MATRÍCULA	NOME	CARGO/FUNÇÃO	MARÇO/2022
00266817	SANDRA MARIA DA SILVA	AUXILIAR DE ADMINISTRAÇÃO	100%
00203815	LUIZ PEREIRA DE LACERDA	AUXILIAR DE SERVIÇOS GERAIS	100%
11678114	JOSÉ AUGUSTO DE SOUSA	AUXILIAR DE SERVIÇOS GERAIS	100%
0032101X	GEORGIA SAMARA RODRIGUES SARAIVA	ASSISTENTE DE ADMINISTRAÇÃO	100%
0032941X	MARIA ELENITA ROCHA DA SILVA	ASSISTENTE DE ADMINISTRAÇÃO	100%
00372110	ADAUTO JOSÉ ARAÚJO MOTA	ASSISTENTE DE ADMINISTRAÇÃO	100%

INSTITUTO DE PESQUISA E ESTRATÉGIA ECONÔMICA DO CEARÁ

PORTARIA Nº10, de 05 de abril de 2022.

INSTITUI A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DOS AMBIENTES DE TIC (POSIC) DO INSTITUTO DE PESQUISA E ESTRATÉGIA ECONÔMICA DO CEARÁ – IPECE.

O DIRETOR GERAL DO IPECE, no uso das atribuições que lhe confere o Art. 5º do Decreto Estadual Nº 33.785, de 26 de outubro de 2020, em consonância com o Decreto Estadual nº 34.100 de 08 de junho de 2021, que promove a revisão da Política de Segurança da Informação e Comunicação dos Ambientes de TIC (PoSIC), do Governo do Estado do Ceará, instituída pelo Decreto nº 29.227, de 13 de março de 2008, e CONSIDERANDO a necessidade de estabelecer princípios e diretrizes para a gestão da Segurança da Informação e Comunicação dos ambientes de TIC do IPECE, RESOLVE:

Art. 1º. Instituir a Política de Segurança da Informação e Comunicação dos Ambientes de TIC do IPECE, na forma do que dispõe o Anexo I da presente Portaria, e cujas normas aplicam-se a todos os agentes públicos atuantes no âmbito do IPECE.

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

INSTITUTO DE PESQUISA E ESTRATÉGIA ECONÔMICA DO CEARÁ, em Fortaleza, 05 de abril de 2022

João Mário Santos de França

DIRETOR GERAL

Registre-se e publique-se.

ANEXO I

A QUE SE REFERE A PORTARIA Nº xx, DE XXXXXXDE 2022

TÍTULO I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DOS AMBIENTES DE TIC DO INSTITUTO DE PESQUISA E ESTRATÉGIA ECONÔMICA DO CEARÁ – IPECE

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º. O IPECE – Instituto de Pesquisa e Estratégia Econômica do Ceará, por meio da Gerência de Estatística, Geografia e Informações - GEGIN, apresenta através deste documento, a sua Política de Segurança da Informa-ção e Comunicação dos Ambientes de TIC (PoSIC).

Art. 2º. Constituem os objetivos da PoSIC do IPECE:

I. estabelecer diretrizes a serem seguidas pelo IPECE quanto à adoção de normas e procedimentos relacionados à segurança da informação e comunicação;

II. fornecer ao órgão normas para a segurança da informação, instituindo responsabilidades e atitudes adequadas para manuseio, tratamento, armazenamento, distribuição, uso e descarte da informação para controle e proteção contra a indisponibilidade e falta de integridade, bem como o acesso não autorizado a dados e informações;

III. definir diretrizes, normas e procedimentos para estabelecer controles e processos que assegurem a preservar a informação quanto à:

a) integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

b) confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

c) disponibilidade: garantia de que os usuários autorizados obte-nham acesso à informação e aos ativos correspondentes sempre que necessário;

d) autenticidade: garantia de que a informação foi produzida, modificada ou descartada por uma determinada pessoa física.

Art. 3º. A Política de Segurança da Informação e Comunicação de-verá ser aplicada a todas as áreas, instalações, equipamentos, materiais, do-cumentos, pessoas e sistemas de informação existentes no IPECE, como tam-bém às atividades de todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço que exercem atividades no âmbito do Insti-tuto ou a quem quer que venha a ter acesso a dados ou informações, incum-bindo a cada um a responsabilidade e o comprometimento para a sua aplica-ção.

CAPÍTULO II

DAS RESPONSABILIDADES

Art. 4º. A Gestão de Tecnologia da Informação e Comunicação será conduzida pela Gerência de Estatística, Geografia, e Informações - GEGIN e terá as seguintes competências:

I. atuar no planejamento estratégico e operacional de tecnologia da informação do IPECE, com vistas a subsidiar a definição das prioridades;

II. supervisionar a execução, revisar e atualizar a Política de Segurança da Informação e Comunicação dos Ambientes de TIC do IPECE;

III. zelar pela garantia da manutenção dos equipamentos e sistemas de informática;

IV. disseminar a cultura e a Política de Segurança da Informação;

V. analisar e monitorar os incidentes de Segurança da Informação;

VI. homologar e autorizar o uso de sistemas e dispositivos de processamento de informações em suas instalações;

VII. suspender, a qualquer tempo, o acesso do usuário a recurso computacional quando evidenciados riscos à segurança da informação e informar o incidente à Gerência de Estatística, Geografia e Informações e demais interessados;

VIII. relatar ao dirigente máximo do órgão, para as devidas providências, as ocorrências, eventos e incidentes de segurança da informação, na forma de relatório detalhado e circunstanciado.

Art. 5º. Às Diretorias, Gerência, Assessorias, Coordenadoria e Nú-cleo cabem a responsabilidade de:

I. disseminar permanentemente a Política de Segurança da Informação;

II. garantir o cumprimento da Política de Segurança da Informação;

III. solicitar a disponibilidade ou cancelamento dos recursos de informática ao suporte de Tecnologia da Informação, pelos meios oficiais e instituídos, necessários aos seus subordinados para o bom desempenho de suas funções.

Art. 6º. Ao usuário dos recursos de informática e sistemas de infor-mações do IPECE cabe a responsabilidade de:

I. conhecer e seguir a Política de Segurança da Informação;

II. comunicar e/ou notificar a seu gestor imediato, ao suporte de tecnologia da informação e/ou a gestão de tecnologia da informação sobre qualquer indício ou falha na Segurança da Informação;

III. manter sigilo sobre as informações consideradas estratégicas e confidenciais do IPECE;

IV. responder por toda atividade executada por meio de sua identificação.

CAPÍTULO III

TERMOS E DEFINIÇÕES

Art. 7º. Para fins desta Portaria, entende-se por:

I. Informação: um conjunto organizado de dados, que constitui uma mensagem sobre um determinado conjunto de dados; conjunto de conhecimento sobre alguém ou alguma coisa;

II. Usuário: pessoa que acessa ou utiliza de forma legítima e autorizada as informações.

III. Terceiros: pessoas que prestam serviço e podem possuir acesso às instalações e recursos de informação;

IV. Rede Local: rede de dados disponibilizada pelo IPECE;

V. Data Center: ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como switches, roteadores e outros;

VI. Colaborador: qualquer indivíduo, seja servidor público, contratado CLT ou prestador de serviço / consultor por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro da Área de Tecnologia da Informação e Comunicação do IPECE.

VII. Pasta pública: Pasta/diretório de acesso permitido a todos os usuários do IPECE, localizada em sua rede interna e dividida por setores (diretorias e gerências), colaboradores e temas diversos;

VIII. Credencial de acesso: Credencial de acesso à rede, sistemas corporativos e demais recursos de TI, disponibilizados ou utilizados pelo IPECE.

Toda credencial concedida para acesso à rede, sistemas e demais recursos de TI do instituto é pessoal e intransferível, sendo o seu proprietário responsável pelas ações executadas;

IX. Recursos de informática: todos os equipamentos necessários ao uso da tecnologia da informação, acesso à rede e aos sistemas. Sejam eles hardwares, como servidores, computadores, monitores, mouses, etc. ou softwares, como programas e sistemas operacionais. Ver item Ativos de TI.

X. Sistemas de informações: sistema informacional computadorizado projetado com a finalidade de coletar, processar, armazenar, transmitir informações e disseminar dados, de maneira a facilitar o acesso de usuários interessados, solucionando problemas e atendendo suas necessidades.

XI. Compartilhamento de recursos: autorizar o uso de terceiros, por meio de sua credencial, aos recursos de informática do instituto.

XII. Credencial: consiste em uma conta de acesso pessoal e intransferível, mediante login de usuário e senha, aos recursos de informática do instituto.

XII. Reset: reconfigurar, restaurar para o zero, restabelecendo uma configuração inicial.

XIV. Infraestrutura de rede: todos os equipamentos e softwares necessários, desde o cabeamento externo até a programas específicos nos servidores e computadores, com o objetivo de conectar, interligar e dar suporte a toda a rede de comunicação da maneira mais adequada para o ambiente corporativo.

XV. Backups: cópia de segurança de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

XVI. Serviços de nuvem: consistem em infraestrutura, plataformas ou software hospedados por fornecedores terceirizados e disponibilizados aos usuários via internet.

XVII. Software: sequência de instruções escritas para serem interpretadas por um computador com o objetivo de executar tarefas específicas. Também pode ser definido como os programas que comandam o funcionamento de um computador.

XVIII. Ativos de TI: Todos os elementos de software, hardware e seus insumos presentes no IPECE, por exemplo:

Softwares (SOs, antivirus, backup, entre outros);

Hardware (computadores, notebooks, data centers, servidores, ro-teadores, impressoras e demais periféricos);

Insumos variados (cartuchos, mídias, materiais de limpeza espe-cíficos, entre outros);

XIX. Acesso lógico: entende-se o acesso aos sistemas ou à rede, local ou remoto, via cabo ou wifi, onde é necessário o uso de credenciais.

Parágrafo único: Para armazenamento incluem-se: notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HDs externos e cartões de memória.

CAPÍTULO IV
CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 8º. Para fins de adoção das diretrizes deste documento, a infor-mação está classificada em:

I. Informação Pública: é toda informação que pode ser acessada por usuários do IPECE e sociedade pública em geral, sem restrição.

II. Informação Interna: é toda informação que só pode ser acessada por usuários do IPECE. São informações que já possuem um certo grau de confidencialidade e que se divulgada, pode comprometer o Instituto.

III. Informação Confidencial: é toda informação que pode ser acessada por usuários IPECE e/ou órgãos do Governo. A divulgação não autorizada dessa informação pode causar impacto (de imagem, de replanejamento e até financeiro) aos princípios e planos do Instituto e do governo estadual.

IV. Informação Secreta: é toda informação que pode ser acessada somente por usuários do IPECE explicitamente autorizados através da indicação feita pelo nome ou por área a qual pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao Instituto.

§ 1º. Cabe a todos os gestores o dever de orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar estudos ainda não divulgados nas impressoras, e mídias em locais de fácil acesso.

§ 2º É também de responsabilidade dos gestores de cada área, estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a classificação definida no caput deste artigo.

CAPÍTULO V
PRINCÍPIOS, DIRETRIZES, NORMAS E PROCEDIMENTOS

Art. 9º. Diretrizes são as regras de alto nível que representam os princípios básicos para a criação e detalhamento das normas e procedimentos. Este documento é a própria diretriz baseado nos princípios do IPECE e por sua vez embasados nas melhores práticas com respaldo de normas técnicas e de qualidade adotadas internacionalmente.

Art. 10. Normas especificam o plano tático. Procedimentos detalham como deverão ser implementados os itens especificados nas normas. Ambos – Normas e Procedimentos – terão seus documentos específicos para tornar cla-ro e compreensível os detalhes e pormenores que devem ser seguidos à risca pelos colaboradores, e serão considerados como parte integrante desta Política de Segurança.

SESSÃO I
CONTROLES DE ACESSO

Art. 11. O colaborador pode utilizar a rede local e os sistemas no IPECE, única e exclusivamente, após identificação por meio de acesso com uma credencial (conjunto de usuário e senha).

Art. 12. O acesso de colaboradores e de prestadores de serviços possuirá prazo de validade, de acordo com o prazo do contrato firmado.

Art. 13. Não é permitido o compartilhamento de recursos, salvo nos seguintes casos:

a) arquivos ou pastas que não possuam cunho reservado ou secre-to, restrito a pessoas autorizadas, de forma temporária, relacionados ao de-sempenho das atividades ou em conformidade com os interesses do IPECE;

b) utilização de impressoras.

Art. 14. O uso de pasta pública nos servidores deve ser consciente e cauteloso, de modo a não incorrer em mau uso, como alocação indevida de espaço, armazenamento de arquivos indevidos, deleção de arquivos, etc.

Art. 15. Cada credencial dá direito a uma sessão, não sendo autori-zado o uso de uma mesma credencial para sessões simultâneas à rede corpo-rativa, salvo exceções que deverão ser encaminhadas à gestão de TIC do IPECE para avaliação e aprovação antes de seu uso.

Art. 16. As contas de acesso são distribuídas em dois grupos – Usu-ários e Administradores – que por sua vez poderão ser segmentadas de acordo a se tornar aderente a este documento e às melhores práticas e de modo a propiciar um ambiente sem problemas, erros ou impactos ocasionados por mau uso ou uso indevido destas credenciais.

Parágrafo único: Considera-se tipos de contas:

I. Contas de usuários: utilizadas por todos os colaboradores, com acesso único à rede corporativa, para utilização conforme suas ati-vidades;

II. Contas administrativas da rede: utilizadas para administrar o ambiente computacional;

III. Contas de sistemas: permite o acesso à rede corporativa para automatizar procedimentos entre sistemas, aplicação, serviço de re-de, sem qualquer intervenção humana no seu uso;

Art. 17. O colaborador tem direito a 5 (cinco) tentativas de autentica-ção de senha para acesso à rede corporativa. O acesso à rede local será blo-queado caso o colaborador não obtenha sucesso após atingir o limite de tenta-tivas de autenticação sendo necessário o colaborador solicitar o restabeleci-mento da conta ao suporte de TIC. Caso o usuário esqueça a senha, deverá ser solicitado um reset da senha.

Art. 18. Todas as senhas de usuários de acesso à rede, sistemas e serviços diversos do IPECE deverão ser trocadas a cada 3 (três) meses.

Art. 19. As contas que ficarem inativas por mais de 90 (noventa) di-as corridos serão bloqueadas.

Art. 20. Não será permitido a nenhum colaborador ou visitante, o acesso lógico sem que este possua uma credencial pessoal que dê o acesso com as restrições aplicadas ao grupo ao qual está inserido.

Art. 21. Caso um colaborador ou visitante insista em realizar um acesso lógico sem atender ao descrito neste documento, estará passivo de sanções aplicáveis de acordo com a gravidade e impacto causado pelo acesso indevido.

Art. 22. Nos ambientes onde exista placa informativa de acesso res-trito, não será permitido a entrada de pessoas estranhas ao grupo de acesso autorizado, sob pena de sanções conforme descrito no capítulo específico nes-te documento.

SESSÃO II
CONTAS E SENHAS

Art. 23. Para a criação, alteração ou exclusão de conta de acesso a serviços para qualquer tipo de usuário no ambiente IPECE:

I. Em caso de criação, o gestor imediato deverá solicitar ao Núcleo Administrativo Financeiro - NUAFI, que encaminhará à gestão de TIC, informando: nome completo do usuário, setor no qual está de-sempenhando suas atividades e ainda os devidos acessos conce-didos: Rede, Internet, Correio Eletrônico, Sistemas e Dados;

II. Em caso de alteração, o gestor imediato deverá solicitar ao Núcleo Administrativo Financeiro - NUAFI, que encaminhará à gestão de TIC, informando: nome completo do usuário, acesso que deve ser alterado (o que remover e o que acrescentar);

III. Quando da mudança de setor, o gestor imediato deverá provi-denciar que a gestão de TIC seja comunicada a realizar o remane-jamento do usuário.

IV. Quando do desligamento, o gestor imediato deverá providenciar junto ao NUAFI que a gestão de TIC seja comunicado a realizar o cancelamento das credenciais do usuário.

V. A gestão de TIC efetuará o cadastro e informará por email ao inte-ressado: o seu usuário, senha provisória e a Política de Segurança;

Parágrafo único. O gestor imediato será responsável pelas contas de acesso pertencentes ao seu setor.

Art. 24. O IPECE se compromete a não acumular ou manter intencionalmente dados pessoais de colaboradores além daqueles relevantes na condução do seu trabalho.

Art. 25. Todos os dados pessoais de colaboradores, sob a responsabilidade do IPECE, serão considerados dados confidenciais, e não serão usados para fins diferentes daqueles para os quais foram coletados nem serão transferidos para terceiros, exceto quando exigido pelo processo e, desde que, tais terceiros mantenham a confidencialidade dos referidos dados.

SESSÃO III
GESTÃO DE ATIVOS

Art. 26. A Gestão de Ativos define os critérios para a elaboração e manutenção de inventário tecnológico, com o objetivo de protegê-los de forma adequada e garantir conformidade com regulamentações em vigor.

Art. 27. O inventário tecnológico deve ser mantido atualizado, permi-tindo a identificação de suas características físicas e lógicas (softwares instala-dos) bem como quando necessário, a identificação do colaborador/setor res-ponsável pelo equipamento.

Art. 28. Deve ser mantido um inventário de todas as licenças de uso utilizadas no ambiente de forma a verificar se todos os softwares em uso no Instituto estão devidamente licenciados.

Art. 29. O IPECE deverá manter devidamente documentado os per-fis padronizados de máquinas e softwares necessários para o desempenho das atribuições de cada área de negócio.

Art. 30. Nenhum hardware ou software poderá dar entrada na infra-estrutura de rede do IPECE se não estiver homologado pela gestão de TIC e devidamente autorizado, devendo essa autorização estar adequada e aderente às diretrizes da TIC e do controle patrimonial do IPECE.

SESSÃO IV
BACKUP E CÓPIAS DE SEGURANÇA

Art. 31. Os tipos de backups mais utilizados são:

I. Completo: contém todo o conteúdo de um conjunto de informa-ções originalmente destinada a guarda.

II. Incremental: realiza backup apenas dos últimos registros altera-dos após o último backup, tenha sido ele completo ou incremental.

III. Diferencial: realiza backup de todos os últimos registros alterados após o backup completo.

Art. 32. A gestão de TIC poderá executar backups pontuais ou sis-temáticos, quando solicitada formalmente por qualquer gestor, preferencial-mente por email, desde que a solicitação esteja de forma clara.

Art. 33. Documentos imprescindíveis para as atividades dos colabo-radores da instituição deverão ser salvos em pastas de rede ou em serviços de nuvem contratada.

Parágrafo único. Serão de responsabilidade do usuário, a perda de arquivos gravados no diretório C do seu computador, pois tais arquivos não terão a garantia de backup.

Art. 34. Todos os backups devem ser automatizados por sistemas de agendamento para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" – períodos em que não há ne-nhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Parágrafo único. Os processos que por algum motivo forem trata-dos manualmente e não automatizados, deverão ser sinalizados adequada-mente para que não haja falhas na execução.

Art. 35. Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar avaliações frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida e sugestões de melhorias.

Art. 36. Os backups imprescindíveis ou críticos obedecerão à regras de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD), LEI Nº 13.709, de 14 de agosto de 2018, capítulo IV, seguindo assim aderente às determina-ções fiscais e legais existentes no país.

Art. 37. O IPECE implantará sua rotina de backup (cópias), armaze-namento e recuperação de dados, utilizando ambiente de nuvem contratada, via Empresa de Tecnologia da Informação do Ceará - ETICE, bem como backups físicos, mantidos nas dependências do Instituto.

Parágrafo único. A rotina de backup realizada no IPECE segue pe-riodicidade definida de acordo com planejamento interno da área de TIC.

SESSÃO V
USO DE SOFTWARES

Art. 38. O IPECE respeita os direitos autorais dos softwares que usa e reconhece que deve pagar o justo valor por eles, não recomendando nem admitindo o uso de programas não licenciados nos computadores do Instituto. É terminantemente proibido o uso de softwares ilegais (sem licenciamento).

Art. 39. A gestão de TIC poderá valer-se deste instrumento para de-sinstalar, sem aviso prévio, todo e qualquer software sem licença de uso ou que estejam em desacordo com esta política em atendimento à Lei 9.609/98 (Lei do Software).

Art. 40. Os softwares instalados nos computadores usados por ser-vidores/colaboradores do IPECE são de propriedade exclusiva, sendo proibi-das as cópias integrais, ou mesmo as parciais, para uso pessoal, dentro ou fora do Instituto.

Art. 41. A instalação indevida de softwares não autorizados que possuam direitos autorais e/ou custos de licenciamento constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, e o infrator está sujeito à pena de detenção e multa.

Art. 42. Quando, por necessidade do serviço, um software precise ser instalado, a gestão de TIC deverá ser comunicada para realizar os proce-dimentos de homologação e posterior aprovação.

SESSÃO VI
PROPRIEDADE DA INFORMAÇÃO

Art. 43. Toda informação produzida ou armazenada no IPECE é de sua propriedade e não de seus colaboradores, exceto os casos onde o Instituto atua como custodiante da informação, devendo seu uso ser destinado, exclu-sivamente, a atender aos interesses da Instituição.

SESSÃO VII
USO DA INTERNET

Art. 44. O acesso à internet provido pelo IPECE, independente se em equipamento do IPECE ou equipamento pessoal de uso autorizado nas dependências da instituição, deverá ser feito sempre com a credencial pessoal e individual do colaborador, obedecendo ao nível de permissão da credencial, sem uso de artifícios com os quais o colaborador consiga obter acesso além do que lhe fora estrita e explicitamente cedido.

Art. 45. Todos os usuários ao utilizarem o serviço de acesso à inter-net deverão fazê-lo no estrito interesse da instituição, mantendo uma conduta profissional, especialmente em se tratando da utilização do bem público, ob-servando as normas e diretrizes desse instrumento.

Art. 46. O direito ao uso da internet provido pelo IPECE será cance-lado/suspenso nas hipóteses de vacância ou remoção do colaborador do qua-dro, licenças por um período longo, afastamento ou qualquer outra espécie de desligamento.

Art. 47. O acesso à Internet provido pelo IPECE será monitorado por meio de ferramentas próprias, podendo ser auditados quando necessário. To-dos os registros de acessos à Internet são passíveis de auditorias.

Art. 48. O uso dos recursos de Internet providos pelo IPECE para atividades ilegais ou que ultrapassem o explicitamente permitido pelo Instituto é passível de punição.

SESSÃO VIII
USO DO CORREIO ELETRÔNICO

Art. 49. Estão sujeitos às regras dessa sessão o uso de qualquer e-mail enviado a partir do domínio da instituição (@ipece.ce.gov.br) por todos os colaboradores.

Art. 50. O sistema de correio eletrônico do IPECE não deve ser utili-zado para recreação ou distribuição de mensagens ofensivas, incluindo co-mentários sobre violência, drogas, orientação sexual, pornografia, práticas reli-giosas, esportes, diversão, loterias, ou qualquer outro assunto que não faça parte do interesse da instituição.

Art. 51. É vedado ao usuário enviar mensagens indesejáveis e/ou realizar cadastro do e-mail corporativo em sites de violência, drogas, orientação sexual, pornografia, práticas religiosas, esportes, diversão, loterias, sendo per-mitido o cadastro somente em sites que façam parte do interesse da instituição e/ou do Governo do Estado.

Art. 52. É recomendado que a conta de email pessoal do servi-dor/colaborador não seja utilizada para questões institucionais.

Art. 53. Usuários de email institucional do IPECE devem observar o nível de classificação da informação tornando-se então responsável e passível de sanções, quando se tratar de sigilo, pela eventual transmissão das informa-ções. O e-mail institucional somente deve ser usado para fins institucionais.

Art. 54. Sendo identificada alguma transgressão à essa política por algum colaborador do IPECE, o seu chefe imediato receberá da gestão de TIC relatório contendo informações sobre a transgressão e os colaboradores pode-rão ser notificados e estarão passíveis de sanções administrativas.

SESSÃO IX
USO DE ANTIVÍRUS

Art. 55. O IPECE disponibilizará software corporativo de antivírus instalado nos equipamentos da instituição para todos os usuários.

Art. 56. O antivírus instalado será atualizado automaticamente no servidor e replicado nas estações de trabalho dos usuários sempre que uma nova versão é disponibilizada pelo fabricante e após homologada pela gestão de TIC através da console de gerenciamento.

Art. 57. As checagens do disco rígido (HD) das estações de trabalho serão programadas para execução automática periódica conforme definições da gestão de TIC e gerenciada pelo aplicativo servidor.

Parágrafo único: Em casos onde seja identificado impacto na ativi-dade do colaborador por conta da execução do processo de checagem do anti-vírus na estação/servidor, o mesmo deve ser relatado à gestão de TIC para que seja avaliada a necessidade de alteração.

Art. 58. A gestão de TIC não autoriza nem recomenda que o usuário remova ou altere as configurações do antivírus a fim de não comprometer a segurança que o software proporciona.

Art. 59. Em caso de equipamentos pessoais ou externos, quando necessários ser inseridos na rede corporativa do IPECE, deverão passar por uma varredura no sistema, utilizando as definições do servidor de antivírus da instituição, sendo o uso permitido somente após estar em acordo com as especificações e livre de vírus.

SESSÃO X

USO DE PERIFÉRICOS, MÍDIAS REMOVÍVEIS E PORTAS USB

Art. 60. O uso das portas USB dos desktops e notebooks é reco-mendado somente por mídias removíveis próprias do IPECE. O usuário que insistir em tal prática será responsável pelos riscos e impactos que o uso de tais dispositivos possam vir a causar nos ativos de informação.

SESSÃO XI

DESCARTE DE MÍDIAS

Art. 61. Mídias contendo dados ou informações referentes ao IPE-CE, deverão ser encaminhados à gestão de TIC para a destruição da informa-ção antes do descarte ou reutilização.

CAPÍTULO VI

SANÇÕES

Art. 62. Nos casos em que houver violação ou não cumprimento de quaisquer das diretrizes estabelecidas por esta Política, serão adotadas san-ções administrativas, com a devida notificação do agente e de sua chefia ime-diata, que podem consistir em advertência formal, suspensão, rescisão do con-trato de trabalho, outra ação disciplinar e/ou processo civil ou criminal, de acordo com a legislação que regulamenta o vínculo empregatício do agente público infrator.

CAPÍTULO VII

VIGÊNCIA E VALIDADE

Art. 63. A presente política passa a vigorar a partir da data de sua publicação, sendo válida por tempo indeterminado.

Art. 64. Sempre que necessário poderá será aditada ou ajustada pa-ra refletir o cenário atualizado, sendo válido sempre o documento mais recentemente publicado.

FUNDAÇÃO DE PREVIDÊNCIA SOCIAL DO ESTADO DO CEARÁ

PORTARIA Nº013/2022 - O PRESIDENTE DA FUNDAÇÃO DE PREVIDÊNCIA SOCIAL DO ESTADO DO CEARÁ, nomeado conforme publicação no DOE nº 186, de 01 de Outubro de 2019, no uso das atribuições que lhe confere a investidura do cargo que ocupa e de acordo com o previsto no Art. 67 da Lei nº 8.666, de 21 de junho de 1993, Resolve: Art. 1º **Designar** a servidora **KAROLINE MARIA SANTOS LEMOS VIDAL**, matrícula nº 3000043-9 e CPF nº 89250907320, para acompanhar e fiscalizar, como fiscal técnico-administrativo, a execução do Contrato nº 004/2022, celebrados entre a FUNDAÇÃO DE PREVIDÊNCIA SOCIAL DO ESTADO DO CEARÁ – CEARAPREV e a EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO CEARÁ – ETICE, CNPJ nº 03.773.788/0001-67, de acordo com as especificações e quantitativos previstos no termo de referência, no contrato, respectivamente, e na proposta da CONTRATADA. Art. 2º São atribuições do fiscal do contrato, resguardado o disposto na legislação pertinente. I - Coordenar as atividades relacionadas à execução do instrumento contratual, subsidiado pelo setor técnico/requisitante, bem como conhecer o teor do contrato, inclusive o Termo de Referência e seus anexos, e demais peças integrantes do processo administrativo, assim como as normas legais e regulamentares aplicáveis aos contratos administrativos, em especial a Lei nº 8.666/1993 e demais legislações que regem a matéria; II - Prestar esclarecimentos relativos a questões operacionais, administrativas e de execução do contrato; III - Supervisionar e acompanhar a execução do contrato, de modo que sejam cumpridas integralmente todas as condições (objeto, prazos, vigência) estabelecidas nas Cláusulas Contratuais; IV - Orientar a contratada e os demais envolvidos na execução do contrato, quanto às questões operacionais e de gerenciamento do contrato; V - Manter atualizado o processo de acompanhamento e fiscalização do contrato contendo registros formais de todas as ocorrências positivas e negativas da execução do contrato, que será o Histórico do Gerenciamento do Contrato, com os seguintes documentos, quando for o caso: a) Cópia do contrato e dos seus eventuais aditivos; b) Registro de tarefas e rotinas; c) Ordens de compra/serviços; d) Termos de recebimento do objeto ou de parcela deste, avaliações, atestes, glosas e sanções; e) Registro formal de ocorrências, de pedidos de alteração e prorrogação do contrato; e f) Todos os demais registros formais referentes à execução do contrato. VI – Registrar todas as ocorrências relacionadas com a execução do contrato, determinando o que for necessário à regularização das falhas ou defeitos observados, propondo a aplicação de multas, ou outras penalidades, quando for o caso, informando à autoridade superior aquelas que ultrapassarem a sua competência; VII - Adotar os procedimentos para o pagamento à contratada, na forma convencionada no instrumento contratual, mediante abertura de processo contendo, no mínimo, o atesto dos comprovantes da execução e recebimento do objeto ou parcela deste, comandadas por Ordem de compra/serviço ou instrumento equivalente; VIII – Verificar e controlar a execução financeira e orçamentária do contrato junto ao setor responsável; IX - Acompanhar o prazo de vigência do Contrato e comunicar à autoridade competente o seu término, com antecedência de 90 (noventa) dias, no caso de prorrogação, e de 120 dias (cento e vinte) dias, no caso de nova contratação; e X - Acompanhar a manutenção das condições classificatórias e habilitatórias da contratada, inclusive quanto à prestação de garantia, quando exigida. Art. 3º - Esta Portaria entra em vigor na data de sua publicação e terá vigência até o vencimento do contrato e de sua garantia, quando houver. FUNDAÇÃO DE PREVIDÊNCIA SOCIAL DO ESTADO DO CEARÁ, em Fortaleza-CE, 08 de abril de 2022.

João Marcos Maia

PRESIDENTE

*** *** ***

PORTARIA Nº014/2022 - O PRESIDENTE DA FUNDAÇÃO DE PREVIDÊNCIA SOCIAL DO ESTADO DO CEARÁ, nomeado conforme publicação no DOE nº 186, de 01 de Outubro de 2019, no uso das atribuições que lhe confere a investidura do cargo que ocupa e de acordo com o previsto no Art. 67 da Lei nº 8.666, de 21 de junho de 1993, Resolve: Art. 1º **Designar** a servidora **FABIANA MOURA BEZERRA**, matrícula nº 3000056-0 e CPF nº 025.265.713-50, para acompanhar e fiscalizar, como fiscal técnico-administrativo, a execução do Contrato N° 003/2020, celebrado entre a FUNDAÇÃO DE PREVIDÊNCIA SOCIAL DO ESTADO DO CEARÁ – CEARAPREV e a empresa FAZ EMPREENDIMENTOS E SERVIÇOS - EIRELI-EPP, CNPJ nº10.533.966/0001-48, de acordo com as especificações e quantitativos previstos no termo de referência, no contrato, respectivamente, e na proposta da CONTRATADA. Art. 2º São atribuições do fiscal do contrato, resguardado o disposto na legislação pertinente. I - Coordenar as atividades relacionadas à execução do instrumento contratual, subsidiado pelo setor técnico/requisitante, bem como conhecer o teor do contrato, inclusive o Termo de Referência e seus anexos, e demais peças integrantes do processo administrativo, assim como as normas legais e regulamentares aplicáveis aos contratos administrativos, em especial a Lei nº 8.666/1993 e demais legislações que regem a matéria; II - Prestar esclarecimentos relativos a questões operacionais, administrativas e de execução do contrato; III - Supervisionar e acompanhar a execução do contrato, de modo que sejam cumpridas integralmente todas as condições (objeto, prazos, vigência) estabelecidas nas Cláusulas Contratuais; IV - Orientar a contratada e os demais envolvidos na execução do contrato, quanto às questões operacionais e de gerenciamento do contrato; V - Manter atualizado o processo de acompanhamento e fiscalização do contrato contendo registros formais de todas as ocorrências positivas e negativas da execução do contrato, que será o Histórico do Gerenciamento do Contrato, com os seguintes documentos, quando for o caso: a) Cópia do contrato e dos seus eventuais aditivos; b) Registro de tarefas e rotinas; c) Ordens de compra/serviços; d) Termos de recebimento do objeto ou de parcela deste, avaliações, atestes, glosas e sanções; e) Registro formal de ocorrências, de pedidos de alteração e prorrogação do contrato; e f) Todos os demais registros formais referentes à execução do contrato. VI – Registrar todas as ocorrências relacionadas com a execução do contrato, determinando o que for necessário à regularização das falhas ou defeitos observados, propondo a aplicação de multas, ou outras penalidades, quando for o caso, informando à autoridade superior aquelas que ultrapassarem a sua competência; VII - Adotar os procedimentos para o pagamento à contratada, na forma convencionada no instrumento contratual, mediante abertura de processo contendo, no mínimo, o atesto dos comprovantes da execução e recebimento do objeto ou parcela deste, comandadas por Ordem de compra/serviço ou instrumento equivalente; VIII – Verificar e controlar a execução financeira e orçamentária do contrato junto ao setor responsável; IX - Acompanhar o prazo de vigência do Contrato e comunicar à autoridade competente o seu término, com antecedência de 90 (noventa) dias, no caso de prorrogação, e de 120 dias (cento e vinte) dias, no caso de nova contratação; e X - Acompanhar a manutenção das condições classificatórias e habilitatórias da contratada, inclusive quanto à prestação de garantia, quando exigida. Art. 3º – Esta Portaria entra em vigor na data de sua publicação e terá vigência até o vencimento do contrato e de sua garantia, quando houver. Art. 4º – Revogam-se as disposições em contrário. FUNDAÇÃO DE PREVIDÊNCIA SOCIAL DO ESTADO DO CEARÁ, em em Fortaleza, 11 de abril de 2022.

João Marcos Maia

PRESIDENTE

*** *** ***