PORTARIA Nº 128/2022

(DOC TCE-MT de 15.6.2022 – Ed. 2512)

Aprova as Políticas Complementares de Segurança (PCS): 001; 002; 004; 005; 006; 007; 008; 009 e 010.

O **PRESIDENTE DO TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO**, no uso das atribuições que lhe são conferidas em Lei e no Regimento Interno, e

Considerando a Resolução Normativa nº 8/2022-TP, que alterou a Política de Segurança da Informação (PSI) no âmbito do Tribunal de Contas do Estado de Mato Grosso;

Considerando que as informações geradas internamente ou prestadas ao Tribunal de Contas do Estado de Mato Grosso, quando no exercício de suas competências constitucionais, legais e regulamentares, são patrimônio da Instituição e, portanto, devem ser protegidas e manter-se íntegras;

Considerando a necessidade de normas gerais de segurança da informação, com a finalidade de complementar a Política de Segurança da Informação (PSI);

RESOLVE:

Art. 1º Aprovar as seguintes Políticas Complementares de Segurança (PCS):

PCS Nº 001 – Norma Geral para Acesso Físico e Lógico;

PCS Nº 002 – Norma Geral para Acesso Remoto Externo;

PCS Nº 004 – Contas de Acessos e Senhas – Cofre de Senhas/Barramento de Segurança;

PCS Nº 005 – Correio Eletrônico;

PCS Nº 006 – Recursos Computacionais;

PCS Nº 007 – Utilização da Internet;

PCS Nº 008 – Dispositivos Móveis;

PCS Nº 009 – Data Center; e

PCS Nº 010 – Gestão de Backup.

Art. 2º Esta Portaria entra em vigor a partir da sua publicação, revogando-se todas as disposições em contrário.

Publique-se. Registre-se. Cumpra-se.

Gabinete da Presidência do Tribunal de Contas, em Cuiabá, 14 de junho de 2022.

Conselheiro **JOSÉ CARLOS NOVELLI**
Presidente

TCE-MT	Política Complementar de Segurança NORMA GERAL PARA ACESSO FÍSICO E LÓGICO	Emissão	Classificação Pública
Código: PCS-Nº 001		Versão	Aprovada pelo Presidente do Tribunal

1. Introdução

1.1. A norma de segurança da informação PCS nº 001 complementa a Política de Segurança da Informação (PSI) – Resolução Normativa nº 8/2022-TP, **definindo as diretrizes para o acesso físico e lógico aos ativos/serviços de informação e recursos computacionais** do Tribunal de Contas do Estado de Mato Grosso (TCE-MT).

2. Propósito

2.1. Estabelecer critérios para a disponibilização e administração do acesso físico e lógico aos ativos/serviços de tecnologia da informação, bem como estabelecer critérios relativos às senhas das respectivas contas dos usuários.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação.

4. Diretrizes

4.1. A conta de acesso é o instrumento para identificação do usuário na rede do TCE-MT e se caracteriza por ser de uso individual e intransferível, sua divulgação é vedada sob qualquer hipótese;

4.2. Qualquer utilização, por meio da identificação e da senha de acesso, é de responsabilidade do usuário, ao qual as informações estão vinculadas;

4.3. Todo material, equipamento, “software” ou componente a ser retirado do ambiente do TCE-MT por servidor, prestador de serviços ou pessoas autorizadas deve estar, obrigatoriamente, acompanhado da respectiva autorização para saída de material, assinada por servidor detentor desta função.

5. Acesso físico

5.1. Os controles de acesso físico visam restringir o acesso aos equipamentos, documentos e suprimentos do ambiente tecnológico do TCE-MT, bem como visam à

proteção dos recursos computacionais, permitindo o acesso apenas às pessoas autorizadas;

5.2. Devem ser adotados controles que restrinjam a entrada e saída de visitantes, pessoal interno, equipamentos e mídias, estabelecendo perímetros de segurança e habilitando o acesso apenas a pessoal autorizado. No caso de sistemas críticos, convém que sejam criados ambientes reservados, de uso exclusivo, para abrigá-los;

5.3. Todo o pessoal envolvido em trabalhos de apoio, tal como a manutenção das instalações físicas, deve ser orientado e capacitado para manter a adoção de medidas de proteção ao acesso;

5.4. Todas as pessoas devem portar algum tipo de identificação visível que informe se é um servidor ou não, bem como informe o nível de autorização de acesso;

5.5. O ingresso de visitantes deve ser controlado e acompanhado, de forma a impedir o acesso destes às redes de armazenamento e/ou processamento de informações sensíveis, salvo quando acompanhados e com autorização do responsável;

5.6. Deverão ser adotadas medidas para coleta e armazenamento do registro de ingresso de visitantes;

5.7. Deverão ser criados procedimentos de acesso aos espaços que contenham equipamentos e à sala dos data centers;

5.8. Deverão ser criados procedimentos contra incêndios e outros desastres naturais;

5.9. Toda entrega/movimentação de materiais, inclusive equipamentos e suprimentos, deve ser comunicada, antecipadamente, à área administrativa responsável pelo patrimônio/almoxarifado, com indicação do tipo de material, da unidade a que se destina e do nome do servidor responsável pelo recebimento;

5.10. Todo material, equipamento, “software” ou componente a ser retirado do ambiente do TCE-MT por servidor, prestador de serviços ou pessoas autorizadas deve estar, obrigatoriamente, acompanhado da respectiva autorização para saída de material, assinada por servidor detentor desta função;

5.11. A autorização para saída de materiais ou de equipamentos deve conter, no mínimo, as seguintes informações:

1. Tipo de material ou equipamento e a respectiva quantidade;

2. Nome da unidade responsável pelo material;

3. Nome e assinatura de quem autorizou a saída;

4. Nome, matrícula ou número do documento de identidade e CPF de quem irá retirar o material;

5. Marca, modelo, número de série e, quando houver, número de inventário de

material, ou seja, número de tombamento;

6. Quantidade e tipo dos acessórios que acompanham o equipamento.

6. Acesso Lógico

6.1. Os controles de acesso lógico são um conjunto de procedimentos, recursos e meios, utilizados com a finalidade de prevenir e/ou obstruir ações de qualquer natureza que possam comprometer recursos computacionais, redes corporativas, aplicações e sistemas de informação;

6.2. Os equipamentos servidores conterão apenas serviços estritamente designados a ele e as suas dependências;

6.3. Os “firewalls” devem ser configurados para restringir o tráfego entre as redes públicas e os servidores da empresa de acesso público;

6.4. Os servidores “internet” que provêm serviços de acesso público ou externo com empresas de relacionamento negocial da Instituição devem estar isolados da rede interna e de qualquer rede pública, por meio da utilização de equipamentos de “firewall” e roteadores;

6.5. Os roteadores devem ser configurados para restringir o tráfego entre os servidores da Instituição de acesso público e a rede interna. Somente poderão ser criadas listas de acesso de caráter específico se aprovadas pelo diretor de TI ou pelo responsável pela área;

6.6. Os locais que abrigam meios de comunicação devem ser protegidos para evitar a interceptação e/ou interferência de dados:

6.6.1. Os computadores e sistemas do TCE-MT devem possuir controle de acesso, de modo a assegurar o uso apenas aos usuários ou processos autorizados. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado;

6.6.2. Os sistemas devem ser avaliados com relação aos aspectos de segurança, antes de serem disponibilizados para a produção. As vulnerabilidades do ambiente devem ser avaliadas periodicamente e as recomendações de segurança devem ser adotadas;

6.6.3. O acesso remoto aos recursos computacionais deve ser realizado adotando os mecanismos de segurança definidos para evitar ameaças à integridade e ao sigilo do serviço;

6.6.4. O suporte técnico poderá ter permissão de acesso remoto às estações de trabalho dos usuários de sua unidade quando necessário para proceder suporte aos usuários;

6.6.5. O acesso à rede por meio de Wi-Fi, no âmbito do TCE-MT, é homologado e liberado

conforme autenticação e concessão de autorização;

6.6.6. É de responsabilidade da Secretaria de Tecnologia da Informação (STI), por meio da subsecretaria de infraestrutura e equipe técnica:

6.6.6.1. Avaliar, aprovar ou negar solicitações para uso de acesso a ativos/serviços de informação ou recursos computacionais do Tribunal de Contas do Estado de Mato Grosso (TCE-MT);

6.6.6.2. Tratar eventuais tentativas de acessos não autorizados ou incidentes de segurança relacionados ao acesso e, quando pertinente, reportar os mesmos ao COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO.

7. Sanções e punições

7.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

8. Revisões

8.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

9. Gestão da Norma

9.1. A norma PCS nº 001 é aprovada pela Comissão de Governança de Tecnologia da Informação, em conjunto com o Presidente do Tribunal de Contas do Estado de Mato Grosso (TCE-MT);

9.2. Os casos omissos a esta norma poderão ser tratados pela STI e equipe técnica a ser convocada, devendo as ações e decisões serem reportadas ao Comitê de Governança de Tecnologia da Informação, as quais serão devidamente documentadas para fins de acervo e atualização da norma, se necessário.

TCE-MT	Política Complementar de Segurança NORMA GERAL PARA ACESSO REMOTO EXTERNO	Emissão	Classificação Pública
Código: PCS-Nº 002		Versão	Aprovada pelo Presidente do Tribunal

1. Introdução

1.1. A norma de segurança da informação PCS nº 002 complementa a Política de Segurança da Informação (PSI) – Resolução Normativa nº 8/2022-TP, definindo as diretrizes para o acesso remoto externo aos ativos/serviços de informação e recursos computacionais do Tribunal de Contas do Estado de Mato Grosso (TCE-MT).

2. Propósito

2.1. Estabelecer critérios para a disponibilização do serviço de acesso remoto externo à rede do TCE-MT, bem como às regras para a sua utilização, visando prevenir o acesso não autorizado às informações do TCE-MT.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação.

4. Diretrizes

4.1. O acesso remoto aos serviços corporativos somente deve ser disponibilizado aos membros, servidores, estagiários e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional do TCE-MT e que necessitam deste serviço para execução de suas atividades institucionais, desde que autorizados;

4.2. O acesso remoto de uma rede externa às estações de trabalho e aos servidores do TCE-MT deverá ser rigorosamente controlado e autorizado, utilizando criptografia por uma VPN e autenticação com senha forte;

4.3. As solicitações de acesso remoto aos usuários devem ser realizadas por meio da Central de Serviços, devendo conter justificativa e período de trabalho para que o acesso seja liberado. Essas solicitações devem ser autorizadas pelo gestor da área ou superior e arquivadas, para fins de auditoria;

4.4. A disponibilização do acesso remoto deve ser autorizada pelo gestor da área ou superior em conformidade com o perfil funcional, priorizando o acesso em expediente

regulamentar de trabalho, salvo casos de exceção devidamente justificados;

4.5. Os usuários com acesso remoto autorizado devem garantir a não utilização do seu perfil de acesso remoto por outras pessoas;

4.6. Os usuários com acesso remoto devem cuidar para que informações sigilosas não sejam capturadas por terceiros que estejam próximos ao equipamento;

4.7. O usuário, quando da utilização do acesso remoto, deverá permanecer conectado à rede do TCE-MT apenas enquanto estiver efetivamente usando os serviços disponibilizados, devendo se desconectar nas interrupções e no término do trabalho;

4.8. Os administradores da rede do TCE-MT lotados na Secretaria de Tecnologia da Informação (STI), para o desempenho de suas atribuições, poderão ter permissão de acesso remoto a todos os recursos computacionais do TCE-MT, quando necessário;

4.9. Os representantes de informática, quando administradores de rede das unidades do TCE-MT, poderão ter permissão de acesso aos servidores de rede e estações de trabalho de sua circunscrição, quando necessário;

4.10. A disponibilização de acesso remoto à rede do TCE-MT para outras organizações deve obedecer às seguintes regras:

4.10.1. Direitos de acesso definidos por contrato formal entre as partes;

4.10.2. Acesso temporário e limitado às necessidades de negócio;

4.10.3. Revisão periódica dos direitos de acesso;

4.10.4. Utilização de solução que permita a implementação e controle de regras de acesso.

4.11. O serviço de acesso remoto deve ser cancelado sob as seguintes condições:

4.11.1. Finalização do período especificado na solicitação ou contrato;

4.11.2. Perda da necessidade de utilização do serviço;

4.11.3. Transferência do usuário para outras unidades;

4.11.4. Identificação de vulnerabilidade, risco ou uso indevido no acesso concedido.

4.12. As conexões remotas à rede do TCE-MT devem ocorrer da seguinte maneira:

4.12.1. Utilização de autenticação;

4.12.2. As senhas e as informações que trafegam entre a estação remota e a rede do TCE-MT devem estar criptografadas;

4.12.3. Cada usuário deve manter suas credenciais de acesso (login e senha) em sigilo absoluto, sem fornecê-las a outra pessoa, garantindo, assim, a impossibilidade de acesso indevido por pessoal não autorizado.

4.13. É vedada a utilização do acesso remoto para fins não relacionados às atividades da instituição.

5. Papéis e responsabilidades

5.1. Caberá a STI, por meio da subsecretaria de infraestrutura e equipe técnica:

5.1.1.1. Avaliar, aprovar ou negar solicitações para uso de acesso remoto dos ativos/serviços de informação ou recursos computacionais do Tribunal de Contas do Estado de Mato Grosso (TCE-MT);

5.1.1.2. Tratar eventuais tentativas de acessos não autorizados ou incidentes de segurança relacionados ao acesso e, quando pertinente, reportar os mesmos ao COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO.

6. Sanções e punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma PCS nº 002 é aprovada pela Comissão de Governança de Tecnologia da Informação, em conjunto com o Presidente do Tribunal de Contas do Estado de Mato Grosso (TCE-MT);

8.2. Os casos omissos a esta norma serão tratados pela STI e equipe técnica a ser convocada, devendo as ações e decisões serem reportadas ao Comitê de Governança de Tecnologia da Informação, as quais serão devidamente documentadas para fins de acervo e atualização da norma, se necessário.

TCE-MT	Política Complementar de Segurança CONTAS DE ACESSOS E SENHAS – COFRE DE SENHAS/BARRAMENTO DE SEGURANÇA	Emissão	Classificação Pública
Código: PCS-Nº 004		Versão	Aprovada pelo Presidente do Tribunal

1. Introdução

1.1. A norma de segurança da informação PCS nº 004 complementa a Política de Segurança da Informação (PSI) – Resolução Normativa nº 8/2022-TP, definindo as diretrizes para contas de acesso e senhas.

2. Propósito

2.1. Estabelecer critérios para a disponibilização e administração do acesso aos serviços de tecnologia de informação do TCE-MT, bem como estabelecer critérios relativos às senhas das respectivas contas.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação para contas de acesso e senhas (cofre de senhas/barramento de segurança).

4. Diretrizes

4.1. Criação de Contas de Acesso

4.1.1. Todo cadastramento de conta de acesso à rede e sistemas de informação do TCE-MT deve ser efetuado mediante solicitação formal para Secretaria de Tecnologia da Informação (STI);

4.1.2. Contas de acesso de terceirizados do TCE-MT devem ter prazo de validade máximo igual ao período de vigência do contrato ou período de duração de suas atividades.

4.1.3. As solicitações relativas à criação de conta devem ser mantidas registradas e armazenadas de forma segura pela STI;

4.1.4. Todos os usuários devem assinar um termo de responsabilidade pela utilização da conta de acesso. Esse termo deve ser entregue com a solicitação de criação da conta de acesso;

4.1.5. A chefia imediata da área que pertence o usuário deve ser informada, formalmente, pela STI, a respeito de qualquer evento relacionado a falhas de segurança referentes à

conta do usuário e senha;

4.1.6. Qualquer anormalidade percebida pelo usuário quanto ao privilégio de seu acesso aos recursos de tecnologia da informação deve ser imediatamente comunicada à STI.

4.2. Exclusão e Bloqueio de Contas de Acesso

4.2.1. Toda alteração, mudança ou bloqueio de conta de acesso à rede do TCE-MT deve ser efetuado mediante solicitação formal à STI;

4.2.2. O bloqueio da conta de acesso do usuário deve ser solicitado caso haja:

4.2.2.1. Contas sem utilização por mais de 45 (quarenta e cinco) dias serão bloqueadas;

4.2.2.2. As contas deverão permanecer bloqueadas até que haja nova solicitação formal para desbloqueio;

4.2.3. As contas de serviços utilizadas em servidores de rede, backup, correio eletrônico, banco de dados, aplicações, entre outros, devem ser utilizadas somente para execução de ações ligadas à sua natureza, de forma automática, sem intervenção manual por meio de login/acesso;

4.2.4. As contas com privilégio de administração de rede devem ser utilizadas somente para execução das atividades correspondentes à administração do ambiente, em equipamentos previamente definidos, conforme as responsabilidades atribuídas. As variáveis necessárias para acesso e administração devem ser de conhecimento restrito aos administradores dos equipamentos de rede e à chefia respectiva;

4.2.5. As contas com privilégio de administrador das estações de trabalho (login de administrador), que permitem livre instalação de “softwares”, administração e configuração avançada são ordinariamente concedidas para membros da STI com perfil técnico, para fins de suporte ao usuário.

4.3. Senhas

4.3.1. Todas as senhas de usuários comuns para autenticação na rede do TCE-MT seguirão os seguintes critérios mínimos:

4.3.1.1. A data de expiração da senha deve ser de, no máximo, 180 (cento e oitenta) dias. Caso não seja alterada, a senha será bloqueada;

4.3.1.2. É obrigatória a troca de senha ao efetuar o primeiro login.

4.3.2. Todas as senhas, de administradores locais e administradores de domínio, para autenticação na rede do TCE-MT, devem seguir os seguintes critérios mínimos:

4.3.2.1. Os critérios definidos acima serão auditados pela STI, por meio de ferramentas adequadas;

4.3.2.2. A base de dados de senhas deve ser armazenada com criptografia;

4.3.2.3. O usuário poderá solicitar a alteração de sua senha, caso não se recorde da

mesma, mediante solicitação formal;

4.3.2.4. O armazenamento de senhas de administração local de servidores de aplicação deve ser feito em arquivos criptografados, em local seguro com acesso físico e lógico controlado;

4.3.2.5. Em caso de comprometimento comprovado da segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas.

4.4. Utilização de Contas

4.4.1. A conta de acesso é o instrumento para identificação do usuário na rede do TCE-MT e se caracteriza por ser de uso individual e intransferível, sendo sua divulgação vedada sob qualquer hipótese;

4.4.2. Qualquer utilização, por meio da identificação e da senha de acesso, é de responsabilidade do usuário, ao qual as informações estão vinculadas;

4.4.3. O acesso aos serviços de tecnologia da informação do TCE-MT deve ser disponibilizado aos membros, servidores, estagiários e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional do TCE-MT;

4.4.4. Para fins de auditoria, as contas de administradores locais das estações de trabalho ou de servidores de rede só devem ser utilizadas quando estritamente necessário;

4.4.5. Poderá ser permitido o acesso a serviços básicos de tecnologia da informação do TCE-MT na qualidade de visitante, de acordo com as regras definidas e por prazo certo.

5. Papéis e responsabilidades

5.1. A gestão de pessoas encaminhará à STI solicitação dos acessos;

5.2. É de responsabilidade da Subsecretaria de Infraestrutura a Gerência de Segurança/Gestor de Infraestrutura:

5.2.1.1. Avaliar, aprovar ou negar solicitações para uso de acesso remoto dos ativos/serviços de informação ou recursos computacionais do Tribunal de Contas do Estado de Mato Grosso (TCE-MT);

5.2.1.2. Tratar eventuais tentativas de acessos não autorizados ou incidentes de segurança relacionados ao acesso e, quando pertinente, reportar os mesmos ao COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO.

6. Sanções e punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1. A norma PCS nº 004 é aprovada pela Comissão de Governança de Tecnologia da Informação, em conjunto com o Presidente do Tribunal de Contas do Estado de Mato Grosso (TCE-MT).

8.2. Os casos omissos a esta norma poderão ser tratados pela STI e equipe técnica a ser convocada, devendo as ações e decisões serem reportadas ao Comitê de Governança de Tecnologia da Informação, as quais serão devidamente documentadas para fins de acervo e atualização da norma, se necessário.

TCE-MT	**Política Complementar de Segurança CORREIO ELETRÔNICO**	**Emissão**	**Classificação Pública**
Código: PCS-Nº 005		**Versão**	**Aprovada pelo Presidente do Tribunal**

1. Introdução

1.1. A norma de segurança da informação PCS nº 005 complementa a Política de Segurança da Informação (PSI) – Resolução Normativa nº 8/2022-TP, definindo as diretrizes para o acesso ao correio eletrônico.

2. Propósito

2.1. Definir os requisitos e as regras de segurança para o uso do correio eletrônico (e-mail) no âmbito do TCE-MT.

3. Escopo

3.1. A disponibilização do serviço de correio eletrônico corporativo do TCE-MT aos usuários.

4. Diretrizes Gerais

4.1. O serviço de correio eletrônico tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados às funções institucionais do TCE-MT;

4.2. As mensagens de correio eletrônico devem ser escritas em linguagem profissional que não comprometa a imagem do TCE-MT e que não vá de encontro à legislação vigente e nem aos princípios éticos da organização;

4.3. A nomenclatura de endereços eletrônicos deve obedecer à composição utilizada para designar o login de rede, isto é, o login do usuário, seguido de @tce.mt.gov.br. No caso de terceiros, o login deve ser precedido de caractere que defina a diferença do endereço de e-mail:

4.3.1. É proibida a utilização de apelidos na nomenclatura de endereços eletrônicos;

4.3.2. Os usuários devem remover do correio eletrônico mensagens consideradas desnecessárias para a continuidade de suas atividades.

4.4. Os usuários devem verificar se a origem da mensagem recebida é de fonte fidedigna, a fim de impedir a instalação de arquivos maliciosos. Quando houver alguma suspeita

com relação à mensagem, o usuário deve enviá-la para a Área de Segurança da Informação;

4.5. É proibida a reprodução de qualquer material recebido pelo correio eletrônico, ou por outro meio, que possa infringir direitos autorias, marcas, licenças de software ou patentes, sem que haja permissão por escrito do criador do trabalho;

4.6. Os usuários somente devem encaminhar arquivos anexados por correio eletrônico quando for imprescindível. A relevância desta ação deve ser considerada, principalmente, quando houver usuários externos envolvidos na troca de mensagens;

4.7. Os usuários devem garantir que cada um dos arquivos anexados possuam o seu nível de confidencialidade, de acordo com a PSI – Classificação da Informação e com relação ao(s) destinatário(s) e aos copiados;

4.8. São usuários do serviço de correio eletrônico corporativo os membros e servidores do TCE-MT, seus órgãos e unidades, os estagiários e os demais agentes públicos ou particulares que oficialmente executem atividade vinculada à atuação institucional do TCE-MT;

4.9. A concessão de contas de correio eletrônico depende de pedido fundamentado da autoridade responsável pela respectiva área, demonstrando a necessidade para a Instituição da utilização do serviço pelo agente;

4.10. Os titulares de órgão ou unidade do TCE-MT podem solicitar a criação de listas de distribuição, restritas aos seus respectivos âmbitos de atuação;

4.11. Cada unidade do TCE-MT manterá, no mínimo, uma conta de correio eletrônico destinada a comunicações institucionais;

4.12. É vedado o acesso ao conteúdo das mensagens tramitadas por meio do serviço de correio eletrônico corporativo, salvo nas hipóteses previstas em lei;

4.13. O acesso indevido às informações tramitadas por meio do serviço de correio eletrônico corporativo do TCE-MT, ou contidas em seus ambientes, será punido na forma da lei;

4.14. O acesso ao serviço de correio eletrônico dar-se-á por meio de senha de uso pessoal e intransferível, vedada a sua divulgação;

4.15. É vedado ao usuário o uso do serviço de correio eletrônico corporativo com o objetivo de:

4.15.1. Praticar crimes e infrações de qualquer natureza;

4.15.2. Executar ações nocivas contra outros recursos computacionais do TCE-MT ou de redes externas;

4.15.3. Distribuir material obsceno, pornográfico, ofensivo, preconceituoso,

discriminatório, ou de qualquer forma contrário à lei e aos bons costumes;

4.15.4. Disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo “corrente”, vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções ou que possam ser considerados nocivos ao ambiente de rede do TCE-MT;

4.15.5. Emitir comunicados gerais com caráter eminentemente associativo, sindical ou político-partidário;

4.15.6. Enviar arquivos de áudio, vídeo ou animações, salvo os que tenham relação com as funções institucionais desempenhadas pelo TCE-MT;

4.15.7. Divulgar, no todo ou em parte, os endereços eletrônicos corporativos constantes do catálogo de endereços do serviço;

4.15.8. Executar outras atividades lesivas, tendentes a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema, ou a imagem institucional.

4.16. Compete à STI disponibilizar o serviço de correio eletrônico corporativo, diretamente ou mediante contrato, competindo-lhe, ainda, o seguinte:

4.16.1. Zelar pelo atendimento aos princípios da segurança, integridade, sigilo e disponibilidade dos serviços e dados transmitidos por meio do sistema de correio eletrônico;

4.16.2. Prover os meios tecnológicos necessários à adequada utilização do serviço;

4.16.3. Definir os padrões e requisitos para cadastramento, concessão, utilização e bloqueio das contas de correio eletrônico e listas de distribuição, regulamentado por resolução normativa;

4.16.4. Manter, em local seguro e restrito, dados de auditoria acerca da utilização do serviço, no sentido de garantir a recuperação de mensagens em caso de danos ao ambiente de rede, devidamente comunicado a todos os usuários do serviço;

4.16.5. Suspender motivadamente o acesso a conta de correio eletrônico quando constatado o uso indevido dos recursos, dando imediata ciência ao respectivo titular e ao responsável pela apuração formal;

4.16.6. Manter proteção contra vírus e mensagens não solicitadas (spam) nos servidores do correio eletrônico;

4.16.7. Restringir a transmissão de arquivos que, em tese, possam significar comprometimento do serviço;

4.16.8. Monitorar o uso do ambiente virtual, por meio de ferramentas sistêmicas, a fim de preservar a integridade das informações e identificar possíveis violações ao disposto nesta Norma;

4.16.9. Providenciar, sempre que necessária, a capacitação dos usuários no uso da ferramenta de correio eletrônico.

4.17. É responsabilidade da chefia de cada setor no âmbito do TCE-MT, sempre que houver ocorrências de afastamento ou desligamento de usuários do serviço que importem a necessidade de bloqueio de contas de correio eletrônico, informar tal fato à STI, por meio da ferramenta oficial de abertura de chamados ou comunicação interna, para a revogação dos respectivos acessos às contas de e-mail;

4.18. As contas de e-mail são exclusivas para setores e assuntos institucionais para uso dos servidores ativos em exercício no TCE-MT;

4.19. São vedadas as utilizações de e-mails hospedados em outros provedores (*gmail, hotmail etc*) para tramitar informações e documentos relativos as atividades do TCE-MT;

4.20. Compete à STI e equipe técnica avaliar, aprovar ou negar solicitações para uso de acesso remoto dos ativos/serviços de informação ou recursos computacionais do Tribunal de Contas do Estado de Mato Grosso (TCE-MT);

4.21. Compete à STI e equipe técnica tratar eventuais tentativas de acessos não autorizados ou incidentes de segurança relacionados ao acesso e, quando pertinente, reportar os mesmos ao COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO.

5. Sanções e punições

5.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

6. Revisões

6.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

7. Gestão da Norma

7.1. A norma PCS nº 005 é aprovada pela Comissão de Governança de Tecnologia da Informação, em conjunto com o Presidente do Tribunal de Contas do Estado de Mato Grosso (TCE-MT);

7.2. Os casos omissos a esta norma poderão ser tratados pela STI e equipe técnica a ser convocada, devendo as ações e decisões serem reportadas ao Comitê de Governança de Tecnologia da Informação, as quais serão devidamente documentadas para fins de acervo e atualização da norma, se necessário.

TCE-MT	Política Complementar de Segurança RECURSOS COMPUTACIONAIS	Emissão	Classificação Pública
Código: PCS-Nº 006		Versão	Aprovada pelo Presidente do Tribunal

1. Introdução

1.1. A norma de segurança da informação PCS nº 006 complementa a Política de Segurança da Informação (PSI) – Resolução Normativa nº 8/2022-TP, definindo as diretrizes dos recursos computacionais do Tribunal de Contas do Estado de Mato Grosso.

2. Propósito

2.1. Estabelecer critérios de Segurança da Informação e Uso de Recursos Computacionais implantados no âmbito do Tribunal de Contas do Estado de Mato Grosso (TCE-MT), para proteger ativos da informação de sua propriedade ou sob sua custódia, contra ameaças internas ou externas, deliberadas ou acidentais.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação.

4. Definições

4.1. Para os efeitos desta Política, entende-se por:

4.1.1 Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

4.1.2 Ativo de informação: recurso utilizado na produção, processamento, armazenamento, transmissão e recuperação da informação, incluindo a própria informação, sistemas de informação, locais onde se encontram esses meios e as pessoas que a eles têm acesso;

4.1.3 Área privativa: área reservada e exclusiva para armazenamento de informações de um usuário interno, incluindo sua caixa postal;

4.1.4 Área compartilhada: área reservada para armazenamento e compartilhamento de informações de um grupo de usuários internos;

4.1.5 Caixa postal: área individual de armazenamento de mensagens do correio eletrônico;

4.1.6 Conta: identificador único que permite acesso aos recursos de TI e o gerenciamento do uso desses recursos;

4.1.7 Dispositivos móveis: equipamentos portáteis dotados de capacidade computacional

ou dispositivos removíveis de memória para armazenamento, entre os quais se incluem, mas não se limitando a estes: *notebooks, smartphones, tabletes, pendrives, USB drives, HDs* externos e cartões de memória;

4.1.8 Rede Corporativa: conjunto dos recursos de TI disponíveis no âmbito do TCE-MT que possibilita o acesso aos diversos serviços de tecnologia da informação;

4.1.9 Usuário: pessoa utilizadora dos recursos de TI do TCE-MT;

4.1.10 Usuário interno: servidor, contratado ou conveniado do TCE-MT, que no exercício de suas funções, tenham acesso aos recursos de TI do TCE-MT;

4.1.11 Usuário externo: pessoa física ou jurídica que tenha acesso aos recursos de TI do TCE-MT e que não seja caracterizada como usuário interno.

5. Das atividades permitidas e dos direitos dos usuários internos

5.1 O uso dos recursos de TI do TCE-MT pelos usuários internos, destina-se às atividades relacionadas com suas atribuições funcionais.

5.2 Os recursos de TI deverão ser utilizados respeitando-se os direitos de propriedade intelectual de qualquer pessoa ou empresa.

5.3 Respeitado o disposto na Lei Federal nº 9609, de 19 de fevereiro de 1998, que trata da propriedade intelectual de programa de computador, e ressalvadas as exceções previstas em contratos e convênios, são de propriedade do TCE-MT os programas desenvolvidos para o Tribunal por usuários internos.

5.4 São garantidos aos usuários internos, no exercício de suas funções, após aprovação:

I - ter conta para acesso à rede corporativa;

II - fazer uso legal dos recursos de TI colocados à sua disposição, respeitadas as normas de utilização estabelecidas pelo TCE-MT;

III - ter acesso às informações que lhe são franqueadas nas áreas privativa e compartilhadas com garantia de integridade, disponibilidade e controle de acesso;

IV - ter privacidade das informações armazenadas em sua área privativa;

V - ter acesso aos registros de suas ações (logs) existentes na rede corporativa;

VI - ter acesso remoto à rede corporativa do TCE-MT, utilizando recursos de TI próprios, observados os requisitos de segurança estabelecidos pela Secretaria de Tecnologia da Informação (STI);

VII - solicitar suporte técnico à Coordenadoria de Tecnologia da Informação (CTI).

5.4.1 Usuários contratados e conveniados terão garantidos apenas os recursos necessários às atividades correspondentes à execução do contrato ou convênio.

5.4.2 Sempre que for necessário para atividades de administração dos recursos de TI e

suporte técnico ou nos casos de suspeita de violação de regras, a CTI poderá acessar arquivos de dados privativos ou compartilhados.

6 Das atividades vedadas aos usuários internos

6.1 É vedado o uso dos recursos de TI do TCE-MT para processar, guardar ou encaminhar material de cunho político, não ético, discriminatório, malicioso, obsceno ou ilegal, além de atividades visando:

I - promoção pessoal;

II - venda de produtos ou engajamento em atividades comerciais de qualquer natureza;

III - constrangimento, assédio, calúnia, injúria, difamação, ameaça, ofensa ou agressão;

IV - distribuição voluntária de mensagens não desejadas, como circulares, manifestos políticos, correntes de cartas ou outros sistemas que possam prejudicar o trabalho de terceiros, causar excessivo tráfego na rede ou sobrecarregar os recursos de TI;

V - ocultação de sua identidade quando utilizar os recursos de TI;

VI - acesso não autorizado ou indevido aos recursos de TI;

VII - violação dos sistemas de segurança dos recursos de TI, no que tange à identificação de usuários, senhas de acesso, sistemas de alarme, registro de eventos (log) e demais mecanismos de segurança e restrição de acesso;

VIII - instalação, alteração ou remoção de software sem acompanhamento ou autorização da equipe técnica da CTI.

6.1.1 Para notebooks do TCE-MT, a autorização para instalação, alteração ou remoção de software é decorrente do Termo de Compromisso assinado pelo custodiante que optar pelo uso da senha de administrador.

6.1.2 Entende-se por custodiante o usuário, grupo de trabalho ou área responsável pela manutenção dos requisitos de segurança associados aos ativos da informação sob sua guarda.

7 Das Obrigações dos usuários Internos

7.1 São obrigações de todos os usuários internos:

I - manter em caráter confidencial e intransferível códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves privadas etc.);

II - alterar periodicamente a senha de acesso de acordo com os procedimentos estabelecidos pela STI;

III - zelar por toda e qualquer informação disponível pelos recursos de TI do TCE-MT contra alteração, destruição, divulgação, cópia e acessos não autorizados;

IV - desligar ou bloquear computadores em uso quando houver necessidade de ausentar-se fisicamente do local;

V - fazer manutenção na sua área privativa periodicamente, evitando o acúmulo de informações desnecessárias.

7.1.1 Os servidores do TCE-MT ou à disposição do TCE-MT deverão firmar compromisso com as práticas, responsabilidades e obrigações normativas referentes à Política de Segurança da Informação, conforme Termo de Responsabilização e Sigilo, a ser assinado.

7.1.2 Nos contratos e convênios celebrados com o TCE-MT, os contratados e os conveniados deverão assinar o Termo de Sigilo das Informações, responsabilizando-se por seus funcionários e prestadores de serviços.

8 Das Obrigações da Secretaria de Tecnologia da Informação - STI

8.1 São obrigações da Secretaria de Tecnologia da Informação – STI:

I - manter e monitorar o uso dos recursos de TI disponibilizados sem interrupções, exceto em casos de imprevistos ou manutenção técnica programada;

II - monitorar a observância deste normativo, devendo, em caso de descumprimento, informar à Comissão de Governança e tomar medidas imediatas de restrições de uso dos recursos, de acordo com o disposto nas normas computacionais;

III - implantar autorização ou restrição de acesso às informações do TCE-MT, disponíveis através dos recursos de TI;

IV - autorizar ou restringir o acesso aos recursos de TI;

V - cancelar o acesso aos recursos de TI disponíveis imediatamente após o término do vínculo do usuário interno ou colaborador com o TCE-MT;

VI - gerenciar os privilégios de usuários, as senhas de usuários, os procedimentos de *logon* e de política de troca de senha;

VII - desenvolver, adquirir, manter e auditar os sistemas de informação;

VIII - registrar as ações dos usuários internos na rede corporativa, inclusive o histórico de utilização da internet;

IX - proteger e manter a segurança dos dados armazenados na rede corporativa;

X - realizar a cópia de segurança de dados armazenados em discos de servidores da rede local;

XI - manter atualizadas as configurações necessárias para o acesso externo à rede

corporativa, e orientar os usuários internos e colaboradores sobre seu uso e requisitos de segurança;

XII - orientar sobre a configuração dos recursos de TI do TCE-MT;

XIII - providenciar o Termo de Compromisso e obter a aceitação dos usuários internos com as práticas, responsabilidades e obrigações previstas na Política Corporativa de Segurança da Informação e seus normativos correlatos.

A autorização e a restrição de acesso aos sistemas de informação também incumbem aos gestores dos respectivos sistemas.

8.2 A autorização e a restrição de acesso aos sistemas e rede, incubem aos gestores a comunicação de contratação/desligamento de servidores.

9 Das normas específicas

9.1 As normas especificas quanto aos demais procedimentos de tecnologia serão publicados no formato de Política Complementar de Segurança;

9.2 As políticas complementares deverão obedecer os objetivos, princípios e diretrizes estabelecidos pela Política de Segurança da Informação.

9.3 Os casos omissos a esta norma poderão ser tratados pela STI e equipe técnica a ser convocada, devendo as ações e decisões serem reportadas ao Comitê de Governança de Tecnologia da Informação, as quais serão devidamente documentadas para fins de acervo e atualização da norma, se necessário.

TCE-MT	Política Complementar de Segurança UTILIZAÇÃO DA INTERNET	Emissão	Classificação Pública
Código: PCS-Nº 007		Versão	Aprovada pelo Presidente do Tribunal

1. Introdução

1.1. A norma de segurança da informação PCS nº 007 complementa a Política de Segurança da Informação (PSI) – Resolução Normativa nº 8/2022-TP, definindo as diretrizes para a utilização da internet no âmbito do Tribunal de Contas do Estado de Mato Grosso (TCE-MT).

2. Propósito

2.1. Estabelecer critérios para administração e utilização de acesso aos serviços de internet no âmbito do TCE-MT.

3. Escopo

3.1. Esta norma obedece ao escopo definido na Política de Segurança da Informação para utilização da internet.

4. Diretrizes

4.1. São usuários da internet do TCE-MT os membros, servidores, terceirizados, estagiários e os demais agentes públicos ou particulares que oficialmente executem atividade vinculada à atuação institucional do TCE-MT;

4.2. O acesso à internet deve restringir-se à esfera profissional, com conteúdo relacionado às atividades desempenhadas pelo Órgão, observando-se sempre a conduta compatível com a moralidade administrativa;

4.3. As contas de usuários deverão ter níveis de acesso distintos, conforme a necessidade dos serviços, de acordo com os perfis definidos pela Secretaria de Tecnologia da Informação (STI);

4.4. Cada usuário é responsável pelas ações e acessos realizados por meio da sua conta de acesso;

4.5. Os usuários devem estar capacitados a utilizar os serviços, de modo a garantir a sua utilização adequada;

4.6. É vedado o uso de provedores de acesso externos ou de qualquer outra forma de conexão não autorizada no ambiente do TCE-MT;

4.7. A STI deverá prover o serviço de conexão à internet, implementando mecanismos de segurança adequados;

4.8. Os níveis de acesso à internet do TCE-MT são estabelecidos conforme lotação de função;

4.9. Toda alteração de nível de acesso somente será realizada mediante solicitação formal pela chefia imediata do usuário, contendo a devida justificativa, que será avaliada pela STI, podendo esta solicitação ser negada em caso de risco ou vulnerabilidade à segurança e à integridade da rede do TCE-MT;

4.10. É vedado acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como:

a) Pornografia, pedofilia, preconceitos, vandalismo, anonimato, entre outros;

b) Acessar ou obter na internet arquivos que apresentem vulnerabilidade de segurança ou possam comprometer, de alguma forma, a segurança e a integridade da rede do TCE-MT;

c) Uso de IM (Inst*ant Messenger*) não homologado ou autorizado;

d) Uso recreativo da internet em horário de expediente;

e) Uso de proxy anônimo, ferramentas de alto risco, intrusiva;

f) Acesso a salas de bate-papo (chats), exceto aqueles definidos como ferramenta de trabalho homologada pela STI;

g) Acesso a rádio e TV em tempo real, exceto os canais corporativos como, por exemplo, a TV Escola;

h) Acesso a jogos;

i) Acesso a outros conteúdos notadamente fora do contexto do trabalho desenvolvido;

j) Divulgação de informações confidenciais da instituição por meio de correio eletrônico, grupos ou listas de discussão, sistemas de mensageria ou bate-papo, blogs, microblogs, ou ferramentas semelhantes;

k) Envio a destino externo de qualquer software licenciado ao TCE-MT ou dados de sua propriedade ou de seus usuários, salvo expressa e fundada autorização do responsável pela sua guarda;

l) Contorno ou tentativa de contorno às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas do TCE-MT;

m) Utilização de softwares de compartilhamento de conteúdos na modalidade *peer-to-peer* (P2P);

n) Tráfego de quaisquer outros dados em desacordo com a lei ou capazes de

prejudicar o desempenho dos serviços de tecnologia da informação do TCE-MT, na forma definida pela STI.

4.11. O usuário poderá solicitar a liberação de determinada página, com a devida justificada, mediante solicitação formal à STI;

4.12. Somente serão liberadas as páginas analisadas e autorizadas pela STI;

4.13. A ocorrência de qualquer hipótese de má utilização da internet deverá ser comunicada, de imediato, à STI;

4.14. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a Instituição, em total conformidade legal, reserva-se o direito de monitorar e registrar todas as informações inerentes a ela;

4.15. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será desinstalado e excluído pela área de TI.

5. Sanções e punições

5.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

6. Revisões

6.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

7. Gestão da Norma

7.1. A norma PCS nº 007 é aprovada pela Comissão de Governança de Tecnologia da Informação, em conjunto com o Presidente do Tribunal de Contas do Estado de Mato Grosso (TCE-MT).

7.2. Os casos omissos a esta norma poderão ser tratados pela STI e equipe técnica a ser convocada, devendo as ações e decisões serem reportadas ao Comitê de Governança de Tecnologia da Informação, as quais serão devidamente documentadas para fins de acervo e atualização da norma, se necessário.

TCE-MT	Política Complementar de Segurança DISPOSITIVOS MÓVEIS	Emissão	Classificação Pública
Código: PCS-Nº 008		Versão	Aprovada pelo Presidente do Tribunal

1. Introdução

1.1. A norma de segurança da informação PCS nº 008 complementa a Política de Segurança da Informação (PSI) – Resolução Normativa nº 8/2022-TP, definindo as diretrizes para acesso de dispositivos móveis disponibilizados para uso funcional, no âmbito do Tribunal de Contas do Estado de Mato Grosso (TCE-MT).

2. Propósito

2.1. Estabelecer critérios para a disponibilização e administração do acesso aos serviços de tecnologia de informação do TCE-MT assim como estabelecer critérios relativos a utilização dos dispositivos móveis.

3. Escopo

3.1. O TCE-MT deseja facilitar a mobilidade e o fluxo de informação entre seus servidores, comissionados, estagiários, terceirizados e prestadores de serviço. Por isso, permite que eles utilizem os equipamentos portáteis.

4. Diretrizes Gerais

4.1. Dispositivos Móveis em Geral

4.1.1. Quando se descreve “dispositivo móvel” se entende qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua STI, como: notebooks, smartphones, *pendrives, tablet, hd* externo entre outros dispositivos móveis;

4.1.2. Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os servidores, comissionados, estagiários, terceirizados e prestadores de serviço que utilizem tais equipamentos;

4.1.3. O TCE-MT, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

4.1.4. O servidor, comissionado, estagiário, terceirizado e prestador de serviço, portanto,

assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções no TCE-MT, mesmo depois de terminado o vínculo contratual mantido com a instituição;

4.1.5. O suporte técnico aos dispositivos móveis de propriedade do TCE-MT e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição;

4.1.6. Todo servidor, comissionado, estagiário, terceirizado e prestador de serviço deverá utilizar senhas de bloqueio automático para seu dispositivo móvel;

4.1.7. Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável, e sem a condução, auxílio ou presença de um técnico da STI;

4.1.8. O servidor, comissionado, estagiário, terceirizado e prestador de serviço deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da STI do TCE-MT;

4.1.9. A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante;

4.1.10. É permitido o uso de rede banda larga de locais conhecidos pelo servidor, comissionado, estagiário, terceirizado e prestador de serviço como: sua casa, hotéis, fornecedores e clientes;

4.1.11. É de responsabilidade do servidor, comissionado, estagiário, terceirizado e prestador de serviço, no caso de furto ou roubo de um dispositivo móvel fornecido pelo TCE-MT, notificar imediatamente seu gestor direto e a STI, também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO);

4.1.12. O servidor, comissionado, estagiário, terceirizado e prestador de serviço deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar ao TCE-MT e/ou a terceiros;

4.1.13. O servidor, comissionado, estagiário, terceirizado e prestador de serviço que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede do TCE-MT deverá submeter previamente tais equipamentos ao processo de autorização da STI;

4.1.14. A norma PCS nº 008 é aprovada pela Comissão de Governança de Tecnologia da

Informação, em conjunto com o Presidente do Tribunal de Contas do Estado de Mato Grosso.

4.1.15. Os casos omissos a esta norma poderão ser tratados pela STI e equipe técnica a ser convocada, devendo as ações e decisões serem reportadas ao Comitê de Governança de Tecnologia da Informação, as quais serão devidamente documentadas para fins de acervo e atualização da norma, se necessário.

TCE-MT	Política Complementar de Segurança UTILIZAÇÃO DO DATA CENTER	Emissão	Classificação Pública
Código: PCS-Nº 009		Versão	Aprovada pelo Presidente do Tribunal

1. Introdução

1.1. A norma de segurança da informação PCS Nº 009 complementa a Política de Segurança da Informação (PSI) – Resolução Normativa nº 8/2022-TP, definindo as diretrizes para o data center no âmbito do Tribunal de Contas do Estado de Mato Grosso (TCE-MT).

2. Propósito

2.1. Dispõe sobre as orientações, as regras e as responsabilidades mandatórias associadas à disciplina e a utilização do Data Center do TCE-MT.

2.2. Data Center é o ambiente projetado onde se localizam equipamentos de armazenamento e processamento de dados do TCE-MT. Projetados com alto nível de segurança, para abrigar servidores e bancos de dados, demandando grande quantidade de informação.

3. Diretrizes Gerais

3.1. Datacenter em Geral

3.1.1. Os controles de acesso físico visam restringir o acesso aos equipamentos de Tecnologia da Informação;

3.1.2. O acesso ao Datacenter somente poderá ser feito por pessoas autorizadas;

3.1.3. O controle de acesso deverá ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão magnético entre outros;

3.1.4. O usuário “administrador” do sistema de autenticação forte ficará de posse e administração do coordenador de infraestrutura, de acordo com o Procedimento de Controle de Contas Administrativas;

3.1.5. Deverá ser executada e registrada semanalmente e/ou quinzenalmente checagem preventiva nos acessos, iluminação, refrigeração, grupo gerador, nobreaks etc., com objetivo de manter o ambiente sempre ativo e seguro.

3.1.6. A chave de alimentação de energia elétrica do data center deverá ser sinalizada e independente do quadro geral de energia elétrica, com o objetivo de evitar o desligamento errôneo do data center e dos equipamentos.

3.1.7. A utilização dos recursos deve ser monitorada e sincronizada e as projeções devem ser feitas para necessidades de capacidade futura, para garantir o desempenho requerido dos Sistemas de Informação Corporativa.

3.1.8. Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança.

3.1.9. Os procedimentos de operação e rotina devem ser documentados, mantidos atualizados e disponíveis a todos os que deles necessitem.

3.1.10. Não são permitidos programas não licenciados ou que infrinjam as leis nacionais ou que coloquem em risco a integridade da rede pela introdução de vírus passiva ou ativa ou incursões destrutivas de hackers e demais invasores, bem como façam valer a propagação de pirataria ou quaisquer técnicas consideradas ilegais.

3.1.11. A lista de funções com direito de acesso ao Datacenter deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao Datacenter, e salva no diretório de rede;

3.1.12. No local em que não existam servidores, comissionados e terceirizados da área de tecnologia da informação, pessoas de outros departamentos deverão ser cadastradas no sistema de acesso para que possam exercer as atividades operacionais dentro do Datacenter, como: troca de fitas de backup, suporte em eventuais problemas, e assim por diante;

3.1.13. O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado, que deverá preencher a solicitação de acesso prevista no Procedimento de Controle de Acesso ao Datacenter, bem como assinar o Termo de Responsabilidade;

3.1.14. O acesso ao Datacenter, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando;

3.1.15. Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer servidor ou comissionado responsável pela administração de liberação de acesso, conforme lista salva em Procedimento de Controle de Acesso ao Datacenter;

3.1.16. O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais;

3.1.17. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável;

3.1.18. No caso de desligamento dos servidores, comissionados ou terceirizados que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de colaboradores autorizados, de acordo com o processo definido no Procedimento de Controle de Acesso ao Datacenter;

3.1.19. A entrada ou retirada de qualquer equipamento dos Data Centers se dará com o preenchimento da solicitação de liberação e autorização formal deste instrumento pelo Secretário da STI ou Subsecretário de Infraestrutura, de acordo com os termos do procedimento e controle de transferência patrimonial;

3.1.20. Todo o cabeamento e equipamentos que estiverem nas dependências dos Data Centers, além de identificados, devem ser documentados para o correto gerenciamento das conexões;

3.1.21. Os Data Centers devem ser dotados de um sistema de geração de energia elétrica em *standby* (com redundância) com nobreaks, geradores e baterias, capazes de fornecer energia elétrica de qualidade e suprir toda a necessidade dos Data Centers em caso de falha no fornecimento externo de energia;

3.1.22. No ambiente de geração de energia elétrica *standby* (com redundância) haverá:

3.1.22.1. Adequada refrigeração, evitando assim a sobrecarga térmica e desligamento dos equipamentos.

3.1.22.2. Uso de diesel nos geradores, dado que a sua combustão é mais rápida que o gás.

3.1.22.3. Controles do armazenamento de combustível, onde o reabastecimento dos geradores deve ser monitorado, a fim de que não ocorram falhas.

3.1.22.4. Sistema de nobreaks em módulos individuais ou em grupos paralelos com um sistema de baterias que pode ser fornecido para cada módulo ou para um grupo de módulos.

3.1.23. Os geradores devem estar configurados para fornecer a tensão e corrente adequadas para os sistemas nobreaks;

3.1.24. Os sistemas geradores deverão ter a capacidade mínima de fornecimento de energia de 5 a 30 minutos, devido a eventos imprevisíveis, que possam ocasionar falhas nos geradores;

3.1.25. A estrutura dos geradores deve possuir um sistema de monitoramento capaz de identificar a capacidade atual de armazenamento das baterias e gravar as tensões, impedância, ou resistência que passam para o sistema de UPS;

3.1.26. Os Data Centers devem conter mecanismos de prevenção e combate a incêndios com vistas a evitar e prevenir que os equipamentos sejam danificados:

3.1.26.1. O sistema de combate e prevenção contra incêndios deve ser composto por sistema de detecção de fumaça e extintores, gases inibidores e procedimentos de brigada de incêndio.

3.1.27. Sempre que houver possibilidade financeira e administrativa, os Data Centers deverão estar protegidos por um sistema contra descargas atmosféricas (para-raios) os quais possuam sistema de aterramento eficiente, observando-se o seguinte:

3.1.27.1. Todo sistema de proteção deve receber manutenção preventiva e inspeção anualmente;

3.1.27.2. O projeto, instalação e manutenção do sistema devem estar em conformidade com a norma NBR-5419-2000;

3.1.27.3. A função do para-raios é proteger edificações e pessoas, não abrangendo necessariamente equipamentos eletroeletrônicos; e

3.1.27.4. Recomenda-se a utilização de protetores para os equipamentos considerados essenciais;

3.1.27.5. Para o grupo-gerador e nobreaks, convém que seja firmado um contrato de manutenção para que as peças e componentes do sistema estejam sempre em perfeito estado e de acordo com as recomendações do fabricante.

3.1.28. As salas de Data Centers devem possuir iluminação de emergência e interruptores elétricos de emergência que permitam o desligamento em caso de necessidade.

4.Sanções e punições

4.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

5. Revisões

5.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

6. Gestão da Norma.

6.1 A norma PCS nº 009 é aprovada pela Comissão de Governança de Tecnologia da Informação, em conjunto com o Presidente do Tribunal de Contas do Estado de Mato Grosso (TCE-MT).

6.2 Os casos omissos a esta norma poderão ser tratados pela STI e Equipe técnica a ser

convocada, devendo as ações e decisões serem reportadas ao Comitê de Governança de Tecnologia da Informação, as quais serão devidamente documentadas para fins de acervo e atualização da norma, se necessário.

TCE-MT	Política Complementar de Segurança GESTÃO DE BACKUP	Emissão	Classificação Pública
Código: PCS-Nº 010		Versão	Aprovada pelo Presidente do Tribunal

1. Introdução

1.1. A norma de segurança da informação PCS nº 010 complementa a Política de Segurança da Informação (PSI) - Resolução Normativa nº 8/2022-TP, definindo as diretrizes para a gestão de backup no âmbito do Tribunal de Contas do Estado de Mato Grosso (TCE-MT).

2. Propósito

2.1. Prover orientações e diretrizes de segurança, visando assegurar a disponibilidade da informação, através de cópias de segurança, nomeadas por backup corporativo, para que, nos casos de perda de dados, desastre, erro de arquivos, falhas de mídia, entre outros incidentes, estes arquivos e/ou sistemas possam ser recuperados e disponibilizados aos usuários.

3. Escopo

3.1. Principal objetivo é a cópia de dados para restauração em caso de perda, alteração não autorizada ou dano a algum tipo de arquivo ou sistema digital.

4.Diretrizes Gerais

4.1. Armazenamento, Retenção e Transporte

4.1.1. Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática;

4.1.2. Deverá ser considerado para a execução das rotinas de Backup o seu impacto sobre o desempenho da rede computacional, garantindo que o tráfego necessário para tal evite a indisponibilidade dos demais sistemas da Instituição em horário de expediente.

4.1.3. Os responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros;

4.1.4. O armazenamento de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de checar espaço utilizado e integridade dos backups.

4.1.5. A escolha das unidades de armazenamento utilizadas na salvaguarda dos dados deverá atender as seguintes características dos dados resguardados:

4.1.5.1. A criticidade;

4.1.5.2. O tempo de retenção;

4.1.5.3. A probabilidade de necessidade de restauração;

4.1.5.4. O tempo esperado para restauração;

4.1.5.5. O custo de aquisição da unidade de armazenamento de backup;

4.1.5.6. A vida útil da unidade de armazenamento de backup.

4.1.6. Deverá ser identificada a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada cenário.

4.1.7. As mídias e discos de armazenamento que apresentarem erros devem ser descartados e substituídas por novas.

4.1.8. Na situação de erro de backup é necessário que ele seja refeito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema;

4.1.9. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Procedimento de Controle de Backup;

4.1.10. Quaisquer atrasos na execução de backup deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento.

4.1.11. Para formalizar o controle de execução de backups, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo coordenador de infraestrutura, nos termos do Procedimento de Controle de Backup;

4.1.12. Os servidores, comissionados, estagiários, terceirizados e prestadores de serviço responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

4.1.13. A periodicidade com a qual são realizadas as cópias de segurança devem ser definidas de acordo com o grau de importância da mesma, dos sistemas operacionais ou aplicativos;

4.1.14. O período de retenção das cópias de segurança deve ser acordado com o Gestor da Informação, respeitados os preceitos legais para o tipo de dado envolvido

4.1.15. A cópia de segurança completa será composta pelo backup full, mais seus complementos, realizados nos períodos definidos com o Gestor da Informação;

4.1.16. A cópia de segurança específica para uma recuperação de desastre deve levar em consideração os sistemas operacionais, aplicações e dados que possibilitem uma completa recuperação da aplicação;

4.1.17. Em caso de desastre, faz-se necessário que a infraestrutura disponibilizada em local de contingência tenha as mesmas características e configurações que o local original;

4.1.18. Regularmente, o backup deverá ser testado e analisado para garantir a confiabilidade, integridade e disponibilidade nos casos de uso emergencial e aderente aos requisitos necessários à recuperação;

4.1.19. Os testes de restauração dos backups deverão ser realizados em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis;

4.1.20. Os novos projetos ou novas aquisições devem seguir os padrões estabelecidos nesta política;

4.1.21. As unidades de armazenamento consideradas inservíveis ou defeituosas deverão passar por procedimentos que impossibilitem a recuperação de dados por terceiros, devendo o descarte ser registrado;

4.1.22. As implementações para o ambiente tecnológico existente deverão ser adequadas a esta política no prazo de 01 (um) ano, a partir de sua publicação;

4.1.23. Caso não seja possível a adequação do recurso técnico ou do processo, a STI deverá documentar essa informação, bem como seus motivos, para fins de auditoria;

4.1.24. A restauração de arquivos terá um prazo máximo de 30 (trinta) dias corridos para os backups diários e de até 60 (sessenta) meses para os backups mensais, em dias alternativos um em cada mês, não sendo possível recuperar arquivos mais antigos que esse período;

4.1.25. É de responsabilidade de cada usuário o armazenamento dos arquivos inerentes ao seu departamento no servidor de arquivos para garantir o backup dos mesmos;

4.1.26. É dever do usuário, a manutenção no diretório que tem acesso, mantendo organizado, evitando acúmulo de arquivos e duplicadas;

4.1.27. Haverá limpeza periódica dos arquivos de rede armazenados na pasta “Lixeira” e “Pública”, para que não haja acúmulo desnecessário de arquivos e de recursos computacionais;

4.1.28. Todos os acessos dentro do servidor de arquivos são auditados;

4.1.29. O backup dos servidores deve ser executado sempre às 19h00, salvo casos especiais;

4.1.30. A periodicidade normal do backup deve seguir a seguinte tabela:

- Diário – de 2ª a 5ª-Feira a partir das 19h00.
- Semanal – 6ª a partir das 22h00.
- Mensal – antes do fechamento mensal, a partir das 22h00.
- Anual – antes do último fechamento mensal do ano.

5. São atribuições dos responsáveis pela execução e gestão das rotinas de backup e restauração

5.1. Planejar os recursos necessários para implantar a política e os planos de backup e restauração;

5.2. Propor soluções de cópia de segurança das informações produzidas ou custodiadas pelo TCE-MT;

5.3. Providenciar a criação e manutenção das cópias de segurança;

5.4. Configurar as soluções de backup;

5.5. Manter as unidades de armazenamento de backups funcionais, preservadas e seguras;

5.6. Solicitar suporte de terceiros em caso de falha nas unidades de armazenamento;

5.7. Elaborar o Plano de backup e restauração específico;

5.8. Verificar periodicamente os eventos gerados pela solução de backup, tomando as providências necessárias para remediação de eventuais falhas;

5.9. Tomar medidas preventivas para evitar falhas;

5.10. Reportar imediatamente os incidentes ou erros que causem indisponibilidade ou que impossibilitem a restauração das cópias de segurança;

5.11. Gerenciar mensagens e registros de auditoria (*LOGs*) dos backups;

5.12. Providenciar a execução dos testes de restauração;

6. Sanções e punições

6.1. Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

7. Revisões

7.1. Esta norma é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

8. Gestão da Norma

8.1 A norma PCS nº 010 é aprovada pela Comissão de Governança de Tecnologia da Informação, em conjunto com o Presidente do Tribunal de Contas do Estado de Mato Grosso (TCE-MT).

8.2 Os casos omissos a esta norma poderão ser tratados pela STI e equipe técnica a ser convocada, devendo as ações e decisões serem reportadas ao Comitê de Governança de Tecnologia da Informação, as quais serão devidamente documentadas para fins de acervo e atualização da norma, se necessário.