SUPERINTENDÊNCIA DE SEGUROS PRIVADOS

DELIBERAÇÃO SUSEP N.º 171, DE 19 MARÇO DE 2015.

Altera e consolida a Política de Segurança da Informação e Comunicações – Posic, da Superintendência de Seguros Privados – Susep e dá outras providências.

O SUPERINTENDENTE DA SUPERINTENDÊNCIA DE SEGUROS PRIVADOS – SUSEP torna público que o Conselho Diretor da Autarquia, em reunião ordinária realizada em 19 de março de 2015, no uso das atribuições que lhe confere o inciso X do art. 68 do Regimento Interno de que trata a Resolução CNSP n.º 320, de 12 de dezembro de 2014; o inciso II do art. 4.º da Instrução Susep n.º 51, de 15 de março de 2011, e considerando o que consta do Processo SUSEP n.º 15414.001400/2012-90,

D E L I B E R O U:

Art. 1.º Alterar e consolidar a Política de Segurança da Informação e Comunicações – Posic da Superintendência de Seguros Privados – Susep.

CAPÍTULO I

DO ESCOPO

Art. 2.º A Política de Segurança da Informação e Comunicações – Posic objetiva instituir diretrizes estratégicas, responsabilidades e competências, visando a assegurar integridade, confidencialidade, disponibilidade e autenticidade dos dados e informações da Susep, sejam eles estáticos ou em trânsito, contra ameaças que possam comprometer seus ativos, inclusive sua imagem institucional.

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

§ 2.º Esta política deverá ser obrigatoriamente observada por todos os agentes públicos a serviço da Susep, doravante denominados agentes públicos.

§ 3.º A Posic 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 vitais 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 e comunicações – SIC.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 3.º Para fins da Posic, 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: todo e qualquer recurso utilizado para armazenar, transmitir e processar informações no âmbito da organização, como documentos em papel, arquivos digitais, computadores, redes, discos rígidos, bancos de dados, instalações físicas usadas para armazenamento etc.;

VI - autenticidade: é a propriedade de garantir a origem da informação;

VII - avaliação de riscos: procedimento de comparar um risco estimado com um critério, com o objetivo de determinar a sua relevância;

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

IX - confidencialidade: propriedade que indica que o acesso à informação é limitado a pessoas autorizadas;

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;

XII - credencial de acesso: permissão que habilita determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo, ou lógica, como identificação de usuário e senha;

XIII - credencial de segurança: certificado, inerente ao cargo, função ou lotação, que habilita determinado agente público a ter acesso a ativos de informação, bem como aos dados e informações que estes contenham, em diferentes graus de sigilo;

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

XV - descarte: eliminação de informações, documentos, mídias e acervos digitais, observando os procedimentos de segurança;

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

XVII - disponibilidade: propriedade que indica que as informações estão acessíveis, aos usuários autorizados, sempre que necessário;

XVIII - evento: ocorrência identificada como uma possível violação da Posic, falha de controles ou uma situação previamente conhecida que possa ter consequências para a segurança da informação;

XIX - gestão de riscos: conjunto de atividades coordenadas no sentido de direcionar e controlar as ações de uma organização em relação aos riscos a que está exposta;

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, 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: mudança adversa no nível estabelecido nos objetivos de negócios;

XXIII - incidente: evento adverso, confirmado, relacionado à SIC;

XXIV - integridade: propriedade que indica que a informação manipulada não sofreu alterações não autorizadas;

XXV - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da SIC;

XXVI - necessidade de conhecer: condição devida à qual determinada informação é indispensável ao desempenho das funções de um agente público;

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

XXVIII - risco: probabilidade de que ameaças explorem vulnerabilidades dos ativos gerando impacto e perdas para a organização;

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

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

XXXI - vulnerabilidade: fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO III

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

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

I - Lei n.º 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 n.º 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;

III – Decreto n.º 3.505, de 13 de junho de 2000, que instituiu a Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

IV - Decreto n.º 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

V – Decreto n.º 4.073, de 3 de janeiro de 2002, que regulamenta a Lei n.º 8.159, de 8 de janeiro de 1991;

VI – Instrução Normativa GSI n.º 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

VII – Norma Complementar n.º 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008, que define a metodologia de gestão de Segurança da Informação e Comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;

VIII - Norma Complementar n.º 03/IN01/DSIC/GSIPR, de 30 de junho de 2009, que estabelece as diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações – Posic nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

IX – Norma Complementar n.º 04/IN01/DSIC/GSIPR, de 14 de agosto de 2009, que estabelece as diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF;

X – Norma Complementar n.º 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;

XI – Norma Complementar n.º 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009, que estabelece diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XII – Norma Complementar n.º 07/IN01/DSIC/GSIPR, de 6 de maio de 2010, que estabelece diretrizes para o implemento de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XIII – Norma Complementar n.º 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;

XIV - 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;

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

XVI – Decreto n.º 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal; e

XVII – Deliberação Susep n.º 135, de 20 de abril de 2009, que aprova o Código de Ética Profissional do Servidor da Superintendência de Seguros Privados – Susep.

CAPÍTULO IV

DOS PRINCÍPIOS

Art. 5.º A Posic observará os seguintes princípios, assim definidos:

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

II – moralidade: a elaboração da Posic, 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 Posic 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 Posic buscará garantir o amplo acesso do público à informação, exceto quando o próprio interesse público justificar seu sigilo; e

V – eficiência: a Posic terá como objetivo tornar a atuação da Susep mais rápida e precisa, por meio do tratamento efetivo das informações.

CAPITULO V

DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES.

Art. 6.º Fica instituído o Gestor de Segurança da Informação e Comunicações – GSIC, cujas funções serão exercidas pelo Diretor da Diretoria de Administração – Dirad.

Art. 7.º Fica instituído o Comitê de Segurança da Informação e Comunicações – CSIC. *(Artigo alterado pela Deliberação SUSEP nº 178/2016)*

§ 1.º O Comitê de Segurança da Informação e Comunicações – CSIC será integrado:

I - pelo Gestor de Segurança da Informação e Comunicações – GSIC (Coordenador);

II - pelo Coordenador-Geral da Coordenação-Geral de Tecnologia da Informação – CGETI;

III - pelo Coordenador-Geral da Coordenação-Geral de Administração e Finanças – CGEAF

IV- pelo Chefe de Gabinete – GABIN;

V - pelo Coordenador da Coordenação de Apoio a Gestão Estratégica – SEGER/COGET

VI - pelo Coordenador da Coordenação de Atendimento ao Público – DICON/COATE;

VII - por um representante da Diretoria de Organização do Sistema de Seguros Privados – DIORG ou de Unidade a ela subordinada, por designação do Superintendente;

VIII - por um representante da Diretoria de Supervisão de Solvência – DISOL ou de Unidade a ela subordinada, por designação do Superintendente;

IX - por um representante da Diretoria de Supervisão de Conduta – DICON ou de Unidade a ela subordinada, por designação do Superintendente;

§ 2.º Os substitutos eventuais das unidades às quais pertencem os integrantes titulares do CSIC integrarão o comitê, na qualidade de suplentes.

§ 3.º Serão nomeados, por ato do Superintendente da SUSEP, suplentes para os representantes mencionados nos incisos VII,VIII e IX do §1º, obedecidas as restrições do referidos incisos.

Art. 8.º Fica instituída Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - Etir, operacionalizada pela área de TI, na forma a ser regulamentada pelo CSIC, com a responsabilidade de receber, analisar e responder a eventos relacionados à segurança computacional.

Parágrafo único. A Etir deverá ser composta pelo Gestor de SIC, ou por servidor por ele indicado, além de servidores da área de TI indicados pelo Coordenador-Geral da CGETI, todos designados por ato do Superintendente da Susep.

CAPÍTULO VI

DAS DIRETRIZES

Seção I

Das diretrizes gerais

Art. 9.º A informação, recebida, produzida ou adquirida, deve ser tratada como patrimônio da Susep, a ser protegido 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. O uso das informações deverá ser feito apenas para o desempenho das atividades profissionais.

Art. 10. Todos os ajustes celebrados pela Susep com prestadores de serviços em suas instalações deverão conter cláusulas referentes ao cumprimento da Posic, 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 Posic.

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 requisitos legais;

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. Os ativos de informação serão classificados em razão do teor de seus elementos intrínsecos e dados sigilosos que contenham, de acordo com os seguintes graus:

I - Ultrassecreto;

II - Secreto;

III - Confidencial; e

IV - Reservado.

Art. 14. A classificação, a reclassificação, a desclassificação e a renovação de classificação de ativos de informação, no âmbito da Susep será feita por servidor portador de credencial de segurança correspondente a cada de grau de sigilo.

Art. 15. Todos os dados e informações sigilosos deverão ser periodicamente analisados e avaliados para verificar a persistência das condições que justificaram seu atual grau de sigilo, bem como para o controle dos prazos legais de sua classificação.

Parágrafo único. A análise estabelecida no caput deverá, sempre que possível, propor a desclassificação do ativo de informação ou sua reclassificação para grau de sigilo mais baixo.

Art. 16. Durante todo o ciclo de vida de um ativo de informação, sua manipulação e uso 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 computacional

Art. 17. Nos contratos de serviços relacionados ao provimento, gerenciamento e suporte da infra-estrutura computacional de TI deverá constar cláusula que exija a existência de estrutura de tratamento de incidentes de segurança computacional por parte do prestador.

Parágrafo único. Em relação aos contratos mencionados no caput, cabe à Etir supervisionar o tratamento de incidentes de segurança computacional para o fiel cumprimento das suas atribuições.

Art. 18. A Etir tem autonomia para tomar ações emergenciais para a resposta aos incidentes de segurança computacional.

Art. 19. A Etir deverá manter mecanismos de articulação com o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR Gov).

Seção IV

Da gestão de riscos

Art. 20. A gestão de riscos em SIC constitui um processo contínuo de levantamentos, análises, avaliações e planos de tratamento que visem manter em níveis aceitáveis os riscos de SIC a que está sujeita a Susep, estando sempre alinhada com o planejamento estratégico da Autarquia.

Art. 21. A metodologia de análise e avaliação de riscos deverá assegurar que estas atividades produzam resultados comparáveis e reproduzíveis, de modo a permitir a priorização de planos de tratamento.

§ 1º A metodologia de que trata o caput deverá contemplar a definição de níveis aceitáveis de riscos.

§ 2º Todos os riscos identificados, mesmo os que forem considerados aceitáveis, deverão ter sua evolução acompanhada para permitir a detecção de possíveis mudanças no seu impacto ou probabilidade de ocorrência.

Art. 22. Será mantido um inventário de informações e ativos de informação.

§ 1.º Do inventário de que trata o caput deverão constar, no mínimo, as informações sobre o gestor e o nível de sensibilidade do ativo com relação à SIC.

§ 2.º O inventário de ativos de informação será revisado em uma periodicidade mínima bienal.

Art. 23. Serão realizadas no âmbito da Susep avaliações periódicas de riscos, de acordo com a metodologia mencionada no art. 21.

§ 1º As avaliações de riscos de SIC terão como escopo os ativos constantes do inventário de que trata o art. 22.

§ 2º Além do inventário mencionado no § 1º, servirão de insumo para as avaliações de riscos:

I - Incidentes que venham a ser reportados ao CSIC ou à Etir;

II - Informações sobre incidentes externos que possam de alguma forma se relacionar com os ativos da Susep;

III - Vulnerabilidades publicadas por fornecedores de softwares, equipamentos ou imprensa especializada;

IV - Vulnerabilidades que tenham sido reportadas ao CSIC, à Etir, ou as que tenham sido detectadas;

V - Boas práticas reconhecidas pelo mercado relacionadas aos ativos em questão.

§ 3º As avaliações serão realizadas com periodicidade mínima bienal. Mudanças significativas nos ativos, ou no ambiente organizacional devem ensejar reavaliações com um intervalo menor.

Seção V

Da gestão de continuidade

Art. 24. A Gestão de Continuidade - GC compreenderá um conjunto de ações que envolvam respostas imediatas a eventos extraordinários que possam prejudicar o funcionamento normal dos serviços e processos críticos da Susep, visando mitigar os impactos de eventuais sinistros, acidentes ou falhas temporárias.

Art. 25. Plano de continuidade, baseado em boas práticas e aprovado pelo CSIC, deverá ser implementado e testado periodicamente para garantir a continuidade dos serviços críticos.

Art. 26. Deverão ser elaborados Planos de Emergência Contra Incêndios para a Sede e para as Regionais.

§ 1.º Para cada Plano aludido no caput deverá ser instituída Brigada de Incêndio com a promoção de seu treinamento em consonância com as normas publicadas pela Associação Brasileira de Normas Técnicas - ABNT;

§ 2.º Nos casos em que as instalações da Susep estiverem em dependências compartilhadas, os Planos de que trata o caput deverão adequar-se às determinações da administração predial, mantendo a consonância com a Posic e zelando pela adequação às normas técnicas vigentes.

Seção VI

Da auditoria e conformidade

Art. 27. 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.

Art. 28. Os processos de negócio, em todas as áreas da Susep, deverão ser auditados na conformidade com as normas de SIC e a pertinente legislação em vigor.

Art. 29. Deverão ser adotados procedimentos apropriados para garantir a conformidade com as restrições legais no uso de materiais protegidos por leis de propriedade intelectual, direitos autoriais, patentes e marcas registradas.

Seção VII

Do controle de acesso

Art. 30. O acesso a informações classificadas dependerá da posse de credencial de segurança e da necessidade de conhecer.

Art. 31. As áreas, instalações, redes e sistemas de computadores deverão possuir mecanismos adequados de controle de acesso físico e/ou lógico, de acordo com seu grau de sigilo, que possibilitem o bloqueio e a identificação das pessoas.

Art. 32. O acesso a áreas, instalações, redes e sistemas de computadores, exceto o 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 segurança 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 É vedado o uso da mesma credencial para acessos simultâneos a redes e sistemas a partir de estações de trabalho diferentes.

§ 3º As credenciais de acesso dos agentes públicos serão válidas apenas durante o período de efetivo exercício de sua função. No caso de afastamentos temporários superiores a 30 (trinta) dias, ficarão suspensas até o retorno às atividades.

§ 4º 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.

§ 5º As credenciais de acesso que habilitarão os visitantes a acessar áreas e instalações da Susep identificarão claramente o local a ser visitado e deverão ser mantidas visíveis durante todo o período da visita. Sua concessão ocorrerá mediante apresentação de documento de identificação do visitante e autorização de servidor da Susep.

§ 6º Os visitantes não poderão possuir credenciais de acesso a redes e sistemas de computadores da Susep, exceto nos casos de redes destinadas para este fim e casos previstos em lei.

§ 7º Nos casos de invalidação temporária ou definitiva das credenciais de acesso de agentes públicos, o acesso destes aos ativos de informação da Autarquia dar-se-á mediante as condições estabelecidas para os visitantes.

Seção VIII

Do uso dos recursos computacionais

Art. 33. 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, difamatório, invasivo à privacidade, obsceno ou injurioso.

§ 2º É proibido utilizar o serviço de correio eletrônico da Susep para enviar 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. 34. O uso dos recursos computacionais pelos usuários da rede da Susep será monitorado, respeitando-se os princípios legais.

Art. 35. Somente é permitida a utilização de software autorizado ou disponibilizado pela Susep.

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

Art. 36. É vedado ao usuário alterar, nos computadores de mesa ou portáteis, configurações restritas à área de TI.

Art. 37. 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. 38. 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. 39. O uso de recursos criptográficos deverá ser considerado no trânsito e no armazenamento de dados sigilosos, de acordo com a sua classificação.

Seção IX

Dos recursos humanos

Art. 40. A Susep buscará o aperfeiçoamento e a atualização contínua de seus agentes públicos em SIC, principalmente os envolvidos diretamente na gestão desta.

Art. 41. Fica facultado à Susep contratar consultorias especializadas para assessoramento do CSIC no desempenho de suas atividades.

CAPÍTULO VII
DAS PENALIDADES

Art. 42. O descumprimento às normas estabelecidas no âmbito da Posic sujeitará o agente público às sanções e obrigações previstas na regulamentação interna e na legislação em vigor.

CAPÍTULO VIII
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 43. Compete à Administração prover os recursos humanos e materiais necessários a aplicação da Posic.

Art. 44. Compete ao GSIC:

I – promover cultura de SIC;

II – acompanhar as investigações e as avaliações dos danos decorrentes de incidentes de segurança;

III – propor recursos necessários às ações de SIC;

IV – coordenar o CSIC;

V - coordenar a Etir, podendo delegar essa função a um agente responsável;

VI – acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIC;

VII - manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República – DSIG/GSI/PR, para o trato de assuntos relativos à SIC;

VIII – propor normas e procedimentos relativos à SIC no âmbito da Susep;

IX – elaborar, com a colaboração dos demais integrantes do CSIC, o relatório das atividades do Comitê, a ser encaminhado ao Conselho Diretor, com periodicidade trimestral;

X – propor a capacitação dos servidores em SIC, inclusive a participação em fóruns, redes, congressos, grupos de discussões e afins;

XI – coordenar a instituição, a implementação e a manutenção da infraestrutura necessária à Etir; e

XIII – decidir sobre os casos omissos relativos à SIC.

Art. 45. Compete ao CSIC:

I – estabelecer padrões, procedimentos e demais aspectos necessários para assegurar a implementação da Posic;

II - propor a constituição de grupos de trabalho para tratar de temas e apresentar soluções

específicas sobre SIC;

III – atualizar a Posic e as normas complementares;

IV - propor normas complementares e procedimentos internos relativos à SIC;

V – propor a implementação de mecanismos que permitam a quantificação, a qualificação e o levantamento de custos dos incidentes de segurança da informação e do mau funcionamento de sistemas; e

VI – coordenar a elaboração do Plano de Continuidade.

Art. 46. Compete à Etir:

I - Receber, filtrar, classificar e responder às solicitações e alertas relacionados a incidentes de segurança computacional;

II - Realizar as análises dos incidentes de segurança computacional;

III - Propor e recomendar ações de segurança computacional;

IV - Executar medidas de recuperação relacionadas a incidentes de segurança computacional;

V - Assessorar o CSIC na proposição de normas relacionadas a incidentes de segurança computacional;

VI - Realizar monitoração de uso e inspeções para avaliação de conformidade do uso dos recursos computacionais com as normas de segurança da informação em vigor; e

VII - Prestar suporte em segurança computacional às diversas Unidades da Susep.

Art. 47. Compete à área de auditoria verificar a conformidade dos procedimentos internos quanto à aplicação da Posic;

Art. 48. Compete à área de recursos humanos:

I - notificar o CSIC e a área de TI sobre qualquer alteração de cargo, função ou lotação de agentes públicos da Susep, bem como sobre afastamentos dos mesmos por períodos superiores a 30 (trinta) dias; e

II – promover a capacitação dos agentes públicos nas normas de SIC adotadas pela Susep.

Art. 49. 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 Posic, no limite de suas atribuições, à Autoridade competente para as providências cabíveis;

III - Prestar assessoria técnica aos gestores de ativos e ao CSIC nos temas relacionadas à TI;
IV - Informar ao CSIC situações que eventualmente comprometam a SIC;

V – Operacionalizar a ETIR no âmbito de suas atribuições;

VI – Monitorar o uso dos recursos computacionais; e

VII – Promover o aperfeiçoamento constante de seu corpo técnico quanto às boas práticas e tecnologias de SIC.

Art. 50. Compete aos titulares de Unidades:

I - Indicar as necessidades de treinamento dos agentes públicos lotados na Unidade pela qual é responsável nas normas de SIC adotadas pela Susep; e

II - Indicar as necessidades de concessão de credenciais de acesso para os agentes públicos em atividade na Unidade de sua responsabilidade.

Art. 51. Compete aos gestores de ativos:

I - Definir os requisitos de SIC para os ativos de informação sob sua responsabilidade;

II - Classificar, reclassificar, renovar classificação e desclassificar os ativos de informação sob sua responsabilidade, de acordo com sua credencial de segurança;

III - Apoiar o CSIC e a Etir na resposta a incidentes relacionados a ativos sob sua gestão; e

IV - Zelar para que os ativos de informação sob sua responsabilidade atendam aos requisitos de SIC estabelecidos pela legislação vigente e normas complementares adotadas pela Susep.

Art. 52. Compete aos usuários:

I - Conhecer a Posic bem como suas normas complementares;

II - Informar imediatamente ao CSIC qualquer evento, confirmado ou sob suspeita, relativo à SIC;

III - Informar imediatamente à Etir qualquer evento relacionado à segurança computacional; 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 sua credencial 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

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 53. A Posic será complementada por normas, procedimentos e outros documentos pertinentes, os quais serão considerados partes integrantes desta política.

Art. 54. Será providenciada a inclusão das cláusulas de que trata o art. 10 nos contratos vigentes na data de publicação desta Deliberação, por meio de termos aditivos, na ocorrência de eventual prorrogação contratual.

Art. 55. As propostas de alteração ou criação de normas internas sobre SIC deverão ser encaminhadas ao CSIC.

Art. 56. Após a publicação desta Deliberação, o CSIC deverá dar ampla divulgação da Posic a todos os agentes públicos, inclusive por meio da intranet.

Art. 57. A Posic deverá ser revisada, sempre que se fizer necessário, não excedendo ao período de 3 (três) anos.

Art. 58. Esta Deliberação entra em vigor na data de sua publicação, ficando revogadas as Deliberações Susep nº s 147 e 154, de 3 outubro de 2011 e 23 de maio de 2012, respectivamente.

ROBERTO WESTENBERGER

Superintendente