ANA
AGÊNCIA NACIONAL DE ÁGUAS

RESOLUÇÃO Nº 1078, DE 14 DE SETEMBRO DE 2015
Documento nº 00000.053869/2015-41

O DIRETOR PRESIDENTE DA AGÊNCIA DE ÁGUAS - ANA, no exercício da atribuição que lhe confere o art. 95, inciso III, da Resolução nº 2.020, de 15 de dezembro de 2014, e tendo em vista as disposições da Lei nº 12.527, de 18 de novembro de 2011, e o Decreto nº 7.845, de 14 de novembro de 2012, torna público que a DIRETORIA COLEGIADA, em sua 584ª Reunião Ordinária, realizada em 14 de setembro de 2015, resolveu:

Art. 1º Instituir a Política de Segurança da Informação e Comunicações - Posic, que fornece as diretrizes e critérios e define o suporte administrativo para o tratamento a ser dado às informações produzidas, processadas, transmitidas e armazenadas no ambiente convencional ou de tecnologia no âmbito da Agência Nacional de Águas – ANA.

Parágrafo único. A Posic abrange os servidores, estagiários, colaboradores, consultores externos e demais agentes públicos ou particulares que, por força de convênios, protocolos, acordos de cooperação e instrumentos congêneres, executem atividades vinculadas à ANA.

Art. 2º Para fins desta Resolução, entende-se por:

I - segurança da informação e comunicações: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento, com a implementação de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

II - comunicação: conjunto de recursos tecnológicos destinados a transmitir ou replicar informações;

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

IV - integridade: propriedade de que a informação não foi modificada, inclusive quanto à origem e ao destino, ou destruída de maneira não autorizada ou acidental;

V - confidencialidade: propriedade de que a informação classificada quanto ao grau de sigilo, ou de acesso restrito, não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

VI - autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por determinada pessoa física, ou por determinado sistema, órgão ou entidade;

VII - gestão de segurança da informação e comunicações: 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, não se limitando, portanto, à tecnologia da informação e comunicações;

VIII - tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive das classificadas quanto ao grau de sigilo;

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

X - ativos de informação: compreende os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios e também os recursos humanos que a eles têm acesso.

Art. 3º As ações relacionadas com a Segurança da Informação e Comunicações na ANA serão norteadas pelos seguintes princípios:

I - responsabilidade: todos mencionados no art. 1º, parágrafo único, são responsáveis pelo tratamento da informação e pelo cumprimento das normas de segurança da informação e comunicações;

II - conhecimento: os servidores, os colaboradores, os consultores externos, os estagiários e os prestadores de serviço na ANA tomarão ciência de todas as normas de segurança da informação e comunicações, para o pleno desempenho de suas atribuições;

III - legalidade: as ações de segurança da informação e comunicações levarão em consideração as leis, as políticas e as normas organizacionais, administrativas, técnicas e operacionais da ANA, formalmente estabelecidas;

IV - proporcionalidade: o nível, a complexidade e os custos das ações de segurança da informação e comunicações na ANA serão adequados ao entendimento administrativo e ao valor do ativo a proteger; e

V - proatividade: todas as unidades da ANA devem manter processo de gestão de continuidade das suas atividades e serviços, evitando a interrupção em caso de incidente de segurança, ou devido a caso fortuito ou de força maior, e assegurar a sua retomada em tempo hábil, quando for o caso.

Art. 4º São valores e diretrizes da Posic:

I - segurança focada na instituição: garantir segurança tanto aos sistemas no ambiente de computação quanto aos meios convencionais de processamento, comunicação e armazenamento em papel;

II - informação é patrimônio: considerar que toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela ANA é patrimônio da instituição e deve ser protegida quanto aos aspectos de confidencialidade, autenticidade, integridade e disponibilidade;

III - proteção compatível com riscos: dimensionar e aplicar os investimentos necessários em medidas de segurança, segundo o valor do ativo que está sendo protegido e de acordo com a identificação de risco de potenciais prejuízos para o negócio, a atividade fim e os objetivos institucionais;

IV - tratamento conforme classificação: tratar todas as informações a partir da classificação de segurança, aplicada de maneira a serem adequadamente protegidas quanto ao seu acesso e uso;

V - responsabilização baseada na credencial: responsabilizar, com base no uso da credencial, que se caracteriza por ser pessoal e intransferível, qualificando aquele que se encontra formalmente associado a ela como responsável por todas as atividades desenvolvidas em seu uso,

sendo pré-requisito para a liberação da credencial o preenchimento de um termo de responsabilidade;

VI - utilização restrita às atividades: administrar o acesso e o uso da informação e dos ativos de informação de acordo com as atribuições necessárias para o cumprimento das atividades institucionais. Qualquer outra forma de uso necessitará de prévia autorização;

VII - utilização orientada à segurança: permitir somente o uso de ativos de informação homologados e autorizados pela ANA, desde que sejam identificados de forma individual, protegidos, inventariados, com documentação atualizada e estando de acordo com a legislação em vigor;

VIII - autorização definida pelos gestores: definir acessos e cancelar acessos aos recursos e aos locais restritos com base na solicitação do gestor de cada Unidade Organizacional – UORG, que também é responsável pelos ativos disponibilizados para uso;

IX - segregação de funções: segregar a administração e execução de funções ou áreas de responsabilidade críticas para o negócio, evitando o controle de um processo na sua totalidade, visando à redução do risco de mau uso acidental ou deliberado;

X - educação: promover continuamente ações educativas sobre segurança da informação e comunicações aos servidores e colaboradores para que realizem suas atividades na instituição de forma segura, utilizando procedimentos que minimizem os riscos e que possibilitem o uso correto dos ativos e ferramentas de informação, com destaque para os serviços de correio eletrônico e acesso à internet;

XI - auditoria: monitorar e auditar, pela área competente da ANA, a implementação e o cumprimento da Política de Segurança da Informação e Comunicações. Consultorias externas especializadas poderão ser utilizadas para avaliação da Posic e de seu cumprimento;

XII - continuidade aplicada aos serviços: planejar e definir estratégias para reduzir a um nível aceitável a possibilidade de interrupção causada por desastres ou falhas nos recursos que suportam os processos de trabalho. O resultado desse planejamento deve ser documentado, testado e revisado conforme a necessidade, assegurados os recursos necessários à sua implementação; e

XIII - notificação imediata de incidentes: notificar o incidente imediatamente ao superior hierárquico que, sem prejuízo dos encaminhamentos necessários à apuração de responsabilidades, dará ciência do fato à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR.

Art. 5º Será criado o Comitê de Segurança da Informação e Comunicações – CSIC da ANA, coordenado pelo Gestor de Segurança da Informação e Comunicações.

Art. 6º O CSIC será instituído e o Gestor de Segurança da Informação e Comunicações será designado mediante Portarias do Diretor-Presidente da ANA.

Art. 7º As normas específicas, necessárias à implementação da Posic, serão sugeridas pelo CSIC e posteriormente aprovadas pela Diretoria Colegiada da ANA.

Art. 8º Esta Resolução entra em vigor na data e sua publicação.

(assinado eletronicamente)
VICENTE ANDREU