PODER JUDICIÁRIO FEDERAL

TRIBUNAL REGIONAL DO TRABALHO DA 13ª REGIÃO

SECRETARIA DE AUDITORIA INTERNA

João Pessoa, Rua Corálio Soares, Centro

Telefone/Ramal: 6136 - E-mail: sci@trt13.jus.br

RELATÓRIO DE AUDITORIA

Auditoria de Gestão de Tecnologia da Informação e Comunicação

Resolução 211/2015 do CNJ – Ênfase em Infraestrutura

João Pessoa/PB – Novembro/2020

PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 13ª REGIÃO
SECRETARIA DE AUDITORIA INTERNA

RELATÓRIO CONCLUSIVO

1. IDENTIFICAÇÃO

1.1. Protocolo 10.160/2020

1.2. Área(s) Auditada(s): SETIC

1.3. Período Auditado: 2020

1.4. Objetivos: a) conformidade da gestão de TIC com os dispositivos da Resolução 211/2015 do CNJ; b) avaliação da qualidade e suficiência dos controles internos administrativos com vistas a garantir que seus objetivos estratégicos sejam atingidos

1.5. Escopo: ênfase em infraestrutura de TIC

1.6. Equipe de Auditoria: Maurício Dias Sobreira Bezerra; Nathália de Almeida Torres; Mari Hara Onuki Monteiro; José Hugo Leite Quinho, Marcos José Alves da Silva

SUMÁRIO

2. INTRODUÇÃO

A Secretaria de Auditoria Interna do Tribunal Regional do Trabalho da 13ª Região, em cumprimento ao seu Plano Anual de Auditoria 2019, instaurou a presente auditoria (comunicado de auditoria 9/2020 da SAI TRT 13ª Região, protocolo TRT PB 10.160/2020) com o objetivo de analisar a conformidade da gestão de TIC deste Regional com os dispositivos da Resolução 211/2015 do CNJ, no que diz respeito, prioritariamente, à infraestrutura de TIC, considerado o exercício de 2020.

Para tanto, delegou-se a responsabilidade aos servidores apontados pelo comunicado supra para desenvolver esta auditoria com vistas a responder as seguintes questões definidas na matriz de planejamento para a obtenção de evidências necessárias ao embasamento dos trabalhos:

- Na contratação de desenvolvimento de sistemas de informação considerados estratégicos, em que a propriedade intelectual não é deste Regional, faz-se constar no instrumento contratual cláusula que determine o depósito da documentação e afins pertinentes à tecnologia de concepção, manutenção e atualização, bem como, quando cabível, do código-fonte junto à autoridade brasileira que controla a propriedade intelectual de softwares, para garantia da continuidade dos serviços em caso de rescisão contratual, descontinuidade do produto comercializado ou encerramento das atividades da contratada?

- Os links de comunicação entre as unidades deste Regional são suficientes para suportar o tráfego de dados e garantir a disponibilidade exigida pelos sistemas de informação, especialmente o processo judicial, com o máximo de comprometimento de banda de 80%?

- Há, pelo menos, 2 (dois) links de comunicação deste Regional com a internet, mas com operadoras distintas para acesso à rede de dados, com o máximo de comprometimento de banda de 80%?

- Há, pelo menos, 1 (uma) solução de backup com capacidade suficiente para garantir a salvaguarda das informações digitais armazenadas, incluindo tecnologias para armazenamento de longo prazo e cópia dos backups mais recentes, em local

distinto do local primário deste Regional, de modo a prover redundância e atender à continuidade do negócio em caso de desastre?

- Há, pelo menos, 1 (uma) solução de armazenamento de dados e respectivos softwares de gerência, em que a capacidade líquida não ultrapasse 80% do limite máximo de armazenamento?

- Há, pelo menos, 1 (um) parque de equipamentos servidores suficientes para atender às necessidades de processamento de dados dos sistemas e serviços deste Regional, com comprometimento médio de até 80% de sua capacidade máxima, e em número adequado para garantir disponibilidade em caso de falha dos equipamentos?

O benefício estimado nesta auditoria consubstancia-se em garantir que os dispositivos da Resolução 211/2015 do CNJ estejam sendo observados por este Regional, o que implicará diretamente em uma melhoria na sua gestão bem como no fortalecimento dos seus controles internos.

3. VISÃO GERAL DO OBJETO

Analisar o grau de aderência deste Regional aos dispositivos da Resolução 211/2015 do CNJ, no que tange à infraestrutura de TIC, bem como avaliar os controles internos da SETIC, considerado o exercício de 2020.

3.1. SETOR(ES) ENVOLVIDO(S) NO ESCOPO DA AUDITORIA

- SETIC

3.2. LEGISLAÇÃO PERTINENTE UTILIZADA NA AUDITORIA

- Constituição Federal de 1988;
- Resolução 211/2015 do CNJ
- ABNT NBR ISO 3100..2009

4. METODOLOGIA

Para alcance dos objetivos e comprovação das questões definidas no planejamento, a equipe seguiu a metodologia relativa à auditoria de conformidade atualmente adotada pelos diversos Órgãos e Entidades de Fiscalização Superior (EFS), notadamente a Resolução 309/2020 do Conselho Nacional de Justiça (CNJ), sendo utilizadas as seguintes técnicas de auditoria:

- Análise documental – verificação de processos e documentos que conduzam à formação de indícios e evidências – foi analisada a documentação apresentada nos autos dos protocolos 10.554/2020 e 10.160/2020, bem como os processos mapeados pela SETIC, conforme melhor visto no capítulo relativo à avaliação dos controles internos.

A presente auditoria não sofreu nenhum tipo de limitação.

5. ACHADOS

Este item relaciona os achados de auditoria decorrentes dos exames realizados.

5.1

a) Achado de Auditoria:

A solução de backup responsável por garantir a salvaguarda das informações digitais armazenadas está centralizada na sede do Regional.

b) Situação Encontrada:

Há apenas uma solução de backup responsável pela salvaguarda dos dados dos servidores do interior e da capital e tal solução está centralizada em um único local, a sede do Regional.

c) Objeto:

A solução de backup dos sistemas informatizados.

d) Critério:

Resolução CNJ 211/2015:

Art. 24. O nivelamento da infraestrutura de TIC deverá obedecer aos seguintes requisitos mínimos:

[…]

VIII – **1 (uma) solução de backup** com capacidade suficiente para garantir a salvaguarda das informações digitais armazenadas, incluindo tecnologias para armazenamento de longo prazo **e cópia dos backups mais recentes, em local distinto do local primário do órgão**, **de modo a prover redundância** e atender à continuidade do negócio em caso de desastre; (destaque nosso)

e) Evidências:

Informações prestadas pela SETIC nos autos dos protocolos 10.554/2020 e 10.160/2020.

“Atendemos ao requisito parcialmente. O backup dos servidores do interior e da sede estão centralizados na sede.

Ha uma iniciativa de ter uma segunda cópia do backup no Fórum Maximiano Figueiredo, demanda formalizada no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC). Porém, esta demanda não pode ser realizada uma vez que ha um problema nas baterias dos no breaks que estabilizam a rede elétrica do Fórum. No momento ha um protocolo para compra de novas baterias (Protocolo 474/2020).

Sem uma rede estabilizada, não podemos levar um robô de backup para la, já que este tipo de equipamento é extremamente sensível a variações elétricas.” (protocolo 10.554/2020, sequencial 3)

“Informo que a implantação da solução de backup no FMF estava prevista no PDTI deste ano de 2020. Porém, não necessários ajustes prévios de engenharia para que seja possível a conclusão desta ação e o consequente atendimento ao que preconiza a Resolução 211. Tais ajustes foram solicitados ao CAEMA por meio do protocolo 11253/2020, no qual ressaltamos a urgência desta ação. Tão logo tais ajustes estejam concluídos, a SETIC promoverá a instalação da solução remota de backup.” (protocolo 10.160/2020, sequencial 4)

f) Causas da ocorrência do achado:

Conforme informado pela SETIC, a implantação de um backup de redundância no Fórum Maximiano Figueiredo depende: a) da compra de baterias para os no breaks que estabilizam sua rede elétrica (tal demanda está tramitando nos autos do protocolo 474/2020); b) instalação de novos circuitos elétricos dedicados (demanda presente no protocolo 11.253/2020).

g) Efeitos/Consequências do achado:

O efeito potencial desta falta de redundância na solução de backup é a perda de informações críticas em caso de desastre, o que poderia impedir a continuidade do negócio.

h) Manifestação do Órgão/Entidade ou do Responsável:

A SETIC informa que "[…] a solução para esta situação já está priorizada no PDTIC para ser realizada este ano, conforme deliberação do Comitê de Governança de TIC (CGOVTIC), na 1ª RAE de TIC de 2020;"

E que "[…] ainda não foi possível a implementação da solução, uma vez que a instalação de novos equipamentos na sala de TIC dependem de alguns requisitos de instalações elétricas que ainda não se encontram plenamente satisfeitos [...]"

E reconhece a "[…] urgência essa agravada pelos recentes ataques cibernéticos a órgãos do poder judiciário que colocam em risco os dados sensíveis das instituições […]"

(Informações colhidas no sequencial 1 do protocolo 11.253/2020)

i) Análise da Equipe de Auditoria:

Restou comprovado que o TRT/13 ainda não possui um backup de redundância em local destinto daquele em que se encontra o backup primário das informações contidas nos servidores da capital e do interior.

Mas, como se vê dos autos dos protocolos 474/2020 e 11.253/2020, a SETIC já iniciou um contato com os setores competentes deste Regional para que possa dar cumprimento ao disposto na Resolução 211/2015 daquele Conselho Superior.

j) Recomendações:

Implantar, pelo menos, 1 (uma) solução de backup com capacidade suficiente para garantir a salvaguarda das informações digitais armazenadas, incluindo tecnologias para armazenamento de longo prazo e cópia dos backups mais recentes, em local distinto do local primário deste Regional, de modo a prover redundância e atender à continuidade do negócio em caso de desastre.

k) Benefícios Esperados:

A implantação de, pelo menos, 1 (uma) solução de backup com capacidade suficiente para garantir a salvaguarda das informações digitais armazenadas, incluindo tecnologias para armazenamento de longo prazo e cópia dos backups mais recentes, em local distinto do local primário deste Regional, garantirá a redundância necessária para atender à continuidade do negócio em caso de desastre.

6. AVALIAÇÃO DA QUALIDADE E SUFICIÊNCIA DOS CONTROLES INTERNOS

O TCU, no Glossário de Termos do Controle Externo (BRASIL, 2017), define controles internos como *"ações estabelecidas por meio de **políticas e procedimentos** que ajudam a garantir o cumprimento das diretrizes determinadas pela adminitração para mitigar os riscos à realização dos objetivos."*

A Avaliação de Controles Internos, seja no nível especifíco dos processos organizacionais (nível de atividades) ou no nível global de uma organização (nível de entidade), fundamenta-se em três conceitos elementares: objetivos, riscos e controles.

Objetivo é 'algo' que se estabeleceu para ser alcançado.

Risco é a possibilidade de algo acontecer e impedir ou dificultar o alcance de um objetivo.

Controle é o que se faz para mitigar riscos, assegurando, assim, com certa razoabilidade, que objetivos sejam alcançados.

Desse modo, para se avaliar os controles internos, é necessário o cumprimento das seguintes etapas:

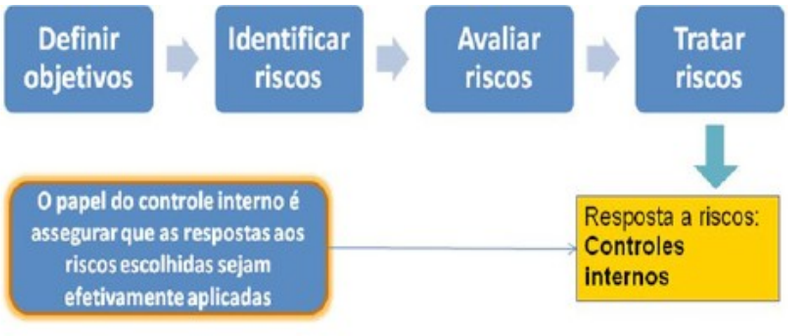

Figura 1: objetivos e riscos: a razão de ser do controle interno (Instituto Serzedello Corrêa – Avaliação de Controles Internos).

Isso significa que a verificação do grau de confiança dos controles internos só poderá ser realizado após a definição dos objetivos e posterior identificação e avaliação dos riscos do processo.

O TRT 13ª possui 19 (dezenove) processos de TIC mapeados onde são descritos **os objetivos** de cada processo, são eles:

PROCESSOS DE TIC MAPEADOS	
GOVERNANÇA E GESTÃO	
PROCESSO	**OBJETIVOS**
Processo de Gerenciamento de Projetos e Portfólio de TIC (Ato TRT GP nº 398/2016 e Ato TRT SGP nº 036/2020).	I - Conferir maior eficiência às atividades desenvolvidas na SETIC, bem como maior visibilidade ao andamento dos projetos de TIC, ao proporcionar amplo controle sobre os recursos humanos e financeiros, assim como sobre a qualidade e o tempo na execução das demandas; II - Assegurar que processos, métodos, procedimentos, técnicas e documentos padronizados sejam usados para análise, registro e gerenciamento dos projetos e do portfólio de TIC; III - Melhor definição de prioridades de forma objetiva, clara e imparcial; IV - Aumentar a eficiência na comunicação entre a área de negócio e a equipe de TIC; V - Promover o alinhamento do Portfólio de TIC aos planos de

	observância obrigatória pela SETIC; VI - Melhorar a satisfação do usuário com a qualidade dos serviços prestados pela SETIC.
Processo de Contratação de Soluções de TIC (Ato TRT GP nº 473/2014 e Ato TRT GP nº 189/2018).	Estabelecer as diretrizes para as contratações de Soluções de Tecnologia da Informação e Comunicação (SETIC).
Processo de Planejamento Estratégico de TIC (Ato TRT GP nº 70/2019). Processo de Planejamento e Monitoramento das Contratações e Orçamento de TIC (Ato TRT SGP nº 161/2019).	Definir a missão, visão, objetivos estratégicos, valores e indicadores estratégicos de TIC do TRT 13. I - Elaborar o plano das contratações e orçamentário de TIC de acordo com as demandas das unidades deste Tribunal; II - Atualizar, quando necessário, os planos das contratações e orçamentário de TIC; III - Assegurar que os planos das contratações e orçamentário de TIC sejam executados.
SOFTWARE	
PROCESSO	**OBJETIVOS**
Processo de Desenvolvimento de Software (Ato TRT GP nº 444/2016).	I - Padronizar os atos de desenvolvimento de sofware no TRT da 13ª Região; II - Especificar os procedimentos necessários à criação, melhoria e correção de software neste Tribunal.
Processo de Homologação e	I - Ter um processo definido para

Implementação de uma nova versão do PJE (Ato TRT SGP nº 139/2019).	implantar novas versões do PJE no âmbito do TRT13; II - Assegurar a homologação e implantação de uma nova versão do PJE no TRT13 de forma confiável e transparente.
SERVIÇOS	
PROCESSO	**OBJETIVOS**
Processo de Cumprimento de Requisições (Ato TRT GP nº 210/2018).	I – Definir, documentar, monitorar e medir o trabalho executado pela equipe da Central de Serviços e do Grupo Solucionador; II – Oferecer um canal para os usuários requisitarem e receberem serviços padronizados de TIC; III – Fornecer informações aos usuários relacionadas à disponibilidade dos serviços de TIC; IV – Auxiliar os usuários com informações gerais sobre os serviços de TIC; V – Receber reclamações e sugestões a respeito dos serviços de TIC.
Processo de Gerenciamento de Incidentes (Ato TRT GP nº 115/2016).	I - Assegurar que métodos e procedimentos padronizados sejam usados para pronta resposta, análise, documentação e gerenciamento de incidentes;

	II – Aumentar a visibilidade e comunicação de incidentes para o negócio e para a equipe de TIC; III – Melhorar a satisfação do usuário com a qualidade dos serviços de TIC.
Processo de Gerenciamento de Problemas (Ato TRT GP nº 053/2018).	I – Padronizar a forma como os problemas de TIC são registrados e solucionados; II – Gerenciar todo o ciclo de vida do problema; III – Eliminar incidentes recorrentes; IV – Assegurar que medidas proativas para melhoria dos serviços sejam implementadas; V – Minimizar o impacto adverso de incidentes inevitáveis; VI – Prevenir a ocorrência de incidentes e problemas resultantes.
Processo de Gerenciamento da Função Central de Serviços (Ato TRT GP nº 112/2018).	I – Definir, documentar, monitorar e medir o trabalho executado pela equipe da Central de Serviços; II – Fornecer e melhorar o relacionamento e a comunicação com o negócio e com os clientes;

	III – Prover um ponto único de contato para todos os usuários da área de TIC para tratamento dos incidentes e requisições de serviço.
Processo de Gerenciamento do Catálogo de Serviços de TIC (Ato TRT GP nº 114/2016).	I - Garantir que o catálogo de serviços seja a fonte central de informações sobre os serviços de TIC providos pela Setic; II - Assegurar a manutenção de informações precisas e atualizadas acerca dos serviços.
Processo de Gerenciamento de Nível de Serviço (Ato TRT GP nº 440/2017).	I – Padronizar a forma como os acordos de nível de serviço são criados ou modificados; II – Definir, documentar, monitorar, reportar e revisar o nível de serviço fornecido; III – Fornecer e melhorar o relacionamento e a comunicação com o negócio e com os clientes; IV – Assegurar que medidas proativas para melhoria dos serviços sejam implementadas; V – Monitorar e melhorar a satisfação do cliente com a qualidade do serviço entregue.
INFRAESTRUTURA	
PROCESSO	**OBJETIVOS**
Processo de Gerenciamento de	I - Responder aos requerimentos de

Mudanças (Ato TRT SGP nº 101/2019).	mudanças necessárias nos serviços, maximizando valor e reduzindo incidentes, rupturas e retrabalhos; II - Responder às solicitações de negócio e de TIC para mudanças que irão alinhar os serviços com as necessidades do negócio; III - Assegurar que as mudanças sejam registradas, avaliadas, autorizadas, priorizadas, planejadas, testadas e implementadas.
Processo de Gerenciamento de Configuração e Ativos de Serviço (Ato TRT GP nº 309/2018).	I – Definir e controlar os componentes de serviços e infraestrutura, mantendo informações precisas da configuração; II – Suportar os objetivos e os requerimentos de controle dos clientes e do negócio; III – Suportar todos os processos de gerenciamento de serviços; IV – Otimizar os ativos do serviço, as configurações de TIC, as capacidades e os recursos.
Processo de Liberação e Implantação (Ato TRT GP nº 004/2020).	I – ter um conjunto de passos definidos para implantar mudanças no ambiente de produção de maneira controlada e planejada; e II – assegurar a qualidade da

	implantação das mudanças no ambiente de produção.
SEGURANÇA DA INFORMAÇÃO	
PROCESSO	**OBJETIVOS**
Processo de Gestão de Riscos de SI (Ato TRT SGP nº 071/2020).	Definir a gestão de riscos de Segurança da Informação no âmbito do Tribunal Regional do Trabalho – 13ª Região, garantindo que os riscos sejam conhecidos, monitorados e tratados, promovendo a manutenção de um nível de risco aceitável.
Processo de Gestão de Incidentes de SI (Ato TRT SGP nº 072/2020).	Definir a gestão de incidentes de Segurança da Informação no âmbito do Tribunal Regional do Trabalho – 13ª Região – , garantindo que eles sejam conhecidos, monitorados, evitados e tratados.
Processo de Gestão de Continuidade de TIC (Ato TRT GP nº 383/2018).	Garantir que os serviços essenciais de TIC do Tribunal Regional do Trabalho – 13ª Região – funcionem em níveis aceitáveis durante incidentes de segurança da informação, e que a recuperação total dos serviços seja realizada em prazo aceitável.
Processo de Gestão de Vulnerabilidades de TIC (Ato TRT SGP nº 373/2019).	Definir a gestão de vulnerabilidades de TIC no âmbito do Tribunal Regional do Trabalho – 13ª Região –, garantindo que elas sejam conhecidas, monitoradas e tratadas.

Em 2019, foi concluída a execução do segundo ciclo do Processo de Gestão de Riscos em Segurança da Informação (protocolo TRT Nº 13.014/2019), regulamentado pelo ATO TRT GP Nº 458/2016, o qual

estabelece o processo e responsabilidades da Gestão de Riscos em Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 13ª Região, bem como descreve as atividades de **identificação, avaliação, tratamento, monitoramento e comunicação dos riscos** inerentes às atividades da instituição, incorporando a visão de riscos à tomada de decisões estratégicas, em conformidade com as melhores práticas de mercado e regulamentações pertinentes.

No decorrer da execução desta auditoria constatou-se que há apenas uma solução de backup responsável pela salvaguarda dos dados dos servidores do interior e da capital e tal solução está centralizada em um único local, a sede do Regional. Tal achado representa falha no componente de controle interno denominado **atividades de controle** e, apesar da previsão de implantação da solução de backup no Fórum Maximiano Figueiredo, tal falha representa um risco, de modo que os controles internos relacionados à Gestão da Tecnologia da Informação deste Regional foram avaliados como MEDIANOS, uma vez que mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes devido à deficiências no desenho ou ferramentas utilizadas.

7. RECOMENDAÇÕES

Com a finalidade de correção da falha apontada nos capítulos anteriores, foi feita a seguinte recomendação:

Implantar, pelo menos, 1 (uma) solução de backup com capacidade suficiente para garantir a salvaguarda das informações digitais armazenadas, incluindo tecnologias para armazenamento de longo prazo e cópia dos backups mais recentes, em local distinto do local primário deste Regional, de modo a prover redundância e atender à continuidade do negócio em caso de desastre.

8. CONCLUSÕES

A presente auditoria procurou analisar a conformidade da gestão de TIC deste Regional com os dispositivos da Resolução 211/2015 do CNJ, no que diz respeito, principalmente, à infraestrutura de TIC, considerado o exercício de 2020, bem como os controles internos da SETIC.

Das análises realizadas, surgiu um achado de auditoria, explicitado no capítulo 5 deste relatório, para o qual foi sugerida a seguinte ação:

a) Implantar, pelo menos, 1 (uma) solução de backup com capacidade suficiente para garantir a salvaguarda das informações digitais armazenadas, incluindo tecnologias para armazenamento de longo prazo e cópia dos backups mais recentes, em local distinto do local primário deste Regional, de modo a prover redundância e atender à continuidade do negócio em caso de desastre.

Importante ressaltar que tal ação, além de já priorizada no PDTIC para ser realizada este ano, onforme deliberação do Comitê de Governança de TIC (CGOVTIC), na 1ª RAE de TIC de 2020, torna-se ainda mais urgente, tendo em vista os recentes ataques cibernéticos a órgãos do poder judiciário que colocam em risco os dados sensíveis das instituições.

Com tal intento, já se encontram em tramitação os protocolos 474/2020 e 11.253/2020, que tem como objeto a instalação de equipamentos e ajustes nas instalações elétricas da sala de TIC do Fórum Maximiano Figueiredo, necessários para a implantação de um sistema de backup de redundância naquela localidade.

O acompanhamento dessas medidas se dará no protocolo de monitoramento da presente auditoria.

9. PROPOSTA DE ENCAMINHAMENTO

Em face do caráter conclusivo deste relatório, sugere-se seu envio ao Exmo. Sr. Presidente deste Tribunal Regional do Trabalho da 13ª Região, para conhecimento e adoção das providências que entender necessárias.

À superior apreciação do Diretor da Secretaria de Auditoria Interna.

Maurício Dias Sobreira Bezerra
(Líder da Equipe de Auditoria)

Nathália de Almeida Torres
(Membro da Equipe de Auditoria)

Mari Hara Onuki Monteiro
(Membro da Equipe de Auditoria)

Marcos José Alves da Silva
(Membro da Equipe de Auditoria)

José Hugo Leite Quinho
(Membro da Equipe de Auditoria)

GLOSSÁRIO

ABNT – Associação Brasileira de Normas Técnicas

CAEMA – Coordenação de Arquitetura, Engenharia e Manutenção

CNJ – Conselho Nacional de Justiça

FMF – Fórum Maximiano Figueiredo

GP – Gabinete da Presidência

ISO – International Organization for Standardization

NBR – Norma Técnica

PDTI – Plano Diretor de Tecnologia da Informação

PJE – Processo Judicial Eletrônico

RAE – Reunião de Avaliação Estratégica

SAI – Secretaria de Auditoria Interna

SETIC – Secretaria de Tecnologia da Informação e Comunicação

SGP – Secretaria-Geral da Presidência

SI – Segurança da Informação

TCU – Tribunal de Contas da União

TIC – Secretaria de Tecnologia da Informação e Comunicação

