SUPERINTENDÊNCIA DE SEGUROS PRIVADOS

INSTRUÇÃO NORMATIVA SUSEP Nº 35, DE 28 DE OUTUBRO DE 2025

Estabelece os Critérios de Acesso aos Recursos Computacionais da Superintendência de Seguros Privados - Susep.

O SUPERINTENDENTE DA SUPERINTENDÊNCIA DE SEGUROS PRIVADOS - SUSEP, no uso das atribuições que lhe confere os incisos V e XXII do art. 42 do Regimento Interno de que trata a Resolução CNSP nº 468, de 25 de abril de 2024, de acordo com a Resolução Susep nº 45, de 17 de outubro de 2024, e o que consta do Processo Susep 15414.613014/2016-79,

R E S O L V E :

CAPÍTULO I

DO ÂMBITO E DA FINALIDADE

Art. 1º Esta instrução normativa estabelece os Critérios de Acesso aos Recursos Computacionais da Superintendência de Seguros Privados - Susep.

Art. 2º Os Critérios de Acesso aos Recursos Computacionais da Susep são o conjunto de diretrizes, responsabilidades e competências para concessão, alteração e revogação de credenciais de acesso aos sistemas, equipamentos físicos ou virtuais e serviços de rede de computadores da Susep.

Parágrafo único. Esta norma complementa a Política de Segurança da Informação da Susep - POSIN e deve ser observada por todos os agentes públicos e terceiros a serviço da Susep.

CAPÍTULO II

CONCEITOS E DEFINIÇÕES

Art. 3º Para os efeitos desta Instrução, considera-se:

I - agente público: aquele que, por força de lei, contrato ou qualquer ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira, à Susep;

II - conta de serviço: conta de acesso a rede, sistema, serviço ou qualquer ativo, necessária a um procedimento automático (aplicação, *script*, etc.) sem qualquer intervenção humana no seu uso;

III - credencial de acesso: é a permissão lógica que habilita determinada pessoa, sistema ou organização ao acesso;

IV - perfil de acesso: é o conjunto de privilégios de acesso a recursos computacionais necessários para o desempenho de determinada função;

V - princípio do menor privilégio: é aquele que preza por delegar somente os privilégios necessários para que seu portador possa realizar sua função;

VI - rastreabilidade: é a capacidade de mapear uma ação executada por usuário ou sistema ao seu responsável, normalmente alcançada pelo uso de registros de segurança, monitoramento e mecanismos eficazes de identificação e autenticação;

VII - recursos computacionais: são sistemas, redes, bancos de dados, serviços de rede ou equipamentos de informática colocados à disposição dos agentes públicos a serviço da Susep;

VIII - senha forte: sequência de caracteres alfanuméricos que seguem as boas práticas do mercado e cumprem as regras indicadas pela área de Tecnologia da Informação - TI, tais como comprimento mínimo, não obviedade, contendo algarismos, letras maiúsculas, minúsculas e caracteres especiais;

IX - serviço de diretório: infraestrutura de TI que, de forma centralizada e segura, armazena, organiza e fornece acesso a informações sobre recursos de rede, como usuários, ativos e políticas;

X - serviço de rede: é um serviço que provê determinada funcionalidade aos usuários ou sistemas de uma rede de computadores;

XI - termo de responsabilidade: documento assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

XII - titular: agente público ocupante de cargo em comissão ou detentor de função gratificada que exerça a chefia de uma unidade organizacional da Susep ou que detenha competência legal ou regulamentar para responder por determinada unidade;

XIII - unidade: unidade organizacional da Susep; e

XIV - usuário: agente público ou qualquer pessoa física que obteve autorização para acesso a um ou mais recursos computacionais da Susep.

CAPÍTULO III
DAS DISPOSIÇÕES GERAIS

Art. 4º Serão centralizados os recursos utilizados na gestão do acesso a recursos computacionais, incluindo a autenticação, autorização e auditoria.

Parágrafo único. A gestão de contas será centralizada por meio de serviço de diretório e identidade.

Art. 5º Os usuários receberão identificação única (*login*) criada pela área de TI.

§ 1º O *login* do usuário comporá as suas credenciais.

§ 2º Todo acesso a recurso computacional lógico cujo acesso seja objeto de controle se dará por meio de credenciais de usuário.

§ 3º A área de TI estabelecerá regras criação de senhas fortes e períodos de redefinição de senhas não superiores que cento e vinte dias.

Art. 6º A Susep deverá adotar técnicas de segmentação de rede visando limitar o acesso de forma eficiente e segura, assegurando que apenas colaboradores e dispositivos autorizados possam interagir com partes específicas da rede.

Art. 7º Os recursos computacionais da Susep podem estar acessíveis aos usuários pelos seguintes meios:

I - conexão direta às redes de computadores da Susep;

II - acesso via *Virtual Private Network* - VPN; e

III - acesso via Internet.

Art. 8º Os sistemas e serviços de rede da Susep desenvolvidos após a entrada em vigor desta norma deverão ter seus acessos registrados de forma a permitir a rastreabilidade e a identificação do usuário pelo período mínimo de cento e oitenta dias.

Parágrafo único. Os recursos mencionados não são obrigatórios em sistemas desenvolvidos por terceiros.

Art. 9º O acesso a recursos computacionais deverá ocorrer através de mecanismos de identificação e autenticação do usuário.

§ 1º A autenticação de usuários para acesso remoto a recursos computacionais de uso exclusivo de usuários da SUSEP será obrigatoriamente por mais de um fator, e preferencialmente dessa forma, para acesso por meio de rede local física.

§ 2º O acesso pela internet a sistemas desenvolvidos pela Susep deverá ser realizado, preferencialmente, por meio do sistema de *login* único do Governo Federal - GOV.BR, observados os níveis de autenticação, conforme a criticidade da informação ou do serviço acessado.

Art. 10. Os acessos automatizados aos recursos computacionais realizados por sistemas deverão ser realizados por meio de contas de serviço, as quais não poderão ser utilizadas para outros fins.

Art. 11. O acesso aos recursos computacionais da Susep é sempre motivado por necessidade de serviço, respeita o princípio do menor privilégio e deve ser controlado e restrito às pessoas autorizadas, sendo concedido mediante a assinatura de Termo de Responsabilidade (Anexo I).

§ 1º As credenciais de acesso aos recursos computacionais são de uso pessoal e intransferível, não podendo a pessoa autorizada deixar qualquer recurso computacional em condições de ser utilizado com suas credenciais de acesso por terceiros.

§ 2º As credenciais de acesso devem ser graduadas de acordo com as atribuições dos agentes públicos.

§ 3º O Termo de Responsabilidade de que trata o *caput* poderá ser substituído por seu equivalente em meio digital assinado uma única vez mediante identificação e autenticação.

§ 4º A área de TI deverá disponibilizar em até noventa dias da entrada em vigor deste normativo procedimento para assinatura do Termo de Responsabilidade em meio físico ou digital.

§ 5º A atualização do teor do Termo de Responsabilidade, pela área de TI, implicará a convocação dos signatários do termo antigo para a assinatura de novo termo.

Art. 12. O acesso ao recurso computacional não gera direito sobre o mesmo.

CAPÍTULO IV
DAS REDES DE COMPUTADORES

Art. 13. O acesso lógico aos ambientes de rede destinados ao desenvolvimento de sistemas é restrito à área de TI.

Art. 14. O acesso às redes de computadores da Susep somente é feito por conexão direta à rede local ou VPN.

§ 1º Deverão ser utilizados mecanismos automáticos para inibir que equipamentos externos, tais como computadores portáteis, celulares e *tablets*, se conectem diretamente à rede local da Susep.

§ 2º Deverá ser mantido mecanismo que permita identificar os endereços IP de origem e destino das conexões, bem como os serviços utilizados.

§ 3º O acesso remoto às redes de computadores deverá utilizar, no mínimo, autenticação por dois fatores, ser criptografado e gerar registros de auditoria que contenham informações que facilitem o rastreamento das ações tomadas.

§ 4º Deverá atender às condições estabelecidas pela área de segurança da informação da Susep o acesso à rede da Susep através de VPN realizado por meio de dispositivo não pertencente à Susep.

CAPÍTULO V

DOS SISTEMAS DE INFORMAÇÃO

Art. 15. Os acessos aos sistemas da Susep que contenham informação classificada em qualquer grau de sigilo deverão obedecer aos requisitos dispostos no Decreto nº 7.845, de 14 de maio de 2012 e demais normas regulamentadoras.

Art. 16. O acesso direto aos bancos de dados da Susep é restrito à área de TI, que deverá buscar o provimento dos meios de consulta necessários.

Parágrafo único. Até a criação de ambiente próprio para consulta direta às bases de dados pelos demais usuários, o acesso será concedido mediante assinatura de Termo de Responsabilidade para acesso de leitura a base de dados (Anexo II).

CAPÍTULO VI

DA CONCESSÃO E DA ALTERAÇÃO DE ACESSOS

Art. 17. O credenciamento de pessoas e a criação de contas para acesso aos recursos computacionais somente podem ser realizados após a entrada em exercício ou contratação do agente público.

Art. 18. O credenciamento de pessoas, a criação de usuários e o controle de acesso aos recursos computacionais da Susep são baseados em perfis de acesso.

§ 1º A área gestora, em conjunto com a área de TI, definirá os perfis de acesso disponíveis a cada recurso computacional, incluídos os ambientes de rede destinados a desenvolvimento, homologação e produção de sistemas.

§ 2º Ao solicitar acesso a recursos computacionais, a unidade organizacional da Susep deverá informar os perfis de acesso a recursos computacionais considerados necessários aos usuários incluídos naquela solicitação.

§ 3º Os perfis de acesso que contenham privilégios de administração somente poderão ser atribuídos a usuários que executem tarefas específicas na administração dos recursos computacionais.

Art. 19. Os titulares das unidades que receberem usuários externos à Susep com necessidade de acesso temporário aos recursos computacionais deverão solicitá-los à área responsável pela configuração do acesso, que consultará os gestores dos recursos computacionais.

§ 1º A concessão de credenciais de acesso a agentes externos dar-se-á apenas nos casos de redes destinadas para este fim ou nos casos previstos em lei.

§ 2º Tão logo o acesso temporário a recursos computacionais deixe de ser necessário, o titular da unidade solicitante deve solicitar a revogação do acesso.

CAPÍTULO VII

DA REVOGAÇÃO DE ACESSOS

Art. 20. Por ocasião do desligamento da Susep todas as credenciais de acesso a recursos computacionais serão revogadas.

Art. 21. Nas alterações de lotação, serão revogadas as credenciais de acesso concedidas na unidade de origem.

Art. 22. Nas alterações de ocupação de cargos ou funções serão revogadas todas as credenciais de acesso relacionadas à unidade de origem do usuário que deixa o cargo ou função.

Art. 23. Nos afastamentos superiores a trinta dias, as credenciais de acesso serão suspensas até o retorno do agente público às suas atividades

CAPÍTULO VIII

DO CONTROLE DO ACESSO FÍSICO

Art. 24. A área de TI definirá perímetros de segurança para proteção de ambientes e ativos de TI contra acesso físico não autorizado.

CAPÍTULO IX

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 25. Compete à área de TI:

I - informar aos titulares das unidades, sempre que necessário, os perfis disponíveis para acesso a determinado recurso computacional bem como os atuais usuários que possuem perfis concedidos;

II - submeter solicitações de acesso aos recursos computacionais aos respectivos gestores;

III - adotar as ações técnicas necessárias para o provimento de acesso aos recursos computacionais da Susep e ao cumprimento integral desta norma;

IV - divulgar e manter atualizada lista de recursos computacionais da Susep e de seus respectivos gestores;

V - estabelecer e manter um inventário dos sistemas de autenticação e autorização da Susep, revisando-o pelo menos uma vez por semestre;

VI - bloquear credenciais, sem prévio aviso:

a) cujo sigilo lhe pareça ter sido violado;

b) envolvidas em tentativas sequenciadas de acesso com senha errada;

c) utilizadas em ataques à infraestrutura da Susep;

d) utilizadas de forma a resultar em degradação ou indisponibilidade de serviço ou recurso de TI; ou

e) utilizadas em desconformidade com a POSIN; e

VII - propor a localização, resistência e requisitos de auditoria dos perímetros de segurança a serem aplicados em torno de áreas e ativos a serem protegidos, em função de sua criticidade para a segurança da informação e continuidade dos negócios da Susep.

Art. 26. Compete ao Comitê de Governança Digital - CGD:

I - chancelar os gestores dos recursos computacionais apresentados pelas unidades da Susep ao CGD;

II - alterar os gestores dos recursos computacionais da Susep; e

III - tratar os casos omissos ou conflitantes relacionados a gestão de recursos computacionais da Susep.

Art. 27. Compete ao Comitê de Segurança da Informação - CSI promover a revisão e a atualização periódicas desta norma.

Art. 28. Compete aos titulares das unidades:

I - informar à área de TI, juntamente com solicitação de acesso a recurso computacional, os perfis de acesso aos recursos computacionais necessários à sua unidade, incluídos os funcionários terceirizados e estagiários;

II - revisar periodicamente, pelo menos uma vez por semestre, as permissões atribuídas a usuários em recursos sob sua responsabilidade, podendo solicitar à área de TI as permissões vigentes sempre que necessário; e

III - autorizar ou solicitar a concessão, alteração e a revogação de credenciais de acesso nos recursos computacionais sob sua responsabilidade.

Art. 29. Compete aos usuários dos recursos computacionais da Susep:

I - informar à área de TI imediatamente sobre o comprometimento e eventual utilização indevida de suas credenciais de acesso aos recursos computacionais;

II - comunicar ao CSI as operações identificadas que resultem em descumprimento de dispositivos desta norma;

III - cumprir o disposto nos Termos de Responsabilidade de que é signatário, conforme Anexos I e II; e

IV - cumprir as boas práticas em privacidade e segurança da informação, especialmente as divulgadas pela área de TI, ao acessar recursos computacionais.

Art. 30. Compete à área de documentação:

I - informar aos titulares das unidades, sempre que necessário, os perfis disponíveis para acesso ao Sistema Eletrônico de Informações - SEI, bem como os atuais usuários que possuem perfis concedidos; e

II - adotar as ações necessárias para o provimento de acesso SEI da Susep e ao cumprimento integral desta norma, observando subsidiariamente o disposto na Instrução Susep nº 89, de 28 de março de 2018.

Art. 31. Compete à área de pessoas informar a área de TI das alterações de lotação, ocupação e alteração de cargos ou funções, afastamentos por períodos superiores a trinta dias e demais assentamentos de servidores e estagiários, que impliquem alteração de credenciais de acesso.

§ 1º As atualizações devem ser feitas por meio de abertura de chamado de TI.

§ 2º As atualizações devem ser comunicadas tão logo o respectivo ato tenha sido publicado.

Art. 32. Compete ao gestor dos contratos que envolvam funcionários terceirizados, informar a área de TI movimentações de funcionários que impliquem alteração de credenciais de acesso.

§ 1º As atualizações devem ser feitas por meio de abertura de chamado de TI.

§ 2º As atualizações devem ser comunicadas tão logo ocorra a movimentação.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 33. Fica revogada a Instrução Susep nº 83, de 31 de março de 2017.

Art. 34. Esta Instrução entra em vigor na data da sua publicação.

Documento assinado eletronicamente por **ALESSANDRO SERAFIN OCTAVIANI LUIS (MATRÍCULA 1860655)**, **Superintendente da Susep**, em 18/11/2025, às 08:34, conforme horário oficial de Brasília, de acordo com o art. 6º do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site https://sei.susep.gov.br/sei/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2553041** e o código CRC **BC13FB7B**.

ANEXO I

SERVIÇO PÚBLICO FEDERAL

SUPERINTENDÊNCIA DE SEGUROS PRIVADOS

TERMO DE RESPONSABILIDADE PARA ACESSO A RECURSOS COMPUTACIONAIS

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, DECLARO , sob pena das sanções cabíveis nos termos da legislação vigente que assumo a responsabilidade por:

I) conhecer e observar o disposto na Resolução Susep nº 45, de 17 de outubro de 2024, POSIN;

II) tratar o(s) recurso(s) computacionais como patrimônio da Susep;

III) utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço da Susep;

IV) assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações sob minha custódia, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 27 de maio de 2020, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

V) utilizar as credenciais, as contas de acesso e os recursos computacionais em conformidade com a legislação vigente e normas específicas da Susep;

VI) responder, perante a Susep, pelo uso indevido das minhas credenciais ou contas de acesso e dos recursos computacionais;

VII) zelar pela segurança e pela integridade dos equipamentos de propriedade da Susep a mim disponibilizados;

VIII) em caso de acesso a informações da Susep através de equipamentos particulares ou de terceiros, garantir que estes possuam recursos mínimos de segurança (sistema operacional, antivírus e cliente VPN atualizados); e

IX) reconhecer o acréscimo de responsabilidade nos casos de perfil de acesso diferenciado como acesso direto a banco de dados, privilégios de administração, ferramentas de desenvolvimento, dentre outros.

Local, _____de _____de _____ .

_____

Assinatura

Nome do usuário, unidade e matrícula

ANEXO II

SERVIÇO PÚBLICO FEDERAL

SUPERINTENDÊNCIA DE SEGUROS PRIVADOS

TERMO DE RESPONSABILIDADE PARA ACESSO DE LEITURA A BASE DE DADOS

Pelo presente instrumento, eu _____, Matrícula SIAPE _____, DECLARO, sob pena das sanções cabíveis nos termos da legislação vigente que assumo a responsabilidade por autorizar o acesso do servidor _____, Matrícula SIAPE _____, para **leitura** na base de dados do sistema _____, devendo informar à área de TI tão logo tal credencial de acesso não seja mais necessária.

O servidor supracitado se compromete a preservar a confidencialidade dos dados consultados, especialmente informações cuja divulgação possa causar risco ou dano à segurança da sociedade ou do Estado, que em função de seu potencial de aproveitamento de oportunidades nos ramos econômico, político, científico, tecnológico, militar e social, possam indevidamente beneficiar a si ou a terceiros, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, utilizando-as no estrito interesse de suas atividades na SUSEP.

Compromete-se, ainda, a não copiar ou reproduzir, por qualquer meio ou modo as informações a que tiver acesso, exceto para a consecução das atividades da SUSEP, caso, em que deverá manter cópia(s) somente pelo período necessário à sua utilização.

Em todo o trato com o acesso concedido, o servidor se compromete a observar e cumprir as disposições da Lei nº 13.709, de 14 de agosto de 2018 - LGPD, responsabilizando-se por qualquer violação decorrente da permissão de leitura a que se refere este Termo.

O servidor se compromete, por fim, a preservar a disponibilidade dos ambientes de sistemas da Susep, notificando a área de TI caso deseje efetuar pesquisa no banco de dados que possa vir a degradar o desempenho dos sistemas implantados. Caso a área de TI identifique o efetivo impacto dessas consultas sobre o desempenho dos sistemas da Autarquia, poderá cancelar imediatamente a execução das mesmas e a credencial de acesso, sem notificação prévia.

_____

Assinatura

Titular de unidade responsável, unidade e matrícula

_____

Assinatura

Nome do usuário, unidade e matrícula