ESTADO DE GOIÁS
SECRETARIA DE ESTADO DA INFRAESTRUTURA

PORTARIA Nº 090, de 12 de abril de 2024

Dispõe sobre a Política de Segurança de Informação (PSI) da SEINFRA.

O SECRETÁRIO DE ESTADO DA INFRAESTRUTURA – SEINFRA, no uso de suas atribuições legais, e;

Considerando a necessidade de promover uma politica de segurança na área de informática no âmbito da estrutura organizacional da SEINFRA;

Considerando a necessidade de se estabelecer diretrizes claras de armazenamento de dados e utilização de programas/software;

Considerando o compromisso da SEINFRA com a segurança e excelência na prestação de serviços;

Considerando as competências elencadas nos artigos 27 a 30 da Lei n° 21.792, de 16 de fevereiro de 2023, que estabelece a organização administrativa básica do Poder Executivo e dá outras providências; resolve:

Art. 1º Aprovar, no âmbito da Secretaria de Estado da Infraestrutura – SEINFRA, a Política de Segurança de Informação (PSI) SEINFRA.

Art. 2º Esta Portaria entra em vigor na data da sua publicação.

PEDRO HENRIQUE RAMOS SALES
Secretário de Estado

ANEXO ÚNICO

CAPÍTULO I
TERMOS E DEFINIÇÕES

Art. 1º Política de Segurança de Informação (PSI) da SEINFRA, consideram-se as seguintes definições:

a) arquivo – conjunto de dados que se relacionam de alguma forma, ou seja, juntos descrevem uma informação ou conjunto de informações. Em função da natureza dos computadores, arquivos são sempre formados por dados digitais, organizados seguindo algum tipo de estrutura (ou formato);

b) autenticidade – conceito de segurança de informação, que dá a garantia de que uma informação, produto ou documento é do autor a quem se atribui;

c) evitar que sejam compartilhadas, seja de forma intencional ou acidental, sem as devidas autorizações;

d) confidencialidade – conceito dentro da segurança da informação que garante o sigilo, ou seja, controla o acesso às informações e/ou dados evitar que sejam compartilhadas, (de forma intencional ou acidental) sem as devidas autorizações;

e) criptografia – prática de proteção das informações por meio do uso de “embaralhamento” das informações, de modo que o acesso e leitura normais dessas informações só podem ser realizadas por ‘chaves’ específicas de descriptografia, essa prática garante a confidencialidade, autenticidade e integridade das informações;

f) disponibilidade – conceito dentro da segurança da informação que garante que os dados estejam disponíveis pelo tempo necessário a quem se destina;

g) estação de trabalho – computador pessoal utilizado para trabalho;

h) integridade – conceito dentro da segurança da informação que garante que os dados e/ou informações sejam verossímeis, corretos, autênticos e confiáveis;

i) privilégios de acesso – conceito que define quem

e em que nível de permissão (alteração, leitura) os acessos são concedidos;

j) programa/software – uma coleção de instruções que descrevem uma tarefa a ser realizada por um computador;

l) recursos de armazenamento de dados – registro e preservação das informações digitais para seu uso em operações (em curso ou futuros);

m) recursos computacionais – recurso dotado de grande capacidade computacional, com possibilidade de interconexão com um computador pessoal e redes de computação;

n) recursos de TI – compreende todo e qualquer recurso computacional (estação de trabalho, laptops, servidores de rede, etc.) utilizado pela Superintendência de Tecnologia e Inovação para executar qualquer tarefa que possa gerar um resultado final para o negócio;

o) storages – área de armazenamento projetada para armazenar dados no nível do datacenter (local físico para armazenamento de grandes recursos computacionais, para utilização em larga escala);

p) T.I. **–** Tecnologia da Informação considerada, na SEINFRA, como a Superintendência de Tecnologia e Inovação, bem como suas Gerências.

CAPÍTULO II

DOS RECURSOS DA SUPERINTENDÊNCIA DE TECNOLOGIA E INOVAÇÃO – STI

Art. 2º Os recursos de hardware disponibilizados pela STI se dividem em duas partes:

§ 1º recursos computacionais (desktops) utilizados diretamente pelos usuários, bem como seus softwares.

§ 2º recursos de grande escala (servidores em datacenter) para armazenamento da massa de dados (em storages) e softwares de uso em grande espectro.

§ 3º para os itens do § 1º do art. 2º, esses são de propriedade da SEINFRA, para os itens descritos no § 2º do art. 2º, esses são de propriedade da SGG, os sistemas/programas desenvolvidos pela STI, pertencem à SEINFRA, independentemente do local onde estão armazenados.

§ 4º Todas as informações geradas, recebidas, processadas ou armazenadas utilizando os recursos de TI da SEINFRA/SGG são passíveis de auditoria.

Art. 3º Os agentes públicos, estagiários aprendizes parceiros e contratados, doravante denominados de forma geral como usuários, devem ter acesso unicamente àqueles recursos de tecnologia da informação que forem indispensáveis às suas atividades, obedecendo ao princípio dos privilégios de acesso.

Parágrafo único. O bom uso dos recursos de TI, sejam de hardware ou de software, disponibilizados aos usuários são de inteira responsabilidade dos próprios usuários.

Art. 4º Os recursos de TI, disponibilizados nas diversas áreas da SEINFRA, são de uso exclusivo para atender às necessidades do serviço público, ficando proibido o uso para fins particulares, salvo pedido via SEI, com autorização do Secretário.

Art. 5° As paralisações programadas de quaisquer serviços disponibilizados pela SEINFRA devem ser comunicadas com antecedência aos usuários, indicando os períodos de indisponibilidade dos serviços, salvo manutenções alheias ao controle da STI.

Art. 6° Os hardwares e softwares e parâmetros de configuração serão definidos pela STI da SEINFRA, tendo em vista os requisitos de segurança, estabilidade, confiabilidade e padronização do ambiente computacional.

§ 1º A STI deverá possuir lista atualizada dos componentes de hardware e software utilizados, bem como os dados do controle de acesso.

§ 2º A utilização de software, hardware ou quaisquer componentes tecnológicos que não estejam licenciados e homologados é vedada pela SEINFRA, sendo assim, quaisquer ocorrências como sanções, penalidades, independentemente da origem são de inteira responsabilidade do usuário que as praticou.

Art. 7º Quaisquer armazenamentos de arquivos, nos servidores ou sistemas de armazenamento centralizado/corporativo da SEINFRA não relacionadas às atividades funcionais é vedada (exemplo: música, fotos, vídeos e outros).

Art. 8° A STI poderá proceder a desinstalação dos hardwares e softwares e a exclusão de arquivos que estejam em

desacordo com o presente documento, sem a possibilidade de quaisquer restaurações.

Art. 9º O deslocamento de qualquer recurso de TI dentro de uma unidade ou entre unidades/departamentos diferentes, deve ser comunicado à área responsável pelo controle de patrimônio, a fim de que seja registrada a ocorrência. Ressaltando que a transferência desses recursos de TI deve ser realizada única e exclusivamente pela equipe da STI.

Art. 10. O usuário deve informar, imediatamente e formalmente, à STI quando identificar violação da integridade física do equipamento por ele utilizado, bem como os casos de furto ou roubo.

CAPÍTULO III

DAS ESTAÇÕES DE TRABALHO

Art. 11. As estações de trabalho fornecidas aos usuários possuem definições estabelecidas pela STI e conterão configurações de hardware e software padronizadas.

§ 1º e vedada a alteração de qualquer componente de hardware e periféricos das estações de trabalho pelos usuários; também é vedada a remoção da localidade sem comunicação e autorização prévia da STI, podendo a administração adotar sistema de controle de inventário de hardware e software.

§ 2º o usuário deve informar à STI quando identificar violação da integridade física do equipamento por ele utilizado, bem como os casos de furto ou roubo.

§ 3º a STI não se responsabiliza por arquivos gravados e manipulados dentro das estações de trabalho, tão pouco pela perda dessas informações, uma vez que existe um sistema de armazenamento específico para tal (vide Capítulo V), bem como das possíveis avarias nesses equipamentos.

§ 4º o empréstimo de estações de trabalho deverá ser solicitado pelo gestor da unidade e atendido pela STI consoante disponibilidade, mediante assinatura de termo de entrega e responsabilidade.

CAPÍTULO IV
RECURSOS DE COMPUTAÇÃO MÓVEIS (LAPTOPS)

Art. 12. Os recursos de computação móveis (laptops) devem ser utilizados obedecendo ao princípio dos privilégios de acesso definidos para tal, conforme art. 3º, capítulo II.

Parágrafo único. Aplicam-se, quando pertinentes, aos dispositivos móveis as mesmas regras de utilização das estações de trabalho.

Art. 13. A STI poderá instalar e ativar sistema de rastreamento quando da entrega do equipamento.

Art. 14. A STI poderá prover sistemas que efetuem o bloqueio de utilização de dispositivos móveis (pendrive, HD externo, entre outros), sem autorização ou aviso prévio, para proteger dados corporativos, ou quando houver risco de invasão/violação, a fim de minimizar risco corporativo.

Art. 15. O empréstimo de recursos de computação móveis deverá ser solicitado pelo gestor da unidade e atendido pela STI consoante disponibilidade e mediante assinatura de termo de entrega e responsabilidade.

§ 1º A STI não se responsabiliza por arquivos gravados e manipulados (fora da rede) nos dispositivos durante o período de utilização; após a devolução dos equipamentos para esta STI, estes não poderão ser formatados para posterior redistribuição.

§ 2º Os acessos aos equipamentos e seus sistemas operacionais deverão ser protegidos por credenciais.

CAPÍTULO V

ARMAZENAMENTO DE DADOS

Art. 16. Todas as informações corporativas devem ser armazenadas em *storages* da SEINFRA/SGG.

Art. 17. A STI deverá prover os mecanismos necessários para a proteção das informações gravadas nos recursos de armazenamento de dados corporativos da SEINFRA visando garantir a integridade, disponibilidade e confidencialidade das informações e obedecendo sempre ao princípio dos privilégios de acesso, conforme política da instituição.

Art. 18. A STI utiliza *storage* e servidores no ambiente do datacenter da SGG, podendo solicitar restauração

de backup periódico dos sistemas e das informações corporativas da SEINFRA, conforme política de cópia de segurança da própria SGG.

Parágrafo único. A STI não é responsável pela salvaguarda das informações armazenadas em local que não esteja em conformidade com a política de segurança.

Art. 19. É vedado o compartilhamento de pastas locais de arquivos nas estações de trabalho dos usuários, vide artigo 16.

Art. 20. A STI deverá prover mecanismos de descarte seguro de informações constantes nos lugares estipulados no artigo 16, de forma a preservar a confidencialidade dos dados da SEINFRA e seus usuários, respeitando a Lei Federal n° 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), mediante quarentena para dispositivos suspeitos e novos recursos de TI que venham a ser disponibilizados.

Art. 21. Para os fins desta portaria, faz necessário firmar as seguintes definições quanto à Política de Controle de Acesso Lógico aos Ativos de Informação:

a) agente público: servidores, estagiários e prestadores de serviço que estejam exercendo atividades na SEINFRA, seja remotamente ou presencialmente;

b) gestor de sistema: agente público oficialmente designado como gestor de determinado sistema de informação;

c) responsável administrativo: servidor responsável pela administração de recursos humanos;

d) unidade institucional: unidade em que está lotado o servidor;

e) usuário: pessoa física ou jurídica que opera algum sistema informatizado da SEINFRA.

CAPÍTULO VI

GERENCIAMENTO DE USUÁRIOS

Art. 22. Todos os usuários deverão conter login e senha de rede para utilização dos sistemas computacionais da SEINFRA, conforme descrito adiante no art. 27 do capítulo VII deste documento. A solicitação do primeiro acesso do usuário deverá ser efetuada pelo departamento de Recursos Humanos,

considerando que este já deu as devidas tratativas de posse.

Parágrafo único. Para usuários não efetivos ou não comissionados do Estado de Goiás, a solicitação de cadastramento de login e senha de rede poderá ser realizada por sua autoridade hierárquica titular do referido departamento ou superior, onde estará lotado.

Art. 23. O Departamento de Recursos Humanos deverá informar previamente sobre o desligamento de usuários da rede, ou seja, a STI deve ser notificada do processo de desligamento antes de sua efetivação, a fim de evitar violações de segurança da informação, bem como garantir a conformidade com esta Política de Segurança da Informação – PSI.

Art. 24. O login e senha deve, preferencialmente, ser compatível com a política de segurança definida pela STI, vide Art. 29, capítulo VII. A autoridade hierárquica titular do departamento ou superior deverá solicitar os acessos pertinentes às atividades a serem desempenhadas pelo novo usuário.

Art. 25. Nos sistemas que porventura não possuam integração com o Sistema de autenticação da SEINFRA gerido pela STI a tarefa de cadastramento, de concessão de direitos e de exclusão deverão ser solicitadas à autoridade competente pelo titular da unidade.

Art. 26. Para os sistemas que não oferecem essa possibilidade descrita no artigo anterior, o responsável administrativo da unidade deverá encaminhar pedido formal ao gestor do respectivo sistema, que manterá registro de todos os pedidos de inclusão, exclusão e de alteração de perfil de usuário, bem como de seu nível de acesso e repassar essa lista de acessos à STI, lembrando que, devido à Lei Federal nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais, em seu Art. 18, os usuários devem ser informados sempre que requisitarem onde estão e quem tem acesso aos seus dados pessoais.

Parágrafo único. O responsável administrativo da unidade institucional deverá proceder imediatamente à desativação de usuários que vierem a se desligar de sua unidade. A exclusão de usuários deve ser vedada, pois impede a possibilidade de rastreio ou de ações que compõe o histórico de atividades desse usuário.

CAPÍTULO VII

POLÍTICA DE SENHAS

Art. 27. A senha cadastrada é pessoal, intransferível e confidencial.

§ 1º O gerenciamento das senhas de rede, bem como da manutenção dos acessos aos sistemas da SEINFRA, é de responsabilidade da STI, ressaltando que ela não pode, arbitrariamente realizar qualquer alteração.

§ 2º A modificação da senha (*reset* de senha) deve ser solicitada pelo próprio usuário, via sistema de chamados. Modificação/adição de acessos devem ser solicitados pelo titular do departamento/unidade administrativa ou superior.

Art. 28. As políticas de complexidade de senhas (tamanho da senha, letras maiúsculas, minúsculas, etc.), bem como de sua expiração e bloqueio automático são de jurisdição da Secretária-Geral de Governo – SGG.

CAPÍTULO VIII

ACESSO À REDE

Art. 29. Apenas poderão ser conectadas às redes cabeadas da SEINFRA equipamentos previamente autorizados pela STI.

§ 1º As exceções ao caput deste artigo devem ser comunicadas à STI, justificando necessidade e prazo de utilização.

§ 2º As exceções autorizadas deverão obrigatoriamente adotar os padrões definidos pela Política de Segurança da SEINFRA, sendo o proprietário do equipamento responsável por qualquer tipo de licenciamento dos produtos nele instalados, além da manutenção e suporte aos sistemas não homologados pela STI, sendo que a SEINFRA não fornecerá licenças para funcionamento de equipamentos particulares, equipamentos e/ou dispositivos portáteis poderão acessar a rede sem fio específica para esse fim, com as devidas autenticações de rede.

Art. 30. A STI poderá desconectar das redes cabeadas e sem fio qualquer dispositivo que constitua ameaça à segurança da informação.

CAPÍTULO IX

ACESSO A PORTAIS DA INTERNET (WORLD WIDE WEB)

Art. 31. É proibido o acesso a sítios que contenham ou que incitem atos:

a) de pornografia, pedofilia, erotismo e correlatos;

b) de racismo;

c) de ferramentas para invasão e evasão de sistemas;

d) de compartilhamento de arquivos (não homologado pela STI);

e) de apologia e incitação a crimes;

f) de acesso remoto.

§ 1º A STI poderá utilizar software específico que realizará o bloqueio automático dos sítios enumerados neste artigo.

§ 2º Caso seja necessário, algum dos sítios enumerados neste artigo, poderá ser liberado, mediante solicitação à STI, justificando a necessidade do desbloqueio.

Art. 32. A política de acesso a portais de internet deve ser a mesma em toda a SEINFRA.

Art. 33. Os pedidos de acesso a portais de internet com acesso vedado devem ser formulados à STI.

CAPÍTULO X

UTILIZAÇÃO DE CORREIO ELETRÔNICO

Art. 34. O correio eletrônico constitui recurso corporativo para comunicação, a ser usado de modo compatível com o exercício do cargo, sem comprometer a imagem da SEINFRA nem o tráfego de dados na rede de computadores da instituição.

Art. 35. Todas as políticas que regem a segurança da informação no tocante ao uso, tamanho, nomenclatura, entre outras configurações relacionadas ao correio eletrônico são de jurisdição da SGG, cabendo à STI da SEINFRA apenas o *reset* de senha e apoio ao usuário junto à SGG.

CAPÍTULO XI

UTILIZAÇÃO DO SISTEMA DE ARQUIVOS

Art. 36. O sistema de arquivos constitui recurso corporativo para armazenamento de arquivos, e deve ser usado de modo compatível com o exercício do cargo.

Parágrafo único. O sistema de arquivos compreende as seguintes pastas:

I – Pastas armazenadas no servidor de arquivos e compartilhadas em rede, que podem ser:

a) pastas de unidades (ex: drive S:), com acesso restrito aos usuários de determinada unidade;

b) pastas compartilhadas entre todos os usuários da SEINFRA (ex: Z: área de transferência).

II – Pastas armazenadas na estação de trabalho do usuário, que podem ser:

a) pastas de sistema, armazenadas no drive C;

b)pastas do usuário, armazenadas no drive D.

Art. 37. A STI deverá realizar backup do tipo cópias de sombra (espelhamento) dos arquivos armazenados no servidor de arquivos, permitindo uma restauração rápida e funcional dos documentos na maioria dos casos.

Parágrafo único. O backup dos arquivos e pastas de usuário armazenadas nas estações de trabalho e/ou estações móveis (laptops) é de responsabilidade completa do usuário.

Art. 38. A STI poderá estabelecer cotas para limitar o espaço de armazenamento das pastas, por unidade e por usuário. Isso ocorre devido ao limite geral (limite de storage) de disco.

Art. 39. A STI não acessará os arquivos armazenados nas pastas das unidades e dos usuários, salvo para atender aos seguintes objetivos:

a) verificar a obtenção, retenção, uso e divulgação de informações por meio ou com fins ilícitos ou em desacordo com as normas regulamentares sobre segurança da informação.

b) recuperar conteúdo de interesse da SEINFRA, no caso de afastamentos legais do usuário e de seu substituto.

c) atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante pedido dos órgãos

competentes.

d) realizar a recuperação de arquivos do backup, a pedido do usuário.

CAPÍTULO XII

UTILIZAÇÃO DE MENSAGERIA INSTANTÂNEA

Art. 40. A utilização ou conexão com sistemas de mensageria instantânea de uso público, como Whatsapp, Discord, Teams dentre outros, poderão ser restringidas a critério da STI.

CAPÍTULO III

POLÍTICA DE BACKUPS

Art. 41. A Política de backups de servidores, banco de dados, aplicações e demais sistemas no nível do datacenter são de jurisdição da STI da SGG. Ressaltando que pedidos exclusivos e justificados de uma nova janela de backup’s podem ser solicitados, ficando a cargo da STI da SGG a autorização ou recusa desses pedidos.

Documento assinado eletronicamente por **PEDRO HENRIQUE RAMOS SALES**, **Secretário (a) de Estado**, em 12/04/2024, às 17:03, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

A autenticidade do documento pode ser conferida no site **http://sei.go.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=1** informando o código verificador **58986151** e o código CRC **C0408C05**.

GERÊNCIA DA SECRETARIA GERAL
RUA 05 Nº 833, QD. 05, LT. 23, EDÍFICIO PALÁCIO DE PRATA, SALA 509 - Bairro SETOR OESTE - GOIANIA - GO - CEP 74115-060 - 62996379624.

Referência:
Processo nº 202320920001591

SEI 58986151