Ato do Conselho Diretor

RESOLUÇÃO Nº 12, DE 31 DE OUTUBRO DE 2014.

Estabelece a Política de Segurança da Informação e Comunicações - PoSIC no âmbito da ENAP.

O CONSELHO DIRETOR DA FUNDAÇÃO ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA, por meio de seu Presidente, baseado na deliberação ocorrida na reunião do dia 29 de outubro de 2014, no uso das atribuições que lhe confere o art. 13, II, do Estatuto aprovado pelo Decreto nº 6.563, de 11 de setembro de 2008, publicado no DOU em 12 de setembro de 2008, c/c o art. 50, II, da Resolução nº 3, de 18 de março de 2014, do Conselho Diretor da ENAP, publicada no DOU de 20 de março de 2014,

RESOLVE:

Art. 1º Estabelecer a Política de Segurança da Informação e Comunicações - PoSIC no âmbito da ENAP, nos termos dos Anexo I e II da presente Resolução.

Parágrafo único: Considerar-se-ão normas complementares à PoSIC, os seguintes normativos vigentes na ENAP:

I – Portaria nº 81, de 11 de maio de 2011, que estabelece a Política de Acesso à internet Escola Nacional de Administração Pública – ENAP.

II – Portaria nº 83, de 27 de abril de 2012, que institui a Comissão de Assessoramento a Classificação de Informações Sigilosas da Fundação Escola Nacional de Administração Pública – ENAP.

III – Portaria n° 165, de 03 de julho de 2013, que designa o servidor Pedro Luiz Costa Cavalcante como autoridade da Lei de Acesso à Informação na ENAP.

IV – Portaria nº 166, de 03 de julho de 2013, que cria Comissão com o objetivo de coordenar a implementação e acompanhamento dos trabalhos relativos à Lei de Acesso à Informação (Lei nº 12.527) na ENAP.

V – Portaria nº 297, de 31 de dezembro de 2013, que institui o Repositório Institucional da ENAP.

VI - Portaria nº 83, de 03 de junho de 2014, que dispõe sobre a Política de Direitos Autorais da ENAP.

Art. 2º Constituir, no prazo de 30 dias, o Comitê de Segurança da Informação e Comunicações - CSIC com a indicação do Gestor de Segurança da Informação e Comunicações (GeSIC) no âmbito da ENAP.

Art. 3º Esta Resolução entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Paulo Sergio de Carvalho
Presidente

RESOLUÇÃO Nº 12, DE 31 DE OUTUBRO DE 2014.
ANEXO I

CAPÍTULO I
DO ESCOPO

Art. 1° A Política de Segurança da Informação e Comunicações - PoSIC institui diretrizes estratégicas, responsabilidades e competências, visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações produzidas ou custodiadas pela ENAP, de modo a preservar os seus ativos e sua imagem institucional.

Art. 2° A PoSIC trata do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito da ENAP, em todo o seu ciclo de vida - criação, manuseio, divulgação, armazenamento, transporte e descarte - visando à continuidade de seus processos críticos, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

Art. 3° Esta PoSIC e demais normas e procedimentos complementares se aplicam a todas as unidades da estrutura organizacional da ENAP, aos seus servidores e, no que couber, a seus terceirizados e a seus usuários.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 4° Para os efeitos desta PoSIC e demais normas, entende-se por:

I - Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

II - Ativos da informação: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas e redes de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

III - Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

IV - Comitê de Segurança da Informação e Comunicações (CSIC): colegiado de caráter consultivo responsável pela proposição de normas, supervisão e a implementação das ações de segurança da informação e comunicações no âmbito da ENAP;

V - Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

VI - Conscientização em SIC: saber o que é segurança da informação e comunicações e como aplicar em sua rotina pessoal e profissional;

VII - Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

VIII - Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

IX - Gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio,

caso essas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;

X - Gestão de riscos: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos da informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

XI - Gestão de Segurança da Informação e Comunicações (GSIC): ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, às tecnologias da informação e comunicações;

XII - Incidente: qualquer evento adverso, indesejado e/ou inesperado, confirmado ou sob suspeita, relacionado à segurança dos ativos da informação e que possa comprometer a continuidade do negócio e ameaçar a SIC;

XIII - Informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XIV - Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XV - Política de Segurança da Informação e Comunicações (PoSIC): documento aprovado pela autoridade máxima do órgão, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações no âmbito da ENAP;

XVI - Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XVII - Segurança física e do ambiente: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que o órgão esteja presente;

XVIII - Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XIX - Tratamento de incidentes: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

XX - Usuário: servidores de outros órgãos da administração pública, alunos, professores, bolsistas, estagiários, hóspedes, convidados e visitantes da ENAP.

CAPÍTULO III
DAS DIRETRIZES GERAIS

Seção I
Do Tratamento da Informação

Art. 5° Toda informação criada, adquirida ou custodiada pelo servidor da ENAP, no exercício de suas atividades, é considerada um bem e deve ser protegida de acordo com as

regulamentações de segurança existentes com o objetivo de minimizar riscos às atividades e serviços prestados pela ENAP, preservando sua imagem.

Art. 6° As informações produzidas ou custodiadas pela ENAP devem ser descartadas conforme o seu nível de classificação.

Seção II
Da Classificação da Informação

Art. 7° As informações custodiadas ou de propriedade da ENAP devem ser classificadas levando-se em consideração seu valor, criticidade, sensibilidade e requisitos legais e receber o nível de proteção condizente com sua classificação, conforme normas e legislações específicas em vigor.

Parágrafo único: Todos devem preservar a integridade e confidencialidade das informações classificadas às quais tiver acesso.

Art. 8° O gestor da informação é responsável por atribuir o nível de classificação das informações sob sua responsabilidade.

Art. 9° A classificação deve ser respeitada durante todo o ciclo de vida da informação.

Seção III
Da Sensibilização, Conscientização e Capacitação

Art. 10° A ENAP desenvolverá processo permanente de divulgação, sensibilização, conscientização e capacitação dos seus servidores sobre os cuidados e deveres relacionados à segurança da informação e comunicações.

Art. 11. Os investimentos em capacitações em SIC deverão ser estabelecidos de forma planejada e contemplados no Plano Anual de Capacitação da ENAP (PACE), com base na priorização dos riscos a serem tratados, considerando a probabilidade, severidade e relevância destes.

Seção IV
Da Gestão de Riscos e da Continuidade

Art. 12. A ENAP deve adotar processo contínuo de gestão de riscos, de forma a identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos da informação.

Art. 13. A ENAP deve manter processo de gestão de continuidade das atividades essenciais relacionadas à sua Missão, visando não permitir que estas sejam interrompidas e assegurar a sua retomada em tempo hábil.

Art. 14. As informações de propriedade ou custodiadas pela ENAP relacionadas à continuidade das atividades essenciais, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança. As informações armazenadas em outros meios devem possuir

mecanismos de proteção que preservem sua integridade, conforme o nível de classificação atribuído.

Seção V
Do Uso de Recursos Computacionais e Comunicações

Art. 15. O uso de recursos computacionais e de comunicações da ENAP pelos seus servidores deve ser direcionado para a realização das atividades profissionais desempenhadas para o órgão, nos limites dos princípios da ética, razoabilidade e legalidade, conforme os normativos existentes.

Seção VI
Dos Controles de Acesso

Art. 16. A ENAP deve sistematizar a concessão e revogação de acesso como forma de evitar a quebra de segurança da informação e comunicações.

Art. 17. O acesso físico às instalações da ENAP deverá ser regulamentado com o objetivo de garantir a segurança dos seus servidores, dos usuários da Escola e a proteção dos seus ativos.

CAPÍTULO IV
DAS NORMAS COMPLEMENTARES DE SEGURANÇA

Art. 18. O disposto nesta política poderá ser regulamentado por normas e procedimentos, partes integrante desta PoSIC, destinados a complementar as diretrizes de SIC.

CAPÍTULO V
DA ESTRUTURA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 19. Fica instituído o Comitê de Segurança da Informação e Comunicações (CSIC), com as seguintes competências:

I - Assessorar na implementação das ações de segurança da informação e comunicações;

II - Propor normas e procedimentos relativos à segurança da informação e comunicações, em conformidade com a legislação e regulamentação interna sobre o tema;

III - Constituir grupos de trabalho para tratar temas e propor soluções específicas sobre segurança da informação e comunicações;

IV - Promover a melhoria contínua nos processos e controles de SIC.

Parágrafo único. O Comitê de Segurança da Informação e Comunicações será composto por membros titulares e suplentes, indicados pelo Conselho Diretor, e coordenado pelo Gestor de Segurança da Informação e Comunicações.

Art. 20. Ao Gestor de Segurança da Informação e Comunicações (GeSIC) compete:

I - promover cultura de segurança da informação e comunicações;

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III - propor recursos necessários às ações de segurança da informação e comunicações;

IV - coordenar o CSIC e a equipe de tratamento e resposta a incidentes em redes computacionais;

V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VI - manter contato direto com o Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações;

VII - propor normas relativas à segurança da informação e comunicações.

Art. 21. Fica instituída, no âmbito da ENAP, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), conforme a Norma Complementar Nº 5 de 14 de agosto de 2009.

Parágrafo único. As atividades da ETIR deverão ser executadas no âmbito da Coordenação-Geral de Tecnologia da Informação – CGTI da ENAP, mediante designação formal e indicação do CSIC.

Art. 22. Os membros titulares e suplentes da Estrutura de GSIC deverão receber regularmente capacitação nas disciplinas relacionadas à SIC.

CAPÍTULO VI
REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 23. Esta PoSIC tem como referência legal e normativa os seguintes dispositivos:

I - Instrução Normativa GSI/PR n° 1 de 13/06/2008 e Normas Complementares IN01/DSIC/GSIPR.

II - Portaria n° 27 MPOG de 03/02/2012.

III - Lei 12.527 de 18/11/2011.

IV - Lei 8.112 de 11/12/1990.

V - Decreto 4.553 de 27/12/2012.

VI - Decreto 3.505 de 13/06/2000.

VII - Boas práticas em segurança da informação / Tribunal de Contas da União - 3. ed. – 2008

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS

Art. 24. A ENAP deve observar as diretrizes e responsabilidades estabelecidas nesta PoSIC, nas normas e procedimentos complementares e nas melhores práticas de segurança da informação recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões e normas de segurança.

Art. 25. Todos os servidores e terceirizados da ENAP devem comunicar aos gestores responsáveis pelos ativos da informação qualquer ocorrência de incidentes de SIC.

Art. 26 Todos os servidores e terceirizados da ENAP são responsáveis pela segurança dos ativos de informação, que estejam sob sua custódia, e por todos os atos executados com suas identificações, tais como: crachá, login, senha eletrônica, certificado digital e endereço de correio eletrônico.

Art. 27. Os contratos, convênios, acordos e instrumentos congêneres devem observar, no que couber, as seguintes diretrizes:

I - conter cláusulas que estabeleçam a obrigatoriedade de observância desta PoSIC.

II - prever a obrigação da outra parte de divulgar esta PoSIC e suas normas complementares aos seus empregados e prepostos envolvidos em atividades na ENAP.

III - nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

Art. 28. Os incidentes, as quebras de segurança e o descumprimento das normas estabelecidas nesta PoSIC serão devidamente apurados e implicará a responsabilidade civil, penal e administrativa dos que estiverem envolvidos na violação, podendo ensejar, do ponto de vista administrativo, apuração de responsabilidade, conforme os art. 124 e art. 143 da Lei nº 8.112, de 1990.

Art. 29. A PoSIC e demais normas e procedimentos complementares à esta deverão ser revisadas sempre que necessário, por deliberação do Conselho Diretor ou proposta do CSIC.

RESOLUÇÃO Nº 12, DE 31 DE OUTUBRO DE 2014.
ANEXO II

TERMO DE CIÊNCIA E RESPONSABILIDADE DE USO DA INFORMAÇÃO NA ENAP

Eu, abaixo identificado, pelo presente termo, declaro estar ciente e concordo que:

Conheço, concordo e cumprirei as diretrizes da Política de Segurança da Informação e Comunicações – PoSIC e demais normas e procedimentos afetas à Segurança da Informação e Comunicações - SIC no âmbito da ENAP.

Agirei sempre com os cuidados necessários e ao correto uso dos recursos de TI a fim de proteger a informação e evitar o comprometimento dos recursos tecnológicos da ENAP.

Sempre farei o uso dos recursos e serviços com propósitos legais, dentro dos objetivos da escola e das minhas atribuições, primando pelos valores éticos e morais e a qualidade dos serviços ofertados pela ENAP à sociedade.

Reconheço que a minha senha e usuário de rede ou sistemas são pessoais e intransferíveis. Portanto, poderei ser responsável penal, civil e administrativamente por todos os atos decorrentes dos seus usos. Também me comprometo a comunicar de imediato a perda ou quebra de sua segurança à chefia imediata e/ou ETIR.

Declaro ter ciência de que a não observância de qualquer das condições mencionadas poderá resultar em penalizações disciplinares, de acordo com as previsões legais.

A assinatura deste termo condiciona o usuário à ciência, concordância e cumprimento das demais normas e procedimentos complementares afetas à SIC e ao uso dos recursos de TI, não o desobrigando na observância e cumprimento de todos os normativos vigentes no âmbito da ENAP.

Brasília, _____ de _____ de _____.

_____.

NOME:

CPF: