SUPERINTENDÊNCIA DE SEGUROS PRIVADOS

RESOLUÇÃO SUSEP Nº 45, DE 17 DE OUTUBRO DE 2024

Institui a Política de Segurança da Informação – Posin, da Superintendência de Seguros Privados – Susep.

O SUPERINTENDENTE DA SUPERINTENDÊNCIA DE SEGUROS PRIVADOS - SUSEP torna público que o Conselho Diretor da Autarquia, em reunião ordinária realizada em 16 de outubro de 2024, no uso das atribuições que lhe confere o inciso V do art. 8º do Regimento Interno de que trata a Resolução CNSP nº 468, de 25 de abril de 2024; na forma estabelecida pela Resolução Susep nº 01, de 24 de agosto de 2021 e considerando o disposto na Resolução Susep nº 31, de 3 de novembro de 2023, e o que consta do Processo Susep nº 15414.632123/2024-03,

R E S O L V E :

Art. 1º Instituir a Política de Segurança da Informação- P o s i n da Superintendência de Seguros Privados - Susep.

CAPÍTULO I

DO ESCOPO

Art. 2º A Política de Segurança da Informação - Posin objetiva instituir diretrizes estratégicas, responsabilidades e competências, visando assegurar integridade, confidencialidade, disponibilidade e autenticidade dos dados e informações da Susep.

§ 1º As diretrizes estabelecidas na Posin devem estar alinhadas ao planejamento estratégico institucional e em consonância com seus valores.

§ 2º A Posin deverá ser observada por todos os agentes públicos a serviço da Susep, doravante denominados agentes públicos.

§ 3º A Posin trata das diretrizes gerais acerca do uso e compartilhamento de ativos de informação durante todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento, transporte e descarte), visando à continuidade dos processos críticos da Susep, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, bem como os valores éticos e as melhores práticas de segurança da informação - SI.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para fins da Posin, entende-se por:

I - acesso: ato de ingressar, transitar, conhecer ou consultar dados ou informações, bem como a possibilidade de usar os ativos de informação;

II - 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;

III - ameaça: conjunto de fatores internos, externos ou causa potencial de um incidente, que pode resultar comprometimento da segurança dos ativos da organização;

IV - ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

V - ativo de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

VI - autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

VII - avaliação de riscos: processo de comparar o risco com critérios de risco predefinidos, para determinar a importância do risco;

VIII - bloqueio de acesso: processo que tem por finalidade suspender temporariamente o acesso;

IX - confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

X - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder, monitorar ou bloquear o acesso;

XI - classificação: atribuição de grau de sigilo a ativo de informação que esteja em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, a qual é classificada como ultrassecreta, secreta ou reservada;

XII - credencial de acesso: permissão concedida por autoridade competente, após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso de recursos, podendo ser física (como por exemplo um crachá), ou lógica (como por exemplo a identificação de usuário e senha);

XIII - credencial de segurança: certificado que autoriza pessoa para o tratamento de informação classificada;

XIV - crítico: ativo de cuja segurança a organização depende, em maior ou menor grau, para a continuidade de suas atividades e serviços;

XV - descarte: eliminação correta de informações, documentos, mídias e acervos digitais;

XVI - desclassificação: cancelamento da classificação de ativos de informação, por agente público ou pelo transcurso de prazo, tornando-os ostensivos;

XVII - disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

XVIII - evento: ocorrência gerada a partir de fontes internas ou externas que pode resultar em uma ou mais consequências de impacto negativo, positivo ou ambos, sendo que os eventos que causam impacto negativo representam riscos negativos e aqueles que causam impacto positivo representam riscos positivos, conforme definido pela Deliberação Susep nº 233, de 06 de Dezembro de 2020 – Política de Gestão de Riscos da Susep;

XIX - gestão de riscos: conjunto de conceitos, princípios, competências e diretrizes para dirigir e controlar uma instituição no que se refere a riscos, conforme definido pela Deliberação Susep nº 233, de 2020 - Política de Gestão de Riscos da Susep;

XX - gestor do ativo: gestor da unidade designada para responder pelo ativo como parte de sua atribuição regimental ou, nos casos omissos, por designação específica de superior hierárquico, ou ato normativo, tornando-se responsável pela sua segurança;

XXI - grau de sigilo: gradação atribuída a ativos de informação em decorrência do teor e elementos intrínsecos das informações e dados sigilosos que contenham;

XXII - impacto: grau ou importância dos efeitos da ocorrência de um risco, estabelecido a partir de uma escala predefinida de magnitudes possíveis, conforme definido pela Política de Gestão de Riscos da Susep;

XXIII - incidente: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação

protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

XXIV - informação sigilosa: informação submetida temporariamente à restrição de acesso público, em razão de sua imprescindibilidade para a segurança da sociedade e do Estado; e aquela abrangida pelas demais hipóteses legais de sigilo;

XXV - integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXVI - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade, descrevendo a restrição de dados que sejam considerados extremamente sigilosos; sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

XXVII - privilégio mínimo: definição de permissões de acesso a informações de modo que as ações possíveis de um colaborador estejam limitadas àquelas necessárias ao desempenho de sua função;

XXVIII - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da Segurança da Informação;

XXIX - reclassificação: alteração da classificação de ativos de informação;

XXX - risco: efeito da incerteza nos objetivos, onde o efeito é um desvio em relação ao esperado (positivo ou negativo), conforme definido pela Política de Gestão de Riscos da Susep;

XXXI - tratamento de riscos: processo de seleção e implantação de medidas que visem a modificar os riscos;

XXXII - unidade: parte integrante da estrutura organizacional da Susep, com sigla e atribuições definidas no Regimento Interno da Autarquia; e

XXXIII - vulnerabilidade: condição que, quando explorada por um criminoso cibernético, pode resultar em uma violação de segurança cibernética dos sistemas computacionais ou redes de computadores, e consiste na interseção de três fatores: suscetibilidade ou falha do sistema, acesso possível à falha e capacidade de explorar essa falha.

Parágrafo único. As definições constantes na Portaria GSI/PR nº 93, de 18 de outubro de 2021, aplicam-se subsidiariamente a este ato normativo.

CAPÍTULO III

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 4º A Posin obedecerá à legislação e às normas específicas, destacando-se:

I - Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

II - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;

III - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências;

IV - Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados;

V - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

VI - Decreto nº 4.073, de 3 de janeiro de 2002, que regulamenta a Lei nº 8.159, de 8 de janeiro de 1991;

VII - Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

VIII - Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

IX - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

X - Decreto nº 10.748, de 16 de julho de 2021, que Institui a Rede Federal de Gestão de Incidentes Cibernéticos;

XI - Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

XII - Instrução Normativa GSI/PR nº 03, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

XIII - Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – Etir nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XIV - Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação;

XV - Norma Complementar nº 08/IN01/DSIC/GSIPR, 19 de agosto de 2010, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - Etir dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XVI - Norma Complementar n.º 09/IN01/DSIC/GSIPR, de 19 de novembro de 2010, que estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF;

XVII - Normas ABNT NBR ISO/IEC 27001, 27002 e 27005, que instituem melhores práticas para gestão da segurança da informação;

XVIII - Deliberação Susep nº 135, de 20 de abril de 2009, que aprova o Código de Ética Profissional do Servidor da Superintendência de Seguros Privados – Susep;

XIX - Deliberação Susep nº 233, de 06 de Dezembro de 2019 - Política de Gestão de Riscos da Susep;

XX - Decreto nº 10.748, de 16 de julho de 2021, que Institui a Rede Federal de Gestão de Incidentes Cibernéticos; e

XXI - *CIS Critical Security Controls Version 8* que consiste em um conjunto priorizado de ações para proteger organizações de vetores de ciberataques conhecidos.

CAPÍTULO IV

DOS PRINCÍPIOS

Art. 5º A Posin seguirá os seguintes princípios:

I - legalidade: a Posin está sujeita aos mandamentos da lei e sua elaboração/atualização seguirá rigorosamente as prescrições da legislação pertinente;

II - moralidade: a elaboração da Posin, bem como sua posterior aplicação, deverá observar os preceitos da boa administração pública, pautando-se pela atuação ética e nos ideais de honestidade e justiça;

III - impessoalidade: a Posin visará ao interesse público no tratamento das informações, buscando evitar que estas sejam utilizadas para finalidades particulares ou para a obtenção de benefícios pessoais;

IV - publicidade: a Posin buscará garantir o amplo acesso do público à informação, exceto quando o próprio interesse público justificar seu sigilo; e

V - eficiência: a Posin terá como objetivo tornar a atuação da Susep mais rápida e precisa, por meio

do tratamento efetivo das informações.

CAPÍTULO V

DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 6º Deverá ser assegurada a manutenção na função de Gestor de Segurança da Informação de um servidor público civil ocupante de cargo efetivo, ou militar de carreira, com formação ou capacitação técnica compatível com as atribuições.

Art. 7º Deverá ser assegurada a manutenção da existência do Comitê de Segurança da Informação, levando em consideração o que consta da Resolução Susep nº 31, de 2023, ou de ato normativo que venha a substituí-la.

Art. 8º Deverá ser instituída uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - Etir, na forma a ser regulamentada em normativo próprio, o qual designará suas atribuições e seu escopo de atuação.

CAPÍTULO IV

DAS DIRETRIZES

Seção I

Das Diretrizes gerais

Art. 9º Qualquer informação recebida, produzida ou adquirida, deve ser tratada como patrimônio da Susep, a ser protegida nos termos desta Política e das demais normas em vigor, com vistas ao atendimento do interesse público e ao cumprimento da missão da Autarquia.

Parágrafo único. Em contratos celebrados com pessoa jurídica, o termo de confidencialidade poderá ser assinado pelo preposto.

Art. 10. Todos os ajustes celebrados pela Susep com prestadores de serviços em suas instalações deverão conter cláusulas referentes ao cumprimento da Posin, de suas normas e padrões complementares, bem como à manutenção do sigilo de suas informações durante e após sua vigência.

Art. 11. Os prestadores de serviços sob contrato com a Susep serão obrigados a assinar termo de confidencialidade, em obediência ao estabelecido na Posin.

Parágrafo único. Em contratos celebrados com pessoa jurídica, o termo de confidencialidade poderá ser assinado pelo preposto.

Seção II

Do tratamento da informação

Art. 12. As informações e dados produzidos ou recebidos pela Susep em decorrência de sua função serão considerados ostensivos, a menos que sua divulgação possa acarretar, entre outros:

I - danos a consumidores e acionistas das entidades supervisionadas;

II - instabilidade dos mercados supervisionados;

III - frustração de estratégias comerciais das entidades supervisionadas;

IV - desrespeito à propriedade intelectual;

V - prejuízo às atividades de supervisão e fiscalização;

VI - riscos à continuidade operacional da Susep;

VII - desobediência a hipóteses legais de sigilo;

VIII - quebra de contratos ou convênios;

IX - riscos à segurança nacional; e

X - violação da intimidade da vida privada, da honra e da imagem das pessoas ligadas ou não à Susep.

Art. 13. As informações poderão ser classificadas como reservadas, secretas ou ultrassecretas em razão do teor de seus elementos intrínsecos e dados que contenham, conforme definido em legislação específica.

Parágrafo único. Durante todo o ciclo de vida de um dado ou informação sigilosa ou classificada, sua hospedagem e tratamento observarão medidas especiais de segurança compatíveis com seu grau de sigilo e em conformidade com a legislação vigente e normas complementares adotadas pela Susep.

Seção III

Do tratamento de incidentes de segurança cibernética

Art. 14. Nos contratos de serviços relacionados ao provimento, gerenciamento e suporte da infraestrutura computacional de TI deverá constar cláusula que exija a existência de estrutura de tratamento de incidentes de segurança cibernética por parte do prestador.

Parágrafo único. Em relação aos contratos mencionados no *caput*, cabe ao fiscal técnico supervisionar o tratamento de incidentes de segurança cibernética para o fiel cumprimento das suas atribuições com o apoio da Etir.

Art. 15. A Etir tem autonomia para tomar ações emergenciais para a resposta aos incidentes de segurança cibernética no âmbito da Susep.

Art. 16. A Etir deverá manter mecanismos de articulação com o Centro de Prevenção, Tratamento e Resposta a de Incidentes Cibernéticos do Governo (CTIR Gov) ou estrutura que o venha a substituir nesta função.

Seção IV

Do processo de gestão de riscos

Art. 17. A gestão de riscos em Segurança da Informação constitui um processo contínuo de levantamentos, análises, avaliações e planos de tratamento que visem manter em níveis aceitáveis os riscos de Segurança da Informação a que está sujeita a Susep, estando sempre alinhada com o planejamento estratégico da Autarquia.

Art. 18. O processo de gestão de riscos de Segurança da Informação será definido em norma complementar e observará a Política de Gestão de Riscos da Susep.

Seção V

Da gestão de continuidade

Art. 19. A implementação do processo de gestão de continuidade de negócios em segurança da informação tem o objetivo de minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades da Susep nessa área, além de recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de resposta a incidentes e recuperação de desastres.

Art. 20. O processo de gestão de continuidade de negócios em segurança da informação deve ser baseado nas estratégias de continuidade para as atividades críticas, na avaliação dos riscos levantados no processo de gestão de riscos e em diretrizes institucionais sobre gestão de continuidade de negócio.

Art. 21. Será elaborado e mantido Plano de Continuidade de Negócios em Segurança da Informação - PCNSI, baseado em boas práticas e aprovado pelo CSI, que deverá ser implementado e testado periodicamente para garantir a continuidade dos serviços críticos de TI.

Seção VI

Da auditoria e conformidade

Art. 22. A avaliação de conformidade nos aspectos de segurança da informação consiste em proporcionar adequado grau de confiança a um determinado processo, mediante o atendimento de requisitos

definidos em políticas, procedimentos, normas ou em regulamentos técnicos aplicáveis.

Art. 23. Deverá ser designado ao menos um servidor efetivo, militar de carreira ou empregado público, lotado na Susep, como responsável pela avaliação de conformidade nos aspectos relativos à segurança da informação.

Parágrafo único. A designação a que se refere o *caput* não poderá recair sobre membros da equipe de gestão de segurança da informação.

Art. 24. Deverá ser criado um processo de avaliação de conformidade nos aspectos relativos à segurança da informação, contendo, no mínimo:

I - as unidades a serem abrangidas;

II - os aspectos a serem observados para verificação da conformidade;

III - as ações e atividades a serem realizadas;

IV - os documentos necessários para fundamentar a verificação de conformidade; e

V - as responsabilidades.

Art. 25. A Susep manterá registros e procedimentos, como trilhas de auditoria e outros, que assegurem o rastreamento, acompanhamento, controle e verificação de acessos aos seus ativos, observando sua criticidade.

Seção VII

Do controle de acesso

Art. 26. Será elaborada norma de gestão de acessos a fim de regular a concessão de credenciais de acesso.

Art. 27. O acesso a informações classificadas ou que tenham sigilo previsto por lei dependerá da posse de credencial de acesso, observando o princípio do privilégio mínimo e da necessidade de conhecer, quando aplicável.

Art. 28. As áreas, instalações, redes e sistemas de computadores deverão possuir mecanismos adequados de controle de acesso físico ou lógico, mediante credenciais de acesso, de acordo com seu grau de criticidade, que possibilitem o bloqueio e a identificação das pessoas.

Art. 29. O acesso a áreas, instalações, redes e sistemas de computadores, exceto as páginas públicas do sítio da Susep na internet e áreas destinadas a atendimento ao público, dependerá necessariamente da posse de credenciais de acesso, pessoais e intransferíveis, a serem concedidas em razão da conveniência e oportunidade, observando, quando aplicável, a credencial de acesso e a necessidade de conhecer.

§ 1º As credenciais de acesso deverão delegar a seu portador somente os privilégios de acesso necessários para o exercício de sua função.

§ 2º As credenciais de acesso dos agentes públicos serão válidas apenas durante o período de efetivo exercício de sua função.

§ 3º A Administração da Susep poderá, a seu critério, estabelecer condições adicionais específicas para o acesso de seus agentes públicos a áreas e instalações classificadas, tais como necessidade de acompanhamento e autorizações de acesso especiais.

§ 4º As credenciais de acesso que habilitarão os visitantes a acessar áreas e instalações da Susep deverão ser mantidas visíveis durante todo o período da visita e sua concessão ocorrerá mediante apresentação de documento de identificação do visitante e autorização de servidor da Susep.

Art. 30. As credenciais de acesso de agentes públicos são de uso pessoal e intransferível e seu compartilhamento é vedado sob qualquer hipótese, devendo ser alterada pelo próprio agente público, a qualquer tempo, ou por determinação da unidade de TI, especialmente quando houver suspeita de sua violação.

Art. 31. Qualquer utilização dos sistemas e demais recursos de informática da Susep é de responsabilidade do agente público ao qual estejam associadas as credenciais de acesso utilizadas.

Art. 32. As credenciais de acesso com permissão de administração de recursos de TI para colaboradores deverão ser pessoais, intransferíveis e distintas daquelas utilizadas para acesso regular, e serão

fornecidas exclusivamente ao pessoal técnico da área de TI, sejam eles servidores ou terceiros devidamente contratados para tal função.

§ 1º Credenciais de acesso criadas para administração ou utilização por sistemas ou serviços de TI, que não possam ser diretamente associadas a uma pessoa física, deverão ser reguladas por norma específica.

§ 2º Os administradores dos recursos de TI da Susep são responsáveis pelo uso adequado dos recursos sob sua responsabilidade, devendo zelar pela integridade, disponibilidade e confidencialidade dos sistemas e dos dados sob seus cuidados.

Seção VIII

Da Gestão de Ativos da Informação

Art. 33. Os ativos da informação da Susep deverão ser protegidos contra indisponibilidade, acessos indevidos, ameaças, ataques, alterações, falhas, perdas, danos, furtos, roubos, interrupções não programadas e outros incidentes de segurança.

Art. 34. Os ativos de informação deverão ser inventariados e mapeados a fim de produzir subsídios para a Gestão de Segurança da Informação, Gestão de Riscos, Gestão de Continuidade de Negócios, bem como para os procedimentos de avaliação da conformidade, de melhorias contínuas e de auditoria.

Art. 35. Ações e controles específicos de segurança deverão garantir a proteção adequada dos ativos de informação da Susep, em níveis compatíveis ao seu grau de importância para a consecução das atividades e objetivos estratégicos da Autarquia.

Seção IX

Do uso dos recursos computacionais

Art. 36. Os recursos de TI são colocados à disposição dos usuários para uso como ferramentas de trabalho.

§ 1º É vedado o uso de recursos computacionais para armazenar ou transmitir conteúdo ilegal, calunioso, difamatório, injurioso, que viole direitos à propriedade intelectual, que seja invasivo à privacidade ou obsceno.

§ 2º Os serviços de trocas de mensagens, como correio eletrônico, mensagens instantâneas, ou quaisquer serviços de comunicação disponibilizados pela Susep devem ser utilizados apenas para atividades inerentes ao exercício do cargo ou função na Susep, sendo vedada sua utilização para fins pessoais, incluindo envio de propaganda ou material não solicitado (*spam*), correntes, esquemas do tipo “pirâmide” ou qualquer outra forma de apelo não autorizado por autoridade competente desta Autarquia.

Art. 37. O uso dos recursos computacionais pelos usuários da rede da Susep poderá ser monitorado, respeitando-se os princípios legais.

Art. 38. Somente é permitida a utilização de *software* autorizado ou disponibilizado pela Susep.

Parágrafo único. Em caso de necessidade comprovada de uso de outros programas, incluindo os gratuitos, ou versões comerciais destinadas à avaliação, estes devem ser previamente autorizados pela área de TI.

Art. 39. É vedado ao usuário alterar, nos computadores de mesa ou portáteis, configurações restritas à área de TI.

Art. 40. É vedada a conexão de equipamentos particulares à rede de dados da Susep, salvo em caso de comprovada necessidade e anuência da área de TI.

Art. 41. A área de TI poderá suspender o acesso de qualquer equipamento à rede da Susep, sem aviso prévio, sempre que for constatada violação das normas de utilização e de segurança da rede.

Art. 42. O uso de recursos criptográficos deverá ser considerado no trânsito e no armazenamento de dados sigilosos, de acordo com a sua classificação.

Seção X

Da Segurança Física e do Ambiente

Art. 43. A segurança física dos equipamentos e os mecanismos de proteção às instalações físicas e áreas de processamento de informações deverão ser protegidas contra acesso indevido, danos e interferências, em resposta aos riscos identificados.

Art. 44. A unidade responsável pela segurança organizacional e corporativa deverá implementar perímetros de segurança a fim de garantir proteção e separação entre ambientes internos e externos.

Art. 45. As áreas seguras serão protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.

Art. 46. A Administração da Susep poderá, a seu critério, estabelecer condições adicionais específicas para o acesso de seus agentes públicos a áreas e instalações específicas, tais como necessidade de acompanhamento e autorizações de acesso especiais.

Art. 47. Os visitantes, ao acessar áreas e instalações da Susep, serão autorizados e acompanhados durante a sua permanência desde o acesso até a saída, por agente público da Susep.

Parágrafo único. Esse acesso deverá ser registrado.

Seção XI

Dos recursos humanos

Art. 48. A Susep buscará o aperfeiçoamento e a atualização contínua de seus agentes públicos em Segurança da Informação, principalmente os envolvidos diretamente na gestão desta.

Art. 49. Fica facultado à Susep contratar consultorias especializadas para assessoramento do CSI no desempenho de suas atividades.

CAPÍTULO VII

DAS PENALIDADES

Art. 50. O descumprimento às normas estabelecidas no âmbito da Posin sujeitará o agente público às sanções e obrigações previstas na regulamentação interna e na legislação em vigor.

CAPÍTULO VIII

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 51. Compete ao Conselho Diretor:

I - promover a simplificação administrativa, a modernização da gestão pública e a integração dos serviços públicos, especialmente aqueles prestados por meio eletrônico, com vistas à segurança da informação;

II - monitorar o desempenho e avaliar a concepção, a implementação e os resultados desta política e das normas internas de segurança da informação;

III - incorporar padrões elevados de conduta para a garantia da segurança da informação e orientar comportamento dos agentes públicos, em consonância com as funções e as atribuições da Autarquia;

IV - estabelecer diretrizes para o planejamento e execução de programas, de projetos e de processos relativos à segurança da informação;

V - estabelecer diretrizes para o processo de gestão de riscos de segurança da informação;

VI - observar as normas que estabelecem requisitos e procedimentos para a segurança da informação publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

VII - implementar controles internos fundamentados na gestão de riscos da segurança da informação;

VIII - instituir uma estrutura de processos e controles para a gestão de segurança da informação;

IX - implantar mecanismo de comunicação imediata sobre a existência de vulnerabilidades ou incidentes de segurança que impactem ou possam impactar os serviços prestados pela Susep;

X - observar as normas e os procedimentos específicos aplicáveis, implementar e manter mecanismos, instâncias e práticas de governança da segurança da informação em consonância com os princípios e as diretrizes estabelecidos na legislação; e

XI - assegurar a manutenção da existência do Comitê de Segurança da Informação, levando em consideração o que consta da Resolução Susep nº 31, de 2023, ou de ato normativo que venha a substituí-la.

Art. 52. Compete ao Superintendente:

I - designar para a função de Gestor de Segurança da informação um entre os um servidor público civil ocupante de cargo efetivo, ou militar de carreira, com formação ou capacitação técnica compatível com as atribuições ; e

II - designar ao menos um servidor efetivo, militar de carreira ou empregado público como responsável pela avaliação de conformidade.

Art. 53. Compete à área de recursos humanos:

I - notificar a área de TI sobre qualquer afastamento, desligamento, alteração de cargo, função ou lotação de agentes públicos da Susep; e

II - promover a capacitação dos agentes públicos nas normas de Segurança da Informação adotadas pela Susep.

Parágrafo único. As ações decorrentes das alterações de pessoal mencionadas no inciso I serão definidas em normas ou procedimentos específicos.

Art. 54. Compete à área de TI:

I - implantar ações técnicas para assegurar integridade, disponibilidade, confidencialidade e autenticidade de informações armazenadas em meio digital no âmbito da Susep;

II - encaminhar solicitação dos recursos necessários para implantação da Posin, no limite de suas atribuições, à Autoridade competente para as providências cabíveis;

III - prestar assessoria técnica aos gestores de ativos e ao CSI nos temas relacionadas à TI;

IV - monitorar o uso dos recursos computacionais; e

V - Promover o aperfeiçoamento constante de seu corpo técnico quanto às boas práticas e tecnologias de Segurança da Informação.

Art. 55. Compete aos titulares de unidades:

I - indicar as necessidades de treinamento dos agentes públicos lotados na unidade pela qual é responsável nas normas de Segurança da Informação vigentes;

II - indicar as necessidades de concessão e revogação de credenciais de acesso para os agentes públicos em atividade na unidade de sua responsabilidade;

III - identificar e classificar os ativos de informação sob sua gestão por nível de criticidade;

IV - identificar potenciais ameaças aos ativos de informação;

V - identificar e comunicar vulnerabilidades dos ativos de informação;

VI - consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação em um relatório;

VII - autorizar a atualização do relatório mencionado no inciso VI;

VIII - avaliar os riscos dos ativos de informação ou do grupo de ativos de informação;

IX - avaliar e, em caso de necessidade, aprovar as solicitações de acesso aos ativos sob sua gestão; e

X - promover o aperfeiçoamento constante de seu corpo técnico quanto às boas práticas e tecnologias de Segurança da Informação.

Art. 56. Compete aos usuários:

I - conhecer e observar a Posin bem como suas normas complementares;

II - informar imediatamente ao CSI qualquer evento, confirmado ou sob suspeita, relativo à Segurança da Informação;

III - informar imediatamente à Etir qualquer evento relacionado à segurança cibernética;

IV - zelar pelo sigilo de suas credenciais de acesso lógico aos ativos de informação da Susep;

V - comunicar a perda ou comprometimento de suas credenciais de acesso;

VI - responder pela quebra de segurança ocorrida com a utilização de suas credenciais de acesso; e

VII - observar, na manipulação e uso de ativos, as medidas especiais de segurança compatíveis com seu grau de sigilo, em conformidade com a legislação vigente e normas complementares adotadas pela Susep.

CAPÍTULO IX

DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 57. A Posin será complementada por normas, procedimentos e outros documentos pertinentes, os quais serão considerados partes integrantes desta política.

Art. 58. Será providenciada a inclusão das cláusulas de que trata o art. 10 nos contratos vigentes na data de publicação desta Resolução, por meio de termos aditivos, na ocorrência de eventual prorrogação contratual.

Art. 59. As propostas de alteração ou criação de normas internas sobre Segurança da Informação deverão ser encaminhadas ao CSI.

Art. 60. Após a publicação desta Resolução, o CSI deverá dar ampla divulgação da Posin a todos os agentes públicos, inclusive por meio da intranet.

Art. 61. A Posin deverá ser revisada, sempre que se fizer necessário, não excedendo ao período de 3 (três) anos.

Art. 62. Fica revogada a Deliberação Susep nº 171, de 19 de março de 2015.

Art. 63. Esta Resolução entra em vigor na data de sua publicação.

Documento assinado eletronicamente por **ALESSANDRO SERAFIN OCTAVIANI LUIS (MATRÍCULA 1860655)**, **Superintendente da Susep**, em 18/10/2024, às 15:12, 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 **2172362** e o código CRC **EC6BECEC**.
