TRIBUNAL DE CONTAS DA UNIÃO

BTCU Especial

Boletim do Tribunal de Contas da União

Diário Eletrônico

Ano 42 | nº 15 | Quinta-feira, 20/04/2023

PORTARIA-TCU Nº 89, DE 20 DE ABRIL DE 2023.

Aprova a regulamentação da Política Corporativa de Segurança da Informação do Tribunal de Contas da União (PCSI/TCU) e do Sistema de Gestão de Segurança da Informação do Tribunal de Contas da União (SGSI/TCU).

TRIBUNAL DE CONTAS DA UNIÃO
Boletim do Tribunal de Contas da União
Regulamentado pelo art. 98 da Lei nº 8.443, de 16 de julho de 1992,
e pelos §§ 3º a 5º do art. 295 do Regimento Interno do TCU

http://www.tcu.gov.br btcu@tcu.gov.br

SAFS Lote 1 Anexo I sala 424 - CEP:70042-900 - Brasília - DF
Fones: 3527-7279/3527-7869/3527-2484/3527-5249

Boletim do Tribunal de Contas da União especial - Ano. 37, n. 24 (2018)- . Brasília: TCU, 2018- .

Irregular.
Continuação de: Boletim do Tribunal de Contas da União Administrativo Especial.

1. Ato administrativo - periódico - Brasil. I. Brasil. Tribunal de Contas da União (TCU).

Ficha catalográfica elaborada pela Biblioteca Ministro Ruben Rosa

PORTARIA-TCU Nº 89, DE 20 DE ABRIL DE 2023.

Aprova a regulamentação da Política Corporativa de Segurança da Informação do Tribunal de Contas da União (PCSI/TCU) e do Sistema de Gestão de Segurança da Informação do Tribunal de Contas da União (SGSI/TCU).

O PRESIDENTE DO TRIBUNAL DE CONTAS DA UNIÃO, no uso de suas atribuições legais e regimentais,

considerando o disposto na Resolução-TCU nº 342, de 28 de setembro de 2022, que dispõe sobre a Política Corporativa de Segurança da Informação do Tribunal de Contas da União (PCSI/TCU);

considerando o disposto no art. 21 da Resolução-TCU nº 261, de 11 de junho de 2014, que dispõe sobre a Política de Segurança Institucional (PSI/TCU);

considerando as diretrizes, os objetivos, os princípios e as definições constantes da Resolução-TCU nº 294, de 18 de abril de 2018, relativamente à classificação das informações produzidas ou custodiadas pelo TCU;

considerando as melhores práticas relativas à segurança da informação, em especial as previstas na família de normas ABNT NBR ISO/IEC 27000, **Control Objectives for Information and related Technology** (COBIT), **Center for Internet Security** (CIS v8), normas complementares previstas na IN01/DSIC/GSIPR - Gabinete de Segurança Institucional da Presidência da República (GSIPR) e **National Institute of Standards and Technology** (NIST); e

considerando as informações constantes do processo TC-012.126/2022-5, resolve:

Art. 1º Fica aprovada a regulamentação da Política Corporativa de Segurança da Informação do Tribunal de Contas da União (PCSI/TCU) e do Sistema de Gestão de Segurança da Informação do Tribunal de Contas da União (SGSI/TCU), na forma estabelecida nos Anexos I a XI desta Portaria, com os seguintes temas:

I - glossário;

II - controle de acesso;

III - infraestrutura de serviços digitais do TCU;

IV - computação em nuvem;

V - dispositivos particulares;

VI - acesso à internet;

VII - acesso remoto;

VIII - correio eletrônico;

IX - gestão de vulnerabilidades;

X - tratamento de incidentes; e

XI - backup.

Art. 2º A revisão da regulamentação da PCSI/TCU poderá ocorrer a qualquer tempo, quando houver mudanças significativas com impacto nos processos ou requisitos de segurança da informação, devendo ser realizada no máximo a cada quatro anos, de modo a atualizá-la frente a novos requisitos corporativos.

Parágrafo único. Compete ao Presidente do TCU, mediante ato normativo, criar, alterar ou excluir os anexos desta Portaria, de forma conjunta ou individualizada, a partir de subsídios encaminhados pela unidade responsável pela segurança da informação, aprovados pelo comitê de segurança da informação e posteriormente pela Comissão de Coordenação Geral (CCG).

Art. 3º Ficam revogadas a Portaria-TCU nº 169, de 31 de julho de 2006, a Portaria - TCU nº 344, de 9 de novembro de 2009, a Portaria-TCU nº 144, de 25 de maio de 2010, a Portaria Conjunta Setic-STI nº 1, de 1 de outubro de 2015, a Portaria-CGTI nº 2, de 16 de dezembro de 2011, e a Portaria-CGTI nº 1, de 2 de dezembro de 2020.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

MINISTRO BRUNO DANTAS

ANEXO I DA PORTARIA-TCU Nº 89, DE 20 DE ABRIL DE 2023

TRIBUNAL DE CONTAS DA UNIÃO

GLOSSÁRIO DE TERMOS DA PCSI/TCU

SUMÁRIO

LISTA DE SIGLAS

2FA - *Two Factor Authentication* (Autenticação em Duplo Fator)

API - *Application Programming Interface* (Interface de Programação de Aplicações)

CB - *Cloud Broker* (Corretor de Serviços em Nuvem)

CSP - *Cloud Service Provider* (Provedor de Serviços em Nuvem ou Provedor)

DAST - *Dynamic Application Security Testing* (Teste Dinâmico de Segurança de Aplicações)

ETIR - Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais

GPO - *Group Policy Objects* (Objetos de Diretiva de Grupo)

GV- Gestão de Vulnerabilidades

IAST - *Interactive Application Security Testing* (Teste Interativo de Segurança de Aplicações)

IoT - *Internet of Things* (Internet das Coisas)

ISD - Infraestrutura de Serviços Digitais do Tribunal de Contas da União

ISD/TCU - Infraestrutura de Serviços Digitais do Tribunal de Contas da União

MFA - *Multi Factor Authentication* (Autenticação em Múltiplos Fatores)

NMS - Nível Mínimo de Serviço

PCSI - Política Corporativa de Segurança da Informação

SAST - *Static Application Security Testing* (Teste Estático de Segurança de Aplicações)

SGSI - Sistema de Gestão de Segurança da Informação

SI - Segurança da informação

TCU - Tribunal de Contas da União

TI - Tecnologia da informação

VDI - *Virtual Desktop Infrastructure* (Infraestrutura de Desktop Virtual) VPN - *Virtual Private Network* (Rede Privada Virtual)

APRESENTAÇÃO

Este glossário fornece definições de termos aplicáveis à Política Corporativa de Segurança da Informação do Tribunal de Contas da União (PCSI/TCU), bem como aos demais normativos que a integram.

Os termos conceituados empregam semânticas específicas em função da natureza dos normativos abrangidos. O anexo serve para facilitar a consulta e o entendimento das definições. Pretende-se também uniformizar a taxonomia empregada em normativos de Segurança da Informação (SI).

A grafia das palavras ou termos em **negrito** no conteúdo das definições, indica que tais termos também estão definidos no glossário.

OBJETIVO

Fornecer definições de termos relacionados à PCSI/TCU, bem como aos demais normativos que a integram, para promover uma compreensão comum e consistente de conceitos.

GLOSSÁRIO

A

Acesso à internet - qualquer acesso à informação ou ao serviço disponível na rede mundial de computadores (**internet**), incluindo conteúdo enviado ou recebido via correio eletrônico.

Acesso remoto - Acesso feito por meio da internet. Ver **Acesso remoto por meio de desktop virtual, Acesso remoto por meio de tunelamento.**

Acesso remoto por meio de desktop virtual - acesso remoto empregando solução de virtualização de estação de trabalho (VDI).

Acesso remoto por meio de tunelamento - acesso remoto empregando rede privada virtual (VPN).

Administrador de ativo de TI - ver **Responsável por ativo de TI**.

Administrador de recurso de TI - ver **Responsável por recurso de TI**.

Arquitetura de serviços de computação em nuvem - ver **Modelo de computação em nuvem baseado na arquitetura de serviços**.

Ativo de TI - sistema de informação ou **recurso de TI** (**elemento de infraestrutura de TI**). Sistemas e infraestrutura (ABNT NBR ISO/IEC 38500, 2018).

Ativo crítico - **Ativo** que em caso de falha, do mesmo e/ou de um de seus componentes, resulte em um dos cenários: atraso e/ou não realização das sessões do plenário ou impacto na imagem do TCU com a indisponibilidade de algum serviço para a sociedade ou impacto financeiro na não execução das atividades de controle externo.

Ativo não crítico - **Ativo** não classificado como crítico e que em caso de falha, do mesmo e/ou de um dos seus componentes, resulte em atraso das atividades de uma equipe e/ou departamento interno ao TCU.

Autenticação - procedimento ou controle tecnológico que visa verificar a associação entre uma pessoa ou usuário de serviço e sua identidade para franquear-lhe o acesso adequado (_____, 2014a), adaptado.

Autenticação em duplo fator (2FA) - procedimento de **autenticação** particular ao **MFA**, empregando dois desafios de naturezas distintas a serem oferecidos pelo usuário.

Autenticação em múltiplos fatores (MFA) - procedimento de **autenticação** empregando múltiplos desafios a serem oferecidos pelo usuário, de natureza distinta ao que se conhece, como senha, do que se possui, como certificado digital, ou do que se é, como biometria.

Autenticidade - propriedade que assegura a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria (_____, 2014a).

Autorização - procedimento ou controle tecnológico que visa associar usuário previamente **autenticado** a **privilégios** de acesso**.**

C

Caixa postal - repositório de armazenamento de mensagens de correio eletrônico integrante da base de dados dos equipamentos **servidores** de correio eletrônico do TCU.

Central de serviços de TI - equipe responsável pelo atendimento centralizado dos usuários de **serviços de TI** do Tribunal (_____, 2017), adaptado.

Certificado digital - arquivo eletrônico que contém dados de uma pessoa física, jurídica, máquina ou aplicação e um par de chaves criptográficas utilizados para comprovar identidade em ambiente computacional (_____, 2010), adaptado.

Ciclo de vida da informação - compreende etapas e eventos de produção, recebimento, armazenamento, acesso, uso, alteração, cópia, transporte e descarte da informação (_____, 2014a).

***Cloud broker* (CB)** - organização responsável por servir de ponto de contato ou interface para um ou mais **provedores** contratados, para gerenciamento de uso, desempenho e entregas de serviços em **computação em nuvem**.

Cloud Service Provider (CSP) - ver **Provedor de nuvem**.

Cofre de mídia - local apropriado para armazenamento de mídias magnéticas com proteção contra temperatura e fogo, com monitoramento por câmeras e controle de acesso físico.

Cofre de mídia local - cofre instalado no mesmo complexo predial onde a informação protegida está armazenada.

Cofre de mídia *off-site* - cofre instalado em localidade geograficamente diferente daquela onde está armazenada a informação protegida.

Colaborador - prestador de serviço terceirizado, estagiário ou qualquer pessoa com vínculo transitório com o Tribunal que tenha acesso, de forma autorizada, aos recursos de TI ou serviços digitais do TCU (_____, 2014b), adaptado.

Componente de integração - parte de um sistema de informação empregada na integração ou no desenvolvimento de componentes de sistema, a exemplo de interface de programação de aplicações (API).

Componente de sistema - parte de um sistema de informação, que pode ser combinada com outros componentes para a constituição de um sistema de informação, a exemplo de microsserviços.

Computação em nuvem - modelo que permite acesso ubíquo ou transparente, conveniente e sob demanda por meio da rede de computadores, a conjunto compartilhado de recursos computacionais configuráveis, que podem ser rapidamente provisionados e disponibilizados com o mínimo de esforço de gerenciamento ou de interação com o **provedor de nuvem** (NC14, 2012), adaptado.

Conexão - ligação de **recurso de TI** à determinada rede por meio físico ou virtual, de equipamentos de radiofrequência ou de comunicação via infravermelho ou micro-ondas (rede sem fio).

Conexão à rede TCU - ligação de **recurso de TI** à **rede TCU** por meio físico ou virtual, de equipamentos de radiofrequência ou de comunicação via infravermelho ou micro-ondas (rede sem fio).

Confidencialidade - propriedade que garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal (_____, 2014a).

Conta administrativa - conta de administrador de **recurso de TI**, contendo identificação única de usuário e senha (_____, 2011a).

Conta de administrador local - tipo de conta administrativa padrão do sistema operacional, comumente chamada de "administrator", "administrador", "admin" ou "root" (_____, 2011a).

Conta de serviço - tipo de conta administrativa específica para a execução de serviços corporativos que requerem privilégios administrativos (_____, 2011a).

Conta de uso coletivo - conta para acesso à **rede TCU** utilizada por mais de um usuário, com finalidade específica.

Conta de usuário de serviço - identificação única de **sistema** ou de **serviço de TI**, com senha associada, para acesso a recursos de TI.

Conta individual - **identificação** única de usuário, com senha associada, para acesso à **rede TCU**.

Controle de segurança da informação - forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal (ABNT NBR ISO/IEC 27002, 2013).

Cópia de segurança (*backup*) - cópia de dados de um meio de armazenamento para outro com vistas a possibilitar a restauração dos dados originais em caso de perda, dano, inutilização do meio de armazenamento original ou ainda por exclusão ou alteração inadvertida de informação.

Cópia *full* - cópia de segurança contendo todos os dados do ativo protegido.

Cópia incremental - cópia de segurança contendo apenas os dados do ativo protegido que foram modificados desde o último ***backup*** realizado.

Cópia redundante em fita - segunda cópia em fita de um mesmo conjunto de ***backup***, gravação da mesma informação em duas fitas diferentes, para armazenamento em locais distintos.

Cópia secundária em disco - segunda cópia em disco de uma **cópia de segurança** armazenada em disco.

Cópia secundária em fita - cópia em fita de uma cópia de segurança armazenada em disco.

Cópia-imagem - cópia da configuração padrão para cada modelo de **dispositivo** de propriedade da organização e perfil distinto de usuário, contendo todos os programas instalados e configurados, conforme definido pela unidade responsável pela infraestrutura de TI.

Custodiante da informação - qualquer pessoa física ou jurídica, interna ou externa, unidade ou projeto do Tribunal que detém a posse, mesmo que transitória, de informação produzida ou recebida pelo Tribunal (_____, 2014a).

Credencial - combinação de informações necessárias para identificação e autenticação de usuários, comumente formado por usuário e um ou mais **fatores de autenticação** (NC07, 2010), adaptado.

Criticidade - grau de importância de um determinado ativo institucional para a continuidade do negócio da instituição (_____, 2014b).

Criticidade de ativo de TI - grau de importância de um **ativo de TI** para a continuidade do negócio da instituição. Ver também **Criticidade**.

D

Dado pessoal - informação relacionada a pessoa natural identificada ou identificável (LGPD, 2018).

***Datacenter* de contingência** - instalação secundária para prover infraestrutura alternativa de processamento e armazenamento de dados.

***Datacenter* principal** - instalação onde está concentrada a infraestrutura de processamento e armazenamento de dados da organização.

Desastre - evento inesperado que afeta **ativos de TI** e requer esforço significativo para restaurar nível original de desempenho, inclusive com adoção de medidas emergenciais para preservar a **integridade**, a **confidencialidade** e a **disponibilidade** das informações por ele tratadas.

Disponibilidade - propriedade que garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido (_____, 2014a).

Dispositivo - qualquer equipamento de uso pessoal que tenha como característica capacidade computacional e conectividade a rede, tais como *desktop*, *notebook*, *smartphone*, *tablet*e organizador pessoal eletrônico.

Dispositivo de IoT - Objetos capazes de receber e transmitir dados por meio de rede, a exemplo de câmeras, sensores de temperatura, detectores de fumaça.

Dispositivo do TCU - dispositivo de propriedade do TCU.

Dispositivo particular - dispositivo que não seja de propriedade do TCU (_____, 2014a).

E

Elemento de infraestrutura de TI - ver **Recurso de TI**.

Equipamento central de armazenamento - equipamento instalado no centro de processamento de dados (***datacenter***) do TCU para prover solução de armazenamento de informação.

Estação de trabalho - ver **Dispositivo**.

Estação de trabalho do TCU - ver **Dispositivo do TCU**.

F

Formulário de comissionamento - formulário próprio, mantido pela unidade responsável pela infraestrutura de TI, utilizado para comissionar os procedimentos de ***backup*** na plataforma de proteção de dados, em que são definidas as políticas de proteção para o **ativo de TI**.

G

Gestão de vulnerabilidades - conjunto de atividades coordenadas que tem por objetivo a redução, a níveis aceitáveis, das **vulnerabilidades** de segurança encontradas durante o processo de "Análise de Segurança" ou "Análise de Vulnerabilidades" em um determinado **ativo ou** conjunto de **ativos** de TI.

I

Identificação - procedimento ou controle tecnológico de verificação da identidade de usuário (_____, 2014a), adaptado.

Incidente - interrupção não planejada ou redução na qualidade de um serviço (ITIL4, 2019).

Incidente crítico de segurança da informação (ICS) - tipo específico de **incidente de segurança da informação** caracterizado pela previsão de longo período para tratamento, pelo risco de impacto a **ativos de TI** considerados críticos pelo Tribunal ou pelo risco de grave dano material, de imagem ao TCU ou de atrair atenção da mídia ou da população em geral. Ver também **incidente**, **incidente de segurança da informação**.

Incidente de segurança da informação - evento adverso, confirmado ou sob suspeita, que pode comprometer, real ou potencialmente, a **disponibilidade**, a **integridade**, a **confidencialidade** ou a **autenticidade** de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Ver também **incidente**, **incidente crítico de segurança da informação**.

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 (_____, 2014a).

Infraestrutura de Serviços Digitais (ISD/TCU ou ISD) - infraestrutura de TI de suporte ao provimento de **serviços digitais** do TCU.

Infraestrutura local - infraestrutura provida e de uso exclusivo do próprio órgão.

Infraestrutura *on premises* - ver **Infraestrutura local**.

Integridade - propriedade que garante a não violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão indevida, acidental ou proposital (_____, 2014a).

Internet - sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes (LEI N° 12.965, 2014).

Internet das coisas (IoT) - sistema interrelacionado de dispositivos computacionais, equipamentos digitais e mecânicos, com habilidade de transferir dados pela rede sem a necessidade de interação do tipo pessoa-pessoa ou pessoa-computador (PORT93/2019), adaptado.

J

Janela de *backup* - espaço de tempo disponível à realização do procedimento de ***backup***.

L

Lista de distribuição - agrupamento de diversas **caixas postais** em um único endereço eletrônico que, uma vez inserido como destinatário de uma mensagem, permite a distribuição desta a todas as **caixas postais** integrantes da lista.

M

Malware - *software* malicioso, projetado para infiltrar um sistema computacional, com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de *software* costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou *sites* (PORT93/2019).

Modelo multi-inquilino (ou multi-locatário) - arquitetura capaz de permitir o compartilhamento de infraestruturas físicas entre diversos usuários ou locatários, proporcionando flexibilidade e eficiência, mas preservando o isolamento de instâncias lógicas dos recursos alocados entre cada usuário.

Modelo *multi-tenant* - ver **Modelo multi-inquilino**.

Modelos de computação em nuvem baseados na arquitetura de serviços - modelo baseado em serviço de computação em nuvem: infraestrutura, plataforma ou *software* como serviço (NC14, 2012), adaptado.

Modelos de computação em nuvem baseados na forma de implantação - modelo baseado em infraestrutura pública, privada, denominadas respectivamente de **nuvem pública** ou **privada**, ou a mescla de ambos (híbrido) (NC14, 2012), adaptado.

N

Necessidade de conhecer - necessidade de acesso à informação em função do interesse do serviço, de ser relativa à própria pessoa ou por expressa previsão legal (_____, 2014a).

Nível mínimo de serviço (NMS) - acordo firmado com o **provedor de serviço**, no qual são estabelecidas metas de qualidade e de desempenho para **serviços de TI**, considerando-se necessidades e impacto para o negócio, bem como custo e capacidade para provimento de serviços.

Nuvem híbrida - infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (**privadas**, **públicas**), que permanecem com suas próprias características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações (IN05, 2021).

Nuvem privada - infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e sua propriedade e seu gerenciamento podem ser da própria organização, de terceiros ou de ambos (IN05, 2021).

Nuvem pública - infraestrutura de nuvem dedicada para uso aberto de qualquer organização, e sua propriedade e seu gerenciamento podem ser de organizações públicas, privadas ou de ambas (IN05, 2021).

Nuvem TCU - serviço de **computação em nuvem**, mediante **arquitetura de serviços**, como infraestrutura, plataforma ou *software*, fornecido por **provedor** de serviços em nuvem, ou localmente, por meios próprios. Ver também **Rede TCU**, **Modelos de computação em nuvem baseados na arquitetura de serviços**, **Modelos de computação em nuvem baseados na forma de implantação**.

P

Plataforma de Colaboração e Mensageria - solução que permite a interação entre pessoas e equipes para o compartilhamento de arquivos e/ou informações, a exemplo do *Microsoft Teams*â.

Porta lógica - conexão virtual empregada para transmissão de dados.

Princípio do menor privilégio - delega somente os privilégios necessários para que uma determinada entidade (serviço, sistema ou pessoa) possa realizar sua função na organização.

Privilégio - permissão concedida à determinada entidade em um ativo de TI.

Procedimento de *backup* - conjunto de ações para obtenção de cópia de segurança, materializados no plano de *backup*.

Procedimento de *restore* - conjunto de ações para restauração de dados a partir da cópia de segurança.

Provedor de nuvem (***cloud service provider***) - organização responsável por disponibilizar serviços de computação em nuvem para clientes, por gerenciar a infraestrutura necessária para provimento de serviços, conforme **níveis mínimos de serviço** e **controles de segurança da informação** acordados.

R

Recurso de TI - dispositivo, equipamento servidor (*storage*, processamento, roteador e *switch)* e *middleware* (*software* virtualizador, SGBD) utilizados para prover serviços digitais.

Rede de computadores do TCU - conjunto de **recursos de TI** que, ligados em rede de comunicação de dados fornecida pelo Tribunal, que possibilitam compartilhamento de informações (PORT93/2019), adaptado. Ver também **Nuvem TCU**.

Rede TCU - ver **Rede de computadores do TCU** e **Nuvem TCU**.

Rede mundial de computadores - ver **internet**.

Responsável pelo ativo de TI - unidade ou grupo de servidores do Tribunal responsável pela administração, ainda que temporária, de **ativo de TI**. Sinônimo de **Administrador de ativo de TI**.

Responsável por recurso de TI - usuário ou grupo de usuários responsável por definir critérios de utilização e autorizar, conceder ou modificar **privilégios** de uso sobre o **recurso de TI** (_____, 2011a). Sinônimo de **Administrador de recurso de TI**.

Risco de segurança da informação - potencial associado à exploração de uma ou mais **vulnerabilidades** de um ativo ou de um conjunto de ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização (PORT93/2019), adaptado.

S

Segurança da informação - 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 (_____, 2014a).

Serviço de diretórios - serviço de gerenciamento centralizado de usuários, grupos, domínios, **ativos de TI**, organizado de forma hierárquica, para controle de privilégios de acesso de usuários e de grupos, por meio de políticas de grupo (*group policy objects*).

Serviço de TI - serviço que se baseia no uso da tecnologia da informação (ITIL4, 2019).

Serviço digital - ver **Serviço de TI**.

Servidor corporativo - computador pertencente ao parque computacional do TCU, com requisitos de segurança e alto desempenho para prover **soluções de TI** corporativas.

Severidade - característica da **vulnerabilidade**, determinada em função da probabilidade de exploração da **vulnerabilidade** e do impacto de sua exploração no funcionamento do **ativo de TI**.

Sistema de Gestão de Segurança da Informação (SGSI/TCU) - parte integrante do Sistema de Gestão de Segurança Institucional do Tribunal, baseada em **riscos** do negócio, que visa estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a **segurança da informação** (_____, 2014b).

***Software* de captura de tráfego** - programa que permite a captura e a apresentação dos dados que trafegam entre **recursos de TI**.

Solução corporativa - solução destinada ao atendimento de necessidade de negócio ou de funcionamento com impacto em todo o Tribunal (_____, 2018).

Solução de TI - conjunto formado por elementos de tecnologia da informação e processos de trabalho que se integram para produzir resultados que atendam necessidades ou oportunidades de negócio, de forma **corporativa** ou **departamental**.

Solução de TI corporativa - ver **Solução corporativa**.

Solução de TI departamental - ver **Solução departamental**.

Solução de virtualização - ver Solução de virtualização de estação de trabalho.

Solução de virtualização de estação de trabalho - solução de virtualização de sistema operacional e aplicações, provida pelo Tribunal. Sinônimo de **Desktop virtual**.

Solução departamental - solução destinada ao atendimento de necessidade específica de determinada unidade ou de conjunto limitado de unidades do Tribunal (_____, 2018).

T

Teste de segurança de aplicações - verificações com o objetivo de identificar **vulnerabilidades** no código-fonte de aplicações. Ver também **teste estático, dinâmico e interativo de segurança de aplicações**.

Teste dinâmico de segurança de aplicações - verificação com o objetivo de identificar **vulnerabilidades** na execução de código-fonte de aplicações (*dynamic application security testing* - DAST).

Teste estático de segurança de aplicações - verificação com o objetivo de identificar **vulnerabilidades** no código-fonte de aplicações (*static application security testing* - SAST).

Teste interativo de segurança de aplicações - verificação com o objetivo de identificar **vulnerabilidades** em tempo real durante a execução de código-fonte no ambiente de produção (*interactive application security testing* - IAST).

Tratamento de incidentes de segurança em TI - atividade que envolve triagem, análise, notificação e resposta aos **incidentes de segurança em TI**.

U

Unidade gestora de TI - responsável pela definição de processos de trabalho, requisitos, regras de negócio e níveis de serviço aplicáveis à **solução de TI**.

Unidades provedoras de TI - unidade responsável pela infraestrutura de TI e unidade responsável por soluções em TI.

Usuário colaborador - prestador de serviço **terceirizado**, **estagiário** ou qualquer outro **colaborador** do Tribunal que tenha acesso, de forma **autorizada**, a informações produzidas ou custodiadas pelo Tribunal.

Usuário externo - pessoa que utiliza serviços digitais do TCU de forma **identificada**, não sendo classificado como **usuário interno**, **inativo** ou **colaborador**, bem como associado a conta de serviço.

Usuário inativo - autoridade emérita, servidor inativo ou pensionista do Tribunal que tenha acesso, de forma **autorizada**, a informações produzidas ou custodiadas pelo TCU.

Usuário interno - autoridade ou servidor ativo que tenha acesso, de forma **autorizada**, a informações produzidas ou custodiadas pelo TCU (_____, 2010), adaptado.

Usuário visitante - pessoa com acesso temporário e restrito à rede sem fio do TCU, não sendo classificado como **usuário interno**, **inativo**, **colaborador** ou **externo**, bem como associado a **conta de serviço**.

V

Vulnerabilidade - fragilidade de um **ativo de TI**, explorável por uma ou várias ameaças (ABNT NBR ISO/IEC 27002, 2013).

Vulnerabilidade crítica - fragilidade de um **ativo de TI**, explorável por uma ou várias ameaças, capazes de comprometer o correspondente ativo (_____, 2019).

FIGURAS

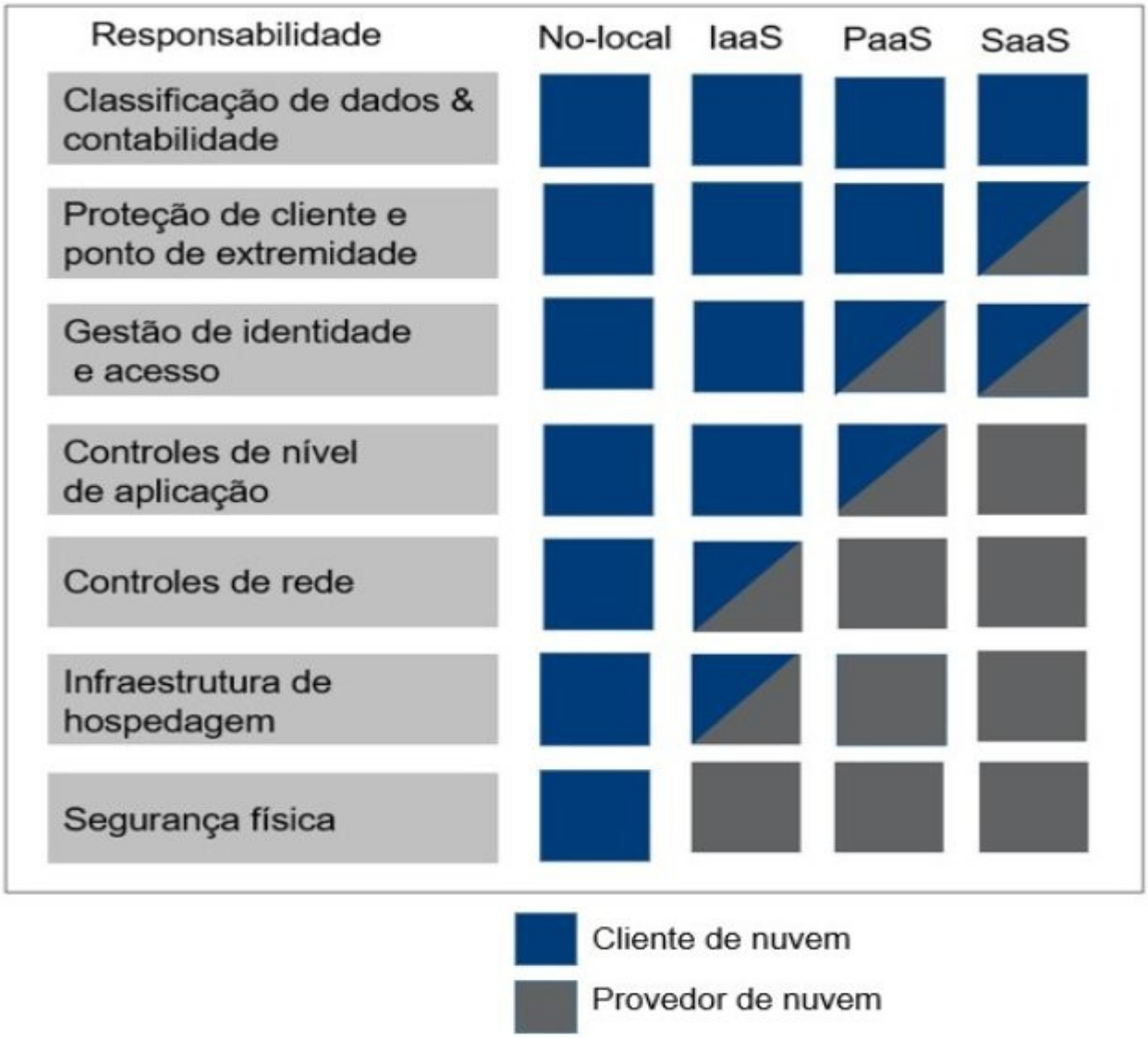

Figura 1 - Modelo de responsabilidade compartilhada em serviços de nuvem. Fonte: ***https://www.softwareone.com/pt-br/blog/artigos/2020/08/06/seguranca-nuvem***

TABELAS

Tabela 1 - Segmentação de recursos da rede TCU, conforme disposto no item 12 do Anexo III desta Portaria.

	I	II	III	IV	V	VI	VII	VIII
A	X	X	X	X	X	X	X	X
B			X		X		X	
C				X		X		X
D			X			X	X	X

Legenda:

A - Sujeitos à segmentação na rede TCU (item 12, Anexo III).

B - Provimento de conexão exclusivamente para acesso à internet (item 13, Anexo III).

C - Provimento de conexão para acesso à internet e a serviços a serem definidos pela unidade responsável pela infraestrutura de TI no TCU (item 14, Anexo III).

D - Provimento de conexão à rede TCU por meio de rede sem fio ou por meio alternativo com segurança superior a ser definido pela unidade responsável pela infraestrutura de TI no TCU (item 15, Anexo III).

I - servidores corporativos do Tribunal (item 12.1, Anexo III).

II - dispositivos de propriedade do TCU (item 12.2, Anexo III).

III - dispositivos do Tribunal destinados a visitantes (público externo) (item 12.3, Anexo III).

IV - recursos de TI destinados a eventos ou treinamentos (item 12.4, Anexo III).

V - recursos de TI de propriedade de outra organização que utilize dependências do Tribunal (item 12.5, Anexo III).

VI - dispositivos particulares de usuários internos (item 12.6, Anexo III).

VII - dispositivos particulares de usuários visitantes (item 12.7, Anexo III) e dispositivos particulares de usuários externos (item 16, Anexo III).

VIII - dispositivos de IoT (item 12.8, Anexo III).

BIBLIOGRAFIA

Portaria-TCU nº188/2010. Dispõe sobre o uso de certificado digital no âmbito do Tribunal de Contas da União. 8 dez. 2010. Disponível em: <www.tcu.gov.br>

Portaria-CGTI nº 2/2011. Dispõe sobre o uso de contas administrativas de recursos de TI do Tribunal de Contas da União. 16 dez. 2011a.

Portaria-TCU nº 329/2014. Dispõe sobre procedimentos de segurança e controles administrativos e tecnológicos afetos à classificação quanto à confidencialidade das informações produzidas ou custodiadas pelo Tribunal de Contas da União. 12 jan. 2014a. Disponível em: <www.tcu.gov.br>

Resolução-TCU nº 261/2014. Dispõe sobre a Política de Segurança Institucional (PSI/TCU) e o Sistema de Gestão de Segurança Institucional do Tribunal de Contas da União (SGSIN/TCU) e altera a Resolução-TCU 253, de 21 de dezembro de 2012, que define a estrutura, as competências e a distribuição das funções de confiança das unidades da Secretaria do Tribunal de Contas da União. 6 nov. 2014b.

Portaria-TCU nº 230/2017. Dispõe sobre o provimento e a gestão de soluções de tecnologia da informação no âmbito do Tribunal de Contas da União. 8 maio. 2017. p. 9. Disponível em: <www.tcu.gov.br>

Resolução-TCU nº 303/2018. Dispõe sobre a Política de Governança e Gestão Digital e de Tecnologia da Informação do Tribunal de Contas da União. 28 nov. 2018. p. 9.

Portaria-TCU nº 28/2021. Institui o Comitê Técnico de Proteção e Segurança da Informação (CPS) no âmbito do TCU. 1 fev 2021.

Acórdão nº 2.585/2012 - TCU - Plenário. Teve por objetivo avaliar a situação da governança de tecnologia da informação na Administração Pública Federal, sobretudo dos processos de gestão da segurança da informação.

Acórdão nº 1739/2015 - TCU - Plenário. Disposições e estudos sobre computação em nuvem.

Acórdão nº 2376/2021 - TCU - Plenário. Recomendações sobre atualização dos normativos relativos à segurança da informação.

Levantamentos de 2014 e 2016 do Índice de Governança de TI do TCU (iGovTI).Referencial básico de governança aplicável a organizações públicas e outros entes jurisdicionados ao TCU (RBGO)/2020. Gerenciamento de vulnerabilidades técnicas de ativos críticos para o negócio.

National Institute of Standards and Technology - NIST - SP 800-145 - *The NIST Definition of Cloud Computing*.

National Institute of Standards and Technology - NIST - SP 800-125 - *Guide to Security for Full Virtualization Technologies*.

National Institute of Standards and Technology - NIST - SP 500-291 - *NIST Cloud Computing Standards Roadmap*.

National Institute of Standards and Technology - NIST - SP 800-46 r2 - *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security*.

National Institute of Standards and Technology - NIST - SP 800-61, *Computer Security Incident Handling Guide*.

National Institute of Standards and Technology - NIST SP 800-40 v2.0 - *Creating a Patch and Vulnerability Management Program*.

Common Vulnerability Scoring System version 3.1: Specification Document, Forum of Incident Response and Security Teams (FIRST), 2019. Disponível em:

<https://www.first.org/cvss/examples>. Acesso em: 8 set. 2021.

ABNT NBR ISO/IEC 27002:2013. Brasil: Associação Brasileira de Normas Técnicas, 2013.

ABNT NBR ISO/IEC 38500:2018. Brasil: Associação Brasileira de Normas Técnicas, 2018.

Instrução Normativa nº 1/2020, do Gabinete de Segurança Institucional da Presidência da República. Disciplina a gestão de segurança da informação e comunicações no âmbito da Administração Pública Federal, direta e indireta. 27 mai 2020.

Instrução Normativa nº 5/2021. Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal. 30 ago. 2021. p. 2. Disponível em: <https://www.gov.br/gsi/ptbr/assuntos/dsi/legislacao>. Acesso em: 1 set. 2021.

ITIL 4 Foundation - Glossário de termos e definições. 4. ed. [s.l: s.n.].

Lei nº 12.965/2014 - Marco Civil da internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. 23 abr. 2014. p. 9. Disponível em: <www.planalto.gov.br>

Lei nº 13.709 - Lei de Proteção Geral de Dados Pessoais. de agosto de. 2018. Disponível em: <www.planalto.gov.br>. Acesso em: 1 set. 2021.

Norma Complementar nº 04/IN01/DSIC/GSIPR/2009. Estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta - APF. 14 set. 2009. Disponível em: <https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao>

Norma Complementar nº 07/IN01/DSIC/GSIPR/2010. Estabelece diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF. 2 maio. 2010. p. 8. Disponível em: <https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao>

Norma Complementar nº 14/IN01/DSIC/GSIPR/2012. Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. 30 jan. 2012. p. 7. Disponível em: <https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao>

Portaria nº 93/2019. Aprova o Glossário de Segurança da Informação. 26 de setembro de 2019. Presidência da República/Gabinete de Segurança Institucional. Disponível em: <https://www.in.gov.br/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>

ANEXO II DA PORTARIA-TCU Nº 89, DE 20 DE ABRIL DE 2023

REGRAS GERAIS DE CONTROLE DE ACESSO À INFRAESTRUTURA DE SERVIÇOS DIGITAIS DO TCU (ISD/TCU)

1. Este anexo estabelece regras gerais de controle de acesso à Infraestrutura de Serviços Digitais do TCU (ISD/TCU) e engloba os seguintes aspectos:

1.1 contas de usuários (identificação);

1.2 autenticação e autorização.

DA IDENTIFICAÇÃO DE USUÁRIOS E DO USO DE SENHAS

2. São usuários da ISD/TCU:

2.1 usuário interno: autoridade ou servidor ativo que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo TCU;

2.2 usuário inativo: autoridade emérita, servidor inativo ou pensionista do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo TCU;

2.3 usuário colaborador: prestador de serviço terceirizado, estagiário ou qualquer outro colaborador do Tribunal que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pelo Tribunal;

2.4 usuário externo: pessoa que utiliza serviços digitais do TCU de forma identificada e que não se enquadre nas definições contidas nos subitens 2.1, 2.2 e 2.3; e

2.5 usuário visitante: pessoa que não se enquadra na definição disposta subitens 2.1, 2.2, 2.3 e 2.4, com acesso temporário, somente à internet.

3. Cada usuário possuirá única conta para acesso à ISD/TCU, exceto nos casos explicitamente definidos e autorizados pela unidade responsável pela infraestrutura de TI.

4. O uso de contas administrativas no Tribunal será regulamentado por normativo próprio.

5. Contas pessoais são intransferíveis e de responsabilidade exclusiva do respectivo titular e seus privilégios não podem ser estendidos a terceiros.

6. Contas de usuários serão empregadas para registro de operações realizadas pelos respectivos titulares e, no mesmo sentido, as operações passíveis de monitoramento serão registradas unicamente por meio de sua conta de usuário.

7. A criação, a atualização e a revogação de conta de usuário interno e inativo para acesso à ISD/TCU serão realizadas pelas unidades provedoras de TI, de forma conjunta, com base em registros contidos em sistema informatizado de gestão de pessoas.

8. A unidade responsável pela infraestrutura de TI definirá e divulgará os procedimentos a serem executados com vistas à criação, à atualização e à revogação de contas de usuários.

9. Conta de uso coletivo é permitida, em caráter excepcional e temporária, restrita à finalidade que ensejou a criação, para usuários em treinamento ou evento, bem como em casos em que não seja considerado viável o uso de conta individual.

10. Criação de conta de uso coletivo para finalidade prevista no item 9 será solicitada, por meio da central de serviços de TI, à unidade responsável pela infraestrutura de TI que analisará as justificativas apresentadas e autorizará o atendimento do pedido ou apresentará solução alternativa.

11. A revogação da conta de uso coletivo referida no item 10 será feita imediatamente após a expiração do prazo definido ou antes, caso o demandante comunicar não ser mais necessária.

12. As contas de usuários para acesso à ISD/TCU têm os seguintes prazos de validade:

12.1 contas de usuários internos e inativos: enquanto durar o vínculo com o TCU;

12.2 contas de usuários colaboradores: logo após o fim de suas atividades para o TCU, com prazo a ser especificado pelas unidades provedoras de TI;

12.3 contas de usuários estagiários: logo após o fim do de suas atividades no TCU, com prazo a ser especificado pelas unidades provedoras de TI;

12.4 contas de usuários visitantes e contas de uso coletivo: pelo período necessário para a execução das atividades que motivaram a criação; e

12.5 contas de usuários externos: prazo definido pela unidade de infraestrutura de TI.

DO USO DE SENHAS

13. A senha associada à conta de usuário é pessoal e intransferível, de responsabilidade exclusiva do respectivo titular, sendo expressamente vedado:

13.1 compartilhamento com usuários não autorizados;

13.2 registro em local inseguro, em papel ou em meio eletrônico; e

13.3 envio de senhas por e-mail ou qualquer outro dispositivo de comunicação em claro.

14. A senha associada à conta de usuário deverá ser de difícil dedução e, preferencialmente, de fácil memorização, sendo vedada a composição de elementos comumente empregados em ataques cibernéticos, como o de força bruta, a exemplo de:

14.1 nome e sobrenome do usuário, de membros da família, de amigos, animais de estimação, suas iniciais ou qualquer outro nome, mesmo que embaralhados;

14.2 informações pessoais, tais como identificador de usuário, matrícula, datas, números de telefone, cartão de crédito, identidade, cadastro de pessoa física, placas, informações sobre veículos ou qualquer outro número de identificação pessoal;

14.3 nomes de pessoas, de lugares em geral ou próprios;

14.4 nome de equipamentos ou da rede que está sendo utilizada;

14.5 palavras que constam em dicionários de qualquer idioma;

14.6 letras ou números repetidos ou sequenciados em teclado padrão QWERTY; e

14.7 locais ou objetos que possam ser associados a partir do ativo.

15. É vedado o reuso de senhas para minimizar o impacto em caso de comprometimento de uma senha.

16. Regra mínima de formação de senhas de contas de usuários serão definidas pela unidade responsável pela infraestrutura de TI.

17. Mecanismo de validação de senhas verificará atendimento com a regra de formação no momento do cadastro.

18. O usuário repetirá a entrada da nova senha para confirmá-la e minimizar riscos de erros de digitação.

19. Mensagem de advertência será mostrada ao usuário caso a senha preenchida não atenda à regra de formação definida, ou, se houver implementação, contenha indícios de que tenha sido vazada a partir de consulta a bases de dados especializadas.

20. A nova senha será diferente das quatro senhas utilizadas anteriormente, a fim de garantir rotação de senhas.

21. A nova senha ou parte dela poderá ser confrontada com bases conhecidas de senhas triviais e/ou vulneráveis.

22. Caso o sistema gere a primeira senha no momento do cadastro, o usuário será obrigado a modificá-la imediatamente após o primeiro login, por meio de procedimento capaz de impedir temporariamente a execução das demais atividades enquanto o usuário não realizar a modificação da senha.

23. Senha associada a conta de usuário será alterada em periodicidade a ser definida pela unidade responsável pela infraestrutura de TI.

24. A alteração da senha associada à conta de usuário poderá ser efetuada pelo próprio usuário ou mediante pedido à chefia imediata ou à central de serviços de TI.

25. O usuário deverá alterar sua senha sempre que existir indício de comprometimento da segurança de sua conta ou da ISD/TCU.

26. A unidade responsável pela infraestrutura de TI disponibilizará mecanismo para recuperação de senhas de usuários.

27. O sigilo da senha associada a conta de uso coletivo será mantido entre os usuários autorizados.

28. A alteração de senha de conta de uso coletivo somente poderá ser solicitada por quem demandou a criação da conta ou pelo responsável pelo treinamento ou evento.

DA AUTENTICAÇÃO E DA AUTORIZAÇÃO

29. A autenticação de contas na ISD/TCU será feita, pelo menos, por meio de mecanismo de usuário e senha, atendendo aos seguintes requisitos mínimos a serem definidos e implantados pela unidade responsável pela infraestrutura de TI:

29.1 a autenticação em dois fatores será obrigatória para acesso a quaisquer serviços e soluções de TI, exceto nos casos definidos pela unidade de infraestrutura do TCU;

29.2 enquanto estiver autenticado, o usuário deverá bloquear o recurso de TI sempre que se afastar dele ou deixá-lo desassistido;

29.3 o mecanismo de autenticação automática (auto login) deverá ser desabilitado nos recursos de TI;

29.4 as informações sobre senhas não devem ser salvas localmente, nem incluídas em processos automáticos de acesso (por exemplo, macros ou autocompletamento); e

29.5 conta de usuário não será empregada em processos de autenticação em serviços do sistema, incluindo rotinas de agendamento de tarefas.

30. Poderão ser requeridos, como meio alternativo de autenticação, mecanismos de segurança adicionais como certificação digital e biometria.

31. O controle de acesso à nuvem TCU poderá ser feito por intermédio de serviços de diretórios localizados na própria nuvem TCU, e atenderá aos seguintes requisitos:

31.1 sincronização unidirecional de contas e privilégios, ou seja, a atualização de contas e privilégios será procedida a partir da rede TCU, inclusive no tocante à troca de senhas; e

31.2 sincronização não envolverá contas administrativas, as quais serão mantidas na rede TCU, exceto as definidas pela unidade responsável pela infraestrutura de TI.

32. A autorização de acesso respeitará o princípio do menor privilégio e a necessidade de conhecer, bem como observará as seguintes diretrizes:

32.1 a definição dos privilégios de acesso a recursos de TI será realizada pelo respectivo administrador do recurso de TI ou unidade gestora da solução de TI, conforme o caso;

32.2 a concessão de acesso será preferencialmente automatizada, sendo realizada e atualizada de acordo com atributos do usuário, a exemplo da unidade de lotação, da função, entre outros;

32.3 nos casos da necessidade de concessão de acesso de forma manual, tal concessão será realizada com autorização do administrador do recurso de TI ou da unidade gestora da solução de TI, conforme o caso, hipótese na qual o responsável deverá garantir a atualização tempestiva do permissionamento sempre que houver alteração de atributos do usuário; e

32.4 no caso de mudança de lotação, os privilégios que foram concedidos em razão das atividades realizadas na unidade devem ser revogados, exceto em caso de necessidade de serviço.

33. As situações abaixo identificadas são passíveis de bloqueio da conta de usuário:

33.1 conta sem uso por período igual ou superior a seis meses, ressalvadas as contas de usuários externos;

33.2 quando o servidor ativo não estiver em efetivo exercício por prazo igual ou superior a quinze dias, em função das licenças e dos afastamentos previstos na Lei n° 8.112, de 1990;

33.3 quando o servidor ativo estiver em afastamento preventivo do exercício do cargo em decorrência do disposto no art. 147 da Lei no 8.112, de 1990; ou

33.4 envio de alerta para a unidade responsável pela infraestrutura de TI e habilitação de mecanismo de verificação por desafio cognitivo em função de erros sucessivos de autenticação, a fim de mitigar riscos de segurança decorrentes de tentativas de comprometimento de conta de usuário.

34. O bloqueio de conta a que se refere o subitem 33.1 poderá ser realizado automaticamente, observados os procedimentos estabelecidos pelas unidades provedoras de TI.

35. O bloqueio de conta em decorrência do subitem 33.1 pode ser revogado pela central de serviços de TI, mediante solicitação do usuário.

36. O bloqueio e a posterior liberação do uso da conta na hipótese prevista no subitem 33.2 são realizados pelas unidades provedoras de TI, a partir de solicitação encaminhada pela Secretaria de Gestão de Pessoas - Segep.

37. O bloqueio e a posterior liberação da conta para a situação indicada no subitem 33.3 são realizados pelas unidades provedoras de TI, a partir de solicitação enviada pela Secretaria-Geral de Administração - Segedam.

38. O bloqueio de conta de usuário poderá ser realizado conforme critérios de risco de segurança da informação definidos pela unidade responsável pela infraestrutura de TI.

39. As contas de usuários externos sem utilização por mais de três anos poderão ser excluídas, nos casos e hipóteses definidas pelas unidades provedoras de TI.

DOS PAPÉIS E RESPONSABILIDADES

40. São responsabilidades dos usuários relacionadas ao emprego de credenciais de acesso à ISD/TCU:

40.1 salvaguardar senhas, certificados digitais e quaisquer outros desafios empregados na autenticação da ISD/TCU sob respectiva responsabilidade;

40.2 proceder troca periódica de senhas sob respectiva responsabilidade;

40.3 revisar periodicamente privilégios recebidos e solicitar a revogação dos considerados não mais necessários;

40.4 reportar incidentes de segurança que tiver conhecimento;

40.5 colaborar para o tratamento de incidentes de segurança;

40.6 observar orientações da unidade responsável pela infraestrutura de TI, no tocante a boas práticas e a configurações específicas de segurança da informação; e

40.7 observar o disposto na PCSI/TCU quanto à salvaguarda de informações produzidas ou custodiadas pelo Tribunal, bem como à proteção da própria ISD/TCU.

41. São responsabilidades das unidades provedoras de TI, como administradoras do serviço de autenticação centralizada da ISD/TCU:

41.1 garantir a disponibilidade de serviços de controle de acesso (CA), de acordo com níveis de serviço definidos;

41.2 implantar e manter atualizados mecanismos e procedimentos de proteção contra ataques externos e internos relacionados a CA, incluindo mecanismos de validação de senhas;

41.3 gerenciar contas configuradas;

41.4 realizar triagem, análise, notificação e resposta a incidentes de segurança da informação relacionados aos serviços CA;

41.5 realizar identificação periódica e notificação de vulnerabilidades, bem como monitorar a aplicação de correções (*patches*) em serviços de CA; e

41.6 executar, manter e restaurar cópias de segurança (*backup*) de informações disponíveis em serviços de CA.

42. São responsabilidades das unidades gestores de soluções de tecnologia da informação:

42.1 definir os perfis e permissões de acesso para as funcionalidades e informações das soluções de tecnologia da informação; e

42.2 definir e revisar periodicamente as regras para conceder, revogar e modificar perfis e permissões de acesso a usuários.

DAS DISPOSIÇÕES FINAIS

43. O presente anexo utilizará o Glossário de Termos da PCSI/TCU, constante no Anexo I, para promover compreensão comum e consistente de conceitos em função da natureza específica do tema.

44. A violação ou a inobservância aos dispositivos deste anexo poderá ser considerada incidente de segurança da informação, e poderá implicar, isolada ou cumulativamente, em sanções previstas na PCSI/TCU, bem como civis e penais, nos termos da legislação pertinente, assegurados aos envolvidos o contraditório e a ampla defesa.

45. As unidades provedoras de TI adotarão as medidas necessárias para operacionalizar o disposto neste anexo, bem como detalhar especificidades do presente normativo.

46. O comitê responsável pela segurança da informação deverá monitorar e avaliar periodicamente as práticas de segurança da informação relativas às regras estabelecidas neste anexo, e propor os ajustes que considerar necessários.

47. Os casos omissos são analisados pela unidade responsável pela segurança da informação, ouvido o responsável pelo recurso de TI em questão, e dirimidos pelo comitê responsável pela segurança da informação.

ANEXO III DA PORTARIA-TCU Nº 89, DE 20 DE ABRIL DE 2023

REGRAS GERAIS DE USO DE SERVIÇOS DIGITAIS PROVIDOS A PARTIR DA REDE TCU.

1. Este anexo estabelece regras gerais para o uso de serviços digitais providos a partir da rede TCU e engloba os seguintes aspectos:

1.1 acesso à rede TCU;

1.2 armazenamento de informações na rede TCU;

1.3 recursos de TI do TCU;

1.4 provimento de serviços digitais; e

1.5 papéis e responsabilidades.

2. A rede TCU é parte integrante da infraestrutura de serviços digitais do TCU.

DO ACESSO À REDE TCU

3. A rede TCU será segmentada de forma a escalonar o acesso e a proteger recursos de TI, bem como informações produzidas ou custodiadas pelo Tribunal neles contidos.

4. A rede TCU poderá ser estendida por meio de serviço de computação em nuvem, nos termos de normativo específico sobre o tema, e herdando, no que couber, as diretrizes do presente documento.

5. O uso de quaisquer recursos de TI, enquanto conectados à rede TCU, deve ser realizado de forma a não comprometer a imagem do TCU, nem colocar em risco a segurança das informações produzidas ou custodiadas pelo Tribunal ou a qualidade e a segurança da rede TCU.

6. O acesso à internet e a redes de outros órgãos, originados a partir da rede TCU, será provido exclusivamente pela unidade responsável pela infraestrutura de TI.

7. Enquanto conectados à rede TCU, quaisquer recursos de TI não poderão estar conectados à internet por outro meio, a exemplo de compartilhamento de conexão provida por operadora de telefonia móvel (*hotspot*, *gateway* ou roteamento), nem poderão servir de meio de conexão para outros recursos de TI (ancoragem).

8. Nas dependências do TCU, é vedada a conexão de mais de um dispositivo a um mesmo ponto de rede, exceto nos casos expressamente autorizados pela unidade responsável pela infraestrutura de TI no TCU.

9. É vedada a conexão de recurso de TI que não seja de propriedade do Tribunal à rede TCU por meio de cabeamento físico, exceto nos casos expressamente autorizados pela unidade responsável pela infraestrutura de TI no TCU.

10. A autorização de que tratam os itens 8 e 9 depende de solicitação prévia, na qual conste o motivo, a duração da conexão excepcional e a identificação prévia de usuários e recursos de TI envolvidos, bem como de verificação da segurança dos equipamentos e de assinatura de termo de sigilo e responsabilidade pelo usuário.

11. Ao acessar rede de computadores de outros órgãos ou entidades por meio de recursos de TI do TCU, o usuário deve obedecer a normas e diretrizes daquelas redes.

12. Serão conectados de forma segmentada à rede TCU, pelo menos, os seguintes recursos:

12.1 servidores corporativos do Tribunal;

12.2 dispositivos de propriedade do TCU;

12.3 dispositivos do Tribunal destinados a visitantes (público externo);

12.4 recursos de TI destinados a eventos ou treinamentos;

12.5 recursos de TI de propriedade de outra organização que utilize dependências do Tribunal;

12.6 dispositivos particulares de usuários internos;

12.7 dispositivos particulares de usuários visitantes; e

12.8 dispositivos de IoT.

13. A conexão será provida exclusivamente para acesso à internet nos casos previstos nos subitens 12.3, 12.5 e 12.7, sendo o mesmo caminho empregado para acesso a serviços digitais do TCU.

14. A conexão à rede TCU será provida para acesso à internet e a serviços a serem definidos pela unidade responsável pela infraestrutura de TI no TCU nos casos previstos nos subitens 12.4, 12.6 e 12.8.

15. Nos casos previstos nos subitens 12.3, 12.6, 12.7 e 12.8, a conexão à rede TCU será provida por meio de rede sem fio ou por meio alternativo com segurança superior a ser definido pela unidade responsável pela infraestrutura de TI no TCU.

16. A conexão à rede TCU de dispositivos particulares de usuários externos será a mesma do disposto no subitem 12.7.

17. A unidade responsável pela infraestrutura de TI no TCU disporá em normativo específico sobre segmentação da rede do TCU, de forma a escalonar domínios de acesso, dispor sobre acesso remoto e a salvaguardar informações armazenadas na rede TCU.

18. Para os casos previstos nos subitens 12.3 e 12.5, caberá à unidade responsável pela infraestrutura de TI no TCU definir os demais critérios e requisitos de segurança necessários.

19. A tabela 1 do Anexo I apresenta disposição visual do conteúdo apresentado no item 12.

20. O acesso remoto será regulamentado no Anexo VII a esta Portaria.

DO ARMAZENAMENTO DE INFORMAÇÕES NA REDE TCU

21. A rede TCU poderá dispor de ambiente seguro para armazenamento de arquivos, conforme critérios definidos pela unidade responsável pela infraestrutura de TI.

22. Unidades, subunidades, grupos de trabalho, comissões, comitês, projetos e usuários internos terão espaço próprio para armazenamento de arquivos na rede TCU.

23. A definição das permissões dos espaços de armazenamento de unidades, subunidades, grupos de trabalho, comissões, comitês e projetos é de responsabilidade do administrador do respectivo recurso de armazenamento.

24. O responsável pelo espaço de armazenamento solicitará à Central de Serviços de TI a concessão, a alteração ou a revogação de permissões quando não houver meio para a autogestão das permissões.

25. A salvaguarda de informações na rede TCU atenderá, no mínimo, aos controles previstos em normativo que dispõe sobre procedimentos de segurança e controles administrativos e tecnológicos afetos à classificação quanto à confidencialidade das informações produzidas ou custodiadas pelo TCU, incluindo aspectos do ciclo de vida da informação:

25.1 produção;

25.2 recebimento;

25.3 armazenamento;

25.4 acesso;

25.5 cópia;

25.6 transporte; e

25.7 descarte.

26. Quando do uso de criptografia, os requisitos e rotulação para salvaguarda e comunicação segura na rede TCU serão definidos pela unidade responsável pela infraestrutura de TI no TCU, sem prejuízo da adoção de novos controles administrativos e tecnológicos.

27. É vedado o armazenamento das seguintes informações nos espaços de armazenamento da rede TCU:

27.1 programa não homologado ou licenciado pelo TCU;

27.2 arquivo ou programa de conteúdo potencialmente prejudicial à segurança da rede TCU, exceto em casos explicitamente autorizados pela unidade responsável pela infraestrutura de TI;

27.3 arquivo ou programa em desacordo com código de ética dos servidores do Tribunal e outras normas pertinentes ou com critérios e requisitos de segurança de que trata a PCSI/TCU; e

27.4 cópia de segurança de espaços de armazenamento de usuário ou backup de estação de trabalho.

28. A unidade responsável pela infraestrutura de TI definirá parâmetros para armazenamento de arquivos em espaços de armazenamento corporativos, incluindo requisitos como tamanho máximo e tipos de arquivo permitidos, com vistas a não comprometer o desempenho e a segurança dos serviços de TI.

29. As informações mantidas em espaços de armazenamento da rede TCU podem ser inspecionadas pela unidade responsável pela infraestrutura de TI, ouvida a unidade responsável pela segurança da informação, quando houver indícios de desconformidade com o disposto no item 27.

30. As informações armazenadas em dispositivo do TCU só podem ser inspecionadas, sem anuência do usuário, no curso de sindicâncias, processos administrativos disciplinares ou em cumprimento de ordem judicial, sendo dispensada, nestes casos, a oitiva da unidade responsável pela segurança corporativa da informação.

31. A informação mantida em espaço de armazenamento da rede TCU em desacordo com o disposto no item 27 será excluída pela unidade responsável pela infraestrutura de TI, e o fato caracterizado como incidente de segurança da informação, com prévia comunicação ao administrador do diretório, à sua chefia imediata e ao titular da unidade em que está lotado.

32. Além do responsável pelos espaços de armazenamento, os respectivos conteúdos somente podem ser acessados pela unidade responsável pela infraestrutura de TI e para os seguintes objetivos:

32.1 verificar a obtenção, retenção, uso e divulgação de informações por meio ou com fins ilícitos, ou em desacordo com as normas regulamentares;

32.2 recuperar conteúdo de interesse do TCU, no caso de afastamentos legais do responsável;

32.3 atender demanda do Corregedor, de processo administrativo disciplinar (PAD) ou de comissão de sindicância formalmente constituída; e

32.4 atender solicitação judicial.

33. Nas hipóteses previstas nos subitens 32.1 e 32.2, o acesso aos respectivos conteúdos serão feitos mediante autorização do Secretário-Geral da Presidência, ouvida a unidade responsável pela segurança da informação, a quem incumbe cientificar oportunamente o comitê de responsável pela segurança da informação.

DOS RECURSOS DE TI DO TCU

34. A identificação lógica de cada recurso de TI de propriedade do TCU é realizada pela unidade responsável pela infraestrutura de TI conforme padrões por ela definidos.

35. Quanto ao uso de recursos de TI do TCU, é vedado:

35.1 modificar a configuração, desabilitar ou desinstalar *software* de segurança;

35.2 conceder privilégio de administração ou acessar conta administrativa local;

35.3 proceder abertura física, desmontagem ou rompimento de lacres de segurança; e

35.4 instalar *software* não homologado pelo Tribunal.

36. A unidade responsável pela infraestrutura de TI poderá autorizar em caráter excepcional os casos previstos no subitem 35.2, quando for estritamente necessário para o desempenho das funções, mediante análise de justificativa, em termos a serem definidos pela referida unidade, e no subitem 35.3, quando for necessária a execução por meio de pessoa ou empresa terceirizada.

37. Caso haja necessidade de uso de programa de *software* não homologado ou licenciado para o TCU, a unidade interessada deve encaminhar solicitação de aquisição ou de instalação à unidade responsável pela infraestrutura de TI acompanhada de justificativa e, quando for o caso, dos requisitos necessários.

38. Os dispositivos de propriedade do TCU disporão de área de armazenamento destinada a dados específicos do usuário.

39. Somente os dados dessa área que estejam de acordo com a PCSI/TCU são resguardados pela central de serviços de TI quando da instalação de cópia-imagem.

40. O inventário de *softwares* e a sua atualização em cada estação de trabalho do TCU serão realizados pela unidade responsável pela infraestrutura de TI conforme procedimentos e padrões por ela definidos.

41. A instalação de *software* em recursos de TI do TCU é atribuição exclusiva da unidade responsável pela infraestrutura de TI ou de pessoa ou empresa por ela expressamente autorizada.

42. A unidade responsável pela infraestrutura de TI deverá elaborar, manter atualizada e divulgar relação de *softwares* homologados para utilização na rede TCU, bem como poderá realizar provas de conceito de novos *softwares*.

43. A unidade responsável pela infraestrutura de TI deverá definir os critérios e requisitos de segurança para a instalação ou a execução de *softwares* em recursos de TI que façam uso da rede TCU.

44. *Software* instalado ou executado em desacordo com os critérios e requisitos de segurança de que trata o item 43 será desinstalado pela unidade responsável pela infraestrutura de TI, e o fato caracterizado como incidente de segurança da informação e previamente comunicado ao dirigente da respectiva unidade em que se encontra o recurso de TI para que sejam tomadas as providências pertinentes.

45. Os procedimentos operacionais de conformidade e segurança, a exemplo de antivírus e *Data Loss Prevention* (DLP), serão realizados em todos os recursos de TI, incluindo dispositivos particulares, que tenha acesso a serviços digitais providos pelo TCU, a critério da unidade de infraestrutura de TI do TCU.

DOS REQUISITOS DE PROVIMENTO DE SERVIÇOS DIGITAIS

46. São requisitos para provimento de serviços digitais:

46.1 definição de arquitetura para provimento de serviços;

46.2 definição de padrões mínimos de segurança;

46.3 definição de níveis mínimos de serviço;

46.4 levantamento de riscos, incluindo acerca da salvaguarda de informações em ambiente fornecido por provedor;

46.5 configuração segura de recursos e TI;

46.6 atualização contínua de correções em sistemas operacionais e de componentes de aplicações;

46.7 tratamento tempestivo de vulnerabilidades de sistemas e de componentes de aplicações;

46.8 aplicação de boas práticas de codificação segura;

46.9 desabilitação de funcionalidades consideradas desnecessárias;

46.10 desabilitação de contas e privilégios considerados desnecessários;

46.11 revisão periódica de privilégios e configurações de ambiente;

46.12 revisão periódica de compartilhamentos;

46.13 habilitação de monitoramento contínuo e auditoria de e ventos;

46.14 realização de avaliação periódica de vulnerabilidades; e

46.15 observância às diretrizes da PCSI/TCU, incluindo às previstas em normativo acerca de controle de acesso.

47. A unidade responsável pela infraestrutura de TI poderá detalhar e definir critérios complementares aos previstos no item 46, a fim de mitigar riscos de segurança e fazer frente a novos paradigmas tecnológicos relacionados a tema.

DOS PAPÉIS E RESPONSABILIDADES

48. O responsável por recurso de TI é o ponto de contato para o respectivo recurso, a quem compete:

48.1 identificar e manter atualizados os metadados necessários à correta identificação do recurso de TI e do responsável, reportando-os à unidade responsável pela infraestrutura de TI do TCU;

48.2 desabilitar serviços, configurações e portas lógicas que não sejam necessárias;

48.3 realizar configuração segura dos recursos administrados;

48.4 tratar tempestivamente vulnerabilidades associadas aos recursos administrados, inclusive as reportadas pela unidade responsável pela infraestrutura de TI, de forma diligente;

48.5 aplicar correções (*patches*), inclusive as reportadas pela unidade responsável pela infraestrutura de TI do TCU;

48.6 zelar para a instalação e configuração de soluções de segurança e auditoria aplicáveis localmente nos recursos administrados, bem como colaborar para a adequada comunicação com soluções de segurança que atuem de forma centralizada;

48.7 reportar incidentes de segurança a que tiver conhecimento;

48.8 garantir a disponibilidade de serviços, de acordo com níveis de serviço definidos, bem como assegurar o tratamento adequado de cópias para recuperação de configurações;

48.9 colaborar para o tratamento de incidentes de segurança;

48.10 colaborar para a realização de análises de vulnerabilidades;

48.11 observar orientações sobre boas práticas e a configurações específicas de segurança da informação; e

48.12 observar o disposto na PCSI/TCU quanto à salvaguarda de informações produzidas ou custodiadas pelo Tribunal, bem como à proteção da própria rede TCU.

49. São responsabilidades da unidade responsável pela infraestrutura de TI, como administradora da rede TCU:

49.1 garantir a disponibilidade de serviços, de acordo com níveis de serviço definidos;

49.2 implantar e manter atualizados mecanismos e procedimentos de proteção da rede contra ataques externos e internos;

49.3 realizar triagem, análise, notificação e resposta a incidentes de segurança da informação relacionados aos serviços e soluções de tecnologia da informação;

49.4 realizar identificação periódica e notificação de vulnerabilidades de TI, bem como monitorar a aplicação de correções (*patches*);

49.5 executar, manter e restaurar cópias de segurança (*backup*) de informações disponíveis em servidores corporativos na rede TCU;

49.6 implantar e manter atualizados sistemas operacionais e mecanismos de proteção das estações de trabalho; e

49.7 coordenar a atualização de sistemas operacionais, serviços e soluções de equipamentos servidores.

50. A unidade responsável pela infraestrutura de TI proporá regras gerais para cópias de segurança de informações disponíveis em servidores corporativos na rede TCU em normativo próprio.

51. A unidade responsável pela infraestrutura de TI é responsável ainda pelo monitoramento da rede TCU com o objetivo de:

51.1 minimizar riscos de segurança da informação da rede TCU;

51.2 gerenciar o uso e prover dimensionamento adequado da rede TCU;

51.3 identificar indício de uso inadequado da rede TCU ou em desacordo com os normativos vigentes;

51.4 bloquear o acesso a sítios de má reputação ou que contenham ou distribuam conteúdo que possa representar risco à segurança da rede TCU;

51.5 identificar e solucionar problema no acesso a conteúdos e serviços por meio da rede; e

51.6 priorizar tráfego de dados de interesse do Tribunal.

52. São responsabilidades dos usuários relacionadas ao uso de recursos de TI, incluindo dispositivos particulares, para acesso à rede TCU:

52.1 ser responsável pelas operações realizadas a partir do respectivo privilégio concedido, sujeito às sanções previstas na PCSI/TCU, bem como nas disposições contratuais associadas à prestação de serviços, quando envolver colaboradores;

52.2 obedecer aos normativos vigentes, inclusive sobre segurança da informação;

52.3 salvaguardar informações armazenadas que possam comprometer a segurança do TCU, incluindo credenciais pessoais;

52.4 zelar pelas atividades realizadas por meio da utilização de sua conta para acesso à rede TCU;

52.5 zelar pela integridade, confidencialidade e disponibilidade dos dados aos quais tiverem acesso;

52.6 alterar imediatamente senha de conta de usuário da rede TCU e qualquer outra que proveja acesso a soluções de TI do Tribunal que tenham sido utilizadas em dispositivo particular, em caso de incidente de segurança da informação ou desfazimento do dispositivo;

52.7 informar imediatamente à unidade responsável pela segurança da informação os incidentes de segurança da informação de que tenham ciência ou suspeita envolvendo ativos de TI, inclusive o respectivo dispositivo particular, incluindo casos de perda, extravio ou roubo;

52.8 configurar os próprios dispositivos particulares para acesso à rede sem fio do TCU;

52.9 colaborar, na respectiva área de competência, com a identificação e o tratamento de incidentes em segurança da informação;

52.10 tratar informações classificadas ou, conforme o caso, classificar informações armazenadas na rede TCU sob sua responsabilidade, nos termos de normativos vigentes sobre o assunto no Tribunal;

52.11 observar disposições quanto ao tratamento de informações com classificação sigilosa quanto ao grau de confidencialidade, previstas em normativos do Tribunal e, em caso de dúvidas, entrar em contato com o responsável pela classificação da respectiva informação;

52.12 selecionar senhas de boa qualidade, atendendo, no mínimo, aos critérios previstos no Anexo II, para contas de usuário da rede TCU, e na Portaria-CGTI nº 2, de 16 de dezembro de 2011, para contas administrativas;

52.13 observar os dispositivos constantes em normativos vigentes de acesso à internet, de uso da rede e demais associados a segurança da informação à rede TCU; e

52.14 configurar e instalar, em seu(s) dispositivo (s) particular(es) utilizados para acesso a rede TCU, os *softwares* necessários em cumprimento das orientações da unidade de infraestrutura de TI com vistas a garantir a segurança da rede TCU e conformidade com os normativos aplicáveis.

53. Ao utilizar rede de computadores externa por meio de dispositivos de propriedade do TCU, o usuário deve obedecer também às normas e às diretrizes daquelas redes.

DAS DISPOSIÇÕES FINAIS

54. O presente anexo utilizará o Glossário de Termos da PCSI/TCU, constante no Anexo I, para promover uma compreensão comum e consistente de conceitos em função da natureza específica do tema.

55. As seguintes ações indevidas relativas à rede TCU são passíveis de apuração de responsabilidade:

55.1 acesso à rede para fins ilegais ou em desacordo com o código de ética dos servidores do Tribunal e outras normas pertinentes;

55.2 conexão cabeada à rede TCU, sem autorização expressa da unidade responsável pela infraestrutura de TI, de recurso de TI que não seja de propriedade do TCU;

55.3 utilização ou tentativa de utilização, com indícios de fraude, sabotagem ou comprometimento da rede TCU, de conta cujo acesso não seja autorizado ao usuário;

55.4 tentativa de acesso não autorizado a recursos de TI, com indícios de fraude, sabotagem ou comprometimento à rede TCU;

55.5 emprego, promoção ou facilitação deliberada de ataque com origem ou destino à rede TCU;

55.6 emprego, promoção ou facilitação de uso de ferramentas de exploração de vulnerabilidades ou afins, exceto quando expressamente autorizados pela unidade responsável pela infraestrutura de TI;

55.7 desenvolvimento, manutenção, utilização, armazenamento ou divulgação de *software* ou procedimento que permita ou tente violar sistemas de segurança da rede TCU, inclusive mecanismos de acesso anônimo (*anonymizing*), de forja de remetente (*spoofing*), de escalonamento de privilégios ou de negação de serviço (DoS);

55.8 propagação deliberada de qualquer tipo de artefato malicioso (*malware*), a exemplo de vírus, *worm*, *backdoor* ou cavalo de tróia;

55.9 utilização com indícios de fraude, sabotagem ou comprometimento da rede TCU, de mecanismo que provoque congestionamento da rede, sobrecarga ou indisponibilidade de serviço;

55.10 utilização de *software* para captura, mapeamento ou geração de tráfego, exceto pelas equipes de administração e de segurança da informação da rede TCU;

55.11 utilizar serviço que permita controle remoto de dispositivo da ISD/TCU a partir da internet, exceto nos casos explicitamente autorizados pela unidade responsável pela infraestrutura de TI;

55.12 não comunicação das vulnerabilidades de que tenha conhecimento à unidade responsável pela segurança da informação; e

55.13 outras utilizações em desacordo com as normas de segurança estabelecidas pela PCSI/TCU.

56. A violação ou a inobservância aos dispositivos deste anexo poderá ser considerada incidente de segurança da informação, e poderá implicar, isolada ou cumulativamente, em sanção prevista na PCSI/TCU e nas seguintes medidas:

56.1 limitação do uso da rede TCU;

56.2 representação para apuração de responsabilidades, que pode ocasionar recolhimento dos recursos computacionais necessários à preservação de evidências;

56.3 comunicação do fato à chefia imediata, à unidade responsável pelo contrato ao qual está vinculado, e ainda a outras instâncias do TCU; e

56.4 outras sanções administrativas, civis e penais, nos termos da legislação vigente.

57. A limitação cautelar do uso da rede TCU é aplicável a:

57.1 servidores ativos, mediante anuência dos titulares das respectivas unidades ou secretaria-geral as quais se encontra vinculado, com posterior comunicação ao usuário envolvido; e

57.2 usuários colaboradores, externos e visitantes, a realizada pela unidade responsável pela infraestrutura de TI, a qualquer tempo, com prévia autorização do comitê de segurança da informação do Tribunal cabendo delegação de competência à área responsável pela segurança da informação.

58. A limitação cautelar do uso da rede TCU pode ser proposta pela unidade responsável pela segurança da informação ou pela unidade responsável pela infraestrutura de TI ou, ainda, pelo titular da unidade de lotação do usuário, mediante solicitação justificada.

59. A liberação da limitação do uso da rede TCU a que se refere os itens 57 e 58 será realizada pela unidade responsável pela infraestrutura de TI no primeiro dia útil após a expiração da medida cautelar.

60. Em caso de suspeita de ataque ou iminente comprometimento da rede TCU, a limitação do uso da rede TCU poderá ser aplicável de imediato pela unidade responsável pela infraestrutura de TI, cabendo posterior comunicação às partes previstas no item 57.

61. A unidade responsável pela infraestrutura de TI adotará as medidas necessárias para operacionalizar o disposto neste anexo.

62. O comitê de responsável pela segurança da informação deverá monitorar e avaliar periodicamente as práticas de segurança da informação relativas às regras estabelecidas neste anexo, e propor os ajustes que considerar necessários.

63. Os casos omissos são analisados pela unidade responsável pela segurança da informação, ouvido o responsável pelo recurso de TI em questão, e dirimidos pelo comitê de responsável pela segurança da informação.

64. Em caso de divergência entre as normas das redes externas e a PCSI/TCU, prevalece o definido nas normas do TCU.

ANEXO IV DA PORTARIA-TCU Nº 89, DE 20 DE ABRIL DE 2023

REGRAS GERAIS DE USO DE COMPUTAÇÃO EM NUVEM (*CLOUD COMPUTING*) NO TCU.

1. Este anexo estabelece regras gerais de uso de computação em nuvem no TCU (nuvem TCU).

DA NUVEM TCU

2. A nuvem TCU é serviço de computação em nuvem, mediante arquitetura de serviços como infraestrutura, plataforma ou software, fornecido por provedor de serviços em nuvem, ou localmente, por meios próprios.

3. A nuvem TCU estende a infraestrutura de serviços providos pela rede TCU.

4. O provimento da nuvem TCU pode ser intermediado por *cloud broker*.

5. A nuvem TCU disporá de ambiente seguro e atenderá, no que couber, às diretrizes estabelecidas no normativo sobre uso da rede TCU.

6. A nuvem TCU atenderá aos seguintes requisitos:

6.1 autoprovisionamento de recursos na nuvem e ajuste de acordo com as necessidades no decorrer do tempo, de maneira automática, sem a necessidade de interação com provedor de serviços;

6.2 elasticidade na alocação e liberação de recursos contratados dinamicamente, conforme demanda;

6.3 mensuração automática de serviços para estabelecimento de níveis mínimos de serviço, otimização de recursos e, se aplicável, precificação por uso;

6.4 isolamento de recursos computacionais oriundos do provedor, caso haja a prestação de serviços para múltiplos clientes, em arquitetura multi-inquilino;

6.5 amplo acesso aos recursos da nuvem por diferentes recursos de TI, como estações de trabalho, *tablets* e *smartphones*;

6.6 monitoramento para assegurar transparência no uso de recursos, controle de uso, verificar inobservâncias às normas definidas na PCSI/TCU e fornecer evidências, no caso de incidentes de segurança da informação, respeitados os direitos e as garantias individuais previstos em lei;

6.7 segurança em múltiplas camadas para proporcionar a sobreposição de controles de segurança a fim de mitigar riscos, particularmente se houver ataque bem-sucedido em uma das camadas; e

6.8 detenção, pelo TCU, do maior nível de privilégio de administração da nuvem pública de que fizer uso.

7. A nuvem TCU será provida exclusivamente pela unidade responsável pela infraestrutura de TI do TCU.

DOS PRINCÍPIOS

8. São princípios para o uso da nuvem TCU:

8.1 *Security by design*: incorporar boas práticas de segurança da informação para diminuir as vulnerabilidades desde a fase de planejamento e projeto dos serviços digitais;

8.2 Governança: implementar mecanismos para garantir a identificação de cargas de trabalho, usuários e permissionamento no ambiente da nuvem, bem como a adequada gestão de recursos e de processos de trabalho por meio da automação;

8.3 Modelo de segurança compartilhada: habilitar os mecanismos de segurança pertinentes à carga de trabalho implementada (security by default) seguindo a divisão de responsabilidade entre provedor de nuvem e TCU de acordo com o modelo de serviço da carga de trabalho implementada (IaaS, PaaS, SaaS); e

8.4 Gerenciamento de risco: incorporar mecanismos de análise de risco e estabelecer medidas de tratamento de risco desde a fase de planejamento e projeto.

DAS FUNÇÕES E RESPONSABILIDADES

9. São funções relativas ao uso de nuvem:

9.1 Gestor de segurança da informação;

9.2 Comitê de Segurança da informação;

9.3 Responsável pelo recurso de TI;

9.4 Responsável pela Infraestrutura de TI; e

9.5 Provedores de nuvem.

10. São responsabilidades do Gestor de Segurança da Informação:

10.1 instituir e coordenar a equipe responsável pelas revisões do ato normativo sobre uso seguro de computação em nuvem; e

10.2 supervisionar a aplicação do ato normativo sobre uso seguro de computação em nuvem.

11. São responsabilidade da unidade responsável pela infraestrutura de TI:

11.1 assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem, que fornece tais serviços ao órgão ou à entidade, de forma a assegurar que os controles e os níveis de serviço acordados sejam cumpridos; e

11.2 supervisionar a aplicação das medidas de correção pelo provedor de serviço de nuvem, em casos de eventuais desvios.

12. Aplica-se no que couber as responsabilidades definidas nos demais anexos que compõem esta Portaria.

13. São responsabilidades do comitê de segurança da informação:

13.1 estabelecer restrições geográficas aplicáveis a dados e informações custodiados pelo TCU de acordo com sua classificação;

13.2 analisar, em caráter conclusivo, as minutas de revisão do ato normativo sobre o uso seguro de computação em nuvem; e

13.3 definir necessidade de criptografia para o armazenamento de dados e informações, custodiados pela administração pública federal, em soluções de computação em nuvem de acordo com sua classificação.

14. As responsabilidades do responsável por recurso de TI estão definidas nos demais anexos a esta Portaria.

15. As responsabilidades relativas ao provedor de nuvem seguem o modelo de responsabilidade compartilhada de acordo com a figura 1 do Anexo I desta Portaria.

DAS DISPOSIÇÕES FINAIS

16. O presente anexo utilizará o Glossário de Termos da PCSI/TCU, constante no Anexo I, para promover uma compreensão comum e consistente de conceitos em função da natureza específica do tema.

17. A violação ou a inobservância aos dispositivos deste anexo poderá ser considerada incidente de segurança da informação, e implicar, isolada ou cumulativamente, em sanção prevista na PCSI/TCU.

18. Aplica-se, no que couber, relativamente ao acesso à nuvem TCU, as situações passíveis de apuração de responsabilidade previstas no item 55 do Anexo III, bem como aos critérios de acesso a espaços de armazenamento de usuários previstos no item 32 do referido anexo.

19. A unidade responsável pela infraestrutura de TI adotará as medidas necessárias para operacionalizar o disposto neste anexo.

20. O comitê responsável pela segurança da informação deverá monitorar e avaliar periodicamente as práticas de segurança da informação relativas às regras estabelecidas neste Anexo, e propor os ajustes que considerar necessários.

21. Os casos omissos são analisados pela unidade responsável pela segurança da informação, ouvido o administrador do recurso em questão, e dirimidos pelo comitê responsável pela segurança da informação.

22. Este anexo deverá ser revisto, no máximo, a cada dois anos.

23. A revisão poderá ocorrer a qualquer tempo, quando houver mudanças significativas nos requisitos de segurança da informação que influenciem o uso seguro de computação em nuvem, de forma a assegurar sua continuidade, sustentabilidade, adequação e efetividade.

ANEXO V DA PORTARIA-TCU Nº 89, DE 20 DE ABRIL DE 2023

CRITÉRIOS PARA UTILIZAÇÃO DE DISPOSITIVOS PARTICULARES, POR USUÁRIOS INTERNOS, PARA EXECUÇÃO DE ATIVIDADES A CARGO DO TCU.

1. Os critérios para uso de dispositivos particulares, por usuários internos, na execução de atividades a cargo do TCU são os estabelecidos neste anexo.
2. O uso de dispositivos particulares será feito de forma identificada, por meio de usuário autenticado, exceto nos casos expressamente autorizados pelas unidades provedoras de TI.
3. O uso de dispositivos particulares, será realizado de forma a não comprometer a imagem do TCU, nem colocar em risco a segurança das informações produzidas ou custodiadas pelo Tribunal ou a qualidade e a segurança da ISD/TCU.
4. São responsabilidades dos usuários relacionadas ao emprego de dispositivos particulares:

4.1 salvaguardar informações armazenadas que possam comprometer a segurança do TCU, incluindo credenciais pessoais;

4.2 zelar pelas atividades realizadas por meio da utilização de sua conta de usuário;

4.3 zelar pela integridade, confidencialidade e disponibilidade dos dados aos quais tiverem acesso;

4.4 alterar imediatamente senha de conta de usuário e qualquer outra que proveja acesso a soluções de TI do Tribunal que tenham sido utilizadas em dispositivo particular, em caso de incidente de segurança da informação ou desfazimento do dispositivo;

4.5 informar imediatamente à unidade responsável pela segurança da informação os incidentes em segurança de que tenham ciência ou suspeita envolvendo o respectivo dispositivo particular, inclusive em caso de perda, extravio ou roubo;

4.6 configurar, de forma segura, os próprios dispositivos particulares utilizados no exercício de atividades a cargo do TCU, inclusive no acesso à ISD/TCU;

4.7 colaborar, na respectiva área de competência, com a identificação e o tratamento de incidentes em segurança da informação;

4.8 tratar informações classificadas ou, conforme o caso, classificar informações sob sua responsabilidade armazenadas no dispositivo particular, nos termos dos normativos vigentes sobre o assunto no Tribunal; e

4.9 observar os dispositivos constantes em normativos vigentes de acesso à internet, de uso da rede, de acesso remoto, de computação em nuvem e demais integrantes da PCSI/TCU.

5. São requisitos para uso de dispositivos particulares:

5.1 utilizar *softwares* originais, provenientes de repositórios confiáveis;

5.2 não utilizar aplicações com qualquer mecanismo de adulteração (*jailbreak*, *rooted*), nem com emprego de chaves de licença indevidas (como geradores automáticos obtidos na Internet);

5.3 manter atualizações (*patches*) de sistemas e aplicações, inclusive de segurança, em dia;

5.4 habilitar mecanismos de controle de acesso físico e lógico ao dispositivo, não compartilhando com terceiros as credenciais utilizadas no exercício das atividades a cargo do TCU;

5.5 zelar pela segurança do dispositivo, inclusive por meio do uso de aplicativos de segurança, mantendo-os atualizados, a exemplo de:

a) antivírus, *firewall* e *antimalware*;

b) criptografia de discos;

c) criptografia de arquivos;

d) deleção segura de arquivos; e

e) gerenciamento de senhas.

5.6 habilitar funcionalidade de controle de acesso individualizado no sistema operacional empregado para acesso remoto (multiusuário) e assegurar que o acesso remoto será feito a partir de conta local empregada exclusivamente pelo usuário;

5.7 habilitar fatores de autenticação no dispositivo particular utilizado, pelo menos por meio de senha;

5.8 manter armazenadas informações produzidas ou custodiadas pelo Tribunal em espaço acessível apenas por contas locais exclusivas do usuário;

5.9 não instalar *softwares* capazes de aumentar riscos de segurança ao ativo, como compartilhadores ponto-a-ponto (*torrents*, *p2p*), mesmo que em usuário local distinto;

5.10 não instalar *softwares* ou armazenar informações cujo conteúdo represente violação às leis vigentes, mesmo que em usuário local distinto;

5.11 não instalar *softwares* que possam produzir riscos às informações produzidas ou custodiadas pelo Tribunal, inclusive localmente, ou à qualidade ou segurança da ISD/TCU, bem como à imagem institucional, mesmo que em usuário local distinto;

5.12 não instalar *softwares* que possam subverter ou prejudicar monitoramento de informações relativas ao acesso remoto, como redes anônimas (ex: Tor) ou serviços de *proxy* anônimos (*anonymizers*), mesmo que em usuário local distinto;

5.13 não configurar liberação de portas lógicas que possam produzir riscos às informações produzidas ou custodiadas pelo Tribunal, inclusive localmente, ou à qualidade ou segurança da ISD/TCU, bem como à imagem institucional; e

5.14 estar em conformidade com mecanismos de segurança a serem definidos pela unidade responsável pela infraestrutura de TI, inclusive com a obrigatoriedade de instalação, pelas unidades provedoras de TI do TCU, de aplicações de segurança no dispositivo particular.

6. O não atendimento de algum dos requisitos elencados no item 5 acarretará a impossibilidade de utilização do dispositivo particular para o exercício de atividades a cargo do TCU.

7. É vedado ao usuário de dispositivos particulares empregar, enquanto o dispositivo particular estiver vinculado à conexão provida diretamente pelo TCU, outro meio de conexão à internet, a exemplo de compartilhamento de conexão provida por operadora de telefonia móvel (*hotspot*, *gateway*, ancoragem ou roteamento).

8. São responsabilidades da unidade de infraestrutura de TI relacionadas aos dispositivos particulares conectados à rede TCU:

8.1 definir procedimentos para mitigar riscos de contaminação, de tentativas de ataques e de uso indevido do dispositivo particular;

8.2 gerenciar a ISD/TCU quanto ao acesso de dispositivos particulares;

8.3 identificar indício de uso inadequado da ISD/TCU ou em desacordo com os normativos vigentes; e

8.4 informar parâmetros básicos de configuração de dispositivos particulares na ISD/TCU.

9. O acesso à internet realizado por meio da rede TCU pode ser submetido a controle quanto ao tempo de uso ou ao volume de dados trafegados, a ser especificado em normativo próprio.

10. Não é responsabilidade do TCU resolver problemas referentes ao dispositivo particular utilizado pelo usuário interno para o exercício de atividades em favor do Tribunal.

11. O uso de dispositivos particulares em desacordo com este anexo ou que comprometa a segurança da ISD/TCU poderá ser considerado incidente de segurança da informação, além de poder acarretar, isolada ou cumulativamente, as sanções previstas na PCSI/TCU e as seguintes medidas:

11.1 comunicação do fato à chefia imediata, à unidade responsável pelo contrato ao qual está vinculado, e ainda a outras instâncias do TCU;

11.2 bloqueio do acesso indevido pela unidade responsável pela infraestrutura de TI; e

11.3 representação para apuração de responsabilidades.

12. Aplica-se, no que couber, relativamente ao uso de dispositivos particulares, as situações passíveis de apuração de responsabilidade previstas no item 26 do Anexo III a esta Portaria.

13. O presente anexo utilizará o Glossário de Termos da PCSI/TCU, constante no Anexo I, para promover compreensão comum e consistente de conceitos em função da natureza específica do tema.

14. A unidade responsável pela infraestrutura de TI adotará as medidas necessárias para operacionalizar o disposto neste anexo.

15. Situações específicas poderão ser submetidas à análise do comitê de segurança da informação.

ANEXO VI DA PORTARIA-TCU Nº 89, DE 20 DE ABRIL DE 2023

CRITÉRIOS PARA ACESSO À INTERNET PROVIDO PELO TCU.

1. Os critérios para acesso a informações e serviços disponíveis na internet por meio da infraestrutura de serviços digitais do TCU são os estabelecidos neste anexo.

2. Dispositivos de propriedade do TCU que acessam à internet mesmo fora da ISD estão sujeitos aos controles do presente anexo, de acordo com critérios definidos pela unidade de infraestrutura do TCU.

3. O acesso à internet provido pelo TCU constitui solução corporativa de tecnologia da informação destinada à obtenção de informações e serviços disponíveis na rede mundial de computadores, para execução de atividades de interesse do Tribunal.

4. O Tribunal é usuário de acesso à internet provido por terceiros, nos termos da Lei nº 12.965/2014, e autoriza servidores e colaboradores a utilizar esse serviço por meio da ISD.

5. O acesso à internet provido pelo TCU será feito de forma identificada, por usuário autenticado, exceto nos casos expressamente autorizados pela unidade responsável pela infraestrutura de TI do Tribunal.

6. O acesso à internet pode ser autorizado a usuário visitante, de acordo com procedimento definido pela unidade responsável pela infraestrutura de TI do Tribunal.

7. É permitido o uso da internet para acesso a informação ou serviço de caráter pessoal, desde que a frequência de uso, o volume e a qualidade dos dados transmitidos não conflitem com as definições deste item nem comprometam ou conflitem com:

7.1 a imagem do Tribunal;

7.2 a segurança ou o desempenho da infraestrutura de serviços digitais do Tribunal ou de terceiros;

7.3 o Código de Ética dos Servidores do TCU e outras normas pertinentes; e

7.4 a produtividade pessoal.

8. O acesso aos serviços e conteúdos enquadrados no item 3 pode estar sujeito a controle quanto aos requisitos de segurança, tempo de uso e/ou volume de dados trafegados.

9. O acesso à internet será realizado de forma a não comprometer a imagem do TCU, nem colocar em risco a segurança das informações produzidas ou custodiadas pelo Tribunal ou a qualidade e a segurança da ISD.

10. É vedado o acesso aos seguintes serviços e conteúdos:

10.1 *download* de arquivo executável;

10.2 jogo ou entretenimento *online*;

10.3 de compartilhamento ou de transferência de arquivos ou de mídias, exceto soluções corporativas do Tribunal;

10.4 que envolvam violação a direito de propriedade, pornografia, pedofilia, fomento ao racismo, estimule o uso de drogas ou cujo conteúdo represente violação às leis vigentes;

10.5 que envolvam violação de dados pessoais;

10.6 disponíveis em porta lógica não especificada pela unidade responsável pelo serviço de TI; e

10.7 outros que não guardem relação com atividade de interesse do Tribunal.

11. O acesso aos serviços e conteúdos descritos no item 10 pode ser liberado, em caráter excepcional, após análise de justificativa apresentada pelo interessado à unidade responsável pela infraestrutura de TI, sujeito a controle quanto aos requisitos de segurança, tempo de uso e/ou volume de dados trafegados.

12. O acesso à internet será monitorado com o objetivo de:

12.1 assegurar a segurança da informação e a qualidade do acesso à internet a partir da ISD;

12.2 gerenciar o uso e prover dimensionamento adequado do serviço;

12.3 preservar a segurança da ISD;

12.4 identificar indício de uso inadequado da internet ou em desacordo com os normativos vigentes;

12.5 bloquear o acesso a sítios de má reputação ou que contenham ou distribuam conteúdo que possa representar risco à segurança da ISD ou que estejam entre as categorias elencadas no item 10;

12.6 identificar e solucionar problema no acesso a conteúdos e serviços por meio da rede;

12.7 garantir a conformidade com leis e normativos vigentes; e

12.8 priorizar tráfego de dados do interesse do Tribunal.

13. O monitoramento de acesso à internet associado a sites bancários ou a sites cujo sigilo é protegido por lei será restrito com vistas a garantir sigilo de operações envolvidas.

14. O acesso à internet em desacordo com este anexo ou que comprometa a segurança da ISD poderá ser considerado incidente de segurança da informação, além de poder acarretar, isolada ou cumulativamente, as sanções previstas na PCSI/TCU e as seguintes medidas:

14.1 comunicação do fato à chefia do infrator, à unidade responsável pelo contrato ao qual está vinculado, e ainda a outras instâncias do TCU;

14.2 bloqueio do acesso indevido pela unidade responsável pela infraestrutura de TI; e

14.3 representação para apuração de responsabilidades, que pode ocasionar recolhimento dos recursos computacionais necessários à preservação de evidências e suspensão temporária do acesso do infrator à ISD ou à internet.

15. Aplica-se, no que couber, relativamente ao acesso à internet, as situações passíveis de apuração de responsabilidade previstas no item 55 do Anexo III.

16. O presente anexo utilizará o Glossário de Termos da PCSI/TCU, constante no Anexo I, para promover compreensão comum e consistente de conceitos em função da natureza específica do tema.

17. A unidade responsável pela infraestrutura de TI adotará as medidas necessárias para operacionalizar o disposto neste anexo.

18. Situações específicas poderão ser submetidas à análise do comitê de segurança da informação.

ANEXO VII DA PORTARIA-TCU Nº 89, DE 20 DE ABRIL DE 2023

USO DE ACESSO REMOTO NO TCU.

1. O acesso remoto à rede TCU obedece ao disposto neste Anexo, mediante os seguintes métodos:

1.1 acesso remoto por meio de tunelamento (VPN);

1.2 acesso remoto por meio de solução de virtualização de estação de trabalho (VDI); e

1.3 acesso por meio de consoles específicos, no caso de nuvem pública.

2. A unidade responsável pela infraestrutura de TI detalhará processos para operacionalização dos métodos enumerados, bem como requisitos de segurança necessários.

3. O acesso remoto, conforme tratado neste anexo, destina-se à execução de atividades de desenvolvimento e manutenção de serviços de TI.

4. O acesso remoto para outras finalidades, bem como o interno, encontra-se fora do escopo do normativo e poderá empregar outros meios disponíveis na rede TCU.

5. O acesso remoto será realizado, em regra, por meio de solução de virtualização de estação de trabalho (VDI).

6. O acesso remoto via tunelamento será avaliado em caráter excepcional, mediante justificativa a ser avaliada pela unidade responsável pela infraestrutura de TI.

7. O acesso remoto será realizado de forma a não comprometer a imagem do TCU, nem colocar em risco a segurança das informações produzidas ou custodiadas pelo TCU ou a qualidade e a segurança da rede TCU.

DOS PROCESSOS DE VPN

8. O acesso remoto por tunelamento contém os seguintes processos:

8.1 concessão; e

8.2 revogação.

9. A unidade responsável pela infraestrutura de TI detalhará procedimentos para operacionalização dos processos enumerados.

10. O chefe imediato da área de lotação do solicitante é o responsável pelas solicitações de acesso remoto de sua equipe.

11. O processo de concessão compreende as seguintes etapas:

11.1 preenchimento e assinatura do formulário de solicitação, contendo Termo de Sigilo e Responsabilidade (TSR), em anexo;

11.2 encaminhamento do formulário à unidade responsável pela infraestrutura de TI, pelo responsável;

11.3 análise do pedido; e

11.4 credenciamento do solicitante, em caso de deferimento.

12. A solicitação indicará o período de acesso, de acordo com a necessidade de serviço.

13. O formulário e o TSR serão assinados pelo solicitante e pelo responsável.

14. O credenciamento da senha será realizado diretamente pelo solicitante.

15. As configurações necessárias para dar atendimento ao pedido de acesso remoto estarão limitadas ao escopo da solicitação.

16. A concessão de acesso remoto estende a rede TCU para os ativos empregados na conexão, ensejando aumento de riscos de segurança e cautela acerca das operações realizadas.

18. O pedido de prorrogação será encaminhado pelo responsável, sendo dispensado encaminhamento de novo TSR.

19. Caso o solicitante seja colaborador, o acesso remoto não ultrapassará o prazo do contrato de estágio ou de prestação de serviços.

20. O prazo de validade do certificado digital para acesso remoto é de 2 (dois) anos, sendo necessária geração de novo certificado, ao final do período, caso a necessidade permaneça.

21. O Tribunal promoverá a reemissão do certificado digital sempre que houver a expiração do respectivo prazo de validade, nos termos da Portaria-TCU n.º 188/2010, bem como as atualizações constantes na Resolução-TCU nº 312/2020.

22. O pedido de novo certificado digital será encaminhado pelo responsável, sendo dispensado preenchimento de novo TSR.

23. O processo de revogação compreende as seguintes etapas:

23.1 verificação periódica de inventário de credenciamentos realizados; e

23.2 revogação de credenciais de acesso remoto.

24. São hipóteses sujeitas à revogação de credenciais de acesso remoto:

24.1 expiração do prazo de concessão de acesso ou de certificado digital;

24.2 a pedido do solicitante ou do responsável;

24.3 perda de vínculo contratual, no caso de colaboradores;

24.4 mudança de lotação de solicitante para área não abrangida pelo normativo;

24.5 situações excepcionais de inatividade e afastamentos; e

24.6 a qualquer tempo em razão de violação do TSR ou de incidente de segurança da informação, com vistas a minimizar riscos às informações produzidas ou custodiadas pelo Tribunal ou à qualidade ou segurança da rede TCU, bem como à imagem institucional.

25. A revogação prevista nos subitens 24.1, 24.2, 24.3, 24.4 e 24.6 poderá ser aplicada automaticamente, sem consulta prévia.

25. O responsável deve solicitar a revogação de acesso remoto tão logo não seja mais considerado necessário.

26. São situações excepcionais relativas de inatividade e afastamentos:

26.1 conta sem uso por período igual ou superior a 6 (seis) meses, para servidores;

26.2 conta sem uso por período igual ou superior a 2 (dois) meses para colaboradores; ou

26.3 quando o servidor ativo estiver em afastamento preventivo do exercício do cargo em decorrência do disposto no art. 147 da Lei nº 8.112, de 1990.

27. A revogação prevista nos subitens 26.1 e 26.2 poderá ser aplicada automaticamente, sem consulta prévia.

28. A revogação prevista no subitem 26.3 é realizada por solicitação enviada pela Secretaria-Geral de Administração (Segedam).

DO PROCESSO DE MONITORAMENTO

29. O processo de monitoramento de acesso remoto tem como objetivo:

29.1 minimizar riscos de segurança da informação da rede TCU;

29.2 gerenciar uso e prover dimensionamento adequado da rede TCU;

29.3 identificar indício de uso inadequado da rede TCU ou em desacordo com os normativos vigentes, incluindo a PCSI/TCU;

29.4 fornecer evidências, no caso de incidente de segurança da informação, respeitados os direitos e as garantias individuais previstos em lei e observados os procedimentos previstos para situações específicas dispostas neste Anexo;

29.5 bloquear acessos que possam representar risco à segurança da rede TCU;

29.6 identificar e solucionar problemas de acesso; e

29.7 priorizar tráfego de dados de interesse do Tribunal.

DA IDENTIFICAÇÃO, DA AUTENTICAÇÃO E DA AUTORIZAÇÃO

30. As credenciais de acesso remoto são únicas, intransferíveis e de responsabilidade exclusiva do titular e seus privilégios não podem ser estendidos a terceiros.

31. Senha associada à credencial de acesso remoto será alterada periodicamente.

32. O período de alteração de senha não será superior a 03 (três) meses.

33. A alteração da senha empregada no acesso remoto poderá ser efetuada pelo próprio usuário ou mediante pedido à central de serviços de TI.

34. O usuário deve alterar a senha sempre que existir indício de comprometimento da segurança das credenciais envolvidas.

35. O acesso remoto será realizado por solução indicada pela unidade responsável pela infraestrutura de TI, com capacidade para manter registros das conexões efetuadas por meio da solução, incluindo, no mínimo, usuário, data-hora de conexão, data-hora de desconexão e endereço de rede de origem e de destino.

36. A autenticação no acesso remoto será feita, pelo menos, por meio de duplo fator de autenticação (2FA), atendendo aos seguintes requisitos mínimos:

36.1 O mecanismo de autenticação automática (*auto login* ou autocompletamento) será desabilitado;

36.2 As informações sobre senhas não devem ser salvas localmente, nem incluídas em processos automáticos de acesso (por exemplo, macros);

36.3 Credenciais de acesso remoto não serão empregadas em processos de autenticação em serviços do sistema, incluindo rotinas de agendamento de tarefas;

36.4 Será admitido como meio alternativo de autenticação, mecanismos considerados mais seguros como certificação digital, biometria e procedimentos com dois fatores; e

36.5 A autenticação poderá ser precedida de rotina automatizada de verificação de condições locais de acesso (*healthcheck*).

37. Enquanto estiver autenticado, o usuário deve bloquear o ativo de TI sempre que se afastar dele ou deixá-lo desassistido.

38. A autorização de acesso remoto respeitará o princípio do menor privilégio e a necessidade de conhecer.

40. Caso as credenciais de acesso remoto envolvam privilégios administrativos de ativos de TI do TCU, serão observadas disposições de normativo próprio sobre contas administrativas.

DOS PAPÉIS E RESPONSABILIDADES

41. São deveres do usuário:

41.1 realizar acesso remoto a partir de ativos de TI de propriedade do Tribunal ou dispositivos particulares, sendo vedado o acesso remoto a partir de equipamentos públicos ou não controlados pelo usuário;

41.2 ser ponto de contato para notificações de incidentes de segurança da informação e de vulnerabilidades relacionadas a credenciais e acessos remotos de sua responsabilidade, bem como colaborar para a resolução de eventos decorrentes;

41.3 armazenar, de forma segura credenciais e certificados digitais, se adotados, para o acesso remoto; e

41.4 selecionar senhas de boa qualidade para o acesso remoto, atendendo, no mínimo, aos critérios previstos na norma referente ao controle de acesso (Anexo II), para contas de usuário da rede TCU, e na Portaria-CGTI nº 2, de 16 de dezembro de 2011, para contas administrativas.

42. São deveres da unidade responsável pela infraestrutura de TI:

42.1 gerenciar solicitações de concessão e revogação de acesso remoto;

42.2 manter inventário de acessos remotos concedidos;

42.3 definir procedimentos para operacionalizar solicitações de acesso remoto;

42.4 monitorar acessos remotos, coletando, pelo menos, os seguintes dados: usuário, data, hora de início e fim do acesso remoto, endereço de rede de origem e de destino;

42.5 observar competências previstas no art. 9 da Portaria-TCU nº 188, de 12 de agosto de 2010, acerca de emissão e distribuição de certificados digitais;

42.6 garantir a disponibilidade da rede TCU relacionada ao acesso remoto, de acordo com níveis de serviço definidos;

42.7 mitigar riscos de segurança à rede TCU e de seu uso indevido decorrentes do acesso remoto;

42.8 realizar triagem, análise, notificação e resposta a incidentes de segurança da informação relacionados à infraestrutura empregada no provimento do acesso remoto;

42.9 realizar identificação periódica e notificação de vulnerabilidades em TI à infraestrutura empregada no provimento do acesso remoto, bem como monitorar a aplicação de correções (patches);

42.10 coordenar a atualização de sistemas operacionais, serviços e soluções relacionadas à infraestrutura empregada no provimento do acesso remoto;

42.11 identificar indício de uso inadequado da rede TCU, em desacordo com normativos vigentes; e

42.12 informar, por meio da central de serviços de TI, parâmetros básicos de configuração para acesso remoto.

43. O acesso remoto pode ser submetido a controle quanto ao tempo de uso ou ao volume de dados trafegados, de forma a garantir disponibilidade do serviço a todos os usuários.

DAS DISPOSIÇÕES FINAIS

44. As seguintes ações indevidas relativas à rede TCU são passíveis de apuração de responsabilidade:

44.1 acesso remoto para fins ilegais ou em desacordo com o código de ética dos servidores do Tribunal, aprovado pela Resolução-TCU nº 330, de 1º de setembro de 2021, e outras normas pertinentes;

44.2 acesso remoto sem autorização expressa da unidade responsável pela infraestrutura de TI; e

44.3 utilização ou tentativa de utilização, com indícios de fraude, sabotagem ou comprometimento da rede TCU, de conta cujo acesso não seja autorizado ao usuário; e

44.4 prejudicar o monitoramento de acessos remotos.

45. Aplica-se, no que couber, relativamente ao acesso remoto, as situações passíveis de apuração de responsabilidade previstas no item 55 do Anexo III.

46. A violação ou a inobservância aos dispositivos deste anexo poderá ser considerada incidente de segurança da informação, e poderá implicar, isolada ou cumulativamente, em sanção prevista na PCSI/TCU e nas seguintes medidas:

46.1 revogação de credenciais de acesso remoto;

46.2 representação para apuração de responsabilidades, que pode ocasionar recolhimento dos recursos computacionais necessários à preservação de evidências;

46.3 comunicação do fato à chefia imediata ou ao responsável, bem como a outras instâncias do TCU; e

46.4 outras sanções administrativas, civis e penais, nos termos da legislação vigente.

47. O disposto no subitem 46.1 poderá ser aplicável de imediato pela unidade responsável pela infraestrutura de TI, cabendo posterior comunicação às partes previstas no subitem 46.3.

48. O presente anexo utilizará o Glossário de Termos da PCSI/TCU, constante no Anexo I, para promover compreensão comum e consistente de conceitos em função da natureza específica do tema.

49. Os casos omissos são analisados pela unidade responsável pela segurança da informação e pela responsável pela infraestrutura de TI.

ANEXO VIII DA PORTARIA-TCU Nº 89, DE 20 DE ABRIL DE 2023

REGRAS GERAIS DE USO DO SERVIÇO DE CORREIO ELETRÔNICO DO TRIBUNAL DE CONTAS DA UNIÃO.

1. As regras gerais para uso do serviço de correio eletrônico do TCU obedecem ao disposto neste anexo e à legislação pertinente.

2. Aplica-se, no que couber, os dispositivos do presente anexo à plataforma de colaboração e mensageria da organização.

3. O correio eletrônico do TCU constitui recurso corporativo para comunicação, a ser usado de modo compatível com o exercício do cargo, sem comprometer a imagem do Tribunal nem a infraestrutura de serviços digitais da instituição.

4. As caixas postais classificam-se em:

4.1 caixa postal individual, destinada a autoridade, servidor ativo ou colaborador;

4.2 caixa postal de unidade, destinada à unidade ou subunidade do TCU; e

4.3 caixa postal de uso coletivo, destinada a grupo de trabalho, comitê, comissão, projeto ou a atividade específica de interesse do TCU.

5. Cada caixa postal tem um responsável, de acordo com as seguintes regras:

5.1 para caixas postais individuais, o responsável é autoridade, servidor ativo ou usuário colaborador para o qual foi destinada a caixa postal;

5.2 para caixas postais de unidade, o responsável é o titular da unidade ou subunidade, para a qual foi destinada a caixa postal, ou a servidor por ele designado; e

5.3 para caixas postais de uso coletivo, o responsável é o coordenador pelo grupo de trabalho, comitê, comissão, projeto ou pela atividade específica de interesse do TCU à qual foi destinada a caixa postal.

6. Substitutos serão previstos em caso de impedimentos legais dos respectivos titulares, nos casos previstos nos subitens 5.2 e 5.3.

7. O responsável pela caixa postal pode autorizar a execução de atividades, objeto dos subitens 5.2 e 5.3, por outro usuário interno ou colaborador.

8. Servidores aposentados não disporão de caixas postais.

9. Cabe ao responsável pela caixa postal:

9.1 examinar o conteúdo da caixa postal para dar tratamento adequado e tempestivo às mensagens recebidas e mantê-lo de acordo com as normas integrantes da PCSI/TCU;

9.2 utilizar a caixa postal de forma a não colocar em risco a segurança das informações produzidas ou custodiadas pelo Tribunal, nem a imagem do TCU;

9.3 adotar medidas para que o volume ocupado pelo conteúdo da caixa postal não exceda os limites estabelecidos;

9.4 definir os critérios de acesso à caixa postal; e

9.5 encaminhar mensagens suspeitas à área responsável pela administração do correio eletrônico.

10. As caixas postais são destinadas a atividades de interesse do Tribunal, sendo vedado o seu uso para fins de natureza pessoal, a exemplo do cadastro em serviços externos estranhos às atividades do TCU.

11. À unidade responsável pela Infraestrutura de Tecnologia da Informação unidade responsável pelo serviço de correio eletrônico, compete:

11.1 garantir a disponibilidade do serviço de correio eletrônico, estabelecida em acordo de níveis de serviço;

11.2 estabelecer e comunicar aos responsáveis por caixas postais os limites de utilização do serviço de correio eletrônico;

11.3 implantar mecanismos que evitem o envio e a recepção de mensagens que possam comprometer a segurança do serviço de correio eletrônico ou da infraestrutura de serviços digitais do TCU;

11.4 criar, manter e excluir caixas postais;

11.5 definir, implantar e executar procedimentos de segurança e rotinas de cópia e recuperação de caixas postais;

11.6 executar as ações necessárias, quando devidamente demandadas, para fins de atendimento aos itens 14 a 16 deste anexo;

11.7 executar os procedimentos de limitação e liberação do uso do serviço de correio eletrônico, de acordo com o disposto neste Anexo; e

11.8 desenvolver outras atribuições inerentes à sua finalidade de provedora de infraestrutura de tecnologia da informação do TCU.

12. Para fins do disposto no subitem 11.3, incumbe à Comissão de Coordenação Geral (CCG) definir regras acerca do envio de mensagens às listas de distribuição integrantes do correio eletrônico do TCU, com subsídio de proposta encaminhada pelo comitê responsável pela segurança da informação.

13. As atribuições dispostas no item 11 serão desenvolvidas pela unidade responsável pelo serviço de correio eletrônico com o apoio, no que couber, da unidade responsável por soluções de tecnologia da informação.

14. Além do próprio responsável pela caixa postal, ou de pessoas por ele autorizadas, nos casos previstos no item 5, o conteúdo das caixas postais somente pode ser acessado pela unidade responsável pelo serviço de correio eletrônico e para os seguintes objetivos:

14.1 verificar a obtenção, retenção, uso e divulgação de informações por meio ou com fins ilícitos, ou em desacordo com as normas regulamentares;

14.2 recuperar conteúdo de interesse do TCU, no caso de vacância ou afastamentos legais do responsável pela caixa postal e de seu substituto;

14.3 atender demanda do Corregedor, de processo administrativo disciplinar (PAD) ou de comissão de sindicância formalmente constituída; e

14.4 atender solicitação judicial.

15. Nas hipóteses previstas nos subitens 14.1 e 14.2, o acesso ao conteúdo de caixas postais será feito mediante autorização do Presidente do TCU, ouvida a unidade responsável pela segurança da informação, a quem incumbe cientificar oportunamente o comitê responsável pela segurança da informação.

16. Aplica-se o disposto no item 14 ao conteúdo gerado em plataforma de colaboração e mensageria.

17. A exclusão de caixas postais individuais destinadas a servidores ocorrerá imediatamente após a respectiva vacância do quadro do TCU, exceto no caso de aposentadoria.

18. Para aposentadorias, as respectivas caixas postais individuais estarão disponíveis por até trintas dias.

19. A criação e a exclusão de caixa postal para usuários colaboradores seguem, no que couber, o disposto em normativo sobre concessão de perfil de acesso a soluções de tecnologia da informação para profissionais de empresas contratadas e estagiários, no âmbito do Tribunal de Contas da União.

20. Cessada a prestação do serviço terceirizado, compete à unidade fiscalizadora do contrato requerer à unidade responsável pelo serviço de correio eletrônico a imediata exclusão das caixas postais associadas aos respectivos colaboradores.

21. Findo o contrato do estágio, devem ser realizados procedimentos para a imediata exclusão das caixas postais dos respectivos estagiários.

22. As seguintes ações indevidas relativas ao correio eletrônico são passíveis de apuração de responsabilidade:

22.1 acesso ou tentativa de acesso à caixa postal sem autorização do respectivo responsável;

22.2 envio, sem autorização, de mensagem com informações protegidas por direito autoral;

22.3 envio, para pessoa física ou jurídica, em desacordo com as normas de classificação da informação quanto à confidencialidade;

22.4 envio ou armazenamento de mensagem de conteúdo ilegal ou em desacordo com o código de ética dos servidores do Tribunal;

22.5 adulteração de dados referentes à origem da mensagem nos campos de controle de cabeçalho;

22.6 propagação deliberada de qualquer tipo de artefato malicioso (*malware*), a exemplo de vírus, *worm*, *backdoor* ou cavalo de tróia;

22.7 propagação deliberada de mecanismo que provoque congestionamento da infraestrutura de serviços digitais do TCU, sobrecarga ou indisponibilidade de serviço;

22.8 propagação deliberada de mensagens em massa (*spam*);

22.9 promoção ou facilitação deliberada de ataque à infraestrutura de serviços digitais do TCU ou rede externa;

22.10 implementar mecanismos de reencaminhamento automático de mensagens sem autorização do responsável pela caixa original do TCU ou para caixas externas;

22.11 compartilhamento indevido de credenciais de acesso; e

22.12 envio ou armazenamento de mensagem em desacordo com as normas de segurança estabelecidas pela PCSI/TCU.

23. Na aplicação do disposto no item 22, considera-se armazenada a mensagem aberta e mantida na caixa postal.

24. Aplica-se o disposto no item 22 ao conteúdo gerado em plataforma de colaboração e mensageria.

25. A inobservância aos dispositivos do item 22 pode acarretar, isolada ou cumulativamente, e nos termos da legislação aplicável:

25.1 limitação do uso do serviço de correio eletrônico do TCU, mediante autorização do comitê de segurança da informação do Tribunal, na qual constará o prazo de duração da medida; e

25.2 outras sanções administrativas, civis e penais.

26. Aplica-se o disposto no item 25 ao conteúdo gerado em plataforma de colaboração e mensageria.

27. A liberação do uso do serviço de correio eletrônico, após a limitação de que trata o subitem 25.1, será realizada pela unidade responsável pelo serviço de correio eletrônico até o primeiro dia útil após:

27.1 o prazo constante no ato que autorizou a limitação; e

27.2 ciência de determinação expressa do comitê de segurança da informação do Tribunal.

28. Incumbe à unidade responsável pela segurança da informação, em consonância com o disposto na Portaria-TCU nº 28, de 1º de fevereiro de 2021, monitorar e avaliar periodicamente as práticas de segurança da informação relativas às regras estabelecidas neste Anexo, e propor ao comitê responsável pela segurança da informação os ajustes que considerar necessários.

29. A violação ou a inobservância aos dispositivos deste anexo poderá ser considerada incidente de segurança da informação, e poderá implicar, isolada ou cumulativamente, em sanções previstas na

PCSI/TCU, bem como civis e penais, nos termos da legislação pertinente, assegurados aos envolvidos o contraditório e a ampla defesa.

30. O presente anexo utilizará o Glossário de Termos da PCSI/TCU, constante no Anexo I, para promover compreensão comum e consistente de conceitos em função da natureza específica do tema.

31. Os casos omissos serão analisados conjuntamente pela unidade responsável pelo serviço de correio eletrônico e pela área de segurança da informação, e dirimidos pelo comitê de segurança da informação.

32. Ficam a unidade responsável pela segurança da informação e a responsável pelo serviço de correio eletrônico autorizadas, no âmbito de suas respectivas competências, a editar os atos que se fizerem necessários para a operacionalização deste Anexo.

33. Os atos a que se refere o item 32 devem ser submetidos previamente ao exame do comitê responsável pela segurança da informação.

ANEXO IX DA PORTARIA-TCU Nº 89, DE 20 DE ABRIL DE 2023

PROCESSO DE GESTÃO DE VULNERABILIDADES (GV) DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO DO TCU.

1. O processo de gestão de vulnerabilidades de ativos de tecnologia da informação do Tribunal de Contas da União (processo de GV) obedece ao disposto neste anexo.

DOS OBJETIVOS E DIRETRIZES

2. O processo de GV apresenta os seguintes objetivos:

2.1 reduzir os riscos de segurança a que estão expostos os ativos de TI do Tribunal;

2.2 minimizar os riscos de indisponibilidade dos serviços de TI e de comprometimento dos níveis de serviço acordados;

2.3 induzir o correto e o tempestivo tratamento das vulnerabilidades encontradas nos serviços digitais do TCU, de modo a mitigar os riscos associados; e

2.4 subsidiar a implementação de controles de segurança aplicados aos ativos de TI.

3. São diretrizes do processo de GV:

3.1 priorização do tratamento de vulnerabilidades mais severas, preferencialmente pela correção;

3.2 conscientização dos responsáveis pelos ativos de TI acerca da importância de manter tais ativos atualizados e configurados de modo a tratar as vulnerabilidades e minimizar riscos;

3.3 ciência aos devidos responsáveis acerca de vulnerabilidades encontradas;

3.4 automatização da identificação periódica e do tratamento de vulnerabilidades;

3.5 tratamento proativo de vulnerabilidades existentes, mitigando riscos de exploração;

3.6 envolvimento de responsáveis pelos ativos de TI, bem como de unidades responsáveis pela detecção, comunicação e tratamento de vulnerabilidades;

3.7 identificação de vulnerabilidade prévia à entrada em produção de novos ativos de TI; e

3.8 busca de eficiência no tratamento de vulnerabilidades.

DO PROCESSO DE GV

4. O processo de GV tem caráter cíclico e contínuo e compreende as seguintes etapas:

4.1 gestão dos ativos de TI;

4.2 identificação de vulnerabilidades;

4.3 notificação de vulnerabilidades;

4.4 tratamento de vulnerabilidades; e

4.5 monitoramento de vulnerabilidades.

5. A gestão de ativos de TI consiste na manutenção da lista de ativos a ser periodicamente verificada em busca de vulnerabilidades e na configuração dos parâmetros de identificação.

6. É fator crítico para o sucesso do processo de GV, a definição de responsáveis por ativos de TI, para servirem de ponto de comunicação com objetivo de facilitar a identificação, notificação e o tratamento das vulnerabilidades.

7. A identificação de vulnerabilidades consiste no levantamento de vulnerabilidades realizado sob demanda ou periodicamente em ativos de TI, priorizando os de maior criticidade.

8. Serviços externos de verificação de segurança de serviços digitais do TCU podem ser contratados, de forma complementar aos procedimentos de identificação de vulnerabilidades, os quais serão acompanhados pela unidade de TI responsável.

9. A notificação de vulnerabilidade compreende a comunicação das vulnerabilidades encontradas aos responsáveis pelos respectivos ativos de TI.

10. O tratamento de vulnerabilidades compreende a correção ou a aceitação das vulnerabilidades encontradas.

11. Vulnerabilidades críticas serão processadas em rito específico com maior prioridade e tratadas como incidente de segurança em TI, nos termos de regulamentação específica.

12. O responsável pelo ativo de TI motivará casos de aceitação de vulnerabilidades encontradas e, sempre que viável, implantará controles compensatórios, que serão avaliados pela unidade de TI responsável.

13. O monitoramento de vulnerabilidades compreende medição, análise e avaliação de resultados a fim de verificar a efetividade do processo de GV, bem como de identificar oportunidades de melhoria.

14. A execução de partes ou da totalidade do monitoramento será preferencialmente automatizada pelo responsável do processo de GV.

DAS RESPONSABILIDADES

15. No âmbito de suas respectivas competências, as unidades provedoras de TI do Tribunal de Contas da União são responsáveis por:

15.1 executar o processo de GV;

15.2 gerenciar e assegurar a identificação periódica de vulnerabilidades em ativos de TI;

15.3 consolidar a lista de ativos de TI a ser periodicamente verificadas em busca de vulnerabilidades;

15.4 comunicar os responsáveis sobre as respectivas vulnerabilidades encontradas;

15.5 manter disponível documentação atualizada do processo em local acessível pelos interessados;

15.6 receber e avaliar propostas de melhorias no processo;

15.7 verificar se as áreas estão atuando conforme definido no processo; e

15.8 levantar e divulgar indicadores do processo.

16. A unidade de coordenação de segurança da informação do TCU deverá:

16.1 formular proposta de revisão da política de modo a atualizá-la frente a novos requisitos corporativos;

16.2 colaborar com as unidades responsáveis pelo processo de GV para alcance de resultados nas diferentes etapas elencadas no item 4, bem como em assuntos diversos relacionados à temática deste anexo;

16.3 apoiar planejamento e priorização de ações com vistas a minimizar vulnerabilidades;

16.4 fomentar ações de conscientização relacionadas à necessidade de minimizar vulnerabilidades; e

16.5 acompanhar e sugerir melhorias na definição de critérios de monitoramento de vulnerabilidades.

17. Compete aos responsáveis por ativos de TI:

17.1 informar às unidades responsáveis pelo processo de GV a lista de ativos de TI sob sua responsabilidade a serem verificados periodicamente em busca de vulnerabilidades, bem como mantê-la atualizada;

17.2 tratar tempestivamente vulnerabilidades detectadas em ativos sob sua responsabilidade, priorizando os ativos de maior criticidade e as vulnerabilidades de maior severidade;

17.3 assegurar existência de processos de instalação de atualizações de segurança e validar que atualizações sejam aplicadas tempestivamente;

17.4 conceder permissões de acesso aos ativos sob sua responsabilidade para permitir a efetiva identificação periódica de vulnerabilidades;

17.5 gerenciar contas administrativas locais caso sejam necessárias para o procedimento de identificação de vulnerabilidades;

17.6 colaborar para o tratamento de incidentes de segurança e de análise de vulnerabilidades;

17.7 reportar incidentes de segurança que tiver conhecimento;

17.8 aderir a boas práticas de configuração ou de desenvolvimento seguro de ativos de TI sob sua responsabilidade, bem como as orientações das unidades provedoras de TI responsáveis sobre o assunto; e

17.9 configurar soluções de segurança aplicáveis localmente nos recursos administrados, se aplicáveis.

18. A responsabilidade de que trata o item 17 estende-se a componentes de sistemas e de integração, cabendo as mesmas tratativas e conforme o caso concreto.

19. As aplicações de atualização de segurança serão efetuadas, preferencialmente, de forma automática.

20. A aplicação manual poderá ser realizada em caráter excepcional, se houver risco de indisponibilidade, mediante comunicação prévia à unidade provedoras de TI responsável, sendo realizada em intervalo máximo de 01 (um) mês.

21. A atualização de ativos de TI de que trata o subitem 17.3, estende-se à atualização decorrente de descontinuidade de suporte do fabricante ou de final de ciclo de vida da versão.

DAS DISPOSIÇÕES FINAIS

22. O presente anexo utilizará o Glossário de Termos da PCSI/TCU, constante no Anexo I, para promover uma compreensão comum e consistente de conceitos em função da natureza específica do tema.

23. Os casos omissos serão decididos conjuntamente pelas unidades responsáveis pela segurança da informação institucional, e pela segurança em TI tanto em infraestrutura como em desenvolvimento.

ANEXO X DA PORTARIA-TCU Nº 89, DE 20 DE ABRIL DE 2023 >>

PROCESSO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA NA REDE DO TRIBUNAL DE CONTAS DA UNIÃO.

DO PROCESSO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO NA REDE TCU

1. O Processo de Tratamento de Incidentes de Segurança na Rede Tribunal de Contas da União, observará o disposto neste Anexo.

2. O processo de tratamento de incidentes seguirá as seguintes etapas:

2.1 preparação: estabelece ações para que o TCU tenha equipe, processos, canais de comunicação, ferramentas e ambientes preparados para tratar incidentes de segurança;

2.2 detecção e análise: determinação de quando o incidente ocorreu, priorização do tratamento do incidente com base em critérios relevantes e compartilhamento do ocorrido com as partes interessadas internas e externas;

2.3 contenção: tentativa de mitigar a ameaça o mais breve possível, com objetivo de evitar e/ou minimizar qualquer dano adicional;

2.4 erradicação: Identificação e mitigação das vulnerabilidades exploradas, com remoção de *malwares*, conteúdos inapropriados e outros componentes do incidente;

2.5 recuperação: uma vez que o incidente de segurança tenha sido contido e as vulnerabilidades tenham sido mitigadas, é realizado recuperação dos recursos de TI afetados, confirmando que tais recursos estão funcionando normalmente, bem como implementação de controles adicionais para identificação e monitoramento mais tempestivos de incidentes futuros; e

2.6 pós-incidente: avaliação do processo de tratamento de incidentes de segurança, com verificação da eficácia das soluções adotadas e das decisões tomadas acerca do incidente, a fim de identificar oportunidades de melhorias.

3. Em todas as fases do processo de tratamento de incidentes serão obtidas, preservadas, protegidas e documentadas as evidências relativas ao incidente.

DA EQUIPE DE TRATAMENTO DE INCIDENTES DE SEGURANÇA NA REDE TCU

4. A Equipe de Tratamento de Incidentes de Segurança na Rede do Tribunal de Contas da União (ETIR-TCU) tem como missão coordenar, centralizar e garantir o tratamento e a resposta a incidentes de segurança em TI da infraestrutura de serviços digitais do TCU, com o objetivo de minimizar impactos que podem comprometer o negócio do TCU.

5. A ETIR-TCU será coordenada pela unidade de Infraestrutura de TI do TCU, unidade responsável pela priorização no atendimento dos incidentes de segurança em TI.

6. A ETIR-TCU atuará de forma compartilhada, composta por integrantes permanentes, respectivos substitutos, bem como temporários, acionados sob demanda, conforme a natureza do incidente suscitado no caso concreto.

7. São competências da ETIR-TCU:

7.1 receber notificações acerca de incidentes de segurança em TI de unidades do TCU e de outras organizações;

7.2 realizar triagem de incidentes de segurança em TI, conforme critérios de priorização e categorização pré-definidos em regulação específica;

7.3 analisar incidentes de segurança em TI para determinar origem, escopo, vulnerabilidades e impactos, bem como pesquisar possíveis estratégias de resposta, erradicação e sanitização do evento;

7.4 responder a incidentes de segurança em TI, provendo recomendações para contenção, recuperação e prevenção;

7.5 notificar responsáveis por ativos de TI, bem como unidades de coordenação do sistema de gestão de segurança da informação e de gestão continuidade de negócio do Tribunal acerca de incidentes de segurança em TI, bem como demais corporações, quando forem parte envolvida ou interessada;

7.6 propor melhorias no processo de tratamento de incidentes de segurança em TI;

7.7 garantir a coleta e a preservação de evidências de incidentes de segurança em TI;

7.8 auxiliar na divulgação de informações relacionadas à segurança da informação;

7.9 comunicar sobre incidentes de segurança da informação em TI às unidades de coordenação do sistema de gestão de segurança da informação e de continuidade de negócio do Tribunal, bem como a comitês de segurança da informação do TCU, conforme critérios a serem definidos em regulação específica, bem como alinhar ações para atuação conjunta conforme o caso;

7.10 comunicar sobre incidentes de segurança da informação às unidades de coordenação do sistema de gestão de segurança da informação e de continuidade de negócio do Tribunal, bem como alinhar ações para atuação conjunta conforme o caso;

7.11 comunicar à unidade de coordenação do sistema de gestão de segurança da informação acerca de necessidade de acionamento ou articulação previstos nos subitens 7.2,7.3 e 7.4; e

7.12 prestar informações relacionadas à sua competência às unidades de coordenação do sistema de gestão de segurança da informação e de continuidade de negócio do Tribunal, bem como a comitês de segurança da informação do TCU.

8. A gestão de incidentes de segurança da informação será coordenada pela unidade responsável pela implantação e funcionamento do sistema de gestão de segurança da informação do Tribunal, conforme regulamentação específica.

9. O presente anexo utilizará o Glossário de Termos da PCSI/TCU, constante no Anexo I, para promover uma compreensão comum e consistente de conceitos em função da natureza específica do tema.

ANEXO XI DA PORTARIA-TCU Nº 89, DE 20 DE ABRIL DE 2023

POLÍTICA E PLANO PARA EXECUÇÃO, GUARDA, MANUTENÇÃO, TESTE E RESTAURAÇÃO DE CÓPIAS DE SEGURANÇA (*BACKUP*) DE INFORMAÇÕES CUSTODIADAS NO AMBIENTE COMPUTACIONAL DO TCU.

1. As regras gerais para execução, guarda, manutenção, teste e restauração de cópias de segurança de informações custodiadas no ambiente computacional do TCU obedecem ao disposto neste anexo.

2. As normas definidas neste anexo não aplicam a informações armazenadas em estações de trabalho.

3. A unidade responsável pela infraestrutura de TI definirá o modelo de contratação da solução de proteção de dados corporativa e será responsável por documentar e manter atualizados os procedimentos operacionais de backup e restauração.

4. O procedimento operacional de backup tem o propósito de permitir a proteção total ou parcial das informações custodiadas pelo Tribunal.

5. Os procedimentos operacionais de backup devem buscar atender aos requisitos de negócio do TCU, em termos de integridade, e criticidade, assim como de tempestividade.

6. O procedimento operacional de restauração tem o propósito de permitir o restabelecimento total ou parcial das informações custodiadas pelo Tribunal, em caso de incidente, desastre, ordem judicial, quando demandado pelo gestor do ativo de TI ou outro evento correlato.

7. A execução regular e sistemática de testes de restauração devem fazer parte dos procedimentos de restauração.

8. A periodicidade de realização dos testes de restauração assim como as informações que serão objeto dos testes serão definidas pelo gestor do ativo de TI em conjunto com a unidade responsável pela infraestrutura de TI.

9. Os procedimentos operacionais de restauração devem buscar atender aos requisitos de negócio do TCU, em termos de integridade, confidencialidade, disponibilidade e criticidade, assim como de tempestividade.

10. O gestor do ativo de TI é o responsável pela verificação, validação e ateste final do resultado do procedimento de restauração.

11. Os procedimentos operacionais de backup e de restauração deverão observar a característica dos dados a serem copiados e serão materializados por meio do plano de backup.

12. O nível de proteção do backup pode variar de acordo com a criticidade do ativo, cuja definição fica a cargo do responsável pelo ativo de TI, quando de seu comissionamento na plataforma de backup.

13. Um backup é considerado suficiente para ativos críticos quando seu ciclo se completa com a cópia feita em disco local, em disco no datacenter de contingência, em fita armazenada em cofre local, em fita armazenada, em cofre off-site e com o teste de *restore* realizado.

14. Um backup é considerado suficiente para ativos de não críticos quando seu ciclo se completa com a cópia feita em disco local, em fita armazenada em cofre local e com o teste de *restore* realizado.

15. Os passos e os elementos descritos nos ciclos de backup podem ser revistos pela unidade responsável pela infraestrutura de TI com vistas à adequação às evoluções tecnológicas.

16. Para informações classificadas como sigilosas ou restritas, as cópias de backup devem ser, preferencialmente, criptografadas.

17. Os parâmetros do plano de backup devem ser definidos pelo gestor do ativo de TI, por meio do preenchimento de formulário de comissionamento próprio, mantido pela unidade responsável pela infraestrutura de TI, sendo de inteira responsabilidade do gestor do ativo de TI a aderência das condições estabelecidas nos procedimentos, definidos no plano, em relação aos requisitos de negócio e aos requisitos legais (regulamentações) da informação custodiada.

18. Em caso de ausência de formulário de comissionamento formalmente preenchido pelo gestor do ativo de TI, a unidade responsável pela infraestrutura de TI fará a proteção por meio do plano de backup padronizado, definido neste Anexo.

19. O gestor do ativo de TI deve manter o plano de backup atualizado, devendo revisar sua efetividade anualmente.

20. O plano de backup padronizado, que deve ser utilizado no caso de ausência de plano específico, deve seguir os seguintes parâmetros:

20.1 definição de seis janelas de backup semanais, cujos horários serão, para todos os fins, de domingo a sexta-feira, entre 20:00 e 08:00, para os backups incrementais e das 20:00 de sexta-feira às 20:00 de domingo, para os *backups full*;

20.2 realização de cópia incremental diária, domingo à quinta-feira, com retenção em disco por quinze dias;

20.3 realização de cópia *full* na janela de sexta-feira, 20:00, com retenção em disco por quinze dias e retenção em fita por seis meses; e

20.4 realização de cópia *full* secundária, em fita, armazenada em cofre off-site, a cada seis meses.

21. Não serão feitas cópias secundárias em disco no ambiente de recuperação de desastres.

22. O CGTI, em expediente próprio, definirá os ativos que, independentemente de manifestação do gestor do ativo de TI, terão proteção especial, com plano de backup diferenciado daquele padronizado.

23. O plano de backup para as proteções especiais deve, preferencialmente, impor a proteção definida no item 16.

24. Em caso de conflito entre os parâmetros definidos pela CGTI e aqueles definidos pelo gestor do ativo de TI, aplicar-se-á aquele mais rigoroso.

25. O tratamento e o armazenamento das mídias de backup obedecerão às seguintes orientações:

25.1 o armazenamento das mídias de *backup*, dentro ou fora do Tribunal, será controlado, mantendo-se relação atualizada das mídias, conteúdos e respectivo local de armazenamento;

25.2 as mídias de *backup* serão acondicionadas e armazenadas em local adequado e com proteção física contra acesso indevido, descargas eletromagnéticas, calor excessivo, incêndio e outras condições ambientais que representem risco à integridade dessas mídias;

25.3 antes da expiração do prazo de validade das mídias de *backup* estabelecido pelo fabricante, as informações nela contidas deverão ser transcritas para uma nova mídia, a fim de zelar pela integridade dos dados;

25.4 as mídias referentes aos *backups* a serem utilizados em situações de desastre serão armazenadas em local seguro e, quando requerido, em prédio distinto do local onde se encontram os dados originais;

25.5 será adotado procedimento de segurança para evitar que pessoa não autorizada tenha acesso às mídias de *backup* e às informações nelas contidas, tanto na geração, quanto no armazenamento e transporte; e

25.6 o descarte sustentável das mídias de *backup* obsoletas ou danificadas deve ser feito de acordo com procedimentos que garantam a eliminação, de forma permanente, de seu conteúdo, com o objetivo de resguardar o sigilo das informações armazenadas.

26. O presente anexo utilizará o Glossário de Termos, constante no Anexo I da PCSI/TCU, para promover uma compreensão comum e consistente de conceitos em função da natureza específica do tema.

27. A unidade responsável pela infraestrutura de TI adotará as medidas necessárias para operacionalizar o disposto neste anexo.

28. Na data de publicação desse normativo, os gestores do ativo de TI devem preencher novo formulário de comissionamento de seus ativos, previsto no item 17, de forma a revisar os planos de proteção definidos.

29. A ausência de preenchimento implicará a aplicação do plano padronizado.

30. Este anexo deverá ser revisto, no máximo, a cada quatro anos.

31. A revisão poderá ocorrer a qualquer tempo, quando houver mudança significativa nos requisitos de segurança da informação que influencie nas atividades relacionados ao backup, de forma a assegurar sua continuidade, sustentabilidade, adequação e efetividade.

32. O comitê responsável pela segurança da informação deverá monitorar e avaliar periodicamente as práticas de segurança da informação relativas às regras estabelecidas neste anexo, e propor os ajustes que considerar necessários.

33. Os casos omissos são analisados pela unidade responsável pela segurança da informação, ouvido o responsável pelo recurso de TI em questão, e dirimidos pelo comitê responsável pela segurança da informação.