INSTRUÇÃO NORMATIVA N.º 118 DE 14 DE MARÇO DE 2024

IMPLEMENTA A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (POSIC) NO ÂMBITO DA AGÊNCIA REGULADORA DE ENERGIA E SANEAMENTO BÁSICO DO ESTADO DO RIO DE JANEIRO (AGENERSA).

O CONSELHO-DIRETOR DA AGÊNCIA REGULADORA DE ENERGIA E SANEAMENTO BÁSICO DO ESTADO DO RIO DE JANEIRO – AGENERSA, no uso de suas atribuições legais e regimentais e tendo em vista o que consta do **Processo nº** SEI-220007/001585/2023.

CONSIDERANDO

- o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) e sua regulamentação pelo Decreto nº 43.597, de 17 de maio de 2012;

- o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);

- o disposto na Instrução Normativa PRODERJ/PRE nº 02 de 28 de abril de 2022;

- a Portaria PRODERJ/PRE Nº 825, de 26 de fevereiro de 2021, que institui a Estratégia da Governança de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro – EGTIC/RJ, notadamente o art. 1º, IV, que prevê a instituição de Instruções Normativas para a efetivação da Governança de Tecnologia da Informação e Comunicação no Estado do Rio de Janeiro, bem como o art. 11, do Anexo B, que trata de ações de governança voltadas à segurança da informação e à proteção de dados;
- a decisão proferida pelo Conselho Diretor na 7ª Reunião Interna Ordinária , realizada em 14 de março de 2024

RESOLVE:

Art. 1º - Instituir a Política de Segurança da Informação (POSIC) no âmbito da Agência Reguladora de Energia e Saneamento Básico do Estado do Rio de Janeiro, conforme Anexos I, II e III.

Art. 2º - Os casos omissos e eventuais dúvidas suscitadas serão objeto de avaliação e decisão por parte deste Conselho Diretor.

Art. 3º - Esta Instrução Normativa entrará em vigor na data de sua publicação no Diário Oficial.

Rio de Janeiro, 14 de março de 2024

Rafael Carvalho de Menezes
Conselheiro-Presidente

Rafael Augusto Penna Franca
Conselheiro

Vladimir Paschoal Macedo
Conselheiro

José Antonio de Melo Portela Filho
Conselheiro

Este texto não substitui o publicado no DOERJ de 18.03.2024

ANEXO I
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (POSIC) NO ÂMBITO DA AGÊNCIA REGULADORA DE ENERGIA E SANEAMENTO BÁSICO DO ESTADO DO RIO DE JANEIRO

SUMÁRIO

TÍTULO I
DAS DIRETRIZES GERAIS

CAPÍTULO I
TRATAMENTO DA INFORMAÇÃO

Art. 1º - O presente documento tem como objetivo direcionar informação e conhecimento, por meio de políticas de segurança, aos usuários de ativos e serviços da informação desta Agência Reguladora de Energia e Saneamento Básico do Estado do Rio de Janeiro (AGENERSA), a fim de garantir a preservação da confidencialidade, integridade e disponibilidade.

Art. 2º - A Política de Segurança da Informação (POSIC) provê as diretrizes, princípios, competências e responsabilidades necessárias a viabilizar a Gestão de Segurança da Informação (GSI) no âmbito da AGENERSA, com vistas a assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações produzidas, transmitidas e custodiadas pelos sistemas de informação desta Autarquia.

Parágrafo único. A POSIC é aplicável a toda a Instituição, devendo ser observada por todos os servidores, colaboradores, fornecedores, prestadores de serviço e por aqueles que, de alguma forma, executem atividades voltadas à atuação institucional da AGENERSA.

Art. 3º - Para efeitos desta Política de Segurança da Informação, são estabelecidos os seguintes conceitos e definições:

I – **ameaça**: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a AGENERSA;
II – **atividades críticas**: atividades que devem ser executadas para garantir a prestação de serviços fundamentais da AGENERSA;
III – **ativo de informação**: recurso utilizado na produção, processamento, armazenamento, transmissão e recuperação da informação, incluindo a própria informação, sistemas de informação, locais onde se encontram esses meios e as pessoas que a eles têm acesso;
IV – **autenticidade**: propriedade pela qual se assegura a informação produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;
V – **celeridade**: as ações relacionadas à segurança da informação deverão oferecer respostas ágeis para os incidentes e para as vulnerabilidades identificadas nos sistema de informação da AGENERSA;
VI – **assessoria de informática (ASSIN):** trata-se da Assessoria da AGENERSA responsável pela área de Tecnologia da Informação;
VII – **computação em nuvem**: modelo computacional que permite o acesso por demanda, e independente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, serviços, processamento, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;
VIII – **confidencialidade**: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;

IX – **disponibilidade**: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;
X – **dispositivos móveis**: equipamentos portáteis dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes: notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HDs externos e cartões de memória;
XI - **gestor da informação**: indivíduo responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades institucionais;
XII – **gestor de segurança da informação**: responsável pelas ações de segurança da informação no âmbito da AGENERSA;
XIII – **incidente de segurança**: qualquer evento adverso, confirmado ou sob suspeita, ou ocorrência que promova uma ou mais ações tendentes a comprometer ou ameaçar a disponibilidade, a integridade, confidencialidade ou autenticidade de qualquer ativo de informação da AGENERSA;
XIV – **integridade**: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
XV – **quebra de Segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

Art. 4º - A POSIC deve obedecer aos seguintes princípios, mas não se limitando a:

I - interesse público;
II - preservação e a defesa do patrimônio público;
III - legalidade;
IV - impessoalidade;
V - moralidade;
VI - transparência;
VII - honestidade;
VIII - integridade;
IX - disponibilidade;
X - publicidade;
XI - autenticidade;
XII - confidencialidade; XIII - responsabilidade; XIV - não-repúdio;
XV – prevenção.

CAPÍTULO II
GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 5º - A Gestão de Segurança da Informação (GSI) compreende ações e métodos que visam à integração das atividades de Segurança da Informação aos processos institucionais, estratégicos, táticos e operacionais.

§ 1º. Todos os sistemas, serviços e recursos computacionais estão sujeitos a monitoramento, controle de acesso e auditoria.
§ 2º. As informações e registros obtidos pelo desenvolvimento das atividades da GSI poderão ser utilizados pela detecção de violações da POSIC e normas vigentes.

Art. 6º - A AGENERSA deverá adotar cláusulas de segurança da informação nos contratos com terceiros, de forma a resguardar o sigilo e a confidencialidade de toda e

qualquer informação constante dos seus ativos tecnológicos, com as quais os prestadores de serviços venham a ter contato.

Art. 7º - Os bens de Tecnologia de Segurança da Informação (TIC) cuja propriedade pertença a AGENERSA ou em nome dela tenham sido disponibilizados aos usuários são de livre acesso à ASSIN, sem necessidade de autorização ou ciência previa do usuário.

CAPÍTULO III
TRATAMENTO DA INFORMAÇÃO E DE INCIDENTES DE REDE

Art. 8º - Os ativos de informação serão protegidos contra ameaças e ações não autorizadas, acidentais ou não, com o objetivo de reduzir riscos e de garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

§ 1º. É vedado ao usuário o acesso a ativos de informação e sistemas que não tenha sido expressamente autorizado pelo Gestor da Informação.
§ 2º. Os documentos eletrônicos considerados imprescindíveis para as atividades da AGENERSA deverão ser armazenados nos sistemas de informação ou nos servidores de arquivos disponibilizados pela ASSIN.
§ 3º. A destruição de documentos eletrônicos deverá observar a sua classificação, adotando procedimentos de segurança que inviabilizem eventual recuperação e acesso não autorizado.

Art. 9º - As informações criadas, armazenadas, manuseadas, transportadas ou descartadas na AGENERSA deverão ser classificadas segundo o grau de sigilo, quando necessário, e protegidas segundo a sua criticidade e outros critérios, conforme as normas e a legislação em vigor.

§ 1º. As informações públicas a que se refere o caput deste artigo serão adequadamente disponibilizadas à sociedade por mecanismos próprios de transparência previstos na Lei de Acesso à Informação e em suas regulamentações infralegais.
§ 2º. As informações pessoais e sigilosas geradas ou mantidas pela AGENERSA serão objeto de tratamento e proteção que lhes garantam a inviolabilidade.
§3º. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
§ 4º. Os usuários são responsáveis pela limpeza dos computadores, garantindo que os arquivos e documentos temporários sejam apagados ou destruídos.

Art. 10 - As ocorrências de incidentes de segurança em redes computacionais, no âmbito da AGENERSA, deverão ser registradas com a finalidade de assegurar a manutenção de histórico das atividades desenvolvidas.

CAPÍTULO IV
GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 11 - A Gestão de Riscos de Segurança da informação deverá identificar e implementar as medidas de proteção necessárias para o tratamento dos riscos.

Parágrafo único. Deverá ser considerado o equilíbrio entre as medidas de proteção referidas no *caput* e os custos operacionais e financeiros envolvidos, evitando que as

ameaças, de origem natural ou humana, de forma acidental ou não, explorem as vulnerabilidades dos ativos de informação e provoquem danos pela destruição não autorizada, revelação indevida, adulteração ou perda das informações da AGENERSA.

CAPÍTULO V

GESTÃO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO

Art. 12 - A Gestão de Continuidade de Negócios em Segurança da Informação tem como finalidade evitar que os serviços institucionais, baseados em TIC, sejam interrompidos e, quando for o caso, assegurar o seu restabelecimento no tempo necessário.

Art. 13 - A AGENERSA deverá definir quais são suas atividades críticas, com o objetivo de subsidiar a elaboração do Programa de Gestão de Continuidade de Negócios.

CAPÍTULO VI
POLÍTICA DE RESPOSTAS A INCIDENTES

Art. 14 - Nenhum tipo de informação sobre incidentes e ocorrências de segurança da informação poderá ser divulgado para entidades ou pessoas externas à AGENERSA sem aprovação expressa e formal da ASSIN.

Art. 15 - Todos os incidentes de segurança da informação ou suspeitas devem ser imediatamente comunicados a área de segurança da informação seja por colaboradores, fornecedores, parceiros de negócios entre outros.

TÍTULO II
POLÍTICAS DE CLASSIFICAÇÃO E DE CONTROLE

CAPÍTULO I
POLÍTICA DE CONTROLE DE ACESSO FÍSICO E DIGITAL

Art. 16 - Para efeitos de classificação da informação, a AGENERSA utiliza as seguintes categorias:

I - informação pública;
II - informação de uso interno; III - informação confidencial.

Art. 17 - O manuseio da informação da AGENERSA deverá obedecer às regras definidas para cada classificação.

Parágrafo único. O descarte da informação deve ser realizado de forma a impedir a sua recuperação, independentemente do seu formato de armazenamento original.

Art. 18 - O controle de acesso físico tem como finalidade proteger os equipamentos, documentos e suprimentos contra ameaças e ações não autorizadas, acidentais ou não, com o objetivo de reduzir os riscos e de garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

Art. 19 - O controle de acesso lógico tem como finalidade proteger os sistemas de informação e demais ativos de informação contra ameaças e ações não autorizadas, acidentais ou não, com o objetivo de reduzir os riscos e de garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

§1º. São consideradas áreas restritas os locais onde informações de clientes são armazenadas e/ou manipuladas (Arquivos internos e externos);
§2º. Os controles de acessos lógicos deverão observar o princípio da proporcionalidade, restringindo o conjunto de privilégios ao mínimo necessário para o desempenho das atribuições profissionais do usuário.

Art. 20 - Todo usuário receberá acessos com privilégios mínimos necessários ao desempenho das atribuições para as quais for designado.

Parágrafo único. Situações excepcionais de acessos diferenciados deverão ser motivadas pelos gestores da informação, por tempo certo, na forma de regulamentação específica dessa disciplina.

Art. 21 - A autorização e o nível permitido de acesso ativos/serviços de informação da ASSIN é feita com base em perfis que definem o nível de privilégio dos usuários.

Art. 22 - As senhas associadas às contas de acesso a ativos/serviços de informação ou recursos computacionais da AGENERSA são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo.

§ 1º. As senhas de acesso a rede, para usuários finais, deverão conter no mínimo 8 (oito) caracteres, sendo obrigatório o uso de letras maiúsculas, minúsculas e números. Como recomendação sugere-se a utilização de caracteres especiais (“$”, “%”, “&”,...).
§ 2º. Deverá ser evitada a composição de senhas com sequências numéricas (123...) e/ou alfabéticas (abc...), além de senhas de fácil dedução (nome da máquina, nome do usuário, data de nascimento).

Art. 23 - As contas de rede (login) e correio eletrônico (e-mail) serão solicitadas pela Assessoria de Recursos Humanos por meio do sistema de Chamados GLPI http://atendeagenersa/glpi ou por processo administrativo, no sistema SEI(Sistema Eletrônico de Informações), direcionados à ASSIN, no momento da admissão do usuário.

§ 1º. A conta deverá ser bloqueada após a 5ª (quinta) tentativa de login;
§ 2º. A conta será desbloqueada automaticamente após decorridos 30 (trinta) minutos;
§ 3º. O usuário que efetuar a troca da senha não poderá repetir as 5 (cinco) últimas.
§ 4º. A senha deverá ser modificada imediatamente caso o usuário suspeite de seu comprometimento.

Art. 24 - A criação de contas de e-mail institucional necessita de solicitação, com validação e autorização da chefia imediata, demonstrando a necessidade desse serviço para o desempenho das atribuições profissionais de cada usuário.

CAPÍTULO II
CÓPIA DE SEGURANÇA

Art. 25 – Todo ativo de informação corporativa deverá ser considerado para inclusão na política de cópia de segurança, observando-se os requisitos legais e a criticidade das informações relacionadas às atividades da AGENERSA.

Parágrafo único. Considera-se ativo de informação corporativa todos os dados armazenados, sistemas de informação, pastas de rede e arquivos digitalizados armazenados e /ou hospedados no CPD da AGENERSA ou nuvem AGENERSA.

TÍTULO III
ACESSO À INTERNET E REDE E POLÍTICA DE ACESSO REMOTO

Art. 26 - O acesso à Internet concedido aos usuários deverá observar o princípio da proporcionalidade, restringindo o perfil de acesso ao mínimo necessário para o desempenho das atribuições profissionais do usuário.

Parágrafo único. Situações excepcionais de acessos diferenciados deverão ser motivadas pelos gestores da informação, por tempo certo, na forma de regulamentação específica dessa disciplina.

Art. 27 - Há 4 (quatro) categorias de acesso à Internet, a saber:

I – acesso Restrito, que consiste na liberação de todas as categorias de sites, exceto aquelas listadas na Tabela 1, Anexo II, que serão bloqueadas.

II– acesso Intermediário, que consiste no acesso Restrito, mais os acessos a vídeos, redes sociais, rádios e músicas.
III – acesso Completo, que consiste no acesso a todos os sites, salvo aqueles de conteúdo ilícito e imoral, que serão bloqueados.
IV – acesso Completo S/ QoS, que consiste no acesso a todos os sites, salvo aqueles de conteúdo ilícito e imoral, que serão bloqueados, sem limitação de banda.

§ 1º. Deverá ser respeitado o princípio do menor privilégio para configurar as contas de acesso dos usuários e colaboradores à Internet da AGENERSA, sendo inicialmente o usuário cadastrado na categoria Intermediário.
§ 2º. À equipe de infraestrutura e a Assessoria de Informática é facultado o acesso irrestrito à internet para fins de pesquisa, rastreio e outros atinentes às rotinas técnicas da área de tecnologia da informação.

Art. 28 - A publicação de conteúdo referente à AGENERSA em mídias e redes sociais é feita por setores e usuários que possuem essa responsabilidade específica, sendo os demais usuários proibidos de publicar qualquer tipo de informação em nome da organização.

Art. 29 - As mudanças de categoria de acesso serão realizadas de acordo com os seguintes procedimentos:

I - autorização por meio do sistema de Chamados GLPI http://atendeagenersa/glpi por processo administrativo no sistema SEI(Sistema Eletrônico de Informações) direcionados à ASSIN, com a devida justificativa da chefia imediata, que deverá ser convalidado pela respectiva Assessoria ou unidade equivalente;
II - deverão ser informados o nome e login de Rede do usuário, além do período em que o acesso permanecerá liberado.

Art. 30 - O acesso remoto a ativos/serviços de informação e recursos computacionais da AGENERSA é restrito a usuários que necessitem deste recurso para execução das atividades profissionais, como atividade de suporte a Servidores e sistemas de terceiros.

§ 1º. Com o intuito de preservar a segurança do ambiente de rede da AGENERSA, o acesso remoto só poderá ser concedido em casos excepcionais e após autorização expressa da chefia imediata.
§ 2º. Caberá a Assessoria de Informática conceder os acessos e monitorar a utilização destes acessos.

Art. 31 – O acesso à rede Wi-Fi corporativa é para uso exclusivo dos recursos computacionais e dispositivos móveis institucionais com a finalidade de apoiar e viabilizar atividades relacionadas aos serviços institucionais.

Parágrafo único. Acessos pessoais ou em recursos computacionais e dispositivos móveis que não sejam caracterizados como institucionais, com finalidades estranhas aos serviços da AGENERSA, somente poderão ser realizados pela rede Wi-Fi para "visitantes".

Art. 32 - O acesso remoto a ativos/serviços de informação e recursos computacionais da AGENERSA poderá ser concedido a terceiros ou prestadores de serviço caso seja necessário para suas atividades laborais.

Art. 33 - Toda informação que é acessada, transmitida, recebida ou produzida por meio do acesso remoto a ativos/serviços de informação ou recursos computacionais da AGENERSA está sujeita a monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade.

Art. 34 - A instalação e a configuração de softwares pertencentes à AGENERSA ou de versões de testes e/ou gratuitas nos recursos computacionais e dispositivos móveis institucionais deverão ser realizadas pela ASSIN, que se responsabilizará pela guarda das mídias e sua eventual desinstalação.

§ 1º. Todo software deverá ser previamente homologado pela ASSIN antes de sua utilização no ambiente da AGENERSA.
§ 2º. Independente do perfil de acesso do usuário, somente a ASSIN poderá instalar softwares nos recursos computacionais e dispositivos móveis institucionais.

TÍTULO V
GESTÃO E USO DE DISPOSITIVOS E RECURSOS TECNOLÓGICOS

Art. 35 - Os equipamentos disponíveis aos colaboradores são de propriedade da AGENERSA, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas áreas responsáveis.

Art. 36 - É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Assessoria de Informática (ASSIN).

Art. 37 - Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Art. 38 - Os sistemas e computadores devem ter versões do software antivírus instalados, ativadas e atualizadas permanentemente.

Art. 39 - O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no GLPI http://atendeagenersa/glpi ou pelos ramais internos que direcionam à ASSIN.

Art. 40 - A gestão de recursos computacionais e o uso de dispositivo móveis deverá ser pautada por comportamento ético e profissional, observando as determinações da POSIC e normativos vigentes.

Art. 41 - O uso de dispositivos móveis de propriedade do usuário somente será permitido nos sistemas ou serviços homologados e/ou autorizados pela ASSIN.

Parágrafo único. A utilização de dispositivos móveis, notebooks e outros equipamentos de propriedade do usuário nas redes da AGENERSA deverá ser previamente autorizada pela ASSIN, mediante solicitação da chefia imediata do usuário, justificando a necessidade do serviço.

Art. 42 - O ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem possibilitar que todas as garantias legais atribuídas à AGENERSA sejam respeitadas.

TÍTULO VI
DAS RESPONSABILIDADES

CAPÍTULO I
GESTOR DE SEGURANÇA DA INFORMAÇÃO

Art. 43 - O Gestor de Segurança da Informação será designado pelo Presidente da AGENERSA dentre os servidores públicos civis ou militares ocupantes de cargos efetivos ou comissionados, desde que lotados nesta Autarquia e com formação ou capacitação técnica compatível às suas atribuições, e terá as seguintes competências:

I - promover a cultura de segurança da informação;

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de SI executadas;
III - propor à autoridade máxima da AGENERSA os recursos necessários às ações de SI executadas;
IV - acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SI; V - propor normas e procedimentos relativos à SI.
VI - elaborar e atualizar periodicamente os procedimentos de segurança da informação do órgão/entidade que seja responsável.
VII - implementar e monitorar permanentemente os mecanismos e procedimentos relacionados à segurança da informação, com o intuito de preservar a integridade, a confidencialidade e a privacidade dos dados sob a guarda e responsabilidade dos órgãos e entidades;

VIII - compartilhar com os demais órgãos e entidades da Administração Pública Estadual, os eventos de segurança, após ocorrência, para fins de prevenção, bem como as eventuais soluções, para fins de replicação de conhecimentos e experiências;
IX - indicar o responsável pelo tratamento de resposta a incidentes no âmbito de atuação do órgão ou entidade elaborador.

Parágrafo único. A promoção de cultura da SI a que se refere este artigo será atendida mediante campanhas de conscientização, palestras e treinamentos, assim como interlocução permanente com a Presidência para garantir que os agentes públicos tomem conhecimento da POSIC e assinem o Termo de Confidencialidade, constante do Anexo II, no ato da admissão.

CAPÍTULO II
RESPONSÁVEL PELO TRATAMENTO E RESPOSTA A INCIDENTES

Art. 44 - O Responsável pelo Tratamento e Resposta a Incidentes será indicado pelo Gestor de Segurança da Informação dentre os servidores públicos civis ou militares ocupantes de cargos efetivos ou comissionados, desde que lotados no órgão ou entidade

e com formação ou capacitação técnica compatível às suas atribuições e nomeado pelo Presidente da AGENERSA e a ele compete:

I - monitorar os recursos de TIC, detectar e realizar as análises dos incidentes de segurança da informação;
II - reportar ao Encarregado pelo Tratamento de Dados Pessoais os incidentes envolvendo tais dados;
III - identificar vulnerabilidades;
IV - receber e propor respostas a notificações relacionadas a incidentes de segurança da informação; e
V - coordenar e executar atividades de tratamento e resposta a eventos de segurança da informação.

CAPÍTULO III
ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

Art. 45 - O Encarregado pelo Tratamento de Dados Pessoais será nomeado pelo Presidente da AGENERSA e ele compete:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II - receber comunicações da Autoridade Nacional de Proteção de Dados - ANPD e adotar providências;
III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares;
V - requerer relatório das áreas responsáveis por tratamento de dados pessoais no âmbito dos órgãos administrativos contendo, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das

informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados;

VI - atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), na forma da Lei nº 13.709/2018.

CAPÍTULO IV
RESPONSABILIDADES DO USUÁRIO

Art. 46 - Aos usuários compete:

I- utilizar os recursos de TIC da AGENERSA exclusivamente para atividades relacionadas com suas atribuições funcionais;
II- responsabilizar-se pelas informações armazenadas na estação de trabalho e nos demais dispositivos móveis que utilizar para desempenho de suas funções; e
III- armazenar informações estritamente corporativas no servidor de arquivos disponibilizados para sua unidade de lotação, respeitando o processo de controle de acesso regulamentado pela ASSIN.
IV- não armazenar informações que não sejam estritamente corporativas no servidor de arquivos disponibilizado para sua unidade de lotação, respeitando o processo de controle de acesso regulamentado pela ASSIN.
V- assinar o Termo de Confidencialidade, constante do Anexo II, sobretudo para as concessões de primeiro acesso.

TÍTULO VII
PENALIDADES

Art. 47 - O descumprimento de um ou mais itens da POSIC sujeita ao infrator a aplicação de sanções administrativas, penais ou civis previstas na legislação vigente.

Art. 48 - Sempre que instada, a AGENERSA deverá cooperar ativamente com as autoridades competentes na apuração de possível prática de atividade ilícita realizada por meio dos seus recursos computacionais ou por usuário desta Agência.

Art. 49 - O usuário que tomar ciência de qualquer violação desta POSIC deverá comunicá-la à ASSIN, que será a responsável pela análise preliminar da infração, pelas medidas de restrição de acesso cabíveis e pelo eventual encaminhamento aos órgãos de apuração competentes.

TÍTULO VIII
DISPOSIÇÕES FINAIS

Art. 50 - Os contratos de prestação de serviços e demais ajustes celebrados pela AGENERSA deverão dispor de cláusula específica sobre a obrigatoriedade do cumprimento da presente Instrução Normativa, bem como das penalidades decorrentes da sua inobservância.

Art. 51 - Cabe aos fiscais de contratos, independente de aditamento, e à Assessoria de Recursos Humanos:

I- informar à ASSIN por meio do sistema de Chamados GLPI http://atendeagenersa/glpi ou por processo administrativo no sistema SEI (Sistema Eletrônico de Informações), imediatamente, sobre desligamentos e/ou substituições de colaboradores para fins de revogação de permissões de acesso e bloqueio de contas de e-mails.

II- no encerramento dos contratos, informar à ASSIN, imediatamente, sobre desligamentos e/ou substituições de colaboradores para fins de revogação de permissões de acesso e bloqueio de contas de e-mails.

Art. 52 - A Política de Segurança da Informação deverá ser revisada sempre que se fizer necessário, não excedendo o período máximo de 3 (três) anos.

ANEXO II
TERMO DE CONFIDENCIALIDADE

Nome:
Setor:
Cargo/ Função / Vínculo:
CPF:
Data:

Cláusula 1ª - Declaro ter conhecimento da Política de Segurança da Informação (POSIC) adotada pela AGENERSA para utilização dos bens e recursos de tecnologia da informação e comunicação (TIC) e me comprometo ao seu fiel cumprimento e observância.

Cláusula 2ª – Responsabilizo-me pelo correto uso dos recursos de TIC da AGENERSA, comprometendo-me a utilizá-los somente para fins institucionais, cumprindo as determinações e recomendações contidas na POSIC e normativos vigentes.

Cláusula 3ª – Comprometo-me a manter sigilo absoluto sobre os sistemas e informações a mim confiados, bem como aos que venha ter conhecimento em função da execução de atividades desenvolvidas para atendimento dos objetivos da instituição.

Cláusula 4ª – Estou ciente e concordo que a utilização do e-mail institucional, da internet e demais acessos devem ocorrer em consonância com o disposto na POSIC e normativas vigentes.

Cláusula 5ª – Estou ciente de que a AGENERSA pode monitorar o uso das informações e recursos de TIC, conforme previsto na POSIC e em suas normas complementares, sem prejuízo das ações preventivas, corretivas ou disciplinares que possam ser tomadas.

Cláusula 6ª – Estou ciente de que as senhas de acesso aos sistemas e a ambientes físicos têm caráter confidencial, pessoal e intransferível, sendo minha responsabilidade zelar pelo seu sigilo.

Cláusula 7ª – Declaro, finalmente, que tenho pleno conhecimento de que todas as minhas ações no ambiente da TIC da AGENERSA podem ser registradas, ciente de que o uso indevido ou fraudulento das informações e dos recursos ensejará apuração de responsabilidade, nos termos da legislação vigente.

ANEXO III
Tabela 1: Categoria de Acesso Bloqueados

Categorias Bloqueadas	Conteúdos Bloqueados
Potencialmente ofensivos	Drogas ilícitas
	Hacking
	Ilegal ou anti-ético
	Racismo e ódio
	Violência
	Burla de proxy
	Spyware
	Malware
	Phishing
	Abuso de crianças
Controversos	Material Adulto
	Apostas
	Grupos extremistas
	Nudez
	Pornografia
Potencialmente não produtivos	Jogos
	Streaming
	Bate-papo (chat)
	Rádio e TV pela internet
Potencial de violação de segurança	Compartilhamento peer-to-peer
	Rede Social, relacionamento pessoal
Outros	Sem classificação