Instrução Normativa nº 5/2024

Institui a Política de Uso Aceitável de Recursos Computacionais da Nuvem Corporativa Estadual no âmbito da Administração Pública direta, autárquica e fundacional do Poder Executivo do Estado de Goiás.

O SECRETÁRIO-CHEFE DA SECRETARIA-GERAL DE GOVERNO, no uso das atribuições que lhe conferem os incisos I e II do § 1º do art. 40 da Constituição do Estado de Goiás; o inciso XIII do art. 5º e o caput c/c inciso I do § 2º do art. 108 da Lei estadual nº 21.792, de 16 de fevereiro de 2023; o inciso XIII do art. 2º, o inciso I do art. 75 e o inciso II do art. 81 do Decreto estadual nº 10.355, de 05 de dezembro de 2023,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Política de Uso Aceitável de Recursos Computacionais da Nuvem Corporativa Estadual, nos termos desta Instrução Normativa, no âmbito da administração pública direta, autárquica e fundacional do Poder Executivo do Estado de Goiás.

Art. 2º Esta Instrução Normativa tem como objetivo definir responsabilidades e requisitos essenciais para o uso dos serviços de computação em nuvem disponibilizados pela Unidade Central de Tecnologia da Informação, estabelecendo diretrizes claras para os órgãos usuários e administradores desses serviços, visando garantir a sua utilização exclusiva e padronizada para os fins institucionais dos órgãos e entidades da administração pública direta, autárquica e fundacional do Poder Executivo do Estado de Goiás.

Art. 3º A Nuvem Corporativa Estadual é composta por infraestrutura tecnológica capaz de suportar demandas de hospedagem de serviços de computação em nuvem, processados e armazenados nos Data Centers estaduais e em ambiente de nuvem pública e privada, sob gestão e operacionalização da Unidade Central de Tecnologia da Informação.

Art. 4º Os órgãos e entidades pertencentes à administração pública direta, autárquica e fundacional do Poder Executivo do Estado de Goiás devem aderir às disposições estabelecidas nesta Instrução Normativa, ao utilizar os recursos computacionais e soluções fornecidas por intermédio da Nuvem Corporativa Estadual em seus sistemas de tecnologia da informação e comunicação.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 5º Para fins do disposto nesta Instrução Normativa, considera-se:

I - *appliance*: dispositivo de hardware independente e dedicado com software integrado, especificamente projetado para fornecer um recurso de computação específico;

II - computação em nuvem: modelo que permite acesso universal e sob demanda, por intermédio da rede, a um conjunto compartilhado de recursos computacionais configuráveis, que podem ser rapidamente provisionados e disponibilizados com o mínimo de esforço de gerenciamento ou de interação com o provedor de serviços de nuvem;

III - *FinOps*: abordagem que utiliza práticas e metodologias para simplificar o gerenciamento e a governança financeira no uso da nuvem, garantindo que o investimento seja justificado por valor tangível para o negócio;

IV - Infraestrutura como Serviço (*Infrastructure as a Service - IaaS*): provisionamento, por parte do provedor de serviços de nuvem, de recursos essenciais de computação, como processamento, armazenamento, comunicação de rede, segurança, entre outros, nos quais o cliente tem a capacidade de instalar e executar uma variedade de softwares, incluindo sistemas operacionais, bancos de dados e aplicativos, sobre essa infraestrutura fornecida. Embora o cliente não gerencie ou controle a infraestrutura física subjacente da nuvem, ele tem controle total sobre as máquinas virtuais, sistemas operacionais, bancos de dados e aplicativos instalados;

V - multilocação: hospedagem compartilhada, na qual os recursos de computação em nuvem são divididos entre clientes diferentes, sendo que seus dados são mantidos totalmente separados;

VI - nuvem híbrida: infraestrutura de nuvem composta por uma ou mais infraestruturas distintas de nuvem, sejam elas públicas ou privadas, que permanecem como entidades únicas e são conectadas por tecnologias proprietárias ou padronizadas, permitindo a portabilidade de aplicações e dados entre as nuvens;

VII - nuvem privada: infraestrutura de nuvem destinada exclusivamente a uma única organização, mas que pode servir a diversos clientes internos. Sua propriedade, gerenciamento e operação podem ser conduzidos pela própria organização, por terceiros ou por uma combinação de ambos. Além disso, ela pode ser localizada dentro ou fora das instalações da organização;

VIII - nuvem pública: infraestrutura de nuvem que está disponível para uso público e que reside nas instalações do provedor de serviços de nuvem. Sua gerência, operação e propriedade podem ser de uma organização governamental, acadêmica, empresarial, ou até mesmo uma combinação entre elas. A infraestrutura física é compartilhada, mas há uma separação lógica por cliente;

IX - Plataforma como Serviço (*Platform as a Service - PaaS*): provisionamento, por parte do provedor de serviços de nuvem, de recursos de hospedagem de sistemas e aplicações em diversas linguagens de programação, bibliotecas, serviços e ferramentas de suporte ao desenvolvimento de aplicações, para que o cliente possa implantar, na infraestrutura da nuvem, aplicativos criados ou adquiridos por ele. Nesse modelo, o cliente não precisa gerenciar nem controlar a infraestrutura subjacente da nuvem, que é fornecida como IaaS, nem a camada de sistema operacional, servidor de aplicação e banco de dados. No entanto, ele tem controle sobre os sistemas e aplicações implantadas sob sua responsabilidade;

X - Software como Serviço (*Software as a Service - SaaS*): provisionamento, por parte do provedor de serviços de nuvem, de aplicações de interesse comum, que são acessíveis de forma transparente e independente de dispositivo. Nesse modelo, o cliente gerencia apenas as configurações dos aplicativos, específicas do usuário;

XI - provedor de serviços de nuvem: empresa ou órgão central que possui recursos de tecnologia da informação (TI) destinados ao fornecimento de infraestrutura, plataformas e aplicativos baseados em computação em nuvem;

XII - Unidade Central de Tecnologia da Informação: unidade central que coordena a gestão de Tecnologia da Informação no âmbito do Estado de Goiás, atualmente, a Subsecretaria de Tecnologia da Informação, da Secretaria-Geral de Governo, com suas respectivas unidades básicas e complementares; e

XIII - Unidades Setoriais de Tecnologia da Informação: unidades administrativas pertencentes a órgão ou entidade estadual, responsáveis por atuar nas atividades de Tecnologia da Informação, sob o direcionamento técnico da Unidade Central de Tecnologia da Informação.

CAPÍTULO III DAS DIRETRIZES

Art. 6º São diretrizes da Política de Uso Aceitável de Recursos Computacionais da Nuvem Corporativa Estadual:

I - garantir que as soluções baseadas em computação em nuvem atendam aos requisitos de negócio, legislação e políticas governamentais, e que estejam alinhadas às melhores práticas de mercado;

II - gerir e racionalizar a gestão de custos de infraestrutura e licenciamento através da implementação de práticas *FinOps*, visando ganho de escala e otimização dos esforços e recursos financeiros;

III - prover informação quanto ao uso dos recursos tecnológicos, por meio de indicadores gerenciais, que habilite

o usuário administrar o uso racional dos recursos da Nuvem Corporativa Estadual;

IV - assegurar a prestação do serviço por meio de um conjunto compartilhado de recursos computacionais, promovendo o atendimento a todos os órgãos e entidades da administração pública do Poder Executivo estadual por meio de um modelo de alocação dinâmica de recursos computacionais, conforme a demanda;

V - garantir elasticidade rápida, permitindo o provisionamento e a liberação ágeis de recursos conforme demandados, possibilitando que os órgãos usuários ajustem facilmente o uso de serviços em nuvem para atender suas necessidades;

VI - assegurar a proteção dos negócios e informações do governo por meio de uma abordagem gerenciada por riscos, considerando a criticidade do serviço e a sensibilidade dos dados;

VII - garantir que as informações e dados armazenados estejam seguros, íntegros e confiáveis, protegendo-os contra acessos não autorizados, destruição, perda ou alteração acidentais ou ilícitas, por meio de medidas técnicas e administrativas adequadas; e

VIII - garantir a disponibilidade da Nuvem Corporativa Estadual, por meio da equipe de operação gestora, informando aos usuários os níveis de serviço previamente acordados (*Service Level Agreement - SLA*).

CAPÍTULO IV
DOS PAPÉIS E COMPETÊNCIAS

Art. 7º Compete à Unidade Central de Tecnologia da Informação, no papel de provedora de serviços de nuvem:

I - planejar e conduzir a implantação desta Política, por intermédio de suas estruturas administrativas;

II - gerenciar, orquestrar e prover serviços de computação em nuvem aos demais órgãos e entidades da administração pública do Poder Executivo estadual;

III - coordenar, padronizar e administrar a infraestrutura e os recursos necessários para manutenção dos serviços de computação em nuvem, a fim de manter a sua integridade, disponibilidade e continuidade; e

IV - fornecer visibilidade do uso dos recursos tecnológicos da Nuvem Corporativa Estadual e dos custos financeiros associados, por meio de painéis e indicadores gerenciais que permitam aos usuários otimizar o uso desses recursos de forma racional e eficiente.

Art. 8º Compete às Unidades Setoriais de Tecnologia da Informação, no papel de usuárias dos serviços de computação em nuvem, a observância e o cumprimento dos requisitos desta Política, em conformidade com seus princípios e suas diretrizes.

CAPÍTULO V
DOS DEVERES E RESPONSABILIDADES OPERACIONAIS

Art. 9º São deveres e responsabilidades operacionais da Unidade Central de Tecnologia da Informação, na qualidade de provedora de serviços de nuvem:

I - oferecer os serviços de computação em nuvem em ambiente de alta disponibilidade, com redundância dos componentes fundamentais da infraestrutura de Data Center, nas modalidades de Infraestrutura como Serviço, Plataforma como Serviço e Software como Serviço;

II - implementar e manter controle de acesso físico adequado ao ambiente de Data Center, incluindo monitoramento do ambiente por meio de circuito fechado de TV, vigilância dos ambientes internos e externos e segurança física contra acessos não autorizados;

III - garantir que o ambiente esteja protegido de usuários externos do serviço de computação em nuvem e de pessoas não autorizadas, implementando controles de segurança da informação de forma a propiciar o isolamento adequado dos recursos utilizados pelos diferentes órgãos e entidades da administração pública do Poder Executivo estadual, bem como por outros usuários do serviço de computação em nuvem;

IV - manter e gerir os recursos humanos, tecnológicos, financeiros e procedimentais necessários à sustentação de todo o ambiente de Nuvem Corporativa Estadual;

V - disponibilizar sistema de abertura de chamados para o registro de incidentes, solicitações de serviços e pedidos de informação ou apoio técnico;

VI - manter Central de Operação de Redes (*Network Operation Center - NOC*) operando 24 horas por dia, 7 dias por semana, para monitorar e gerenciar eventos de TI, atendendo a chamados fora do horário comercial conforme a matriz de acionamento e escalonamento para as equipes responsáveis;

VII - informar às Unidades Setoriais de Tecnologia da Informação, com no mínimo 5 (cinco) dias úteis de antecedência, sobre as interrupções necessárias para ajustes técnicos ou manutenções programadas, que possam causar prejuízo à disponibilidade e operacionalidade dos serviços de computação em nuvem, exceto em casos de urgência e emergência que possam comprometer o funcionamento regular da infraestrutura da Nuvem Corporativa Estadual;

VIII - comunicar às Unidades Setoriais de Tecnologia da Informação caso sejam identificadas falhas, vulnerabilidades ou incidentes que possam impactar a disponibilidade dos serviços de computação em nuvem, ou afetar o serviço como um todo;

IX - zelar pela eficiência e efetividade do uso dos recursos compartilhados da Nuvem Corporativa Estadual, adotando, junto aos usuários do serviço de computação em nuvem e fornecedores, as medidas necessárias para evitar prejuízos aos serviços dependentes desses recursos;

X - realizar e manter cópias de segurança dos dados hospedados na infraestrutura da Nuvem Corporativa Estadual, de forma a garantir a disponibilidade das informações, serviços e sistemas, reduzindo o tempo de indisponibilidade de sistemas críticos e informações devido a falhas ou desastres; e

XI - manter sigilo total sobre todos os dados armazenados e processados no ambiente computacional da Nuvem Corporativa Estadual, implementando recursos e procedimentos seguros que

garantam a integridade, confidencialidade, disponibilidade e o tratamento adequado de acordo com o nível de criticidade da informação.

Art. 10. São deveres e responsabilidades das Unidades Setoriais de Tecnologia da Informação, enquanto usuárias dos serviços de computação em nuvem:

I - operar e administrar os recursos computacionais disponibilizados pelo provedor de serviços de nuvem, responsabilizando-se pelo conteúdo dos sistemas e dados instalados e armazenados, pela capacidade de utilização do ambiente, pelas licenças de uso dos sistemas operacionais e softwares que estejam sob sua responsabilidade, e pela atualização periódica dos mesmos;

II - respeitar as demais normas e padrões de utilização dos recursos computacionais da Nuvem Corporativa Estadual que estejam em vigor;

III - utilizar os recursos computacionais exclusivamente para fins institucionais, ou seja, para dar apoio às atividades finalísticas ou de área meio do órgão ou entidade, sendo vedada a sublocação ou disponibilização desses recursos à terceiros;

IV - garantir a correta utilização dos recursos computacionais, realizando verificações periódicas de vulnerabilidades no código das aplicações que acessam esses serviços, a fim de prevenir ataques maliciosos por meio ou provenientes dos sistemas e aplicações sob sua responsabilidade;

V - instalar os softwares de segurança e de gerenciamento e monitoramento de máquinas virtuais e de aplicações, quando solicitado pelo provedor de serviços de nuvem, como meio de padronizar a gestão e a segurança de todo o ambiente de computação em nuvem;

VI - monitorar o ambiente sob sua responsabilidade, adotando em seus sistemas as melhores práticas de mercado e de segurança;

VII - manter atualizada a lista de contatos técnicos para questionamentos ou verificação de eventuais falhas nos serviços disponibilizados, inclusive com contato que possa ser acionado a qualquer momento, dia ou noite, em regime integral, em caso de desastre ou indisponibilidade dos serviços oferecidos;

VIII - comunicar imediatamente ao provedor de serviços de nuvem qualquer anormalidade ou comprometimento dos sistemas, serviços e informações sob sua responsabilidade; e

IX - submeter previamente ao provedor de serviços de nuvem quaisquer projetos que demandem grandes quantidades de recursos computacionais ou que possam afetar a performance e disponibilidade do ambiente, a fim de possibilitar o planejamento adequado de capacidade da infraestrutura necessária.

CAPÍTULO VI
DAS CONDIÇÕES GERAIS DE UTILIZAÇÃO

Art. 11. A Unidade Central de Tecnologia da Informação, na qualidade de provedora de serviços de nuvem, reserva-se ao direito de realizar qualquer uma das seguintes ações, a qualquer momento e sem aviso prévio:

I - limitar o fornecimento e a quantidade de qualquer recurso computacional ou serviço, caso seja detectada subutilização ou se sua utilização estiver afetando a performance e disponibilidade do ambiente;

II - monitorar e limitar o tráfego efetuado por meio das redes de comunicação, incluindo o acesso à Internet e o uso de correio eletrônico, se for detectado qualquer tipo de tráfego suspeito pelas soluções de segurança da informação ou que esteja causando impactos na performance e disponibilidade do ambiente;

III - bloquear temporariamente ou permanentemente IPs, blocos de IPs ou IPs de países cujo acesso esteja gerando problemas de performance do ambiente devido a sobrecargas ou ataques;

IV - suspender, bloquear ou excluir o acesso dos usuários dos serviços de computação em nuvem caso seja detectada violação das políticas de segurança ou das condições e regras estabelecidas nesta Instrução Normativa;

V - suspender, bloquear ou excluir contas de usuários inativas ou quando for detectada qualquer ação maliciosa;

VI - realizar verificações periódicas de vulnerabilidades em todo o ambiente de computação em nuvem, incluindo o ambiente sob responsabilidade das Unidades Setoriais de Tecnologia da Informação, devendo estas fornecer as permissões necessárias de acesso para a devida verificação;

VII - reiniciar servidores virtuais, mediante necessidade técnica justificada e previamente informada ao órgão responsável, que deverá acatar ou indicar uma janela para a execução da atividade, designando um responsável técnico pelo acompanhamento ou aceitando o reinício não assistido;

VIII - movimentar automaticamente ou manualmente servidores virtuais entre servidores físicos (*hosts*) e unidades de armazenamento (*datastores*) da Nuvem Corporativa Estadual para balancear e redistribuir as cargas de trabalho conforme a disponibilidade dos recursos computacionais;

IX - desativar, arquivar ou excluir servidores virtuais inativos, após comunicação prévia ao órgão responsável, que deverá acatar ou justificar a necessidade de mantê-los no ambiente em até 10 (dez) dias úteis;

X - solicitar alterações em sistemas, serviços, bases de dados ou outros componentes não conformes com as melhores práticas ou políticas estabelecidas; e

XI - encerrar a oferta ou fornecimento de qualquer serviço de computação em nuvem, informando as etapas necessárias para sua substituição ou migração para um novo serviço.

Art. 12. As Unidades Setoriais de Tecnologia da Informação, enquanto usuárias dos serviços de computação em nuvem, assumem os seguintes compromissos:

I - manter os recursos computacionais a sua disposição dimensionados em conformidade com as demandas reais do órgão, evitando a ociosidade de recursos, como servidores virtuais ligados sem execução de rotinas e sistemas para qual foi destinado ou com subutilização de processamento, memória e espaço de armazenamento, garantido o uso eficiente dos recursos computacionais da Nuvem Corporativa Estadual;

II - informar, com justificativa técnica, as regras de afinidade dos servidores virtuais sob sua responsabilidade para aplicações de alta disponibilidade que exijam processamento em servidores físicos (*hosts*) e unidades de armazenamento (*datastores*) distintos;

III - manter equipe técnica capacitada e suficiente para operacionalização das tecnologias disponibilizadas pelo provedor de serviços de nuvem;

IV - fornecer informações detalhadas sobre os servidores virtuais sob sua responsabilidade, incluindo versão de sistema operacional, aplicações em execução e versão de serviços;

V - gerir, configurar e manter sistema operacional, bancos de dados, sistemas, aplicações e demais serviços em execução nos servidores virtuais sob sua responsabilidade, eximindo totalmente o provedor de serviços de nuvem dessas atividades e responsabilidades;

VI - manter os servidores virtuais, sistemas e aplicações sob sua responsabilidade totalmente agnósticos à camada física de hardware, de forma que seja possível garantir a movimentação e compatibilidade dos servidores virtuais com os servidores físicos (*hosts*) e unidades de armazenamento (*datastores*) da Nuvem Corporativa Estadual;

VII - tomar medidas necessárias em resposta a manutenções programadas comunicadas pela Unidade Central de Tecnologia da Informação; e

VIII - corrigir ou mitigar vulnerabilidades de segurança identificadas pelo provedor de serviços de nuvem em seu parque de sistemas, aplicações e serviços publicados, dentro de um prazo adequado, e informar sobre impossibilidades técnicas da correção ou mitigação, apresentando soluções paliativas.

CAPÍTULO VII DAS VEDAÇÕES

Art. 13. Fica vedado aos órgãos e entidades da administração pública direta, autárquica e fundacional do Pode Executivo do Estado de Goiás, enquanto usuários dos serviços de computação em nuvem:

I - contratar salas-cofre, salas seguras, data centers e racks inteligentes, além de adquirir servidores, *appliances*, soluções de armazenamento ou outros recursos e soluções que possam ser disponibilizados por meio da Nuvem Corporativa Estadual;

II - manter sistemas operacionais, softwares e outras aplicações que estejam em seu ciclo final de vida, não sendo mais suportados ou atualizados pelo fabricante;

III - disponibilizar, utilizar, armazenar ou divulgar qualquer informação, dado ou material que viole leis, regulamentações ou possua direitos reservados e de propriedade intelectual; e

IV - transferir a terceiros ou permitir o uso dos serviços de computação em nuvem para benefício próprio, uma vez que tais serviços são exclusivamente para uso dos órgãos e entidades da administração pública do Poder Executivo estadual.

CAPÍTULO VIII
DO ACORDO DE NÍVEL DE SERVIÇO

Art. 14. A Unidade Central de Tecnologia da Informação, na qualidade de provedora de serviços de nuvem, compromete-se a manter o nível de disponibilidade do ambiente da Nuvem Corporativa Estadual em 99,4% (noventa e nove vírgula quatro por cento) ao longo de cada mês civil.

Art. 15. Para fins de apuração do nível de disponibilidade, não serão considerados os períodos de inatividade nas seguintes circunstâncias:

I - interrupções necessárias para ajustes técnicos ou manutenções programadas, previamente comunicadas, normalmente realizadas em horários noturnos ou de baixa utilização;

II - bloqueios temporários ou suspensões de operações visando preservar a segurança e a integridade do ambiente;

III - suspensão dos serviços de computação em nuvem por determinação de autoridades competentes, ou em caso de descumprimento por parte das Unidades Setoriais de Tecnologia da Informação de qualquer artigo desta Instrução Normativa;

IV - perda de performance que não resulte em indisponibilidade total do serviço de computação em nuvem; e

V - outros eventos não controláveis, provocados por agentes externos, caracterizados como força maior ou caso fortuito.

Art. 16. Para fins de atendimento do nível de disponibilidade acordado, o provedor de serviços de nuvem se compromete a restaurar o acesso ao ambiente da Nuvem Corporativa Estadual no prazo máximo de:

I - 2 (duas) horas úteis, no caso de indisponibilidade total do ambiente que gere impacto a todos os usuários dos serviços de computação em nuvem; e

II - 4 (quatro) horas úteis, no caso de indisponibilidade parcial do ambiente que ocasione perda de performance significativa dos serviços de computação em nuvem ou paradas intermitentes.

Parágrafo único. Para serviços em nuvem gerenciados pela Unidade Central de Tecnologia da Informação, mas hospedados em ambiente de nuvem pública, o nível de disponibilidade e os prazos de restauração dos serviços seguirão o disposto no Contrato de Prestação de Serviços.

CAPÍTULO IX
DA LIMITAÇÃO DE RESPONSABILIDADES

Art. 17. A Unidade Central de Tecnologia da Informação, enquanto provedora de serviços de nuvem, não será responsável por:

I - falhas decorrentes da não observância comprovada das instruções e recomendações expressamente fornecidas pelo provedor de serviços de nuvem;

II - falhas comprovadas em produtos e serviços não fornecidos ou mantidos pelo provedor de serviços de nuvem;

III - falhas resultantes do uso indevido dos recursos de computação em nuvem pelos usuários do serviço; e

IV - violações de dados e informações originadas de ações de funcionários, prepostos ou de pessoas autorizadas pelo órgão usuário do serviço de computação em nuvem, tampouco daquelas resultantes de atividades criminosas ou irregulares de terceiros, fora dos limites da previsibilidade técnica no momento em que ocorrerem.

Art. 18. A Unidade Central de Tecnologia da Informação não se responsabiliza por quaisquer perdas ou danos decorrentes do fornecimento, desempenho ou uso dos recursos de computação em nuvem e programas de software utilizados pelos órgãos e entidades estaduais, na condição de usuários dos serviços, mas não limitado a quaisquer danos indiretos, especiais ou incidentais, desde que comprovadamente tenha concorrido para o dano causado ao provedor de serviços de nuvem.

CAPÍTULO X
DA PRIVACIDADE E TRATAMENTO DOS DADOS

Art. 19. A Unidade Central de Tecnologia da Informação se compromete a:

I - manter a conformidade com a legislação vigente, especialmente observando os princípios legais estabelecidos na Lei Geral de Proteção de Dados - LGPD;

II - zelar pela privacidade e proteção dos dados pessoais dos titulares durante as operações de tratamento;

III - garantir o cumprimento das normas, diretrizes e melhores práticas relacionadas à proteção e privacidade de dados, alinhadas com as políticas internas e a LGPD; e

IV - manter e assegurar medidas técnicas e organizacionais para a proteção de dados em todas as operações, mitigando os riscos de acordo com a criticidade da informação.

CAPÍTULO XI
DAS DISPOSIÇÕES FINAIS

Art. 20. Compete à Unidade Central de Tecnologia da Informação revisar, atualizar e divulgar esta Política sempre que necessário.

Art. 21. Os casos omissos serão resolvidos pela Unidade Central de Tecnologia da Informação, por intermédio de suas unidades administrativas.

Art. 22. As empresas públicas e as sociedades de economia mista estaduais, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, poderão, mediante Acordo de Cooperação Técnica, utilizar os serviços de computação em nuvem conforme estabelecido nesta Instrução Normativa.

Art. 23. A Unidade Central de Tecnologia da Informação e os demais órgãos e entidades da administração pública do Poder Executivo estadual que utilizam dos recursos computacionais e soluções da Nuvem Corporativa Estadual terão o prazo de 180 (cento e oitenta) dias para tomar as providências necessárias para se adequarem aos requisitos e diretrizes estabelecidos nesta Instrução Normativa.

Art. 24. Esta Instrução Normativa entra em vigor na data de sua publicação.

Gabinete do Secretário-Chefe da Secretaria-Geral de Governo, aos 28 dias do mês agosto de 2024.

ADRIANO DA ROCHA LIMA
Secretário-Chefe da Secretaria-Geral de Governo

Protocolo 483957

Instrução Normativa nº 4/2024

Estabelece as diretrizes e padrões para utilização do Serviço de Correio Eletrônico Corporativo no âmbito da administração pública direta, autárquica e fundacional do Poder Executivo do Estado de Goiás.

O SECRETÁRIO-CHEFE DA SECRETARIA-GERAL DE GOVERNO, no uso das atribuições que lhe conferem os incisos I e II, § 1º do art. 40 da Constituição do Estado de Goiás; o inciso XIII do art. 5º e o caput c/c inciso I do § 2º do art. 108 da Lei estadual nº 21.792, de 16 de fevereiro de 2023; o inciso XIII do art. 2º, o inciso I do art. 75 e o inciso IV do art. 81 do Decreto estadual nº 10.355, de 05 de dezembro de 2023,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Ficam estabelecidos as diretrizes e padrões para utilização do Serviço de Correio Eletrônico Corporativo, nos termos desta Instrução Normativa, no âmbito da administração pública direta, autárquica e fundacional do Poder Executivo do Estado de Goiás.

Art. 2º As diretrizes e padrões previstos neste instrumento têm como objetivo principal garantir que o Serviço de Correio Eletrônico Corporativo seja utilizado exclusivamente para finalidades institucionais, assegurando a confiabilidade e a integridade dessa forma de comunicação oficial.

Art. 3º O uso do Serviço de Correio Eletrônico Corporativo, conforme disciplinado por esta Instrução Normativa, é de observância obrigatória pelos usuários e administradores do serviço.

Art. 4º A solução Microsoft Exchange Online, estabelecida como a tecnologia padrão para o Serviço de Correio Eletrônico Corporativo, está disponível para os usuários autorizados mediante contrato de licenciamento firmado entre a Unidade Central de Tecnologia da Informação e o fornecedor de produtos Microsoft.

Art. 5º O domínio de e-mail padrão a ser utilizado por todos os órgãos e entidades da administração pública direta, autárquica e fundacional do Poder Executivo do Estado de Goiás, no uso do Serviço de Correio Eletrônico Corporativo, é o "@goias.gov.br".

Parágrafo único. As Unidades Setoriais de Tecnologia da Informação deverão realizar as migrações e adequações necessárias em seus domínios e contas de e-mail, a fim de padronizar a identificação e comunicação dos usuários do Serviço de Correio Eletrônico Corporativo em seus respectivos órgãos ou entidades.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 6º Para os fins desta Instrução Normativa, considera-se:

I - administrador do Serviço de Correio Eletrônico Corporativo: unidade administrativa integrante da Unidade Central de Tecnologia da Informação responsável pela gestão, manutenção e operação do Serviço de Correio Eletrônico Corporativo;

II - assinatura de e-mail: texto automaticamente adicionado ao final de cada mensagem de e-mail enviada, contendo as informações básicas de identificação do remetente;

III - caixa de correio compartilhada: caixas postais usadas quando várias pessoas precisam acessar a mesma caixa de correio eletrônico, como uma unidade organizacional do órgão ou entidade, ou qualquer outra função compartilhada. As mensagens enviadas para uma caixa de correio compartilhada não aparecem na caixa de correio individual do usuário;

IV - caixa postal: área de armazenamento que contém as mensagens eletrônicas do usuário nos servidores do Serviço de Correio Eletrônico Corporativo;

V - conta de e-mail pessoal: conta destinada ao uso individual de pessoa com vínculo institucional, para tramitar informações exclusivamente relacionadas às atividades desempenhadas no órgão ou entidade;

VI - conta de e-mail administrativa: conta não personalizada, utilizada para representar unidades organizacionais, comissões, grupos de trabalho, entre outros, tratando de informações de interesse institucional representadas pela área envolvida;

VII - conta de e-mail de sistemas: conta utilizada por sistemas exclusivamente para envio de mensagens e alertas característicos da aplicação a qual se destina. Não possuem caixa postal, não recebem mensagens de e-mail e não possuem área de armazenamento de mensagens e anexos;

VIII - conta de recursos: conta de correio eletrônico dedicada a recursos físicos compartilhados, como salas de reunião ou projetores, que podem responder automaticamente a convites de agendamento de reunião usando regras pré-definidas;

IX - cota de e-mail: capacidade máxima de armazenamento da caixa postal eletrônica associada a uma conta de e-mail institucional, incluindo mensagens e seus anexos;

X - domínio de e-mail: nome exclusivo que aparece após o símbolo "@" nos endereços de correio eletrônico;

XI - endereço de correio eletrônico/e-mail: nome definido para a individualização e identificação de uma conta de e-mail, formado pelo identificador e pelo domínio, separados pelo símbolo "@";

XII - grupo de lista de distribuição de e-mail: endereço de e-mail que agrega um conjunto de endereços cadastrados, onde os usuários pertencentes ao grupo de lista de distribuição recebem uma cópia das mensagens enviadas para o endereço do grupo;

XIII - identificador: parte inicial do endereço de correio eletrônico, localizada antes do símbolo "@";

XIV - Microsoft Exchange Online: plataforma de correio eletrônico da Microsoft Corporation baseada em nuvem pública, que fornece e-mail, calendário, contatos e tarefas;

XV - Microsoft OneDrive: serviço de armazenamento de arquivos em nuvem da Microsoft Corporation, para compartilhamento e acesso online por meio de qualquer dispositivo;

XVI - Microsoft Sharepoint: plataforma colaborativa da Microsoft Corporation para gerenciamento de documentos, conteúdos, portais e aplicações web;

XVII - *phishing*: mensagens de correio eletrônico com conteúdo falso destinadas a enganar o usuário e obter informações pessoais ou institucionais restritas, ou acesso indevido a contas de e-mail/sistemas;

XVIII - Serviço de Correio Eletrônico Corporativo: serviço de tecnologia da informação disponibilizado pela Unidade Central de Tecnologia da Informação, que permite o envio e recebimento de mensagens eletrônicas, hospedado e mantido em nuvem computacional ou em servidores internos do Data Center Corporativo;

XIX - SPAM: mensagens eletrônicas indesejadas enviadas sem o consentimento do destinatário, geralmente associadas a propaganda de bens e serviços, mas que podem envolver práticas de *phishing* usadas por criminosos;

XX - Unidade Central de Tecnologia da Informação: unidade central que coordena a gestão de Tecnologia da Informação no âmbito do Estado de Goiás, atualmente, a Subsecretaria de Tecnologia da Informação, da Secretaria-Geral de Governo, com suas respectivas unidades básicas e complementares;

XXI - Unidade Setorial de Tecnologia da Informação: unidade administrativa, pertencente a órgão ou entidade estadual, responsável por atuar nas atividades de Tecnologia da Informação, sob o direcionamento técnico da Unidade Central de Tecnologia da Informação; e

XXII - usuários do Serviço de Correio Eletrônico Corporativo: servidores estatutários, comissionados e empregados públicos permanentes ou contratados por tempo determinado, todos em efetivo exercício, bem como estagiários e prestadores de serviços terceirizados que necessitam de acesso nas suas atividades laborais, atuando no âmbito da administração pública direta, autárquica e fundacional do Poder Executivo do Estado de Goiás.

CAPÍTULO III
DAS DIRETRIZES GERAIS

Art. 7º O Serviço de Correio Eletrônico Corporativo é destinado ao uso institucional, apoiando as atividades finalísticas e administrativas dos órgãos e entidades da administração direta, autárquica e fundacional do Poder Executivo do Estado de Goiás, devendo os usuários zelar pelo seu uso adequado.

Art. 8º Os órgãos e entidades do Poder Executivo estadual devem incentivar seus servidores a utilizarem o uso Serviço de Correio Eletrônico Corporativo no desempenho de suas atividades funcionais, visando à padronização da comunicação e ao aumento da produtividade.

§ 1º As mensagens enviadas pelo Serviço de Correio Eletrônico Corporativo devem seguir os padrões de redação oficial, adotando critérios de norma culta, linguagem simples e postura profissional.

§ 2º As mensagens devem conter a identificação do usuário emissor, por meio da assinatura de e-mail, incluindo nome completo, cargo ou função, dados da unidade e órgão de lotação e informações de contato.

§ 3º Os usuários devem se abster de enviar e-mails sem texto no corpo e sem título no campo de assunto.

Art. 9º O acesso ao Serviço de Correio Eletrônico Corporativo será concedido de forma pessoal e intransferível, sendo o usuário o único responsável pelo seu uso.

Parágrafo único. Cada usuário tem direito a apenas uma caixa postal.

Art. 10. Será concedido acesso ao Serviço de Correio Eletrônico Corporativo para:

I - servidores estatutários, comissionados e empregados públicos permanentes ou contratados por tempo determinado desde que em efetivo exercício; e

II - estagiários e prestadores de serviços terceirizados que necessitam de acesso ao serviço nas suas atividades laborais.

Parágrafo único. Aos servidores cedidos para órgão ou entidade que não integre o Poder Executivo estadual não será concedido ou mantido acesso ao Serviço de Correio Eletrônico Corporativo.

Art. 11. O Serviço de Correio Eletrônico Corporativo é hospedado em nuvem pública, administrado pela Unidade Central de Tecnologia da Informação, podendo, excepcionalmente, ser hospedado no Data Center Corporativo.

§ 1º As novas contas de e-mail pessoal e administrativa serão criadas, preferencialmente, em ambiente de nuvem pública.

§ 2º As novas contas de e-mail de sistemas serão criadas, exclusivamente, em ambiente do Data Center Corporativo.

Art. 12. As contas de e-mail podem ser auditadas e estão sujeitas a monitoramento e rastreamento de segurança, com observância ao disposto na Lei nº 13.709, de 2018 - Lei Geral de Proteção de Dados Pessoais.

CAPÍTULO IV
DO FORNECIMENTO E MANUTENÇÃO DAS CONTAS DE E-MAIL

Art. 13. O Serviço de Correio Eletrônico Corporativo é fornecido, administrado e mantido pela Unidade Central de Tecnologia da Informação, por intermédio dos administradores do serviço, responsáveis pela criação e gestão das contas de correio eletrônico e demais configurações avançadas do serviço.

§ 1º As solicitações para criação de contas de e-mail devem ser encaminhadas à Unidade Central de Tecnologia da Informação via sistema de abertura de chamados, contendo os dados cadastrais dos usuários.

§ 2º Poderá ser delegada às Unidades Setoriais de Tecnologia da Informação a operacionalização de determinadas funcionalidades e recursos básicos do Serviço de Correio Eletrônico Corporativo, relacionadas aos usuários de seu órgão ou entidade, desde que tais permissões não gerem impacto negativo no ambiente.

Art. 14. As contas de e-mail são criadas conforme padrões de nomenclatura determinados pela Unidade Central de Tecnologia da Informação.

Art. 15. As contas de e-mail administrativas solicitadas pelas unidades organizacionais formais da estrutura administrativa do Poder Executivo estadual são criadas no formato "unidadeorganizacional.orgao@goias.gov.br".

§ 1º A conta de e-mail administrativa mencionada no caput deste artigo é do tipo caixa de correio compartilhada e deve ser acessada por meio de delegação de acesso ao usuário titular da unidade organizacional, que é o seu responsável.

§ 2º Demais usuários podem ter acesso à caixa de correio compartilhada da unidade administrativa, desde que devidamente autorizados pelo titular.

§ 3º Poderão, excepcionalmente, ser criadas contas de e-mail administrativas temáticas, referentes a comissões, grupos de trabalho, demandas de trabalho específicas ou eventos temporários, mediante requerimento fundamentado encaminhado à Unidade Central de Tecnologia da Informação, informando o usuário responsável pela conta, que será do tipo compartilhada.

Art. 16. Os sistemas informatizados podem ter conta de e-mail, criada no formato "sistema.orgao@sistemas.goias.gov.br".

Parágrafo único. As contas de e-mail de sistemas não possuem caixa postal, sendo sua finalidade exclusiva para o envio de avisos, notificações e alertas.

Art. 17. Os prestadores de serviços terceirizados podem possuir contas de e-mail funcionais, criadas no domínio "@ fornecedores.goias.gov.br".

Art. 18. Podem ser criadas contas de recursos, atribuídas a salas de reuniões, laboratórios, salas de treinamento, equipamentos, entre outros, com a finalidade de controle de agenda e utilização compartilhada.

Art. 19. É permitida a criação de grupos de lista de distribuição com endereços de e-mail internos, visando facilitar e otimizar a troca de informações sobre assuntos de interesse institucional.

Art. 20. O acesso do usuário ao Serviço de Correio Eletrônico Corporativo será encerrado no prazo de até 10 (dez) dias corridos quando:

I - ocorrer a perda de vínculo com a administração pública direta, autárquica e fundacional ou com a empresa terceirizada contratada;

II - ocorrer o afastamento, não considerado como de efetivo exercício, ou cessão do servidor para outro órgão ou entidade que não integre o Poder Executivo estadual; e

III - ocorrer a desativação da credencial de acesso.

§ 1º Cabe à Unidade Setorial de Tecnologia da Informação solicitar ao administrador do Serviço de Correio Eletrônico a remoção imediata do acesso à conta de e-mail, quando da ocorrência de qualquer uma das situações elencadas no caput deste artigo.

§ 2º Os dados das contas de e-mail serão definitivamente excluídos após 30 (trinta) dias do encerramento do acesso do usuário ao Serviço de Correio Eletrônico Corporativo.

Art. 21. A suspensão e/ou exclusão da conta de e-mail não exime o usuário de suas responsabilidades perante a lei, políticas e normas vigentes, por qualquer ato decorrente do uso indevido e/ou inadequado de sua conta.

CAPÍTULO V
DOS LIMITES DE UTILIZAÇÃO

Art. 22. O acesso ao correio eletrônico deve ser realizado por meio de navegador para internet ou por dispositivos móveis através do aplicativo Outlook para iOS ou Android.

Parágrafo único. O acesso deve ser realizado obrigatoriamente com múltiplo fator de autenticação, sendo a habilitação e configuração deste recurso de segurança em dispositivos móveis, pessoais ou não, de responsabilidade do usuário.

Art. 23. O espaço de armazenamento padrão das contas de e-mail pessoais e administrativas é de 50 GB (cinquenta gigabytes), sem possibilidade de aumento deste limite.

Parágrafo único. Caso o limite estabelecido no caput deste artigo seja alcançado e seja necessário mais espaço de armazenamento, o usuário deverá adotar medidas para otimização do uso, como realizar a limpeza das mensagens de e-mails antigas ou desnecessárias, ou utilizar o Microsoft OneDrive pessoal para armazenar os anexos das mensagens de e-mail.

Art. 24. O tamanho máximo permitido para anexos nas mensagens é de 100 MB (cem megabytes).

§ 1º O tamanho máximo permitido para anexos nas mensagens é de 30 MB (trinta megabytes) quando enviado por meio do aplicativo Outlook para iOS e Android em dispositivos móveis.

§ 2º Caso seja necessário o envio de anexos com tamanho superior aos limites estabelecidos, estes deverão ser compartilhados por meio de soluções de armazenamento em nuvem, como o Microsoft Sharepoint ou OneDrive.

§ 3º O número máximo de anexos permitidos em uma única mensagem de e-mail é de 250 (duzentos e cinquenta) arquivos.

Art. 25. Os limites de envio de mensagens de e-mail por meio do Serviço de Correio Eletrônico Corporativo são:

I - quantidade máxima de destinatários por dia: até 10.000 (dez mil); e

II - quantidade máxima de destinatários por mensagem de e-mail: até 1.000 (um mil) nos campos “Para:”, “Cc:” e “Cco:”.

Parágrafo único. Nos casos em que houver necessidade de envio de grande quantidade de e-mails com conteúdo institucional, acima dos limites estabelecidos, deverão ser contratados provedores de terceiros especializados em serviços de envio de e-mails em massa.

Art. 26. As mensagens de e-mail suspeitas de SPAM serão enviadas para a pasta de Lixo Eletrônico, onde permanecerão por um período de 30 (trinta) dias, sendo permanentemente excluídas de forma automática após este período.

Parágrafo único. A classificação das mensagens de e-mail como SPAM é realizada automaticamente por ferramentas especializadas.

Art. 27. As mensagens de e-mail e os seus anexos podem ser bloqueados, rejeitados ou liberados de acordo com os critérios estabelecidos nesta Instrução Normativa e conforme as regras de filtragem de conteúdo, visando manter a integridade do Serviço de Correio Eletrônico Corporativo.

Art. 28. As mensagens de e-mail excluídas pelo usuário serão enviadas para a pasta “Itens Excluídos”, onde ficarão retidas indefinidamente, podendo ser recuperadas a qualquer momento pelo usuário.

Parágrafo único. Quando o usuário excluir permanentemente as mensagens de e-mail da pasta “Itens Excluídos” e da pasta “Lixo Eletrônico”, estas não poderão ser recuperadas.

CAPÍTULO VI
DOS DEVERES E RESPONSABILIDADES

Art. 29. São deveres e responsabilidades da Unidade Central de Tecnologia da Informação, no papel de administradora do Serviço de Correio Eletrônico Corporativo:

I - disponibilizar o Serviço de Correio Eletrônico Corporativo a todos os usuários da administração pública direta, autárquica e fundacional do Poder Executivo estadual, conforme estabelecido nesta Instrução Normativa, observando as melhores práticas de mercado;

II - estabelecer um modelo de gestão que contempla a coordenação, o planejamento, a manutenção, a administração, a divulgação, o controle e o monitoramento do uso do Serviço de Correio Eletrônico Corporativo;

III - definir os padrões e requisitos para cadastramento, concessão, utilização, bloqueio ou exclusão das contas de correio eletrônico, listas de distribuição e demais recursos;

IV - zelar pelo atendimento aos princípios da segurança, integridade, sigilo e disponibilidade dos serviços e dados transmitidos por meio do Serviço de Correio Eletrônico Corporativo;

V - manter serviço de proteção contra vírus e mensagens não solicitadas (SPAM), bloqueando automaticamente mensagens e anexos que impliquem riscos à segurança da informação;

VI - bloquear de forma imediata contas de e-mail identificadas como comprometidas, cabendo ao usuário providenciar e executar as recomendações emitidas pelo administrador do Serviço de Correio Eletrônico;

VII - suspender, motivadamente, o envio de mensagens a partir de uma conta de correio eletrônico quando constatada infringência desta Instrução Normativa pelo respectivo usuário; e

VIII - acompanhar e garantir o cumprimento das diretrizes e padrões dispostos nesta Instrução Normativa.

Art. 30. São deveres e responsabilidades dos usuários do Serviço de Correio Eletrônico Corporativo:

I - utilizar o Serviço de Correio Eletrônico Corporativo exclusivamente para a troca de mensagens e documentos relacionados a assuntos institucionais, preservando a segurança das informações organizacionais;

II - gerenciar compromissos, contatos, tarefas, arquivos e atividades de sua conta de e- mail pessoal e das contas de e-mail administrativas sob sua responsabilidade;

III - manter sigilo de sua senha de acesso ao correio eletrônico, visto que esta senha é de uso pessoal e intransferível;

IV - verificar periodicamente o conteúdo de sua conta de e-mail pessoal e das contas de e-mail administrativas sob sua responsabilidade, considerando que o correio eletrônico é uma das formas oficiais de comunicação da administração pública do Poder Executivo estadual;

V - enviar mensagens de e-mail somente aos destinatários relacionados com o assunto, evitando sobrecarregar a caixa de entrada dos demais usuários;

VI - utilizar sempre que possível, no envio de mensagens de e-mail para vários destinatários, o campo “Com cópia oculta - Cco”, de forma a não identificar os endereços de e-mails dos demais destinatários;

VII - comunicar imediatamente a sua Unidade Setorial de Tecnologia da Informação e ao administrador do Serviço de Correio Eletrônico Corporativo qualquer ocorrência que não esteja alinhada ao cumprimento desta Instrução Normativa;

VIII - excluir periodicamente mensagens de e-mails antigas ou desnecessárias, inclusive e-mails da pasta de “Itens Excluídos”, para evitar que sua cota de e-mail seja atingida;

IX - delegar, por necessidade de serviço, funções relativas a sua conta de e-mail e calendário a outros usuários;

X - configurar, quando necessário, resposta automática de e-mail durante suas férias ou demais afastamentos legais, para comunicar a data de retorno e o contato dos responsáveis durante a ausência; e

XI - observar e fazer cumprir as diretrizes e padrões definidos nesta Instrução Normativa.

CAPÍTULO VII DAS VEDAÇÕES

Art. 31. É vedado aos usuários do Serviço de Correio Eletrônico Corporativo:

I - utilizar o endereço eletrônico em cadastros de sites na internet que não sejam de interesse institucional, a fim de reduzir os riscos de SPAM;

II - enviar, armazenar ou encaminhar mensagens de e-mail com conteúdo obsceno, ilegal, antiético, ofensivo, preconceituoso ou discriminatório, assim como material protegido por leis de propriedade intelectual;

III - enviar mensagens não solicitadas para múltiplos destinatários, distribuindo propaganda, entretenimento, correntes e outros temas similares que não sejam de interesse específico do órgão ou entidade;

IV - enviar mensagens de e-mail divulgando informações classificadas como sigilosas a usuários não autorizados, sem a expressa autorização dos respectivos proprietários dessas informações;

V - disseminar vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções ou que possa ser considerado nocivo às estações de trabalho e ao Serviço de Correio Eletrônico Corporativo;

VI - forjar ou tentar forjar mensagens de e-mail, ou disfarçar ou tentar disfarçar sua identidade ao enviar uma mensagem;

VII - disseminar catálogos de endereços de e-mail institucionais ou listas de contato dos servidores;

VIII - veicular mensagens de e-mail para fins pessoais, comerciais, político-partidárias, religiosos, associativos, entre outros diversos da utilização institucional;

IX - encaminhar mensagens de e-mail institucionais para contas de e-mail hospedadas em serviços de correio eletrônico públicos ou de terceiros;

X - realizar o envio de grande quantidade de mensagens de e-mail, ou e-mails em massa com muitos destinatários, de forma a impactar na capacidade técnica do Serviço de Correio Eletrônico ou gerar reclamações por parte dos destinatários;

XI - utilizar uma conta de e-mail de sistemas para envio de mensagens de e-mail de forma diversa ao qual foi destinada, bem como reaproveitar uma conta de e-mail de sistemas para envio de mensagens por outro sistema;

XII - compartilhar suas credenciais de acesso e outros métodos de autenticação da solução; e

XIII - responder a mensagens de e-mail recebidas com conteúdo não institucional ou de remetentes desconhecidos, nem mesmo para solicitar o cancelamento da inscrição do envio de e-mail.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Art. 32. Os usuários do Serviço de Correio Eletrônico Corporativo que o utilizarem incorretamente, infringindo as disposições legais e determinações contidas nesta Instrução Normativa, estarão sujeitos às seguintes sanções, sem prejuízo de suas responsabilidades administrativas, civis e penais:

I - notificação por e-mail, com cópia ao superior imediato, mediante reclamação de algum dos destinatários ou iniciativa do administrador do Serviço de Correio Eletrônico Corporativo; e

II - persistindo o uso indevido, solicitar-se-á apuração da eventual responsabilidade.

Art. 33. Compete à Unidade Central de Tecnologia da Informação revisar, atualizar e divulgar esta Instrução Normativa sempre que necessário.

Art. 34. Os casos omissos serão resolvidos pela Unidade Central de Tecnologia da Informação.

Art. 35. As empresas públicas e as sociedades de economia mista estaduais, ao operacionalizarem políticas públicas e no âmbito da execução delas, poderão utilizar o Serviço de Correio Eletrônico Corporativo disposto nesta Instrução Normativa, mediante Acordo de Cooperação Técnica.

Art. 36. A Unidade Central de Tecnologia da Informação e os demais órgãos e entidades da administração pública do Poder Executivo estadual que utilizam do Serviço de Correio Eletrônico Corporativo terão o prazo de 180 (cento e oitenta) dias para adequarem às diretrizes e padrões definidos nesta Instrução Normativa.

Art. 37. Ficam revogados:

I - a Resolução nº 2, de 30 de junho de 2022, expedida pelo Comitê Estadual de Tecnologia da Informação e Comunicação (CETIC); e

II - as disposições em contrário dos atos anteriores emitidos pelos órgãos e entidades do Poder Executivo estadual sobre o tema.

Art. 38. Esta Instrução Normativa entra em vigor na data de sua publicação.

Gabinete do Secretário-Chefe da Secretaria-Geral de Governo, aos 28 dias de agosto de 2024.

ADRIANO DA ROCHA LIMA
Secretário-Chefe da Secretaria-Geral de Governo

Protocolo 483962

Instrução Normativa nº 03/2024

Institui Política de Backup e Recuperação de Dados Digitais da Nuvem Corporativa Estadual no âmbito da Administração Pública direta, autárquica e fundacional do Poder Executivo do Estado de Goiás.

O SECRETÁRIO-CHEFE DA SECRETARIA-GERAL DE GOVERNO, no uso das atribuições que lhe conferem os incisos I e II, § 1º do art. 40 da Constituição do Estado de Goiás; o inciso XIII do art. 5º e o caput c/c inciso I do § 2º do art. 108 da Lei estadual nº 21.792, de 16 de fevereiro de 2023; o inciso XIII do art. 2º, o inciso I do art. 75 e o inciso V do art. 81, do Decreto estadual nº 10.355, de 05 de dezembro de 2023,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Política de Backup e Recuperação de Dados Digitais da Nuvem Corporativa Estadual, nos termos desta Instrução Normativa, no âmbito da Administração Pública direta, autárquica e fundacional do Poder Executivo do Estado de Goiás.

Art. 2º Esta Instrução Normativa tem por objetivo criar diretrizes, requisitos básicos, responsabilidades e competências que visam à segurança, à proteção, à integridade e à disponibilidade dos dados digitais sob custódia da Unidade Central de Tecnologia da Informação, para se manter a continuidade do negócio.

Art. 3º A salvaguarda e recuperação dos dados digitais abrange exclusivamente dados armazenados na infraestrutura de tecnologia da informação da Nuvem Corporativa Estadual, mantida e gerida pela Unidade Central de Tecnologia da Informação.

Parágrafo único. Não serão salvaguardados nem recuperados dados armazenados localmente nos microcomputadores dos usuários ou em quaisquer outros sistemas que porventura estiverem hospedados fora da Nuvem Corporativa Estadual, ficando sob a responsabilidade do usuário a cópia de seus dados locais para os servidores de armazenamento de arquivos.

Art. 4º A salvaguarda dos dados em formato digital pertencentes a serviços de computação em nuvem disponibilizados pela Unidade Central de Tecnologia da Informação, mas hospedados em ambiente de nuvem pública, seguirá as políticas e definições acordadas nos contratos de prestação de serviço que formalizem a relação entre os envolvidos, e serão informadas em Plano de Backup específico.

Art. 5º A Unidade Central de Tecnologia da Informação se reserva ao direito de realizar, a qualquer momento, a exclusão de recursos ou dados digitais das rotinas de backup, ou alteração nos tempos de retenção, mediante justa necessidade técnica, que deve ser previamente informada ao Proprietário da Informação, e atualizada no Plano de Backup relacionado.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 6º Para os fins desta Instrução Normativa, considera-se:

I - administrador de backup: unidade administrativa integrante da Unidade Central de Tecnologia da Informação, responsável pelo planejamento de soluções de backup, definição de padrões, configurações e atendimento avançado de resolução de incidentes e problemas referentes a backups;

II - backup ou cópia de segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação em caso de perda ou alteração dos dados originais;

III - backup completo: estratégia de backup que promove a cópia de segurança completa de todos os dados de um sistema computacional para um repositório de dados, in-

dependentemente de terem sido ou não alterados desde o último backup;

IV - backup diferencial: estratégia de backup que promove a cópia de segurança somente dos dados novos ou modificados de um sistema computacional desde o último backup completo;

V - backup incremental: estratégia de backup que promove a cópia de segurança somente dos dados novos ou modificados de um sistema computacional desde o último backup, independente da modalidade;

VI - backup on-site: cópia de segurança que, uma vez realizada, é acessível dentro do mesmo Data Center;

VII - backup off-site: cópia de segurança que, uma vez realizada, é armazenada em outro Data Center geograficamente separado ou em serviço de backup em nuvem;

VIII - custódia: consiste na responsabilidade de guardar um ativo para terceiros, sem permitir acesso automático ou o direito de conceder acesso a outros;

IX - disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

X - janela de backup: período durante o qual cópias de segurança sob execução agendada poderão ser executadas;

XI - integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XII - Nuvem Corporativa Estadual: infraestrutura tecnológica capaz de suportar demandas de hospedagem de serviços de computação em nuvem, processados e armazenados nos Data Centers estaduais e em ambiente de nuvem pública e privada, sob gestão e operacionalização da Unidade Central de Tecnologia da Informação;

XIII - plano de backup: planejamento que detalha a execução da Política de Backup, no qual são informados os requisitos e as rotinas/roteiros de backup de cada conjunto de dados ou informação a serem salvaguardados;

XIV - proprietário da informação: área interessada do órgão ou indivíduo legalmente instituído por sua posição ou cargo, que é responsável primário pela viabilidade e sobrevivência da informação, e que pode requisitar a restauração dos dados digitais por ele gerenciados;

XV - *Recovery Point Objective* (RPO): ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente;

XVI - *Recovery Time Objective* (RTO): tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados, após um incidente;

XVII - repositório de dados de backup: unidade de armazenamento com características específicas para retenção de cópia de segurança de dados digitais;

XVIII - restauração: processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de backup;

XIX - retenção: período pelo qual os dados devem ser salvaguardados e estarem aptos à

restauração; backup;
estado anterior;
XX
XXI - rotina/roteiro de backup: conjunto de procedimentos utilizados para se realizar um XXI - snapshot: ponto de restauração de máquinas virtuais que permite o retorno a um XXII - Unidade Central de Tecnologia da Informação: unidade central que coordena a

gestão de Tecnologia da Informação no âmbito do Estado de Goiás, atualmente, a Subsecretaria de Tecnologia da Informação, da Secretaria-Geral de Governo, com suas respectivas unidades básicas e complementares; e

XXIII - Unidades Setoriais de Tecnologia da Informação: unidade administrativa, pertencente a órgão ou entidade estadual, responsável por atuar nas atividades de Tecnologia da Informação, sob o direcionamento técnico da Unidade Central de Tecnologia da Informação.

CAPÍTULO III DAS DIRETRIZES

Art. 7º São diretrizes da Política de Backup e Recuperação de Dados Digitais da Nuvem Corporativa Estadual:

I - assegurar o acesso continuo às informações definidas por esta Instrução Normativa, por meio de procedimentos para backup e restauração que observem criteriosamente o modo e a periodicidade de cada cópia de segurança dos dados;

II - garantir que todos os sistemas de informação críticos façam parte da rotina de backup, para um restabelecimento completo e no menor tempo possível, assegurando a continuidade do negócio em caso de desastres;

III - prover resiliência dos dados por meio do armazenamento de diversas cópias de backup dos dados originais, espalhadas por repositórios de dados diferentes e replicadas, e armazenadas remotamente em localidade geograficamente distante e segura;

IV - certificar que as rotinas de backup possuam requisitos mínimos diferenciados de acordo com o tipo de serviço, recurso ou dado salvaguardado, dando prioridade aos serviços ou recursos definidos como críticos pelos proprietários da informação;

V - atestar que as rotinas de backup utilizem soluções próprias e especializadas para este fim, de forma que as tarefas de backup sejam realizadas de forma automatizada, assim como as rotinas de testes de integridade e recuperabilidade; e

VI - resguardar que as rotinas de backup atendam aos requisitos mínimos de segurança da informação e demais requisitos legais e normativos, especialmente os relacionados à Lei Geral de Proteção de Dados Pessoais - LGPD, Lei federal nº 13.709, de 14 de agosto de 2018, e à norma ABNT NBR ISO/IEC 27002:2013.

CAPÍTULO IV
DAS FERRAMENTAS DE BACKUP

Art. 8º As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, que possuam funcionalidades de automatização das rotinas, e de realização de testes de integridade e recuperabilidade dos dados digitais protegidos.

Art. 9º Os equipamentos, softwares e demais componentes envolvidos no processo de backup são considerados ativos críticos para a Unidade Central de Tecnologia de Informação.

CAPÍTULO V
DA FREQUÊNCIA E RETENÇÃO DOS DADOS

Art. 10. As rotinas de backup do ambiente da Nuvem Corporativa Estadual devem ser realizadas com a frequência diária, incluindo finais de semana e feriados.

Parágrafo único. Deverá ser avaliado pelo proprietário da informação, em conjunto com o administrador de backup, a necessidade de realização de cópias de segurança dos dados digitais em frequência menor que a diária, conforme a criticidade do serviço ou recurso.

Art. 11. Os serviços e recursos hospedados na Nuvem Corporativa Estadual devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/tempo de retenção de dados/RPO e RTO estabelecida a seguir:

I - Frequência: Diária;

II - Tempo de Retenção de Dados: 4 (quatro) semanas;

III - *Recovery Point Objective* (RPO): 24 (vinte e quatro) horas; e IV - *Recovery Time Objective* (RTO): 4 (quatro) horas.

Art. 12. Poderão ser estabelecidos frequência, tempo de retenção, RPO e RTO diferenciados para cada sistema de informação ou dados digitais, de acordo com o nível de criticidade,

mediante solicitação formal e justificativa motivada do proprietário da informação.

Art. 13. Poderão ser realizados, mediante solicitação e justificativa formal, backups extras individualizados, de forma a atender demandas específicas e excepcionais, à exemplo de necessidades legais ou de litigio de maior tempo de retenção, mudanças e manutenções no ambiente, ou desativação de servidores virtuais que requeiram um tempo maior de retenção dos dados digitais para possíveis auditorias futuras.

Art. 14. A recuperação de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança.

Art. 15. Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de backup.

Art. 16. Na ocorrência de falha ou incompletude de alguma rotina de backup, uma nova rotina deve ser executada visando ao armazenamento, sendo que o administrador de backup deve identificar a causa da falha e adotar ação corretiva antes da execução da próxima rotina agendada.

Art. 17. O *Recovery Time Objective* (RTO) desta Instrução Normativa refere-se a incidentes ou falhas que não afetam de maneira significativa o ambiente computacional, não se aplicando a situações de desastres causados por eventos incontroláveis, classificados como força maior ou caso fortuito, que afetem todo ou grande parte do ambiente.

CAPÍTULO VI
DO PLANO DE BACKUP

Art. 18. O plano de backup deve conter as rotinas de backup para cada grupo de serviço ou recurso que armazene dados digitais, cumprindo as diretrizes desta Política, refletindo os requisitos de negócio do órgão ou entidade, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

I - escopo do plano de backup: definir quais os dados digitais a serem salvaguardados e quaisquer exceções ao escopo definido;

II - tipo do backup: definir a estratégia da cópia dos dados digitais, como completo, incremental ou diferencial;

III - frequência de realização: definir a periodicidade como diária, semanal, mensal ou

anual;

requisitos legais; segurança;

IV

V - tempo de retenção: definir o tempo de acordo com o nível de criticidade ou V - janela de backup: definir o período preferencial para a execução das cópias de VI - RPO: definir o prazo máximo aceitável de perda de dados em caso de incidente;

VII - RTO: definir o prazo máximo aceitável de inoperância dos serviços de TI até a

restauração dos dados após um incidente;

VIII - repositório de dados de backup: informar as unidades de armazenamento e locais seguros, diferentes do local original, e a replicação dos dados;

IX - estratégia de backup: informar as tecnologias e soluções que serão utilizadas na execução das cópias de segurança, e como se dará o monitoramento dos resultados das rotinas;

X - procedimentos de teste de integridade: detalhar os procedimentos de teste de recuperação das cópias de segurança para detectar tempestivamente eventuais falhas lógicas e físicas;

XI - periodicidade do teste de integridade: informar o período regular de teste de restauração das cópias de segurança, conforme definido nesta Política;

XII - procedimento de restauração: detalhar os procedimentos para realizar a restauração das cópias de segurança, quando necessário;

XIII - requisitos de segurança da informação: definir os controles de acesso lógico, uso de criptografia, imutabilidade, entre outros;

XIV - requisitos legais e normativos: informar, caso aplicável, as legislações, regulamentações de conformidade ou de litigio que determinam tempo de retenção diferenciado para os dados salvaguardados ou determinada frequência de backup; e

XV - aprovação: aprovação e assinatura dos responsáveis pela execução e gestão das rotinas de backup, bem como das demais partes interessadas.

Art. 19. Os planos de backup devem ser aprovados pelo administrador de backup, comunicados às partes interessadas (Unidades Setoriais de TI e proprietários das informações) e devidamente publicados e disponibilizados.

CAPÍTULO VII
DA JANELA DE EXECUÇÃO DAS ROTINAS DE BACKUP

Art. 20. A execução das rotinas de backup deve ser concentrada, preferencialmente, no período definido como janela de backup.

Parágrafo único. Para definição da janela de backup, deve-se considerar o impacto das rotinas de backup no desempenho da rede computacional, garantindo que o tráfego necessário não cause indisponibilidade dos recursos computacionais e sistemas durante o horário de expediente.

Art. 21. O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com o proprietário da informação.

CAPÍTULO VIII
DOS REPOSITÓRIOS DE DADOS DE BACKUP

Art. 22. As unidades de armazenamento utilizadas como repositórios de dados de backup devem considerar as seguintes características dos dados resguardados:

I - criticidade dos dados salvaguardados;

II - requisitos de segurança da informação; III - tempo de retenção dos dados;

IV - probabilidade de necessidade de restauração; V - tempo esperado para restauração;

VI - custo de aquisição das unidades de armazenamento de backup; e VII - vida útil da unidade de armazenamento de backup.

Art. 23. As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade e temperatura, e com acesso restrito a pessoas autorizadas pelo administrador de backup.

Art. 24. A execução das rotinas de backup deve prever a ampliação da capacidade dos dispositivos envolvidos no armazenamento.

Art. 25. O administrador de backup deve avaliar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

Art. 26. Podem ser utilizadas técnicas de compressão e deduplicação de dados, desde que o acréscimo no tempo de backup e de recuperação dos dados seja considerado aceitável.

Art. 27. Os backups devem ter, no mínimo, 2 (duas) cópias realizadas em repositórios de dados distintos, sendo uma on-site e outra off-site.

Art. 28. Os backups que contenham dados sensíveis e que requeiram tratamento específico quanto à segurança da informação devem ser criptografados e ter seus acessos devidamente controlados.

Art. 29. Os repositórios de backup devem possuir funcionalidade de imutabilidade, fornecendo proteção adicional contra possíveis ataques de *ransomware*.

Art. 30. Os repositórios de backup devem ser fisicamente separados do ambiente dos dados digitais de produção, sendo utilizados exclusivamente para a salvaguarda dos dados digitais, sem compartilhamento de recursos para outras finalidades.

Art. 31. A vida útil das unidades de armazenamento que compõem os repositórios de backup deve ser de, no mínimo, 5 (cinco) anos.

Art. 32. Quando houver necessidade de descarte de unidades de armazenamento de backups, estas devem ser logicamente destruídas para garantir a inutilização e sanitização dos dados, observando-se práticas de descarte sustentável e ambientalmente corretas.

CAPÍTULO IX
DOS TESTES DE INTEGRIDADE DE BACKUP

Art. 33. Os backups devem ser testados periodicamente para garantir sua confiabilidade e a integridade dos dados salvaguardados.

Art. 34. O administrador de backup deve elaborar um cronograma de testes, priorizando os backups mais importantes para a continuidade das rotinas de trabalho, conforme o nível de criticidade ou relevância dos dados, aplicações e sistemas, com o conhecimento e concordância do proprietário da informação.

§ 1º Após uma restauração bem-sucedida, o proprietário da informação deve realizar os testes de validação da integridade dos dados.

§ 2º O teste de integridade será considerado válido quando o ambiente original puder ser recriado em um estado consistente.

§ 3º Ações corretivas devem ser tomadas sempre que problemas de backup forem identificados durante os testes de integridade, visando reduzir os riscos associados a backups falhos.

§ 4º Os resultados dos testes de integridade devem ser devidamente documentados.

Art. 35. Os testes de restauração e integridade dos backups de dados digitais categorizados como críticos devem ser realizados quadrimestralmente, enquanto os de dados não críticos devem ser realizados, no mínimo, anualmente.

Art. 36. Os testes de restauração e integridade dos backups devem ser realizados por amostragem, em equipamentos servidores diferentes dos que atendem os ambientes de produção, considerando os recursos humanos e tecnológicos disponíveis.

Parágrafo único. Sempre que possível, os testes de restauração e integridade dos backups devem ser realizados de forma automática, simulando um ambiente produtivo e realizando as devidas validações customizadas pelo proprietário da informação.

Art. 37. A periodicidade, a abrangência, os procedimentos e as rotinas dos testes de integridade serão definidos no plano de backup.

CAPÍTULO X
DAS RESPONSABILIDADES

Art. 38. São atribuições da Unidade Central de Tecnologia da Informação, por intermédio dos administradores de backup:

I - garantir a disponibilização de infraestrutura e recursos adequados para a realização dos procedimentos de backup;

II - apresentar soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela Unidade Central de Tecnologia da Informação;

III - propor modificações visando o aperfeiçoamento desta Política de Backup e Recuperação de Dados Digitais da Nuvem Corporativa Estadual;

IV - elaborar os planos de backup específicos para cada grupo de serviço ou recurso que armazene dados digitais;

V - providenciar a criação e manutenção das rotinas de backup;

VI - gerir e manter os componentes e ferramentas envolvidas nas rotinas de backup;

VII - preservar, manter funcionais e garantir a segurança dos repositórios de dados de backup;

VIII - realizar a execução dos testes de integridade e restauração;

IX - providenciar a recuperação dos backups em caso de necessidade;

X - implementar e manter procedimentos de controle de acesso e segurança da informação para garantir ao máximo o não vazamento das informações;

XI - tratar e zelar pela segurança dos dados salvaguardados, de acordo com os princípios e diretrizes da Lei Geral de Proteção de Dados Pessoais - LGPD;

XII - disponibilizar informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos backups;

XIII - providenciar a verificação diária dos eventos gerados pela solução de backup, tomando as providências necessárias para remediar eventuais falhas;

XIV - sanar dúvidas técnicas do proprietário da informação e das Unidades Setoriais de Tecnologia da Informação acerca das informações salvaguardadas;

XV - manter profissionais com alto grau de conhecimento sobre as ferramentas e componentes da solução de backup, com capacidade de realizar ajustes finos no ambiente conforme as melhores práticas de mercado; e

XVI - promover medidas preventivas para evitar falhas nas rotinas de backup. Art. 39. São atribuições dos proprietários da informação:

I - informar, mediante justificativa formal e motivada, quais serviços e dados necessitam de rotina de backup diferente do padrão estabelecido nesta Instrução Normativa, especificando o escopo de dados, a frequência e o tempo de retenção apropriados, e demais informações relevantes; e

II - providenciar a validação, negocialmente, do resultado das restaurações solicitadas e dos testes de restauração dos backups dos dados sob sua responsabilidade.

Art. 40. São atribuições das Unidades Setoriais de Tecnologia da Informação:

I - analisar e encaminhar à Unidade Central de Tecnologia da Informação as solicitações e justificativas dos proprietários da informação referentes às necessidades de rotinas de backup e restaurações;

II - garantir que quaisquer procedimentos programados nos servidores virtuais sob sua responsabilidade, que impliquem em riscos de funcionamento ou perda de informação, sejam executados somente após a realização de snapshot ou backup desses servidores;

III - assegurar que, no âmbito de seu órgão ou entidade, os usuários armazenem os documentos institucionais nos servidores de armazenamento da Nuvem Corporativa Estadual; e

IV - submeter previamente à Unidade Central de Tecnologia da Informação quaisquer alterações, projetos ou demandas que necessitem de grande quantidade de recursos de armazenamento e possam afetar os procedimentos de backup, a fim de possibilitar o planejamento adequado de capacidade da infraestrutura necessária.

CAPÍTULO XI
DAS DISPOSIÇÕES FINAIS

Art. 41. Compete à Unidade Central de Tecnologia da Informação a revisão, atualização e divulgação desta Instrução Normativa sempre que necessário.

Art. 42. A Unidade Central de Tecnologia da Informação, as Unidades Setoriais de Tecnologia da Informação e os proprietários das informações terão o prazo de 180 (cento e oitenta) dias para adequarem as rotinas e procedimentos de backup às diretrizes definidas nesta Instrução Normativa.

Art. 43. Os casos omissos serão dirimidos pela Unidade Central de Tecnologia da Informação, por intermédio de suas unidades administrativas.

Art. 44. Esta Instrução Normativa entra em vigor na data de sua publicação.

Gabinete do Secretário-Chefe da Secretaria-Geral de Governo, aos 28 dias de agosto de 2024.

ADRIANO DA ROCHA LIMA
Secretário-Chefe da Secretaria-Geral de Governo

Protocolo 483967

EXTRATO DE PUBLICAÇÃO DO SEGUNDO TERMO ADITIVO AO CONTRATO Nº 017/2023 - SGG

Contratante: **ESTADO DE GOIÁS, por intermédio da SECRETARIA-GERAL DE GOVERNO - SGG - CNPJ nº 34.049.214/0001-74.**
Contratada: Pazini Empreendimentos e Negócios Ltda. - CNPJ nº 03.611.949/0001-16.
Objeto do Contrato: Prestação do serviço de locação com serviços de transporte, montagem, manutenção e desmontagem, sob demanda, de equipamentos e estruturas e materiais para a realização de eventos do Governo de Goiás, compreendendo: lonas, estruturas metálicas, ar-condicionado, painel de LED, móveis, banheiros químicos e outros, pelo período de 12 (doze) meses.
Objeto do Aditivo: Alteração do preâmbulo e acréscimo de, aproximadamente, 25% (vinte e cinco por cento) do quantitativo do objeto contratado.
Valor do Aditivo: R$ 1.687.157,50 (um milhão, seiscentos e oitenta e sete mil cento e cinquenta e sete reais e cinquenta centavos).
Processo nº: 202318037003304.
Data da Assinatura: 28/08/2024.

Protocolo 483937

AVISO DE LICITAÇÃO
AVISO DE PREGÃO ELETRÔNICO
PREGÃO ELETRÔNICO - PE Nº 45/2024 - SGG
PROCESSO N° 202400005008556

O Estado de Goiás, por intermédio da **SGG - SECRETARIA-GERAL DE GOVERNO** torna público, para conhecimento dos interessados, que realizará procedimento na modalidade **Pregão Eletrônico**, tipo **Menor Preço do Lote**, nos termos do art. 28, inciso I, da Lei federal nº 14.133, de 1º de abril de 2021 e na forma do Decreto estadual nº 10.247, de 30 de março de 2023. Objeto: **Contratação de serviços de auditoria externa para certificar, conforme norma ABNT NBR ISO 9001:2015, 2 (dois) processos de trabalho selecionados pela Superintendência de Sistemas e Inovação, quais sejam, "Digitalização de Serviços Públicos Estaduais" e "Gestão de Contratos" pelo período de 36 (trinta e seis) meses.** Valor Estimado: R$ 21.832,24 (vinte e um mil e oitocentos e trinta e dois reais e vinte e quatro centavos). Data e horário de início da sessão eletrônica de lances: **09:00** (horário de Brasília-DF) do dia **16/09/2024.** Endereço eletrônico: **www.sislog.go.gov.br**. **Número da Contratação: 104770.** O fornecedor interessado em participar do certame deverá ser previamente cadastrado no sistema oficial de cadastro de fornecedores do Estado, devendo para tanto encaminhar, exclusivamente por meio do sistema eletrônico, a proposta com a descrição do objeto e preço ofertado, até a data e horário estabelecidos para início da sessão eletrônica de lances. Informações acerca do cadastro de fornecedores, Termo de Referência e demais documentos da contratação encontram-se disponíveis nos sites: www.sislog.go.gov.br. Maiores informações pelo telefone: (62) 3270-8645.

MARCUS VINÍCIUS DE SANTANA AMARAL
Pregoeiro

Protocolo 484085

EXTRATO DO 1º TERMO ADITIVO À ATA DE REGISTRO DE PREÇOS Nº 05/2024-SGG

ÓRGÃO LICITANTE: SECRETARIA-GERAL DE GOVERNO (34.049.214/0001-74)
ÓRGÃO GERENCIADOR: SECRETARIA DE ESTADO DA ADMINISTRAÇÃO (02.476.034/0001-82)
FORNECEDOR REGISTRADO: DELL COMPUTADORES DO BRASIL LTDA (72.381.189/0010-01)
OBJETO: atualização de configurações do produto registrados (computadores do tipo desktop) para os itens 1 e 3 da Ata de Registro de Preços nº 05/2024-SGG, conforme cláusula segunda do instrumento aditivo.
DATA DE ASSINATURA: 28/08/2024
LEGISLAÇÃO DE REGÊNCIA: Lei nº 8.666/1993, Decreto Estadual 9.666/2020 (regulamento estadual do pregão), Lei Estadual nº 17.928/2012 (normas complementares de licitações e contratos) e Decreto Estadual nº 7.437/2011 (regulamento estadual do SRP).

Protocolo 483975

Defensoria Publica

PORTARIA Nº 683, DE 28 DE AGOSTO DE 2024

O **Defensor Público-Geral do Estado de Goiás**, no uso de suas atribuições legais contidas no art. 12, incisos I, XII, XX, e XXI, da Lei Complementar Estadual nº 130, de 11 de julho de 2017, e;

Considerando a necessidade de adequação da estrutura orgânica da Defensoria Pública do Estado de Goiás;

Considerando o inteiro _teor dos processos administrativos de nºs 202410892008299 e 202410892008181;

RESOLVE:

Art. 1º Nomear *Laís Amancio de Queiroz Pereira*, inscrita no CPF sob o nº XXX.753.451-XX, no cargo de Assessor Especial 1 (CC-5), com efeitos a partir de 02 de setembro de 2024.

Art. 2º Nomear *Luana de Assis Pinto*, inscrita no CPF sob o nº XXX.146.891-XX, no cargo de Assessor Especial 1 (CC-5), com efeitos a partir de 02 de setembro de 2024.

Art. 3º Esta Portaria entra em vigor na data de sua assinatura.

Gabinete do Defensor Público-Geral do Estado, aos 28 dias do mês de agosto de 2024.

TIAGO GREGÓRIO FERNANDES
Defensor Público-Geral do Estado

Protocolo 484021

Extrato da Contrato n. 009/2024

Processo: 202310892007857. **Objeto:** Contratação de empresa especializada para a capacitação em Língua Portuguesa na perspectiva da utilização/emprego da "linguagem simples" com o professor Wanderson Melo, sob demanda, divididos em duas turmas, trazendo-lhes a ampliação conhecimentos gramaticais e possibilitando desenvolver estruturas de pensamento a partir da compreensão e da interpretação de leituras variadas para expressar-se, criticamente, de forma oral e escrita, com clareza e logicidade de ideias, observando o padrão culto da língua. **Contratante:** Defensoria Pública do Estado de Goiás. **Contratada**: Inovecapacitação - Consultoria e Treinamento Ltda . **Cnpj:** 27.883.894/0001-61. **Vigência**: 12 meses. **Valor total**: R$ 60.000,00

Protocolo 484001

EXTRATO DE ACORDO DE COOPERAÇÃO

Partícipes: Defensoria Pública do Estado de Goiás e Defensoria Pública do Distrito Federal. **Objeto:** Realização de eventos para atendimento conjunto entre os partícipes no Distrito Federal e nos municípios do Estado de Goiás que compõem a Região Integrada de Desenvolvimento do Distrito Federal e Entorno - RIDE. **Processo administrativo SEI nº** 202410892007716. **Assinatura:** 29/08/2024. Pela Defensoria Pública do Estado de Goiás: Defensor Público-Geral, Tiago Gregório Fernandes. Pela Defensoria Pública do Distrito Federal: Defensor Público-Geral, Celestino Chupel.

Protocolo 484175