AGENERSA
Agência Reguladora de Energia e Saneamento Básico do Estado do Rio de Janeiro

NORMAS DE UTILIZAÇÃO DOS COMPUTADORES E RECURSOS TECNOLÓGICOS

1- Objetivo

Estabelecer responsabilidades e requisitos básicos de utilização dos computadores e recursos tecnológicos no ambiente da AGENERSA.

2- Documentos de referência

Diretrizes Gerais de Segurança da Informação da AGENERSA.

3- Abrangência

Esta norma deverá ser aplicada a todos os usuários que utilizam os recursos de Tecnologia da Informação da AGENERSA para acesso à computadores e recursos tecnológicos.

4- Conceito

Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os usuários devem estar cientes, portanto, da peculiaridade da navegação na Internet, antes de acessá-la e antes de utilizar os seus recursos.

Considerando que o uso da Internet, no âmbito da AGENERSA, é uma concessão e não um direito, é de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada desse importante recurso tecnológico. Todos os usuários dos ativos de informação de propriedade ou sob controle da AGENERSA, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse da agência, mantendo uma conduta profissional, especialmente em se tratando da utilização de bem público.

O computador e a Internet são ferramentas de trabalho fornecidas pela AGENERSA, exclusivamente para este propósito.

5- Normas para utilização dos computadores e recursos tecnológicos

I. 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.

II. 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, ou de quem este determinar.

III. 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.

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

V. 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/

VI. A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

VII. Arquivos pessoais e/ou não pertinentes ao negócio do AGENERSA (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

VIII. Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

IX. Qualquer mudança de local físico do usuário, será utilizada a máquina disponível, em havendo, no novo local, estando vedada a mudança de local de máquina a fim de evitar incidentes com máquinas e periféricos.

X. Todos os computadores de uso individual deverão ter senha de Bios, lacres na cpu e desabilitado o boot através de cdrom e/ou usb, para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela Gerência da Assessoria de Informática, que terá acesso a elas para manutenção dos equipamentos.

XI. Os colaboradores devem informar ao departamento de suporte técnico qualquer identificação de dispositivo estranho conectado ao seu computador.

XII. É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da Assessoria de Informática da AGENERSA ou por terceiros devidamente contratados para o serviço.

XIII. É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

XIV. O colaborador deverá manter a configuração do equipamento disponibilizado pela AGENERSA, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.

XV. Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

XVI. A aquisição e/ou doação de novos equipamentos de informática (impressoras, computadores e periféricos) para AGENERSA, deverão ser avaliadas e seguidas rigorosamente às especificações padronizadas pela Assessoria de Informática.

XVII. Todos os recursos tecnológicos adquiridos pela AGENERSA devem ter imediatamente suas senhas padrões (default) alteradas.

XVIII. Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

XIX. É vedado tentar ou obter acesso não autorizado a outro computador, servidor ou rede.

XX. É vedado burlar quaisquer sistemas de segurança.

XXI. É vedado acessar informações confidenciais sem explícita autorização do proprietário, e/ou vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).

XXII. É vedado interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

NORMAS DE CONTAS E SENHAS PARA USUÁRIOS

1- Objetivo

Estabelecer os procedimentos adequados para a correta utilização das contas de usuários no ambiente de Tecnologia da Informação e Comunicação da AGENERSA.

2- Documentos de referência

Diretrizes Gerais de Segurança da Informação da AGENERSA.

Catálogo de Serviços da AGENERSA.

3- Abrangência

Esta Norma deverá ser aplicada a todos os usuários que possuam contas de acesso (sem privilégios de “administrador”) aos ativos do tipo estações de trabalho e servidores do ambiente de Tecnologia da Informação da AGENERSA.

4- Conceito

Segundo a nova norma ABNT NBR ISO/IEC 17799:2005, item 11.2, é importante que procedimentos formais sejam implementados para controlar a distribuição de direitos de acesso a sistemas de informação e serviços. Convém ainda que, a concessão e o uso de privilégios sejam restritos e controlados (item 11.2.2) e que a concessão de senhas seja controlada através de um processo de gerenciamento formal (item 11.2.3). Diante disso, a AGENERSA elaborou esta norma de contas e senhas para usuários, de forma a evitar o uso inapropriado de senhas, que pode vir a

ser um grande fator de contribuição para falhas ou violações de sistemas.

5- Formação de Contas e Senhas

As senhas de acesso a rede, para usuários finais, deverão conter no mínimo 6 (seis) caracteres, sendo obrigatório o uso de letras maiúsculas, minúsculas e números. Como recomendação sugere-se a utilização de caracteres especiais (“$”, “%”, “&”,...).

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).

6- Distribuição de Acessos e Senhas

6.1- Senhas de rede, *e-mail:*

As contas de rede (*login*) e correio eletrônico (*e-mail*) serão solicitadas pela Assessoria de Recursos Humanos através do sistema de Chamados GLPI, ou via SEI no momento da admissão/nomeação do usuário.

7- Bloqueio de senhas

A conta deverá ser bloqueada após a 3ª (Terceira) tentativa frustrada de *login*.

Contas que ficarem inativas por mais de 90 (noventa) dias serão bloqueadas.

8- Reativação de contas

As contas só poderão ser reativadas por solicitação formal da chefia direta através da ferramenta de Solicitação de Chamados GLPI, no endereço http://atendeagenersa/glpi/

Caso o usuário suspeite do comprometimento de sua senha, esta deverá ser modificada imediatamente.

9- Disposições Gerais

A senha é pessoal e intransferível, devendo ser mantida em sigilo. O usuário será responsabilizado pelo mau uso da mesma, conforme previsto na legislação.

Para o novo usuário ou para aquele que esteja retornando após desligamento ou remanejamento, a Assessoria de Recursos Humanos - ASRHU/AGENERSA deverá solicitar a concessão de acesso mínimo necessário, para que este exerça suas tarefas (exemplo: login de acesso).

Deve-se atribuir o menor privilégio possível a uma conta, que deverá permitir apenas a realização das tarefas pertinentes ao seu usuário.

Os usuários finais não poderão ter contas com perfil de administrador, nem contas do

domínio com privilégio de administrador local da estação.

Os acessos e as falhas nas tentativas de *logon* deverão ser auditados.

A eventual necessidade de instalação de *softwares* deve ser solicitada via serviço GLPI, no endereço http://atendeagenersa/glpi/ da à Assessoria de Informática, de forma que haja um controle centralizado de *softwares* e licenças disponíveis para a AGENERSA.

NORMAS DE UTILIZAÇÃO DA INTERNET

1- Objetivo

Estabelecer responsabilidades e requisitos básicos de utilização da Internet no ambiente de Tecnologia da Informação da AGENERSA.

2- Documentos de referência

Diretrizes Gerais de Segurança da Informação da AGENERSA.

3- Abrangência

Esta norma deverá ser aplicada a todos os usuários que utilizam os recursos de Tecnologia da Informação da AGENERSA para acesso à Internet.

4- Conceito

Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os usuários devem estar cientes, portanto, da peculiaridade da navegação na Internet, antes de acessá-la e antes de utilizar os seus recursos.

Considerando que o uso da Internet, no âmbito da AGENERSA, é uma concessão e não um direito, é de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada desse importante recurso tecnológico.

Todos os usuários dos ativos de informação de propriedade ou sob controle da AGENERSA, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse da Agência, mantendo uma conduta profissional, especialmente em se tratando da utilização de bem público.

5- Normas para utilização da Internet

I. A AGENERSA possui mecanismos de autenticação, que determinam a titularidade de todos os acessos à Internet feitos por seus usuários;

II. É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações sigilosas em listas de discussão ou bate-papo;

III. Usuários com acesso à Internet não podem efetuar carga (*upload)* de qualquer *software*

licenciado à AGENERSA ou de dados de propriedade da AGENERSA sem a autorização expressa da chefia ou do responsável pelo *software/dado*;

IV. Os usuários poderão carregar ou copiar (fazer *download)* arquivos da Internet que sejam necessários ao desempenho de suas atividades, desde que observado os termos de licença de uso e registro desses programas;

V. A Internet deve ser utilizada exclusivamente para atividades ligadas ao trabalho da Agência;

VI. O usuário deve utilizar a Internet de forma adequada e diligente;

VII. O usuário deve utilizar a Internet observando os preceitos legais, a moral, os bons costumes e a ordem pública;

VIII. O usuário deve se abster de utilizar a internet com objetivos ou como meio para a prática de atos ilícitos, proibidos por lei ou pela presente norma, lesivos aos direitos e interesses da Agência ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (*hardware e software*), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros;

IX. O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de sua senha de acesso;

X. É vedada a utilização de "*modem*" ou outra conexão de rede que não seja autorizada pela ASSINF/AGENERSA, em máquinas que estejam conectadas ao ambiente da rede da AGENERSA;

XI. Os usuários que desejarem utilizar outras conexões, além daquelas já estabelecidas, deverão obrigatoriamente informar à assessoria de Informática ASSINF/AGENERSA, de forma a não comprometer a segurança da rede da AGENERSA.

XII. Não é permitida a utilização de *software* de conexão ponto-a-ponto (*peer-to-peer* ou P2P), tais como *Emule, Torrents* e afins;

XIII. Não é permitido o acesso à redes sociais, tais como *Facebook, Instagram, Twitter* e afins;

XIV. Não é permitido acesso a sites de *Proxy*;

XV. A AGENERSA monitora e bloqueia automaticamente sites de pornografia, pedofilia e outros contrários à lei. O acesso a esses sites é terminantemente proibido, mesmo que os mesmos não estejam sendo bloqueados no sistema de segurança;

XVI. Será de responsabilidade de cada usuário zelar pelo fiel cumprimento ao estabelecido na presente norma;

XVII. A não observância de qualquer item acima implicará em sanções previstas nesta norma.

Observações: Devido o bloqueio de sites ser efetuado por um sistema automatizado, algumas páginas poderão ser bloqueadas indevidamente. Caso isto ocorra, o chefe da unidade deverá solicitar o desbloqueio do site desejado através da ferramenta de Solicitação de Chamados GLPI no endereço http://atendeagenersa/glpi, bastando preencher a solicitação descrevendo a URL bloqueada e o motivo que justifique o seu desbloqueio.

6- Sanções

De acordo com as Diretrizes Gerais de Segurança da Informação da AGENERSA, esta se reserva o direito de monitorar o tráfego efetuado através das suas redes de comunicação, incluindo o acesso à Internet.

A monitoração do cumprimento das normas de utilização da Internet dar-se-á da seguinte forma:

I. Técnicos da Assessoria de Informática - ASSINF/AGENERSA identificarão os usuários - doravante chamados de infratores - que violarem qualquer item desta norma de segurança.

II. Na primeira transgressão, esses infratores serão notificados, via *e-mail*, do descumprimento das normas estabelecidas neste documento.

Caso na infração cometida esteja caracterizado qualquer tipo de crime (acesso a sites de pedofilia, racismo e etc.), aplicar-se-á a sanção especial desta norma.

III. Caso haja uma segunda transgressão da norma, esses infratores serão novamente notificados, via *e-mail*, sendo que uma cópia da notificação será enviada ao titular da unidade e o seu superior hierárquico.

IV. Na terceira transgressão, serão aplicadas as sanções administrativas previstas nas Diretrizes Gerais de Segurança da Informação da AGENERSA.

7- Sanção especial

É terminantemente proibido qualquer acesso a sites que apresentarem conteúdo de pedofilia, racismo ou qualquer outro assunto contrário à lei que, eventualmente, não esteja bloqueado no sistema de proteção da AGENERSA,. A violação deste item implica em abertura de inquérito policial na Delegacia de Repressão a Crimes de Informática do Estado do Rio de Janeiro – DRCI.

NORMAS DE UTILIZAÇÃO DE *E-MAIL*

1- Objetivo

Estabelecer responsabilidades e requisitos básicos de uso dos serviços de Correio Eletrônico, no ambiente de Tecnologia da Informação e Comunicação da AGENERSA.

2- Documentos de referência

Diretrizes Gerais de Segurança da Informação da AGENERSA.

3- Abrangência

Esta Norma deverá ser aplicada aos ativos de informação e comunicação da AGENERSA.

4- Conceito

Prover a comunicação é, sem dúvida, a essência das redes. As pessoas sempre procuraram se corresponder da maneira mais rápida e fácil possível. O Correio Eletrônico (*e*-mail) é a aplicação que mais ilustra esta procura, pois reúne, entre outros, estes atributos. Entretanto, a facilidade de Correio Eletrônico fornecido pela AGENERSA deve ser usada no interesse do serviço.

Considerando que o uso dos serviços de Correio Eletrônico, no âmbito da AGENERSA, é uma concessão e não um direito, é de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada desse importante recurso tecnológico.

Todos os usuários dos ativos de informação de propriedade ou sob controle da AGENERSA, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse da Agência, mantendo uma conduta profissional, especialmente em se tratando da utilização do bem público.

5- Acesso ao Correio Eletrônico

Todas as contas de Correio Eletrônico terão uma titularidade, determinando a responsabilidade sobre a sua utilização.

Os usuários da AGENERSA poderão ser titulares de uma única caixa postal individual no Servidor de Correio Eletrônico, com direitos a envio/recebimento de mensagens, via Internet, e enquanto perdurar o seu vínculo com a AGENERSA.

Contas com inatividade por um período igual ou superior a 90 (noventa) dias serão bloqueadas, a fim de evitar o recebimento de novas mensagens.

Regras para utilização do Correio Eletrônico (*E-mail*)

O usuário é o responsável direto pelas mensagens enviadas por intermédio do seu endereço de Correio Eletrônico.

O usuário deve utilizar o Correio Eletrônico de forma adequada e diligente; É vedada a utilização do Correio Eletrônico, nas situações abaixo:

I. Envio de mensagens não autorizadas, divulgando informações sigilosas e/ou de propriedade da AGENERSA;

II. Acesso não autorizado à caixa postal de outro usuário;

III. Acesso não autorizado ao Banco de Dados do Correio Eletrônico de outro órgão;

IV. Uso de contas particulares dos usuários, através dos serviços *Post Office Protocol* -POP, *Internet Message Access Protocol* -IMAP e *Simple Mail Transfer Protocol* -SMTP de provedores não pertinentes ao domínio agenersa.rj.gov.br;

V. Envio, armazenamento e manuseio de material que contrarie o disposto na legislação vigente, a moral e os bons costumes e a ordem pública;

VI. Envio, armazenamento e manuseio de material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos por lei ou pela presente norma, lesivos aos direitos e interesses da Agência ou de terceiros, ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (*hardware* e *software*), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;

VII. Envio, armazenamento e manuseio de material que caracterize promoção, divulgação ou incentivo a ameaças, difamação ou assédio a outras pessoas; assuntos de caráter obsceno; prática de qualquer tipo de discriminação relativa a raça, sexo ou credo religioso; distribuição de qualquer material que caracterize violação de direito autoral garantido por lei; uso para atividades com fins comerciais e o uso extensivo para assuntos pessoais ou privados;

VIII. Envio de mensagens do tipo “corrente” e “*spam*”;

IX. Envio intencional de mensagens que contenham vírus eletrônico ou qualquer forma de rotinas de programação de computador, prejudiciais ou danosas;

X. Envio de mensagens que contenham arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf, .msi) ou qualquer outra extensão represente um risco à segurança de acordo com os critérios estabelecidos pela Assessoria de Informatica – ASSINF/AGENERSA;

XI. Utilização de listas e/ou caderno de endereços da AGENERSA para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão do responsável pelas listas e/ou caderno de endereços em questão;

XII. Todo e qualquer procedimento de uso do Correio Eletrônico não previsto nesta Política, que possa afetar de forma negativa a AGENERSA.

6- Cadastramento e Exclusão

A Assessoria de informática ASSIN/AGENERSA é responsável pela inclusão, exclusão e alteração dos usuários de correio eletrônico da AGENERSA. Esta tarefa será realizada de acordo com o procedimento definido na Política de Segurança da Informação da AGENERSA.

7- Disposições finais

A AGENERSA se reserva o direito de verificar, sempre que julgar necessário, a obediência às normas/procedimentos citados neste documento.

As mensagens eletrônicas trafegam de forma aberta na Internet, passíveis de visualização. Para evitar que pessoas não autorizadas possam ter acesso a essas mensagens, a AGENERSA faz uso de técnicas e ferramentas de criptografia.

O uso indevido dos serviços de correio eletrônico, tratados neste documento, é passível de sanção disciplinar, de acordo com a legislação vigente e demais normas aplicadas à matéria.

Será de responsabilidade de cada usuário zelar pelo fiel cumprimento ao estabelecido na presente resolução.

NORMAS DE UTILIZAÇÃO DA VPN

1- Objetivo

Prover as diretrizes gerais para o uso apropriado de conexões VPN (Virtual Private Network), para acesso à rede computacional da AGENERSA, visando o bom desempenho do serviço e a segurança da informação no que tange aos aspectos de confidencialidade e integridade.

A VPN (Virtual Private Network) é uma rede privada virtual que permite ao usuário receber um número IP da rede da AGENERSA em seu equipamento remoto. Dessa forma, mesmo não estando nas dependências da AGENERSA, o equipamento estará na rede da AGENERSA. O acesso via VPN utiliza encriptação de dados para a comunicação entre o equipamento remoto e a rede local da AGENERSA.

2. Documentos de referência

Diretrizes Gerais de Segurança da Informação da AGENERSA.

3. Abrangência

Esta Norma deverá ser aplicada aos ativos de informação e comunicação da AGENERSA.

E a todos os funcionários e terceirizados, na utilização da VPN e que estejam devidamente autorizados e cadastrados na base de contas institucionais gerenciadas pela ASSIN/ AGENERSA.

4. Acessos via VPN

A conexão via VPN ao ambiente computacional instalado na AGENERSA é provido pelo PRODERJ mediante solicitação da ASSIN/AGENERSA, por meio de uma conta de usuário, com vínculo institucional atualizado.

4.1 Os usuários autorizados a usar a VPN são:

Servidores e terceirizados, que comprovem a necessidade do seu uso.

5. Responsabilidades

I. Garantir a veracidade e exatidão dos dados pessoais fornecidos para o cadastro.

II. Ser responsável pelo seu acesso à internet, por qualquer instalação de software necessário ou por qualquer valor associado à isto.

III. Assegurar que outras pessoas não autorizadas tenham acesso permitido às redes internas da AGENERSA através de sua conta para utilização da VPN.

IV. Todos os computadores conectados às redes internas da AGENERSA via VPN devem estar com as versões mais atualizadas de softwares antivírus, e com os últimos "patches" de segurança instalados.

V. Estabelecer somente uma única conexão VPN com a rede da AGENERSA.

VI. Utilizar equipamentos com sistemas operacionais compatíveis com a infraestrutura de computação da AGENERSA.

VII. Não alterar, sem prévio consentimento, a configuração default da VPN fornecida pela Assessoria de informática, ASSIN/ AGENERSA.

VIII. Aceitar que os equipamentos pessoais para acesso à VPN passam a ser uma extensão da rede da AGENERSA e como tal, estão sujeitas às mesmas regras, políticas e regulamentações que se aplicam aos equipamentos de propriedade da AGENERSA, ou seja, suas máquinas devem ser configuradas para atender às normas da instituição.

IX. Não utilizar programas "peer-to-peer" sobre VPN.

X. Não utilizar o acesso VPN para transferência de grandes volumes de dados.

6. Disposições finais

A AGENERSA se reserva o direito de verificar, sempre que julgar necessário, a obediência às normas/procedimentos citados neste documento.

O uso indevido dos serviços de VPN, tratados neste documento, é passível de sanção disciplinar, de acordo com a legislação vigente e demais normas aplicadas à matéria.

Será de responsabilidade de cada usuário zelar pelo fiel cumprimento ao estabelecido na presente Resolução.

AGENERSA
Agência Reguladora de Energia e Saneamento Básico do Estado do Rio de Janeiro

NORMAS PARA GESTÃO DE ATIVOS

1- Objetivo

Alcançar e manter a proteção adequada dos ativos do ambiente de Tecnologia da Informação da AGENERSA, definindo as responsabilidades dos proprietários e custodiantes de cada ativo tecnológico.

2- Documentos de referência

Diretrizes gerais de Segurança da Informação da AGENERSA.

3- Abrangência

Esta Norma deverá ser aplicada a todos os usuários que sejam proprietários e/ou custodiantes dos ativos tecnológicos da AGENERSA. Ela também se aplica a qualquer usuário que de alguma forma interaja com esses ativos.

4- Conceitos

Segundo a nova norma ABNT NBR ISO/IEC 17799:2005, item 7.1, é importante que todos os ativos sejam inventariados e tenham um proprietário responsável. É importante ainda que os proprietários dos ativos sejam identificados e a eles seja atribuída a responsabilidade pela manutenção apropriada dos controles. A implementação de controles específicos pode ser delegada pelo proprietário, conforme apropriado. Porém, o proprietário permanece responsável pela proteção adequada dos ativos.

Ademais, de acordo com o item 7.1.1 da mesma norma, é importante que todos os ativos sejam claramente identificados e um inventário de todos os ativos importantes seja estruturado e mantido. Diante disso, a AGENERSA elaborou esta Norma de gestão de ativos, de forma a definir claramente quais as responsabilidades que os gestores da AGENERSA terão ao serem designados como proprietário e/ou custodiante de algum ativo.

5- Responsabilidades Garantir que sistema operacional e aplicativos estejam sujeitos a rígido controle de gestão de mudanças;

XI. Criar e implantar os procedimentos para a geração de cópias de segurança – *backup* – e sua recuperação – *restore* – em um tempo aceitável;

XII. Garantir que registros (log) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso;

XIII. Estar ciente de que a não observância a estas normas sujeita-o às sanções previstas no item XVI das Diretrizes Gerais de Segurança da Informação.

5.2- Custodiante

Todo ativo tecnológico do tipo servidor instalado no CPD (Central de Processamento de Dados) terá designado um custodiante, que será responsável por:

I. Ajudar o gestor da Assessoria de informática a manter as informações cadastrais sobre o ativo atualizadas – *hardware, software* e serviços disponibilizados através daquele ativo;

II. Atuar como suporte nível 2, conforme item 6 (seis) deste documento;

III. Cuidar do ativo no dia-a-dia, notificando ao gestor qualquer anomalia encontrada;

IV. Comunicar imediatamente ao gestor qualquer problema de segurança lógica do ativo – invasões de *hackers*, pichação de *sites,* as ações que foram tomadas para sanar/minimizar o problema e problemas na aplicação e etc;

V. Comunicar imediatamente, por escrito, qualquer incidência de dano, furto ou roubo dos equipamentos sob sua custódia;

VI. Atualizar, a pedido do gestor, os programas (*software)* de qualquer natureza que rodem no ativo, desde atualizações (*upgrade)* de versão à aplicação de correções (*patches*);

Observação: Toda a documentação necessária para realizar as atualizações deverá ter sido previamente fornecida pelo gestor.

VII. Realizar as modificações necessárias nos ativos, de acordo com o planejamento de gestão de mudanças definido pelo proprietário;

VIII. Garantir que as cópias de segurança – *backup* estão sendo geradas;

IX. Monitorar os registros (*log*) de auditoria, avisando imediatamente ao gestor qualquer problema encontrado;

X. Evitar o acesso aos ativos por pessoas não autorizadas ao serviço de sua área;

XI. Estar ciente de que a instalação de *software* de qualquer natureza ou a modificação de qualquer configuração sem a autorização por escrito do proprietário do ativo não é permitida. Para casos de suporte no ativo, esta cláusula não é válida.

XII. Coibir qualquer modificação nos equipamentos e/ou *softwares*, por quem quer que seja, exceto quando autorizada por escrito, pelo proprietário do ativo;

6- Estar ciente de que a não observância a estas normas sujeita-o às sanções previstas no item XVI das Diretrizes Gerais de Segurança da Informação.

6.1 - Foram definidos 3 (três) níveis de suporte para os ativos dos tipos servidor

instalados no CPD (Central de Processamento de Dados), a saber:

Nível de suporte	Responsável	Atividades
Suporte 1º nível	Coordenação de Sistema Operacional e Coordenação de Produção	Testes de conectividade – Exemplo: *ping*, *traceroute* e similares; Monitoramento de serviços – *up*/*down*. Aviso ao custodiante e/ou proprietário em caso de falha no ativo. "Reboot" após autorização por escrito do proprietário outros – a serem acordadas entre os envolvidos.
Suporte 2º nível	Custodiante do ativo	Realizar todas as atividades definidas no item 5.2. Quando na impossibilidade de resolução do problema, notificar imediatamente o suporte de 3º nível.
Suporte 3º nível	Proprietário do ativo	Realizar todas as atividades definidas no item 5.1. Quando na impossibilidade de resolução do problema, este será responsável em acionar suporte externo.

NORMAS DE CONTAS E SENHAS PARA ADMINISTRADORES

1- Objetivo

Estabelecer os procedimentos adequados para a correta utilização das contas com privilégios de "administrador" das estações de trabalho e servidores do ambiente de Tecnologia da Informação da AGENERSA.

2- Documentos de referência

Diretrizes Gerais de Segurança da Informação da AGENERSA.

3- Abrangência

Esta Norma deverá ser aplicada a todos os usuários que possuam contas com privilégios de "administrador" nos ativos do tipo estações de trabalho e servidores do ambiente da AGENERSA.

4- Conceito

Segundo a nova norma ABNT NBR ISO/IEC 17799:2005, item 11.2, é importante que procedimentos formais sejam implementados para controlar a distribuição de direitos de acesso a sistemas de informação e serviços. Convém ainda que a concessão e o uso de privilégios sejam restritos e controlados (item 11.2.2) e que a concessão de senhas seja controlada através de um processo de gerenciamento formal (item 11.2.3). Diante disso, a AGENERSA elaborou esta

norma de contas e senhas para administradores, de forma a evitar o uso inapropriado de privilégios de administrador de sistemas, que pode vir a ser um grande fator de contribuição para falhas ou violações de sistemas.

5- Usuários com privilégios de administrador

Os ativos do tipo estação de trabalho, de propriedade da AGENERSA, instalados na Secretaria ou em qualquer outra unidade administrada direta ou indiretamente terão as seguintes regras para as senhas com privilégios de administrador:

I. Somente os funcionários da TI que comprovem a necessidade de trabalho, serão autorizados a receber contas com privilégios de administrador local.

6- Formação de Contas e Senhas

As senhas para administradores deverão ser fortes e conter no mínimo 8 caracteres, sendo obrigatório o uso de letras maiúsculas, minúsculas e caracteres numéricos e especiais (“$”, “%”, “&”,...). Para aqueles ambientes que não suportarem o mínimo de 8 caracteres, deverão ser utilizados o limite máximo que o ambiente permitir.

Deverão ser evitadas as composições de senhas com seqüências numéricas (123...) e/ou alfabéticas (abc...), além de senhas de fácil dedução (nome da máquina, nome do usuário, data de nascimento...).

7- Tempo de vida de contas e senhas

A conta deverá ser bloqueada após a 3ª (terceira) tentativa de *login*.

8- Reinicialização de senhas

Caso haja suspeita do comprometimento de uma senha, esta deverá ser reinicializada.

Disposições Gerais

A senha deverá ser mantida em sigilo pelo administrador durante o período de uso. O administrador será responsabilizado, conforme previsto na legislação, pelo mau uso da mesma.

SISTEMAS DE INFORMAÇÃO

1- **Objetivo**

Estabelecer os conceitos e diretrizes de segurança da informação, visando proteger as informações da AGENERSA e de seus usuários. Posiciona-se como documento estratégico, com vistas a promover o uso seguro dos ativos de informação da AGENERSA. Assim, deve ser entendida como uma declaração formal da Alta Administração acerca de seu compromisso com a proteção das informações sob sua custódia, a ser cumprida por todos os colaboradores, estagiários e colaboradores terceirizados da AGENERSA.

2- **Pilares da segurança da informação**

A segurança da informação é aqui caracterizada pela preservação dos seguintes pilares:

Confidencialidade: A Assessoria de Informática visa garantir que o acesso às informações do órgão e de seus usuários sejam obtidos somente por pessoas autorizadas e quando o acesso de fato for necessário;

Integridade: A Assessoria de Informática visa garantir a exatidão e a completude das informações e dos métodos de seu processamento, bem como a integridade dos dados de usuários que estejam sob sua responsabilidade.

Disponibilidade: A Assessoria de Informática visa garantir que a informação esteja sempre disponível aos profissionais que de fato possuam o acesso necessário para tal e assegure que os dados estejam disponíveis de acordo com suas regras de confidencialidade.

Rastreabilidade: A Assessoria de Informática visa garantir a disponibilidade de trilhas de auditoria de informações e meios de processamento, através de registros das transações e alterações realizadas em seus sistemas e aplicações.

3- **Permissão de acesso**

Os acessos devem sempre obedecer ao critério de menor privilégio, no qual os usuários devem possuir somente as permissões necessárias para a execução de suas atividades;

4- **Distribuição de conta de usuário**

Devem ser seguidas as **NORMAS DE CONTAS E SENHAS PARA USUÁRIOS**.

5- **Disponibilização de software**

Todos os softwares em execução na AGENERSA devem estar devidamente documentados e registrados na Assessoria de Informática e só devem ser disponibilizados para utilização após análise e cumprimento das exigências.

DESENVOLVIMENTO DE SOFTWARE

Cabe à Assessoria de Informática:

O desenvolvimento de software seguindo o alinhamento estratégico, a gestão de projetos, produção colaborativa, gestão da contratação, arquitetura de software, gestão de segurança e gestão de sustentação.

Cabe ao setor interessado:

Solicitar à Assessoria de Informática a análise e parecer para um projeto de desenvolvimento de software ou aquisição. Para os casos de parceiras ou convênios de

desenvolvimento de soluções com outras instituições, o setor interessado deverá consultar a Assessoria de Informática sobre a viabilidade de continuidade do projeto para que as informações referentes ao desenvolvimento e sustentação como, arquitetura de software e modelo de dados sejam repassados.

Esta política tem o objetivo de mitigar o desenvolvimento de softwares que inviabilizem sua manutenção e evolução pela da Assessoria de Informática.

UNIDADES EXTERNAS

Cabe a unidade externa de administração direta ou indireta:

I. Realizar o envio da cópia total do banco de dados dos *softwares* que operacionalizam a unidade no início e no fim da gestão de forma segura e integra para a Assessoria de Informática, a fim de preservar os dados ou realização de análise de dados;

II. Solicitar o parecer da Assessoria de Informática para a aquisição de um novo *software* ou substituição de um preexistente;

III. Realizar a migração dos dados do *software* quando houver a substituição do mesmo;

IV. Disponibilizar os acessos às bases de dados de produção ou realizar o envio dos dados solicitados após pedido oficial da Assessoria de Informática;

V. A gestão vigente da unidade é responsável por manter e preservar os dados em segurança, bem como o dever de responder sobre o dado quando solicitado de forma oficial pela Assessoria de Informática ou por um órgão de controle estadual.

TERMOS E DEFINIÇÕES

I. **Administrador** – contas que permitem acesso total e irrestrito a quaisquer recursos do sistema em que estão configuradas.

II. **Análise de riscos** - processo completo de análise e avaliação de riscos [CANCELADA] **ABNT NBR ISSO/IEC 31000:2018**

III. **Arquivos infectados** – aqueles que sofreram a ação de vírus eletrônico.

IV. **Ativo** - qualquer coisa que tenha valor para a organização (ISO/IEC 13335-1:2004). Os ativos podem ser de vários tipos, incluindo: a) ativos de informação. b) ativos de *software*; c) ativos físicos; d) serviços; e) intangíveis, tais como reputação e a imagem da organização.

V. **Avaliação de riscos** - processo de comparar o risco estimado com critérios de risco pré-definidos para determinar a importância do risco. CANCELADA **ABNT NBR ISO/IEC 31000:2018**

VI. **Chave de Acesso** – código de acesso atribuído a cada usuário. A cada chave de acesso é

associada uma senha individual e intransferível, destinada a identificar o usuário, permitindo-lhe o acesso aos recursos disponíveis.

VII. **Códigos Maliciosos ou Agressivos** – qualquer código adicionado, modificado ou removido de um Sistema, com a intenção de causar dano ou modificar o funcionamento correto desse Sistema, como por exemplo, vírus eletrônico.

VIII. **Controle** - forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

IX. **Correio Eletrônico** - meio de comunicação baseado no envio e recepção de mensagens, através de uma rede de computadores.

X. **Criptografia** - ciência que consiste na codificação e decodificação de mensagens, de forma a garantir a segurança e o sigilo no envio de informações.

XI. **Custodiante do ativo** – Identifica uma pessoa ou organismo que cuida do ativo no dia-a-dia [ISO/IEC 133351:2004 Item 7.1.2].

XII. **Diretrizes** – são as regras de alto nível que representam os princípios básicos que a Secretaria resolveu incorporar à sua gestão de acordo com a visão estratégica da alta Administração. Servem como base para que as normas e os procedimentos sejam criados e detalhados.

XIII. ***Download*** – baixar um arquivo ou documento de outro computador, através da Internet.

XIV. **Evento de segurança da informação** - ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falta de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

XV. **Ferramenta Tecnológica** – sistema (conjunto de programas) e/ou equipamento destinado a proteger, monitorar ou agregar valor aos ativos de informações.

XVI. **FTP (*File Transfer Protocol*)** - protocolo padrão da Internet, usado para transferência de arquivos entre computadores.

XVII. **Gestão de riscos** - atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos cancelada **ABNT NBR ISO/IEC 31000:2018*IMAP* (*Internet Message Access Protocol*)** - protocolo de acesso a mensagens eletrônicas.

XVIII. **Incidente de segurança da informação** - um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação [CANCELADA Substituída por : ISO/IEC 27035:2011].

XIX. **Informações Controladas pelo Governo** – são aquelas pertencentes a terceiros, sendo da competência dos Órgãos Públicos a responsabilidade sobre a sua guarda, utilização e divulgação.

XX. **Informações de Propriedade do Governo** – são aquelas geradas nos ambientes dos Órgãos Governamentais.

XXI. ***Internet*** - associação mundial de redes de computadores interligadas, que utilizam protocolos de comunicação de dados. A Internet provê um meio abrangente de comunicação através de transferência de arquivos, conexões à distância, serviços de correio eletrônico e etc.

XXII. ***Intranet*** - rede interna, de usos corporativos, que utiliza a mesma tecnologia da Internet, para que os funcionários possam acessar as informações dos seus respectivos órgãos.

XXIII. **Licença de *Software*** – direito de uso de um determinado programa de computador, protegido pela legislação que dispõe sobre propriedade, marcas e patentes.

XXIV. ***Modem*** – equipamento de comunicação de dados que utiliza os mecanismos de modulação e demodulação para transmissão de informações.

XXV. **Normas** – especificam no plano tático as escolhas tecnológicas e os controles que deverão ser implementados para alcançar a estratégica definida nas diretrizes.

XXVI. **Nota:** controle é também usado como um sinônimo para proteção ou contramedida.

XXVII. **Órgão Público** – qualquer ente da Administração Pública Direta ou Indireta, Fundações, Autarquias e Empresas Públicas.

XXVIII. ***Peer-to-Peer* (*P2P*)** – é um tipo de programa que permite a distribuição de arquivos a outros usuários através da Internet.

XXIX. **Política de Segurança da Informação** – São as normas que definem, regulamentam e apoiam a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

XXX. **POP (*Post Office Protocol*)** - protocolo usado por usuários de Correio Eletrônico para manipulação de arquivos de mensagens em servidores de Correio Eletrônico.

XXXI. **Proprietário do ativo** – identifica uma pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos. O termo “proprietário” não significa que a pessoa realmente tenha qualquer direito de propriedade do ativo (ISO/IEC 13335- 1:2004 item 7.1.2).

XXXII. **Recursos de processamento da informação** - qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem.

XXXIII. **Risco** - combinação da probabilidade de um evento e de suas consequências [ABNT ISO/IEC Guia 73:2005].

XXXIV. **Segurança da informação** - preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade podem também estar envolvidas.

XXXV. **Servidor de Correio Eletrônico** – equipamento que provê o serviço de envio e recebimento de mensagens de Correio Eletrônico.

XXXVI. **Sistemas Informatizados** – sistema constituído de programas e/ou equipamentos computacionais.

XXXVII. ***Site*** – páginas contendo informações, imagens, fotos, vídeos, sons e etc que ficam armazenadas em provedores de acesso (computadores denominados servidores) à Internet, para serem acessadas por qualquer pessoa que se conecte à rede.

XXXVIII. **SMTP (*Simple Mail Transfer Protocol*)** - protocolo de comunicação usado para troca de mensagens na Internet, via Correio Eletrônico.

XXXIX. ***Software*** – Programa de Computador.

XL. ***Spam*** - qualquer mensagem, independentemente de seu conteúdo, enviada para vários destinatários, sem que os mesmos a tenham solicitado.

XLI. **Tratamento do risco** - processo de seleção e implementação de medidas para modificar um risco cancelada **ABNT NBR ISO/IEC 31000:2018**

XLII. ***Upload*** – envio de um arquivo de seu computador para outro, através da Internet.

XLIII. **Usuários** - funcionários, prestadores de serviços, colaboradores, bolsistas e estagiários.

XLIV. **Vírus Eletrônico** - são pequenos programas que, como os vírus biológicos, têm a propriedade de se juntar a outros arquivos, alterar seu funcionamento normal e se reproduzir (fazer cópias de si), contaminando outros arquivos.

XLV. ***URL*** - *Universal Resource Locator* - *link* ou endereço de uma pagina *WEB*, como por exemplo *https://www.agenersa.rj.gov.br/.*

Legislação e Normas Técnicas

- Decreto n.º 2.479, de 08 de março de 1979 (Regulamento do Estatuto dos Funcionários Públicos Civis do Poder Executivo do Estado do Rio de Janeiro).

- Lei Federal n.º 8.159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados).

- Decreto Federal n.º 4.553, de 27 de dezembro de 2002 (Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado no âmbito da Administração Pública Federal).

- Lei Federal n.º 9.610, de 19 de fevereiro de 1998 (Dispõe sobre o Direito Autoral).

- Lei Federal n.º 9.279, de 14 de maio de 1996 (Dispõe sobre Marcas e Patentes).

- Lei Federal n.º 10.406, de 10 de janeiro de 2002 (Institui o Código Civil).

- Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 (Institui o Código Penal).

- Lei Federal n.º 9.983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 -Código Penal e dá outras providencias).

- Decreto n.º 26.209, de 19 de abril de 2000 (Cria a Delegacia de Repressão aos Crimes de Informática – DRCI e dá outras providências).

- Medida Provisória n.° 2.200-2, de 24 de agosto de 2001 (Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências).

- **LEI Nº 9.609 , DE 19 DE FEVEREIRO DE 1998. -** Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências.

- **LEI Nº 9.610, DE 19 DE FEVEREIRO DE 1998. -** Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.

- Lei Geral de Proteção dos Dados - lei nº 13.709, de 14 de agosto de 2018 com vigência a partir de 14 de agosto de 2020 (é a legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet).

- ABNT NBR ISO/IEC 17799:2005 - Segurança da Informação (Estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização).

- ABNT NBR ISO/IEC 31000:2018 - Gestão de Riscos (tem por finalidade fornecer diretrizes para gerenciar riscos enfrentados pelas organizações. A aplicação destas diretrizes pode ser personalizada para qualquer organização e seu contexto).

Observação: Na medida de suas competências, outras legislações poderão ser aplicadas à matéria, de acordo com o caso concreto.