RESOLUÇÃO Nº 10, DE 22 DE JULHO DE 2021

Aprova a Política de Segurança da Informação (PSI) da ARCE.

O **CONSELHO DIRETOR DA AGÊNCIA REGULADORA DE SERVIÇOS PÚBLICOS DELEGADOS DO ESTADO DO CEARÁ – ARCE**, no uso das atribuições que lhe conferem o artigo 11 da Lei Estadual nº 12.786/97 e o artigo 3º, inciso II, do Decreto Estadual nº 25.059, de 15 de julho de 1998, e **CONSIDERANDO** o Decreto nº 29.227, de 13 de março de 2008, que dispõe sobre a instituição da Política de Segurança da Informação dos ambientes de Tecnologia da Informação e Comunicação - TIC do Governo do Estado do Ceará, **CONSIDERANDO** a deliberação do Conselho Diretor da ARCE na reunião ordinária realizada no dia 22 de julho de 2021; **RESOLVE**:

Art. 1º Fica aprovada a Política de Segurança da Informação (PSI) no âmbito da Agência Reguladora de Serviços Públicos Delegados do Estado do Ceará – ARCE, nos termos do Anexo Único desta Resolução.

Parágrafo único. Aplica-se ao ambiente de Tecnologia da Informação e Comunicação da ARCE a Política de Segurança da Informação e Comunicação do Governo do Estado do Ceará, instituída pelo Decreto nº 29.227, de 13 de março de 2008.

Art. 2º Compete à Coordenadoria de Planejamento e Informação Regulatória – CPR a supervisão e implementação da PSI.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

SEDE DA AGÊNCIA REGULADORA DESERVIÇOS PÚBLICOS DELEGADOS DO ESTADO DO CEARÁ, em Fortaleza, aos 22 de julho de 2020.

HÉLIO WINSTON LEITÃO
Presidente do Conselho Diretor da Arce

FERNANDO ALFREDO R. FRANCO
Conselheiro Diretor da Arce

JARDSON SARAIVA CRUZ
Conselheiro Diretor da Arce

JOÃO GABRIEL LAPROVÍTERA ROCHA
Conselheiro Diretor da Arce

MATHEUS TEODORO RAMSEY SANTOS
Conselheiro Diretor da Arce

FRANCISCO RAFAEL DUARTE SÁ
Conselheiro Diretor da Arce

MARCELO CAPISTRANO CAVALCANTE
Procurador-Chefe

ANEXO ÚNICO A QUE SE REFERE A RESOLUÇÃO Nº 10, DE 22 DE JULHO DE 2021
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA ARCE

DIRETRIZES GERAIS

1. INTRODUÇÃO

1.1. A Política de Segurança da Informação (PSI) é o documento que orienta e estabelece as diretrizes corporativas para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários da ARCE. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

1.2. A presente PSI está baseada nas recomendações da norma ABNT NBR ISSO/IEC 27002:2005, reconhecida como um código de prática para a gestão da segurança da informação, além de estar de acordo com o Decreto nº 9.367 de 26 de dezembro de 2018 , que atualiza a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, instituída pelo Decreto nº 3.505 de 13/06/2000 e outras leis vigentes , inclusive o Decreto nº 29.227, de 13 de março de 2008 do Estado do Ceará que institui a Política de Segurança de Informação dos ambientes de tecnologia de Informação do Estado.

1.3. A informação é um ativo de grande valor para a administração pública, por isso necessita ser adequadamente protegida. "Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio" (ABNT NBR ISO/IEC 17799:2005). Por princípio, a Segurança da Informação deve abranger três propriedades básicas:

a) **Confidencialidade:** Propriedade que estabelece que a informação deva estar acessível apenas para pessoas autorizadas;
b) **Integridade:** Propriedade que estabelece que a informação esteja correta, confiável, sem a ocorrência de mudanças não autorizadas;
c) **Disponibilidade:** Propriedade que estabelece que a informação esteja sempre acessível para uso legítimo de pessoas autorizadas.

1.4. Esta PSI será composta:

a) pelas Diretrizes Gerais constantes neste Anexo Único;
b) por Instruções Específicas constantes neste Anexo Único, que versarão sobre regras de utilização e boas práticas de temas específicos; e devem ser complementada por
c) por Procedimentos Operacionais, que documentarão como os vários procedimentos técnicos devem ser executados, estabelecendo atribuições e responsabilidades de agentes públicos específicos, tanto para sua autorização como para sua execução.

2. OBJETIVO

2.1. O objetivo da PSI consiste em estabelecer diretrizes para a Segurança da Informação e utilização dos recursos de Tecnologia da Informação e Comunicação (TIC) da ARCE, de acordo com seus requisitos de negócio e com as leis e regulamentos pertinentes.

3. ABRANGÊNCIA

3.1. A PSI deverá ser aplicada a todos os setores que compõem a ARCE, bem como às entidades externas que fazem uso de sua infraestrutura, como também a todos os agentes públicos que exerçam atividades nessa secretaria, cabendo a cada um a responsabilidade e o comprometimento para sua aplicação.

4. FATORES CRÍTICOS DE SUCESSO PARA IMPLANTAÇÃO DA PSI

4.1. Comprometimento e apoio visível da alta gestão e de todos os níveis gerenciais.

4.2. Bom entendimento dos requisitos de Segurança da Informação e da gestão de riscos.

4.3. Divulgação eficiente da Segurança da Informação para todos os gestores, agentes públicos e outras partes envolvidas, por meio de palestras, treinamento e educação adequados para se alcançar a conscientização.

4.4. Provisão de recursos financeiros para as atividades da gestão de Segurança da Informação.

4.5. Estabelecimento de um eficiente processo de gestão de incidentes de Segurança da Informação.

5. CONCEITOS E DEFINIÇÕES

5.1. **Agente Público:** todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função em órgão público.

5.2. **Ativo de Informação:** qualquer pessoa, tecnologia, processo ou ambiente que processe, armazene, transporte ou descarte informação institucional.

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

5.4. **Conformidade legal:** atender a todos os requisitos legais aplicáveis ao negócio e estipulados em legislações, resoluções, normas técnicas e outros dispositivos legais.

5.5. **Diretriz:** conjunto de instruções ou indicações que orientam o que deve ser feito para que os objetivos estabelecidos na política sejam alcançados.

5.6. **Disponibilidade:** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

5.7. **Equipe de Tratamento e Resposta a Incidentes:** grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores.

5.8. **Incidente de Segurança:** qualquer evento indesejado ou inesperado, que comprometa as operações ou ameace a Segurança da Informação.

5.9. **Informação de Caráter Sigiloso:** são informações que recebem classificação de segurança, que não devem ser de conhecimento público, às quais somente possuem acesso determinadas pessoas ou grupo de pessoas da instituição.

5.10. **Fornecedor:** pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como entes despersonalizados, que desenvolvem atividades de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.

5.11. **Gestão de Continuidade de Negócios em Segurança da Informação:** processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado.

5.12. **Gestão de Riscos de Segurança da Informação:** conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos.

5.13. **Gestor de Sistema:** responsável por coordenar, durante todo o ciclo de vida do sistema, os trabalhos relativos ao sistema de informação que trata da sua área de negócio e/ou conhecimento, bem como definir os requisitos funcionais que o sistema deve atender.

5.14. **Malware:** (abreviatura para "software malicioso") considerado um tipo de software "maligno" que pretende acessar secretamente um dispositivo sem o conhecimento do usuário. Os tipos de malware incluem spyware, adware, phishing, vírus, Cavalos de Tróia, worms, rootkits, ramsoware e sequestradores de navegador.

5.15. **Metodologia de Desenvolvimento de Sistemas:** processo padrão para desenvolvimento de sistemas de informação.

5.16. **Quebra de Segurança:** ação ou omissão, intencional ou acidental, que resulta no comprometimento da Segurança da Informação.

5.17. **Responsável pela Segurança da Informação:** profissional que tem como responsabilidade zelar pelo cumprimento da PSI, bem como tomar decisões, dar encaminhamento e tratamento a casos relacionados ao tema. Essa função será desempenhada pelo Coordenador da CPR ou por profissional por ele designado.

5.18. **Spam:** termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

5.19. **Terceiros:** agentes externos que não possuem relação direta com as ações desempenhadas pela Arce.

5.20. **Termo de Responsabilidade:** documento por meio do qual o agente público, seja ele servidor de carreira, terceirizado ou outra forma de contratação, assume o compromisso de manter confidencialidade e sigilo sobre todas as informações a que tiver acesso em razão do exercício de suas atribuições.

6. DIRETRIZES GERAIS DA PSI

6.1. **DO ALINHAMENTO ESTRATÉGICO:** A PSI deve contribuir para a realização da missão e a obtenção dos resultados estratégicos almejados pela ARCE.

6.2. **DO GERENCIAMENTO DE OPERAÇÕES E COMUNICAÇÕES:**

a) Devem-se adotar medidas para que os meios de computação e comunicação disponibilizados pela ARCE não sejam usados para infringir as leis que vigoram no país.
b) Devem-se adotar medidas para que o uso dos recursos ofertados aos agentes públicos da ARCE, tais como correio eletrônico, internet, microcomputadores, impressoras e outros, seja disciplinado tendo como fim principal a realização das atividades da instituição.
c) Fica estabelecido que todo conteúdo armazenado ou trafegado nos meios de computação disponibilizados pela ARCE devem estar de acordo com esta PSI, sendo passíveis de inspeção automatizada ou manual.
d) Fica estabelecido que todo equipamento ou serviço disponibilizado para os agentes públicos da ARCE é fornecido em caráter de concessão de uso.

6.3. **DA CONFORMIDADE LEGAL:**

a) A PSI tem que estar em conformidade com requisitos legais, visando evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de Segurança da Informação.
b) Devem ser adotadas medidas para o cumprimento do decreto estadual vigente que estabelece a Política de Segurança da Informação para o Governo do Estado do Ceará, ficando estabelecido que toda a normatização contida no decreto é incorporada por esta PSI independente de transcrição.
c) Deve-se buscar aderência às normas técnicas e boas práticas que regem a Gestão da Segurança da Informação.

6.4. **DA SEGURANÇA EM RECURSOS HUMANOS:** Os Agentes públicos devem ter pleno conhecimento das diretrizes, bem como de suas responsabilidades, limitações e penalidades. Devem agir de acordo com seus papéis para reduzir riscos, roubos, fraudes ou mau uso de recursos.

6.5. **DOS CONTROLES DE ACESSO:**

a) Todo acesso à informação armazenada em meio digital, não publicizada, ocorrerá por meio de mecanismos de identificação e controle de acesso.
b) Qualquer mudança funcional implicará na revisão dos direitos de acesso à informação.
c) Os acessos aos sistemas de informação (sistema de gerenciamento de senhas e permissões de acessos aos sistemas da ARCE) serão precedidos de anuência a termo de responsabilidade.

6.6. **DA AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS:** De acordo com critérios estabelecidos pela ARCE, deve-se buscar garantir a disponibilidade e a continuidade dos sistemas de informação, inclusive dos adquiridos ou desenvolvidos por terceiros para uso da ARCE.

6.7. **DA SEGURANÇA FÍSICA E DO AMBIENTE:** Todo ambiente que contenha ativos de informação deve ser protegido de acordo com sua severidade.

6.8. **DO TRATAMENTO DAS INFORMAÇÕES:**

a) Deve-se buscar garantir confidencialidade, integridade e disponibilidade das informações, quando geradas, armazenadas ou trafegadas no âmbito da ARCE.
b) Toda informação produzida ou armazenada na ARCE é considerada como de sua propriedade, exceto nos casos de obras autorais ou em que a Instituição atue como custodiante da informação.

6.9. **DO ZELO DA IMAGEM DA ARCE E DO GOVERNO:** Devem ser tomadas medidas de segurança específicas nos ativos e nas aplicações que sustentam as páginas WEB da ARCE, visando prevenir dano à imagem do órgão e/ou do Governo do Estado.

7. DAS RESPONSABILIDADES GERAIS DA PSI

7.1. **SÃO DEVERES DO PRESIDENTE DO CONSELHO DIRETOR DA ARCE:**

a) Executar ou delegar poderes para prepostos para supervisionar a execução da PSI.
b) Promover a elaboração, a atualização, a validação e a divulgação das diretrizes e objetivos estratégicos da PSI.

7.2. **SÃO DEVERES DA DIRETORIA EXECUTIVA, DOS COORDENADORES E DOS ASSESSORES QUE COMPÕEM A ARCE:**

a) Auxiliar na supervisão e na execução da PSI.
b) Disseminar a cultura e a PSI.
c) Auxiliar na execução dos programas, planos, projetos e ações de Segurança da Informação.
d) Auxiliar na análise e na avaliação da efetividade de processos, procedimentos, sistemas e dispositivos de Segurança da Informação.
e) Relatar, para as devidas providências, ocorrências, eventos e incidentes de Segurança da Informação, na forma de relatório detalhado e circunstanciado.

7.3. **TAMBÉM SÃO DEVERES DOS COORDENADORES DE CADA SETOR:**

a) Disseminar permanentemente a PSI.
b) Adotar ações que viabilizem o cumprimento da PSI.
c) Solicitar a disponibilidade ou o cancelamento dos recursos de informática necessários aos seus subordinados para o bom desempenho de suas funções.

7.4. **SÃO DEVERES ESPECÍFICOS DO COORDENADOR DE PLANEJAMENTO E INFORMAÇÃO REGULATÓRIA – CPR:**

a) Coordenar as ações para implantação da PSI.
b) Elaborar e/ou atualizar e divulgar os procedimentos que operacionalizem a PSI.
c) Propor, analisar, validar, acompanhar e avaliar as principais iniciativas de Segurança da Informação.

d) Propor e executar os planos de contingência e recuperação de desastres de TIC.
e) Atuar como Responsável pela Segurança da Informação.
f) Planejar e coordenar a execução dos programas, planos, projetos e ações de Segurança da Informação.
g) Supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de Segurança da Informação.
h) Recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança, determinando ações corretivas ou de contingência em cada caso.
i) Coordenar e/ou acompanhar a execução de auditorias de segurança nos sistemas de informação.
j) Suspender, a qualquer tempo, o acesso de usuário a recurso computacional quando evidenciados riscos à Segurança da Informação.
k) Homologar e autorizar o uso de sistemas e dispositivos de processamento de informações.

7.5. **SÃO DEVERES DOS AGENTES PÚBLICOS:**
a) Cumprir as determinações e recomendações estabelecidas nesta PSI.
b) Notificar à sua chefia imediata ou à CPR, indício ou falha na Segurança da Informação, bem como qualquer violação a esta PSI.
c) Responder por toda atividade executada por meio de suas identificações digitais (*token* de assinatura digital, usuário e senha de acesso a sistemas e serviços).
d) Seguir as recomendações e as boas práticas de utilização dos recursos ofertados pela ARCE para a execução de suas atividades.

7.6. **SÃO DEVERES DOS FORNECEDORES:**
a) Cumprir os preceitos estipulados por esta PSI, quando estiverem executando atividades no ambiente da ARCE
b) Notificar à CPR, indício ou falha na Segurança da Informação, bem como qualquer violação a esta PSI.
c) Responder por toda violação de segurança praticada por seu pessoal. d. Seguir as recomendações e as boas práticas de utilização dos recursos ofertados pela ARCE para a execução de suas atividades.

8. DA VIOLAÇÃO À PSI

8.1. A violação de um ou mais dispositivos da PSI ou quebra de segurança por agente público estará sujeita a sanções da esfera administrativa, civil ou penal. O tratamento dessas violações seguirá os trâmites normais estabelecidos por esfera.

9. DA ATUALIZAÇÃO DA PSI

9.1. A PSI, bem como o conjunto de instrumentos normativos gerados a partir dela, deverão ser revisados de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de quatro anos.

10. INSTRUÇÃO ESPECÍFICA: CRIAÇÃO E USO DE CONTAS E SENHAS DE USUÁRIOS

10.1. **OBJETIVO:** Estabelecer um padrão para a criação, utilização e proteção de contas e senhas de usuários.

10.2. **RESPONSABILIDADES:** Cabe, de maneira geral, a todas as Coordenadorias e Assessorias que compõem a ARCE, o acompanhamento e a execução da Política de Criação e Uso de Contas e Senhas de Usuários. Cabe, de maneira específica:

a) AO AGENTE PÚBLICO DA ARCE

- Seguir esta Instrução Normativa.
- Resguardar o sigilo de suas contas e senhas que permitem seu acesso a serviços e sistemas da ARCE.
- Comunicar imediatamente a CPR, a perda ou roubo de senhas de acesso a rede ou a sistemas.
- Responder por todas as ações efetuadas por meio de suas contas e senhas, mesmo que seja por conduta culposa.

b) AO ADMINISTRADOR DE REDE, ADMINISTRADOR DE DADOS E DESENVOLVEDOR DE SISTEMA DA ARCE: preservar a confidencialidade dos arquivos e bancos de dados de senhas que estejam sob sua responsabilidade.

10.3. **NORMAS ESPECÍFICAS PARA USO DE CONTAS E SENHAS:**

a) Os usuários são classificados em usuários internos e externos. São usuários internos os colaboradores que tem autorização de acesso a rede interna da ARCE. São usuários externos os cidadãos e empresas que tiverem necessidade de acessar os sistemas da ARCE.
b) Todos os usuários internos deverão ter uma identificação centralizada na rede que, obrigatoriamente servirá como identificador nos sistemas aplicativos desenvolvidos pela ARCE e, preferencialmente, para sistemas não desenvolvidos internamente.
c) As contas de rede e de serviços serão criadas e mantidas pela CPR.
d) A cada identificador será associado uma senha que pode ser acrescida de outros mecanismos de verificação de identidade como biometria, cartões magnéticos, *tokens*, etc.
e) Para praticidade dos usuários externos podem ser admitidos protocolos abertos de verificação de identidade tais como o OPENID, Oauth e os utilizados no Gmail e Facebook.
f) As contas e senhas geradas para os usuários são do seu uso exclusivo, não podendo ser reveladas ou compartilhadas com terceiros sob circunstância alguma.
g) A gestão das contas de usuários de sistemas é de responsabilidade dos respectivos gestores de sistemas.
h) As senhas não devem ser inseridas em mensagens de e-mails ou outras formas eletrônicas de comunicação. A única exceção a essa regra ocorre no envio de senhas temporárias por meio de comunicação direta entre o administrador de serviço/sistema e o agente público ou entre a central de atendimento ao usuário e o agente público.
i) Contas de outros serviços e sistemas, como correio eletrônico, banco de dados, aplicativos e outros, devem possuir o recurso de bloqueio automático após um número de tentativas inválidas.
j) O agente público deve avisar imediatamente à CPR em caso de suspeita de sua senha ter sido comprometida.
k) Todas as senhas de usuários de acesso à rede, serviços e sistemas da ARCE devem ser trocadas periodicamente.
l) As contas de acesso à rede não utilizadas por seis meses serão bloqueadas.

m) A CPR deverá ser comunicada quando do desligamento de colaboradores para bloqueio do acesso à rede e aos sistemas.
n) O Agente Público que estiver aguardando os trâmites para nomeação ou cessão e que se encontre exercendo as suas atividades na ARCE, somente deverá ter acesso aos Sistemas da ARCE, mediante autorização do Gabinete ou do Coordenador da área à qual o Agente Público estará subordinado.

10.4. **AUDITORIA:** A tentativa de decodificação ou determinação de senhas fracas, poderá ser executada dentro de um processo de auditoria interna ou externa, com o objetivo de verificar o cumprimento das regras estabelecidas na política de senhas. Tal processo será conduzido ou supervisionado pelo Responsável pela Segurança da Informação da ARCE ou por Agente Público por ele determinado. Se uma senha for determinada ou decodificada durante uma dessas auditorias, o usuário terá sua conta bloqueada e será solicitado a substituir a senha decodificada.

11. INSTRUÇÃO ESPECÍFICA: USO DA INTERNET

11.1. **OBJETIVO:** Estabelecer um padrão para o uso da internet condizentes com as finalidades da Arce.

11.2. **RESPONSABILIDADES:** Cabe, de maneira geral, a Diretoria Executiva, todas as Coordenadorias e Assessorias que compõem a ARCE, o acompanhamento e a execução da Política de Uso da Internet. Cabe, de maneira específica:

a) AOS AGENTES PÚBLICOS:
- Seguir a Instrução Normativa de Uso da Internet.
- Responsabilizar-se por todas as ações efetuadas por meio da sua conta de acesso à Internet.

b) AOS ADMINISTRADORES DO SERVIÇO DE INTERNET:
- Respeitar o direito dos agentes públicos quanto à privacidade de suas informações, em face dos poderes administrativos que detêm.
- Zelar pela integridade operacional, disponibilidade e segurança dos servidores de rede que compõem a infraestrutura de Internet da ARCE.
- Monitorar o uso do serviço de Internet, identificando e tratando os casos de abuso de uso da banda de Internet, priorizando os acessos de caráter institucional.
- Assegurar que os registros dos acessos dos agentes públicos à Internet (histórico de URL's acessadas) sejam realizados e mantidos.
- Administrar a relação dos sites bloqueados.

c) À CPR: Monitorar o uso do serviço de Internet, para obtenção de dados estatísticos (consumo de banda, taxa de download, taxa de upload, entre outros), para certificar-se quanto à disponibilidade e confiabilidade desse serviço.

d) AO RESPONSÁVEL PELA SEGURANÇA DA INFORMAÇÃO:
- Analisar os casos de descumprimento da política de uso da Internet, avaliar os riscos e as medidas cabíveis a serem aplicadas. Quando o caso exigir, adotar, em primeira instância, medidas imediatas de contenção quanto ao mau uso dos serviços de Internet, até avaliação da gestão superior.
- Definir a relação de sites a serem bloqueados.

- Analisar as solicitações de acesso a sites bloqueados, avaliando os riscos envolvidos e conceder ou vetar tais solicitações.

11.3. **USO AUTORIZADO:**

a) O serviço de Internet da ARCE deve ser usado preferencialmente para atividades de caráter institucional.
b) É permitido que os agentes públicos façam uso do serviço de Internet da ARCE para acesso a seus correios particulares e a serviços de "home banking". Contudo, o uso do serviço de Internet para outros objetivos que não os institucionais, ocorrerá por conta e risco do agente público, não cabendo a ARCE nenhuma responsabilidade sobre eventuais danos ou perdas sofridas pelo agente público em decorrência desse uso.

11.4. **PRIVILÉGIO PADRÃO:**

a) É garantida aos agentes públicos a prestação do serviço de acesso à Internet da ARCE, estando esse serviço vinculado a criação da conta de rede.
b) A concessão de uso do serviço de Internet ao agente público será fornecida apenas com os privilégios mínimos necessários para realizar atividades condizentes com as finalidades de trabalho da ARCE.
c) É possível a elevação de privilégios de uso da Internet para acesso a sites bloqueados ou execução de serviços na nuvem, desde que formalmente justificado pela Chefia Imediata, endossado pela Coordenadoria da Área e aceito pelo Responsável pela Segurança da Informação.

11.5. **IDENTIDADE DO AGENTE PÚBLICO NA INTERNET:** A identificação e responsabilização do agente público no acesso à Internet se dará por meio de sua conta de rede da ARCE.

11.6. **DO USO DA INFRAESTRUTURA DE INTERNET DA ARCE:**

- A infraestrutura e os recursos computacionais de acesso à Internet da ARCE não podem ser usados para violar as leis e regras brasileiras ou de qualquer outro país.
- Quando nas dependências da ARCE, o agente público deve utilizar somente a infraestrutura de Internet da ARCE para executar suas atividades institucionais.
- Todo e qualquer acesso à Internet (URLs acessadas) realizado por um agente público será registrado. Esses registros deverão ser mantidos, para efeito de auditoria, pelo período mínimo de 01 (um) ano.
- É proibido fazer download (cópia remota) de programas que necessitem de licenciamento e para os quais a ARCE não possua tal licenciamento.
- É proibido distribuir softwares ou conteúdo não autorizado (pirataria).
- É proibido disseminar códigos maliciosos.
- É proibida a execução de jogos ou programas de entretenimento pela Internet.
- É proibida a cópia de arquivos (download) de qualquer tipo, relacionados a pedofilia, obscenidades ou com contexto de racismo.
- Somente pessoal autorizado pelo Conselho Diretor a falar, analisar ou publicar documentos em nome da ARCE, pode emitir comunicações eletrônicas em nome da ARCE. Todos os usuários devem privar-se de advogar causas políticas e de emitir afirmações não autorizadas, ou algo que se assemelhe, em nome da ARCE sobre quaisquer serviços, produtos, contextos políticos, entre outros.
- A ARCE mantém o direito de cópia de qualquer material postado na Internet por qualquer agente público no curso de suas obrigações.

- É proibida a utilização dos recursos da ARCE para a realização de ações que firam direitos autorais de qualquer natureza.
- O agente público deve manter postura ética e cordial na troca de comunicações pela Internet, ficando proibido de proferir qualquer comunicação que possa promover constrangimento ou comprometer a imagem da ARCE.
- Arquivos contendo informações sigilosas da ARCE, que precisam ser transferidos por meio da Internet devem ser codificados/criptografados.
- É proibido utilizar a conta de terceiros para realizar acessos ao serviço de Internet.
- Agentes públicos não podem interceptar, revelar, ajudar na interceptação ou revelação dos acessos e comunicações eletrônicas via Internet de terceiros, a menos que para fins de investigação e desde que tenham autorização formal do Responsável pela Segurança da Informação.
- A rede da ARCE deve ser organizada em níveis de segurança com respeito ao tráfego oriundo da Internet. No nível mais seguro deverão estar os servidores de bancos de dados, e serviços de rede. No nível seguinte os servidores de aplicação, no terceiro nível a rede cabeada de micro computadores, no quarto a rede WIFI de dispositivos da ARCE e no quinto nível Smartphones e dispositivos dos colaboradores e de visitantes. Para cada nível a CPR deve estabelecer protocolos, sites permitidos bem como controlar o consumo e a largura de banda oferecidas.

12. INSTRUÇÃO ESPECÍFICA: USO DO CORREIO ELETRÔNICO

12.1. **OBJETIVO:** Estabelecer um padrão para a utilização do serviço de correio eletrônico.

12.2. **RESPONSABILIDADES:** Cabe, de maneira geral, a todas as Coordenadorias e Assessorias que compõem a ARCE, o acompanhamento e a execução da Política de Uso do Correio Eletrônico. Cabe, de maneira específica:

a) AOS AGENTES PÚBLICOS:
- Seguir esta Instrução Normativa.
- Responsabilizar-se por todas as ações efetuadas por meio da sua conta de correio.

b) AOS ADMINISTRADORES DO CORREIO ELETRÔNICO:
- Respeitar o direito dos agentes públicos quanto à privacidade de suas informações, em face dos poderes administrativos que detêm.
- Executar ações buscando garantir integridade operacional, disponibilidade e segurança do serviço de correio eletrônico da ARCE.

c) À CPR:
- Monitorar o uso das comunicações eletrônicas, para obtenção de dados estatísticos (quantidade de mensagens enviadas, quantidade de mensagens recebidas, espaço em disco ocupado pelas caixas postais, entre outras), para certificar-se quanto à disponibilidade e confiabilidade deste serviço.
- Administrar o serviço de correio eletrônico, ficando a seu critério o estabelecimento de limites, regras de uso e afins.
- Dimensionar, especificar, adquirir e implementar os mecanismos de segurança necessários ao uso do correio eletrônico na rede de computadores da ARCE, incluindo segurança na estação do cliente.

12.3. **USO AUTORIZADO:**

a) O serviço de correio eletrônico da ARCE deve ser usado unicamente para atividades de caráter institucional.
b) É permitido que os agentes públicos façam uso de ferramentas de correios eletrônicos populares para atividades pessoais, por meio da infraestrutura de rede da ARCE.

12.4. **PRIVILÉGIO PADRÃO:**

a) É garantido aos agentes públicos a criação de uma conta de correio eletrônico no serviço de correio da ARCE.
b) A CPR deve definir o perfil mínimo (privilégio mínimo) para criação de caixas postais, estabelecendo cota de armazenamento de mensagens e limite do número de usuários para encaminhamento de mensagens.
c) A concessão de uso do correio eletrônico ao agente público será fornecida com os privilégios mínimos necessários para realizar atividades normais.
d) É possível a elevação de privilégios de uso do correio eletrônico (redimensionamento de cota da caixa postal, permissão para envio de mensagem para múltiplos usuários), desde que formalmente justificado.

12.5. **IDENTIDADE DO USUÁRIO DO CORREIO ELETRÔNICO:**

a) A senha da conta do correio eletrônico não deve ser compartilhada ou revelada, mesmo por suposta solicitação dos administradores do serviço de correio da ARCE.
b) O nome do agente público, o endereço do correio eletrônico, o cargo, a afiliação organizacional, e informações relacionadas incluídas nas mensagens individuais ou para listas devem refletir o emissor da mensagem.
c) É proibido, quando da utilização do correio eletrônico, se fazer passar por outrem quando do envio de mensagens.
d) Agentes públicos não devem enviar comunicações eletrônicas anônimas.
e) Contas institucionais são, a princípio, de responsabilidade do gestor de cada unidade administrativa ou de funcionário formalmente autorizado por requisição à CPR.

12.6. **REGRAS GERAIS DE USO DO CORREIO ELETRÔNICO:**

a) O serviço de correio eletrônico bloqueará automaticamente a conta de usuário no caso de tentativas sucessivas de entrada de senha sem sucesso.
b) As contas de correio serão bloqueadas em conjunto com as de rede
c) O serviço de correio eletrônico deve implementar mecanismo de varredura, detecção e eliminação de *malwares* nos arquivos anexos dos e-mails transitados.
d) Uma vez detectados conteúdos, armazenados nas caixas postais, potencialmente perigosos para a segurança da rede de computadores, de ordem ofensiva ou potencialmente ilegal, será lavrado registro da ocorrência e o conteúdo removido ou apagado da caixa postal, sem que seja necessário anuência prévia do responsável pela respectiva caixa postal.

12.7. **USO DO CORREIO ELETRÔNICO PELO AGENTE PÚBLICO**

a) As comunicações institucionais virtuais devem, prioritariamente, ser realizadas por meio do serviço de correio eletrônico da ARCE.
b) Em casos excepcionais, e plenamente justificados, podem ser utilizadas as contas particulares de correio eletrônico, ou outros meios, para enviar ou receber mensagens de teor institucional. Para tanto é necessária a autorização formal da chefia imediata, após consulta formal ao Responsável pela Segurança da Informação. Nestes casos, a

comunicação deve ocorrer levando em consideração as recomendações e restrições impostas pelo Responsável pela Segurança da Informação.

c) Mecanismos de envio de mensagens para vários usuários simultaneamente devem ser usados somente quando necessário.
d) Os agentes públicos devem gerenciar sua cota de armazenamento de mensagens de forma a evitar que o seu limite de armazenamento seja excedido.
e) Os anexos de mensagens eletrônicas devem provocar o bloqueio das mensagens quando configurarem risco.
f) O serviço de correio eletrônico não deve ser utilizado para difundir, promover ou incentivar discussões de assuntos que não estejam relacionados com as atividades desenvolvidas pela ARCE.
g) Todas as comunicações eletrônicas da ARCE devem ser consistentes com padrões convencionais de conduta ética e cortesia.
h) Anexos inesperados, recebidos de terceiros devem ser tratados como suspeitos. Caso o assunto da mensagem não indique se tratar de assunto da instituição, a mensagem deve ser prontamente descartada.
i) Informações da ARCE que possuam caráter sensível não devem ser enviadas para terceiros, fora da ARCE, sem aprovação antecipada da chefia imediata. De preferência, tais comunicações quando trafegadas por correio eletrônico devem ser criptografadas e assinadas digitalmente quando possível.
j) O encaminhamento interno de mensagens recebidas, de caráter sensível, só deve ser realizado com autorização do remetente e da chefia imediata, após ter sido verificado se o encaminhamento é necessário.
k) Mensagens recebidas sejam de origem interna ou externa, que não sejam condizentes com os objetivos da ARCE ou do Governo do Estado, não devem ser encaminhadas para terceiros.
l) Nos casos em que um agente público receba mensagens ofensivas, não deve responder diretamente para o remetente e sim reportar estas comunicações a sua chefia imediata. Caberá então a chefia imediata adotar as medidas cabíveis de acordo com o caso.
m) Agentes Públicos devem reportar todas as notificações sobre alertas de segurança, avisos de vulnerabilidades e seus afins ao Responsável pela Segurança da Informação. Os mesmos não devem utilizar os sistemas da ARCE para encaminhar as referidas notificações para outros usuários, considerando que somente o Responsável pela Segurança da Informação está autorizado a determinar as ações adequadas em resposta a tais notificações.
n) Nenhum agente público pode utilizar o correio eletrônico da ARCE para expressar posição como representante da ARCE a menos que possua clara autoridade para realizar tais atos ou autorização formal do Gabinete.
o) Os agentes públicos não podem utilizar o correio eletrônico da ARCE para enviar mensagens não solicitadas, tais como spam, correntes ou propagandas de qualquer natureza.

12.8. **PROTEÇÃO DOS DIREITOS DE PROPRIEDADE INTELECTUAL:** As leis para direitos de cópia, patentes, marcas registradas, e outras desta natureza se aplicam ao material obtido através do correio eletrônico. Para este fim, agentes públicos usando o serviço de correio eletrônico da ARCE devem:

a) Reproduzir material somente depois de obter permissão da origem.
b) Citar material de outras origens somente se estas estiverem identificadas adequadamente.

c) Não distribuir material ou conteúdo sem autorização do proprietário intelectual.

12.9. **REGRAS DE PRIVACIDADE DA MENSAGEM:**

a) Todo conteúdo de mensagens trafegadas por meio do serviço do correio eletrônico da ARCE deve ser de cunho institucional, portanto de sua propriedade. Logo, as mensagens trafegadas por esse meio são passíveis de inspeção. Entretanto, cada inspeção deve autorizada formalmente pela Diretoria Executiva e informada ao usuário.
b) A ARCE poderá utilizar ferramentas de inspeção de conteúdo para monitorar todo tráfego da sua rede com o objetivo de garantir o não vazamento de informações sigilosas. Neste contexto, poderão estar inclusas as mensagens trafegadas por meio de outras ferramentas de correio eletrônico, consideradas de uso pessoal. Tais inspeções também deverão ser autorizadas pela Diretoria Executiva e informadas ao usuário.
c) A exposição do conteúdo de mensagens de um agente público ocorrerá somente por mandato judicial ou por solicitação formal da alta gestão da ARCE, mediante supervisão do Responsável pela Segurança da Informação.

12.10. **PROTEÇÃO DOS DIREITOS DE PRIVACIDADE**

a) Agentes públicos não podem interceptar, revelar, ajudar na interceptação ou revelação de comunicações eletrônicas, a menos que para fins de investigação e desde que tenham autorização formal do Responsável pela Segurança da Informação.
b) O Responsável pela Segurança da Informação só pode autorizar a interceptação de comunicações eletrônicas, mediante ordem judicial ou por solicitação por escrito de autoridade superior da ARCE.

12.11. **CÓPIA DE SEGURANÇA DAS MENSAGENS DE CORREIO ELETRÔNICO**

a) Se o agente público considerar que uma mensagem de correio eletrônico contém informação relevante às atividades essenciais da ARCE, contém informação potencialmente importante ou têm valor de evidência para decisões da gerência da ARCE, deve mantê-la no servidor de correio para referência futura.
b) A CPR deve prover mecanismos de cópia de segurança de caixas postais do correio institucional, para a estação de trabalho dos usuários, desde que solicitado por chefia imediata.
c) O usuário pode realizar cópia de segurança de seu correio institucional

12.12. **USO DE PROGRAMAS DE CRIPTOGRAFIA**

a) O serviço de correio eletrônico da ARCE não codifica as mensagens por padrão. Se informações sensíveis precisam ser enviadas pelo serviço de correio eletrônico, é recomendada a utilização de mecanismos de criptografia para proteger a informação.
b) A CPR deve fornecer as ferramentas necessárias para realização de processos de criptografia de mensagens sigilosas a serem enviadas por correio eletrônico.
c) Agentes públicos não devem usar mecanismo de codificação/criptografia, no envio de mensagens pelo correio eletrônico da ARCE, sem antes fazer uma cópia de segurança de suas chaves. As chaves públicas devem obrigatoriamente ser encaminhadas para o Responsável pela Segurança da Informação, que providenciará seu armazenamento de forma segura.

d) Agentes públicos que necessitarem de criptografia para o desempenho de suas atividades de trabalho, devem solicitar a CPR a instalação das ferramentas necessárias.

13. INSTRUÇÃO ESPECÍFICA: USO ACEITÁVEL DOS RECURSOS DE TIC

13.1. **OBJETIVO:** Estabelecer um padrão para o uso aceitável dos recursos de TIC.

13.2. **RESPONSABILIDADES:** Cabe, de maneira geral, à Diretoria Executiva, todas as Coordenadorias e Assessorias que compõem a ARCE, o acompanhamento e a execução da Política de Uso Aceitável dos Recursos de TIC. Cabe, de maneira específica:

a) AOS AGENTES PÚBLICOS:
- Seguir a Instrução Normativa de Uso Aceitável dos Recursos de TIC.
- Zelar pela conservação e pelo bom uso de todo recurso de TIC colocado a sua disposição.

b) À CPR:
- Contribuir com a GAF na gestão dos recursos de TIC da ARCE.
- Monitorar o uso aceitável dos recursos de TIC da ARCE, identificando e tratando os casos de abuso ou mau uso desses recursos.
- Definir as configurações técnicas dos recursos de TIC a serem adquiridos pela ARCE.

c) À EQUIPE DE SUPORTE DA CPR:
- Zelar pela integridade operacional, disponibilidade e segurança dos recursos de TIC da ARCE.
- Realizar as intervenções técnicas nos recursos de TIC da ARCE respeitando a privacidade e a integridade das informações neles armazenadas em face dos poderes administrativos que detém.
- Preferencialmente, informar antecipadamente ao usuário qualquer acesso aos computadores e contas dos usuários. Informar ao usuário, com cópia à DEX, posteriormente nos demais casos justificando o motivo do acesso.

d) AO RESPONSÁVEL PELA SEGURANÇA DA INFORMAÇÃO: Analisar os casos de descumprimento da política de uso dos recursos de TIC, avaliar os riscos e as medidas cabíveis a serem aplicadas. Quando o caso exigir, adotar, em primeira instância, medidas imediatas de contenção quanto ao mau uso dos recursos até avaliação da gestão superior.

13.3. **USO GERAL E PROPRIEDADE:**

a) Os recursos de TIC da ARCE devem ser usados para as atividades de caráter institucional.
b) Os agentes públicos devem estar cientes que as informações que eles criam, utilizam e armazenam nos recursos de TIC da ARCE passam a ser de propriedade da ARCE.
c) A ARCE reserva-se ao direito de inspecionar os arquivos armazenados em quaisquer equipamentos da rede, quando necessário.

d) Quando formalmente autorizada pelo Responsável pela Segurança da Informação, a Equipe de Suporte da CPR pode realizar inspeção de conteúdo nos servidores e computadores da ARCE, garantindo, contudo, a integridade e confidencialidade das informações inspecionadas.
e) Quando formalmente autorizada pelo Responsável pela Segurança da Informação, a Equipe de Suporte da CPR pode realizar nos servidores e computadores da ARCE, extração de conteúdos considerados de natureza ilegal ou que não sejam pertinentes às atividades institucionais da ARCE.
f) Para propósitos de manutenção e segurança, pessoas autorizadas dentro da ARCE podem monitorar equipamentos, tráfego de rede e sistemas em qualquer momento durante a execução de atividades de auditoria.
g) A ARCE reserva-se ao direito de fazer auditoria em redes e sistemas a fim de garantir a obediência a esta norma.
h) Qualquer auditoria, monitoramento ou inspeção devem ser formalmente informados ao usuário, de preferência antecipadamente ou, tempestivamente, se *a posteriori*, com a cabível justificativa, exceto se realizados por autorização judicial.
i) A prerrogativa de inspecionar os ativos de TI e as atividades realizadas na rede de computadores não subjuga indevidamente a privacidade individual e o sigilo de documentos portanto não pode ser indevidamente utilizada sem cabível justificativa técnica, como pretexto para quebra de privacidade ou para indevida exclusão ou alteração de arquivos.
j) A utilização indevida da prerrogativa de inspecionar a rede de computadores ensejará os cabíveis processos administrativos e criminais.

13.4. **REQUISITOS MÍNIMOS DE SEGURANÇA:**
a) Devem ser observadas condições mínimas de segurança física para a utilização, instalação ou guarda de qualquer recurso de TIC da ARCE.
b) Todos os computadores e notebooks de uso dos agentes públicos, devem estar protegidos por antivírus regulamentado pela ARCE, possuir senha de acesso ao sistema, possuir protetor de tela com ativação automática estabelecida em 05 (cinco) minutos ou por meio de desconexão quando o usuário tiver que se afastar do computador.

13.5. **USO INACEITÁVEL:** Sob nenhuma circunstância, agentes públicos da ARCE poderão executar atividades que sejam ilegais, classificadas como crime ou contravenção perante as leis locais, estaduais, federais ou internacionais, enquanto utilizando os recursos computacionais sob o domínio da ARCE. As atividades ou ações listadas a seguir são proibidas:
a) Violar os direitos de qualquer pessoa ou empresa protegida pelo direito de cópia, segredo comercial, patente ou outro tipo de propriedade intelectual, assim como outras leis e regulamentos, incluindo a instalação ou distribuição de softwares que não estejam adequadamente licenciados para uso pela ARCE.
b) Usar os recursos computacionais da ARCE para efetivamente obter, transmitir ou armazenar materiais pornográficos, sobre pedofilia, racismo, ofensivos, segregatórios, discriminatórios ou que violem quaisquer leis.
c) Promover ou manter um negócio para ganhos pessoais, com uso de informações ou recursos da ARCE.
d) Criar ou autorizar pontos de acesso, gerar interrupções na segurança da rede de comunicação ou utilizar técnicas de obtenção de informação não autorizadas sobre a topologia da rede, incluindo acesso à dados que não estejam expressamente

autorizados, varredura na rede, parada de serviços, roteamento falsificado e outros como inundação de pacotes, ou falsificação/ injeção de pacotes para propósitos maliciosos.

e) Executar ações de monitoramento da rede que intercepte dados de usuários, a menos que esta atividade seja parte das obrigações ou função de determinado agente público, e desde que formalmente autorizado pelo Responsável pela Segurança da Informação.
f) Executar atividades intencionadas a enganar a autenticação do usuário ou segurança de qualquer serviço, computador, rede ou conta de qualquer organização, incluindo o uso de ferramentas de hardware ou software para remover/burlar a proteção de cópias de software, descobrir senhas, identificar vulnerabilidades de segurança, decodificar arquivos, ou comprometer a Segurança da Informação por qualquer outro modo.
g) Realizar quaisquer tipos de ataques à rede, sistemas ou serviços da ARCE ou de outras entidades.
h) Realizar quaisquer atividades que envolvam suporte técnico, tais como abertura de equipamentos, mudança de localização, alteração nas configurações e outras similares. Exceção para os agentes públicos que possuem estas atividades como parte de suas funções.
i) Usar quaisquer programas/scripts/comandos ou enviar mensagens de qualquer tipo, com a intenção de interferir ou desabilitar uma sessão autenticada de um usuário.
j) Se apropriar ou copiar arquivos eletrônicos sem permissão.
k) Visualizar arquivos e/ou contas de outras pessoas.
l) Escrever, copiar, executar, ou tentar introduzir qualquer código computacional malicioso designado para se auto replicar, danificar, ou atrasar a performance de acesso para qualquer computador corporativo, rede ou informação.
m) Acessar a rede corporativa da ARCE ou de outras organizações por meio da ARCE, usando modem ou outros mecanismos de acesso remoto sem a aprovação do Responsável pela Segurança da Informação.