VI - impor regras e filtros de classificação de e-mails enviados e recebidos, de forma impessoal e automatizada, para conteúdo que possua características de spam, phishing, hoax, vírus entre outros tipos de ameaças, impondo políticas de quarentena, reclassificação e bloqueio, quando necessário; e

VII - bloquear de forma imediata contas de e-mail que tenham sido identificadas como comprometidas por agente diverso ao titular da conta, cabendo ao titular providenciar e executar as recomendações que serão emitidas pela Unidade Setorial de TI para fins de desbloqueio desta.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 18 Cabe à Superintendência Integrada de Tecnologias em Segurança Pública desta Pasta, por meio da Gerência de Telecomunicações, decidir os casos omissos desta Norma.

Art. 19 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. 20 Determinar o encaminhamento desta Portaria ao Gabinete do Subsecretário de Segurança Pública/SSP, 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 384666

PORTARIA Nº 0462, DE 29 DE MAIO DE 2023

Institui a Norma de Uso dos 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 Uso dos 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, 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
DIRETRIZES BÁSICAS

Art. 3º Os Recursos de Tecnologia da Informação e Comunicação - TIC colocados à disposição dos usuários da SSP-GO devem ser utilizados exclusivamente no atendimento dos serviços que lhe são afetos.

I - a Unidade responsável por realizar o controle e

monitoramento dos usuários dos Recursos de TIC no âmbito da SSP-GO é a Gerência da Telecomunicações - GETEL da Superintendência Integrada de Tecnologias em Segurança Pública - SITSP, conforme Decreto nº 9.690, de 06 de julho de 2020. Esta poderá, em casos específicos, delegar responsabilidades para a equipe de informática de cada instituição;

II - o acesso aos Recursos de TIC só será feito por usuário devidamente cadastrado;

III - a identificação do usuário (login) e senha inicial de acesso é obrigatória para o uso da estação de trabalho conectada à rede da SSP-GO;

IV - a senha de acesso é de uso pessoal e intransferível e sua divulgação é vedada sob qualquer hipótese, devendo ser alterada pelo próprio usuário no primeiro acesso, em períodos regulares definidos pela SITSP ou em casos em que haja necessidade de troca imediata devido à ameaça de falhas de segurança após comunicado da GETEL/SITSP;

V - a utilização do login e senha de acesso é de responsabilidade exclusiva do usuário a eles vinculado;

VI - ao ser credenciado para uso dos Recursos de TIC, o usuário é relacionado a um perfil de acordo com sua lotação, que indica seus direitos de acesso a serviços e informações, sendo proibido seu compartilhamento com terceiros;

VII - o responsável pela Unidade Administrativa deve solicitar à Unidade Local de TI correspondente o cadastro de novos usuários na rede corporativa;

VIII - o responsável pelo Departamento de Pessoal / RH da SSP-GO e das instituições que a compõem deve comunicar à Unidade de TI todos os desligamentos de servidores, afastamentos, mudança de lotação ou qualquer movimentação que exija remoção de permissões ou desativação de usuário da rede corporativa de forma imediata; e

IX - deve-se sempre observar a legalidade no uso dos Recursos de TIC, sendo expressamente proibida a manipulação, cópia mesmo que temporária e uso de software ou qualquer recurso sem o devido licenciamento exigido.

CAPÍTULO III
DOS OBJETIVOS

Art. 4º Esta norma tem como principais objetivos:

I - regulamentar o uso dos Recursos de Tecnologia da Informação e Comunicação - TIC da SSP-GO visando garantir confiabilidade, integridade, disponibilidade, autenticidade e legalidade no acesso e manipulação de dados e informações no ambiente de TIC do Órgão;

II - definir competências, obrigações e restrições quanto ao uso dos Recursos de Tecnologia da Informação e Comunicação - TIC da SSP-GO;

III - criar mecanismos para prevenção de vazamento ou acesso indevido a informações e serviços sigilosos desenvolvidos pela SSP-GO;

IV - criar procedimentos para controles de acesso, gerência, monitoramento e auditoria dos Recursos de Tecnologia da Informação e Comunicação e Sistemas Corporativos da SSP-GO;

V - definir mecanismos para proteção dos recursos e serviços de TIC de ameaças e vulnerabilidades; e

VI - proteger a reputação do Órgão e aumentar a garantia da continuidade dos serviços de Segurança Pública.

CAPÍTULO IV
DAS COMPETÊNCIAS

Art. 5º Compete à Unidade Setorial de TI da SSP-GO:

I - disponibilizar meios e ferramentas de controle e gerência dos Recursos de TIC visando alta disponibilidade, confiabilidade e integridade dos dados e das informações tratadas;

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 uso de software pirata, zelando pela legalidade no tratamento de informações no ambiente de TIC do Órgão, possibilitando identificação e bloqueio de computadores e usuários que não estejam de acordo;

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 - estabelecer políticas, normas e procedimentos de operação e uso dos Recursos de TIC da SSP-GO;

VI - 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

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

Art. 6º 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 usuários ativos para fins de auditoria.

Art. 7º 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 Serviços de Infraestrutura de TIC da SSP-GO, de acordo com permissões delegadas e recomendações da Unidade Setorial de TI.

Art. 8º 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 V
USO DOS RECURSOS DE TIC

Art. 9º São deveres dos usuários:

I - zelar pelo sigilo, guarda e manutenção de suas credenciais de autenticação, login e senha, e seguir as recomendações de segurança expedidas pela Unidade Setorial de TI;

II - zelar pelos equipamentos e sistemas de informática;

III - zelar pela integridade e confidencialidade das informações sob sua responsabilidade;

IV - encerrar as sessões dos sistemas que estiverem abertos ou bloquear o acesso ao computador, quando se ausentar de seu local de atividade, ainda que temporariamente; e

V - comunicar imediatamente à Unidade Setorial de TI a ocorrência de fatos que possam atentar contra a segurança do ambiente informatizado do órgão, dentre outros, perda ou extravio de credenciais de autenticação, dano, furto, roubo, suspeita de infecção por vírus, tentativas de invasão ou acessos não autorizados e falhas nos recursos informatizados que possam torná-los vulneráveis.

Art. 10 É vedado aos usuários ou qualquer pessoa que faça uso dos Recursos de TIC ou Sistemas Corporativos da SSP-GO:

I - instalar software não homologado pela Unidade Setorial de TI;

II - instalar componente de hardware nos equipamentos fornecidos pela Unidade Setorial de TI sem a devida autorização;

III - baixar, hospedar, copiar ou instalar software pirata, sem licença específica, que fere direitos autorais ou de propriedade intelectual, em qualquer dispositivo da rede corporativa da SSP-GO;

IV - alterar configuração de hardware em equipamentos fornecidos pela SITSP ou software nos dispositivos conectados à rede corporativa sem a devida autorização da Unidade Setorial de TI;

V - fazer uso dos serviços de rede corporativa, impressão ou

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,