WHANDER JEFFSON DA SILVA COSTA
EDSON FURTADO ALVES JUNIOR

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
Secretaria de Auditoria Interna

# RELATÓRIO FINAL DE ACHADOS DE AUDITORIA

AUDITORIA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

**TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO - RO/AC**

**A1 - Falhas no Processo de Gerenciamento de Incidentes de Segurança da Informação**

**Situação Encontrada:**

Por intermédio das respostas ao questionário de auditoria interna e de consulta aos documentos apresentados como evidência das respostas ao referido questionário, esta unidade de auditoria interna constatou o seguinte:

**- Item 1.2.3:** Não foram realizadas ações para o desenvolvimento das competências sobre segurança da informação nos últimos 2 anos;

**- Item 1.2.5:** A fase de detecção não prevê interação com o monitoramento e gerenciamento de eventos;

**- Item 1.2.6:** O processo de gerenciamento de incidentes de SI não prevê as ações responsivas a serem colocadas em prática quando ficar evidente que um incidente de segurança cibernética não será mitigado rapidamente;

**- Item 1.2.7:** Apesar de a SETIC responder que o processo de gerenciamento de incidentes de segurança da informação estabelece critérios para iniciar o gerenciamento de crise, esta Unidade de Auditoria não localizou os referidos critérios na Política de Segurança da Informação nem no processo formal de gerenciamento de incidentes de SI do Tribunal;

**- Item 1.2.8:** O processo de gerenciamento de incidentes de segurança da informação não contempla incidentes ocorridos nos serviços em nuvem contratados pelo órgão;

**- Item 1.2.9:** O processo não prevê a comunicação de todos os incidentes graves ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário;

**- Item 1.2.10:** O processo de gerenciamento de incidentes de SI não contempla a etapa de lições aprendidas pós-crise.

**- Item 1.2.11:** Embora o processo de incidentes de segurança da informação preveja a elaboração de um Relatório de Comunicação de Incidente de Segurança da Informação, não há um modelo padronizado, contendo a descrição e o detalhamento da crise e o plano de ação tomado, que contemple, no mínimo, os subitens do item 4.4. Anexo III (Protocolo – Investigação para Ilícitos Cibernéticos do Poder Judiciário) da Portaria CNJ 162/2021.

**Manifestação do Auditado:**

Em resposta ao Mapa de Achados Preliminar da Ação de Auditoria de Gestão de Avaliação da Segurança da Informação, coordenada pelo Conselho Superior da Justiça do Trabalho - CSJT, a Secretaria de Tecnologia de Informação e Comunicação - SETIC informou que:

**Item 1.2.3**: os servidores da Seção de Segurança da Informação realizam frequentemente cursos relacionados à área de segurança da informação - SI. (Conforme Proads 1846/2021, 4094/2021, 622/2022), mas que adotará as providências necessárias para definir um Plano de Capacitação em SI, conforme tarefa já iniciada (registro no redmine: Tarefa #31038), porém ainda não finalizada.

Em relação às lacunas de competências que exigirão capacitação complementar, para atendimento do item 1.2.3 da Matriz de Planejamento (questionário), a SETIC informou que os Membros da ETIR necessitam das seguintes

capacitações elencadas no item 2.2, do anexo VII da Portaria CNJ 162/2021, abaixo:

a) governança e gestão de segurança cibernética;
b) tratamento de incidentes de segurança cibernética;
c) forense computacional;
d) inteligência e investigação em crimes cibernéticos;
e) gestão de riscos de TIC e SI;
f) auditoria e conformidade de sistemas de informação;
g) segurança em computação em nuvem;
h) segurança em redes sociais.

**Itens 1.2.5, 1.2.6, 1.2.7, 1.2.8, 1.2.9 e 1.2.10**: revisará o Plano de Continuidade de TIC, o qual está em processo de revisão para atender ao Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ - Anexo II da ENSEC-JUD).

Porém, ressaltou que o Plano de Continuidade de TIC está aguardando a definição do Plano de Continuidade de Negócios - PCN do TRT14 (Solicitado via Proad 4045/2022, desde 26/07/2022), documento necessário para a identificação dos ativos e atividades críticas de TIC e que outra necessidade encontrada para identificação dos ativos de TIC é a finalização da Ação de Contratação (redmine:Tarefa #33126) da Solução de gerenciamento de vulnerabilidades de ativos de TIC (coparticipação TRT8 - Proad 2329/2022).

Informou ainda que está com a solicitação de mapeamento do Macroprocesso Crítico de Segurança da Informação/Proteção de Dados, conforme Proad Nº 4094/2022, o qual providenciará a interação entre os processos de monitoramento e gerenciamento de eventos de TIC.

**Item 1.2.11**: a Seção de Segurança da Informação possui um modelo, mas que, entretanto providenciará a adequação do modelo de relatórios contendo os itens que faltam incluir da Portaria CNJ 162/2021, Anexo III - Protocolo – Investigação para Ilícitos Cibernéticos do Poder Judiciário, item 4.4.

**Análise e Conclusão:**

**Item 1.2.3**: Em sua manifestação, a SETIC informa que os servidores da Seção de Segurança da Informação realizam frequentemente cursos relacionados à área de segurança da informação, mas que adotará as providências necessárias para definir um Plano de Capacitação nessa área.

No entanto, esta Unidade de Auditoria constatou que, dos membros da ETIR, somente os 2 servidores lotados na Seção de Segurança da Informação da SETIC receberam capacitação em segurança cibernética, sendo que a maioria dos membros da ETIR não participou de treinamento relacionados à Segurança da Informação nos últimos 2 anos. Logo, conclui-se pela necessidade que os outros membros da ETIR realizem capacitação complementar nas áreas apontadas pela SETIC em resposta aos item 1.2.3.

**Item 1.2.11**: Tendo em vista a manifestação da SETIC e o encaminhamento do Modelo de Relatório de Incidentes de Segurança da Informação utilizado no TRT14 contendo a descrição e o detalhamento da crise e o plano de ação tomado, esta Unidade de Auditoria constatou que resta apenas um ajuste no referido modelo de relatório para que contemple os subitens ‘a’ e ‘’b’ do item 4.4, Anexo III, da Portaria CNJ 162/2021.

| | |
|---|---|
| **Objeto(s):** | Processo de Gestão de Incidentes de Segurança da Informação. |
| **Critério(s):** | - Resolução CNJ 396/2021, art. 19, inciso IV;<br><br>- Norma Complementar nº 08/IN01/DSIC/GSIPR, item 8.4;<br><br>- Portaria CNJ 162/2021, Anexo I - Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário, item 2.1.3;<br><br>- Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, itens 1.1, 2.2, 5.9 e 6;<br><br>- Instrução Normativa GSI/PR 5/2021, art. 16, inciso IV. |
| **Evidência(s):** | Resposta da SETIC aos itens 1.2.3, 1.2.5, 1.2.6, 1.2.7, 1.2.8, 1.2.9, 1.2.10 e 1.2.11 do questionário de auditoria. |
| **Causa(s):** | - Incipiência na implantação do sistema de gestão de segurança da informação; |

| | |
|---|---|
| | - Ausência de capacitação para os membros da ETIR e disseminação do assunto em âmbito institucional. |
| **Efeito(s)** | Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT;<br><br>Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT. |
| **Proposta de Encaminhamento** | Recomendar à Secretaria de Tecnologia da Informação e Comunicação do TRT da 14ª Região que:<br><br>**I - Promova a capacitação técnica para os membros da Equipe de Tratamento e Respostas a Incidentes de Segurança da Informação - ETIR**, com vistas ao aprimoramento e à efetiva implantação de seu processo de gerenciamento de incidentes de segurança da informação, nos seguintes temas elencados no item 2.2, do anexo VII da Portaria CNJ 162/2021:<br>a) governança e gestão de segurança cibernética;<br>b) tratamento de incidentes de segurança cibernética;<br>c) forense computacional;<br>d) inteligência e investigação em crimes cibernéticos;<br>ei) gestão de riscos de TIC e SI;<br>fj) auditoria e conformidade de sistemas de informação;<br>g) segurança em computação em nuvem;<br>h) segurança em redes sociais.<br><br>**II - Aperfeiçoe o processo de gerenciamento de incidentes de segurança da informação**, nos termos da Portaria CNJ 162/2021, de forma que contemple, no mínimo, os seguintes elementos:<br><br>a) a interação com os processos de monitoramento e gerenciamento de eventos de TI, de acordo com a Portaria CNJ 162/2021, Anexo I, item 2.1.3.<br><br>b) a previsão das ações responsivas a serem colocadas em prática quando ficar evidente que um incidente de segurança cibernética não será mitigado rapidamente (identificação de crise cibernética) e os critérios para iniciar o gerenciamento de crise, em consonância com a Portaria CNJ 162/2021, Anexo II, item 1.1;<br><br>c) o estabelecimento de critérios para iniciar o gerenciamento de crise, que contemple as situações descritas no item 2.2 do Anexo II da Portaria CNJ 162/2021;<br><br>d) os incidentes ocorridos nos serviços em nuvem contratados pelo órgão (Ex.: *GOOGLE SUITE*), conforme a Instrução Normativa - IN GSI/PR 5/2021, art. 16, inciso IV.<br><br>e) a comunicação de todos os incidentes graves ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), de acordo com a Portaria CNJ 162/2021, Anexo II, item 5.9; e<br><br>f) a etapa de lições aprendidas pós-crise, conforme descrito na Portaria CNJ 162/2021, Anexo II, item 6.<br><br>**III - Ajuste o Modelo do Relatório de Incidente de Segurança da Informação - RISI**, previsto no Processo de Gerenciamento de Incidentes de Segurança da Informação do TRT14, para que contemple os subitens ‘a’ e ‘’b’ do item 4.4, Anexo III, da Portaria CNJ 162/2021, descritos abaixo:<br><br>4.4. O Relatório de Comunicação de Incidente de Segurança Cibernética deverá conter as seguintes informações, sem prejuízo de outras julgadas relevantes:<br>a) nome do responsável pela preservação dos dados do incidente, com informações de contato;<br>b) nome do agente responsável pela ETIR e informações de contato; |

**A2 - Falhas na Gestão de Continuidade dos Serviços Essenciais de TIC**

**Situação Encontrada:**

Por intermédio das respostas ao questionário de auditoria interna e de consulta aos documentos apresentados como evidência das respostas ao referido questionário, esta unidade de auditoria interna constatou o seguinte:

**- Item 2.2.2:** O programa de Gestão da Continuidade dos Serviços Essenciais de TI não contém a definição das atividades críticas de negócio a serem contempladas, abarcando, no mínimo, os seguintes serviços: PJE-JT, SIGEP-JT (FOLHA + CADASTRO) ou sistema equivalente, Processo Administrativo, Portal Internet e solução de comunicação (EX: *GOOGLE SUITE*);

**- Item 2.2.3:** O programa não prevê a identificação dos ativos de informação críticos, incluindo as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação;

**- Item 2.2.4:** O programa não prevê a capacitação para as pessoas envolvidas nos procedimentos e processos definidos;

**- Item 2.2.5:** Não existe previsão de interação com o processo de gestão de riscos, com vistas a assegurar a avaliação contínua dos riscos a que as atividades críticas estão expostas e que possam impactar diretamente na continuidade do negócio;

**- Item 2.2.6:** Não há previsão de categorização dos incidentes e estabelecimento de procedimentos de resposta específicos (Por ex., Guia, Manual, Cartilha etc…);

**- Item 2.2.7:** Não há planos de contingência que detalham o monitoramento, o acompanhamento e o tratamento dos riscos de maior criticidade, em razão de possíveis cenários de crise; apenas estratégias simplificadas descritas no Plano de Continuidade dos Serviços Essenciais de TIC, conforme resposta ao questionário.

**- Item 2.2.8:** O programa de gestão da continuidade dos serviços essenciais de TI (Plano de Continuidade de TIC) não contém os elementos II, III e VI da Instrução Normativa GSI/PR 3/2021, art. 23, descritos abaixo:

> II - as atividades críticas de negócio a serem contempladas no plano (contemplado PC 2.2.1);
> III - os requisitos para ativação do plano, em especial, o tempo máximo aceitável de permanência da falha;
> VI - a definição:
> a) das ações necessárias para operacionalização das medidas cuja implementação dependa da aquisição de recursos físicos e/ou humanos;
> b) dos limites de decisão para os responsáveis pela aplicação das medidas de contingência perante situações inesperadas;
> c) dos parâmetros para encerramento do plano e para a volta à normalidade;
> d) dos responsáveis por essas ações, incluindo seus dados de contato;
> e) da forma de monitoramento desse processo; e
> f) de um roteiro de simulação de teste de funcionamento e da forma de sua aplicação.

**- Item 2.2.10:** O programa não estabelece critérios para sua revisão, como periodicidade (pelo menos anualmente), em função dos resultados dos testes de funcionamento realizados, uma vez comprovada a perda da validade e eficácia das medidas adotadas diante de novas situações; ou após mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes.

**Manifestação do Auditado:**

Em resposta ao Mapa de Achados Preliminar da Ação de Auditoria de Gestão de Avaliação da Segurança da Informação, coordenada pelo CSJT, a Secretaria de Tecnologia de Informação e Comunicação - SETIC informou que:

**Itens 2.2.2 e 2.2.3, 2.2.6:, 2.2.7, 2.2.8 e 2.2.10:** revisará o Plano de Continuidade de TIC, o qual está em processo de revisão para atender ao Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ) (Anexo II da ENSEC-JUD). Porém, ressaltamos que nosso Plano de Continuidade de TIC está aguardando a definição do Plano de Continuidade de Negócios - PCN do TRT14 (Solicitado via Proad 4045/2022, desde 26/07/2022), documento necessário para identificarmos os ativos e atividades críticas de TIC. Outra necessidade encontrada para identificação dos ativos de TIC é a finalização da Ação de Contratação #33126 (Solução de gerenciamento de vulnerabilidades de ativos de TIC (coparticipação TRT8 - Proad 2329/2022);

**Item 2.2.4:** A Seção de Segurança da Informação, juntamente com a Seção de Governança de TIC, definirá um Plano de Capacitação em S.I., conforme tarefa já iniciada (registro no redmine: Tarefa #31038), porém ainda não finalizada;

Em relação às lacunas de competências que exigirão capacitação complementar, para atendimento do item 2.2.4 da Matriz de Planejamento (questionário), a SETIC informou que as pessoas envolvidas nos procedimentos e processos de Gestão da Continuidade dos Serviços Essenciais de TIC necessitam das seguintes capacitações elencadas no item 2.2, do anexo VII da Portaria CNJ 162/2021, abaixo:

a) gerenciamento de identidades, acesso e privilégios;
b) gestão de continuidade de negócios;
c) gestão de riscos de TIC e SI.

**Item 2.2.5:** está com a solicitação de mapeamento do Macroprocesso Crítico de Segurança da Informação/Proteção de Dados (Conforme Proad Nº 4094/2022), o qual providenciará a integração entre os processos de segurança da informação, mas que entretanto, algumas ações requerem as mesmas providências que a solução dos itens “a)” e “b)”.

**Análise e Conclusão:**

Em sua manifestação, a SETIC ratifica o achado, logo, conclui-se pela necessidade de aprimoramento do Programa de Gestão da Continuidade dos Serviços Essenciais de TIC do TRT da 14ª Região.

| | |
|---|---|
| **Objeto(s):** | Programa de gestão da continuidade dos serviços essenciais de TI (Planos de Continuidade de TI) |
| **Critério(s):** | Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alíneas 'b', 'c', 'd', 'e' e 'f'.<br><br>NBR ISO 27002, item 17.1.2 - Implementando a continuidade da segurança da informação, alínea a;<br><br>NBR ISO 27002, item 17.1.3 - Verificação, análise crítica e avaliação da continuidade da segurança da informação, alínea b;<br><br>Instrução Normativa GSI/PR 3/2021, arts. 23 e 24. |
| **Evidência(s):** | Resposta da SETIC aos itens 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.7, 2.2.8 e 2.2.10 do questionário de auditoria. |
| **Causa(s):** | - Incipiência na implantação do sistema de gestão de segurança da informação;<br><br>- Ausência de capacitação para os membros da ETIR e disseminação do assunto em âmbito institucional. |
| **Efeito(s)** | Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT;<br><br>Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT. |
| **Proposta de encaminhamento** | Recomendar à Secretaria de Tecnologia da Informação e Comunicação do TRT da 14ª Região que **aprimore seu Programa de Gestão da Continuidade dos Serviços Essenciais de TIC**, de forma a contemplar, no mínimo, os seguintes elementos:<br><br>a) a definição das atividades críticas de negócio a serem contempladas, abarcando, no mínimo, os seguintes serviços: PJE-JT, SIGEP-JT (FOLHA + CADASTRO) ou sistema equivalente, Processo Administrativo e solução de comunicação (Ex.: *GOOGLE SUITE*);<br><br>b) a identificação dos ativos de informação críticos, incluindo as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação;<br><br>c) a capacitação dos servidores envolvidos nos procedimentos e processos da gestão da continuidade dos serviços de TIC nas seguintes temas: |

| | |
|---|---|
| | a) gerenciamento de identidades, acesso e privilégios;<br>b) gestão de continuidade de negócios;<br>c) gestão de riscos de TIC e SI.;<br><br>d) a integração com o processo de gestão de riscos, com vistas a assegurar a avaliação contínua dos riscos a que as atividades críticas estão expostas e que possam impactar diretamente na continuidade do negócio;<br><br>e) a categorização dos incidentes e estabelecimento de procedimentos de resposta específicos, incluindo os planos de contingência/recuperação, se aplicável, para cada tipo de incidente;<br><br>f) planos de contingência que detalham o monitoramento, o acompanhamento e o tratamento dos riscos de maior criticidade, em razão de possíveis cenários de crise;<br><br>f) planos de continuidade para os serviços essenciais de TIC, contendo os elementos II, III e VI da Instrução Normativa GSI/PR 3/2021, art. 23, descritos abaixo:<br><br>Art. 23. O plano de continuidade de negócios em segurança da informação deverá conter, no mínimo:<br>[...]<br><br>II - as atividades críticas de negócio a serem contempladas no plano (contemplado PC 2.2.1);<br>III - os requisitos para ativação do plano, em especial, o tempo máximo aceitável de permanência da falha;<br>VI - a definição:<br>a) das ações necessárias para operacionalização das medidas cuja implementação dependa da aquisição de recursos físicos e/ou humanos;<br>b) dos limites de decisão para os responsáveis pela aplicação das medidas de contingência perante situações inesperadas;<br>c) dos parâmetros para encerramento do plano e para a volta à normalidade;<br>d) dos responsáveis por essas ações, incluindo seus dados de contato;<br>e) da forma de monitoramento desse processo; e<br>f) de um roteiro de simulação de teste de funcionamento e da forma de sua aplicação.<br><br>g) critérios para a revisão do programa, tais como: periodicidade anual, em função dos resultados dos testes de funcionamento realizados e/ou após mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes; |

| **A3 - Falta de testes e simulações para validação dos Planos de Continuidade de TIC** |
|---|
| **Situação Encontrada:** |
| Por intermédio das respostas ao questionário de auditoria interna e de consulta aos documentos apresentados como evidência das respostas ao referido questionário, esta unidade de auditoria interna constatou que, em relação ao **item 2.2.9**, não foram realizados, até a presente data, simulações e testes para validação dos planos de continuidade de TIC. |
| **Manifestação do Auditado:** |
| Em resposta ao Mapa de Achados Preliminar, a SETIC informou que a Seção de Segurança da Informação vai elaborar um Plano de Ação para a realização de simulações e testes para validar o Plano de Continuidade de TIC, o qual está em processo de revisão para atender ao Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ), Anexo II da ENSEC-JUD. |

| | |
|---|---|
| Porém, ressaltou que o Plano de Continuidade de TIC está aguardando a definição do Plano de Continuidade de Negócios - PCN do TRT14 (Solicitado via Proad 4045/2022, desde 26/07/2022), documento necessário para identificarmos os ativos e atividades críticas de TIC. | |
| **Análise e Conclusão:** | |
| Em sua manifestação, a SETIC ratifica o achado, logo, conclui-se pela necessidade da realização de simulações e testes para validação dos planos de continuidade de TIC. | |
| **Objeto(s):** | Processo de Gestão de Incidentes de Segurança da Informação. |
| **Critério(s):** | Portaria CNJ 162/2021, Anexo II - Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário, item 4.1, alínea 'g'. |
| **Evidência(s):** | Resposta da SETIC ao item 2.2.9 do questionário de auditoria. |
| **Causa(s):** | - Incipiência na implantação do sistema de gestão de segurança da informação;<br>- Ausência de capacitação para os membros da ETIR e disseminação do assunto em âmbito institucional. |
| **Efeito(s)** | Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócios do TRT;<br>Indisponibilidade de serviços essenciais de TI, com prejuízo das atividades estratégicas do TRT. |
| **Proposta de encaminhamento** | Recomendar à Secretaria de Tecnologia da Informação e Comunicação do TRT da 14ª Região que **elabore um plano de ação para a realização de simulações e testes para validação dos planos de continuidade de TIC**. |

Porto Velho/RO, 31 de agosto de 2022.

| Auditor Responsável | Gestor da Unidade Auditoria |
|---|---|
| (assinado digitalmente)<br>EDSON FURTADO ALVES JÚNIOR<br>Matrícula 101579 | (assinado digitalmente)<br>WHANDER JEFFSON DA SILVA COSTA<br>Matrícula 101384 |

## ANEXO - SIGLAS

**CNJ** - CONSELHO NACIONAL DE JUSTIÇA

**CSJT** - CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO

**CGSI-PJ** - COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO DO PODER JUDICIÁRIO

**ENSEC-PJ** - ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA DO PODER JUDICIÁRIO

**ETIR** - EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA CIBERNÉTICA

**G SUITE** - CONJUNTO DE SERVIÇOS DO GOOGLE — GMAIL COMERCIAL, DRIVE, AGENDA, CHAT, DOCUMENTOS, PLANILHA, APRESENTAÇÃO, DENTRE OUTROS SERVIÇOS

**IN** - INSTRUÇÃO NORMATIVA

**PROAD** - SISTEMA DE PROCESSO ADMINISTRATIVO ELETRÔNICO

**PSI** - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

**RISI** - RELATÓRIO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

**SEAUDI** - SECRETARIA DE AUDITORIA INTERNA

**SETIC** - SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

**SI** - SEGURANÇA DA INFORMAÇÃO

**TI** - TECNOLOGIA DA INFORMAÇÃO

**TRT** - TRIBUNAL REGIONAL DO TRABALHO