Ato serão dirimidos pela Presidência do Tribunal.

Art. 17. Este Ato entra em vigor na data de sua publicação, revogando-se o Ato nº 132, de 2 de setembro de 2021, a Portaria Presidência nº 62, de 13 de dezembro de 2021 e a Portaria Presidência nº 14, de 08 de março de 2022.

CÉLIO HORST WALDRAFF
Desembargador Presidente do TRT da 9 ª Região

ANEXO A - DA ESTRUTURA ORGANIZACIONAL E INTEGRANTES DA CSIRT
(v. 1. de 16 de maio de 2024)
Ato 157/2024

- A CSIRT-TRT9 é composta pelos seguintes integrantes:
    - O Gestor Institucional de Segurança da Informação;
    - O Chefe do Núcleo de Gestão da Segurança da Informação;
    - O Chefe da Seção de Operação da Segurança da Informação;
    - O Chefe da Seção de Banco de Dados;
    - O Chefe da Seção de Servidores Web;
    - O Chefe da Seção de Servidores Corporativos;
    - O Chefe da Seção de Telecomunicação Corporativa;
    - O Chefe da Subseção de Disponibilidade e Capacidade;
    - O Chefe da Seção de Central de Serviços.

- O Gestor Institucional de Segurança da Informação é o agente responsável pela CSIRT-TRT9 que chefia e gerencia a equipe.
- Os membros listados acima terão como suplentes seus substitutos legais.

ATO n° XXX, de XX DE MAIO DE 2024.

Institui o **Subcomitê de Crises Cibernéticas (SCC)** no âmbito do Tribunal Regional do Trabalho da 9ª Região.

O DESEMBARGADOR DO TRABALHO, PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 9ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO:

- a Resolução CNJ Nº 396 de 07 de junho de 2021 que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

- a Portaria CNJ Nº 162 de 10 de junho de 2021 e seus anexos que aprovou os Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;

- a Política de Segurança da Informação (PSI) e o Sistema de Gestão de Segurança da Informação (SGSI) no âmbito do Tribunal Regional do Trabalho da 9ª Região;

- a Política Presidência nº 64/2022, que estabelece regras para constituição, funcionamento e extinção de Órgãos Colegiados Temáticos no âmbito do Tribunal Regional do Trabalho da 9ª Região;

- a Portaria CNJ nº 172 de 25 de maio de 2022, que instituiu o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ);

- o Ato Presidência 118/2022 de 06 de setembro de 2022, que instituiu o Comitê de Segurança da Informação e Proteção de Dados (CSIPD) e o Grupo de Trabalho Técnico da LGPD (GT-LGPD) no âmbito do Tribunal Regional do Trabalho da 9a Região; e

- o Ato que dispõe sobre a instituição e o funcionamento da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) no âmbito do Tribunal Regional do Trabalho da 9ª Região.

RESOLVE, *ad referendum* do Tribunal Pleno:

CAPÍTULO I

DAS DISPOSIÇÕES INICIAIS

Art. 1º Instituir o **Subcomitê de Crises Cibernéticas (SCC)**, órgão colegiado temático local de apoio às funções de gestão, na área segurança da informação, associado ao Comitê de Segurança da Informação e Proteção de Dados (CSIPD).

§ 1º A vinculação referida no caput deste artigo consiste na comunicação ao Comitê de Segurança da Informação e Proteção de Dados (CSIPD) das deliberações tomadas pelo Subcomitê de Crises Cibernéticas (SCC), nos termos do art. 33, I, da Resolução nº 325, de 11 de fevereiro de 2022, do Conselho Superior da Justiça do Trabalho (CSJT).

§ 2º O Colegiado instituído por meio deste Ato subordina-se às regras para constituição, funcionamento e extinção de Órgãos Colegiados Temáticos no âmbito do Tribunal Regional do Trabalho da 9ª Região estabelecidas pela Política Presidência nº 64/2022.

CAPÍTULO II
DA COMPOSIÇÃO

Art. 2° O **Subcomitê de Crises Cibernéticas (SCC)** será composto pelos seguintes membros:

I - Desembargador(a) Presidente ou Magistrado(a) indicado(a) por ele(a);

II - Secretário(a) da Secretaria-Geral da Presidência (SGP);

III - Secretário(a) da Secretaria-Geral Judiciária (SGJ);

IV - Diretor(a)-Geral (DG);

V - Secretário(a) da Secretaria-Geral de Tecnologia da Informação e Sistemas Judiciários (SGTIC);

VI - Diretor da Secretaria de Infraestrutura e Operações; e

VII - Assessor(a) da Assessoria de Comunicação Social (ASCOM).

§ 1º O membro referenciado no inciso I deste artigo será coordenador(a) do colegiado.

§ 2º O(a) Coordenador(a) do colegiado possuirá autoridade e autonomia para tomar decisões sobre conteúdo de comunicação a ser divulgado, bem como delegar atribuições, estabelecer metas e prazos de ações.

§ 3º Os membros constantes nos incisos anteriores terão como suplentes os(as) respectivos(as) substitutos(as) legais.

§ 4º Os(As) integrantes desempenharão suas atividades sem prejuízo das respectivas funções administrativas ou jurisdicionais.

Art. 3º Fica designada como Unidade de Apoio Executivo – UAE do Subcomitê de Crises Cibernéticas (SCC), a Unidade da Secretaria Geral de Tecnologia da Informação e Sistemas Judiciários (SGTIC), no âmbito deste Tribunal, cabendo ao seu(sua) gestor(a), ou respectivo(a) substituto(a) legal, ou ao servidor(a) indicado pelo(a) Gestor(a) atuar como secretário(a).

Art. 4° Em apoio ao Órgão Colegiado fica definida a "SALA DE SITUAÇÃO", localizada no 4º andar do edifício Rio Branco, padronizada nos termos do anexo II da Portaria CNJ Nº 162, de 10 de Junho de 2021, local a partir do qual serão geridas as situações de crise, presencialmente ou virtualmente.

CAPÍTULO III
DAS ATRIBUIÇÕES

Art. 5° Cabe ao Subcomitê de Crises Cibernéticas (SCC), sem prejuízo do disposto nos protocolos aprovados pela Portaria n. 162, de 10 de junho de 2021, do CNJ, ou outro instrumento normativo que vier substituí-la:

I - reunir-se imediatamente na sala de situação, assim que a Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR identificar e comunicar que um incidente constitui uma crise cibernética, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas;

II - deliberar sobre a comunicação dos incidentes graves ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ);

III - entender claramente o incidente que gerou a crise, sua gravidade e os impactos negativos;

IV - levantar todas as informações relevantes, verificando fatos e descartando boatos;

V - levantar soluções alternativas para a crise, avaliando sua viabilidade e consequências;

VI – avaliar a necessidade de suspender serviços e/ou sistemas informatizados;

VII - centralizar a comunicação na figura de um porta-voz para evitar informações equivocadas ou imprecisas;

VIII - realizar comunicação tempestiva e eficiente, de forma a evidenciar o trabalho diligente das equipes e a enfraquecer boatos ou investigações paralelas que alimentem notícias falsas;

IX - definir estratégias de comunicação com a imprensa e/ou redes

sociais e estabelecer qual a mídia mais adequada para se utilizar em cada caso;

X - apoiar a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética – ETIR (CSIRT-TRT09) com gerentes de crise experientes;

XI - avaliar a necessidade de recursos adicionais extraordinários a fim de apoiar as equipes de resposta;

XII - orientar sobre as prioridades e estratégias da organização para recuperação rápida e eficaz;

XIII - propor ou deliberar sobre procedimentos de compartilhamento de informações relevantes para a proteção de outras organizações com base nas informações colhidas sobre o incidente; e

XIV - propor ou deliberar sobre o plano de retorno à normalidade.

Parágrafo único. Após o retorno das operações à normalidade, o Subcomitê de Crises Cibernéticas (SCC) deverá realizar a análise criteriosa das ações tomadas, observando as que foram bem-sucedidas e as que ocorreram de forma inadequada.

CAPÍTULO V
DAS REUNIÕES

Art. 6º As reuniões do Subcomitê de Crises Cibernéticas ocorrerão de forma extraordinária, sempre que houver necessidade, a critério da coordenação do subcomitê.

§1º A convocação para reunião extraordinária dar-se-á por qualquer meio admitido em direito, dispensada a exigência de antecedência mínima.

§2º As reuniões poderão ocorrer de forma presencial ou remota.

§3º Poderão participar como convidados(as) colaboradores(as), sem direito a voto, representantes de órgãos ou unidades organizacionais da instituição e profissionais de outras organizações ligadas a campo de conhecimento afim.

CAPÍTULO VI
DA PERIODICIDADE E QUÓRUM DAS REUNIÕES

Art. 7° Para instalar-se reunião do Subcomitê de Crises Cibernéticas (SCC), serão exigidas, no mínimo, as presenças de seu Coordenador e do representante da Secretaria Geral de Tecnologia da Informação e Sistemas Judiciários (SGTIC).

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 8º Este ato entra em vigor na data de sua publicação.

Publique-se e cumpra-se.

CÉLIO HORST WALDRAFF
Desembargador Presidente do TRT da 9 ª Região

JUSTIÇA DO TRABALHO
TRT da 9ª Região (PR)

Sistema de Gestão da Segurança da Informação - SGSI

(Macroprocesso de Segurança da Informação)

Documentação de Processo de Trabalho

Núcleo de Gestão de Segurança da Informação - NGSI

Coordenadoria de Governança da Segurança da Informação - CGSI

2024

OBJETIVOS

- Definir o macroprocesso que estabelece o Sistema de Gestão de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 9ª Região (TRT9).
- Descrever as atividades de preparação, execução e avaliação de Gestão da Segurança da Informação do TRT9.
- Orientar a execução das ações relativas à preservação da confidencialidade, integridade e disponibilidade da informação.

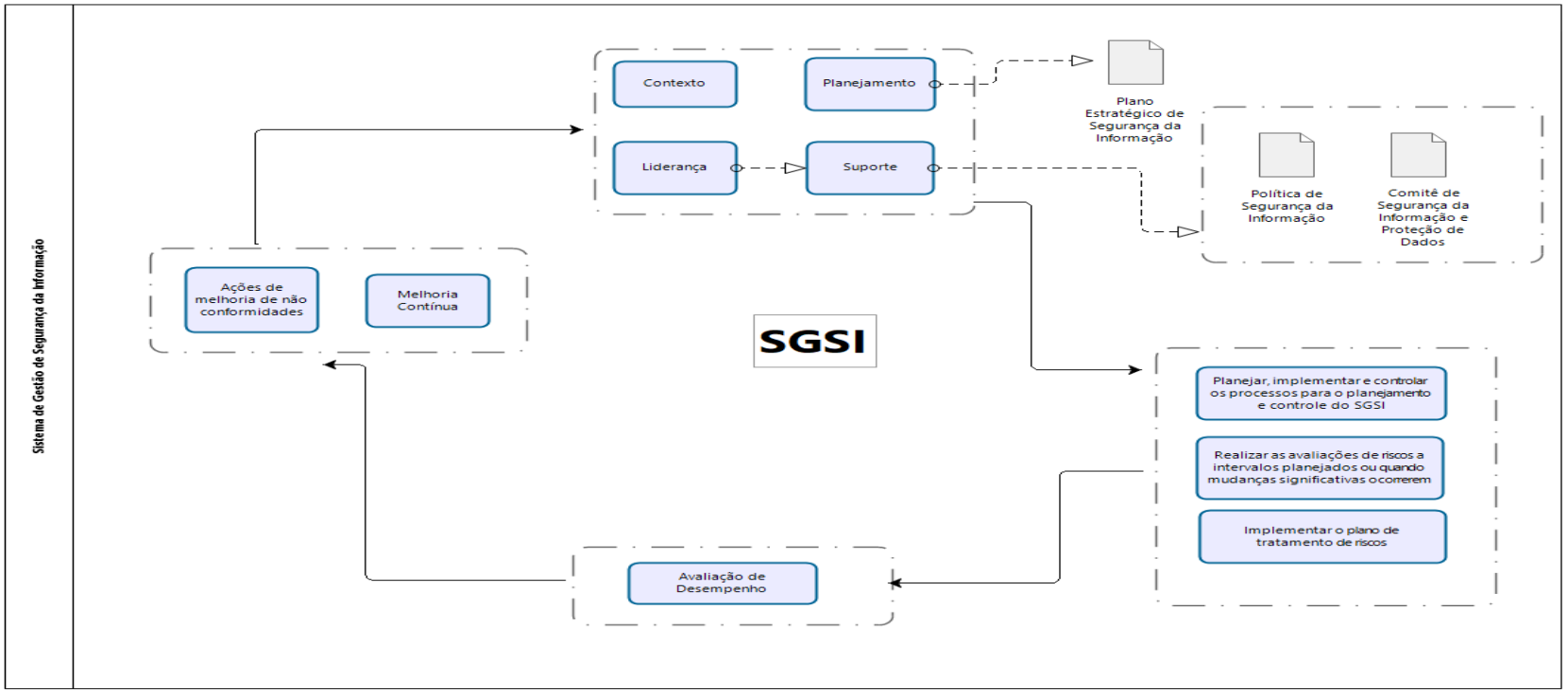
DEFINIÇÕES

- Macroprocesso: é um agregado de processos, políticas, normas e/ou atividades afins.
- Política de Segurança da Informação (PSI): declaração das intenções e diretrizes da instituição relativas à segurança da informação.
- CSIRT: *"Computer Security Incident Response Team (CSIRT)"* ou Grupo de Resposta a Incidentes de Segurança é um grupo técnico responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em redes e/ou sistemas computacionais.
- SGSI: o Sistema de Gestão da Segurança da Informação (SGSI) representa um conjunto de políticas, procedimentos e vários outros controles que definem as regras de segurança da informação em uma organização.
- PLSI: o Plano de Segurança da Informação (PLSI), ou simplesmente Plano de Segurança da Informação, contempla as recomendações e ações a serem implementadas a curto, médio e longo prazos, além do nível de capacidade dos processos e controles de segurança da informação, seu nível de criticidade e priorização.

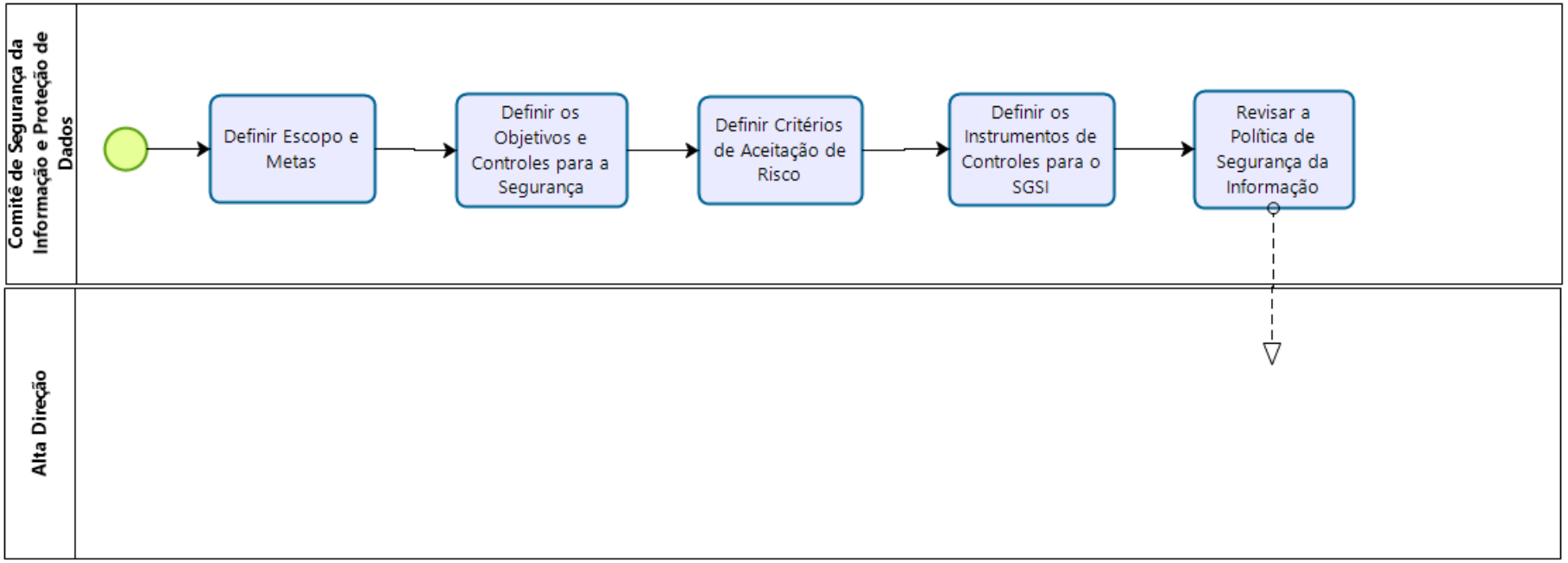
PAPÉIS E RESPONSABILIDADES

PAPEL	RESPONSABILIDADE	RESPONSÁVEL
Dono do Processo	● Garantir a qualidade, eficiência e abrangência do macroprocesso. ● Promover a integração com outros macroprocessos de trabalho relacionados. ● Aprovar mudanças no macroprocesso visando seu aperfeiçoamento. ● Avaliar os resultados e o desempenho apresentados por este macroprocesso. ● Promover a capacitação continuada do gerente e dos executores do macroprocesso. ● Aprovar a Política de Segurança da Informação, suas normas, processos e planos.	Presidente do Tribunal Regional do Trabalho da 9ª Região
Gerente do Processo	● Assegurar que todos os envolvidos na execução do macroprocesso sejam informados das mudanças efetuadas no desenho do macroprocesso. ● Promover a execução das atividades do macroprocesso. ● Manter e revisar periodicamente o macroprocesso, propondo mudanças, se necessário. ● Assegurar a correta execução do macroprocesso. ● Planejar e coordenar as atividades necessárias para execução e monitoramento do macroprocesso. ● Elaborar e/ou revisar as normas da Política de Segurança da Informação e o Plano de Segurança da Informação.	Coordenador da Governança da Segurança da Informação
Executor do Processo	● Executar as atividades do macroprocesso. ● Registrar todas as etapas do macroprocesso. ● Coletar as informações necessárias para a composição dos indicadores de desempenho do processo e registrar seus controles. ● Gerar relatórios de segurança. ● Elaborar e/ou revisar os processos e procedimentos de Segurança da Informação de acordo com o Plano de Segurança da Informação.	Gestores das unidades técnicas e administrativas relacionadas à Segurança da Informação.

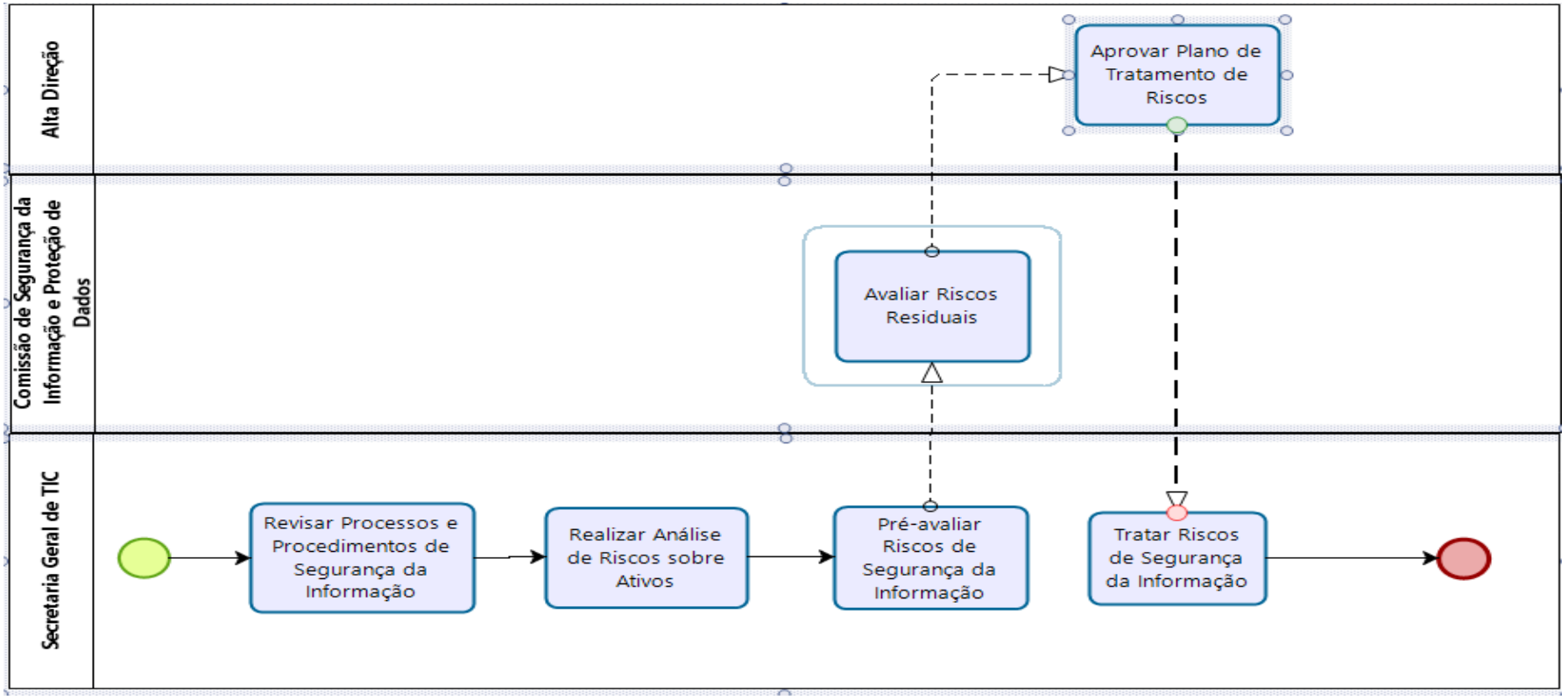
FLUXOGRAMAS - MACROPROCESSO DE SEGURANÇA DA INFORMAÇÃO



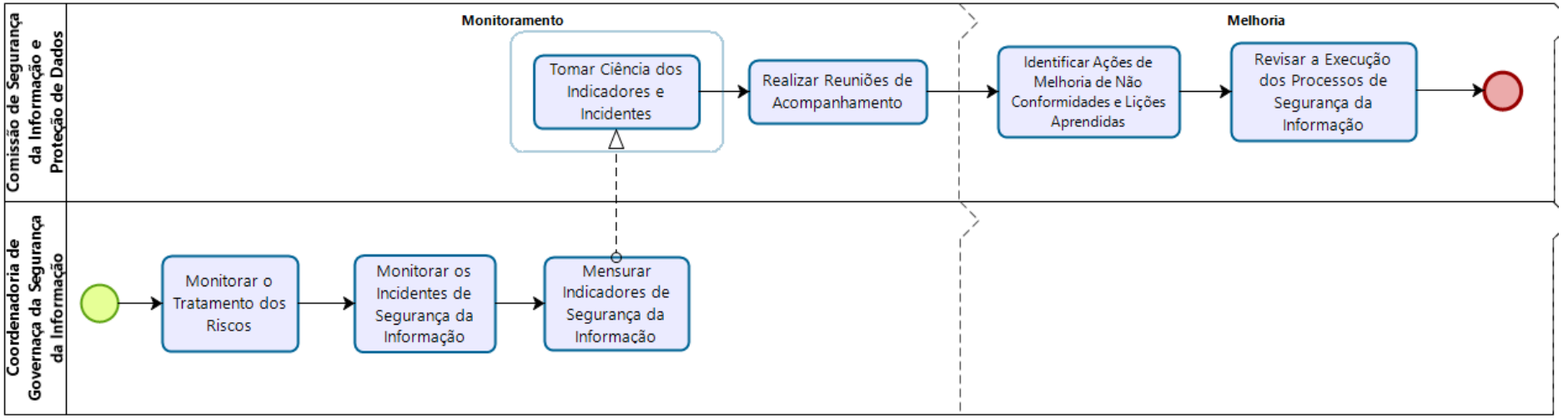
ETAPA PLANEJAMENTO



ETAPA EXECUÇÃO



ETAPAS MONITORAMENTO E MELHORIA



DESCRIÇÃO DO MACROPROCESSO

PLANEJAMENTO			
ID	**ATIVIDADE**	**RESPONSÁVEL**	**DESCRIÇÃO**
	Definir o escopo e as metas	Comitê de Segurança da Informação e Proteção de Dados	Entradas: PEI, ISO27002, COBIT, lições aprendidas do ciclo anterior. Processamento: Definir quais ativos devem ser considerados Saídas: Escopo e metas da segurança da informação
	Definir os objetivos e controles para a segurança	Comitê de Segurança da Informação e Proteção de Dados	Entradas: PEI, ISO27002, COBIT Processamento: Identificar os objetivos de controle (ISO27001) que devem ser implementados e controlados no novo ciclo Saídas: Relação de controles e objetivos para a segurança da informação
	Definir critérios de aceitação de risco	Comitê de Segurança da Informação e Proteção de Dados	Entradas: PEI, ISO27002, COBIT, relatórios de análise de risco passados. Processamento: Definir o grau de tolerância aos riscos de segurança da informação: a) qual o limiar de tratamento automático do risco? b) qual o limiar de aceitação automática do risco? Saídas: Critérios de risco

	Definir os instrumentos de controle para o SGSI	Comitê de Segurança da Informação e Proteção de Dados	Entradas: novo escopo definido, ISO27002, critérios de risco Processamento: Definir a forma com a qual o comitê acompanhará e controlará a segurança das informações. Quais artefatos devem ser apresentados? Qual a periodicidade? Saídas: Instrumentos de controle
	Revisar a Política de Segurança da informação	Comitê de Segurança da Informação e Proteção de Dados	Entradas: novo escopo definido, ISO27002, lições aprendidas, PSI anterior Processamento: a) Revisar o texto da Política de Segurança da Informação, sugerindo alterações para refletir as intenções do novo ciclo. b) Identificar revisões necessárias nas normas de segurança da informação, a fim de compatibilizá-las com a nova estratégia Saídas: Nova Política de Segurança da Informação
	Aprovar o Plano de Segurança da informação	Alta Direção	Entradas: plano de segurança da informação (consolidação das definições do planejamento) Processamento: Aprovação do plano Saídas: plano aprovado para o novo ciclo

EXECUÇÃO

ID	Atividade	Responsável	Descrição
	Revisar processos e procedimentos de segurança da Informação	SGTIC	Entradas: plano de segurança da informação, processos e procedimentos anteriores. Processamento: a) Revisar os procedimentos de segurança para efetivar as definições realizadas na etapa de planejamento b) Encaminhar para aprovação quando necessário c) Revisar os processos de segurança da informação d) Executar os processos de segurança da informação Saídas: Processos e procedimentos revisados de acordo com o novo plano de segurança
	Realizar análise de risco sobre ativos	SGTIC	Entradas: plano de segurança da informação Processamento: a) inventariar ativos para a análise, baseando-se no plano de segurança b) realizar a identificação dos riscos de segurança da informação nos ativos inventariados c) Mensurar os riscos de segurança da informação, segundo os critérios definidos no planejamento (estimativa qualitativa e quantitativa) Saídas: Relatórios de Análise de Riscos

	Pré-avaliar riscos de segurança da informação	Coordenadoria de Governança da Segurança da Informação e áreas de gestão de Segurança da Informação da SGTIC	Entradas: Relatórios de Análise de Riscos, plano de segurança da informação. Processamento: Segundo os critérios pré-definidos no plano de segurança da informação: a) Aceitar os riscos definidos como automaticamente aceitáveis, b) encaminhar para o tratamento os riscos definidos como de tratamento automático. c) Solicitar informações adicionais a respeito do tratamento dos riscos residuais (custo, tempo, responsáveis, etc.) Saídas: Relatório de Análise de risco consolidado
	Avaliar riscos de segurança residuais	Comitê de Segurança da Informação e Proteção de Dados	Entradas: Relatório de Análise de risco consolidado Processamento: Analisar os riscos identificados e sugerir a aceitação ou tratamento dos riscos Saídas: Plano de Tratamento de Riscos
	Aprovar plano de tratamento de riscos	Alta Direção	Entradas: Plano de Tratamento de Riscos Processamento: a) Analisar e aprovar do Plano de Tratamento de Riscos b) Conceder apoio e os recursos necessários ao tratamento dos riscos envolvidos. Saídas: Plano de Tratamento de Riscos aprovado

	Tratar riscos de segurança da informação	Áreas de gestão de Segurança da Informação da SGTIC	Entradas: Plano de Tratamento de Riscos Processamento: Efetuar as operações necessárias ao tratamento e/ou mitigação dos riscos elencados no plano Saídas: Riscos controlados

MONITORAMENTO			
ID	**Atividade**	**Responsável**	**Descrição**
	Monitorar o tratamento dos riscos	Coordenadoria de Governança da Segurança da Informação	Entradas: relatórios de progresso Processamento: Acompanhar as movimentações sobre o tratamento dos riscos Saídas: Relatório de tratamento dos riscos
	Monitorar os incidentes de segurança da informação	Coordenadoria de Governança da Segurança da Informação	Entradas: processo de tratamento de incidentes de segurança da informação, relatórios de progresso Processamento: a) Armazenar informações relevantes acerca dos incidentes de segurança da informação b) Identificar não conformidades com normas e procedimentos de segurança da informação c) revisar normas e procedimentos de segurança da informação Saídas: relatórios de incidentes de segurança da informação
	Mensurar indicadores de Segurança da Informação	Coordenadoria de Governança da Segurança da Informação	Entradas: relatórios de segurança e base de conhecimento Processamento: Calcular os indicadores de acordo com o previsto nos planos estratégicos e de segurança da informação Saídas: Indicadores calculados

	Tomar ciência dos indicadores e incidentes	Comitê de Segurança da Informação e Proteção de Dados	Entradas: indicadores calculados, relatório de incidentes de segurança da informação Processamento: a) Tomar ciência dos valores calculados b) Sugerir ações corretivas que se fizerem necessárias Saídas: Conhecimento da situação e dos eventos de segurança
	Realizar Reuniões de Acompanhamento	Comitê de Segurança da Informação e Proteção de Dados	Entradas: periodicidade, relatórios de segurança, outras questões, etc. Processamento: Agendar e realizar reuniões periódicas de acompanhamento Saídas: atas de reuniões

MELHORIA			
ID	**Atividade**	**Responsável**	**Descrição**
	Identificar ações de melhoria de não-conformidades e lições aprendidas	Comitê de Segurança da Informação e Proteção de Dados	Entradas: relatórios de progresso Processamento: Revisar as normas de segurança para efetivar as definições realizadas na etapa de planejamento Saídas: lições aprendidas
	Revisar a execução dos processos de segurança da informação	Comitê de Segurança da Informação e Proteção de Dados	Entradas: plano de segurança, normas de segurança da informação, informações de incidentes, informações de riscos, processos Processamento: Revisar as normas e processos de segurança da informação Saídas: sugestão de melhorias nas normas e processos de segurança da informação

TABELA RACI - MACROPROCESSO SGSI

Papéis: (R) Responsável - (C) Consultado - (I) Informado

RACI	ATIVIDADE	SGTIC	GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO	COMITÊ DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS	ALTA DIREÇÃO
PLANEJAMENTO	Definir o escopo e as metas		C	R	C
	Definir os objetivos e controles para a segurança		C	R	
	Definir critérios de aceitação de risco		C	R	C
	Definir os instrumentos de controle para o SGSI		C	R	
	Revisar a Política de Segurança da informação		C	R	C
	Aprovar o Plano de Segurança da informação	I	I	I	R
EXECUÇÃO	Revisar processos e procedimentos de segurança da Informação	R		I	
	Realizar análise de risco sobre ativos	R			
	Pré-avaliar riscos de segurança da informação	R	R		
	Avaliar riscos de segurança residuais		C	R	C
	Aprovar plano de tratamento de riscos	I	I	C	R
	Tratar riscos de segurança da informação	R	C	I	
MONITORAMENTO	Monitorar o tratamento dos riscos	C	R		
	Monitorar os incidentes de segurança da informação	C	R		
	Mensurar indicadores de Segurança da Informação	C	R		
	Tomar ciência dos indicadores e incidentes		C	R	
	Realizar Reuniões de Acompanhamento		C	R	
MELHORIA	Identificar ações de melhoria de não conformidades e lições aprendidas		C	R	C
	Revisar a execução dos processos de segurança da informação			R	

CONTROLES DO PROCESSO

Percentual de incidentes não previstos na Avaliação de Risco de TIC.

ORIGEM	Deste Macroprocesso	
PERIODICIDADE	Anual	
META	*	
CÁLCULO	I10 = (NINP / TI) * 100 NINP = Número de incidentes não previstos na avaliação de risco TI = Total de incidentes	
DESCRIÇÃO	Representa o percentual de incidentes não previstos na avaliação de riscos que causaram indisponibilidade generalizada.	
LINHA DE BASE	**METAS**	
	2024	2025
FONTE	Risk Manager / Módulo Workflow - Gestão de Incidentes	

Percentual dos serviços de TIC, contidos no catálogo de serviços da TI, em que existem requisitos de segurança da informação que não estão sendo atendidos.

ORIGEM	Deste Macroprocesso	
PERIODICIDADE	Anual	
META	*	
CÁLCULO	I15 = (NSRNR / TS) * 100 NSRNR = Número de serviços do catálogo de TIC com algum requisito de segurança não resolvido TS = Total de serviços de TIC do catálogo de serviços de TIC	
DESCRIÇÃO	Representa o percentual dos serviços de TIC do catálogo, em que existem requisitos de segurança que não estão sendo atendidos.	
LINHA DE BASE	**METAS**	
	2024	2025
FONTE	Risk Manager / Módulo Requisitos (Personalizado)	

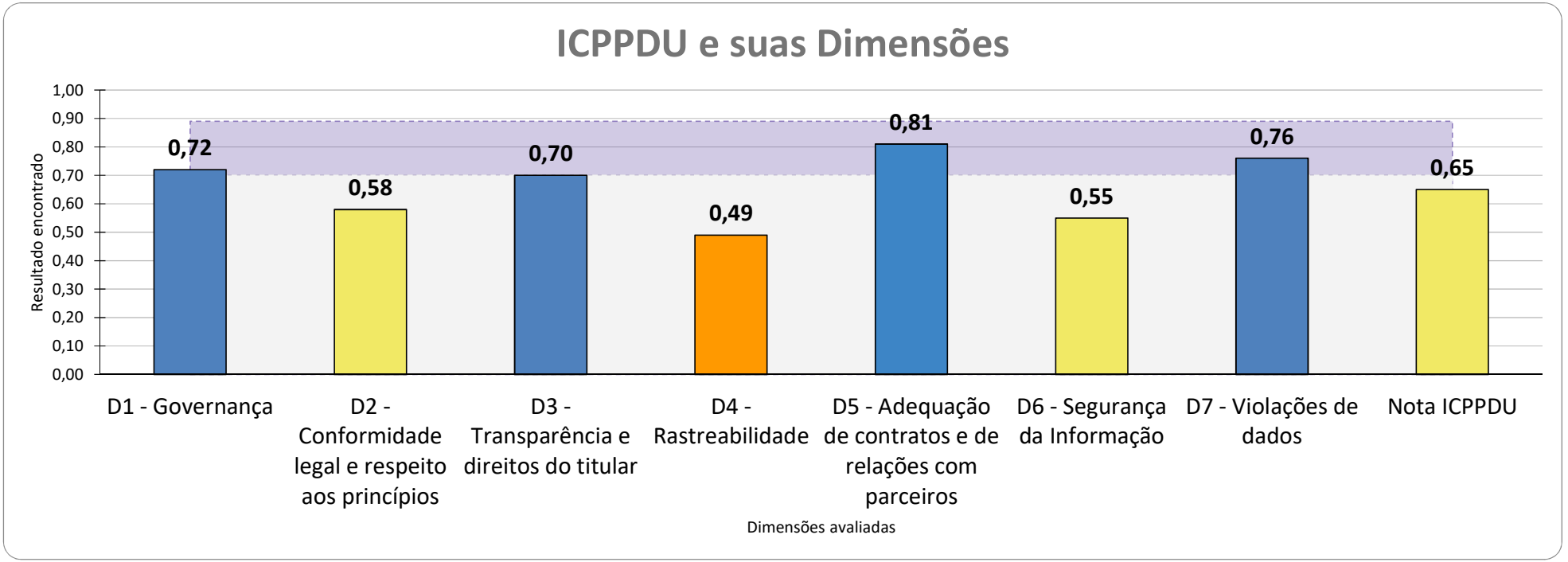
***** As metas serão definidas após a primeira medição, quando será possível estabelecer uma linha de base.

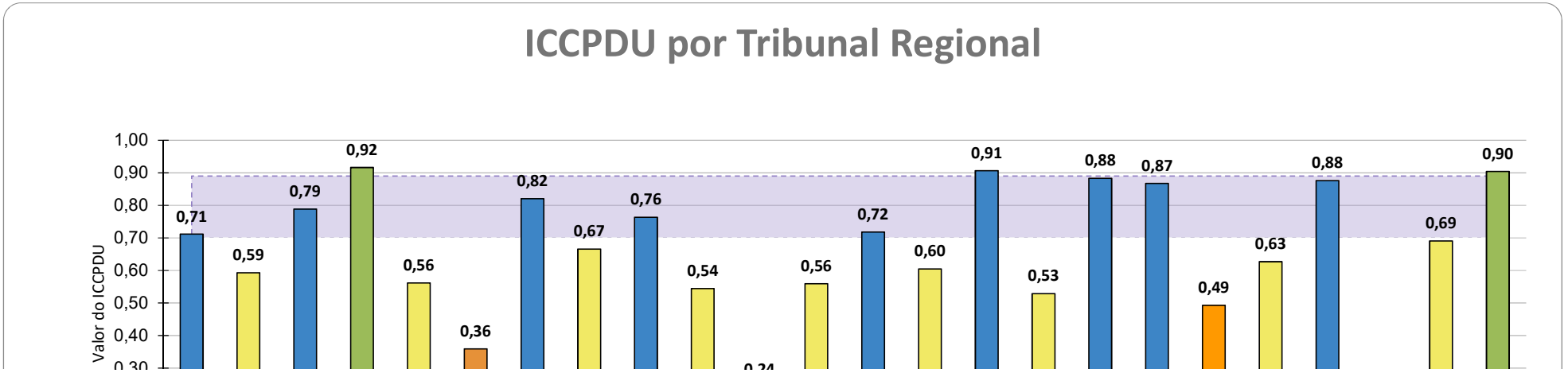
DIVULGAÇÃO DE RESULTADOS E RELATÓRIOS

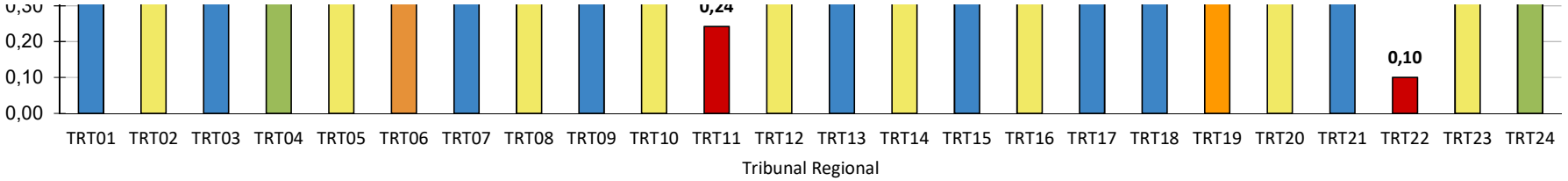
Os resultados do macroprocesso são demonstrados através dos indicadores existentes nos processos que compõem o Sistema de Gestão da Segurança da Informação. Todos os relatórios gerados por estes fazem parte da apresentação dos resultados obtidos por meio da execução do macroprocesso e seus processos componentes.

Painel de resultados do ICPPDU - 6º BIMESTRE/2023

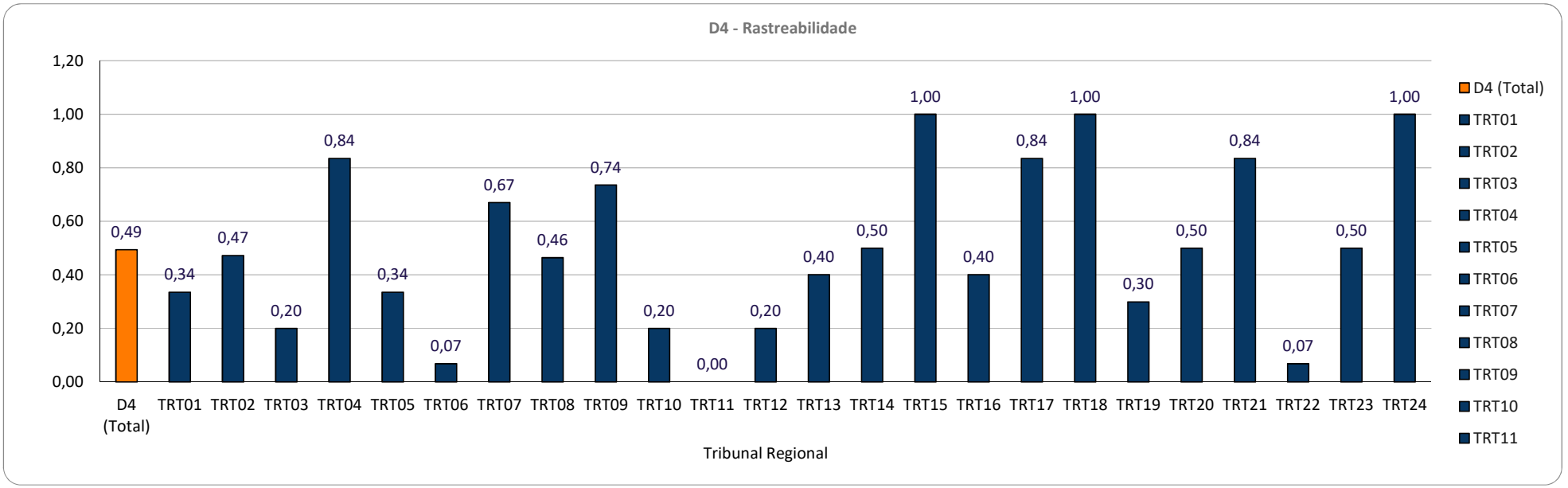
Levantamento realizado em: Dezembro

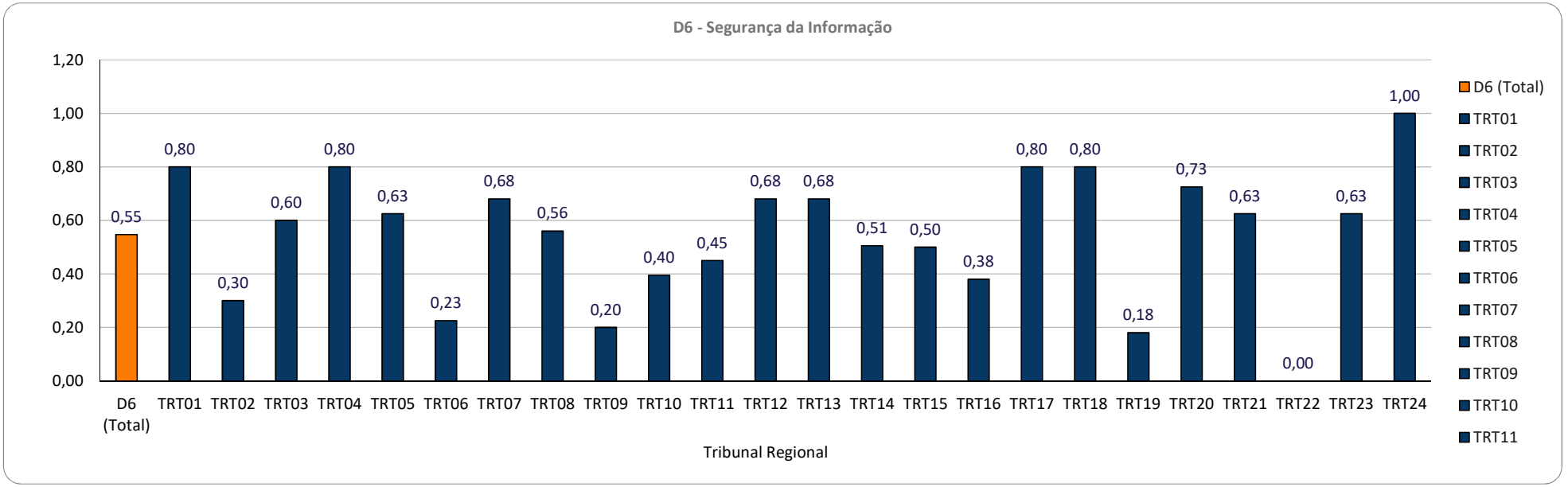






Índice	Nível de Adequação	Cor
0,00 a 0,29	Inicial	
0,30 a 0,49	Básico	
0,50 a 0,69	Intermediário	
0,70 a 0,89	Em Aprimoramento	
0,90 a 1,00	Aprimorado	


D4 - Rastreabilidade
1,20
1,00
0,80
0,60
0,40
0,20
0,00
0,49
0,34
0,47
0,20
0,84
0,34
0,07
0,67
0,46
0,74
0,20
0,00
0,20
0,40
0,50
1,00
0,40
0,84
1,00
0,30
0,50
0,84
0,07
0,50
1,00
D4 (Total)
TRT01
TRT02
TRT03
TRT04
TRT05
TRT06
TRT07
TRT08
TRT09
TRT10
TRT11
TRT12
TRT13
TRT14
TRT15
TRT16
TRT17
TRT18
TRT19
TRT20
TRT21
TRT22
TRT23
TRT24
Tribunal Regional


D6 - Segurança da Informação
1,20
1,00
0,80
0,60
0,40
0,20
0,00
0,55
0,80
0,30
0,60
0,80
0,63
0,23
0,68
0,56
0,20
0,40
0,45
0,68
0,68
0,51
0,50
0,38
0,80
0,80
0,18
0,73
0,63
0,00
0,63
1,00
D6 (Total)
TRT01
TRT02
TRT03
TRT04
TRT05
TRT06
TRT07
TRT08
TRT09
TRT10
TRT11
TRT12
TRT13
TRT14
TRT15
TRT16
TRT17
TRT18
TRT19
TRT20
TRT21
TRT22
TRT23
TRT24
Tribunal Regional

PRIVACIDADE

TRT-9ª REGIÃO
Paraná

PRIVACIDADE

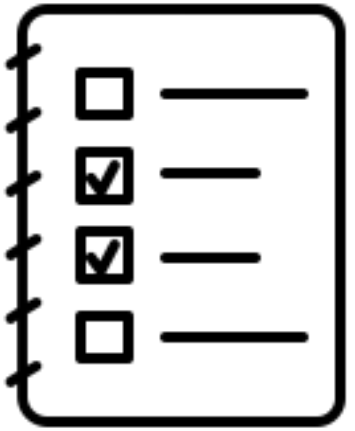
Programa de Governança em Privacidade

A Lei nº 13.709, de 14 de agosto de 2019 (Lei Geral de Proteção de Dados) impôs às organizações públicas e privadas a implementação de um Programa de Privacidade de Dados Pessoais

O Programa de Privacidade de Dados Pessoais no âmbito do TRT da 9ª Região tem como visão

implantar os requisitos exigidos pela LGPD.

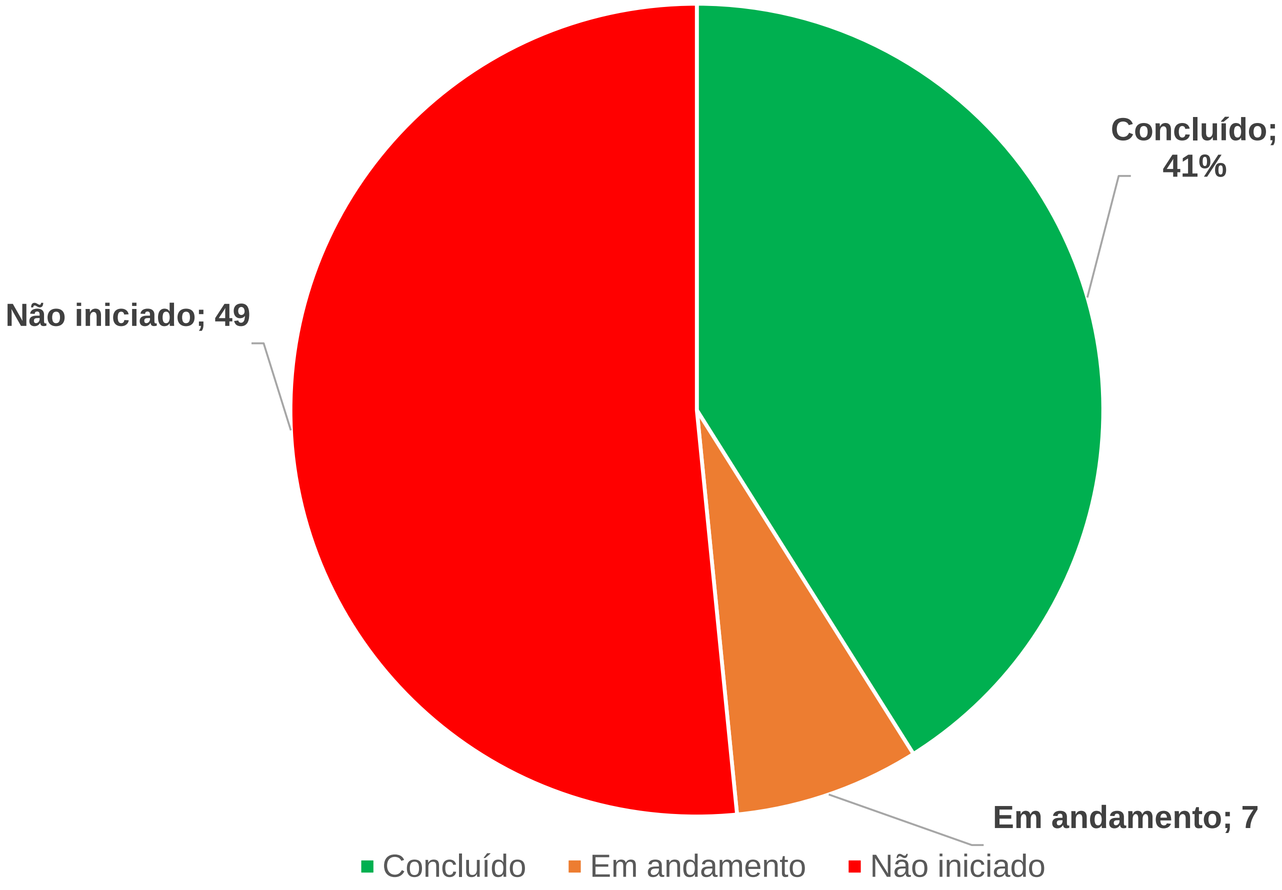
Projetos do Programa



Visão geral do Andamento do Programa

Ações previstas - LGPD	
Concluídas	**39**
Em andamento	**7**
Não iniciadas	**49**

Obs: Considerando todos os projetos do Programa e as atividades identificadas até Março/2024



Andamento/Previsão

Projeto 1 - Normas de segurança e privacidade de dados – concluído

Projeto 2 - Interação com os Titulares dos dados para exercícios de seus direitos – concluído

Projeto 3 - Formação e divulgação – Concluído, porém, treinamento deve ser uma ação constante

Projeto 4 - Descoberta e classificação (Inventário) - Elaboramos o inventário de Dados, porém, não iniciamos a gestão do tratamento de dados pessoais, incluindo o dever de informar ao titular e as obrigações dos envolvidos

Projeto 5 - Gestão do Consentimento – Projeto não caminhou, parou na identificação de todos os pontos de contato e/ou processos onde o consentimento do titular dos dados é necessário

Projeto 6 - Relatório de Impacto à Proteção de Dados Pessoais – Projeto parou na análise/aprovação do processo de avaliação de riscos

PRIVACIDADE

TRT-9ª REGIÃO
Paraná

Andamento/Previsão

Projeto 7 - Implementação de Medidas de Proteção – Identificadas diversas relações com o projeto de atendimento à RES 396 - manual de Referência – Proteção de Infraestruturas Críticas de TIC (Unidade responsável: Seção de Segurança da Informação), cujas ações se encontram em andamento, porém, o andamento do projeto depende da conclusão do projeto 6

Projeto 8 - Tratamento a incidentes de segurança – Estabeleceu-se procedimentos para comunicar à Autoridade Nacional de Proteção de Dados e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, demais questões técnicas não iniciadas por dependência dos projetos 6 e 7

Projeto 9 – Contratos – Inventário dos contratos e modelos de contratos estabelecidos, porém, a ausência de um sistema de contratos capaz de tratar os dados pessoais de forma estruturada inviabilizou a análise e o cruzamento das informações registradas no inventário de dados pessoais com as registradas no inventário de contratos

Projeto 10 - Adequações tecnológicas - Revisão dos sistemas computacionais atuais para que estejam aderentes à LGPD – Projeto não iniciado


PRIVACIDADE
?
Dúvidas ?
TRT-9ª REGIÃO
Paraná

Poder Judiciário
Conselho Nacional de Justiça

PORTARIA PRESIDÊNCIA Nº 140 DE 22 DE ABRIL DE 2024.

Determina a implementação do método de autenticação do tipo Múltiplo Fator de Autenticação (MFA) como requisito funcional para acesso a sistemas judiciais sensíveis.

O **PRESIDENTE DO CONSELHO NACIONAL DE JUSTIÇA (CNJ)**, no uso de suas atribuições legais e regimentais, e o contido no processo SEI nº 10142/2020,

CONSIDERANDO a Resolução CNJ nº 435/2021, que dispõe sobre a política e o sistema nacional de segurança do Poder Judiciário e dá outras providências, estabelecendo diretrizes para a proteção das informações e da infraestrutura crítica de Tecnologia da Informação e Comunicação (TIC);

CONSIDERANDO a Resolução CNJ nº 396/2021, que Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Resolução CNJ nº 370/2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), visando à modernização e à eficiência dos serviços judiciários por meio da tecnologia;

CONSIDERANDO a Resolução CNJ nº 335/2020, que institui política pública para a governança e a gestão de processo judicial eletrônico, integrando os tribunais do país com a criação da Plataforma Digital do Poder Judiciário Brasileiro – PDPJ-Br e mantendo o sistema PJe como sistema de Processo Eletrônico prioritário do Conselho Nacional de Justiça;

CONSIDERANDO a Portaria CNJ nº 316/2023 que Disciplina as práticas de gestão de identidade e controle de acesso ao sistema de Controle de Acessos (SCA) Corporativo do Conselho Nacional de Justiça;

CONSIDERANDO a deliberação da 12ª Reunião do Comitê Gestor de Segurança da Informação do Poder Judiciário (CGSI-PJ), que reconheceu a importância de fortalecer as medidas de segurança da informação e de proteger os sistemas judiciários contra ameaças cibernéticas;

CONSIDERANDO que o Conselho Nacional de Justiça é o Órgão de Gestão Superior (OGS) do Poder Judiciário;

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES INICIAIS

Art. 1º Determinar aos órgãos do Poder Judiciário Brasileiro, com exceção do Supremo Tribunal Federal (STF), a implementação de método de autenticação do tipo Múltiplo Fator de Autenticação (MFA) como requisito funcional para acesso a sistemas judiciais sensíveis.

§ 1º O uso de MFA é obrigatório para usuários internos e externos.

§ 2º A habilitação do MFA é mandatória, não cabendo aos usuários optarem por sua utilização.

§ 3º A implementação do MFA não exclui ou limita a aplicação de outras medidas de segurança ou práticas que contribuam para o fortalecimento da segurança da informação e proteção de dados, devendo ser associada a uma cadeia de credenciais confiáveis adequadamente protegidas.

Art. 2º Consideram-se sistemas judiciais sensíveis:

a) sistemas de processo judicial eletrônico;

b) sistemas ou serviços que permitam acesso a dados sensíveis ou confidenciais;

c) sistemas ou serviços que permitam a emissão de mandados de prisão e alvarás de soltura;

d) sistemas ou serviços que permitam a pesquisa de ativos financeiros, sua constrição e movimentação;

e) sistemas de tramitação de processos administrativos;

f) ferramentas de acessos a redes privadas virtuais (VPNs);

g) sistemas ou serviços que permitam acesso remoto ao ambiente interno de rede;

h) sistemas ou serviços de e-mail funcional ou corporativo;

i) quaisquer outros sistemas ou serviços considerados críticos na avaliação interna do Tribunal, incluindo quaisquer sistemas expostos ao acesso remoto via internet.

§ 1º Sistemas de processo judicial eletrônico e módulos da Plataforma Digital do Poder Judiciário Brasileiro (PDPJ-Br) deverão utilizar o Serviço de Autenticação Única (Single Sign-On - SSO) disponibilizado na PDPJ-Br.

§ 2º Ficam excluídos da obrigatoriedade de implementação do MFA os serviços públicos cuja utilização não depende de autenticação.

CAPÍTULO II
DA GESTÃO DO MÚLTIPLO FATOR DE AUTENTICAÇÃO

Seção I
Dos Critérios de Seleção

Art. 3º Os Órgãos integrantes do Poder Judiciário brasileiro deverão considerar os seguintes critérios na seleção dos métodos de MFA:

I - Compatibilidade: escolha de métodos de MFA que se integrem de maneira eficiente com a infraestrutura tecnológica existente;

II - Usabilidade: priorização de soluções que ofereçam facilidade de uso para promover ampla adoção pelos usuários; e

III - Segurança: avaliação rigorosa do nível de segurança fornecido por cada método de MFA, visando proteção efetiva contra ameaças cibernéticas.

Seção II
Mecanismos de Revisão e Atualização do Múltiplo Fator de Autenticação (MFA)

Art. 4º Determinar aos órgãos do Poder Judiciário brasileiro que desenvolvam e implementem mecanismos eficientes de monitoramento para avaliar, de forma contínua, a eficácia das medidas de MFA adotadas. Este monitoramento deverá incluir a análise de tentativas de acesso, a taxa de sucesso de autenticações MFA e a detecção de padrões anormais que possam indicar tentativas de violação.

Parágrafo único. Caso o método de MFA implementado seja considerado insuficiente em termos de eficácia, eficiência, segurança ou usabilidade, o órgão deverá tomar as medidas necessárias para sua revisão ou substituição, podendo incluir a avaliação de novas tecnologias de autenticação e a implementação de soluções mais robustas e adaptáveis às necessidades atuais e futuras.

Art. 5º Determinar aos órgãos que adotem processo de revisão regular, pelo menos anualmente, para identificar necessidades de aprimoramento tecnológico ou ajustes nas políticas de MFA. Este processo considerará as evoluções tecnológicas, as novas ameaças de segurança cibernética e as melhores práticas de segurança recomendadas por entidades nacionais e internacionais de segurança da informação.

Parágrafo único. Todas as revisões, atualizações e substituições de soluções MFA deverão ser devidamente documentadas, incluindo justificativa para as mudanças, impactos esperados e orientações para implementação. As atualizações serão comunicadas a todos os usuários afetados de forma clara e acessível, garantindo a compreensão e a adoção das novas medidas.

Seção III
Capacitação e Compartilhamento

Art. 6º Determinar aos órgãos do Poder Judiciário brasileiro que desenvolvam ações periódicas de capacitação e conscientização de seus usuários, internos e externos, destinadas a garantir uso seguro e eficaz do MFA.

Parágrafo único. A periodicidade das ações de que trata o caput deste artigo será definida pelo órgão e informado anualmente ao Conselho Nacional de

Justiça.

CAPÍTULO III
DAS DISPOSIÇÕES FINAIS

Art. 7º É responsabilidade do Comitê Gestor de Segurança da Informação do Poder Judiciário realizar o monitoramento da implementação do múltiplo fator de autenticação nos órgãos do Poder Judiciário, propondo as adaptações necessárias e compartilhando melhores práticas.

Art. 8º Fixar o prazo de 90 (noventa) dias para implementação do múltiplo fator de autenticação (MFA), nos termos desta Portaria.

Art. 9º Esta Portaria entre em vigor na data de sua publicação.

Documento assinado eletronicamente por **Luís Roberto Barroso**, **PRESIDENTE**, em 24/04/2024, às 14:33, conforme art. 1º, §2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no portal do CNJ informando o código verificador **1834303** e o código CRC **957CF237**.

PODER JUDICIÁRIO FEDERAL
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 9ª REGIÃO
COMITÊ DE DOCUMENTAÇÃO E MEMÓRIA

EDMILSON ANTONIO DE LIMA 01/04/2024

Ofício CDOM n. 02/2024

Curitiba, 26 de março de 2024.

A Sua Excelência, o Senhor
Desembargador **MARCUS AURELIO LOPES**
Comitê de Segurança da Informação e Proteção de Dados (CSIPD) e do Grupo de Trabalho Técnico LGPD
Curitiba-PR

Assunto: **Participação nas reuniões do Comitê de Segurança da Informação e Proteção de Dados (CSIPD) e do Grupo de Trabalho Técnico LGPD.**

Senhor Desembargador,

Cumprimentando-o, informo que, nos termos do artigo 14, incisos I e II, da RA 45/2018 do Tribunal Pleno, compete à Coordenadoria de Arquivo e Gestão Documental:

> "I – orientar quanto aos procedimentos para classificação da informação e dos documentos e disponibilizar instrumentos necessários, de forma a subsidiar o trabalho das unidades do TRT, inclusive promovendo ações de capacitação aplicáveis;
>
> II – auxiliar a unidade de tecnologia da informação responsável pela solução informatizada de gestão de documentos e informações para utilização dos instrumentos mencionados no inciso I deste artigo;"

Nesse contexto, solicito que seja autorizada a participação do Coordenador da CAGD e da Chefe da DMEP, ou de substitutos por eles indicados, na condição de convidados, nas reuniões do Comitê de Segurança da Informação e Proteção de Dados (CSIPD) e do Grupo de Trabalho Técnico LGPD.

Contando com a colaboração de Vossa Excelência, renovo votos de elevada estima e distinta consideração.

(assinado digitalmente)
EDMILSON ANTONIO DE LIMA
Desembargador Coordenador do Comitê de Documentação e Memória