CRCPB
CONSELHO REGIONAL DE CONTABILIDADE DA PARAÍBA

RESOLUÇÃO CRCPB N.º 415, DE 04 DE NOVEMBRO DE 2021.

INSTITUI A POLÍTICA DE CONTROLE DE ACESSO LÓGICO DO CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DA PARAÍBA.

O **CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DA PARAÍBA**, no exercício de suas atribuições legais e regimentais,

CONSIDERANDO o Decreto n.º 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, em especial o inciso II do Art. 15;

CONSIDERANDO o Decreto n.º 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

CONSIDERANDO as normas técnicas ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos, ABNT NBR ISO/IEC 27002:2013 — Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação e ABNT NBR ISO/IEC 27003:2020 — Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Orientações;

CONSIDERANDO que a Resolução CRCPB n.º 408, de 02 de junho de 2021, que aprova o plano diretor de tecnologia da informação (PDTI) do Conselho Regional de Contabilidade da Paraíba, biênio 2021-2021 estabelece o objetivo atender às necessidades de informação, de tecnologia e de serviços de TI, alinhadas aos objetivos estratégicos do Sistema CFC/CRCs, visando agregar valor ao negócio e à melhoria dos processos desenvolvidos no âmbito da instituição.

CONSIDERANDO a Portaria CRCPB nº 54, de 01 de junho de 2021, que criou o Comitê de Segurança da Informação (CSI) no âmbito do Conselho Regional de Contabilidade do Estado da Paraíba.

R E S O L V E:

Art. 1º - Fica instituída a Política de Controle de Acesso Lógico aos ativos e aos sistemas de informação, para possibilitar o controle de acesso à rede, aos sistemas e às informações produzidas pelo Conselho Regional de Contabilidade do Estado da Paraíba (CRCPB), nos termos do Anexo desta Resolução.

Art. 2º - Esta Política de Controle de Acesso Lógico aplica-se aos conselheiros, empregados, assessores, terceirizados, estagiários, aprendizes, colaboradores, usuários da rede visitante (sem fio) do CRCPB, parceiros e/ou empresas contratadas pelo CRCPB

Art. 3º - A íntegra da política de controle de acesso lógico do conselho regional de contabilidade do estado da paraíba, será disponibilizada em seu Portal e em sua intranet.

Art. 4º - Esta resolução entra em vigor a partir da data da sua assinatura.

Contador **Brunno Sitonio Fialho de Oliveira**
Presidente

Aprovada na 678ª Reunião Plenária de 2021, realizada em 04 de novembro de 2021.

ANEXO

CAPÍTULO I
DA INSTITUIÇÃO, APLICAÇÃO E CONTROLES DE ACESSO

Art. 1º - A elaboração e atualização deste documento é de responsabilidade do Comitê de Segurança da Informação.

Art. 2º - O acesso a informações rotuladas como públicas e de uso interno não é restringido com controles de acesso que discriminam o usuário.

Art. 3º - O acesso às informações confidenciais e restritas serão permitidas apenas quando uma necessidade de trabalho tiver sido identificada e tal acesso aprovado pela Unidade Organizacional responsável.

Art. 4º - O acesso a alguns equipamentos de hardware e/ou software especiais (tais como equipamentos de diagnóstico de rede) é restrito aos profissionais do Setor de TI e Desenvolvimento Profissional, com uso registrado, baseado nas necessidades do CRCPB.

Art. 5º - Será dado a todos os usuários do CRCPB, automaticamente, o acesso aos serviços básicos como correio eletrônico (e-mail), aplicações de produtividade e browser WEB.

§ 1º - Estas facilidades básicas irão variar de acordo com os cargos e serão determinadas pela autoridade competente em cada Unidade Organizacional.

§ 2º - Todos os outros recursos dos sistemas serão providos via perfis de trabalho ou por solicitação feita ao proprietário da informação envolvida.

§ 3º - Quaisquer questões sobre controle de acessos privilegiados deverão ser direcionadas à Unidade Organizacional responsável pela informação.

CAPÍTULO II
DOS TERMOS E DEFINIÇÕES

Art. 6º - Os seguintes termos são utilizados nesta Política de Controle de Acesso Lógico aos ativos e aos sistemas de informação do CRCPB com os significados específicos que se seguem:

I-Arquivo: agrupamento de registros que, geralmente, seguem uma regra estrutural e que possuem informações (dados).

II- Autenticidade: garantia de que uma informação, produto ou documento é do autor a quem se atribui.

III- Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

IV- Credenciais de acesso: conjunto composto pelo nome de conta e respectiva senha, utilizado para o ingresso ou acesso (login) em equipamentos, rede ou sistema.

V- Criptografia: arte e ciência de esconder o significado de uma informação de receptores não desejados.

VI- CSI-CRCPB: Comitê de Segurança da Informação do CRCPB.

VII- Disponibilidade: propriedade de estar acessível e utilizável sob demanda por um usuário autorizado.

VIII- Estações de trabalho: computador pessoal utilizado para trabalho nas Unidades Organizacionais.

IX- Gestor de Sistema: empregado oficialmente designado como gestor de determinado sistema de informação.

X- Integridade: propriedade de salvaguarda da exatidão e completeza da informação contra alterações, intencionais ou acidentais, em seu estado e atividades.

XI- Ponto de acesso sem fio: equipamento que compõe uma rede sem fio (wireless), concentrando as conexões de um ou mais equipamentos.

XII- Privilégio mínimo: conceito que define que uma pessoa só precisa acessar os sistemas e recursos mínimos necessários para realizar suas atividades.

XIII- Programa: coleção de instruções que descrevem uma tarefa a ser realizada por um computador.

XIV- Recursos de armazenamento de dados corporativos: armazenamento de massa projetado para ambientes de grande escala e alta tecnologia.

XV- Recursos de TI: todo equipamento ou dispositivo que utiliza tecnologia da informação, bem como qualquer recurso ou informação que seja acessível por meio desses equipamentos ou dispositivos tecnológicos, tais como impressoras, sistemas, programas, softwares, acessos à rede local, internet, VPN (rede particular virtual), pendrives, smartcards, tokens, smartphones, modens sem fio, desktops, pastas compartilhadas em rede, entre outros.

XVI- Rede local do CRCPB: conjunto de recursos compartilhados por meio dos servidores de rede, switches e computadores clientes, por onde circulam as informações corporativas do CRCPB.

XVII- Rede sem fio (wireless): sistema que interliga equipamentos utilizando o ar como via de transmissão por meio de ondas eletromagnéticas.

XVIII- Sistema de informação: aplicação da tecnologia da informação que dá apoio às atividades de determinada área de conhecimento, visando otimizar as operações, o gerenciamento e a decisão, trabalhando os dados e transformando-os em informação.

XIX- Sistemas de mensageria: sistemas que permitem o envio e a recepção de mensagens de correio eletrônico ou de mensagens instantâneas entre usuários, dentro e fora da instituição.

XX- Storages: rede de área de armazenamento projetada para agrupar dispositivos de armazenamento de computador.

XXI- TI: Tecnologia da Informação.

XXII- TIC: Tecnologia da Informação e Comunicação são um conjunto de recursos tecnológicos utilizados de forma integrada com um objetivo comum.

XXIII- Unidade Organizacional: unidade em que está lotado o empregado, assessor, terceirizado, estagiário ou aprendiz.

XXIV- Usuário: pessoa física ou jurídica que opera algum sistema informatizado do CRCPB..

XXV- Web: Rede Mundial de Computadores.

XXVI- Webconferência: reunião ou encontro virtual realizado pela internet por meio de aplicativos ou serviço com possibilidade de compartilhamento de apresentações, voz, vídeos, textos e arquivos por meio da web.

CAPÍTULO III
DO CADASTRAMENTO DE USUÁRIOS

Art. 7º - A criação de novas contas de acesso à rede se dará da seguinte forma:

I. para empregados e assessores: após a abertura de chamado pelo Setor de TI e Desenvolvimento Profissional no helpdesk, informando o nome completo, a lotação e a matrícula do empregado;

II. para estagiários e menores aprendizes: após a abertura de chamado pelo Setor de TI e Desenvolvimento Profissional no helpdesk, informando a Unidade Organizacional de lotação, matrícula do estagiário e a vigência do contrato; e

III. para prestadores de serviço: após a abertura de chamado pelo gestor do contrato no helpdesk, informando o nome completo, Unidade Organizacional de lotação, número e vigência do contrato, nome da empresa contratada e matrícula na empresa contratada (ou outro documento legalmente válido).

Parágrafo único. Nas eventuais substituições, caberá ao responsável informar o período para a configuração adequada da conta de acesso do empregado, assessor ou prestador de serviço.

Art. 8º - As contas dos estagiários, menores aprendizes e prestadores de serviço serão configuradas para expiração automática, concomitantemente à vigência do contrato.

Art. 9º- Caberá ao titular da Unidade Organizacional solicitar a coordenação de TI e Desenvolvimento Profissional a liberação ou restrição de privilégios de acesso aos documentos de sua unidade.

Art. 10- Para evitar a expiração automática da conta de estagiários, menores aprendizes ou de prestadores de serviços, deverá ser aberto chamado pelo superior hierárquico imediato do estagiário ou do menor aprendiz, ou pelo gestor do contrato do prestador de serviços no helpdesk, com antecedência mínima de 72 (setenta e duas) horas à expiração da conta.

Art. 11- Todos os usuários que utilizam aplicações e sistemas do CRCPB devem assinar o Termo de Responsabilidade sobre o conhecimento da Política de Controle de Acesso Lógico do CRCPB, conforme o Anexo II.

Art. 12 - A assinatura do documento de que trata o artigo anterior indica que o usuário em questão entende e concorda com as políticas, padrões, normas e procedimentos do CRCPB relacionados ao ambiente de TI, incluindo as instruções contidas nesta resolução, bem como as implicações legais decorrentes do não cumprimento do disposto no termo.

Art. 13 - O gestor do contrato ficará responsável por recolher a assinatura desse no Termo de Responsabilidade sobre o conhecimento da Política de Controle de Acesso Lógico do CRCPB, conforme o Anexo II, a ser arquivado no respectivo processo de gestão do contrato.

Art. 14 - O solicitante de acesso para empregado, comissionado, estagiário ou menor aprendiz deverá recolher a assinatura desses no Termo de Responsabilidade sobre o conhecimento da Política de Controle de Acesso Lógico do RCPB, conforme o Anexo II, a ser arquivado pelo Setor de TI e Desenvolvimento Profissional.

Art. 15 - Em casos excepcionais, poderão ser criadas contas para conselheiros, contadores membros de grupos e/ou comissões instituídas pela Presidência do CRCPB ou empregados de Conselhos Regionais de Contabilidade que estejam desempenhando serviços no CRCPB, após abertura de chamado, via helpdesk, pelo titular da Unidade Organizacional onde o conselheiro, membro de grupo ou comissão ou empregado de CRC atuará.

Parágrafo único. O Termo de Responsabilidade sobre o conhecimento da Política de Controle de Acesso Lógico do CRCPB, conforme o Anexo II, deverá ser assinado pelo conselheiro, membro de grupo ou comissão ou empregado de CRC e ficará arquivado no Setor de TI.

Art. 16 - É de responsabilidade do gestor do contrato solicitar, via helpdesk, o cancelamento da conta de acesso quando do desligamento ou afastamento do prestador de serviço.

Art. 17 – A coordenação de TI e Desenvolvimento Profissional deverá informar, por meio do helpdesk, o desligamento e a movimentação de lotação de empregados, assessores, estagiários e de menores aprendizes para as providências de bloqueio e posterior eliminação da conta, se for o caso.

Art. 18 - Não haverá identificação genérica e de uso compartilhado para acesso aos recursos de rede, excetuando-se os casos de necessidade, justificada e acompanhada de parecer da coordenação de TI e Desenvolvimento Profissional, acerca da possibilidade de aceitação dos riscos associados.

Art. 19 - As novas contas de acesso à rede serão compostas por nome e sobrenome, sendo a forma padrão o nome e o último sobrenome, separados por ponto.

Parágrafo único. Caso a forma padrão incorra em homonímia com conta já existente, será escolhida forma alternativa do seguinte modo:

a) nome e o penúltimo sobrenome completo, separados por ponto; e
b) letras iniciais do prenome e o último sobrenome completo, separados por ponto.

Art. 20 - No ato da criação de conta de acesso à rede, será automaticamente criada conta dos serviços de correio eletrônico (e-mail), mensageria e agenda correspondente, bem como de outros serviços que utilizem a mesma base de dados para autenticação.

Art. 21 - Após a criação da conta solicitada, a coordenador do setor de TI e Desenvolvimento Profissional deverá informar ao solicitante a criação da conta e a senha de acesso inicial, juntamente com as instruções para a sua alteração.

Art. 22 – Em nenhuma hipótese será admitido o empréstimo ou o compartilhamento de credenciais de acesso.

Parágrafo único. No descumprimento dos casos tratados neste item, os atos praticados serão de responsabilidade de todos os envolvidos, estando sujeitos às sanções administrativas e penais cabíveis, tanto o titular das credenciais quanto aquele que as utilizar indevidamente.

CAPÍTULO IV
DA POLÍTICA DE SENHAS

Art. 23 – A identificação de usuários que operam a rede local do CRCPB deve ser feita mediante a autenticação usuário-senha.

Art. 24 – A senha cadastrada é pessoal, intransferível e confidencial.

Art. 25 – A senha deverá observar as seguintes regras de formação:

I-não pode conter o nome da conta do usuário ou partes do nome completo do usuário que excedam dois caracteres consecutivos;
II-deve conter, no mínimo, 12 (doze) caracteres; e
III-deve conter caracteres de três das quatro categorias seguintes:

a) caracteres alfabéticos maiúsculos;
b) caracteres alfabéticos minúsculos;
c) caracteres numéricos; e
d) caracteres especiais, não alfabéticos (por exemplo: !, $, #, %).

Art. 26 - A senha cadastrada terá prazo de validade de 90 (noventa) dias, ao fim do qual o usuário deverá cadastrar nova senha.

Parágrafo único. A nova senha não poderá ser igual às últimas 4 (quatro) senhas anteriormente utilizadas no período de 12 (doze) meses.

Art. 27 - Após 5 (cinco) tentativas erradas, o usuário ficará bloqueado, necessitando recadastrar nova senha.

Art. 28 - Em caso de suspeita de exposição indevida do ambiente de TI, todas as senhas de acesso devem ser imediatamente alteradas.

Art. 29 - Em caso de comprometimento comprovado de segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas.

Art. 30 - Independentemente das circunstâncias, as senhas de acesso não devem ser compartilhadas ou reveladas para outras pessoas que não o usuário autorizado, ficando o proprietário da senha responsável legal por qualquer prática indevida cometida.

CAPÍTULO V
DOS ACESSOS

Seção I
DO ACESSO À REDE

Art. 31 - Apenas poderão ser conectadas à rede cabeada do CRCPB microcomputadores e notebooks previamente autorizados pela coordenação de TI e Desenvolvimento Profissional.

§ 1º - Exceções devem ser comunicadas à Diretoria Executiva do CRCPB, justificando a necessidade e o prazo de utilização.

§ 2º - As exceções autorizadas deverão, obrigatoriamente, adotar os padrões definidos pela Política de Segurança da Informação do CRCPB, sendo o proprietário do

equipamento responsável pelo licenciamento dos produtos nele instalados, uma vez que o CRCPB não fornecerá licenças para o funcionamento de microcomputadores particulares.

Art. 32 - Microcomputadores e dispositivos portáteis poderão acessar a rede sem fio específica para esse fim.

Parágrafo único. O usuário, antes de acessar a rede visitante, deverá se identificar e concordar como termo de uso da rede sem fio.

Art. 33 – A coordenação de TI e Desenvolvimento Profissional poderá desconectar das redes cabeada e sem fio qualquer dispositivo que constitua ameaça à segurança da informação.

Art. 34 - Computadores com acesso à rede deverão ser desligados ou bloqueados na ausência do usuário.

Seção II
DO ACESSO À INTRANET E À INTERNET

Art. 35 - Os acessos a portais da internet e aos demais serviços disponíveis na intranet do CRCPB serão efetuados, preferencialmente, por meio da rede local e deverão ser identificados por usuário.

§ 1º - Os rastros de acesso deverão, no mínimo, identificar usuários, endereço IP, URL acessada, data e hora.

§ 2º - A coordenação de TI e Desenvolvimento Profissional deverá reter os rastros de acesso pelo prazo mínimo fixado pela política de log.

Art. 36 - É proibido o acesso a sítios que tratem de pornografia, pedofilia, erotismo e correlatos; de racismo; de ferramentas para invasão e evasão de sistemas; de compartilhamento de arquivos; e de apologia e incitação a crimes.

Parágrafo único. A coordenação de TI e Desenvolvimento Profissional poderá utilizar software específico que realizará o bloqueio automático desses sítios.

Art. 37 - Os acessos a sites e serviços disponíveis na internet serão controlados por filtros de conteúdo e reguladores de tráfego implementados nos dispositivos de segurança da rede do CRCPB, cuja operacionalização é de responsabilidade da coordenação de TI e Desenvolvimento Profissional.

Art. 38 - As Unidades Organizacionais do CRCPB devem definir, com base nas categorias de conteúdo fornecidas pela coordenação de TI e Desenvolvimento

Profissional, os perfis de filtro de conteúdo a serem aplicados a cada uma de suas unidades.

§ 1º As solicitações de criação ou alteração nas permissões de acesso deverão ser formalizadas e juntadas em processo próprio.

§ 2º - Os titulares das Unidades Organizacionais do CRCPB devem fiscalizar o bom uso dos acessos à internet e solicitar ajustes e restrições, em caso de má utilização.

§ 3º - Mediante solicitação do titular da Unidade Organizacional, a coordenação de TI e Desenvolvimento Profissional poderá fornecer relatórios mensais dos acessos para permitir o devido controle.

Art. 39 – A coordenação de TI e Desenvolvimento Profissional poderá, eventualmente e quando necessário, fazer ajustes temporários no controle de banda para viabilizar eventos específicos como vídeo conferências e acesso a visitantes.

Art. 40 - Todas as operações de acesso realizadas serão registradas para fins de auditoria.

Art. 41 - Não será admitido burlar ou tentar burlar os filtros de conteúdo ou restrições de acesso à internet, sob pena de responsabilização dos envolvidos, que estarão sujeitos às sanções administrativas e penais cabíveis.

Seção III
DO ACESSO REMOTO A SISTEMAS DE INFORMAÇÃO

Art. 42 - O acesso remoto à rede corporativa do CRCPB deve ser realizado somente para atender aos interesses de trabalho.

Art. 43 - Compete a coordenação de TI e Desenvolvimento Profissional definir os perfis de acesso, aplicando técnicas de autenticação e de segurança.

I – o acesso remoto, no âmbito da rede corporativa, deve ser provido por meio de canal criptografado, preferencialmente utilizando as recomendações da ICP-Brasil;

II – o acesso remoto à rede corporativa terá privilégios diferenciados do acesso local, de acordo com o perfil de acesso, com serviços explicitamente controlados;

III – a permissão para se realizar acesso remoto à rede corporativa deve ser solicitada à área de administração da rede pela Coordenação ou área superior a que o usuário da rede está subordinado, com definição do prazo de validade e horários para se realizar o acesso; e

IV – o acesso remoto à rede corporativa será gravado, para posterior auditoria, em logs *contendo data e hora, serviço utilizado, usuário e informações específicas que facilitem o rastreamento da ação tomada.*

Art. 44 - Quaisquer computadores que tenham comunicação remota em tempo real com os sistemas do CRCPB devem se submeter ao mecanismo de controle de acesso, levando-se em consideração os privilégios necessários ao acesso a cada tipo de informação.

Art. 45 - Os usuários da rede devem reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação à Coordenação de TI e Desenvolvimento Profissional.

Art. 46 - Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a coordenação de TI e Desenvolvimento Profissional deverá ser imediatamente acionada para tomar as providências necessárias a sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação do CRCPB.

Art. 47 - Os casos omissos serão resolvidos pelo Comitê de Segurança da Informação.

CAPÍTULO VI
DA UTILIZAÇÃO DO CORREIO ELETRÔNICO CORPORATIVO

Art. 48 - O correio eletrônico é o recurso corporativo para comunicação a ser utilizado de modo compatível com o exercício da função, sem comprometer a imagem do CRCPB nem o tráfego de dados na rede de computadores da instituição.

§ 1º - Todas as mensagens eletrônicas enviadas e recebidas nos domínios do CRCPB terão registrados os dados: data e hora do envio ou recebimento, remetente e destinatário.

§ 2º - A coordenação de TI e Desenvolvimento Profissional deverá implantar mecanismos que evitem o envio e a recepção de mensagens que possam comprometer a segurança do serviço de correio eletrônico.

§ 3º - A coordenação de TI e Desenvolvimento Profissional poderá estabelecer cotas para limitar o espaço de armazenamento das caixas postais, por Unidade Organizacional e por usuário.

§ 4º - A coordenação de TI e Desenvolvimento Profissional não acessará mensagens individuais de caixas de e-mail, salvo para atender aos seguintes objetivos:

I. verificar a obtenção, retenção, uso e divulgação de informações por meio ou com fins ilícitos, ou em desacordo com as normas regulamentares sobre segurança da informação, mediante autorização da Presidência do CRCPB ou da Diretoria Executiva;

II. recuperar conteúdo de interesse do CRCPB, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização da Presidência do CRCPB ou da Diretoria Executiva;

III. atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização da Presidência do CRCPB ou da Diretoria Executiva;

IV. atender à determinação judicial; e

V. realizar a recuperação de mensagens do backup, a pedido do próprio usuário.

§ 5º - O envio de mensagens a componentes da lista de endereços e grupos de e-mails do CRCPB restringir-se-á a assuntos de interesse geral da instituição ou do Sistema CFC/CRCs.

§ 6º - A exclusão de caixas postais ocorrerá com o desligamento do usuário.

Art. 49- São vedadas as seguintes ações relacionadas à utilização do correio eletrônico:

I. acesso ou tentativa de acesso à caixa postal em desacordo com o previsto no § 4º do Art. 50;
II. envio ou armazenamento de mensagem de conteúdo incompatível com as atribuições do usuário, incluindo as que contém ofensas, comentários discriminatórios e pornografia; e
III. adulteração de dados referentes à origem da mensagem nos campos de controle e cabeçalho.

Parágrafo único. Para os fins deste artigo, considera-se armazenado o e-mail aberto e mantido na caixa postal do usuário.

Art. 50 – A coordenação de TI e Desenvolvimento Profissional prestará suporte para a configuração e utilização da tecnologia adotada para o serviço de correio eletrônico corporativo.

CAPÍTULO VII

DA UTILIZAÇÃO DO SISTEMA DE ARQUIVOS

Art. 51 - O sistema de arquivos compreende um conjunto de pastas armazenadas em servidor de arquivos e compartilhadas em rede, que podem ser compartilhadas entre

todos os usuários ou restrito a usuários de determinada Unidade Organizacional ou de determinado projeto.

Art. 52 – A coordenação de TI e Desenvolvimento Profissional realizará o backup dos arquivos armazenados no servidor de arquivos, conforme discriminado na Política de Backup.

Parágrafo único. O backup de arquivos de pastas de usuário armazenadas nas estações de trabalho é de responsabilidade do usuário.

Art. 53 – A coordenação de TI e Desenvolvimento Profissional poderá limitar o tipo de extensão dos arquivos a serem armazenados nas pastas das Unidades Organizacionais.

Art. 54 – A coordenação de TI e Desenvolvimento Profissional não acessará os arquivos armazenados nas pastas das Unidades Organizacionais e dos usuários, salvo nas seguintes situações:

I. verificar a obtenção, retenção, uso e divulgação de informações por meio ou com fins ilícitos, ou em desacordo com as normas regulamentares sobre segurança da informação, mediante autorização da Presidência do CRCPB ou da Diretoria Executiva;

II. recuperar conteúdo de interesse do CRCPB, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização da Presidência do CRCPB ou da Diretoria Executiva;

III. atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização da Presidência do CRCPB ou da Diretoria Executiva;

IV. atender à solicitação judicial; e

V. realizar a recuperação de arquivos do backup, a pedido do usuário.

Art. 55 - Os casos omissos serão dirimidos pela Comissão de Segurança da Informação do CRCPB.

ANEXO II

Termo de Responsabilidade

Pelo presente termo, eu, _____, declaro ter conhecimento da Política de Controle de Acesso Lógico do Conselho Regional de Contabilidade do Estado da Paraíba (CRCPB), disponível para consulta na Intranet (link....).

Declaro que estou recebendo uma conta com privilégios adequados ao exercício das atividades que executo, a qual será utilizada somente para tal fim.

Declaro estar ciente que minhas ações serão monitoradas nos termos da Política de Controle de Acesso Lógico do CRCPB, e que qualquer alteração será de minha responsabilidade, feita a partir de minha identificação, autenticação e autorização.

Estou ciente, ainda, que serei responsável pelo dano que possa causar em descumprimento da Política de Controle de Acesso Lógico do CRCPB, ao realizar uma ação de iniciativa própria de tentativa quanto à modificação da configuração, física ou lógica, dos recursos computacionais sem a permissão da área competente.

João Pessoa (PB), ____ de _____ de 20XX.

Nome:

Matrícula:

Unidade Organizacional:

Nome:

Unidade Organizacional:

(titular da unidade organizacional ou gestor do contrato, para o caso dos terceirizados)

Diante destas argumentações, solicitamos aos nobres pares a aprovação desta matéria.

PLENÁRIO DA CÂMARA DE VEREADORES DE MAMANGUAPE, 27 DE OUTUBRO DE 2021.

Luiz Cornélio da Silva Júnior
Presidente

Feliciano Fragoso dos Santos
1º Secretário

Antônio Carlos Souza da Silva
2º Secretário

Antônio Máximo da Silva Neto
Vice Presidente

Carlito Ferreira da Silva Filho
Vereador

Diego de M.Peixoto Toscano de Lira
Vereador

Edmilson de Paula Pinto
Vereador

Guilherme Antônio de Andrade Fernandes
Vereador

João Belino e Silva Neto
Vereador

Lenilton Oliveira de Lima
Vereadores

Maria das Graças Ribeiro da Silva
Vereadora

Maria do Socorro de Oliveira
Vereadora

Raniery Oliveira Veríssimo
Vereador

CÂMARA MUNICIPAL DE MAMANGUAPE

PROPOSTA DE RESOLUÇÃO Nº075/2021,
MAMANGUAPE, 27 DE OUTUBRO DE 2021.

DISPÕE SOBRE ALTERAÇÃO DOS ARTS. 5º, caput e § 8º, 7º, 22, 23, 27, 95, 101 e 144 § 2º DOREGIMENTO INTERNO DA CÂMARA MUNICIPAL DE MAMANGUAPE E DÁ OUTRAS PROVIDÊNCIAS CORRELATAS.

A Câmara Municipal de Mamanguape, faz saber que o plenário aprovou e Mesa promulga a seguinte alterações ao Regimento Interno desta casa legislativa:

Art. 1º – O caput do art. 5º e § 8º doRegimento Interno da Câmara Municipal de Mamanguape passará a ter a seguinte redação:

"Art. 5º – A sessão preparatória de instalação da legislatura, prevista no art. 24 da Lei Orgânica, será realizada no dia 1º de janeiro, às 16:00 horas, do ano subsequente da eleição, em sessão solene, independente do número de vereadores diplomados pela Justiça Eleitoral, sob a presidência do último presidente, se reeleito vereador, na falta deste, o mais votado, que convidará os vereadores, de preferência de partidos diferentes, para servir de secretário no ato de compromisso e posse.

(...)

§8º – Empossada a mesa, o Presidente provisório, em exercício, declara instalada a Câmara, cessando com este ato seu desempenho legal e dos secretários, assumindo a Presidência permanente dos trabalhos os vereadores Presidente e Secretários eleitos.

Art. 2º – O caput do art. 7º do Regimento Interno da Câmara Municipal de Mamanguape passará a ter a seguinte redação:

"Art. 7º – A Sessão Legislativa ordinária compreenderá dois períodos: de 1º de fevereiro a 30 de junho e de 1º de agosto a 31 de dezembro, conforme previsto no art. 17 da Lei Orgânica do Município.

Art. 3º - O caput do 22 e § 4º do Regimento Interno da Câmara Municipal de Mamanguape passará a ter a seguinte redação:

"Art. 22 – Durante a Sessão de instalação da legislatura, de acordo com artigo 5º, deste regimento, realizar-se-á a eleição da Mesa Diretora, sob a presidência do último vereador presidente, se reeleito vereador, na falta deste, o mais votado dentre os presentes, e, havendo maioria absoluta, elegerão os membros para o primeiro biênio e consequentemente já com a mesa eleita será procedida a eleição do segundo biênio, não sendo permitida a recondução.

(...)

§ 4º – Os mandatos dos membros da atual Mesa Diretora da Câmara Municipal empossados em 1º de janeiro de 2021 terminará em 31 de dezembro de 2022 e os membros do segundo biênio a serem empossados iniciará em 01 de janeiro de 2023 e terminará em 31 de dezembro de 2024."

Art. 4º – O caput do 23 do Regimento Interno da Câmara Municipal de Mamanguape passará a ter a seguinte redação:

"Art. 23 – A eleição para renovação da Mesa Diretora, far-se-á após prévia aprovação de projeto de resolução e publicação da devida resolução, onde será fixada a data para a dita eleição, empossado-se os eleitos no dia 1º de janeiro do ano inicial da legislatura, não sendo, inclusive, permitida a recondução, devendo ser observado na referida resolução os prazos legais para registro de chapa e demais situações pertinentes em normas vigentes aplicáveis à espécie."

Art. 5º – O caput do 27 do Regimento Interno da Câmara Municipal de Mamanguape passará a ter a seguinte redação:

"Art. 27 - O Mandato da Mesa Diretora será de 02 (dois) anos, sem direito a reeleição."

Art. 6º – O caput do 95 do Regimento Interno da Câmara Municipal de Mamanguape passará a ter a seguinte redação:

"Art. 95 – Aparte é a intervenção breve de até 02 (dois) minutos e oportuna ao orador, para indagação, esclarecimento ou contestação a pronunciamento do Vereador que estiver com a palavra."

Art. 7º – O caput do 101 do Regimento Interno da Câmara Municipal de Mamanguape passará a ter a seguinte redação:

"Art. 101 – As sessões ordinárias realizar-se-ão às quintas-feiras, com início às 18:00 horas e término às 22:00 horas.

Art. 8º – O § 2º do 144 do Regimento Interno da Câmara Municipal de Mamanguape passará a ter a seguinte redação:

"(...)

§ 2º Será de exclusiva competência da Mesa a apresentação do projeto de decreto legislativo a que se refere o item I do parágrafo anterior. Os demais poderão ser de iniciativa da Mesa, das comissões ou dos vereadores.(...)"

Art. 09º - Os demais artigos da Resolução nº 020/2009 (Regimento Interno da Câmara de Vereadores) permaneceram inalterados.

Art. 10 - presente Emenda ao Regimento Interno entrará em vigor na data de sua publicação, revogando as disposições em contrário.

PLENÁRIO DA CÂMARA DE VEREADORES DE MAMANGUAPE, 27 DE OUTUBRO DE 2021.

Luiz Cornélio da Silva Júnior
Presidente

Feliciano Fragoso dos Santos
1º Secretário

Antônio Carlos Souza da Silva
2º Secretário

Antônio Máximo da Silva Neto
Vice Presidente

Carlito Ferreira da Silva Filho
Vereador

Diego de M.Peixoto Toscano de Lira
Vereador

Edmilson de Paula Pinto
Vereador

Guilherme Antônio de Andrade Fernandes
Vereador

João Belino e Silva Neto
Vereador

Lenilton Oliveira de Lima
Vereadores

Maria das Graças Ribeiro da Silva
Vereadora

Maria do Socorro de Oliveira
Vereadora

Raniery Oliveira Veríssimo
Vereador

JUSTIFICATIVA

A legitimidade da referida proposição toma como pressuposto a ampliação dos avanços na busca do aperfeiçoamento do processo legislativo nesta Casa.

A proposição ora proposta vem respaldar a eficácia dos trabalhos legislativos em uma comunhão de esforços para atualizações da legislação.

Diante destas argumentações, solicitamos aos nobres pares a aprovação desta matéria.

PLENÁRIO DA CÂMARA DE VEREADORES DE MAMANGUAPE, 27 DE OUTUBRO DE 2021.

Luiz Cornélio da Silva Júnior
Presidente

Feliciano Fragoso dos Santos
1º Secretário

Antônio Carlos Souza da Silva
2º Secretário

Antônio Máximo da Silva Neto
Vice Presidente

Carlito Ferreira da Silva Filho
Vereador

Diego de M.Peixoto Toscano de Lira
Vereador

Edmilson de Paula Pinto
Vereador

Guilherme Antônio de Andrade Fernandes
Vereador

João Belino e Silva Neto
Vereador

Lenilton Oliveira de Lima
Vereadores

Maria das Graças Ribeiro da Silva
Vereadora

Maria do Socorro de Oliveira
Vereadora

Raniery Oliveira Veríssimo
Vereador

LICITAÇÃO

CÂMARA MUNICIPAL DE MAMANGUAPE

RESULTADO FASE PROPOSTA
TOMADA DE PREÇOS Nº 00001/2021

OBJETO: Execução dos serviços de construção da sede da Câmara Municipal de Mamanguape - primeira etapa. CLASSIFICAÇÃO FINAL: 1° - CONSTRUTORA PARAIBANA EIRELI - R$ 923.973,00; 2° - N&G CONSTRUCOES E SERVICOS LTOA - R$ 976.982,58; 3° - D2R3 SERVICOS DE CONSTRUCAO CIVIL EIRELI - R$ 1.013.253,63; 4° - RETA CONSTRUCOES E INCORPORACOES LTOA - R$ 1.067.154,82; 5° - DIAS ENGENHARIA E LOCACOES EIRELI - R$ 1.097.639,24; 6° - CONSTRUTORA EDFFICAR EIRELI - R$ 1.107.453,89; 7° - CONSTRUTORA NACIONAL LOCACOES E SERVICOS EIRELI - R$ 1.132.823,45; 8° - ATLAS CONSTRUCAO E COMERCIO EIRELI - R$ 1.144.947,73; 9° - CONSTRUTORA SF EIRELI - R$ 1.146.899,54; 10° - GMF CONSTRUCOES SERVICOS E LOCACOES LTOA - R$ 1.155.054,39; 11° - HUMBERTO RAMALHO TRIGUEIRO MENDES - R$ 1.155.082,12; 12° - ESTRUTURAL SERVICOS DE CONSTRUCAO CIVIL E LOCACOES EIRELI - R$ 1.161.949,14; 13° - AGUIAR & AGUIAR CONSTRUÇOES LTDA - R$ 1.190.411,85; 14° - NOVA SERVICOS, COMERCIO E CONSTRUCOES EIRELI - R$ 1.197.856,94; 15° - ALX CONSTRUCOES LTOA - R$ 1.250.084,50; 16° - DUARTE MARTINS CONSTRUCOES, SERVICOS E LOCACOES LTDA - R$ 1.271.344,41; 17° - CLN LOCACOES E SERVICOS EIRELI - R$ 1.282.909,74; 18° - SERRA CONSTRUCOES E SERVICOS EIRELI - R$ 1.343.214,87; 19° - GR CONSTRUTORA EIRELI - R$ 1.343.705,87; 20° - AGRESTE CONSTRUTORA E COMERCIO LTDA - R$ 1.358.184,90; 21° - G S C CONSTRUTORA E SERVICOS LTDA - R$ 1.358.803,05; 22° - LA ENGENHARIA E LOCACOES EIRELI - R$ 1.358.803,05; 23° - CONSTRUTORA APODI EIRELI - R$ 1.358.803,05; 24° - J R MUNIZ ENGENHARIA EIRELI - R$ 1.358.803,05; 25° - B & F EDIFICARE ENGENHARIA LTOA - R$ 1.358.803,05; 26° - R F SERVICOS DE CONSTRUCAO CIVIL EIRELI - R$ 1.358.803,05; e 27° - MSM CONSTRUCOES E REFORMAS EIRELI - R$ 1.358.803,05. EMPRESAS DESCLASSIFICADAS: QUALITY CONSTRUCOES LTOA - não atendeu aos itens 9.2.1 e 9.2.2 do Edital; e TRABES CONSTRUCOES E SERVICOS LTOA - não atendeu aos itens 9.2 e 9.4 do Edital. OBSERVAÇÃO: Ocorrência de empate - a classificação foi decidida por sorteio em ato público. Maiores informações poderão ser obtidas junto a Comissão Permanente de Licitação, Rua Duque de Caxias, 123 - Centro - Mamanguape PB, no horário das 08:00 às 12:00 dos dias úteis. E-mail: camaramamanguape@hotmai.lcom.

Mamanguape - PB, 02 de Dezembro de 2021.

CLÁUDIO LEITE FILHO
Presidente da Comissão

ATOS EMPRESARIAIS

CONSELHO REGIONAL DE CONTABILIDADE DA PARAIBA

RESOLUÇÃO CRCPB N.º 415, DE 04 DE NOVEMBRO DE 2021.INSTITUI A POLÍTICA DE CONTROLE DE ACESSO LÓGICO DO CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DA PARAÍBA.O CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DA PARAÍBA, no exercício de suas atribuições legais e regimentais, **CONSIDERANDO** o Decreto n.º 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, em especial o inciso II do Art. 15; **CONSIDERANDO** o Decreto n.º 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética; **CONSIDERANDO** as normas técnicas ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos, ABNT NBR ISO/IEC 27002:2013 — Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação e ABNT NBR ISO/IEC 27003:2020 — Tecnologia da informação — Técnicas de segurança — Sistemas

de gestão da segurança da informação — Orientações; **CONSIDERANDO** que a Resolução CRCPB n.º 408, de 02 de junho de 2021, que aprova o plano diretor de tecnologia da informação (PDTI) do Conselho Regional de Contabilidade da Paraíba, biênio 2021-2021 estabelece o objetivo atender às necessidades de informação, de tecnologia e de serviçosde TI, alinhadas aos objetivos estratégicos do Sistema CFC/CRCs, visando agregar valor ao negócio e à melhoria dos processos desenvolvidos no âmbito da instituição. **CONSIDERANDO** a Portaria CRCPB nº 54, de 01 de junho de 2021, que criou o Comitê de Segurança da Informação (CSI) no âmbito do Conselho Regional de Contabilidade do Estado da Paraíba. **R E S O L V E:Art. 1º** - Fica instituída a Política de Controle de Acesso Lógico aos ativos e aos sistemas de informação, para possibilitar o controle de acesso à rede, aos sistemas e às informações produzidas pelo Conselho Regional de Contabilidade do Estado da Paraíba (CRCPB), nos termos do Anexo desta Resolução. **Art. 2º** - Esta Política de Controle de Acesso Lógico aplica-se aos conselheiros, empregados, asscssores, terceirizados, estagiários, aprendizes, colaboradores, usuários da rede visitante (sem fio) do CRCPB, parceiros e/ou empresas contratadas pelo CRCPB. **Art. 3º** - A íntegra da política de controle de acesso lógico do conselho regional de contabilidade do estado da paraíba, será disponibilizada em seu Portal e em sua intranet. **Art. 4º** - Esta resolução entra em vigor a partir da data da sua assinatura. Contador **Brunno Sitonio Fialho de Oliveira** -Presidente. Aprovada na 678ª Reunião Plenária de 2021, realizada em 04 de novembro de 2021.**RESOLUÇÃO CRCPB N.º 417, DE 04 DE NOVEMBRO DE 2021. ESTABELECER A POLÍTICA DE CONTROLE DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO DO CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DA PARAÍBA. O CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DA PARAIBA,** no uso de suas atribuições legais e regimentais, **CONSIDERANDO** o Decreto n.º 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação, em especial o inciso II do Art. 15; **CONSIDERANDO** o Decreto n.º 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética; **CONSIDERANDO** as normas técnicas ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos, ABNT NBR ISO/IEC 27002:2013 — Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação e ABNT NBR ISO/IEC 27003:2020 — Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Orientações; **CONSIDERANDO** que o Planejamento Estratégico do Sistema CFC/CRCs estabelece os objetivos estratégicos de "Assegurar adequada infraestrutura e suporte logístico às necessidades do Sistema CFC/CRCs" e "Ampliar e integrar o uso da Tecnologia da Informação no Sistema CFC/CRCs"; e **CONSIDERANDO** a Portaria CRCPB nº 54, de 01 de junho de 2021, institui o comitê gestor de implantação do sistema eletrônico de informações no Conselho Regional de Contabilidade do Estado da Paraíba. **CONSIDERANDO** a portaria CRCPB Nº 97, de 18 de Outubro de 2021, que cria o Comitê de Segurança da Informação (CSI) do Conselho Regional de Contabilidade do Estado da Paraíba (CRCPB).**R E S O L V E:Art. 1º** - Eestabelecer a Política de Controle de Ativos de Tecnologia da Informação no âmbito do Conselho Regional de Contabilidade do Estado da Paraíba (CRCPB), com o objetivo de estabelecer controles de segurança, resguardando e gerenciando o acesso aos ativos de Tecnologia da Informação, nos termos dos anexos desta Resolução. **Parágrafo único.** A gestão de ativos físicos de TI é realizada por meio do controle efetivo de seus ciclos de vida, da avaliação dos riscos e das oportunidades, do atendimento aos requisitos regulatórios e da apresentação de soluções inovadoras e sustentáveis, que contribuam para a realização dos resultados institucionais e do Planejamento Estratégico do Sistema CFC/CRCs. **Art. 2º** - Esta Política se aplica aos conselheiros, empregados, assessores, estagiários, terceirizados e menores aprendizes do CRCPB que executem atividades visando atender às demandas do Conselho Regional de Contabilidade do Estado da Paraíba. **Art. 3º** - A íntegra da política de controle de ativos de tecnologia da informação do CRCPB será disponibilizada em seu Portal e em sua intranet. **Art. 4º** - Esta resolução entra em vigor a partir da data da sua assinatura. Contador **Brunno Sitonio Fialho de Oliveira** - Presidente - Aprovada na 678ª Reunião Plenária de 2021, realizada em 04 de novembro de 2021. **RESOLUÇÃO CRCPB N.º 418, DE 04 DE NOVEMBRO DE 2021 - APROVA A POLÍTICA DE ARMAZENAMENTO DE DADOS, DOCUMENTOS E ARQUIVOS (PADDA) DO CONSELHO REGIONAL DE CONTABILIDADE DA DO ESTADO PARAÍBA E DÁ OUTRAS PROVIDÊNCIAS. O PRESIDENTE DO CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DA PARAÍBA** no uso de suas atribuições legais e regimentais, **CONSIDERANDO** a necessidade de estabelecer diretrizes e padrões para garantir um ambiente digital e não digital controlado, eficiente e seguro, de forma a oferecer todas as informações necessárias à classe contábil e à sociedade com integridade, confidencialidade e disponibilidade, **CONSIDERANDO** que o Conselho Regional de Contabilidade do Estado da Paraíba recebe e produz informações de caráter e procedência diversos, as quais devem permanecer íntegras, disponíveis e, nas situações em que a observância for obrigatória, com o sigilo resguardado; **CONSIDERANDO** que as informações no CRCPB são armazenadas em diferentes formas, veiculadas em diferentes meios físicos e eletrônicos, portanto vulneráveis a incidentes como casos fortuitos e de força maior, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto; **CONSIDERANDO** o número progressivo de incidentes cibernéticos no ambiente da rede mundial de computadores e a necessidade de processos de trabalho orientados para a boa gestão da segurança a informação; **CONSIDERANDO** a Lei Federal n.º 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD), de 14 de agosto de 2018, que "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"; **CONSIDERANDO** o Decreto n.º 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação, em especial o inciso II do Art. 15; **CONSIDERANDO** o Decreto n.º 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética; **CONSIDERANDO** a Instrução Normativa n.º 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal; **CONSIDERANDO** a Resolução Conarq n.º 39, de 29 de abril de 2014, que estabelece diretrizes para a implementação de repositórios arquivísticos digitais confiáveis para o arquivamento e manutenção de documentos arquivísticos digitais em suas fases corrente, intermediária e permanente, dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (Sinar); **CONSIDERANDO** a Resolução Conarq n.º 38, de 9 de julho de 2013, que dispõe sobre a adoção das "Diretrizes do Produtor – A Elaboração e a Manutenção de Materiais Digitais: Diretrizes Para Indivíduos" e "Diretrizes do Preservador – A Preservação de Documentos Arquivísticos digitais: Diretrizes para Organizações"; **CONSIDERANDO** a Recomendação Técnica do Arquivo Nacional n.º 2, de junho de 2019, que dispõe sobre as Recomendações para Elaboração de Política de Preservação Digital; **CONSIDERANDO** a necessidade de estabelecer responsabilidade internas quanto ao armazenamento de dados, documentos e arquivos, **RESOLVE: Art. 1º** - Fica instituída a Política de Armazenamento de Dados, Documentos e Arquivos (PADDA) do Conselho Regional de Contabilidade do Estado da Paraíba (CRCPB), nos termos do Anexo desta Resolução. Parágrafo único. Todos os instrumentos normativos gerados a partir da Política de Armazenamento de Dados, Documentos e Arquivos (PADDA) do Conselho Regional de Contabilidade do Estado da Paraíba (CRCPB) são partes integrantes desta e emanam dos princípios e diretrizes nela estabelecidos. **Art. 2º** - A Política de Armazenamento de Dados, Documentos e Arquivos (PADDA) do Conselho Regional de Contabilidade do Estado da Paraíba se aplica a todos os conselheiros, empregados, estagiários, prestadores de serviços e, quando aplicável, a terceiros e a quaisquer outras pessoas que prestem serviços ao CRCPB e que tenham acesso a qualquer documento, arquivo e meio de informação e comunicação, obrigando-os ao cumprimento de suas diretrizes para manuseio, tratamento, controle, proteção das informações e conhecimentos produzidos, armazenados ou transmitidos pelos sistemas de informação ou por meio de outros recursos. **Art. 3º** - A íntegra da Política de Armazenamento de Dados, Documentos e Arquivos (PADDA) do Conselho Regional de Contabilidade do Estado da Paraíba será disponibilizada em seu Portal e em sua intranet. **Art. 4º** - Esta Resolução entra em vigor na data de sua assinatura. Contador **Brunno Sitonio Fialho de Oliveira** - Presidente. Aprovada na 678ª Reunião Plenária de 2021, realizada em 04 de novembro de 2021.

CONSELHO REGIONAL DE CONTABILIDADE DA PARAIBA

RESOLUÇÃO CRCPB N.º 416, DE 04 DE NOVEMBRO DE 2021. APROVA A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) DO CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DA PARAÍBA E DÁ OUTRAS PROVIDÊNCIAS. O CONSELHO REGIONAL DE CONTABILIDADE DO ESTADO DA PARAIBA, no uso de suas atribuições legais e regimentais, **CONSIDERANDO** a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico e não digital controlado, eficiente e seguro, de forma a oferecer todas as informações necessárias à classe contábil e à sociedade, com integridade, confidencialidade e disponibilidade; **CONSIDERANDO** que o Conselho Regional de Contabilidade do Estado da Paraíba recebe e produz informações de caráter e procedência diversos, as quais devem permanecer íntegras, disponíveis e, nas situações em que a observância for obrigatória, com o sigilo resguardado; **CONSIDERANDO** que as informações no CRCPB são armazenadas em diversas formas e veiculadas em diferentes meios físicos e eletrônicos, sendo portanto vulneráveis a incidentes, como desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto; **CONSIDERANDO** o número progressivo de incidentes cibernéticos, no ambiente da rede mundial de computadores, e a necessidade de processos de trabalho orientados para a boa gestão da segurança a informação; **CONSIDERANDO** a Lei Federal n.º 13.709 (Lei Geral de Proteção de Dados Pessoais – LGPD), de 14 de agosto de 2018, que "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"; **CONSIDERANDO** o Decreto n.º 9.637, de 26 de dezembro de 2018, que instituiu a Política Nacional de Segurança da Informação, em especial, o inciso II do Art. 15; **CONSIDERANDO** o Decreto n.º 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética; **CONSIDERANDO** a Instrução Normativa n.º 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal; **CONSIDERANDO** as boas práticas preconizadas pelas normas ABNT NBR ISO/IEC, série 27000, e outras normas nacionais e internacionais relativas à Segurança da Informação; **CONSIDERANDO** a necessidade de estabelecer responsabilidades internas quanto à Segurança da Informação; **CONSIDERANDO** a Portaria CRCPB nº 54, de 01 de junho de 2021, institui o comitê gestor de implantação do sistema eletrônico de informações no Conselho Regional de Contabilidade do Estado da Paraíba. **RESOLVE: Art.1º**-Fica instituída a Política de Segurança da Informação (PSI) no âmbito do Conselho Regional de Contabilidade do Estado da Paraíba, nos termos do Anexo desta Resolução. Parágrafo único. Todos os instrumentos normativos gerados a partir da Política de Segurança da Informação do Conselho Regional de Contabilidade do Estado da Paraíba são partes integrantes desta e emanam dos princípios e diretrizes nela estabelecidos. **Art. 2º** - A Política de Segurança da Informação se aplica a todos os empregados, estagiários, prestadores de serviços, conselheiros e, quando aplicável, a terceiros e a quaisquer outras pessoas que prestem serviços ao CRCPB e que tenham acesso a qualquer meio de informação e comunicação, obrigando-os ao cumprimento de suas diretrizes para manuseio, tratamento, controle, proteção das informações e conhecimentos produzidos, armazenados ou transmitidos pelos sistemas de informação ou por meio de outros recursos. **Art. 3º** - A íntegra da Política de Segurança da Informação do CRCPB será disponibilizada em seu Portal e em sua intranet. **Art. 4º** -Esta resolução entra em vigor a partir da data da sua assinatura. - Contador **Brunno Sitonio Fialho de Oliveira** – Presidente- Aprovada na 678ª Reunião Plenária de 2021, realizada em 04 de novembro de 2021.

CONSELHO REGIONAL DE MEDICINA DO ESTADO DA PARAÍBA

PORTARIA CRM—PB Nº 038/2021

O Presidente do CONSELHO REGIONAL DE MEDICINA DO ESTADO DA PARAÍBA, com o objetivo de defender o interesse público e a regularidade administrativa desta Entidade amparada no ordenamento jurídico em vigor, nas atribuições que lhes conferem a Lei nº 3.268/57, alterada pela Lei nº 11.000/2004, regulamentada pelo Decreto nº 44.045/58, o Regimento Interno deste Conselho de Medicina e o decidido na sessão plenária realizada no dia 25 de outubro de 2021.

CONSIDERANDO a realização de Concurso Público para preenchimento vagas para os cargos de Assistente Administrativo, Agente Fiscal e cadastro de reserva para o cargo de Técnico de Informática;

R E S O L V E:

1. Designar a Comissão responsável pela organização do Concurso Público do CRM PB, composta pelos Conselheiros: Valdir Delmiro Neves, Walter Fernandes de Azevedo e a servidora Márcia Kelly Gomes de Brito, sendo o primeiro o Presidente.

2. Conforme Instrução Normativa CRM PB nº 01/2019, fica estabelecido o pagamento mensal de 25% (vinte e cinco), do salário base dafuncionária durante suas atividades junto a Comissão do Concurso.

3. Revoguem-se as disposições contrárias.

João Pessoa, 1º de dezembro de 2021.

João Modesto Filho
Presidente do CRM PB

LICENÇA

LUPERCIO SANTANA GENTIL, CPF 038.945.964-06 TORNA PÚBLICO QUE REQUEREU A SEMAPA- SECRETARIA DO MEIO AMBIENTE PESCA E AQUICULTURA DE CABEDELO Á LICENÇA DE OPERAÇÃO(LO) DE UM IMOVEL RESIDENCIAL UNIFAMILIAR SITUADO NA QUADRA E, LOTE 21 DO CONDOMINIO HORIZONTAL PONTA DE CAMPINA, EM PONTA DE CAMPINA, CABEDELO PB.