da Internet, para fins alheios às atividades de trabalho;

VI - fazer ou permitir que terceiros façam uso de serviços de rede corporativa para os quais não estejam autorizados;

VII - utilizar os recursos de TIC para armazenar ou realizar backup de dados não relacionados às atividades do Órgão, tais como arquivos pessoais de áudio, vídeo e imagem, ainda que temporariamente;

VIII - baixar, fazer download, copiar ou hospedar em qualquer serviço da SSP-GO, sejam eles servidores de arquivos, estação de trabalho, sites ou demais meios de armazenamento, qualquer arquivo de vídeo, filmes, texto ou imagem que não sejam relacionados à atividade fim do Órgão ou de atividades relacionadas;

IX - fornecer a terceiros, compartilhar ou enviar para serviços de hospedagem, e-mail ou qualquer serviço fora da rede corporativa sem a devida autorização do Titular do Órgão, manuais, códigos de programação, arquitetura, diagramas de sistemas ou qualquer artefato relacionado aos Recursos de Tecnologia da Informação e Comunicação do Órgão;

X - utilizar mecanismos, ferramentas, programas ou qualquer meio visando obtenção de acessos, dados ou informações não autorizados, ou que, direta ou indiretamente, atentem contra a segurança, a autenticidade, a confiabilidade, a confidencialidade, a disponibilidade, a privacidade e a integridade dos dados, informações, sistemas, infraestrutura e demais recursos de TI do Órgão ou de terceiros;

XI - acessar sites com conteúdo relacionado à pornografia, racismo, preconceitos de qualquer natureza, jogos e demais serviços que possam acarretar riscos aos serviços de TIC ou prejudicar a imagem da instituição;

XII - acessar serviços na Infraestrutura de TIC sem a devida autorização da Unidade Setorial de TI e contra as recomendações de segurança vigentes;

XIII - conectar equipamentos na rede corporativa do órgão tais como switches, hubs, ponto de acesso de rede sem fio (access point) ou qualquer dispositivo não homologado pela Unidade Setorial de TI;

VIX - alterar qualquer configuração da rede corporativa, topologias, conexões, cabeamento, tipos de equipamentos sem autorização formal da Unidade Setorial de TI;

XV - fazer acesso remoto a qualquer computador ou dispositivo conectado na rede corporativa da SSP-GO sem autorização formal da Unidade Setorial de TI;

XVI - fazer acesso remoto, RDP, SSH, ou qualquer conexão direta a serviços na Infraestrutura de Data Center do Órgão tais como servidores de banco de dados, sites e serviços que contenha dados reais ou em ambientes de produção sem autorização formal da Unidade Setorial de TI.

Parágrafo Único. Ao ser detectado arquivos de vídeo, filmes, texto ou imagem que não sejam relacionados à atividade fim do Órgão ou de atividades relacionadas, a Unidade Setorial de TI poderá excluí-los sem aviso prévio ao proprietário, sendo que, em seguida, a Unidade a qual pertence o servidor responsável pela informação, notificada da ocorrência e em caso de nova ocorrência, efetuará o bloqueio do usuário, até que seja solicitado o desbloqueio pela chefia imediata.

CAPÍTULO VI
CONTROLE DE ACESSO

Art. 11 O controle de acesso na segurança da informação visa gerenciar e verificar todo usuário, concedendo ou bloqueando permissões aos dados solicitados.

§1 º. Deve armazenar relatórios de acessos autorizados ou tentativas bloqueadas por meio de registro que permitem auditoria futura, tendo como objetivo proteger equipamentos da infraestrutura de TI em uma rede corporativa, computadores, sistemas, dados e informações contra perda, roubo, acesso indevido, modificação ou divulgação não autorizada.

§ 2º. O controle de acesso pode ser do tipo lógico, que inclui uso de login/senha, biometria, criptografia e certificação ou físico, como o monitoramento de ambientes por meio de câmeras de segurança, alarmes, portas eletrônicas ou qualquer meio que permita autorizar ou bloquear o acesso de pessoas a um local específico.

Art. 12 Todo Recurso de TIC, tais como e-mail, acesso internet, acesso ao computador, sistemas, rede sem fio e servidor de arquivos deve ser utilizado por meio de senha pessoal, sendo que:

I - a senha é pessoal, intransferível e de responsabilidade única do usuário, sendo necessário sua alteração de acordo com políticas definidas pela Unidade de TI;

II - as senhas de acesso a todo sistema ou serviço deverá ter validade máxima de 180 (cento e oitenta) dias e deverão ser trocadas pelo usuário ou desativadas automaticamente em caso de descumprimento da regra;

III - as senhas de acessos deverão ser “fortes”, contendo letras, números e caracteres especiais conforme regras específicas a serem definidas pela Unidade Setorial de TIC, em conjunto com o proprietário do serviço, de acordo com a criticidade dos dados e informações envolvidas;

IV - todo usuário que não efetuar login pelo período de 90 (noventa) dias terá sua conta desativada;

V - o controle de acesso, permissão, gerência, ativação e desativação de usuários nos Recursos de TIC são de responsabilidade da Unidade Setorial de TIC-SITSP ou da Unidade Local de TIC, no caso de delegação da Unidade Setorial;

VI - o controle de acesso, permissão, gerência, ativação e desativação de usuários nos Sistemas Corporativos da SSP-GO são de responsabilidade das Unidades de Inteligência ou unidade delegada, de acordo com deliberação do titular do Órgão;

VII - a Unidade Setorial de TI apenas realizará controle de acesso aos Sistemas Corporativos da SSP-GO em caso de portaria específica onde conste autorização do titular do Órgão; e

VIII - a Unidade Setorial de TI irá estabelecer normativa complementar que implementará demais procedimentos relacionados ao controle de acesso no âmbito da SSP-GO.

CAPÍTULO VII
DISPOSIÇÕES FINAIS

Art. 13 Cabe à Superintendência Integrada de Tecnologias em Segurança Pública desta Pasta, por meio da Gerência de Telecomunicações, decidir os casos omissos desta Norma.

Art. 14 Esta Portaria entra em vigor na data de sua publicação, revogando-se a Instrução Normativa nº 0001/2011-SSPJ (000029366999) e a Portaria nº 0303/2019 - SSP (7356949).

Art. 15 Determinar o encaminhamento desta Portaria ao Gabinete do Subsecretário de Segurança Pública/SSP-GO, à Superintendência de Gestão Integrada/SSP, à Superintendência de Inteligência Integrada/SSP, à Superintendência de Proteção aos Direitos do Consumidor/SSP, à Superintendência de Polícia Técnico-Científica/SSP, à Superintendência de Combate à Corrupção e ao Crime Organizado/SSP, à Superintendência de Ações e Operações Integradas/SSP, à Superintendência Integrada de Tecnologias em Segurança Pública/SSP, ao Comando-Geral da Polícia Militar, ao Comando-Geral do Corpo de Bombeiros Militar, à Diretoria-Geral da Polícia Civil, e à Diretoria-Geral de Administração Penitenciária para conhecimento e demais providências.

RENATO BRUM DOS SANTOS

Protocolo 384672

PORTARIA Nº 0463, DE 29 DE MAIO DE 2023

Institui a Norma de Controle de Acesso aos Recursos de Tecnologia da Informação e Comunicação - TIC no âmbito da Secretaria de Estado da Segurança Pública de Goiás.

O SECRETÁRIO DA SEGURANÇA PÚBLICA DO ESTADO DE GOIÁS, nomeado pelo Decreto de 05 de abril de 2022, publicado no Diário Oficial do Estado n.º 23.772 - Suplemento, no uso de suas atribuições que lhe confere o inciso III, do art. 56 da Lei estadual nº 20.491, de 25 de junho de 2019, e tendo em vista o disposto no Processo SEI nº 202200016009372,

Considerando que compete à Gerência de Telecomunicações da Superintendência Integrada de Tecnologias em Segurança Pública - SITSP da SSP-GO, conforme Decreto nº 9.690, de 06 de julho de 2020, que aprova o Regulamento da Secretaria de Estado da Segurança Pública: "I - gerenciar os serviços de data center, rede corporativa, acesso à internet e intranet, correio eletrônico, armazenamento de arquivos, hospedagem de sites web, banco de dados, servidores de análise de dados/business intelligence (BI) e aplicações; assim como, gerir a segurança da informação, definir a política de segurança e controlar acessos";

Considerando o previsto no art. 6º da Portaria nº 0556, de 08 de junho de 2022 (000030796861), que institui a Política de Segurança da Informação no âmbito da Secretaria de Estado da Segurança Pública de Goiás; e

Considerando a necessidade de maior gerenciamento e controle do ambiente de Tecnologia da Informação e Comunicação - TIC quanto aos riscos crescentes de ataques cibernéticos, perda, roubo ou acesso indevido às informações sigilosas relacionados ao serviço de Segurança Pública, resolve:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º Aprovar a Norma de Controle de Acesso aos Recursos de Tecnologia da Informação e Comunicação - TIC no âmbito da Secretaria de Estado da Segurança Pública de Goiás - SSP-GO.

Art. 2º Para fins desta Norma, considera-se:

I - Confidencialidade: garante que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário;

II - Integridade: garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida;

III - Disponibilidade: garante que a informação esteja disponível para as pessoas autorizadas sempre que se fizer necessária;

IV - Autenticidade: garante que a informação mantenha sua origem e não possa ser alterada, exceto por pessoas autorizadas;

V - Legalidade: garante que o uso dos Recursos de TIC esteja de acordo com a legislação vigente;

VI - Segurança da informação: ações que objetivam viabilizar e assegurar a confidencialidade, integridade, disponibilidade e a autenticidade das informações;

VII - Unidade central de tecnologia da informação: unidade que coordena a gestão de Tecnologia da Informação no âmbito do Estado de Goiás: Subsecretaria de Tecnologia da Informação - STI/SGG;

VIII - Unidade setorial de tecnologia da informação: unidade responsável por atuar nas atividades de tecnologia da informação e comunicação na SSP-GO sob o direcionamento técnico da Unidade Central: Superintendência Integrada de Tecnologias em Segurança Pública - SITSP/SSP-GO;

IX - Unidade local de tecnologia da informação: unidade interna da Polícia Militar, Polícia Civil, Corpo de Bombeiros Militar, Superintendência da Polícia Técnico-Científica, Superintendência de Proteção aos Direitos do Consumidor - PROCON ou Diretoria-Geral de Administração Penitenciária responsável pelo atendimento de TIC ao usuário final;

X - Usuários: servidores ocupantes de cargo efetivo, cargo em comissão ou emprego público, deste quadro ou à disposição, estagiários e jovens aprendizes que exercem atividades em qualquer uma das unidades básicas ou complementares da SSP-GO, bem como das instituições que a compõem: Polícia Militar, Polícia Civil, Corpo de Bombeiros Militar, Diretoria-Geral de Administração Penitenciária, Superintendência da Polícia Técnico-Científica e PROCON;

XI - Política: define a estrutura, as diretrizes e os papéis referentes à segurança da informação;

XII - Normas: estabelecem regras, definidas de acordo com as diretrizes da política, a serem seguidas em diversas situações em que a informação é tratada;

XIII - Procedimentos: instrumentam as regras dispostas nas normas, permitindo a direta aplicação nas atividades da SSP-GO;

XIV - Sistemas Corporativos: Sistemas utilizados exclusivamente para as atividades de Segurança Pública tais como: RAI, SPP, GEOCONTROL, MPORTAL, SISP e GOIÁS BIOMÉTRICO; e

XV - Recursos de Tecnologia da Informação e Comunicação - TIC: Meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios e demais serviços prestados pela Unidade Setorial de TI tais como: Data Center, Salas Técnicas, Servidores de e-mail, de Arquivos, dos Sites e dos Sistemas, Links de Dados, Acesso Internet, Rede Sem Fio, Active Directory, Serviços de Firewall, Antivírus, IPS e AntiSPAM.

CAPÍTULO II
DOS OBJETIVOS

Art. 3º Esta norma tem como principais objetivos:

I - estabelecer controles de identificação, autenticação e autorização para proteção das informações trafegadas nos ambientes de TIC da SSP-GO, a fim de evitar acessos não autorizados que impliquem no risco de perda, roubo, destruição, alteração ou divulgação indevida; e

II - os controles aplicados a todos os usuários de serviços de TIC da SSP-GO, bem como demais pessoas que se relacionam direta ou indiretamente na manutenção e operacionalização destes.

CAPÍTULO III
DAS COMPETÊNCIAS

Art. 4º Compete à Unidade Setorial de TI da SSP-GO:

I - disponibilizar meios e ferramentas de controle, monitoramento e gerência dos Sistemas Corporativos e Recursos de TIC visando controles de acesso;

II - implementar soluções que garantam a autenticidade das informações trafegadas no ambiente de TIC do Órgão;

III - implementar soluções que auditem o ambiente de TIC visando evitar acesso indevido e conexão de equipamentos e sistemas não homologados ao ambiente de TIC do Órgão;

IV - monitorar o uso dos recursos visando mitigar riscos, corrigir vulnerabilidades, tratar permissões e controlar os acessos aos Recursos de Tecnologia da Informação e Comunicação - TIC da SSP-GO;

V - controlar o acesso aos Recursos de Tecnologia da Informação e Comunicação - TIC através do uso de mecanismos tais como Firewall, Antivírus, IPS e AntiSPAM; e

VI - implementar sistemas e ferramentas de auditoria e governança corporativa visando proteção e controle de acessos aos Recursos de TIC.

Art. 5º Compete às Unidades de Recursos Humanos / Departamento de Pessoal da SSP-GO e das Forças que a compõem:

I - informar à Unidade Setorial de TI ou Unidade responsável pelo controle de acesso a sistema específico, saídas ou movimentações de servidores para que o usuário seja desabilitado ou retiradas permissões, no mesmo dia ou primeiro dia útil após seu desligamento; e

II - informar à Unidade Setorial de TI, quando solicitada, relação de pessoal para fins de auditoria.

Art. 6º Compete às Unidades Locais de TI:

I - seguir as orientações e normativas expedidas pela Unidade Setorial de TI; e

II - controlar os acessos de usuários aos Recursos de Infraestrutura de TIC da SSP-GO, de acordo com permissões delegadas e recomendações da Unidade Setorial de TI.

Art. 7º Compete às Unidades de Inteligências da SSP ou unidade delegada, de acordo com deliberação do titular do Órgão:

I - controlar o acesso a Sistemas Corporativos, por meio da concessão e remoção de permissões, ativação e desativação dos acessos aos sistemas; e

II - autorizar o compartilhamento, acesso, manipulação e demais tratamentos de dados e informações produzidas ou armazenadas por meio do uso dos Recursos de Tecnologia da Informação e Comunicação - TIC da SSPGO.

CAPÍTULO IV
DIRETRIZES BÁSICAS

Art. 8º O controle de acesso na segurança da informação consiste em gerenciar e verificar todo usuário, concedendo ou bloqueando permissões aos dados ou locais solicitados.

§ 1º. Deve armazenar relatórios de acessos autorizados ou tentativas de acesso bloqueadas através de registro que permitem auditoria futura pelo período mínimo de 60 (sessenta) dias e tem como objetivo proteger equipamentos da infraestrutura de TIC na rede corporativa, computadores, sistemas, dados e informações contra perda, roubo, acesso indevido, modificação ou divulgação não autorizada; e

§ 2º. O controle de acesso pode ser do tipo lógico, que inclui uso de login e senha, biometria, criptografia e certificação ou físico, como o monitoramento de ambientes por meio de câmeras de segurança, alarmes, portas eletrônicas ou qualquer meio que permita autorizar ou bloquear o acesso de pessoas a um local específico.

Art. 9º O acesso físico a salas de servidores, data center, salas de nobreaks, geradores e outras salas técnicas onde haja equipamentos de redes e infraestrutura de TIC deve ser controlado e gerenciado. As salas devem permanecer trancadas e apenas pessoas autorizadas devem acessar o local.

Art. 10 Todo Recurso de TIC, tal como e-mail, acesso internet, acesso ao computador, sistemas, rede sem fio e servidor de arquivos, deve ser utilizado por meio de login com senha pessoal, sendo que:

I - a senha é pessoal, intransferível e de responsabilidade única do usuário, sendo necessário sua alteração de acordo com políticas definidas pela Unidade Setorial de TI;

II - as senhas de acesso a todo sistema ou serviço deverá ter validade máxima de 180 (cento e oitenta) dias e deverão ser trocadas pelo usuário quando solicitado, e em caso de descumprimento desta determinação, será bloqueada automaticamente;

III - as senhas de acessos deverão ser “fortes”, contendo letras, números e caracteres especiais conforme regras específicas a serem definidas pela Unidade Setorial de TIC, em conjunto com o proprietário do serviço, de acordo com a criticidade dos dados e informações envolvidas;

IV - todo usuário que não efetuar login pelo período de 90 (noventa) dias terá sua conta desativada;

V - o controle de acesso, permissão, gerência, ativação e desativação de usuários nos Recursos de TIC são de responsabilidade da Unidade Setorial de TI ou da Unidade Local de TI, no caso de delegação da Unidade Setorial;

VI - o controle de acesso, permissão, gerência, ativação e desativação de usuários nos Sistemas Corporativos da SSP-GO são de responsabilidade das Unidades de Inteligência ou unidade delegada de acordo com deliberação do titular do Órgão; e

VII - a Unidade Setorial de TIC apenas realizará controle de acesso aos Sistemas Corporativos da SSP-GO em caso de portaria específica onde conste autorização do titular do Órgão.

Art. 11 Todo dispositivo da rede corporativa que não estiver de acordo com as políticas de antivírus, licenciamento de software, atualização de sistemas ou normativas de uso dos recursos de TIC será bloqueado até que o problema seja resolvido pelo responsável.

Art. 12 O padrão adotado para o formato da conta de acesso do usuário é a sequência: primeiro nome + ponto + último nome do usuário. Exemplo: “jose.silva”.

Parágrafo único. Nos casos de já existir conta de acesso idêntica para outro usuário, deverá ser adotada outra combinação, devendo então ser utilizado o nome completo do usuário para o qual a conta está sendo criada.

Art. 13 O padrão adotado para o formato da senha deve considerar o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores:

I - a formação da senha da identificação (login) de acesso aos Recursos de TIC deve seguir as regras de:

a) possuir tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras e números;

b) recomenda-se a utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &, ...);

c) não ser formada por sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações;

d) não utilizar termos óbvios, tais como: Brasil, senha, usuário, password ou system; e

e) não reutilizar as últimas 2 (duas) senhas já usadas.

II - será fornecida uma senha temporária para cada conta de acesso, criada no momento da liberação dessa conta e a mesma deverá ser alterada pelo usuário quando do primeiro acesso.

CAPÍTULO V
BLOQUEIO E DESBLOQUEIO DE CONTAS

Art. 14 A conta de acesso será bloqueada nos seguintes casos:

I - após 3 (três) tentativas consecutivas de acesso incorreto;

II - solicitação do superior imediato do usuário, com a devida justificativa;

III - quando da suspeita de mau uso dos serviços disponibilizados pela Unidade Setorial de TI ou descumprimento da Política de Segurança da Informação e normas correlatas em vigência; e

IV - após 90 (noventa) dias consecutivos sem movimentação pelo usuário;

Art. 15 O desbloqueio da conta de acesso será realizado apenas após solicitação formal do superior imediato do usuário.

Art. 16 Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato ou do Setor responsável pela Gestão de Pessoas.

CAPÍTULO VI
ACESSO REMOTO

Art. 17 O acesso remoto tal como SSH, RDP, etc., a ambiente de servidores, sites, sistemas e bancos de dados de produção, que não seja o acesso padrão a sistemas publicados, será bloqueado para qualquer dispositivo fora do Data Center ou fora da rede dos administradores da infraestrutura de TIC do Órgão.

Parágrafo único. Excepcionalmente será liberado acesso ao serviço de produção de forma pontual e temporária, para computadores dentro da rede da Unidade Setorial de TI e usuários desenvolvedores lotados na Unidade Setorial de TI, com duração máxima limitada de 2h (duas horas), desde que o pedido seja formalizado e justificado, observando que:

I - a solicitação deve ser enviada via SEI, do responsável pela Unidade, para a Unidade Setorial de TI, contendo justificativa da necessidade do acesso, serviço a ser acessado, horários de início e fim, usuário e endereço IP de origem;

II - o acesso será nominal, com login e senha do responsável pelo acesso, restrito por endereço IP, e deverá ser auditado e solicitado com antecedência mínima de 24h (vinte e quatro horas);

III - não será permitido qualquer acesso por meio de login e senha de sistema;

IV - após deliberação da Unidade Setorial de TI, caso consentida, a liberação de acesso será de forma excepcional, esporádica e não deve se tornar rotina, sendo que a necessidade deve ser tratada o quanto antes, de forma sistêmica, para que o acesso futuro não seja necessário; e

V - o acesso somente será liberado caso seja possível monitoramento das ações realizadas, com registro dos comandos digitados.

Art. 18 É proibido acesso remoto a partir da Internet ou outra rede que não seja a da SSP-GO a qualquer dispositivo na rede interna, fora da Infraestrutura de Servidores e Data Center da SSP-GO, tais como computadores de usuários, servidores locais, câmeras de videomonitoramento, etc.

Art. 19 O acesso remoto a serviços específicos, que não seja o acesso padrão a sistemas publicados, somente será autorizado a equipamentos ou serviços localizados na infraestrutura de servidores e Data Center da SSP-GO, em caráter excepcional e pontual, mediante uso de ferramentas de VPN providas pela Unidade Setorial de TI e deverá ser de forma temporária, monitorada e gerenciada.

Art. 20 A Unidade Setorial de TI proverá ambiente de homologação, que será atualizado mensalmente com os dados de produção e será acessado apenas por sistemas em homologação no ambiente de servidores e Data Center da SSP-GO.

Art. 21 A Unidade Setorial de TI proverá ambiente de desenvolvimento, que não terá dados de produção atualizados e terão os dados mascarados e embaralhados, sendo permitido o acesso dos desenvolvedores apenas a partir da rede da Unidade Setorial de TI de acordo com permissões individuais.

Art. 22 A Unidade Setorial de TI proverá acesso para construção de painéis estatísticos de BI que deverão ser por meio de conexão a banco de dados de réplica, que deverá ser atualizado com o banco de produção em intervalos regulares, construído unicamente para este fim. Este acesso também será liberado apenas para servidores no ambiente do Data Center e rede de servidores da SSP, podendo em caráter excepcional se estender a computadores na rede da Unidade Setorial de TI, desde que haja mecanismos de auditoria e não seja permanente.

CAPÍTULO VII
DISPOSIÇÕES FINAIS

Art. 23 Cabe à Superintendência Integrada de Tecnologias em Segurança Pública desta Pasta, por meio da Gerência de Telecomunicações, decidir os casos omissos desta Norma.

Art. 24 Esta Portaria entra em vigor na data de sua publicação, revogando-se a Instrução Normativa nº 0001/2011-SSPJ (000029366999) e a Portaria nº 0303/2019 - SSP (7356949).

Art. 25 Determinar o encaminhamento desta Portaria ao Gabinete do Subsecretário de Segurança Pública/SSP-GO, à Superintendência de Gestão Integrada/SSP, à Superintendência de Inteligência Integrada/SSP, à Superintendência de Proteção aos Direitos do Consumidor/SSP, à Superintendência de Polícia Técnico-Científica/SSP, à Superintendência de Combate à Corrupção e ao Crime Organizado/SSP, à Superintendência de Ações e Operações Integradas/SSP, à Superintendência Integrada de Tecnologias em Segurança Pública/SSP, ao Comando-Geral da Polícia Militar, ao Comando-Geral do Corpo de Bombeiros Militar, à Diretoria-Geral da Polícia Civil, e à Diretoria-Geral de Administração Penitenciária para conhecimento e demais providências.

RENATO BRUM DOS SANTOS

Protocolo 384675

PORTARIA Nº 0467, DE 30 DE MAIO DE 2023

O SUBSECRETÁRIO DE ESTADO DA SEGURANÇA PÚBLICA, nomeado pelo Decreto de 12 de abril de 2022, publicado no Diário Oficial do Estado nº 23.777 - Suplemento, no uso de suas atribuições legais e usando da competência que lhe confere a Portaria nº 0332, de 18 de abril de 2022, publicada no Diário Oficial do Estado de Goiás nº 23.780, e tendo em vista o Processo SEI nº 202300016010281, resolve:

Art. 1º Designar a servidora FLÁVIA CHRISTINE SOUZA COSTA ARAÚJO, inscrita no CPF nº XXX.422.971-XX, ocupante do cargo de Escrivã de Polícia de Classe Especial, para, sem prejuízo de suas atribuições e no período de 24 de maio de 2023 a 2 de junho de 2023, responder pelo expediente da Gerência de Projetos e Captação de Recursos desta Secretaria, em substituição ao titular da referida Unidade Administrativa, o servidor CARLOS BORGES DOS SANTOS, inscrito no CPF nº XXX.502.981-XX, ocupante do cargo de Gerente, que, por sua vez, estará em gozo de suas férias regulamentares, conforme requerimento (SEI nº 46341448).

Art. 2º Esta Portaria entra em vigor na data de sua publicação, revogando-se as disposições em contrário.

Art. 3º Determinar o encaminhamento desta Portaria à Superintendência de Gestão Integrada/SSP e à Gerência de Gestão e Desenvolvimento de Pessoas/SSP para conhecimento e demais providências.

DEUSNY APARECIDO SILVA FILHO

Protocolo 384680

PORTARIA Nº 0468, DE 30 DE MAIO DE 2023

O SUBSECRETÁRIO DE ESTADO DA SEGURANÇA PÚBLICA, nomeado pelo Decreto de 12 de abril de 2022, publicado no Diário Oficial do Estado nº 23.777 - Suplemento, no uso de suas atribuições legais e usando da competência que lhe confere a Portaria nº 0332, de 18 de abril de 2022, publicada no Diário Oficial do Estado de Goiás nº 23.780, e tendo em vista o Processo SEI nº 202300016015773, resolve:

Art. 1º Designar o servidor PEDRO ARCANJO ROZENFELD RODRIGUES, inscrito no CPF nº XXX.725.217-XX, ocupante do cargo de Perito Criminal, para, sem prejuízo de suas atribuições, e no período de 17 de julho de 2023 a 29 de julho de 2023, responder pelo expediente da 10ª Coordenação Regional de Polícia Técnico-Científica de Anápolis, em substituição ao titular da referida unidade administrativa, o servidor LEANDRO CARNEIRO NASCIMENTO, inscrito no CPF nº XXX.778.311-XX, ocupante do cargo de Perito Criminal, que, por sua vez, estará em gozo de férias regulamentares, conforme processo SEI nº 202300016014352.

Art. 2º Esta Portaria entra em vigor na data de sua publicação, revogando-se as disposições em contrário.

Art. 3º Determinar o encaminhamento desta Portaria à Superintendência de Polícia Técnico-Científica - SPTC e à Gerência de Gestão e Desenvolvimento de Pessoas/SSP para conhecimento e demais providências.

DEUSNY APARECIDO SILVA FILHO

Protocolo 384684

PORTARIA Nº 0469, DE 30 DE MAIO DE 2023

O SUBSECRETÁRIO DE ESTADO DA SEGURANÇA PÚBLICA, nomeado pelo Decreto de 12 de abril de 2022, publicado no Diário Oficial do Estado nº 23.777 - Suplemento, no uso de suas atribuições legais e usando da competência que lhe confere a Portaria nº 0332, de 18 de abril de 2022, publicada no Diário Oficial do Estado de Goiás nº 23.780, e tendo em vista o Processo SEI nº 202300016015897, resolve:

Art. 1º Designar o servidor EMILIANO LUIZ NETO, inscrito no CPF nº XXX.209.971-XX, ocupante do cargo de Perito Criminal, para, sem prejuízo de suas atribuições e no período de 1º de junho de 2023 a 30 de junho de 2023, responder pelo expediente da 1ª Coordenação Regional de Polícia Técnico-Científica de Aparecida de Goiânia, em substituição ao titular da referida Unidade Administrativa, o servidor MURILO TOSCANO DE CARVALHO, inscrito no CPF nº XXX.046.881-XX, ocupante do cargo de Perito Criminal, que, por sua vez, estará em gozo de férias regulamentares, conforme processo SEI nº 202300016014971.

Art. 2º Esta Portaria entra em vigor na data de sua publicação, revogando-se as disposições em contrário.

Art. 3º Determinar o encaminhamento desta Portaria à Superintendência de Polícia Técnico-Científica - SPTC e à Gerência de Gestão e Desenvolvimento de Pessoas/SSP para conhecimento e demais providências.

DEUSNY APARECIDO SILVA FILHO

Protocolo 384688