RESOLUÇÃO N° 264/2024

Aprova as Normas de Uso para o SISTEMA SESP INTRANET e Termo de Responsabilidade, na forma do Anexos que integram a presente Resolução.

O SECRETÁRIO DE ESTADO DA SEGURANÇA PÚBLICA, no uso das atribuições que lhe são conferidas pelo artigo 90 da Constituição da Estadual, incisos I e XVI, do artigo 6 da Lei 19.848 de 03 de maio de 2019, bem como pelos incisos IX e X, do art. 9º do Decreto 5.887 de 15 de dezembro de 2005.

CONSIDERANDO que o sistema SESP Intranet está em constante evolução, desenvolvido como ferramenta de segurança dos sistemas da Secretaria da Segurança Pública funcionando como um portal de SSO (login único) entre todos os sistemas cadastrados neste.

CONSIDERANDO que o sistema permite aos usuários o acesso a informações sensíveis tais como informações pessoais e de veículos de todo o Estado do Paraná que são utilizados pelos agentes da Segurança Pública nas diversas atuações ao combate e repreensão ao crime.

CONSIDERANDO que se faz necessário a aplicação eficiente da gestão de acesso ao sistema sendo uma parte fundamental da segurança da informação em órgãos que lidam com informações sensíveis.

CONSIDERANDO a necessidade de padronização dos acessos de usuários ao Sistema SESP Intranet e a importância de restringir tais acessos para evitar o uso inadequado ou desvirtuado de seus objetivos.

RESOLVE:

Art. 1º Aprovar o Anexo I - NORMAS DE USO PARA O SISTEMA SESP INTRANET, o qual define diretrizes de segurança da informação, operacionalização e controle de acessos do Sistema SESP Intranet e o Anexo II - Termo de responsabilidade.

Art. 2º Esta resolução entrará em vigor na data de sua publicação.

Curitiba-Paraná, 27 de maio de 2024.

Cel. PM RR Hudson Leôncio Teixeira
Secretário de Estado da Segurança Pública

ANEXO I - NORMAS DE USO PARA O SISTEMA SESP INTRANET

Capítulo I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º O presente conjunto de normas dispõe sobre as diretrizes de segurança da informação, operacionalização e controle de acessos ao Sistema SESP Intranet.

Parágrafo único. O sistema SESP Intranet é um portal de autenticação e segurança que, através de um login único, permite acessar um ou vários sistemas pertencentes à Secretaria da Segurança Pública do Paraná.

Art. 2º Sujeitam-se ao presente conjunto de normas todos os usuários pertencentes a Secretaria de Segurança do Paraná e aos órgãos de execução programática, bem como aos usuários decorrentes de convênios firmados com esta. Secretaria.

Capítulo II
DAS DIRETRIZES DE CONTROLE DE ACESSO

Seção I
CONTROLES APLICADOS AOS USUÁRIOS EM GERAL

Art. 3º Todo usuário cadastrado deverá ser identificado, contendo as seguintes informações:

I. Nome Completo;
II. CPF;
III. E-mail institucional;
IV. Telefone Celular para Contato;
V. Função;
VI. Órgão vinculado – Instituição;
VII. Unidade de Trabalho;
VIII. Seção; e
IX. Cidade.

Art. 4º Os gestores do sistema devem atentar para que todas as informações sejam inseridas corretamente de modo a garantir a confiabilidade dos dados inseridos, principalmente durante a realização dos cadastros de novos usuários no sistema.

Parágrafo único. Os gestores do sistema são responsáveis pelos cadastros realizados, bem como pelas inclusões dos grupos de responsabilidade por meio da inserção de grupos de permissões aos usuários.

Art. 5º Para acesso ao sistema SESP INTRANET será necessário que todo usuário preencha o Termo de Responsabilidade, Confidencialidade e Sigilo da Informação com todas as informações solicitadas à realização de seu cadastro. O termo deverá ser assinado pelo usuário e devidamente autorizado por sua Chefia Imediata.

Parágrafo único. O Termo de Responsabilidade, Confidencialidade e Sigilo da Informação deverá conter as normativas que regulam a segurança da informação e gestão ao uso do sistema como: Política de Segurança da Informação e das Comunicações da SESP, Lei Geral de Proteção de Dados Pessoais; Código Penal; Código de Processo Penal; Código Civil; Código de Processo Civil e legislações pertinentes.

Art. 6º. O usuário poderá ter um dispositivo móvel ativo sob sua responsabilidade devidamente cadastrado no SESP Intranet. Este dispositivo, por sua vez, permitirá o acesso apenas do usuário vinculado no sistema como responsável.

Parágrafo único. Poderá ser realizado o cadastramento de múltiplos dispositivos quando os mesmos forem vinculados a um órgão e considerados assim como equipamentos funcionais. Nestes dispositivos poderão ocorrer acessos de múltiplos usuários.

Seção II

CONTROLES APLICADOS AOS USUÁRIOS DOS ÓRGÃOS DE SEGURANÇA PÚBLICA DO ESTADO DO PARANÁ

Art. 7º O acesso ao sistema deverá ser solicitado pela chefia imediata ao responsável pela Tecnologia da Informação de cada órgão de execução programática vinculado à SESP.

Art. 8º Nas situações de desligamentos, aposentadorias, exonerações, demissões, processos administrativos disciplinares e alteração de lotação dos servidores, a fim de garantir a segurança do acesso das informações, e atendendo ao disposto no artigo 4º do Decreto Estadual nº 2.484/2019, segue:

I. Os departamentos de recursos humanos dos órgãos de execução programática vinculados a SESP deverão encaminhar e-mail ao controle interno e ao responsável pela Tecnologia da Informação do respectivo órgão informando sobre as situações previstas neste caput, para que o acesso ao sistema seja removido;

I. Em situação de instauração de processo administrativo disciplinar, cabe à corregedoria do respectivo órgão deliberar sobre a retirada ou não do acesso do usuário ao sistema SESP Intranet até que todo o rito processual seja concluído, quando o usuário deverá solicitar novamente o acesso ao sistema

III. No caso de alteração de lotação do servidor, deverá ser requerido novamente o acesso ao sistema SESP Intranet, passando pelo conhecimento do novo Chefe de Seção.

Seção III
CONTROLES APLICADOS AOS USUÁRIOS DECORRENTES DE CONVÊNIOS FIRMADOS COM A SESP

Art. 9º As solicitações de acesso deverão ser recebidas, gerenciadas e executadas pelo Centro de Tecnologia da Informação e Comunicação da SESP. Cabe ao CTIC o cadastro e concessão dos acessos delimitados nos convênios aos usuários, desde que tenham sido solicitados pelo gestor técnico ou fiscal devidamente nomeados pelo órgão conveniado no contrato firmado, bem como a manutenção atualizada dos dados para contato com os gestores e fiscais.

Parágrafo único. O órgão deverá informar imediatamente ao CTIC/SESP qualquer alteração, modificação ou substituição do gestor técnico nomeado pelo órgão conveniado.

Art. 10 O órgão conveniado poderá indicar mais de um gestor técnico dependendo da amplitude de utilização do sistema.

Art. 11 O gestor técnico deverá assinar o Termo de Responsabilidade, Confidencialidade e Sigilo da Informação que conterá as diretrizes de segurança de utilização dos sistemas como Política de Segurança da Informação e das Comunicações da SESP, Lei Geral de Proteção de Dados Pessoais, Código Penal, Código de Processo Penal, Código Civil, Código de Processo Civil e legislações pertinentes às responsabilidades e obrigações inerentes à função.
Art. 12 A solicitação de cadastro e acesso ao SESP Intranet deverá ser formalizada e encaminhada a esta Secretaria contendo as seguintes informações:

I. Nome Completo;
II. CPF;
III. E-mail institucional;
IV. Telefone celular para contato;
V. Função;
VI. Órgão vinculado;
VII. Unidade de Trabalho;
VIII. Seção;
IX. Termo de responsabilidade do requisitante assinado pelo requisitante e sua chefia;
X. Número do convênio/acordo de cooperação técnica; e
XI. Data final do convênio;

Art. 13 Deverá ser realizado pelo CTIC, a cada ciclo de 12 (doze) meses da assinatura do convênio, o bloqueio de acesso de todos os usuários vinculados, devendo o gestor técnico verificar a renovação e validar os usuários pertencentes ao convênio para manutenção de acesso ao sistema.

Parágrafo único. O gestor técnico será notificado via e-mail com antecedência mínima de 60 (sessenta) dias antes do bloqueio para iniciar o processo de renovação.

Art. 14 O cadastro para o primeiro acesso será realizado pelo CTIC/SESP, enquanto a renovação poderá ser realizada pelo gestor técnico do órgão conveniado.

Seção IV
CONTROLES APLICADOS AOS USUÁRIOS ADMINISTRADORES DO SISTEMA

Art. 15 Os órgãos de execução programática deverão indicar no mínimo dois servidores de carreira para assumirem a função de usuários administradores do sistema SESP INTRANET.

Parágrafo único. Fica condicionada a indicação como administradores do sistema a servidores de carreira e devidamente vinculados com os órgãos de segurança pública do Estado do Paraná.

Art. 16 A indicação para o exercício das funções de administrador no âmbito de cada órgão deve ser formalizada, constando o Termo de Responsabilidade, Confidencialidade e Sigilo da Informação que conterá as Diretrizes de segurança de utilização dos sistemas como Política de Segurança da Informação e das Comunicações da SESP, Lei Geral de Proteção de Dados Pessoais, Código Penal, Código de Processo Penal, Código Civil, Código de Processo Civil e legislações pertinentes às responsabilidades e obrigações inerentes à função.

Art. 17 A indicação dos representantes de cada órgão de execução programática deverá ser formalizada a esta Secretaria, sendo de responsabilidade do CTIC o conhecimento e controle dos indicados, devendo ser notificado a esta Secretaria toda alteração de nome que ocorra relacionada aos representantes.

Capítulo III
DOS CONVÊNIOS E ACORDOS DE COOPERAÇÃO TÉCNICA

Art. 18 Para a realização de convênios e acordos de cooperação técnica, preliminarmente será necessária a criação de um Grupo de Trabalho técnico, com objetivo de avaliar quais sistemas pertencentes ao SESP Intranet que serão acessados e suas permissões.

Art. 19 O grupo será formado pelos gestores dos sistemas envolvidos, por representantes desta Secretaria e servidores indicados pelo órgão interessado ao convênio.

Art. 20 Os indicados para a composição do grupo serão convocados por esta secretaria para realização dos trabalhos, onde irão avaliar os seguintes aspectos técnicos:

I. Informações a serem disponibilizadas pelo convênio;
II. Sistemas a serem disponibilizados pelo convênio;
III. Contrapartida relacionada a disponibilização das informações;
IV. Risco em relação a segurança e disponibilização das informações;
V. Objetivo da disponibilização das informações;
VI. Quantidade de acessos ao(s) sistema(s) que será(ão) concedido(s); e

VII. Perfil(is) de acesso que será(ão) concedido(s).

Art. 21 O grupo técnico elaborará um documento com recomendações e o resultado da avaliação será entregue para ciência e apreciação do Encarregado de Dados Pessoais da SESP (DPO) e ao departamento responsável pela confecção do convênio.

Art. 22 O departamento responsável pela confecção do convênio deverá notificar ao responsável pela Tecnologia da Informação, Corregedoria e Inteligência do órgão de execução programática antes da assinatura do convênio quando tratar de acesso ao sistema crítico de gestão da força.

Art. 23 Todo convênio firmado deverá constar as seguintes informações técnicas no contrato:

I. Objetivo do acesso aos sistemas de informação presentes no SESP INTRANET;
II. As informações disponibilizadas pelos sistemas de informação;
III. Os sistemas liberados pelo sistema de informação;
IV. A quantidade de chaves disponibilizadas;
V. O prazo vigente do convênio;
VI. A função desempenhada por quem irá acessar os sistemas de informação; e
VII. Diretrizes e políticas de segurança de utilização dos sistemas (Política de Segurança da Informação e das Comunicações da SESP, Lei Geral de Proteção de Dados, Código Penal, Código de Processo Penal, Código Civil, Código de Processo Civil e legislações pertinentes).

Art. 24 O CTIC/SESP será responsável por coordenar e executar a liberação e revogação dos acessos disponibilizados pelo convênio.

Capítulo IV
DAS DIRETRIZES DE AUDITORIA E MONITORAMENTO

Seção I
DAS AÇÕES DE MONITORAMENTO E AUDITORIA

Art. 25 O CTIC/SESP realizará periodicamente a verificação da conformidade em relação aos acessos realizados no sistema.

Art. 26 O CTIC/SESP deverá providenciar junto à prestadora de serviço responsável pela sustentação do SESP Intranet o fornecimento de uma interface no sistema SESP Intranet que gere relatórios contendo dados dos logs realizados nas consultas pelos usuários, para fins de conhecimento da DIEP e departamentos correcionais dos órgãos de execução programática.

Art. 27 O órgão conveniado, quando tiver conhecimento de algum desvio de conduta de seus integrantes que possuam acesso ao SESP Intranet, deverá informar imediatamente ao CTIC/SESP para que diligencie as medidas pertinentes de segurança.

Seção II
DOS PEDIDOS DE RASTRO (LOGS INDIVIDUALIZADOS)

Art. 28 As solicitações de registros de rastro poderão ser formalizadas pela SESP, pelas Corregedorias e pelas Centrais de Inteligência dos órgãos de segurança pública de maneira direta à prestadora de serviços responsável pela sustentação do SESP Intranet, através do sistema e-Protocolo ou em sistema específico, limitando-se às solicitações de rastros de usuários referentes ao sistemas que se encontram sob responsabilidade de cada órgão.

§ 1 Solicitações direcionadas diretamente aos órgãos, a exemplo de requisições judiciais, cujos rastros sejam relacionados aos sistemas que não sejam de competência do órgão demandado, deverão ser remetidas a esta Secretaria a qual fará gestões junto à prestadora de serviço responsável pela sustentação do SESP Intranet.

§ 2 O Departamento de Inteligência do Estado do Paraná possui competência para formalizar solicitações de logs de acesso junto à prestadora de serviço responsável pela sustentação do SESP Intranet para fins de inteligência.

Art. 29 Os departamentos mencionados no artigo 29 possuem competência de ajustar os canais técnicos diretamente com a prestadora de serviço responsável pela sustentação do SESP Intranet.

Parágrafo único. O CTIC/SESP deverá ser cientificado dos fluxos definidos entre as partes via E-protocolo.

Art. 30 A permissão para solicitação de rastro de cada órgão é restrito aos sistemas que estejam sob a sua gestão, com exceção do DIEP e CTIC, os quais possuem permissão para solicitar rastros de todos os sistemas pertencentes ao SESP INTRANET.

Art. 31 Somente o CTIC terá competência de solicitar rastros de usuários vinculados a partir de convênios ou acordos de cooperação técnica.

Capítulo V
DA POLÍTICA DE SENHAS

Art. 32 No primeiro acesso o usuário deverá realizar a troca da senha, bem como se atentar para que a nova senha cumpra os seguintes requisitos:

I. Comprimento da senha: mínimo de dez caracteres;
II. Caracteres numéricos: mínimo de dois números;
III. Caracteres especiais: mínimo de um caractere especial;
IV. Letras maiúsculas: mínimo de uma letra maiúscula; e
V. Letras minúsculas: mínimo de uma letra minúscula.

Art. 33 A cada 6 (seis) meses o usuário deverá realizar a troca de senha, não podendo utilizar as últimas duas senhas cadastradas.

Art. 34 A senha é confidencial, intransferível e é responsabilidade do usuário mantê-la como tal, observando mecanismos de segurança e integridade.

§ 1º O usuário será responsabilizado pelas ações de outros se, desrespeitando o item anterior, deliberadamente, compartilhar sua senha e/ou acesso.

§ 2º O usuário deverá trocar sua senha imediatamente após suspeitar que foi violada ou for orientado a fazê-la pelo CTIC/SESP ou pelo responsável de TI pertencente ao órgão de execução programática na qual se encontra lotado.

Capítulo VI
DO USO INDEVIDO DO SISTEMA

Art. 35 O CTIC deverá notificar as seções correcionais e às seções de segurança da informação dos órgão vinculado ao usuário que seja identificado atividades de consultas não condizentes com suas atividades laborais, demonstrando desvio padrão comportamental para o uso individual, como a utilização da senha do usuário por terceiros ou ainda por métodos automatizados.

Art. 36 O DIEP deverá coordenar os trabalhos em conjunto com as corregedorias de cada órgão de execução programática, caso seja detectado o envolvimento de agentes de diversos órgãos de segurança.

Art. 37 É vedado o acesso ao sistema SESP Intranet e sistemas pertencentes a este ou a manipulação de seus dados a partir de softwares terceiros não homologados por esta Secretaria, ou a partir de softwares que executem tarefas automatizadas e repetitivas (bots).

Parágrafo único. O compartilhamento de dados ou a transferência de dados entre os sistemas poderá ser permitido caso esteja estabelecido nos convênios ou acordos de cooperação técnica, onde a comunicação entre os sistemas da SESP e aplicativos externos ocorrerão através de soluções de integração, interfaces de programação de aplicativos e microsserviços.

Art. 38 Em caso confirmado de uso indevido do sistema, será instaurado um Processo Administrativo para apurar os fatos.

Art. 39 O DIEP terá acesso a funcionalidade de consulta de todos os usuários do SESP Intranet, para fins de inteligência.

Capítulo VII
DAS DISPOSIÇÕES FINAIS

Art. 40 O CTIC deverá divulgar periodicamente informativos abordando tópicos relacionados à gestão de acesso e práticas de segurança.

Art. 41 O CTIC realizará gestões junto à prestadora de serviço responsável pela sustentação do SESP Intranet de modo a fornecer um manual de operação básica do sistema para fins de auxiliar os gestores técnicos.

Art. 42 O CTIC deverá promover em conjunto com os órgãos de segurança avaliações periódicas do sistema SESP INTRANET, identificando áreas de melhoria e implementando ajustes conforme necessário para manter a segurança e eficácia.

Art. 43 Os casos omissos serão avaliados pelo CTIC e, caso necessário, levados ao Comitê de Tratamento e Padronização do SESP Intranet.

Art. 44 Este conjunto de normas entrará em vigor na data da sua publicação, revogadas as disposições em contrário.

ANEXO II - TERMO DE RESPONSABILIDADE
(Órgão ou Departamento requisitante)

TERMO DE RESPONSABILIDADE, CONFIDENCIALIDADE E SIGILO DA INFORMAÇÃO - SESP INTRANET

NOME	
RG:	CPF:
ÓRGÃO VINCULADO:	UNIDADE DE TRABALHO
UNIDADE DE TRABALHO:	TELEFONE: ( )
E-MAIL INSTITUCIONAL (INDIVIDUAL)	
SOLICITO ACESSO AO SISTEMA SESP INTRANET (Módulos que serão fornecidos os acessos)	

Declaro sob as penas da lei, verdadeiras as informações neste ato prestadas, compreendendo o que estabelecem os Art. 153, 313-A, 313-B, 299, 325 e 327 do Código Penal Brasileiro, abaixo discriminados. Declaro, ainda, estar ciente das responsabilidades, confidencialidades e sigilo dos acessos a dados de segurança pública, bem como do contido na Lei Federal nº 13.709/2018 (LGPD) e o dever de não utilizar as informações acessadas para gerar benefício próprio e/ou unilateral ou para uso de terceiros, nem sequer apropriar-se de tais informações protegidas por esta legislação, e de responsabilizar-me por qualquer mau uso de minha senha, seja qual for a circunstância, estando ciente que minhas ações e consultas realizadas no sistema deverão estar restritas às atividades de serviço e delimitadas às competências e atribuições a mim designadas, passíveis de monitoramento e controle.

Comprometo-me a respeitar a Política de Segurança da Informação e Comunicações da SESP e demais normas e procedimentos de segurança, a contribuir para assegurar as propriedades de disponibilidade, integridade, confidencialidade e autenticidade das informações, bem como manter meus dados pessoais sempre atualizados junto ao cadastro.

CÓDIGO PENAL BRASILEIRO

Divulgação de Segredo – Art. 153 § 1º. A divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em Lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: Pena – detenção de 1(um) a 4 (quatro) anos e multa.

Inserção de Dados Falsos em Sistemas de Informações – Art. 313 – A .Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou banco de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena – reclusão de 2(dois) a 12(doze) anos e multa.

Modificação ou Alteração não Autorizada de Sistemas de Informações – Art. 313 – B . Modificar ou alterar, o funcionário, sistema de informação ou programa de informática sem autorização ou solicitação de autoridade competente: Pena – detenção de 3(três) meses a 2(dois) anos e multa. Parágrafo único: As penas são aumentadas de um terço até a metade se a modificação ou alteração resulta dano para a Administração Pública ou para o administrado.

Falsidade Ideológica Art. 299 - Omitir, em documento público ou particular, declaração que dele deva constituir, ou nele inserir, fazer inserir declaração falsa ou diversa da que deva ser escrita, com fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante. Pena - Reclusão de 01 (um) a 05 (cinco) anos e multa se o documento é público, e reclusão de 01 (um) a 03 (três) anos e multa se o documento é particular. Parágrafo único - Se o agente é funcionário público e comete o crime prevalecendo-se do cargo ou se a falsificação ou alteração é de assentamento de registro civil, aumenta-se a pena da sexta parte.

Violação de Sigilo Funcional - Art. 325 - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo,ou facilitar-lhe a revelação: Pena: detenção, de 6(seis) meses a 2(dois) anos, ou multa, se o fato não constitui crime mais grave.

Art. 325 § 1º - Nas mesmas penas deste artigo incorre quem: I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistema de informações ou banco de dados da Administração Pública. II – se utiliza, indevidamente, do acesso restrito. § 2º - Se da ação ou omissão resulta dano à Administração Pública ou a outrem: Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa.

Funcionário Público - Art. 327 – Considera-se funcionário público para os efeitos penais, quem, embora transitoriamente ou sem remuneração, exerce cargo, emprego ou função pública.

Art. 327 § 1º - Equipara-se a funcionário público quem exerce cargo, emprego ou função em entidade paraestatal e quem trabalha para empresa prestadora de serviço contratada ou conveniada para execução de atividade típica da Administração Pública.

327 § 2º - A pena será aumentada da terça parte quando os autores dos crimes previstos neste capítulo, forem ocupantes de cargos em comissão ou de função de direção ou assessoramento de órgão da administração direta, sociedade de economia mista, empresa pública ou fundação instituída pelo poder público.

Local e data:_____, ____/ ____/ _____.

Assinatura.

AUTORIZAÇÃO DA CHEFIA

Local e data:_____, ____/ ____/ _____.

Nome da Chefia:

Assinatura da Chefia: