TRIBUNAL DE CONTAS DO
ESTADO DE GOIÁS

Comitê de Segurança da Informação

MANUAL DE SEGURANÇA DA INFORMAÇÃO

Versão nº: 003

26/09/2024

SUMÁRIO

1. OBJETIVO

Este manual objetiva instituir diretrizes, responsabilidades e normas específicas de segurança da informação, em consonância com a Resolução Administrativa nº 17/2024, que estabeleceu a Política de Segurança da Informação do TCE-GO. As normas aqui dispostas devem ser observadas e cumpridas por todos os proprietários, gestores e usuários de informações que trafegam na organização, com vistas à garantia da disponibilidade, integridade, confidencialidade e autenticidade dessas informações.

Ainda, em anexo a este Manual, encontra-se a Planilha de Requisitos Legais de Segurança da Informação, a qual identifica os requisitos legais dessa temática aplicáveis ao TCE-GO.

2. DOCUMENTOS DE REFERÊNCIA

- NBR ISO 9001:2015 – Sistema de Gestão da Qualidade
- NBR ISO 14001:2015 – Sistema de Gestão Ambiental
- NBR ISO/IEC 27001:2022 – Sistema de Gestão da Segurança da Informação
- NBR ISO 37001:2017 – Sistema de Gestão Antissuborno
- Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD)
- Resolução Administrativa n.º 001/2014 – Código de Ética do TCE-GO
- Resolução Normativa n.º 010/2017 – Classificação das informações de acordo com grau de confidencialidade
- Resolução Administrativa n.º 17/2024 – Política de Segurança da Informação

3. DEFINIÇÕES

Para fins de uniformidade de entendimento, neste manual são utilizadas as definições estabelecidas pela NBR ISO/IEC 27001:2022 e pelo art. 9º da Resolução Administrativa n.º 17/2024, assim como diretrizes e informações presentes nos processos operacionais padronizados pelo TCE-GO.

4. DIRETRIZES, RESPONSABILIDADES E NORMAS ESPECÍFICAS DE SEGURANÇA DA INFORMAÇÃO

4.1 Controle de acesso virtual

I. Os acessos à infraestrutura interna de tecnologia da informação do TCE-GO são permitidos apenas mediante identificação e autenticação de usuários, que terão acesso restrito ao que lhes é autorizado e de acordo com perfis de acesso;

II. A definição e alteração dos perfis de acesso é de responsabilidade do superior imediato do colaborador/prestador de serviço em conjunto com a Diretoria de TI (DI-TI);

III. Alterações nos perfis de acesso dos colaboradores e prestadores de serviços são registradas e armazenadas para possíveis consultas e auditorias;

IV. Os perfis de acesso dos usuários serão revisados periodicamente pelos gestores dos colaboradores/prestadores de serviço em conjunto com a DI-TI, além de que a cada biênio é realizada a revisão de acessos e responsabilidades;

V. Os colaboradores e prestadores de serviço são responsáveis por todas as ações realizadas com sua identificação de acesso à infraestrutura interna, ativos de informações e dispositivos móveis do TCE-GO;

VI. O acesso a infraestrutura interna de TI é pessoal e intransferível;

VII. Os colaboradores e prestadores de serviço possuem acesso às informações e ativos de informações necessários para a realização das suas respectivas atividades, conforme seu perfil de login e acesso;

VIII. Os colaboradores e prestadores de serviço devem realizar alteração imediata da senha, caso haja suspeita de um possível vazamento de informação do TCE-GO utilizando-se de sua conta de acesso;

IX. A DI-TI deve ser imediatamente comunicada da falha de segurança com registro formal, para as devidas providências, conforme determinação do PO Gerir Incidentes de Segurança da Informação;

X. A DI-TI deve instituir mecanismos de controle e criptografia nas bases de dados que contenha as informações das identificações e senhas dos colaboradores e prestadores de serviços;

XI. Os acessos à infraestrutura interna de TI do TCE-GO são registrados e sujeitos à rastreabilidade, visando à identificação de acessos que violem as diretrizes e políticas técnicas correlatas;

XII. Login seguro é requerido em todos os sistemas sendo que são consideradas 5 tentativas para acesso à rede (Active Directory) e na última tentativa não aprovada o sistema gera o bloqueio do usuário. Nos acessos ao TCENET/SINI são consideradas 5 tentativas para acesso e na última tentativa não aprovada o sistema gera o bloqueio do usuário;

XIII. Os sistemas de informação são analisados criticamente, em intervalos regulares não superiores a 12 meses, para verificar a conformidade com as normas, políticas e diretrizes de segurança da informação determinadas pelo TCE-GO;

XIV. Rotineiramente deve-se realizar a avaliação junto a equipe terceirizada com objetivo de controle de limites de acessos e disponibilidade dos mesmos;

XV. Rotina automatizada será executada diariamente para bloqueio dos usuários desligados do TCE-GO.

4.1.1 Permissões para acesso a informações em Banco de Dados

I. Não se deve disponibilizar às aplicações acesso à algum banco de dados utilizando login de usuário;
II. Não se deve disponibilizar às aplicações acesso à algum banco de dados utilizando login de usuário com permissões para execução de comandos em *Data Definition Language* (DDL);
III. Não se deve disponibilizar às aplicações acesso à algum banco de dados utilizando login de usuário com permissões além das estritamente necessárias ao seu funcionamento.

4.1.2 Gerenciamento e distribuição de senhas para acesso a dados

I. Não é permitido a elaboração de senhas que não sigam os padrões estabelecidos pelo TCE-GO. As senhas do Active Directory devem possuir no mínimo 8 (oito) a 14 (quatorze) caracteres alfanuméricos, caracterizando a gestão de senha seguras para acesso. As senhas do SINI/TCENET devem possuir no mínimo 8 (oito) a 10(dez) caracteres alfanuméricos, caracterizando a gestão de senha seguras para acesso.

II. Não se deve utilizar o armazenamento de senhas em código-fonte;

III. Deve-se armazenar de forma segura os dados de usuários e os sistemas que utilizam cada senha fornecida;

IV. Não se devem utilizar as mesmas senhas para ambientes de desenvolvimento, teste, homologação e produção.

4.1.3 Autorização e autenticação de usuários

I. São utilizados controle de usuário e senha nominais para determinar a identidade do usuário;

II. São utilizados autenticação via SINI sempre que possível para autenticar usuários internos;

III. São utilizados grupos de Active Directory (AD) / Sistema de Gerenciamento de Acesso (GPAC) para determinar as políticas de acesso e roles de usuário;

IV. Os usuários administradores da TI (Domain Admin no AD), devem utilizar contas nomeadas e separadas com privilégios suficientes para executar as tarefas necessárias. Portanto, não devem compartilhar um mesmo usuário administrador;

V. As contas administrativas (Domain Admin e Banco de Dados Oracle) serão revisadas semestralmente;

VI. Redes sociais corporativas são acessadas pela área de comunicação do TCE-GO a qual realiza o gerenciamento de senha por meio de termo de responsabilização e alteração de senhas a cada alteração na equipe ou a cada 6 meses, consideramos ainda o eventual acesso realizado por equipe terceirizada e servidores da área de TI, considerando ações específicas como transmissões de sessões plenárias e acesso ao canal Youtube.

4.1.4 Acesso e uso de e-mail corporativo

I. Toda e qualquer mensagem distribuída pelo e-mail do TCE-GO são de sua propriedade;

II. Sua caixa de entrada corporativa pode ser monitorada, com devida notificação prévia caso o TCE-GO achar necessário;

III. Evite abrir mensagens de destinatários suspeitos de modo a evitar que o sistema de e-mails seja infectado por alguma ameaça digital;

É estritamente proibido:

IV. Enviar e-mails contendo comentários ofensivos, racistas, sexistas ou obscenos.

V. Enviar Spam ou “correntes”;

VI. Falsificar ou tentar forjar mensagens de e-mail, disfarçar ou tentar disfarçar sua identidade ao enviar um e-mail;

VII. Acessar conta de outro servidor;

VIII. Senhas devem ser armazenadas conforme as diretrizes de controle de acesso apresentadas neste manual.

4.1.5 Autenticação em sistemas web

I. Sendo o HTTP um protocolo *stateless*, que utiliza cookies para manter sessões de usuário, faz-se necessário garantir tanto a segurança da troca de credenciais quanto a segurança das demais páginas acessadas pelos usuários dos sistemas web;

II. Dessa forma deve-se utilizar HTTPS em todas as telas dos sistemas, visto que o protocolo HTTPS visa contribuir para que essa segurança seja garantida.

4.2 Segurança física e do ambiente

I. As instalações do TCE-GO são protegidas conforme o valor dos ativos que estão em seu interior, preservando a continuidade e a competitividade.

II. O acesso físico ao TCE-GO é controlado por meio de um sistema integrado formado por barreiras físicas, documentos que registram os procedimentos internos, sistemas eletrônicos de segurança, pessoal contratado, treinado e equipado para exercer suas funções, assim como apoio da assessoria da polícia militar do estado de Goiás.

III. Somente o pessoal autorizado e identificado pode permanecer dentro do TCE-GO, podendo assim negar acesso a qualquer um que não queira se submeter ao procedimento de identificação.

IV. No interior da organização é obrigatório a utilização, por todos e em local visível, do crachá de identificação fornecido pela recepção.

V. O acesso de pessoas ao local está condicionado ao cadastro prévio no sistema eletrônico de controle de acesso.

VI. O acesso de visitantes é devidamente monitorado via sistema interno de câmeras e não é permitida a entrada de ninguém portando armas de fogo (a não ser que seja policial ou outro profissional da área de segurança em efetivo exercício).

VII. A instalação e manutenção de chaves e fechaduras (portões, armários, gavetas, cofres) estão sob controle da área de manutenção predial e paisagismo, assim como a gestão de acessos de cada área que constitui o TCE-GO.

VIII. Áreas consideradas críticas e sensíveis possuem acesso por meio de fechadura eletrônica e requerem cadastro especial.

IX. O trânsito de veículos no TCE-GO deve cumprir os limites de velocidades internos assim como a preferência de estacionamento em marcha ré facilitando a segurança no momento da saída.

X. A organização adota um rígido controle dos materiais e produtos existentes nos depósitos e almoxarifados, os quais são de acesso restrito às pessoas que neles trabalham, sendo estes servidores e equipe terceirizada do TCE-GO.

XI. O acesso aos componentes de infraestrutura das instalações do TCE-GO, como cabine de força, painéis de controle de energia, sistemas de comunicações e reservatórios de água, são controlados via sistema eletrônico e de acesso restrito ao pessoal autorizado.

XII. Os colaboradores devem responder por todo e qualquer acesso aos ativos do TCE-GO, sob sua responsabilidade, assim como pelos efeitos desses acessos efetivados, através de seu consentimento voluntário ou negligente.

XIII. Os prestadores de serviço devem adotar medidas de segurança compatíveis com a Política de Segurança Física do TCE-GO, e estarem aptos à recepção de auditorias ao longo da prestação de serviços, seguindo determinações conforme contrato.

4.3 Desastres Naturais

O TCE-GO adota medidas para contenção e mitigação de desastres naturais conforme determinado no PO – Responder Situações de Emergência, o qual considera, dentre outros, os seguintes cenários: (I) Em Caso de Incêndio; (II) Em Caso de Inundação; (III) Em Caso de Explosão; (IV) Em Caso de Derrame; (V) Fuga de Gases (GPL); (VI) Erosão do Solo; (VII) Eventos individuais; (VIII) Riscos com insetos / animais peçonhentos (abelhas, cobras, aranhas...) etc.

Ainda, outras condições de emergência estão associadas ao Manual de Abandono de Área e ao Manual de Práticas Seguras e demais políticas e diretrizes consideradas neste manual.

4.4 Controles criptográficos

I. O uso de criptografia poderá ser utilizado somente quando aprovado pela DI-TI, ou seja, em casos específicos, devidamente formalizados, e seguindo normas ou procedimentos relativos ao manuseio de informações classificadas e rotuladas;

II. Os algoritmos e os métodos de criptografia utilizados devem se basear em padrões de mercado e utilizar apenas tecnologias homologadas;

III. Certificação digital e assinatura digital poderão ser utilizados como forma de garantir a segurança nas comunicações institucionais;

IV. O gerenciamento de chaves utilizadas deve atender aos padrões internos determinados em processo operacional e diretrizes de gestão e operação, assim como devem estar sob o monitoramento e controle da DI-TI.

4.5 Mesa limpa e tela limpa

I. Os documentos em papéis e mídias eletrônicas não devem permanecer sobre a mesa desnecessariamente, devem ser armazenados em armários ou gavetas, quando não estiverem em uso, especialmente fora do horário do expediente;

II. Informações sensíveis ou críticas para o negócio da organização devem ser armazenadas em local separado e seguro (um armário ou cofre à prova de fogo);

III. Anotações, recados e lembretes não devem ser deixados à mostra sobre a mesa ou colados em paredes, divisórias ou monitor do computador;

IV. Não anotar informações sensíveis em locais visíveis;

V. Não guardar pastas com documentos sensíveis em prateleira de fácil acesso;

VI. Destruir os documentos impressos antes de jogá-los fora. Sempre que possível utilizar máquinas desfragmentadoras;

VII. Não imprimir documentos apenas para lê-los. Leia-os na tela do computador, se possível;

VIII. Informações sensíveis ou confidenciais, quando impressas em local coletivo, devem ser retiradas da impressora imediatamente;

IX. A disponibilização de documentação entre áreas de serviços deve ser protocolada e gerenciada pela área provedora da ação;

X. Computadores pessoais e terminais de computador e impressoras não devem ser deixados “logados”, caso o usuário responsável não esteja presente;

XI. Nos computadores, deve-se fazer uso de um protetor de tela que solicite uma senha para acesso. A política geral aplicada aos computadores bloqueará a tela e exigirá senha após 15 minutos de inatividade.

XII. Nunca deixar crachá de identificação ou chaves em qualquer lugar; mantenha-os junto a você;

XIII. Notificar o pessoal da segurança do TCE-GO imediatamente se suas chaves sumirem;

XIV. Não deixe mídias nos drives;

XV. Mesas e móveis deverão ser posicionados de forma que dados sensíveis não sejam visíveis de janelas ou corredores;

XVI. Ao final do expediente, ou no caso de ausência prolongada do local de trabalho, limpar a mesa de trabalho, guardar os documentos, trancar as gavetas e armários, e desligar o computador;

XVII. Sempre limpar sua área de trabalho antes de ir para casa, garantindo adequada organização dos itens/objetos manipulados.

4.6 Uso e controle de mídias removíveis

I. É proibida a utilização de mídias removíveis pelos colaboradores do TCE-GO em suas estações de trabalho. Somente em casos extremos, colaboradores previamente autorizados podem utilizar esses dispositivos considerando todo arcabouço de gestão de antivírus instalado, monitorado e controlado pela organização.

II. É proibido o armazenamento de informações sensíveis em dispositivos de mídia removíveis, caso a ação seja necessária estas devem ser criptografadas de acordo com a política de uso de criptografia vigente e o grau de sigilo exigido para a informação.

III. Toda e qualquer mídia removível só poderá ser descartada ou doada após a devida sanitização de informações ali contidas, solicitando sempre o apoio da equipe da DI-TI e a área de patrimônio. O processo de sanitização consiste em uma formatação de baixo nível, reescrevendo (bit a bit) todo o espaço de armazenamento de dados no dispositivo algumas vezes. Os dados contidos nos setores apagados são normalmente substituídos por zeros ou valores aleatórios. Desta maneira, garante-se que não sejam recuperados os arquivos de dados da unidade de armazenamento, nem mesmo através de métodos de recuperação de arquivos baseados em software ou hardware.

IV. É vedada toda e qualquer transferência de mídias removíveis, estando o servidor ciente desta regra via termo de responsabilidade para uso dos recursos de tecnologia da informação.

Nota 1: o propósito dessas normas é minimizar os riscos de exposição e perda de dados sensíveis mantidos pelo TCE-GO e reduzir os riscos de proliferação de malwares nos computadores da organização, assim como o devido controle do uso de mídias removíveis.

Nota 2: cabe ressaltar que o TCE-GO não declara como aplicável o uso de mídias removíveis como uma prática pela organização, sendo este ativo considerado como um risco aceitável pela organização, o qual requer controle e monitoramento contínuo a fim de garantir sua adoção sistêmica.

4.7 Uso de dispositivos móveis

I. É proibido instalar ou remover softwares nos computadores TCE-GO sem a prévia autorização;

II. É proibido abrir computadores ou outros ativos de informática para qualquer tipo de reparo, devendo notificar a DI-TI quando qualquer problema for identificado;

III. É proibido alterar as configurações de rede e da BIOS das máquinas, bem como, efetuar qualquer modificação que possa causar algum problema futuro;

IV. É proibido retirar ou transportar qualquer equipamento do TCE-GO sem autorização prévia do DI-TI e Área de Patrimônio;

V. É proibido instalar, desinstalar, desabilitar ou alterar qualquer software ou hardware a fim de tornar o mesmo total ou parcialmente inoperante;

VI. É proibido retirar ou desconectar qualquer equipamento da rede sem um motivo aceitável do TCE-GO

VII. É proibido comprometer, por mau uso ou de forma intencional, equipamento pertencente ao TCE-GO;

VIII. É proibido autorizar, sem devido conhecimento e liberação da DI-TI, a utilização de equipamentos de informática por pessoas sem vínculo com o TCE-GO;

IX. É proibido utilizar equipamentos e informações para outros fins, que não sejam atividades ligadas ao TCE-GO;

X. É proibido retirar/danificar licenças/placas identificadoras de patrimônio afixadas nos equipamentos de informática ou travas/lacres de segurança disponível em tais;

XI. É proibido conectar e/ou configurar equipamento à rede, sem a prévia liberação da DI-TI;

XII. É proibido alterar, excluir ou inutilizar informações ou meios de acesso a aplicativos/equipamentos de forma indevida ou sem prévia autorização do TCE-GO;

XIII. É proibido apropriar-se de segredos de pesquisa, de informações de outros colaboradores ou pertencentes ao TCE-GO através de qualquer meio, eletrônico ou não, sem prévia autorização do proprietário de tais informações;

XIV. É proibido tornar vulnerável a segurança dos ativos de informática portáteis (notebook, data show, pen drive etc.);

XV. Compartilhar arquivos ou diretórios somente através de meios tecnológicos autorizados pela DI-TI. (Ex: vpn, nuvem privada, diretório na rede)

Nota 3: os dispositivos móveis possuem identificação própria de inventário em local visível e não removível, a partir do qual será efetuado o controle de entrada e saída ou transferência do respectivo bem patrimonial, controlados conforme descrito em PO - Gerir Patrimônio.

Nota 4: o suporte técnico da DI-TI do TCE-GO é exclusivamente para equipamentos e recursos de tecnologia da informação institucionais. Não é permitido nem exercido suporte técnico para equipamentos pessoais dos colaboradores ou prestadores de serviço dentro das dependências do Tribunal.

4.8 Transferência das informações

A transferência da informação é o momento mais delicado e de vulnerabilidade. Carece, portanto, de cuidado. Antes de transferir qualquer informação, por e-mail, WhatsApp, telefone, redes sociais ou outro meio de comunicação, verifique se você tem autorização para passá-la, se a pessoa a receber tem condições de recebê-la e qual a consequência de tal transferência, para garantir a segurança desta ação o TCE-GO determina é **expressamente proibido:**

I. Transmissão ou posse de informação que contenha materiais obscenos, indecentes, lascivos ou outro material que explícita ou implicitamente se refira à conduta sexual;

II. Transmissão ou posse de informação que contenha linguagem profana ou constitua apologia ao fanatismo, à prática sexual ou a quaisquer formas de discriminação;

III. Transmissão ou posse de informação que ameace a integridade física ou que intimide outra pessoa ou organização;

IV. Transmissão de informação que implique violação de quaisquer leis ou constitua incitamento de qualquer crime;

V. Violação de direitos autorais;

VI. Divulgação de qualquer informação restrita ou confidencial sem a permissão de seu proprietário ou do Gestor do recurso ao qual a informação pertence.

Nota 5: a gestão de informações segue determinação da Resolução nº. 010/2017, assim como demais requisitos legais envolvidos ao tema.

4.9 Comunicação segura

I. Deve-se empregar canal de comunicação com controle de duplicação e perda de informações/mensagens. Dessa forma deve-se utilizar HTTPS em todas as telas dos sistemas.

II. Deve-se empregar canal de comunicação que provenha controle de integridade dos dados transmitidos (HTTPS).

III. Deve-se empregar canal de comunicação com controle de autenticação (HTTPS, certificados digitais gerados por autoridades confiáveis, VPNs).

IV. Deve-se armazenar de maneira segura os dados a serem transmitidos em ambas as extremidades da comunicação.

V. Deve-se empregar canal de comunicação que provenha confidencialidade dos dados transmitidos (HTTPS e VPNs).

4.10 Proteção contra malware

Objetivando aplicar medidas preventivas de proteção, detecção e correção corporativamente, para resguardar o ambiente tecnológico do TCE-GO contra softwares maliciosos (vírus, worms, spyware, spam), determina:

I. O uso de softwares não autorizados por parte da área de tecnologia da informação do TCE-GO é proibido, sendo controlado por meio de firewalls de aplicação, caso o usuário possua dúvidas as mesmas devem ser encaminhadas via Help Desk.

II. Caso o usuário perceba que no seu equipamento de trabalho os sistemas de proteção, como antivírus e firewall, não estejam instalados ou funcionando adequadamente, este deve entrar em contato via Help Desk para as devidas providências;

III. São aplicados acessos restritos e são registradas tentativas de acesso a websites maliciosos ou suspeitos, por parte dos usuários.

IV. A intenção de introduzir ou espalhar softwares maliciosos no ambiente tecnológico do TCE-GO poderá acarretar sanções administrativas disciplinares e/ou contratuais aos seus respectivos usuários, sem prejuízo das responsabilizações nas esferas cível e criminal.

V. São realizadas ações para promover o isolamento, ao máximo possível, de ambientes sigilosos do TCE-GO que possam ser contaminados por malwares para evitar impactos de grande magnitude às atividades do negócio.

VI. São configuradas varreduras automáticas e completas, realizadas regularmente por soluções de antivírus.

VII. Arquivos recebidos por meio de redes, em qualquer mídia de armazenamento, correio eletrônico, arquivos baixados (download) ou em páginas web, devem ser verificados automaticamente quanto à presença de códigos maliciosos, antes de serem utilizados;

4.11 Gestão de mudança

Todas as mudanças em sistemas de TI e também outros processos que possam afetar a segurança da informação são estritamente controlados, tendo o devido controle quanto à confidencialidade, integridade e disponibilidade das informações envolvidas no processo.

I. Mudanças que tenham ocorrido e que não estejam contempladas no Plano de Continuidade de TI devem gerar atualizações.

II. Quando novos requisitos forem identificados, os procedimentos relacionados devem ser ajustados de forma apropriada.

III. Diversas situações podem demandar atualizações no Plano de continuidade de TI, tais como as mudanças:

a) no parque ou ambiente computacional (ex.: aquisição de novo equipamento, atualização de sistemas operacionais, migração de sistemas de grande porte para ambiente cliente-servidor);

b) administrativas, de pessoas envolvidas e responsabilidades;

c) de endereços ou números telefônicos;

d) na localização e instalações;

e) na legislação;

f) em prestadores de serviço e fornecedores;

g) de processos (inclusões e exclusões);

h) na gestão de riscos;

i) na gestão do TCE-GO.

IV. O controle de mudanças deve ser formalizado conforme PO - Gerir Melhoria Contínua, sendo seu registro analisado conforme cada cenário.

Nota 6: deve-se ainda considerar que tais mudanças também estão previstas no manual do Sistema de Gestão Integrado (SGI), nos tópicos “Planejamento de Mudanças” e “Controle de Mudanças”.

Nota 7: mudanças advindas de questões internas, solicitadas via Help Desk, são registradas em sistema de controle de tarefas da TI como ações de correção ou evolução, possuindo tratativas e planos de ação devidamente monitorados e controlados via sistema.

4.12 Ataques à sistemas e suas defesas

Com objetivo de instituir diretrizes vinculadas à prevenção, detecção e recuperação a ameaças e possíveis ataques contra sistemas e aplicações, garantindo a segurança de redes. O TCE-GO determina:

I. Deve-se realizar proteção de hardware, impedindo acessos físicos não autorizados à infraestrutura da rede, prevenindo roubo de dados e desligamento de equipamentos.

II. Instituir a proteção de arquivos e dados por meio de autenticação, controle de acesso e sistema antivírus. Sendo que no processo de autenticação, deve-se verificar a identidade do usuário, o seu controle de acesso (conforme permissões pertinentes a cada usuário) e programas de antivírus que garantam a proteção do sistema contra programas maliciosos.

III. Deve-se restringir as permissões de acesso ao banco de dados para o usuário da aplicação.

IV. Deve-se prevenir ataques de injeção de SQL (SQL *Injection*).

V. Não se deve criar SQLs concatenando parâmetros textuais de origem não-segura, como parâmetros preenchidos pelo usuário ou mesmo armazenados no banco de dados.

VI. Deve-se, sempre que possível, passar parâmetros em comandos SQL (DML ou DDL) utilizando *prepared statements*. Consultas que não podem ser parametrizadas devem receber tratamento especial, como escapes ou codificação em hexadecimal.

VII. Deve-se prevenir ataques de injeção de HTML e *Javascript*.

VIII. Deve-se prevenir ataques do tipo *cross-site scripting* (XSS).

IX. Deve-se garantir o uso de medidas preventivas a fim de prevenir e sanar vulnerabilidades técnicas rotineiras e não rotineiras.

X. Deve-se prevenir ataques de quebra de autenticação e gerenciamento de sessão *Broken Authentication and Session Management*.

XI. Aplicar Proteção de Perímetro, por meio de ferramentas firewall e routers, mantendo a rede protegida contra tentativas de intrusão (interna e externa)

XII. Deve-se submeter os sistemas a ferramentas de testes de invasão.

XIII. Aplicar ferramentas para detecção de ataques sendo estes alertas e ações de auditoria contínuas nos sistemas e aplicações.

XIV. Realizar ações de recuperação, por meio de cópia de sistemas de dados (Backup), aplicativos de backup e backup de hardwares.

Nota 8: a aplicação de diretrizes e politicas descritas neste manual garantem a configuração e manuseio seguro de dispositivos *endpoint* utilizados em ações operacionais e sob o controle da organização.

4.13 Conformidade de requisitos legais e contratuais

Objetivando impedir a violação de quaisquer normas legais, regulamentares ou contratuais relacionadas à segurança da informação, fica determinado:

I. É necessário que a DI-TI e a Sec-Admin mantenham atualizadas as planilhas de requisitos legais aplicáveis.

II. Adquirir apenas softwares de fontes conhecidas e bem reputadas, para garantir que o direito autoral não esteja sendo violado.

III. Implementar controles que garantam que o número máximo de usuários por licença de software, não esteja sendo excedido.

IV. Os sistemas de informação do TCE-GO devem ser analisados a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação do órgão.

V. Todas as atividades, sistemas e serviços desenvolvidos e prestados pelo TCE-GO devem estar em consonância com as leis, normas e regulamentações jurídicas municipais, estaduais e federais vigentes.

Nota 9: o TCE-GO realiza toda a gestão de requisitos legais vinculados à segurança da informação por meio de Planilha de Controle de Requisitos Legais de Segurança da Informação, anexada a este manual, a qual é atualizada rotineiramente e monitorada a cada ciclo de auditoria interna do SGI.

Nota 10: o TCE-GO terceiriza atividade de desenvolvimento de softwares, sendo esta ação controlada e monitorada por meio de requisitos contratuais específicos, os quais garantem integridade de ações realizadas e atendimento às políticas e diretrizes de segurança da informação descritas neste manual e demais documentos de apoio.

4.14 Política de Privacidade

O TCE-GO oferece uma ampla variedade de serviços providos por meio da internet, tais como sites e aplicativos. Sendo assim fica determinado:

I. Quanto ao Sigilo de informações: as informações coletadas pelo TCE-GO seguem as diretrizes dadas pela Lei Geral de Proteção de Dados - LGPD (Lei 13.709/2018), que dispõe sobre o tratamento de dados pessoais, pela Lei Federal nº 12.527/2011, que trata o direito constitucional de acesso às informações públicas e também pela Lei Estadual Nº 18.025/2013, regulamentadas pela Resolução Normativa Nº 004/2012 do TCE-GO e alterada pela Resolução Normativa Nº 003/2015. No tocante a tais informações, observa-se ainda o Regulamento da Ouvidoria do TCE-GO.

II. Neste sentido, a Lei Estadual Nº 18.025/2013 - em seu art. 4º, inc. IV - veda o acesso irrestrito às informações relativas a processos de inspeções, auditorias, prestações e tomadas de contas realizadas pelos órgãos de controle interno e externo, assim como às informações referentes a procedimentos de fiscalização, investigação policial, sindicâncias e processos administrativos disciplinares, enquanto não concluídos.

III. Em relação às informações pessoais coletadas pelo TCE-GO, o sigilo é garantido por meio da Resolução Normativa nº 10/2017, que dispõe sobre os critérios para promover a classificação das informações confidenciais produzidas ou custodiadas pelo TCE-GO. Esta regulamentação estipula o prazo de cem anos de restrição para informações classificadas como pessoais, ou seja, que digam respeito a informação referente à intimidade, vida privada, honra e imagem da pessoa, bem como às liberdades e garantias individuais.

IV. Quanto à possibilidade de manifestação anônima: o TCE-GO permite a manifestação anônima, dispensando a coleta de dados pessoais para a maior parte dos serviços oferecidos. Excetuam-se as comunicações de irregularidades ou ilegalidades ocorridas na administração pública estadual, realizadas por meio de denúncia ou representação. Estes institutos encontram-se regulados na Lei Orgânica do TCE-GO (Lei n° 16.168, de 11 de dezembro de 2007, arts. 87 a 90) e no Regimento Interno do TCE-GO (Resolução n° 22/2008, arts. 231 a 235). Mesmo nestes casos, quando houver a opção pelo sigilo dos dados da sua manifestação, os interlocutores e responsáveis pela tramitação se comprometerão a resguardá-los.

V. Quanto à Gestão da Política de Segurança da Informação: a gestão da privacidade e da proteção de dados pessoais no TCE-GO é acompanhada pela DI-TI e Comitê de Segurança da Informação.

VI. Entre outros aspectos é vedado armazenar ou transferir informações de conteúdo ofensivo, ou que incentivem a violência ou a discriminação de raça ou credo, além da utilização desses recursos para fins diversos dos previstos nos regulamentos aplicáveis.

VII. Ao adotarmos as melhores práticas de segurança, garantimos a integridade e a confidencialidade dos dados coletados e fortalecemos os mecanismos de proteção contra: uso indevido, tentativas de acesso não autorizados, fraudes, danos e sabotagens, evitando a ocorrência de incidentes.

VIII. Dados Pessoais coletados: o TCE-GO coleta dados para atuar de forma eficaz e proporcionar as melhores experiências com os serviços. A maior parte destas informações é solicitada de maneira explícita e são diretamente fornecidas através de formulários disponibilizados, como, por exemplo, quando você cria uma conta no aplicativo ou em algum dos portais do TCE-GO, ou quando entra em contato conosco para fazer algum tipo de manifestação. Outra parte desses dados é obtida ao registrar sua forma de interação com nossos serviços, por exemplo, na utilização de tecnologias como cookies e ao receber relatórios de erros ou dados de uso de software que estejam sendo executados em seu dispositivo. Também podemos obter dados de terceiros.

IX. Os seguintes dados podem ser coletados a partir do preenchimento voluntário de formulários: nome, e-mail, telefone, CPF, RG, data de nascimento, endereço, gênero, escolaridade e ocupação.

X. Outras informações que podem ser consideradas dados pessoais e também poderão ser tratadas pelo TCE-GO, tais como: informações referentes aos seus dispositivos eletrônicos (telefone celular, computadores, entre outros).

XI. Como utilizamos Dados Pessoais: devidamente observados os regulamentos citados, o TCE-GO usa as informações coletadas para disponibilizar e aprimorar os serviços

oferecidos as partes interessadas, que incluem dados de uso para melhorar os nossos serviços e personalizar as suas experiências. Também podemos usar os dados para nos comunicarmos com você, por exemplo, para informá-lo sobre a sua conta, as atualizações sobre informações solicitadas ou serviços oferecidos.

XII. Compartilhamos dados pessoais com o consentimento do usuário ou conforme necessário para concluir qualquer transação ou fornecer um determinado serviço solicitado ou autorizado. Podemos também compartilhar dados com outros órgãos da Administração Pública quando exigido por lei ou para responder perante um processo jurídico; para proteger vidas; para manter a segurança de nossos serviços e para proteger outros direitos garantidos em Lei.

XIII. Como cuidamos de seus Dados Pessoais: nós adequamos constantemente nossos processos de tratamento de dados para usar apenas as informações necessárias, de acordo com a finalidade pretendida. Por essa razão, cuidamos para que o acesso aos seus dados seja restrito aos colaboradores e terceiros autorizados que necessitem tratar essas informações.

XIV. Em alguns casos, usamos técnicas (anonimização, por exemplo) para que não seja possível que os dados a serem utilizados sejam associados a seus respectivos titulares, diminuindo assim os riscos de uso indevido dos dados pessoais armazenados pelo TCE-GO.

XV. Repudiamos e não autorizamos o tratamento de dados para fins discriminatórios abusivos ou ilícitos.

XVI. Disseminamos a cultura de sigilo, privacidade e proteção dos dados por meio de programas de conscientização e capacitação que, inclusive, contemplam ações educativas voltadas para toda equipe que constitui o TCE-GO.

XVII. O TCE-GO adota procedimentos para prevenir, detectar e responder a incidentes de segurança que envolvam seus dados pessoais. Além disso, elabora planos para a continuidade de negócios, planos de gestão de crises e relatórios de impacto, mapeia processos relacionados a segurança da informação e adota mecanismos de mitigação de riscos que são atualizados frequentemente.

4.15 Backup

Esta seção regulamenta as normas específicas de backup das informações eletrônicas no âmbito do TCE-GO, com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos dados sob a guarda da DI-TI, visando garantir a segurança, integridade e disponibilidade, em conformidade com a Política de Segurança da Informação.

I. Todo e qualquer ativo que armazene dados e que esteja sob responsabilidade da DI-TI deverá ser considerado para avaliação de inclusão no processo de backup.

II. O responsável por cada recurso deverá definir quais diretórios e arquivos serão incluídos no backup, tendo como prioridade:

a) Arquivos de configurações de sistemas operacionais e aplicativos instalados em servidores;

b) Arquivos de log dos aplicativos, inclusive log da ferramenta de backup e restauração;

c) Informações e configurações de banco de dados;

d) Conteúdo de repositórios de dados associados a sistemas

e) Arquivos institucionais de usuários (documentos e e-mails);

f) Arquivos de aplicações desenvolvidas pelo TCE-GO ou quaisquer outros não descritos neste, mas que a perda de suas informações gere prejuízo a este Tribunal.

III. Para os aplicativos e/ou bancos de dados devem ser seguidas as recomendações sugeridas pelo desenvolvedor e/ou fabricante.

IV. A criação e operação dos backups deverão obedecer às orientações determinadas em “PO - Gerir Backup”.

V. Os procedimentos de backup deverão ser atualizados quando houver:

a) Novas aplicações desenvolvidas;

b) Novos locais de armazenamento de dados ou arquivos;

c) Novas instalações de bancos de dados;

d) Novos aplicativos instalados;

e) Outras informações que necessitem de proteção através de backups deverão ser informadas ao Administrador de Backup (equipe terceirizada), pelo Diretor de TI.

VI. O prazo de retenção é definido na ferramenta de backup conforme requisitos disponibilizados pela solução. Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada ou destruída, observando sempre seu estado de utilização e número de leitura/gravação. A mídia não deverá ultrapassar 30 anos de armazenamento, devendo, nesse caso, ser copiada para outra mídia, destruída de forma segura e descartada em lugar destinado para tal, obedecendo às leis ambientais.

VII. Sempre que necessário deverá ser realizada a atualização das mídias de backup com a finalidade de preservar o acesso aos dados nelas contidas.

VIII. O backup deverá ser programado para execução automática em horários de menor utilização dos sistemas;

IX. O backup deverá ser monitorado pelo Administrador de Backup;

X. Para todos os backups realizados, deve ser gerado um extrato automatizado pela própria ferramenta de backup. Tal extrato deverá ser enviado por e-mail para o Administrador de Backup;

XI. Para os backups que apresentarem falhas, o Administrador de Backup deverá criar uma entrada registrando em solução específica citando os backups e se houve ação corretiva adotada. Competirá ao Administrador de Backup tratar falhas remanescentes.

XII. Os backups deverão ser realizados preferencialmente como disposto a seguir:

a) Os backups diários serão executados de segunda à sexta-feira, entre 18h e 6h do dia posterior, em modo incremental;

b) Os backups semanais serão executados nos finais de semana, iniciando aos sábados, em modo incremental. Não haverá execução de backup semanal quando coincidir com o backup mensal ou anual;

c) Os backups mensais serão executados no primeiro sábado do mês, em modo incremental. Não haverá execução de backup mensal quando coincidir com o backup anual;

d) Em caso de falha, após verificação do motivo da falha, se houver janela disponível o backup é executado novamente, em casos que não existe janela disponível aquele backup é ignorado refazendo o processo novamente.

XIII. Para todos os testes realizados deverá ser gerado um relatório que ficará sob guarda da DI-TI.

XIV. Além dos testes executados automaticamente pela ferramenta de backup, os testes de integridade definidos no “PO - Gerir Backup” serão executados trimestralmente.

5. Anexos

Quadro dos Dispositivos Legais de Segurança da Informação.

6. Elaboração, Revisão e Aprovação

Manual de Segurança da Informação		
Diretoria de Tecnologia da Informação (DI-TI)		
Responsável por	**Nome**	**Função**
Elaboração	Leandro dos Santos	Chefe do Serviço de Infraestrutura e Segurança em TI
Elaboração/Aprovação	Membros do Comitê de Segurança da Informação	Comitê de Segurança da Informação
Controle de Qualidade	Fabrício Borges dos Santos	Chefe do Serviço de Gestão da Melhoria Contínua

Controle de Versionamento		
Versão anterior: 002 de 20/11/2023	Versão atual: 003 de 26/09/2024	Próxima Revisão Programada: 26/09/2027