SEI Nº 0019.014994.00004/2023-43
Objeto: Aquisição de Equipamentos e Materiais Permanentes para reestruturar o Hospital Geral de Clínicas de Rio Branco, contemplados com a Portaria Nº 3.340/2020, no âmbito da Secretaria de Estado de Saúde do Estado do Acre - SESACRE.
A DIVISÃO DE PREGÃO torna público que fica suspenso o Processo Licitatório acima mencionado, previamente marcado para o dia 30/01/2024 às 09h15min (horário de Brasília), publicado no Diário Oficial do Estado, no Diário Oficial da União Seção 3 e nos sites, www.licitacao.ac.gov.br e www.comprasnet.gov.br, em razão de haver pedido de esclarecimentos pendentes de resposta no órgão demandante.
Rio Branco-AC, 29 de Janeiro de 2023.

ASS Francisco Alves de Souza NetoCAR Pregoeiro

Processo nº 0006.016657.00003/2023-68
TERMO DE HOMOLOGAÇÃO
Para que produza os efeitos legais em sua plenitude, HOMOLOGO o PREGÃO ELETRÔNICO SRP Nº 259/2023, cujo objeto é Contratação de empresa especializada na execução de serviços de infraestrutura de telecomunicações, visando futura e eventual instalação para interconectividade, manutenção preventiva e corretiva em rede de fibra óptica do Estado do Acre, sob demanda da CONTRATANTE, com fornecimento de material necessário ao pleno funcionamento do serviço, possibilitando a continuidade dos serviços de Comunicação de Dados, conforme especificações contidas no Termo de Referência, adjudicado em favor da empresa APC TECNOLOGIA LTDA, CNPJ Nº 11.241.567/0001-76 vencedora do Lote Único, com valor total de R$ 4.821.665,00 (quatro milhões, oitocentos e vinte e um mil, seiscentos e sessenta e cinco reais).

PAULO ROBERTO CORREIA DA SILVA
Secretário de Estado de Administração
Decreto nº 08-p, de 1º de janeiro de 2023

INSTRUÇÃO NORMATIVA SEAD Nº 5, DE 16 DE JANEIRO DE 2024
Estabelece diretrizes e normas para a operação, o acesso físico e as eventuais manutenções a serem realizadas nos ambientes (principal e de contingência) do Data Center corporativo, sob responsabilidade da Secretaria de Estado de Administração - SEAD.
O SECRETÁRIO DE ESTADO DE ADMINISTRAÇÃO, no uso de suas atribuições legais,
RESOLVE:
Art. 1º Estabelecer normas e diretrizes para a operação, o acesso físico e as eventuais manutenções a serem realizadas nos ambientes (principal e de contingência) do Data Center corporativo, sob responsabilidade da Secretaria de Estado de Administração – SEAD.
Parágrafo único. Considera-se Data Center corporativo, para efeito desta norma, infraestrutura física projetada para abrigar servidores e outros recursos computacionais, como sistemas de armazenamento de dados (storages), ativos de redes (switches e roteadores) e passivos de redes (cabeamento de redes de dados e eletricidade).
CAPÍTULO I
DAS DISPOSIÇÕES GERAIS
Art. 2º Esta norma aplica-se a todos os usuários que necessitem de acesso físico aos ambientes (principal e de contingência) do Data Center corporativo.
Art. 3º O objetivo principal do Data Center corporativo é garantir a disponibilidade de equipamentos que suportem sistemas fundamentais para o funcionamento da Administração Pública do Governo do Estado do Acre, garantindo assim a continuidade dos serviços prestados pelos mesmos.
Art. 4º A Segurança Física do Data Center corporativo tem como objetivos específicos:
I.proteger edificações e equipamentos
II. prevenir perda, dano ou comprometimento dos ativos de rede;
III. manter a continuidade das atividades institucionais; e
IV. prevenir as ameaças que coloquem em risco o bom funcionamento dos sistemas.
Art. 5º É de competência da SEAD, órgão gestor do Data Center corporativo:
I. gerenciar o ambiente do data center como um todo, sendo este de acesso restrito, visto que abriga equipamentos computacionais e guarda dados institucionais da administração pública do governo do estado do acre, em funcionamento ininterrupto;
II. elaborar um procedimento de operação do data center;
III. elaborar um procedimento de controle e transferência de equipamentos para o data center;
IV. definir a abrangência do data center, incluindo o ambiente principal, o de contingência e as demais áreas (sala de energia, sala de equipamentos, cercamento perimetral do grupo gerador e condensadoras e etc); e
V. definir o controle de acesso ao ambiente físico do Data Center.
§ 1º O Data Center deverá ser mantido limpo e organizado, e qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração da equipe de Serviços Gerais sob supervisão do setor responsável.
§ 2º Situações emergenciais que venham a ocorrer no extra-horários, finais de semana e feriados deverão ser encaminhadas pelos operadores de turno ao setor competente.
§ 3º Todas as tratativas deverão ser registradas pelo operador do turno em questão.
CAPÍTULO II
DAS NORMAS DE UTILIZAÇÃO E DE ACESSO
Art. 6º Dada a criticidade dos Data Centers, o acesso às suas infraestruturas e aos seus sistemas deve ser totalmente controlado, onde a administração de dados e de serviços constitui uma tarefa tecnicamente complexa e sua realização deve balizar-se nas melhores práticas de mercado e na alocação de profissionais com perfil técnico adequado.
Art. 7º o acesso físico é restrito àquelas pessoas previamente autorizadas pela SEAD em observância à criticidade e/ou necessidade emergencial que ofereça risco a equipamento e/ou serviço, nele hospedado (devem ser informadas antecipadamente, especificando o horário, o equipamento e ações planejadas).
Seção I
Da solicitação de acesso
Art. 8º A solicitação deverá ser formalizada através de Ofício, registrada no sistema SEI e deverá conter as informações mínimas:
I. finalidade da solicitação para o acesso;
II. criticidade;
III. impacto;
IV. nome do indicado para o acesso;
V. CPF e matrícula; e
VI. cargo/função.
Parágrafo único. Se autorizado, o acesso ao Data Center Corporativo limitar-se à 01 (um) membro indicado pela instituição solicitante, que será acompanhado por servidor da SEAD, pertencente à equipe técnica responsável pela gestão do Data Center.
Art. 9º A solicitação de acesso será registrada e disponibilizada para quaisquer investigações futuras.
Seção II
Do Sigilo Profissional
Art. 10. Deve-se manter absoluto sigilo profissional, zelando pela proteção dos dados, informações e recursos pertencentes ou sob a guarda da SEAD, a que tenham acesso.
Seção III
Da entrada ao Data Center
Art. 11. A entrada no Data Center deve ser condicionada a pessoas portando a identificação física (documento com foto – RG ou similar) para conferência da autorização.
Art. 12. Após o horário normal de trabalho, o acesso para qualquer pessoa que não esteja envolvida na administração, gerenciamento ou operação dos Data Centers, será permitido somente através de autorização emitida pela chefia da área responsável pela gestão do Data Center.
Art. 13. É de responsabilidade dos agentes públicos lotados no Data Center, registrar e acompanhar os prestadores de serviço e visitantes, sendo responsáveis pelas ações destes enquanto permanecerem no ambiente.
Art. 14. A coleta de lixo e limpeza do Data Center deve ser realizada por pessoas instruídas quanto os cuidados necessários para tal serviço, devendo sempre ser autorizadas, registradas e acompanhadas por agente público lotado no ambiente.
Art. 15. Devem-se definir os dias e horários destinados à limpeza do Data Center, de forma a não comprometer a prestação dos serviços disponibilizados pela área.
Art. 16. A entrada e saída de qualquer ativo devem ser registradas. A entrada ou retirada de qualquer equipamento dos Data Centers se dará com o preenchimento do FORMULÁRIO DE AUTORIZAÇÃO DE SAÍDA E ENTRADA DE MATERIAIS, que deve ser enviado através do sistema SEI para análise e, autorização formal deste instrumento pelo Diretor de Modernização e Desenvolvimento Institucional.
Art. 17. Os ramais telefônicos internos do Data Center devem ser restritos a chamadas para membros da equipe da SEAD.
Art. 18. Somente pessoas autorizadas podem portar equipamentos eletrônicos portáteis (celular, pen drive, palms, HD externos, etc.) no interior do Data Center.
Art. 19. O acesso aos Data Centers sem identificação prévia só poderá ocorrer em situações de emergência, quando a segurança física dos Data Centers estiver comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação não estiver funcionando.
Seção IV
Dos Controles de segurança do Data Center
Art. 20. O Controle de Segurança do Data Center deverá possuir sistemas eletrônicos complementares como:
I. circuito Fechado de TV: nas áreas consideradas estratégicas, haven-

do registro da imagem local por meio de câmeras de vídeo, que deverão ser armazenadas em alguma mídia, de forma que as imagens possam ser resgatadas em caso de alguma ocorrência ou auditoria;
II. alarme: que envie alguma mensagem a uma estação de gerenciamento remota caso ocorra algum acesso não autorizado; e
III. câmeras de monitoramento: que devem monitorar locais estratégicos do ambiente, seja ele interno ou externo.
§ 1º Os circuitos das câmeras de monitoramento devem ser protegidos por conduítes de metal e ficar fora do alcance manual, evitando-se desativação intencional ou acidental.
§ 2º As imagens captadas pelas câmeras do circuito interno de TV devem ser gravadas de forma contínua, visando embasar futuras investigações em caso de suspeitas ou incidentes de segurança.
§ 3º Os arquivos das imagens gravadas devem ser guardados pelo período mínimo de um ano, sendo tratados com os mesmos critérios das mídias de cópia de segurança.
§ 4º O sistema de circuito fechado de TV deve ser diariamente inspecionado, de forma a garantir a efetiva gravação das imagens.
§ 5º As imagens gravadas pelo circuito interno de TV devem ser periodicamente analisadas, a fim de identificar possíveis eventos que contrariem a Política de Segurança.
Seção V
Das áreas de Segurança do Data Center
Art. 21. Todas as instalações de processamento ou armazenamento de informações sensíveis devem ser mantidas em áreas de segurança do Data Center.
Art. 22. As permissões de acesso físico às áreas de segurança do Data Center devem ser mensalmente revisadas.
Art. 23. As áreas de segurança do Data Center devem ser claramente definidas com a utilização de barreiras de segurança e mecanismos de controle de acesso, de forma a impedir o acesso não autorizado.
Art. 24. Deve ser evitada a utilização de informações visuais que identifiquem as áreas de atividade de processamento e guarda das informações.
Art. 25. As portas das áreas de segurança do Data Center devem possuir mecanismos para fechamento automático.
Seção VI
Da Instalação e proteção dos equipamentos
Art. 26. É proibida a ligação de mais de um equipamento em uma mesma tomada.
Art. 27. Os equipamentos de TI do Data Center devem ser instalados em racks.
Art. 28. Todos os racks do Data Center devem ser seguros, possuírem portas dotadas de chaves em todos os seus lados e permitirem trancamentos, de maneira que as tomadas de energia permaneçam no seu interior e os fios e cabos sejam acondicionados sem contato com a parte externa, diretamente do piso para o interior do rack.
Art. 29. Os equipamentos cuja dimensão impeça a instalação dentro de racks devem ter seus botões de ligar/desligar devidamente protegidos contra acessos ou internamente desconectados, de forma a evitar seu acionamento local.
Art. 30. As chaves dos racks e dos quadros de força devem receber identificação e serem guardadas em um claviculário em local adequado, protegido contra acesso indevido.
Art. 31. Deve ser designado um responsável pela chave do claviculário, que deverá registrar todas as retiradas e devoluções de chaves.
Art. 32. A identificação adotada deve ser de difícil dedução para pessoas estranhas ao ambiente.
Seção VII
Da Segurança ambiental
Art. 33. A localização do Data Center deve ser ocultada às pessoas que transitam em áreas públicas.
Art. 34. As portas do Data Center devem ser mantidas fechadas.
Art. 35. Materiais combustíveis ou perigosos devem ser guardados de forma segura, a uma distância apropriada das áreas de trabalho e áreas de segurança.
Art. 36. Suprimentos e materiais de escritório não devem ser armazenados em áreas de segurança, a menos que requeridos.
Art. 37. Equipamentos de contingência e mídias com cópias de segurança devem ser armazenados a uma distância segura da instalação principal.
Art. 38. Todo trabalho realizado por terceiros no Data Center deve ser registrado e supervisionado.
Art. 39. É proibido o manuseio de alimentos, bebidas e cigarros, bem como o consumo no Data Center.
Seção VIII
Da Segurança do cabeamento
Art. 40. Todo o cabeamento e equipamentos que estiverem nas dependências dos Data Centers, além de identificados, devem ser documentados para o correto gerenciamento das conexões.
Art. 41. Os pontos de rede excedentes devem ficar inativos.
Seção IX
Do Sistema de combate a incêndio
Art. 42. Levar ao conhecimento da brigada de incêndio do governo do estado, quando da ocorrência de incidentes no local ou proximidades dos ambientes, a relevância dos serviços contidos nos Data Center.
Art. 43. manter os sempre carregados os extintores portáteis compatíveis com os tipos de materiais existentes (classe de fogo a ser combatido).
Art. 44. É proibido manter materiais inflamáveis (diesel, álcool, etc.) no Data Center.
Art. 45. Devem ser elaborados planos de teste dos detectores de fogo e fumaça, sendo executados mensalmente variando o local de procedência e a intensidade da fumaça.
Art. 46. Os equipamentos de combate a incêndio devem ser periodicamente inspecionados e testados por empresa tecnicamente qualificada, registrando-se a revisão.
Seção X
Da Segurança de Equipamentos
Art. 47. Para impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização, devem ser adotadas as seguintes medidas:
I. Gestão de Capacidade: a utilização dos recursos deve ser monitorada e sincronizada e as projeções devem ser feitas para necessidades de capacidade futura, para garantir o desempenho requerido dos Sistemas de Informação Corporativa;
II. Instalação: os equipamentos devem ser colocados no local protegido para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado;
III. Cabeamento: o cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação ou danos;
IV. Equipamento Fora do Datacenter: devem ser garantidas medidas de segurança para equipamentos que operem fora do Data Center, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências do Data Center;
V. Manutenções: as manutenções em equipamentos em período de garantia somente poderão ser realizadas pela assistência técnica autorizada; o rompimento do lacre do equipamento hospedado no Data Center somente poderá ser realizado por técnico da equipe de Infraestrutura e Recursos da SEAD, preferencialmente, na presença do responsável pelo equipamento; não é permitida a entrada e ou saída de peças, equipamentos e acessórios da sala do Data Center sem o prévio conhecimento e autorização. A entrada ou retirada de quaisquer equipamentos do Data Center somente se dará com o preenchimento do FORMULÁRIO DE AUTORIZAÇÃO DE SAÍDA E ENTRADA DE MATERIAIS, que deve ser enviado através do sistema SEI e, a autorização formal desse instrumento pelo responsável do Data Center;
VI. Reutilização e Alienação Segura: todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobre gravados com segurança; e
VII. Remoção de Propriedade: equipamentos, informações ou software não devem ser retirados do local sem a solicitação de retirada, expedida pelo gestor da instituição solicitante e, a ciência/autorização prévia por escrito do responsável do Data Center.
Seção XI
Da Segurança de Sistemas de Informação Corporativa
Subseção I
Da Aceitação de Sistemas
Art. 48. Devem ser seguidos os critérios de aceitação para novos sistemas, atualizações e novas versões e que sejam efetuados testes apropriados do(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação.
Subseção II
Da Aceitação de Recursos físicos
Art. 49. Deve ser seguido o critério de avaliação de disponibilidade para hospedagem e armazenamento.
Art. 50. Devem ser seguidos os critérios de aceitação para novos recursos e componentes (servidores, ativos de rede, armários), de modo que sejam novos, que estejam em linha de produção e fabricação, que ainda possuam pelo menos 3 anos de garantia a partir da data de hospedagem nos Data Center Corporativo, que havendo sistema operacional proprietário o mesmo deverá estar devidamente licenciado, assim como o solicitante deverá apresentar a relação de
todos os serviços, sistemas, aplicações de modo detalhado informando o tipo de licença de uso, e ainda, o gerenciamento e administração do recurso seja exclusivamente de modo remoto.
Seção XII
Da Operação
Art. 51. os procedimentos de operação devem ser documentados, mantidos atualizados e disponíveis a todos os que deles necessitem.
Art. 52. As modificações nos recursos de processamento da informação e sistemas devem ser controladas.
Art. 53. As funções e áreas de responsabilidade devem ser segregadas para reduzir as oportunidades de modificação ou uso indevido não auto-

rizado ou não intencional dos ativos da organização.
Art. 54. As cópias de segurança das informações e dos softwares devem ser efetuadas e testadas regularmente.
Seção XIII
Servidores
Art. 55. Os computadores servidores destinos hospedados no Data Center Corporativo devem:
I. Operar em conformidade com o acordo de nível de serviço; e
II. Dispor de mecanismo de redundância, em caso falha em um dos discos, controlado via hardware.
Parágrafo único. Os administradores do recurso obedecerão aos procedimentos previamente definidos.
CAPÍTULO III
DAS DISPOSIÇÕES FINAIS
Art. 56. Não serão permitidos programas não licenciados ou que infrinjam as leis nacionais, ou que coloquem em risco a integridade da rede pela introdução de vírus passiva ou ativa, ou incursões destrutivas de hackers e demais invasores, bem como façam valer a propagação de pirataria ou quaisquer técnicas consideradas ilegais.
Art. 57. Os colaboradores lotados nos setores vinculados às áreas de Infraestrutura e Recursos e de Redes e Telecomunicações da SEAD devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma à chefia imedita.
Art. 58. Em casos de quebra de segurança da informação por meio de recursos de TI, a SEAD deve ser imediatamente notificada a fim de adotar as providências necessárias, em observância ao art. 5º, inciso XXXIII da Constituição Federal, Lei Geral de Proteção de Dados, Código Penal Brasileiro em seu Título XI - Dos Crimes contra a Administração Pública - Capítulo I - Dos Crimes Praticados por Funcionário Público contra a Administração em Geral.
Art. 59. As notificações à SEAD devem ser feitas através do sistema SEI.
Art. 60. Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo “Penalidades” da Política de Segurança da Informação e Comunicações da SEAD no âmbito da Administração Estadual.
Art. 61. Os casos omissos e as dúvidas suscitadas quanto à aplicação desta norma serão dirimidas pelo Secretário da Administração, com o assessoramento das áreas técnicas de Infraestrutura e Recursos, e de Redes e Telecomunicações.
Art. 62. Esta Instrução Normativa entra em vigor na data de sua publicação.

Paulo Roberto Correia da Silva
Secretário de Estado de Administração
Decreto Estadual nº 08-P, de 1º de janeiro de 2023.

ANEXO I
Contrato de Acordo de Segurança da Informação e Proteção de Dados (ASIPD)
CLÁUSULA 1ª – O Contrato de Acordo de Segurança da Informação e Proteção de Dados (ASIPD) tem por objetivo estabelecer as diretrizes fundamentais a serem obedecidas, para proteger os dados e informações institucionais da gestão que estão sob a guarda da Secretaria de Estado de Administração - SEAD, bem como os sistemas e ativos que os mantêm.
CLÁUSULA 2ª - Este Contrato institui:
2.1 - Segurança da informação como garantia de que as informações estarão sempre protegidas, mantidas íntegras e disponíveis apenas àqueles com direito de acessá-las. Disciplinando a segurança da informação quanto aos controles físicos de acesso ao Datacenter Corporativo.
2.2 - Segurança cibernética como a preservação da confidencialidade, integridade e disponibilidade das informações no meio cibernético.
CLÁUSULA 3ª - Princípios Gerais para a Segurança dos Dados e Recursos Tecnológicos
3.1 – Classificação - Deve-se respeitar a classificação dos dados e informação atribuída pela SEAD, quando essa classificação não estiver disponível, deve-se tratar os dados, informações institucionais e recursos como confidenciais.
3.2 - Proteção - Os dados e informações de propriedade ou sob a guarda da SEAD devem ser protegidos, desde o momento de sua criação, contra acesso, modificação, subtração, destruição ou divulgação não-autorizada. Para tal, orientamos a utilização de mecanismos que garantam:
a) Confidencialidade: devem ser aplicados mecanismos de preservação da confidencialidade adequados para cada tipo de dado e informação transmitido, processado ou armazenado, evitando sua utilização indevida.
b) Integridade: devem ser aplicados mecanismos de preservação da integridade adequados para cada tipo de dado e informação transmitido, processado ou armazenado, evitando sua adulteração.
c) Autenticidade: devem ser aplicados mecanismos de preservação da autenticidade, adequados para cada tipo de dado e informação transmitido, processado ou armazenado, garantindo sua legitimidade e não-repúdio.
d) Disponibilidade: devem ser mantidas cópias de segurança dos dados e informações utilizados por sistemas críticos, em ambientes protegidos e gerenciados, mantendo a disponibilidade aos seus proprietários em caso de necessidade de restauração por período razoável de tempo.
e) Rastreabilidade: devem ser aplicados mecanismos adequados para cada tipo de dado e informação a ser protegido, e informações de rastreabilidade devem ser mantidas por tempo razoável, conforme as necessidades de auditoria e atendimento às legislações vigentes.
f) Outras proteções: declaradas nos demais Princípios ao longo desse Contrato.
3.3 - Sigilo Profissional - Os colaboradores do Terceiro devem manter absoluto sigilo profissional, zelando pela proteção dos dados, informações e recursos pertencentes ou sob a guarda da SEAD, a que tenham acesso.
3.3.1 - Não é permitida a gravação de conversas dentro dos ambientes: Data Center, POP (Point of Presence) ou Anti-Sala do Data Center, NOC (Núcleo de Operações e Controle), salvo com expressa autorização para assim proceder. Por analogia, também não é permitida a gravação de reuniões envolvendo assuntos contratuais da SEAD, nas dependências de Terceiros.
CLÁUSULA 4ª - Gestão de Acesso e proteção Física do Ambiente
4.1 - As partes concordaram em celebrar este Acordo de Proteção de Dados, doravante denominado como “DPA”, para confirmar as regras de proteção de dados relativas ao seu relacionamento, bem como para cumprir os requisitos da Legislação de Proteção de Dados aplicável.
4.2 - Os locais onde estão instalados os Data Centers corporativos são considerados parte crítica da sua infraestrutura tecnológica, razão pela qual o cuidado com a proteção e segurança deve ser obrigatoriamente redobrado. Por esse motivo, o acesso físico será restrito àquelas pessoas previamente autorizadas pela SEAD.
4.3 - Acessos permanentes serão permitidos somente aos servidores ou prestadores de serviços indicados e autorizados pela SEAD, que tenham a necessidade de acesso liberado para executar suas atividades.
4.4 - Acessos temporários poderão ser permitidos somente aos servidores ou prestadores de serviços autorizados pela SEAD, mediante avaliação da justificativa de solicitação prévia, e estão sujeitos a uma política de acesso com privilégios mínimos, o que significa que o acesso ao Data Center é restrito aos servidores ou prestadores de serviços indicados e autorizados pela SEAD com uma necessidade de negócios comprovada e aprovada, sem mais acesso do que o necessário ao concedido para executar suas atividades.
4.5 - Acessos temporários por outros servidores ou terceirizados externos somente poderão ocorrer com autorização prévia da SEAD desde que, para fins de controle, o acesso seja registrado pela equipe de Infraestrutura e Recursos da SEAD (nome, data e hora, justificativa) e o servidor ou terceirizado seja acompanhado em tempo integral por servidor designado pela SEAD.
4.6 - Acessos solicitados por outras instituições públicas ou privadas, somente poderão ser autorizados pela SEAD, desde que possuam contrato vigente com a instituição solicitante e/ou que a solicitante apresente declaração formal expedida pelo responsável da pasta vínculo funcional, técnico ou operacional com o colaborador indicado, que sejam acompanhados em tempo integral por pessoa designada pelo solicitante e que justifique a necessidade do acesso.
4.7 - O acesso ao Data Center corporativo limita-se à:
a) 01 membro da equipe de Infraestrutura e Recursos;
b) 01 membro da equipe de Redes Corporativas;
c) 01 membro da instituição solicitante.
4.8 - Durante o acesso físico ao Data Center o servidor ou terceirizado, interno ou externo, não poderá:
a) Adentrar nas dependências do Data Center sem identificação e autorização prévia;
b) Portar, no local de armazenamento do Data Center, alimentos, líquidos, materiais inflamáveis ou qualquer utensílio que possa danificar os equipamentos;
c) Introduzir ou retirar equipamentos da sala do Data Center, a menos que haja autorização prévia e por escrito pela SEAD;
d) Realizar a gravação de vídeos ou a captura de imagens dentro das dependências do Data Center e no seu perímetro; e
e) As portas deverão permanecer sempre fechadas durante a permanência dentro da sala do Data Center.
4.9 - Os registros de acesso ao Data Center serão mantidos na forma de solicitações aprovadas. As solicitações só poderão ser aprovadas pela SEAD, e todas as solicitações de acesso aos Data Centers serão registradas e disponibilizadas para quaisquer investigações futuras.
CLÁUSULA 5ª - Este contrato prevê que posterior ao acesso ao Data Center corporativo fica estabelecido o cumprimento formal da não divulgação a terceiros, sobre informações a que tiver acesso durante a visita ao ambiente, em observância ao art. 5º, inciso XXXIII da Constituição Federal, Lei Geral de Proteção de Dados, Código Penal Brasileiro em seu Título XI - DOS CRIMES CONTRA A ADMINISTRAÇÃO PÚBLICA - CAPÍTULO I - DOS CRIMES PRATICADOS POR FUNCIONÁRIO PÚBLICO CONTRA A ADMINISTRAÇÃO EM GERAL.
CLÁUSULA 6ª - A assinatura deste contrato é condicionante para a au-

torização de acesso ao Data Center.
Declaro estar CIENTE e de ACORDO com os termos do Acordo de Segurança da Informação e Proteção de Dados (ASIPD).

_____

Nome
Cargo
Órgão

ANEXO II

FORMULÁRIO DE AUTORIZAÇÃO DE SAÍDA E ENTRADA DE MATERIAIS			
	Entrada	Data:	
	Saída	Data:	
1. IDENTIFICAÇÃO DO SOLICITANTE			
Nome Completo do Solicitante:			
CPF:		Telefone para contato:	
Cargo:			
Órgão/Setor:			
Responsável pelo Setor:			
2. DESCRIÇÃO DOS ITENS A SEREM DESLOCADOS			
QTD	Itens		Patrimônio/Serial Number
OBSERVAÇÕES:			
_____ _____ _____ Assinatura do Solicitante Assinatura do Aprovador			
Rio Branco – Acre, _____ de _____de 20_____.			

ESTADO DO ACRE
SECRETARIA DE ESTADO DE PLANEJAMENTO E GESTÃO

EXTRATO DA ATA DE REGISTRO DE PREÇOS Nº 02/2024
PROCESSO SEI Nº 0006.016657.00003/2023-68
PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOS Nº 259/2023
OBJETO: Contratação de empresa especializada na execução de serviços de infraestrutura de telecomunicações, visando futura e eventual instalação para interconectividade, manutenção preventiva e corretiva em rede de fibra óptica do Estado do Acre, sob demanda da CONTRATANTE, com fornecimento de material necessário ao pleno funcionamento do serviço, possibilitando a continuidade dos serviços de Comunicação de Dados, conforme especificações contidas no Termo de Referência.
DA VIGÊNCIA: A vigência da Ata de Registro de Preço será de 12 (doze) meses contados da data da sua assinatura, com eficácia legal após a da data da publicação do seu extrato no Diário Oficial do Estado do Acre, tendo início e vencimento em dia de expediente, devendo-se excluir o primeiro e incluir o último.
É vedado efetuar acréscimos nos quantitativos fixados pela ata de registro de preços, inclusive o acréscimo de que trata o § 1º do art. 65 da Lei nº 8.666, de 1993.
Os contratos decorrentes do Sistema de Registro de Preços deverão ser assinados no prazo de validade da ata e poderão ser alterados, desde que verificado o disposto no art. 65 da Lei nº 8.666, de 1993.”
A publicação resumida do instrumento de Ata de Registro de Preços é condição indispensável para sua eficácia, será providenciada pela Administração até o quinto dia útil do mês seguinte ao de sua assinatura, para ocorrer no prazo de vinte dias daquela data, no Diário Oficial do Estado do Acre
DOS PREÇOS REGISTRADOS

Fornecedor: APC TECNOLOGIA E ENGENHARIA LTDA EPP – CNPJ: 11.241.567/0001-76 END. SHN QUADRA 01 CONJUNTO A LOTE A SALA 520 – ASA NORTE – BRASÍLIA/DF, CEP: 70.701-000 Contato: (61) 3426-7500. Representante Legal: Ana Clara de Almeida Pedrosa.					
Lote 01 – Serviços/materiais de infraestrutura de telecomunicações					
Serviço sob demanda					
Item	Descrição do Serviço	Métrica	Quantidade para registro	Valor Unitário	Valor Total
1	Serviços de Fusões de Fibra Óptica	unidade	4.000	R$ 70,00	R$ 280.000,00
2	Serviço de infraestrutura de telecomunicações	hora técnica	1.000	R$ 200,00	R$ 200.000,00
3	Serviço de diagnóstico com uso de reflectômetro óptico no domínio do tempo (OTDR)	unidade	4.000	R$ 45,00	R$ 180.000,00
4	Serviços de projeto executivo Externo com compartilhamento de infraestrutura	metro linear	50.000	R$ 5,00	R$ 250.000,00
5	Serviços de projeto executivo Interno	unidade	30	R$ 1.000,00	R$ 30.000,00
6	Serviços de atualização "As Built" Externo dos projetos com compartilhamento de infraestrutura	metro linear	50.000	R$ 2,50	R$ 125.000,00
7	Serviços de atualização "As Built" Interno dos projetos	unidade	30	R$ 500,00	R$ 15.000,00
8	Serviço de abertura e fechamento de vala por metro – MD SOLO BRUTO	metro linear	500	R$ 120,00	R$ 60.000,00
9	Serviço de abertura e fechamento de vala por metro – MD SOLO ASFÁLTICO	metro linear	200	R$ 250,00	R$ 50.000,00
10	Serviço de perfuração com Método não destrutivo - MND	metro linear	100	R$ 320,00	R$ 32.000,00
11	Serviço de lançamento de PEAD 40mm liso específico de telecomunicações ou similares em valas e perfurações	metro linear	800	R$ 30,00	R$ 24.000,00
12	Serviço de lançamento de Cabo Óptico subterrâneo de 48 Fibras	metro linear	2.000	R$ 34,00	R$ 68.000,00
13	Serviço de lançamento de Cabo Óptico subterrâneo de 36 Fibras	metro linear	2.000	R$ 30,00	R$ 60.000,00
14	Serviço de lançamento de Cabo Óptico subterrâneo de 24 Fibras	metro linear	2.000	R$ 25,00	R$ 50.000,00
15	Serviço de lançamento de Cabo Óptico subterrâneo de 12 Fibras	metro linear	2.000	R$ 22,00	R$ 44.000,00
16	Serviço de lançamento de Cabo Óptico subterrâneo de 4 Fibras	metro linear	2.000	R$ 20,00	R$ 40.000,00
17	Serviço de lançamento de Cabo DROP Óptico subterrâneo de 2 Fibras	metro linear	2.000	R$ 11,00	R$ 22.000,00
18	Serviço de lançamento de Cabo Óptico aéreo de 48 Fibras Autosustentado para vão de 80 metros	metro linear	2.000	R$ 34,00	R$ 68.000,00