ESTADO DE GOIÁS
AGÊNCIA GOIANA DE INFRAESTRUTURA E TRANSPORTES
Portaria 328/2020 - GOINFRA

Institui a Política de Segurança de Informações da Agência Goiana de Infraestrutura e Transportes – GOINFRA e dá outras providências.

O PRESIDENTE DA AGÊNCIA GOIANA DE INFRAESTRUTURA E TRANSPORTES no uso de suas atribuições legais, e,

Considerando as competências elencadas nos artigos 55 e 56 da Lei Estadual n.º 20.491/2019, que estabelece a organização administrativa do Poder Executivo e dá outras providências;

Considerando a necessidade de padronizar os procedimentos de Tecnologia da Informação, no âmbito desta Agência, visando a efetivação dos princípios da Segurança da Informação: Confiabilidade, Integridade e Disponibilidade;

RESOLVE:

Art. 1º. Instituir no âmbito desta Agência a Política de Segurança de Informações da Agência Goiana de Infraestrutura e Transportes, nos termos do instrumento constante do Anexo Único desta Portaria.

Art. 2º. Esta Portaria entra em vigor a partir da data de sua publicação.

CUMPRA-SE e PUBLIQUE-SE.

Pedro Henrique Ramos Sales
Presidente

Gabinete do Presidente do (a) AGÊNCIA GOIANA DE INFRAESTRUTURA E TRANSPORTES, aos 19 dias do mês de agosto de 2020.

ANEXO ÚNICO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA AGÊNCIA GOIANA DE INFRAESTRUTURA E TRANSPORTES - GOINFRA

CAPÍTULO I
TERMOS E DEFINIÇÕES

Art. 1º. Para os fins desta resolução, consideram-se as seguintes definições:

I - Arquivo — agrupamento de registros que, geralmente, seguem uma regra estrutural, e que contém informações (dados);

II - Autenticidade - garantia de que uma informação, produto ou documento é do autor a quem se atribui;

III - Confidencialidade — sigilo. Preservar a confidencialidade de uma informação significa garantir que apenas as pessoas que devem ter conhecimento a seu respeito poderão acessá-las;

IV - Criptografia — arte e ciência de esconder o significado de uma informação de receptores não desejados;

V - Disponibilidade — uma informação disponível é aquela que pode ser acessada por aqueles que dela necessitam, no momento em que precisam;

VI - Estação de trabalho - computador pessoal utilizado para trabalho;

VII - Integridade a preservação da integridade envolve proteger as informações contra alterações, intencionais ou acidentais, em seu estado original;

VIII - Privilégio Mínimo — conceito que define que uma pessoa só precisa acessar os sistemas e recursos mínimos necessários para realizar suas atividades;

IX - Programa — uma coleção de instruções que descrevem uma tarefa a ser realizada por um computador;

X - Recursos de armazenamento de dados corporativos — armazenamento de massa projetado para ambientes de grande escala e alta tecnologia;

XI - Recursos de computação e comunicação móveis — recurso dotado de grande capacidade computacional, com possib ilidade de interconexão com um computador pessoal e redes de computação;

XII - Recursos de TI — Todo equipamento ou dispositivo que utilize tecnologia da informação, bem como qualquer recurso ou informação que seja acessível através desses equipamentos ou dispositivos tecnológicos, tais como impressoras, sistemas, programas, softwares, acessos à rede local, internet, vpn (rede particular virtual), pendrives, smartcards, tokens, smartphones, modens sem fio, desktops, pastas compartilhadas na rede, entre outras;
XIII. Storages - Rede de área de armazenamento projetada para agrupar dispositivos de armazenamento de computador;

XIV - TI - Tecnologia da Informação considerada, na Agência, como a Gerência de Tecnologia;

XV - TI - Tecnologias da Informação são um conjunto de recursos tecnológicos, utilizados de forma integrada, com um objetivo comum.

CAPÍTULO II
DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO – TI

Art. 2º. Todos os recursos de TI disponibilizados pela Agência Goiana de Infraestrutura e Transportes são de propriedade da Agência.

Parágrafo único. Todas as informações geradas, recebidas, processadas ou armazenadas utilizando os recursos de TI da GOINFRA 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 à rede suas atividades obedecendo ao princípio do privilégio mínimo.

Parágrafo único. Os usuários são responsáveis pelos recursos de TI por eles utilizados, devendo contribuir para seu funcionamento e segurança.

Art. 4º. Os recursos de TI, disponibilizados nas diversas áreas da GOINFRA, destinam-se, exclusivamente, ao atendimento das necessidades do serviço público, sendo vedada a utilização para fins particulares, a menos que, após solicitação via SEI, seja autorizado pelo Presidente, pelo Diretor de Gestão Integrada, ou servidor com delegação, para tanto.

Art. 5º. As paralisações programadas de quaisquer serviços disponibilizados pela GOINFRA devem ser comunicadas com antecedência aos usuários, indicando os períodos de indisponibilidade dos serviços.

Art. 6º. Os hardwares e softwares e parâmetros de configuração serão definidos pela Gerência de Tecnologia da GOINFRA, tendo em vista os requisitos de segurança, estabilidade, confiabilidade e padronização do ambiente computacional.

§ 1º. A área de TI deverá manter lista atualizada de hardwares e softwares homologados que poderão ser utilizados no ambiente da GOINFRA obedecendo ao princípio do privilégio mínimo.

§ 2º. É vedada a utilização de hardwares e softwares que não estejam previamente licenciados e homologados.

Art. 7º. É vedada a gravação de arquivos (música, fotos, vídeos e outros) que não estejam estritamente relacionados às atividades funcionais, nos servidores e sistemas de armazenamento centralizados/corporativos da GOINFRA.

Art. 8º. A área de TI poderá proceder à desinstalação dos hardwares e softwares e a eliminação de arquivos que estejam em desacordo com o presente ato normativo, autorizada pelo Presidente, pelo Diretor de Gestão Integrada, ou servidor com delegação para tanto.

Art. 9º. O deslocamento de qualquer recurso de TI dentro de uma unidade ou entre unidades diferentes, deve ser comunicado à área responsável pelo controle de patrimônio, a fim de que seja registrada a ocorrência.

Parágrafo único. Caso seja necessário a deslocamento/remoção de computadores, somente será realizado pela área de TI.

Art. 10. O usuário deve informar, imediatamente, à área de TI 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 possuirão configurações de hardware e software padronizadas, de acordo com as definições estabelecidas pela Gerência de Tecnologia.

§ 1º. É vedada a alteração das estações de trabalho pelos usuários, podendo a administração adotar sistema de controle de inventário de hardware e software.

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

CAPÍTULO IV
RECURSOS DE COMPUTAÇÃO E COMUNICAÇÃO MÓVEIS

Art. 12. Os recursos de computação e comunicações móveis devem ser utilizados obedecendo ao princípio do privilégio mínimo.

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

Art. 13. A TI deverá instalar e ativar o sistema de rastreamento quando da entrega do equipamento.

Art. 14. A TI deverá prover sistemas que efetuem o bloqueio de utilização de dispositivos móveis, sem autorização, 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 e comunicação móveis deverá ser solicitado pelo gestor da unidade e atendido pela TI consoante disponibilidade, mediante assinatura de termo de responsabilidade.

§ 1º. A área de TI não se responsabiliza por arquivos gravados e manipulados durante o período de utilização de recursos de computação e comunicação móveis emprestados.

§ 2º. O acesso 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 GOINFRA.

Art. 17. A área de TI deverá prover os mecanismos necessários para a proteção das informações gravadas nos recursos de armazenamento de dados corporativos da GOINFRA visando garantir a integridade, disponibilidade e confidencialidade das informações e obedecendo sempre ao princípio do privilégio mínimo, conforme política da instituição.

Art. 18. A área de TI deverá efetuar backup periódico dos sistemas e das informações corporativas nos recursos de armazenamento de dados corporativos da GOINFRA, conforme política de cópia de segurança da instituição.

Parágrafo único. A TI 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 de arquivos nas estações de trabalho dos usuários.

Art. 20. A TI deverá prover mecanismos de descarte seguro de informação armazenada em meio digital, de forma a preservar a confidencialidade dos dados da GOINFRA, mediante quarentena para dispositivos suspeitos e novos recursos de TI que venham a ser disponibilizados.

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

I - Agente público: servidores, estagiários e prestadores de serviço que estejam exercendo atividades na Agência;

II - Gestor de Sistema: agente público oficialmente designado como gestor de determinado sistema de informação;

III - Responsável Administrativo: servidor responsável pela administração de recursos humanos;

IV - Unidade Institucional: unidade em que está lotado o servidor;

V - Usuário: pessoa física ou jurídica que opera algum sistema informatizado da GOINFRA.

CAPÍTULO VI
CADASTRAMENTO DE USUÁRIOS

Art. 23. Todos os sistemas deverão manter integração automática com o Sistema de Apoio ao Recursos Humanos para concessão de direitos básicos aos usuários, conforme sua lotação elou cargo.

Art. 24. Nos sistemas ainda não integrados com o Sistema de Apoio ao Recursos Humanos, que permitam a gestão de direitos pelo responsável da unidade administrativa, a tarefa de cadastramento, de concessão de direitos e de exclusão serão feitas por ele.

Art. 25. Para os sistemas que não oferecem essa possibilidade, o responsável administrativo da unidade deverá encaminhar, eletronicamente, por meio do Sistema de Atendimento ao Usuário - SAU, pedido formal ao gestor do respectivo sistema, que manterá registro de todos os pedidos de inclusão, exclusão e de alteração de perfil de usuário.

Parágrafo único. O responsável administrativo da unidade institucional deverá proceder imediatamente à exclusão de usuários que se desligaram de sua unidade.

CAPÍTULO VII
POLÍTICA DE SENHAS

Art. 26. A identificação de usuários que operam os sistemas deve ser feita mediante a autenticação usuário-senha.

Parágrafo único. Essa identificação está dispensada para consulta a sistemas públicos da GOINFRA, como o Portal, contudo a área de Tecnologia da Informação deverá manter registro dos endereços de internet (IP) que acessaram esses sistemas.

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

Art. 28. A senha deverá observar as seguintes regras de formação:

I - Não pode conter o nome da conta do usuário ou partes do nome completo do usuário que ultrapassem 2 (dois) caracteres consecutivos.

II - Deve conter pelo menos 6 (seis) caracteres.

III - Deve conter caracteres de 2 (duas) das 4 (quatro) seguintes categorias:

a) caracteres alfabéticos maiúsculos;

b) caracteres alfabéticos minúsculos;

c) caracteres numéricos;

d) caracteres especiais, não alfabéticos (por exemplo, "$$").

Art. 29. A senha cadastrada terá prazo de validade de no máximo 6 (seis) meses, ao fim do qual o usuário deverá cadastrar nova senha.

Art. 30. Após 6 (seis) tentativas erradas o sistema ficará indisponível por 30 (trinta) minutos com aviso ao administrador.

CAPÍTULO VIII
ACESSO À REDE

Art. 31. Apenas poderão ser conectadas às redes cabeadas da GOINFRA microcomputadores previamente autorizados pela respectiva área de Tecnologia da Informação.

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

§ 2º. As exceções autorizadas deverão obrigatoriamente adotar os padrões definidos pela Política de Segurança da GOINFRA, sendo o proprietário do equipamento responsável pelo licenciamento dos produtos nele instalados, além da manutenção e suporte aos sistemas não homologados pela área de Tecnologia da Informação, sendo que a GOINFRA não fornecerá licenças para funcionamento de microcomputadores particulares. Microcomputadores elou dispositivos portáteis poderão acessar a rede sem fio específica para esse fim.

Art. 32. A área de Tecnologia da Informação 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. 33. Todo acesso a portais de internet deverá ser identificado por usuário. Os rastros de acesso deverão, no mínimo, identificar usuários, endereço IP, URL acessada, data e hora.

Art. 34. A área de Tecnologia da Informação deverá reter os rastros de acesso pelo prazo mínimo de 30 (trinta) dias.

Art. 35. É proibido o acesso a sítios que tratem:

I - de pornografia, pedofilia, erotismo e correlatos;

II - de racismo;

III - de ferramentas para invasão e evasão de sistemas;

IV - de compartilhamento de arquivos;

V - de apologia e incitação a crimes.

§ 1º. A área de Tecnologia de Informação 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 Diretoria de Gestão Integrada, justificando a necessidade do desbloqueio, comunicada à Gerência de Tecnologia.

Art. 36. A política de acesso a portais de internet deve ser a mesma em toda a GOINFRA.

Art. 37. Os pedidos de acesso a portais de internet com acesso vedado devem ser formulados à Gerência de Tecnologia da GOINFRA.

CAPÍTULO X
UTILIZAÇÃO DE CORREIO ELETRÔNICO

Art. 38. O correio eletrônico constitui recurso corporativo para comunicação, a ser usados de modo compatível com o exercício do cargo, sem comprometer a imagem da GOINFRA nem o tráfego de dados na rede de computadores da instituição.

Art. 39. Todas as mensagens eletrônicas enviadas e recebidas nos domínios da GOINFRA terão registrados os dados: data e hora do envio ou recebimento; remetente; destinatário.

Art. 40. A área de Tecnologia da Informação deverá implantar mecanismos que evitem o envio e a recepção de mensagens que possam comprometer a segurança do serviço de correio eletrônico.

Art. 41. A área de Tecnologia da Informação poderá estabelecer cotas para limitar o espaço de armazenamento das caixas postais, por unidade e por usuário.

Art. 42. A área de Tecnologia da Informação não acessará mensagens individuais de caixas de e-mail, salvo para atender aos seguintes objetivos:

I - 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, mediante autorização do Presidente da Agência ou do Diretor de Gestão Integrada;

II - Recuperar conteúdo de interesse da GOINFRA, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização do Presidente da Agência ou do Diretor de Gestão Integrada;

III - Realizar a recuperação de mensagens do backup, a pedido do usuário.

Art. 43. A exclusão de caixas postais ocorrerá com a vacância ou afastamento do cargo, sendo vedada a prática das seguintes ações relativas ao correio eletrônico:

I - Acesso ou tentativa de acesso à caixa postal em desacordo com a política de segurança da GOINFRA;

II - Envio ou armazenamento de mensagem de conteúdo incompatível com as atribuições dos usuários, incluindo as que contêm ofensas e comentários discriminatórios;

III - Adulteração de dados referentes à origem da mensagem nos campos de controle de cabeçalho.

Art. 44. A área de Tecnologia da Informação prestará suporte para configuração e utilização da tecnologia adotada.

Art. 45. Para os demais usuários de e-mail, a área de Tecnologia da Informação disponibilizará os parâmetros de configuração para acesso por outros dispositivos.

CAPÍTULO XI
UTILIZAÇÃO DO SISTEMA DE ARQUIVOS

Art. 46. O sistema de arquivos constitui recurso corporativo para armazenamento de arquivos, a ser usados 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 Z), com acesso restrito aos usuários de determinada unidade;

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

II - Pastas armazenadas no microcomputador do usuário, que podem ser:

a) pastas de sistema, armazenadas no drive C;

b) pastas do usuário, armazenadas no drive D.

Art. 47. A área de Tecnologia da Informação deverá realizar backup dos arquivos armazenados no servidor de arquivos.

Parágrafo único. O backup dos arquivos de pastas de usuário armazenadas no microcomputador é de responsabilidade do usuário.

Art. 48. A área de Tecnologia da Informação poderá estabelecer cotas para limitar o espaço de armazenamento das pastas, por unidade e por usuário.

Art. 49. A área de Tecnologia da Informação não acessará os arquivos armazenados nas pastas das unidades e dos usuários, salvo para atender aos seguintes objetivos:

I - 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, mediante autorização do Presidente da Agência ou do Diretor de Gestão Integrada;

II - Recuperar conteúdo de interesse da GOINFRA, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização do Presidente da Agência ou do Diretor de Gestão Integrada;

III - Atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização do Presidente da Agência ou do Diretor de Gestão Integrada;

IV - Realizar a recuperação de arquivos do backup, a pedido do usuário.

CAPÍTULO XII
UTILIZAÇÃO DE MENSAGERIA INSTANTÂNEA

Art. 50. O sistema de mensageria instantânea constitui recurso corporativo para comunicação, a ser usados de modo compatível com o exercício do cargo, sem comprometer a imagem da GOINFRA nem o tráfego de dados na rede de computadores da instituição.

Art. 51. A Diretoria de Gestão Integrada e a Gerência de Tecnologia não armazenarão mensagens instantâneas enviadas por seus usuários, com exceção de armazenamento temporário das mensagens enviadas a usuário desconectado.

Parágrafo único. A Diretoria de Gestão Integrada e a Gerência de Tecnologia poderão manter registros de login de usuário e de envio de mensagens pelo sistema de mensageria instantânea.

Art. 52. A utilização ou conexão com sistemas de mensageria instantânea de uso público, como Windows Live Messenger, Yahoo!, Messenger, Google Talk, Skype, WhatsApp, Pandion (Psi), dentre outros, poderão ser restringidas a critério da Gerência de Tecnologia

Art. 53. A área de Tecnologia da Informação da Agência deverá ter técnicos responsáveis pela aplicação da presente política.

CAPÍTULO III
POLÍTICA DE BACKUPS

Art. 54. A Política de Beckups busca estabelecer os critérios de Backup, Replicação e Restauração de Dados da GOINFRA.

Parágrafo único. A política, mencionada no *caput*, define os procedimentos de cópia de segurança e testes, a fim de manter a integridade e disponibilidade das informações armazenadas no ambiente de Tecnologia da Informação da GOINFRA.

Art. 55. Para os efeitos desta Resolução, segundo o presente capítulo, são estabelecidos os seguintes conceitos e definições:

I - Backup (cópia de segurança): é a cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados;

II - Backup completo: é realizada a cópia de todos arquivos, independente de terem ou não sido alterados. Nesta estratégia de backup, a restauração de um sistema implica restaurar a última cópia completa;

III - Backup incremental: é realizada a cópia dos arquivos que foram alterados ou criados desde o último backup incremental. Nesta estratégia de backup, a restauração de um sistema implica restaurar a última cópia completa e todas as cópias incrementais realizadas entre a cópia completa e o incidente;

IV - Backup diferencial: é realizada a cópia dos arquivos que foram alterados desde o último backup completo. Nesta estratégia de backup, a restauração de um sistema implica restaurar a última cópia completa e a última cópia diferencial;

V - RPO (recovery point objective): o quanto é necessário voltar no tempo para encontrar um backup dos dados, ou seja, o tempo máximo de perda de dados tolerado;

VI - RTO (recovery time objective): tempo estimado para restaurar os dados ou para tornar os sistemas novamente operacionais;

VII - Janela de Backup: Período de tempo requerido para a geração do backup (total, diferencial ou incremental);

VIII - Tape Library (robô): equipamento que realiza backup e restore e armazena as mídias de backup em escaninhos. Dispõe de acionadores automáticos para movimentação das mídias entre os escaninhos e os drives de leitura/gravação;

IX - Sistema de backup: conjunto de programas especializados no planejamento, processamento e controle do backup de servidores storage e demais dispositivos que armazenam dados.

CAPÍTULO III
CÓPIAS DE SEGURANÇA

Art. 56. Os procedimentos para geração das cópias de segurança deverão ser automatizados.

Art. 57. O objeto, extensão (completo, incremental ou parcial), frequência, retenção, quantidade de cópias, local de armazenamento, RPO e RTO devem ser propostos pelos gestores técnicos e aprovados pelos gestores de negócio dos sistemas, a fim de que reflitam os requisitos de negócio da Agência, bem como os requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da GOINFRA.

Art. 58. As cópias de segurança devem ser armazenadas em uma localidade remota, fora do local primário do órgão, podendo ser em outro órgão público, em um ambiente com nível de proteção física compatível com o ambiente com maior nível de cada órgão, para prover redundância e atender à continuidade do negócio em caso de desastre.

Art. 59. Deverão ser retidos no mínimo 3 (três) gerações ou ciclos de cópias de arquivos de dados das aplicações críticas.

Art. 60. Em situações onde a confidencialidade é importante, os gestores técnicos dos sistemas devem solicitar que as cópias de segurança sejam protegidas por meio de encriptação.

Art. 61. As mídias utilizadas pelos sistemas de backup devem seguir as recomendações estabelecidas pelo fabricante, bem como considerar o tempo de vida útil da mesma.

Art. 62. Devem ser retiradas imediatamente dos sistemas de backup todas as mídias com data de vida útil (validade) vencidas.

Art. 63. As mídias armazenadas por prazo acima do período de vida útil ou obsolescência devem ser substituídas e os dados nela contidos que estejam dentro do período de retenção devem ser transferidos para outra mídia.

Art. 64. Os dados armazenados em microcomputadores, notebooks e dispositivos móveis (tablets, smartphones etc.) não serão objetos de backup, de modo que a realização de cópias de segurança destes dados é de inteira responsabilidade do usuário do dispositivo.

Art. 65. As cópias de segurança devem ser periodicamente testadas, de modo a garantir sua confiabilidade.

Parágrafo único. Os resultados dos testes, previsto no *caput*, serão validados pelas equipes designadas pelo Gerente de Tecnologia.

Art. 66. Os testes de restauração e simulação de recuperação dos dados devem ser realizados em servidores diferentes do ambiente de produção.

Art. 67. Esta "Política de Segurança da Informação da Agência Goiana de Infraestrutura e Transportes - GOINFRA" entra em vigor na data de sua publicação.

CUMPRA-SE e PUBLIQUE-SE.

Pedro Henrique Ramos Sales
Presidente

Gabinete do Presidente do (a) AGÊNCIA GOIANA DE INFRAESTRUTURA E TRANSPORTES, aos 19 dias do mês de agosto de 2020.

Documento assinado eletronicamente por **PEDRO HENRIQUE RAMOS SALES**, **Presidente**, em 20/08/2020, às 19:28, 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 **000014807777** e o código CRC **C25592A3**.
