



SUPERINTENDÊNCIA DE SEGUROS PRIVADOS

INSTRUÇÃO SUSEP Nº 83, DE 31 DE MARÇO DE 2017.

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 o inciso X do artigo 73 do Regimento Interno de que trata a Resolução CNSP nº 338, de 9 de maio de 2016, e o que consta do Processo Susep nº 15414.613014/2016-79,

RESOLVE:

CAPÍTULO I

DO ÂMBITO E DA FINALIDADE

Art. 1º Estabelecer 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 e serviços de rede de computadores da Susep.

Parágrafo único. Esta norma complementa a Política de Segurança da Informação e Comunicações – Posic e deve ser observada por todos os agentes públicos 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, serviços de rede ou equipamentos de informática colocados à disposição dos agentes públicos a serviço da Susep;

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

IX - 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;

X - 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;

XI - unidade: unidade organizacional da Susep;

XII - 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 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 rede privada virtual (VPN); e

III – acesso via Internet.

Art. 5º 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 180 dias.

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

Art. 6º Os recursos computacionais deverão contemplar mecanismos de identificação e autenticação do usuário.

Parágrafo único. Sempre que possível, deverão ser contemplados mecanismos de autenticação por pelo menos dois fatores, tais como biometria e certificação digital.

Art. 7º 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. 8º 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 90 (noventa) dias da entrada em vigor deste normativo procedimento para assinatura do Termo de Responsabilidade em meio físico ou digital.

Art. 9º O acesso ao recurso computacional não gera direito sobre o mesmo.

CAPÍTULO IV DAS REDES DE COMPUTADORES

Art. 10. O acesso lógico aos ambientes de rede destinados ao desenvolvimento de sistemas é restrito à área de TI.

Art. 11. O acesso às redes de computadores da Susep somente é feito por conexão direta à rede local ou rede privada virtual (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.

CAPÍTULO V DOS SISTEMAS DE INFORMAÇÃO

Art. 12. Os acessos aos sistemas da Susep que contenham informação classificada em qualquer grau de sigilo deverão obedecer aos requisitos dispostos no Decreto nº 7845/12 e demais normas regulamentadoras.

Art. 13. 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. 14. 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. 15. 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. 16. 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. 17. Por ocasião do desligamento da Susep todas as credenciais de acesso a recursos computacionais serão revogadas.

Art. 18. Nas alterações de lotação, a revogação de credenciais de acesso deverá ser objeto de solicitação por parte do titular da unidade de origem.

Art. 19. 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. 20. Nos afastamentos superiores a 30 (trinta) dias, as credenciais de acesso serão suspensas mediante comunicação dos titulares de unidades até o retorno do agente público às suas atividades.

CAPÍTULO VIII

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 21. 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; e

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

Art. 22. Compete ao CTIC:

I – definir os gestores dos recursos computacionais da Susep; e

II – divulgar e manter atualizada as listas de recursos computacionais da Susep e de seus respectivos gestores.

Art. 23. Compete ao CSIC:

I – promover a revisão e a atualização periódicas desta norma.

Art. 24. 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 as permissões atribuídas a usuários em recursos sob sua responsabilidade, tais como servidor de arquivos, caixas corporativas, sistemas de processos e emissão de documentos, entre outros, podendo solicitar à área de TI as permissões vigentes sempre que necessário;

III – informar a área de TI das alterações de lotação, ocupação e alteração de cargos ou funções, afastamentos por períodos superiores a 30 (trinta) dias e demais assentamentos de servidores, funcionários terceirizados e estagiários que impliquem em alteração de credenciais de acesso. As atualizações devem ser feitas nos seguintes prazos:

a) nos casos de afastamento, tão logo tome conhecimento do fato, informando também a data de retorno;

b) na alteração de cargos ou funções, tão logo seja realizada a publicação; e

c) na alteração de lotação, tão logo a mesma seja formalizada.

IV – informar a área de TI das alterações de lotação de funcionários terceirizados tão logo tome conhecimento do fato;

V - realizar a concessão, alteração e a revogação de credenciais de acesso nos recursos computacionais em que as permissões de usuário sejam gerenciadas pela unidade, tal qual as caixas corporativas do serviço de correio eletrônico.

Art. 25. 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; e

II – comunicar ao CSIC as operações identificadas que resultem em descumprimento de dispositivos desta norma.

Art. 26. 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;

II – adotar as ações necessárias para o provimento de acesso ao Sistema Eletrônico de Informações – SEI da Susep e ao cumprimento integral desta norma, observando subsidiariamente o disposto na Instrução Susep nº 78/2016.

CAPÍTULO IX DAS DISPOSIÇÕES FINAIS

Art. 27. Esta Instrução entra em vigor após decorridos 90 dias de sua publicação oficial.

JOAQUIM MENDANHA DE ATAÍDES

Superintendente



Documento assinado eletronicamente por **JOAQUIM MENDANHA DE ATAÍDES (MATRÍCULA 2325827)**, Superintendente da Susep, em 03/04/2017, às 10:41, conforme horário oficial de Brasília, com fundamento nos art. artigos 369, 405 e 425 da lei nº 13.105/2015 c/c Decreto nº 8.539/2015 e Instruções Susep 78 e 79 de 04/04/2016 .



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 **0091776** e o código CRC **872F2EA9**.

ANEXO I À MINUTA DE INSTRUÇÃO

TERMO DE RESPONSABILIDADE PARA ACESSO A RECURSOS COMPUTACIONAIS

SERVIÇO PÚBLICO FEDERAL

SUPERINTENDÊNCIA DE SEGUROS PRIVADOS

TERMO DE RESPONSABILIDADE

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

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

III) contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

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

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

Rio de Janeiro - RJ, _____ de _____ de _____.

Assinatura

Nome do usuário, unidade e matrícula

ANEXO II À MINUTA DE INSTRUÇÃO

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.

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

Referência: Processo nº 15414.613014/2016-79

SEI nº 0091776