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

ANA
AGÊNCIA NACIONAL DE ÁGUAS

RESOLUÇÃO. Nº 1099, DE 26 DE JUNHO DE 2017
Documento nº 00000.039713/2017-10

Estabelece regras para a Política de Segurança da Informação e Comunicação - POSIC no âmbito da Agência Nacional de Águas - ANA.

O DIRETOR-PRESIDENTE DA AGÊNCIA NACIONAL DE ÁGUAS - ANA, no uso da atribuição que lhe confere o art. 95, inciso XVII, do Regimento Interno aprovado pela Resolução 2020, de 15 de dezembro de 2014 e, considerando o disposto no Decreto nº 3.505, de 13 de junho de 2000 e na Instrução Normativa GSI/PR nº1, de 13 de junho de 2008 e seus Normativos Complementares, torna público que a DIRETORIA COLEGIADA, em sua 661ª Reunião Ordinária, realizada em 26 de junho de 2017, resolveu:

Art. 1º Aprovar as regras para a Política de Segurança da Informação e Comunicação - POSIC no âmbito da Agência Nacional de Águas – ANA, instituída por meio Resolução ANA nº 1078, de 14 de setembro de 2015.

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 2º Para os efeitos desta Resolução, considera-se:

I – artefato malicioso: qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

II – ativos de informação: 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 (Ref. NC 10/IN01/DSIC/GSIPR);

III – conta de acesso: permissão lógica, expressa por meio de usuário e senha, que habilita determinada pessoa a acessar os sistemas e recursos de Tecnologia da Informação da Agência;

IV – correio eletrônico: sistema usado para criar, transmitir e receber mensagem eletrônica e outros documentos digitais por meio de rede de computadores;

V – equipe de tratamento e resposta a incidentes em redes computacionais – ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

VI – incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

VII - *links*: palavra, expressão ou imagem que permite o acesso imediato à outra

parte de um mesmo texto, ou de outro documento, bastando ser acionado pelo ponteiro do *mouse* . Quando o *link* é expresso na forma de uma palavra ou expressão (também denominado hiperlink ou hipertexto), ele vem sublinhado ou grafado em cor distinta da utilizada para o resto do texto;

VIII – proprietário do ativo de informação: servidor ou unidade organizacional responsável primário pela viabilidade e sobrevivência do ativo de informação (Ref. NC 10/IN01/DSIC/GSIPR);

IX – protocolo de transferência de arquivos (*file transfer protocol – FTP*): protocolo utilizado para transferir arquivos através de redes computacionais, incluindo a Internet;

X – registros de auditoria (*logs*): registro dos eventos relevantes ocorridos em um sistema computacional ou uma rede de computadores, utilizado para restabelecer o estado original ou para que o administrador conheça o seu comportamento no passado;

XI – *secure shell (SSH)*: protocolo de rede criptográfico que fornece um canal seguro sobre uma rede insegura (ex. Internet), possibilitando, assim, a execução de comandos remotos (ex. *login* remoto a um computador ou servidor específico);

XII - *site*: conjunto de documentos escritos em linguagem HTML, pertencentes a um mesmo endereço (URL), disponível na Internet;

XIII – *software*: o mesmo que programa ou aplicativo;

XIV – *service desk*: equipe designada pela Coordenação de Infraestrutura - COINF da Superintendência de Tecnologia da Informação - STI responsável pelo atendimento de todas demandas relativas a Tecnologia da Informação;

XV – usuário: pessoa física, seja servidor, colaborador ou estagiário habilitado para fazer uso de uma conta de acesso;

XVI – vírus: programa desenvolvido com intenção nociva, que inserido em um computador, pode causar queda da sua *performance*, destruição de arquivos e disco rígido, ocupar espaço livre de memória, entre outros danos. As formas mais comuns de contaminação são os dispositivos móveis de armazenamento e arquivos enviados por correio eletrônico;

XVII – rede privada virtual (v*irtual private network - VPN*): rede privada construída sobre a infraestrutura de uma rede pública, normalmente a Internet, sem a necessidade de utilização de conexões dedicadas.

Art. 3º Caberá à Superintendência de Tecnologia da Informação - STI prover a infraestrutura necessária para implementação desta Resolução.

CAPÍTULO II

DO CONTROLE DE ACESSO DO USUÁRIO

Seção I

Contas de Acesso à Rede Corporativa da ANA

Art. 4º Cada servidor da ANA receberá, após o devido credenciamento pela Coordenação-Geral de Gestão de Pessoas – CGGEP, uma conta de acesso única, pessoal e intransferível.

§ 1º O fornecimento da conta de acesso será realizado pela Coordenação de Infraestrutura de Tecnologia da Informação - COINF da Superintendência de Tecnologia da Informação - STI, mediante solicitação encaminhada pela CGGEP, por meio do "Formulário de

Solicitação de Cadastro de Usuário na Rede ANA", no qual constarão os dados cadastrais do usuário e os recursos de TI que deverão ser fornecidos (ex.: caixa de correio eletrônico, acesso ao Próton, certificado digital, dentre outros).

§ 2º O servidor deverá assinar o "Termo de Responsabilidade e Sigilo" (Anexo I), no qual declara ter conhecimento da POSIC e suas normas.

§ 3º O nome de usuário seguirá a nomenclatura padronizada pelas regras de formação de nomes para a composição de endereço eletrônico (e-mail) no Governo Federal, composto pelo nome seguido de ponto e de um sobrenome.

§ 4º A utilização de mensagens e de correio eletrônico corporativos deverá observar a Resolução ANA nº 1775, de 21 de novembro de 2014.

Art. 5º Os colaboradores e estagiários poderão receber conta de acesso, desde que o acesso à rede corporativa da ANA seja imprescindível à execução de suas atividades, a critério da CGGEP, seguindo o mesmo procedimento definido no art. 4º.

Art. 6º Os colaboradores que prestam serviços por demanda e que necessitam acesso à rede corporativa para executar atividades específicas poderão receber conta de acesso, sem caixa de e-mail pessoal, mediante solicitação do gestor do contrato à STI.

§ 1º A solicitação deverá conter dados cadastrais e o período que o colaborador desempenhará suas atividades.

§ 2º Caso o colaborador seja desligado da empresa antes do prazo estabelecido na ativação da conta, o gestor do contrato deverá informar o desligamento à STI para o bloqueio da conta.

Art. 7º Serão fornecidas, inicialmente, senhas seguras e temporárias com troca obrigatória no primeiro acesso realizado pelo usuário.

§ 1º É responsabilidade do usuário manter a confidencialidade de sua senha pessoal.

§ 2º As senhas deverão ter as seguintes características:

I – tamanho mínimo de 8 (oito) caracteres;

II – validade não superior a 12 (doze) meses;

III – compostas por ao menos uma letra e um número; e

IV – diferente das 3 (três) últimas senhas utilizadas pelo usuário.

§ 3º Em casos de perda ou esquecimento de senhas, uma nova senha deverá ser solicitada à COINF, pela chefia imediata do servidor ou colaborador, por meio de formulário específico cadastrado no Próton.

Art. 8º O perfil de administrador de rede somente será concedido para usuários que executam tarefas específicas na administração dos recursos de tecnologia da informação que compõem a rede corporativa da ANA.

Art. 9º A concessão de perfis para acessar sistemas específicos dependerá de prévia autorização do proprietário do ativo de informação correspondente.

Seção II

Bloqueio das Contas de Acesso

Art. 10. As contas de acesso serão bloqueadas nas seguintes situações:

I – após 5 (cinco) tentativas de acesso sequenciais malsucedidas;

II – quando não for utilizada, sem justificativa, por mais de 90 (noventa) dias, ocasião em que o bloqueio deverá ser informado à chefia imediata ou superior do usuário; e

III – em casos de suspeita de infração à POSIC, mediante autorização do Superintendente de Tecnologia da Informação.

§ 1º O bloqueio da conta de acesso impede que o usuário acesse a rede corporativa e a respectiva caixa de correio eletrônico, mas a conta continua existindo e os e-mails endereçados ao usuário são recebidos.

§ 2º O desbloqueio da conta de acesso, sem alteração da senha, deverá ser solicitado ao *Service Desk*.

§ 3º No caso de servidor em licença ou afastamento, previstos na Lei n.º 8112/90, cujo prazo seja superior ao estabelecido no inciso II, do caput, a CGGEP informará à STI para aplicação de regra especifica de bloqueio da conta.

Seção III

Exclusão das Contas de Acesso

Art. 11. A exclusão da conta de acesso do servidor, colaborador ou estagiário será realizado pela COINF, mediante solicitação encaminhada pela CGGEP, nos seguintes casos:

I – desligamento;

II – término do contrato de trabalho; e

III – falecimento.

§ 1º Os arquivos armazenados na estação de trabalho e na rede corporativa serão movidos e disponibilizados à última UORG de lotação do servidor, colaborador ou estagiário.

§ 2º Em caso de desligamento de diretor, a exclusão deverá ocorrer após o prazo correspondente à quarentena e os arquivos disponibilizados à SAF.

§ 3º Será mantida cópia da caixa de correio por 10 (dez) anos, para fins de auditoria. Após este prazo o conteúdo da caixa será excluído.

Seção IV

Procedimentos Durante os Afastamentos

Art. 12. A CGGEP deverá comunicar à STI, previamente, os servidores em licença ou afastamento, previstos na Lei n.º 8112/90, cujo prazo seja superior a 90 (noventa) dias, para que sejam tomadas as seguintes providências:

I – os arquivos de trabalho armazenados no computador *desktop* e nas pastas corporativas deverão ser movidos para que fiquem disponíveis à última UORG do servidor;

II – o computador desktop e notebook, se houver, serão formatados e ficarão disponíveis para nova distribuição; e

III – os servidores serão incluídos em política de acesso específica, que permite a utilização do webmail, restringe o acesso à rede interna da ANA e não bloqueia por prazo de inutilização.

Seção V

Autorização de Acesso às Contas

Art. 13. O acesso à conta de usuário será possível mediante indício de descumprimento dos termos desta Resolução ou de outros normativos, apurado em procedimento administrativo, assegurando-se o direito ao contraditório e à ampla defesa.

CAPÍTULO III

RESPONSABILIDADES E RECOMENDAÇÕES AO USUÁRIO

Seção I

Responsabilidades do Usuário

Art. 14. A conta de acesso disponibilizada ao usuário é pessoal e intransferível, sendo seu titular o único e total responsável pelas ações e danos que venham a ser ocasionados por mau uso do serviço.

Art. 15. É vedada a utilização da conta de acesso e dos recursos de TI corporativos para receber de forma consentida, armazenar e enviar/encaminhar mensagens contendo:

I - códigos maliciosos, conteúdo potencialmente perigoso, tais como arquivos executáveis, vírus, Cavalos de Tróia ou qualquer outro tipo de programa danoso;

II - materiais com conteúdo obsceno, ilegal, antiético, ofensivo ou que incentivem a violência, discriminação ou preconceito ou que façam sua apologia;

III - conteúdos tendentes a comprometer a intimidade de usuários ou a imagem institucional;

IV - materiais protegidos por leis de propriedade intelectual;

V - materiais com objetivos comerciais, particulares e anúncios publicitários; e

VI - materiais de natureza político-partidária ou sindical, que promova a eleição de candidatos para cargos públicos eletivos, clubes, associações e sindicatos.

Art. 16. Caracterizam-se como utilização indevida dos recursos de tecnologia da informação as seguintes ações:

I – ataque, monitoração ou acesso não autorizado aos recursos de tecnologia da informação da organização ou de redes externas, utilizando recursos da organização ou outros meios;

II – instalação de *softwares* sem licença ou não autorizados pela organização;

III – utilização dos recursos de TI em atividades particulares ou com fins lucrativos;

IV – instalação ou disseminação de vírus de computadores ou *software* que coloquem em risco as instalações e os recursos de tecnologia da informação da organização;

V – alteração da configuração de *hardware* dos recursos de tecnologia da informação, sem a devida solicitação à STI;

VI – cópia de arquivos, programas de computador, conteúdos de bases de dados, ou outros ativos de informação da ANA, sem a devida autorização do proprietário do ativo; e

VII – todo e qualquer procedimento no uso dos recursos de TI não previsto nesta norma que possam afetar de forma negativa a organização, seus servidores e seus colaboradores.

Art. 17. É vedada a utilização dos recursos de TI corporativos para armazenamento de arquivos particulares ou outros que não tenham relação direta com as atividades da Agência.

Seção II

Estações de Trabalho e Notebooks

Art. 18. Não será concedido perfil de administrador das estações de trabalho e notebooks aos usuários, devendo quaisquer alterações em sua configuração ou instalação de aplicativos serem solicitadas ao *Service Desk*.

§ 1º Em caso de necessidade devidamente justificada, poderá ser concedido perfil de administrador da estação de trabalho e notebook, mediante solicitação realizada pelo chefe da UORG de lotação do servidor ou colaborador.

§ 2º Não poderão ser instalados nas estações de trabalho e notebooks programas não autorizados pela STI e sem o devido licenciamento. Em caso de dúvidas, o *Service Desk* deve solicitar autorização da COINF para realizar a referida instalação.

Art. 19. O usuário deverá bloquear o acesso à sua estação de trabalho sempre que se ausentar do equipamento.

Art. 20. Ao final do expediente, o usuário deverá encerrar a sessão em sua estação de trabalho, de forma que o equipamento não permaneça ligado, sem utilização, por períodos prolongados.

Seção III

Uso da Internet

Art. 21. O acesso à internet deve ser realizado por meio das conexões disponibilizadas e autorizadas pela Agência e terá controle de tráfego para fins de aplicação desta Política.

Art. 22. A internet não deve ser utilizada para:

I – transmitir, para si ou para terceiros, *softwares* ou informações custodiadas ou de propriedade da organização, sem prévia autorização;

II – acessar sites de pornografia, pedofilia, que façam incitação à violência e outros contrários à legislação e regulamentação em vigor, mesmo que alguns desses sites não estejam bloqueados pelos mecanismos de segurança implementados na rede corporativa;

III – acessar sites com materiais atentatórios à moral e aos bons costumes, ofensivos ou que façam sua apologia, incluindo os de pirataria ou que divulguem número de série para registro de *softwares*;

IV – executar atividades relacionadas a jogos eletrônicos; e

V – acessar conteúdo multimídia, como vídeos e música, exceto nos casos em que tais ações sejam condizentes com as atividades de trabalho realizados.

Parágrafo único. Sites que possuam conteúdos relacionados aos itens acima poderão ser bloqueados pela Agência e sua liberação dependerá de análise do Comitê de Segurança da Informação e Comunicação - CSIC.

Seção IV

Acesso Remoto

Art. 23. O acesso remoto à rede corporativa deve ser realizado por meio seguro através de uma VPN disponibilizada e autorizada pela STI.

Parágrafo único. *Softwares* que permitam acesso remoto diferente daquele autorizado pela COINF serão bloqueados.

Art. 24. O acesso remoto por meio de VPN será disponibilizado aos diretores, assessores de diretores, chefes de UORGs e respectivos substitutos.

§ 1º Poderá ser concedido acesso remoto a outros servidores, por período determinado, para atender a necessidades de trabalho, desde que devidamente justificado, mediante solicitação do respectivo chefe da UORG.

§ 2º Será realizado, anualmente, uma reavaliação dos servidores que possuem acesso à VPN.

§ 3º O acesso remoto não poderá ser utilizado em substituição ao trabalho presencial no horário regular de trabalho.

Art. 25. Devem ser criados e armazenados os registros de auditoria (*logs*) dos acessos remotos contendo informações do usuário, data, hora e outros dados específicos que possibilitem o rastreamento das ações tomadas para posterior auditoria.

Seção V

Impressoras e Scanners

Art. 26. É vedada a utilização das impressoras e *scanners* para fins pessoais, cabendo à SAF a implementação de controle mediante a utilização da conta de acesso e divulgar o correto funcionamento desses recursos.

Parágrafo único. Os arquivos digitalizados nos *scanners* ficarão disponíveis em uma pasta pública e serão excluídos automaticamente ao final do dia.

CAPÍTULO IV

SEGURANÇA DA REDE CORPORATIVA

Seção I

Monitoramento da Rede Corporativa

Art. 27. A STI deve manter, na rede corporativa, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados, armazenando os registros de auditoria – *logs* (Ref. NC 07/IN01/DSIC/GSIPR).

Art. 28. A fim de preservar a integridade das informações institucionais, a imagem da organização e garantir a segurança de seus sistemas e, também, para fins de apuração de eventual prática indevida, poderão ser monitorados, de forma contínua, e gerados relatórios anuais sobre os seguintes conteúdos:

I – endereços de correio eletrônico;

II – sites acessados;

III – arquivos residentes em recursos de tecnologia da informação e afins;

IV – programas de computador (*software*); e

V – bases específicas de controle (*logs*).

Parágrafo único. O conteúdo das mensagens de correio eletrônico e dos arquivos

armazenados nas estações de trabalho só serão acessados, sob demanda, nos casos previstos no art. 13.

Seção II

Proteção Contra Códigos Maliciosos

Art. 29. Os recursos de TI devem estar providos de soluções de detecção e bloqueio de programas com códigos maliciosos, como *antispyware*, antivírus e filtros de análise de conteúdo de correio eletrônico e tráfego internet.

§ 1º O *software* antivírus é obrigatório nos recursos de TI disponibilizados aos usuários e deve ser mantido sempre ativado e atualizado.

§ 2º O *software* antivírus deve ser configurado para executar a varredura completa nos recursos de TI da Agência, com periodicidade máxima semanal.

§ 3º É proibida a inativação do antivírus ou a interrupção da execução da varredura pelo usuário da rede.

Seção III

Do Tratamento de Incidentes de Segurança

Art. 30. Deve ser instituída, no âmbito da STI, a Equipe de Tratamento e Resposta a Incidentes - ETIR, conforme disposto na NC 05/IN01/DSIC/GSIPR, a ser coordenada pelo Gestor de Segurança, conforme definido na Portaria ANA nº 333, de 22 de setembro de 2015.

Art. 31. Compete à ETIR:

I – o tratamento de incidentes e artefatos maliciosos (definir);

II – o tratamento de vulnerabilidades na rede da ANA;

III – a emissão de alertas e advertências, em resposta a um incidente de segurança ocorrido;

IV – o anúncio aos usuários sobre vulnerabilidades identificadas e formas de mitigá-las;

V – a prospecção de novas tecnologias relativas à segurança da informação; e

VI – a avaliação da infraestrutura de segurança.

Parágrafo único. Deve ser mantido o registro de todos os incidentes notificados ou detectados, com a finalidade de assegurar o registro histórico das atividades da ETIR.

Art. 32. Os usuários da rede devem, por meio da caixa corporativa etir@ana.gov.br, informar à ETIR sobre quaisquer incidentes ou vulnerabilidades de segurança que tomarem conhecimento.

Seção IV

Acesso de Usuários Externos

Art. 33. É proibida a conexão na rede corporativa interna da ANA, seja por VPN ou qualquer outro meio, sem a autorização da STI.

§ 1º Antes da conexão de um usuário externo com a rede corporativa da ANA, deve ser realizada análise de riscos, a fim de identificar possíveis vulnerabilidades que possam

expor as informações às pessoas não autorizadas e impactos provenientes deste acesso.

§ 2º Os usuários externos somente poderão ter acesso aos serviços que tenham sido especificamente autorizados pela STI e que sejam comprovadamente relativos às atividades que serão desempenhadas.

§ 3º As conexões de usuários externos à rede corporativa da ANA devem ser precedidas da assinatura do Termo de Responsabilidade e Sigilo (Anexo I).

Art. 34. Os serviços de rede que podem ser disponibilizados a usuários externos são:

I – troca de arquivos via FTP: a troca de arquivos deve ser realizada via FTP nos servidores destinados a este fim;

II – acesso via SSH: acessos por meio de SSH a servidores específicos da rede corporativa podem ser disponibilizados a usuários externos, desde que autorizados e de forma controlada por lista de controle de acesso, rotas estáticas ou qualquer outro modo de controle;

III – acesso a sistemas web internos: acessos a sistemas web internos somente devem ser fornecidos a usuários externos quando formalmente justificados, homologados e autorizados;

IV – acesso ao repositório de códigos fonte de sistemas - este tipo de acesso deve ser analisado e, se for o caso, autorizado pelos proprietários dos ativos de informação; e

V – acesso a bancos de dados: este tipo de acesso deve ser provido com devida autorização dos proprietários dos ativos de informação: bases de dados e sistemas.

Seção V

Acesso à Rede sem Fio

Art. 35. A ANA proverá, para os usuários da rede e para usuários externos, acesso à internet por meio de rede sem fio, disponível nas dependências da Agência.

§ 1º Os usuários que possuem conta de acesso, deverão utilizar a mesma conta para utilizar a rede sem fio;

§ 2º Durante a realização de eventos, poderá ser disponibilizada aos participantes, mediante solicitação prévia da UORG organizadora do evento, rede específica para acesso à internet.

§ 3º Os servidores poderão gerar credenciais de acesso à internet por meio de rede sem fio para usuários externos, válidas por 24 (vinte e quatro) horas, por meio de formulário específico disponível na intranet da Agência.

Seção VI

Solicitação de Acesso aos Registros de Auditoria (*logs*)

Art. 36. Poderão ser mantidos registros de auditoria (*logs*) para os sistemas específicos, conforme necessidade levantada durante o desenvolvimento do referido sistema, e registros de auditoria gerais para monitorar as atividades da rede, contemplando:

I – acesso à rede corporativa;

II – acesso à internet; e

III – utilização de VPN;

Art. 37. Quaisquer registros de auditoria poderão ser solicitados à STI, em casos de processos apuratórios, pela autoridade competente ou pela Diretoria Colegiada.

Parágrafo único: Os registros de auditoria relativos às atividades de rede de uma conta de acesso específica poderão ser solicitados à STI pela chefia da UORG a qual a conta de acesso está vinculada.

Art. 38. Os registros de auditoria gerados pelos sistemas específicos poderão ser solicitados pelo respectivo proprietário do ativo da informação ou pelo chefe da UORG correspondente.

Parágrafo único. Caso seja necessário, poderão ser também solicitadas à STI auditorias técnicas específicas para dirimir eventuais dúvidas quanto à integridade dos dados armazenados.

CAPÍTULO V

CÓPIA DE SEGURANÇA (*BACKUP*) E RETENÇÃO DE DADOS

Art. 39. Os arquivos armazenados nas pastas corporativas, caixas de correio eletrônico e bases de dados terão política de *backup* e retenção de dados conforme critérios mínimos apresentados abaixo:

I - *backups* diários serão mantidos por no mínimo 5 (cinco) dias;

II - *backups* mensais serão mantidos por no mínimo 12 (doze) meses; e

III - *backups* anuais serão mantidos por no mínimo 5 (cinco) anos.

Art. 40. Os arquivos do sistema informatizado de gestão arquivística de documentos, denominado PRÓTON DIGITAL, terão política de *backup* específica, conforme estabelecido na Resolução nº 1774 de 21 de novembro de 2014.

Parágrafo único. Os documentos eliminados fisicamente, conforme normatização do Arquivo Nacional, deverão ser também eliminados digitalmente e excluídos dos *backups* existentes.

Art. 41. Os arquivos armazenados nos computadores *desktops* não participarão da política de *backup* e retenção de dados, sendo a cópia de segurança de responsabilidade de cada servidor.

CAPÍTULO VI

DISPOSIÇÃO FINAL

Art. 42. As infrações ao disposto nesta Resolução estão sujeitas aos processos e penalizações previstos nas legislações de regência.

Art. 43. Esta Resolução entra em vigor na data de sua publicação.

(assinado eletronicamente)
VICENTE ANDREU

Anexo I

MODELO DE TERMO DE Responsabilidade e SIGILO

Declaro ter conhecimento da Política de Segurança da Informação e Comunicações (POSIC) da Agência Nacional de Águas (ANA) e suas normas específicas e estou ciente dos princípios de conduta ética e moral que regem todas as relações de trabalho e atividades exercidas.

Comprometo-me a realizar meu trabalho de forma íntegra, respeitando os preceitos fundamentais que pautam a missão, a visão e os valores desta instituição.

Afirmo que as normas constantes na POSIC, os princípios éticos e demais parâmetros de conduta, orientarão o meu comportamento em todas as futuras iniciativas e decisões profissionais, como usuário de ativos de informação.

Reconheço que, ao término da minha relação de trabalho, devo entregar todo e qualquer material de propriedade da Instituição como, por exemplo, equipamentos portáteis, arquivos envolvendo informações pertencentes à Instituição, documentos e processos de qualquer natureza que tenham sido usados, criados ou estado sob meu controle, entre outros.

Obrigo-me a informar, imediatamente, qualquer violação das regras da POSIC, por minha parte ou de quaisquer outras pessoas, que possam prejudicar a confidencialidade, a disponibilidade, a integridade e a autenticidade das informações.

[Local], ___ de _____ de _____.

_____
Nome e unidade organizacional: [Agente Público]
Matrícula

_____
Nome e unidade organizacional: [Responsável pela área ou departamento]

ANA
AGÊNCIA NACIONAL DE ÁGUAS

RESOLUÇÃO Nº 38, DE 24 DE JUNHO DE 2019
Documento nº 02500.044526/2019-12

Altera os artigos 4º e 7º da Resolução nº 1.099, de 26 de junho de 2017, que define as regras para a Política de Segurança da Informação e Comunicação – POSIC, no âmbito da Agência Nacional de Águas - ANA.

A DIRETORA-PRESIDENTE DA AGÊNCIA NACIONAL DE ÁGUAS - ANA, no uso da atribuição que lhe confere o art. 112, inciso III e XVII, da Resolução nº 32, de 23 de abril de 2018, que aprovou o Regimento Interno da ANA, torna público que a DIRETORIA COLEGIADA, em sua 750ª Reunião Ordinária, realizada em 24 de junho de 2019, e com base nos elementos constantes no Processo 02501.002347/2014-85, resolve:

Art. 1º Os artigos 4º e 7º da Resolução ANA 1.099, de 26 de junho de 2017, passam a vigorar com as seguintes alterações:

"Art. 4º .....

.....

§ 3º O nome de usuário seguirá a nomenclatura padronizada pelas regras de formação de nomes para a composição de endereço eletrônico (e-mail) no Governo Federal, composto pelo nome seguido de ponto e de um sobrenome. No caso de terceirizados e estagiários, além do nome e sobrenome, será acrescentado o termo terceirizado e estagiário na composição do endereço eletrônico.

....."

"Art. 7º .....

.....

§ 2º .....:

.....

IV – diferente da última senha utilizadas pelo usuário."

Art. 2. Esta Resolução entra em vigor na data de sua publicação.

(assinado eletronicamente)
CHRISTIANNE DIAS FERREIRA