PCSI

Politica corporativa de segurança da informação

o que eu tenho a ver com isso?

IMAGINE O QUE ACONTECERIA SE...

Documentos sigilosos que você coletou em uma auditoria vazassem na mídia?

Uma certidão emitida pelo TCU fosse adulterada e não fosse possível confirmar ou refutar sua autenticidade?

Você fosse redigir a versão final do seu relatório ou parecer e as informações da minuta tivessem desaparecido?

As informações que embasam o seu relatório ou parecer tivessem sido alteradas e você não pudesse ter certeza que elas estão corretas?

Alguém se manifestasse fraudulentamente nos autos utilizando sua assinatura?

Os acórdãos do TCU e os fundamentos das decisões não estivessem acessíveis aos cidadãos?

Houvesse vazamento de minuta de parecer de uma unidade sobre assunto polêmico?

A lista de responsáveis com contas julgadas irregulares encaminhada à Justiça Eleitoral fosse questionada por estar incompleta ou conter nomes cujas contas foram julgadas regulares?

Quando riscos à segurança da informação se materializam, podem comprometer a imagem do TCU e até o alcance de sua missão, além de imputar responsabilização aos servidores públicos envolvidos.

A segurança da informação visa à proteção da informação contra ameaças a sua confidencialidade, integridade, disponibilidade e autenticidade, para minimizar riscos, garantir a eficácia das ações do negócio e preservar a imagem do TCU.

QUEM É QUEM NA SEGURANÇA DA INFORMAÇÃO DO TCU

Você

Qualquer pessoa que tenha acesso a informações do TCU é responsável pela segurança da informação.

Gestor da Informação

(Colegiado, autoridade ou dirigente)
Responsável por classificar as informações sob sua gestão, e definir procedimentos e critérios de acesso.

Custodiante da Informação

(qualquer pessoa que detém a posse da informação)
Responsável por garantir a segurança da informação sob sua posse e comunicar sobre situações que comprometam essa garantia.

Dirigente de unidade ou subunidade do TCU

Responsável por conscientizar seus servidores e colaboradores em relação aos conceitos e práticas de segurança da informação, bem como incorporá-las aos processos de trabalho da unidade. Em caso de comprometimento da segurança da informação, devem tomar medidas administrativas para que sejam adotadas ações corretivas em tempo hábil.

Diretoria de Segurança da Informação e Continuidade de Negócio (Disic)

Apoia as unidades do TCU na definição de procedimentos para proteção de suas informações, monitora e avalia as práticas de segurança da informação do TCU e coordena ações de conscientização e treinamento, bem como de tratamento de incidentes de segurança da informação.

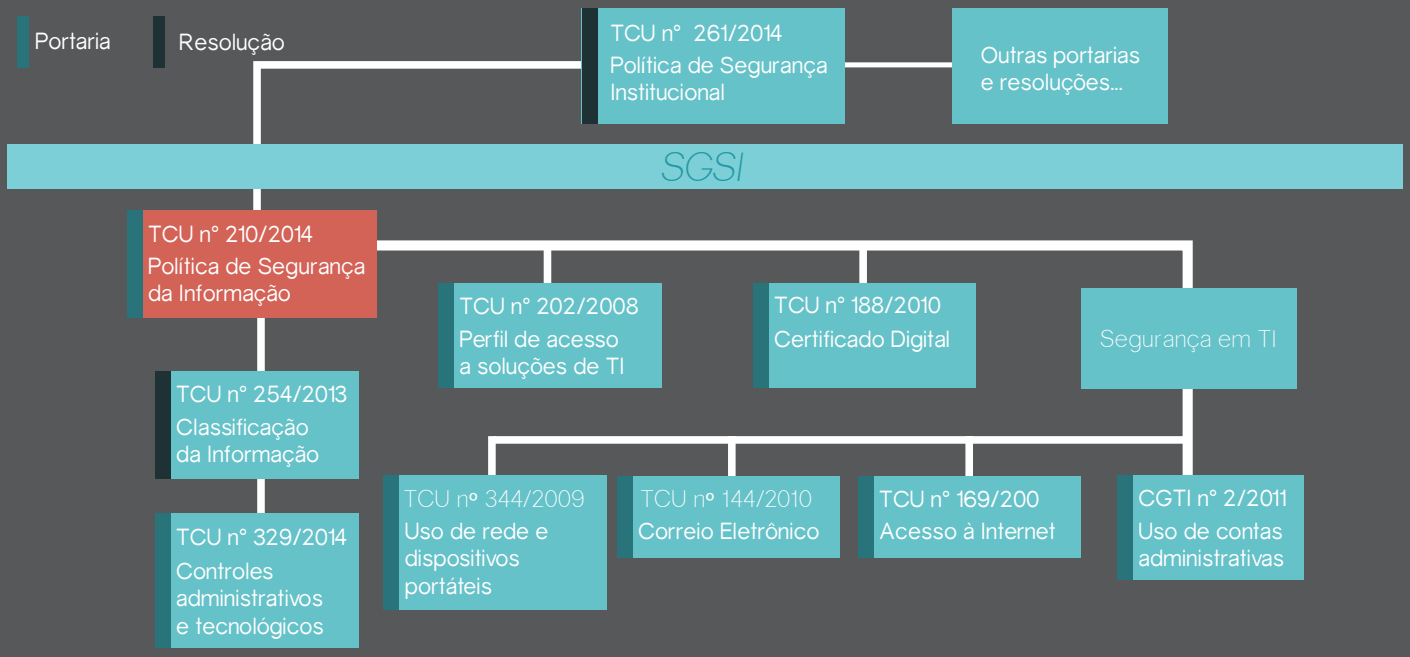
Comitê de Segurança Institucional (Cosin)

Constituído por representantes de diversas áreas de negócio, o Cosin formula e conduz diretrizes, analisa a efetividade e propõe melhorias para a Política de Segurança Institucional.

ESTRUTURA NORMATIVA

A PCSI é parte integrante da Política de Segurança Institucional (Resolução-TCU nº 261/2013). Essa política estabelece o Sistema de Gestão de Segurança da Informação (SGSI) do TCU, cujos processos são definidos na PCSI (Portaria-TCU nº 210/2014). A PCSI define diretrizes gerais de segurança da informação, enquanto outros normativos complementares tratam temas específicos como a classificação da informação ou uso de recursos de TI, por exemplo.

Para consultar a versão mais atual da estrutura normativa, acesse o Portal TCU – comunidade de segurança da informação.



CLASSIFICAÇÃO DAS INFORMAÇÕES QUANTO À CONFIDENCIALIDADE

Informações são classificadas (isto é, agrupadas em "classes") para otimizar os controles que garantem seu acesso apenas por pessoas autorizadas.

Essas classes alinham-se ao disposto na Lei nº 12.527/2011 (Lei de Acesso à Informação) e nas leis que definem outros sigilos, como fiscal, bancário, comercial e aquele relativo a denúncias.

É por isso que: a Resolução TCU nº 254/2013 integra a PCSI/TCU e especifica a classificação quanto à confidencialidade, definindo:

Público	*Acesso livre a qualquer pessoa*	*Livre*
Reservado	*Afeta a segurança da sociedade ou do Estado, nos termos do art. 7º da Resolução-TCU nº 254*	*5 anos*
Secreto		*15 anos*
Ultrasecreto		*25 anos*
Pessoal	*Diz respeito à intimidade, vida privada, honra e imagem da pessoa*	*100 anos*
Sigiloso	*Hipóteses de sigilo previstas em legislação específica, tal como informação relativa a denúncias, de natureza fiscal ou protegida por segredo de justiça.*	*conforme legislação*

É IMPORTANTE SABER

Enquanto as informações produzidas no TCU são classificadas pelo gestor da informação, as recebidas de fontes externas devem ser classificadas na origem.

CONTROLE DE ACESSO À INFORMAÇÃO

Tem por objetivo garantir que o acesso à informação seja franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação. Deve haver equilíbrio para que não haja restrição demais ou de menos

É por isso que :

- O acesso às informações que não sejam públicas deve ser restrito às pessoas que tenham necessidade de conhecê-las e se submete a controles compatíveis com a classificação quanto à confidencialidade.

- Havendo necessidade de acesso a informações não públicas por pessoas com vínculo transitório com o TCU, é obrigatório o aceite de termo de sigilo e responsabilidade.

É IMPORTANTE SABER

Toda vez que estiver de posse de informações relativas ao seu trabalho, você é responsável por respeitar os controles de acesso definidos pelo gestor da informação e garantir a segurança dessas informações.

SEGURANÇA EM RECURSOS HUMANOS E AÇÕES DE CONSCIENTIZAÇÃO

As pessoas são parte fundamental da segurança da informação.

Qualquer pessoa que tenha vínculo estatutário, funcional, contratual ou processual com o TCU deve entender suas responsabilidades e atuar em consonância com os preceitos da PCSI/TCU.

É por isso que :

É importante influenciar os comportamentos das pessoas e a cultura organizacional por meio da internalização de conceitos e práticas de Segurança da Informação nas atividades diárias.

Para isso, a Disic promove diversas ações de conscientização, tais como:

- Dicas Semanais no União
- Cartilhas e Tutoriais (disponíveis no Portal)
- Coluna "Aprendendo com a notícia" no União
- Quiz em Segurança da Informação
- Treinamentos Institucionais (presenciais e à distância)
- Dia da Segurança da informação

Essas ações são dirigidas a todos no TCU. Quando possível, busca-se alcançar também gestores e servidores públicos em geral.

É IMPORTANTE SABER

Ações de conscientização criam condições para que tratemos a segurança da informação como um hábito saudável, incorporado em nossas atividades diárias.
Promover a conscientização não é só responsabilidade da Disic, mas de todos os dirigentes e gestores do TCU.

SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES

Tem por objetivo proteger as informações armazenadas ou transferidas em meio eletrônico.

É por isso que:
Abrange o desenvolvimento de sistemas seguros, configurações adequadas de estações de trabalho e o uso seguro de recursos como computação em nuvem, redes sociais, dispositivos móveis, correio eletrônico e outros serviços, soluções e recursos de TI.

É IMPORTANTE SABER

Segurança da Informação não se resume à proteção das informações eletrônicas. O objetivo maior da Segurança da Informação é a proteção adequada de todas as informações, independentemente do meio em que elas se encontrem.

Tem como principais responsáveis:

Setic e STI	implementação centralizada de soluções de TI corporativas
Sesti	serviço da Setic que atua na definição de normas e procedimentos de Segurança da Informação aplicáveis internamente pela Setic e STI, assim como na monitoração e na gestão de incidentes que afetem soluções e recursos de TI.
Unidades gestoras de soluções de TI	definição de requisitos de segurança da informação das soluções
Qualquer unidade que realize a implementação descentralizada de soluções de TI departamentais (APEX).	

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Tem por objetivo realizar o diagnóstico preventivo para decidir quais riscos são aceitáveis e quais necessitam de controles especiais, priorizando seu tratamento e evitando a ocorrência de incidentes.

É por isso que :
A Disic, em conjunto com as unidades técnicas, realiza a análise de riscos de segurança da informação em processos de trabalho do TCU. O apetite a risco, a probabilidade e o impacto da materialização do risco direcionam a definição dos controles a serem adotados.

É IMPORTANTE SABER

A Disic pode ajudar sua unidade coordenando a realização de análise de riscos de segurança da informação nos seus processos de trabalho, a fim de priorizar o tratamento de riscos importantes.

GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Registrar e tratar os incidentes em segurança da informação(SI) é fundamental para a tomada de ações corretivas em tempo hábil. Além disso, busca-se a prevenção da ocorrência desses eventos indesejados.

É por isso que :

A Disic coordena a gestão de incidentes de SI do Tribunal e atua diretamente no tratamento de incidentes que não se refiram à TI. Para atuar na gestão de incidentes de SI relacionados aos serviços e soluções de TI, conta com o apoio do Serviço de Segurança em TI (Sesti), subunidade da Secretaria de Infraestrutura de TI (Setic).

São exemplos de incidentes em SI: furto de equipamentos que contenham informações corporativas, vazamento de informações não públicas, e-mails enviados sem autorização do remetente, etc.

É IMPORTANTE SABER

Autoridades, servidores e quaisquer colaboradores devem informar à **Disic** os incidentes de SI de que tenham ciência ou suspeita.
A identificação e o tratamento dos incidentes de SI acontece com a colaboração de todos em suas respectivas áreas de competência.

Para mais informações, entre em contato com a Secretaria de Planejamento, Governança e Gestão (Seplan/Disic) ou envie email para segurancadainformacao@tcu.gov.br

TRIBUNAL DE CONTAS DA UNIÃO