



ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO Nº 0565232 / 2023 - PRESI/DG/STI/CIE/SEREDE

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

1. ANÁLISE DE VIABILIDADE TÉCNICA

1. Justificativa

- A demanda se justifica pela necessidade de equipar o parque tecnológico do TRE/AC com total eficiência com foco na continuidade do serviço público, por meio de solução que garanta eficiência, confiabilidade, segurança e robustez, o que resultará em alto desempenho e disponibilidade dos backups (cópias de segurança). Dessa forma, é essencial ao adequado funcionamento da estrutura de backup, a aquisição de itens com a integração e compatibilidade com as soluções de storage, bancos de dados e gerenciadores de máquinas virtuais, o que proporcionará bom aproveitamento do investimento já aplicado nessas soluções.
- O TRE/AC possui a solução de backup comercial Arcserve UDP 6.5, que é utilizado para realizar backups do Exchange 2013, e Active Directory, que rodam em windows servers 2012, que findarão o suporte do fabricante, em abril de 2023, caso do exchange 2013, e em outubro do corrente ano, no caso do windows 2012 R2. A atual ferramenta de backup utilizado para os serviços de TI citados, não oferece suporte aos sistemas operacionais mais novos, tornando-se um impeditivo à atualização destes serviços, explicando melhor, não conseguiremos atualizar o sistema operacional windows server 2012 para windows server na versão 2019, pois a atual ferramenta de backup não oferece suporte para a nova versão do sistema operacional citado, o mesmo acontece com o software Microsoft Exchange 2013.
- A situação se complica, pois os sistemas citados anteriormente cessam o suporte por parte do fabricante, em meados de abril deste ano (2023), caso do Sistema de Correio Eletrônico Microsoft Exchange, e em outubro deste ano, no caso do Microsoft Windows Server 2012 R2, podendo levar a infraestrutura informatizada do TRE/AC a riscos cibernéticos inaceitáveis.
- A ser assim, torna-se necessária a atualização das ferramentas de backup, para que possamos realizar a atualização dos sistemas operacionais que suportam importantes e críticos serviços de TI (Active Directory e Servidor de emails, Exchange 2013).
- Por outro lado, este Tribunal já se utiliza de ferramentas de backup comunitárias, para realização de backups de outros serviços como bancos de dados oracle, mysql, servidores linux, e etc.. A citada ferramenta comunitária é o software Bacula Backup System community, que está em produção, há mais de 4 anos, e a aquisição da licença de uso comercial proporcionará o reaproveitamento de todos os backups já realizados, dispensando a necessidade de qualquer processo de migração ou conversão.**
- Outro ponto a ressaltar é o total aproveitamento do conhecimento já adquirido com o uso da versão atual, o que torna a curva de aprendizado da solução, muito mais suave, diferente de uma nova solução, na qual seria necessário a execução de todo o processo de migração e aprendizado sem falar na conversão dos backups já realizados ou manutenção de um sistema legado até o final do ciclo de vida dos dados backupados.**
- O licenciamento é necessário para que novas facilidades, funcionalidades não disponíveis na versão comunitária sejam incorporadas ao processo de proteção dos dados de forma a facilitar o processo de recuperação dos dados quando da necessidade de recuperação de desastres quer sejam ocasionados por falha ou por resultado de ataques cibernéticos, a exemplo dos danos já causados por *ransomware* em outras instituições.
- As novas funcionalidades a serem alcançadas com a aquisição da versão comercial são as seguintes:
 - Backup e restauração usando a tecnologia conhecida como "bare metal", tanto para servidores linux, quanto para servidores windows, o que garante rápida restauração em caso de sinistros
 - Backup de máquinas virtuais Xenserver (nosso Hypervisor), aqui há um detalhe, **desconhecemos outro software capaz de realizar backup de máquinas virtuais xenserver, com a metodologia "agentless", que agregue também o envio direto dos dados de backup para fita;**
 - Backup de Active Directory e Exchange server com restore granular, e restauração de desastres habilitado, bem como backup diretamente para fita, algo inexistente em nossa ferramenta atual (Arcserve UDP 6.5);
 - Backup e restauração do SGBD Oracle, integrado ao RMAN.
- Relação entre a demanda prevista e a quantidade de serviço a ser contratado**
 - Para atendimento da demanda da implantação de sistema de backup corporativo, será necessária a aquisição de apenas 01 unidade do software Bacula Enterprise Backup Server e demais plugins de acordo com as necessidades do Tribunal, quais sejam:
 - Backup e restauração bare metal de máquinas linux e windows
 - Backup e restauração de máquinas virtuais xenserver, utilizando a tecnologia "agentless";
 - Backup e restauração do Active Directory;
 - Backup e restauração do Exchange Server (VSS)
 - Backup e restauração do SGBD Oracle, integrado ao RMAN.

3. Demonstrativo dos resultados a serem alcançados em termos de economicidade e eficiência

- Ao fim da aquisição e implantação da solução seriam obtidos resultados satisfatórios pelos próximos 03 anos, em termos de backup e restauração das mais diversas tecnologias em uso no Regional, com garantia de atualização pelo período citado.
- Considerando a atual conjuntura econômica e seu processo de recuperação, o qual deverá ser lento, além do escasso orçamento, a aquisição das aludidas licenças garantirão que a justiça eleitoral do TRE/AC possa manter seus serviços protegidos atendendo a necessidade da continuidade do serviço público;

4. Alinhamento ao planejamento estratégico e planejamento de Tecnologia da informação e comunicação

- A contratação em tela está em harmonia com os seguintes itens do PDTI (0439644):

PTS - Segurança da Informação e Proteção de Dados

ID da Ação	Identificação dispositivo legal	Tema/ Grupo	Descrição das Ações	Procedimento (Como será realizado?)	Data de Início	Data de Término	Responsável pela Execução no Órgão
PTS-01	ENSEC-JUD - Art. 19 II	Grupo 3: Segurança da informação e proteção de dados	Definir e manter Política de Segurança da informação (PSI)	1. Acompanhar a aprovação da Política de Segurança da Informação de Justiça Eleitoral (PSI-JE) em consonância com os objetivos institucionais, da área de TIC e segurança da informação. 2. Disseminar, no âmbito do TRE/AC, a PSI-JE.	julho / 2021	dezembro / 2021	CSI / STI
PTS-02	ENSEC-JUD - arts 21	Grupo 3: Segurança da informação e proteção de dados	Revisar o ato de constituição do Comitê Gestor de Segurança da Informação multidisciplinar, conforme orientação do CNU	1. Revisar o ato de instituição do Comitê Gestor de Segurança da Informação multidisciplinar, considerando a ENSEC-JUD	julho / 2021	dezembro / 2021	STI
PTS-03	ENSEC-JUD - Portaria CNU 142/2021	Grupo 3: Segurança da informação e proteção de dados	Definir processo de gestão de incidentes de serviços de tecnologia de informação	1. Estabelecer e formalizar processo de gestão de incidentes que: a) contenha regras para a priorização e o escalamento de incidentes; b) considere os níveis de serviços especificados em acordos com as áreas clientes; c) gere base de conhecimento sobre erros conhecidos e problemas são utilizadas como insumos na resolução de incidentes; d) defina responsabilidades 2. Elaborar o Plano de Gestão de Incidentes Cibernéticos, com, no mínimo, a categoria do incidente, a indicação do procedimento de resposta específico e a severidade (exemplo Anexo I da Portaria 290)	julho / 2021	julho / 2022	ETIR
PTS-04	ENSEC-JUD - Portaria CNU 142/2021	Grupo 3: Segurança da informação e proteção de dados	Revisar a PCN - Política de Continuidade de Negócios	Definir e Publicar o PCN e os principais procedimentos	agosto / 2021	agosto / 2021	Membros da CSI e COSET
PTS-05	ENSEC-JUD - Portaria CNU 142/2021	Grupo 3: Segurança da informação e proteção de dados	Criar/revisar a Política de Gestão de Riscos de Segurança da Informação	Definir e Publicar a Política de Gestão de Riscos de Segurança da Informação	dezembro / 2021	dezembro / 2021	Membros da CSI e COSET
PTS-06	ENSEC-JUD - Portaria CNU 142/2021	Grupo 3: Segurança da informação e proteção de dados	Criar o Comitê de Crises Cibernéticas	Definir e Publicar portaria com os membros do Comitê de Gestão de Crises Cibernéticas	maio / 2021	maio / 2021	CSI e COSET
PTS-07	ENSEC-JUD - Portaria CNU 142/2021	Grupo 3: Segurança da informação e proteção de dados	Treinamentos Técnicos para equipes de TI	Contratação de treinamentos com empresas especializadas	dezembro / 2022	dezembro / 2022	STI

1.

ID da Ação	Identificação do dispositivo da Resolução	Tema/ Grupo	Descrição das Ações	Procedimento (Como será realizado?)	Data de Início	Data de Término	Responsável pela Execução no Órgão
PTE-12	Art. 36	Grupo 3: Segurança da informação e proteção de dados	Implementar a Gestão de Continuidade de Serviços Essenciais de TIC	1. Revisar a Política de Gestão de Continuidade de serviços essenciais de TIC, com papéis e responsabilidades; 2. Revisar o processo de gestão da continuidade dos serviços essenciais de TIC; 3. Realizar nova avaliação dos serviços críticos contemplados no PCN; 3. atualizar, testar e implementar o plano de continuidade de serviços essenciais de TIC;	agosto/2021	dezembro/2021	CSI
PTE-13	Art. 37	Grupo 3: Segurança da informação e proteção de dados	Manter o plano de Gestão de Riscos de Segurança de TIC	1. Estabelecer / Revisar o processo de gestão de riscos de Segurança de TIC (Estudar o Processo de Gerenciamento de Riscos existente e reformulá-lo para abranger riscos de Segurança da Informação) 2. Elaborar / Revisar Plano de Gestão de Riscos de TIC, com foco na continuidade do negócio e manutenção dos serviços; 3. Implementar controles; 4. Definir e comunicar os papéis e as responsabilidades na gestão de riscos; 5. Reuniões dos Comitês com decisões baseadas em análise de riscos; 1. Elaborar Plano de Gestão de Riscos com foco na proteção de dados pessoais;	julho/2021	julho/2022	CSI / STI
PTE-14	Art. 38	Grupo 3: Segurança da informação e proteção de dados	Fomentar adesão a práticas e processos de segurança da informação e proteção de dados	Execução do PTS (plano de trabalho de Segurança, atendendo a Resolução CNU 396/2021 e Portaria 162/2021, e normativos da LGPD)	junho/2021	julho/2022	CGPD / CSI / STI
PTE-15	Art. 41	Grupo 3: Segurança da informação e proteção de dados	Constituir um Comitê Gestor de Proteção de Dados Pessoais (Resolução 363/2021, art. 20, III)	Instituir o Comitê Gestor de Proteção de Dados Pessoais.	agosto/2021	dezembro/2021	GAPRES

2.

PTS - **Segurança** da Informação e Proteção de Dados

ID da Ação	Identificação do dispositivo legal	Tema/ Grupo	Descrição das Ações	Procedimento (Como será realizado?)	Data de Início	Data de Término	Responsável pela Execução no Órgão
PTS-08	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Criação de protocolos complementares de gerenciamento de crises cibernéticas	Discussão das propostas na CSI e com as áreas técnicas afetadas, como STI	dezembro / 2021	dezembro / 2021	CSI
PTS-09	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Elaborar norma técnica para gerenciamento de logs	1. Elaborar norma técnica que determine os eventos, o tempo de guarda, as ferramentas usadas e procedimentos de gestão dos logs; 2. Apresentar proposta para CSI e posterior avaliação da COSET	dezembro / 2021	dezembro / 2021	CSI
PTS-10	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Criar servidor de LOGS centralizado	Utilizar ferramenta open source e padrão de mercado como o SYSDLOG-NG	dezembro / 2021	dezembro / 2021	Membros da CSI e da STI e gestores de infraestrutura
PTS-11	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Criação de protocolos complementares para investigação de ilícitos cibernéticos	Apresentação da proposta da CSI e posterior avaliação da COSET	dezembro / 2022	dezembro / 2022	CSI - Gestor de Segurança da Informação
PTS-12	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Revisão das permissões de usuários em sistemas, serviço de diretório e bancos de dados	Levantamento dos ativos, revisão dos usuários e suas permissões	dezembro / 2021	dezembro / 2021	Gestores de áreas técnicas de infraestrutura, sistemas e bancos de dados
PTS-13	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Atualização de sistemas legados	Levantamento dos ativos obsoletos, sem atualização recente ou com falhas de segurança. Após, atualização ou descontinuação do ativo	dezembro / 2022	dezembro / 2022	Gestores de áreas técnicas de infraestrutura, sistemas e bancos de dados
PTS-14	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Implementação de solução para gestão de identidades	Levantar bases de usuários, interoperabilidade com serviço de SSO (Single-sign-on), adquirir ferramenta de IAM, caso necessário	dezembro / 2022	dezembro / 2022	CSI - Gestores de áreas técnicas de infraestrutura, sistemas e bancos de dados
PTS-15	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Implementação de solução para gestão de acesso privilegiado	Finalização da implementação da ferramenta guacamole, bem como adoção de novas ferramentas	julho / 2021	dezembro / 2022	CSI - Gestores de áreas técnicas de infraestrutura, sistemas e bancos de dados
PTS-16	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Implementação de ferramentas de segurança, como IDS/IPS/GSI/SIEM/antivírus no proxy de navegação	Analisar e implementar ferramentas open source e de mercado	dezembro / 2022	dezembro / 2022	CSI/STI - Gestores da área de infraestrutura
PTS-17	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Reconfiguração de nossa infraestrutura de backup	Adquirir ativos necessários	dezembro / 2021	dezembro / 2021	CSI/STI - Gestores da área de infraestrutura
PTS-18	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Atualização dos servidores de correio eletrônico microsoft exchange 2013 e office	Adquirir os softwares necessários	dezembro / 2021	dezembro / 2021	STI/CIE - Gestores da área de infraestrutura
PTS-19	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Confeção de um ambiente de contingência ativo-ativo, bem como reestruturação do datacenter principal	Proceder a criação de um minidatacenter na CAE, estender o cluster principal para o datacenter citado	dezembro / 2021	dezembro / 2021	CSI/STI - Gestores da área de infraestrutura

3.

PTS - **Segurança** da Informação e Proteção de Dados

ID da Ação	Identificação dispositivo legal	Tema/ Grupo	Descrição das Ações	Procedimento (Como será realizado?)	Data de Início	Data de Término	Responsável pela Execução no Órgão	
PTS-20	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Realizar incrementos de segmentos de rede para proteger os ativos de informação mais críticos e as interfaces de gerenciamento	Analisar estratégias para incrementar redes isoladas	abril / 2021	abril / 2021	CSI/STI - Gestores da área de infraestrutura	
PTS-21	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Implementar Firewall de Aplicações Web (WAF)	Analisar ferramentas de mercado e implementar o uso do firewall externo do TSE para aplicações acessíveis pela Internet	dezembro / 2021	dezembro / 2021	CSI/STI - Gestores de áreas técnicas de infraestrutura e de sistemas	
PTS-22	ENSEC-JUD Art. 10	Grupo 3: Segurança da informação e proteção de dados	Realizar a gestão de Segurança da Informação	Estabelecer o Sistema de Gestão da Segurança da Informação baseado em riscos	julho / 2021	julho / 2022	CSI E COSET	
PTS-23	Política de Segurança da Informação	Grupo 3: Segurança da informação e proteção de dados	Definir processo de gestão de vulnerabilidades técnicas de TI relacionada à segurança da informação	1. Estabelecer processo de gestão de vulnerabilidades; 2. Implantar ferramenta open source para gestão de vulnerabilidades;	julho / 2021	julho / 2022	CSI	
PTS-24	Plano de ação da LGPD	Grupo 3: Segurança da informação e proteção de dados	Revisar política de backup	Garantir alinhamento com LGPD	verificação de conformidade da retenção de dados corrente	julho / 2021	julho / 2022	CSI
PTS-25	Plano ação LGPD	Grupo 3: Segurança da informação e proteção de dados	Revisão ou Proposição de procedimentos técnicos de segurança e ferramentas para adequação à LGPD	Revisão de procedimentos e ferramentas com o objetivo de obter controle de dados aderentes à LGPD	julho / 2021	julho / 2022	CIE	
PTS-26	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Instalar ferramenta de detecção de intrusão	Estudar ferramentas disponíveis; instalar em ambiente de homologação; Avaliar impacto e riscos da instalação no ambiente em produção	julho / 2021	julho / 2022	CIE	
PTS-27	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Habilitar modelo de portas seguras na rede lógica (port security)	Realizar estudo para escolha de modelo e avaliar impacto na implantação	julho / 2021	julho / 2022	CIE	
PTS-28	ENSEC-JUD - Portaria CNU 162/2021	Grupo 3: Segurança da informação e proteção de dados	Aplicar modelo de hardening dos servidores, infraestrutura de sistema operacional seguro	Realizar estudo para escolha de modelo e avaliar impacto na implantação	julho / 2021	julho / 2022	CIE	

4.

5. Requisitos da Contratação

1. Requisitos legais

1. A presente contratação deve observar as seguintes leis e normas:

1. Lei nº 8.666/93, de 21 de junho de 1993, que institui normas para licitação e contratos da Administração Pública.
2. Lei nº 8.248/91, de 23 de outubro de 1991, que dispõe sobre a capacitação e competitividade do setor de informática e automação e
3. Resolução CNJ nº 182/2013

2. Requisitos tecnológicos

1. Deverá possuir mecanismos contra ransomware, incluindo:

1. Processos de backup e restauração dedicados;
2. Volumes de backup imutáveis;
3. Catálogo externo;
4. Antivírus integrado com detecção de ransomware;
5. Conexão socket própria;
6. Suporte nativo desde a concepção de gravação direta em todas as fitas, cartuchos, VTL, WORM, etc
7. Estado do volume de backup Append Only.

2. Deverá suportar deduplicação de dados tanto no lado do cliente sendo protegido quanto do lado do servidor de backup. Este suporte deve valer para Linux e Windows, tanto para VMs quanto para servidores "bare metal";

3. Deverá armazenar o catálogo de backup em banco de dados relacional na VM fornecida;

4. Deverá suportar compactação nos backups;

5. Deverá suportar criptografia nos backups;

6. Deverá suportar backup de máquinas virtuais (VMs) para os ambientes Xenserver, com as seguintes características:
 1. Suporte a VMs Linux e Windows Server;
 2. Permitir backups incrementais das VMs. Será aceita solução que apresente ou backup incremental a nível de arquivo ou a nível de bloco, via deduplicação;
 3. Permitir restaurações de arquivos individuais ou pastas dos guests das VMs;
 4. Permitir backups e restaurações completas das VMs;
 5. Não serão aceitas políticas de backup das VMs que exijam backups “redundantes”. Por exemplo, um backup sendo feito via agente instalado dentro da VM e outro via “API” do virtualizador.
 6. Um backup único deverá garantir tanto a restauração completa do filesystem da VM em caso de desastre quanto a restauração granular de arquivos da citada VM;
 7. Em caso de perda total de uma VM, sua restauração completa diretamente no virtualizador deverá ser feita de forma automatizada, sem a necessidade de instalação prévia de um sistema operacional, e deverá ser restaurada com a mesma configuração de memória, CPUs e particionamento de discos que possuía antes do desastre;
 8. Deverá possuir console gráfica central que permita: Configuração do ambiente;
 9. Agendamento e execução de backups e restaurações de servidores “bare metal”, VMs e bancos de dados;
 10. Monitoramento em tempo real do andamento de backups de servidores “bare metal”, VMs e bancos de dados;
 11. Execução imediata de restaurações, mesmo que o servidor de onde foi feito o backup não esteja no ar;
 12. Instalação de agentes de backup em novos servidores;
 13. Geração de relatórios gerenciais que contenham pelo menos os backups com sucesso, backups com falha, volume de backup realizado, ocupação no destino de backup;
 14. Os backups feitos do data center principal deverão ser copiados para o data center secundário. Tal cópia deve poder ocorrer tanto imediatamente após o fim do backup, quanto em horário programado;
7. Deverá suportar recuperação de desastre de servidores “bare metal” Windows ou Linux sem a necessidade de instalação prévia de sistema operacional em tais servidores, utilizando uma mídia especial - que deverá ser fornecida pelo licitante - para boot e recuperação em tais servidores, ou então fazendo boot e recuperação no servidor via rede;
8. Deverá fornecer agentes especializados (plugins) para backups dos seguintes ambientes:
 1. Backup e restauração de Bancos de dados Oracle, integrando-se a ferramenta RMAN;
 2. MS Active directory;
 3. Microsoft Exchange Server
 4. Deverá fornecer agente especializado (plugin) para ambiente de virtualização Xenserver;
 5. Deverá fornecer agente especializado (plugin) para ambiente de virtualização Proxmox;
 6. Deverá fornecer agente especializado (plugin) para ambiente Docker;
 7. Deverá possuir plugin para fazer backups e restaurações em nuvem;
 8. Deverá possuir suporte, via interface web ou plugin instalado em estações windows, para que o próprio usuário possa restaurar seus backups;
 9. Deverá possibilitar backups e restaurações utilizando múltiplos canais simultâneos;
9. Em caso de descontinuidade da solução, por qualquer motivo que seja, inclusive fim do contrato, deverá ser fornecida ferramenta que permita restauração dos backups armazenados na solução. O uso de tal ferramenta deverá ser feito por um mínimo de 180 (cento e oitenta) dias;
10. Deverá permitir a instalação de media servers adicionais sem acréscimo no custo do licenciamento;
11. A instalação do software de backup, assim como seus softwares de apoio (sistema operacional, banco de dados, etc), deverá ser feita pelo fornecedor do software de backup. O suporte que seja necessário a tais softwares adicionais deverá ser prestado pelo fornecedor da solução de backup ou por outra empresa por ele indicada;
12. Toda a configuração e migração do ambiente de backup, incluindo políticas de retenção, agendamento de backups, cópia dos backups entre o armazenamento primário e secundário, e outras configurações, deverá ser feita pelo fornecedor em conjunto com os técnicos deste Tribunal;
13. A configuração dos agentes e plugins de backup nos diversos servidores a serem protegidos, inclusive no ambiente de virtualização, deve ser efetuada pelo fornecedor;
14. Deverá ser fornecido um treinamento de no mínimo 24 (vinte e quatro) horas na solução, nas dependências deste Tribunal, após a instalação e configuração do ambiente;
15. Deverá ser possível abrir chamados de suporte tanto via interface web quanto via telefone. O número de chamados não poderá ser limitado. O fornecedor deverá fornecer qualquer tipo de suporte que seja relacionado à solução, como por exemplo: esclarecimento de dúvidas, configurações no ambiente, apoio a melhorias, problemas de performance, etc.
16. O suporte deverá poder ser fornecido tanto em modalidade 8x5, em casos mais simples, quanto em modalidade 24x7, em caso de problemas críticos. O início de atendimento deverá ocorrer no máximo 2 (duas) horas após a abertura do chamado;
17. A instalação deverá ser feita num prazo máximo de 30 (trinta) dias contados da ORDEM DE SERVIÇO a ser emitida pela Seção de Infraestrutura e Comunicação.
18. O recebimento provisório será dado após a instalação inicial do ambiente.
19. O recebimento definitivo e o início do período de garantia deverão ocorrer após o ambiente estar em produção.

6. Levantamento das alternativas de TI

1. Foram identificados 3 caminhos, ou soluções possíveis para atendimento da demanda levantada neste documento:

1. Solução 01:

1. Contratação de empresa especializada no fornecimento de software de backup Arcserve UDP, versão mais atual.

1. Trata-se da contratação de software de backup Arcserve, porém este tecnicamente menos compatível com as necessidades da infraestrutura tecnológica do TRE/AC, pois:

1. A solução não tem a capacidade de realizar backup "sem agente" nos hypervisores Xenserver (que é a solução de virtualização amplamente utilizada pelo TRE/AC)
2. A solução não tem a capacidade de enviar backups diretamente pra fita (em tempos de *ransomware* é imprescindível), necessita sempre de uma área para backup em disco, para dar condições de backup em fita, deve ser adquirido outro software, que é o Arcserve Backup, trazendo mais complexidade ao sistema.
3. O formato dos arquivos de backup é proprietário, realizando, por conta disso, o "aprisionamento tecnológico".

2. Considerando o elencado acima, a Solução 01 não é uma solução viável ou oportuna para o Regional, e não traria nenhum benefício ao ambiente atual.

2. Solução 02:

1. Contratação de uma nova solução de backup corporativo:

1. Trata-se de contratação de uma nova solução de backup corporativo, como o software Veeam

1. A solução elencada, apesar de se tratar de uma solução empresarial, não traz a capacidade realizar backup "sem agente" nos hypervisores da família Xenserver (que é a solução de virtualização amplamente utilizada no TRE/AC, tanto na sede quanto nos cartórios)
2. A solução não tem a capacidade de enviar backups diretamente para fita, concomitante com funcionalidade de backup bare metal, a não ser que se use de protocolos proprietários como o catalyst da HP, o que leva, no nosso entendimento a um aprisionamento tecnológico inapropriado.
3. O formato dos arquivos de backup é proprietário, realizando, por conta disso, o "aprisionamento tecnológico".
4. Como não tem a funcionalidade de realizar backups sem agente nos hypervisores xenserver, teríamos que instalar agente o agente da solução em cada vm, individualmente, trazendo um retrabalho incompatível com as demandas tecnológicas modernas, posto que outras soluções, realizam o backup de todas as vms do hypervisor sem a necessidade de instalação do agente nas máquinas virtuais (guest).
5. outra questão é que a solução de backup geralmente não tem compatibilidade com os mais diversos sistemas operacionais rodando em máquinas virtuais, no nosso caso para citar um exemplo, não proporcionaria o backup em máquinas virtuais que rodam em cima de FreeBSD (sistema operacional que utilizamos em nosso parque)
6. **Não menos importante, a solução em questão, tem o custo estimado em R\$ 965.402,00 (0564964), um valor bastante elevado,**

considerando o custo da solução 03

2. Considerando o explanado acima, a solução 02 não é um caminho viável a ser seguido por nosso Regional, no tocante a software de backup.

3. Solução 03:

1. Contratação de empresa especializada para fornecimento e implantação do software Bacula Enterprise Backup Server, por meio da adesão a ata de registro de preços do TRE/RR (0560743), da qual o TRE/AC é partícipe.

1. Tecnicamente, a contratação em tela se adequa perfeitamente às necessidades tecnológicas do Tribunal Regional Eleitoral do Acre, pois:

1. Tem a propriedade de realizar backups de máquinas virtuais, com tecnologia agentless de hypervisores Xenserver (Hypervisor utilizado no datacenter do Tribunal Regional Eleitoral do Acre)
2. Possui a possibilidade de enviar os backups diretamente para fitas (**faculdade indispensável, em tempos de ransomware**), por conta de fornecer a possibilidade de termos backups desconectados.
3. Possui a possibilidade de realizar backups bare-metal de máquinas windows e linux, diretamente para a fita.
4. Possui a capacidade de realizar backup e restauração granular do correio eletrônico, Microsoft Exchange Server, diretamente para a fita
5. Possui a capacidade de realizar backup e restauração granular do Active Directory, diretamente para fita

2. Análise da Solução escolhida:

1. Esta comissão entende que a melhor escolha é a Solução 03, o software de Backup Bacula Enterprise, pelos seguintes motivos:

1. A retrocompatibilidade com o acervo de Backup de nossa instituição, pois atualmente utilizamos principalmente o software de backup Bacula Community;
2. O reaproveitamento de todos os backup já realizados no bacula community, sem a necessidade de qualquer processo de migração ou conversão;
3. O total aproveitamento do conhecimento já adquirido com o uso da versão atual o que torna a curva de aprendizado da solução muito mais suave, diferente de uma nova solução na qual será necessário a execução de todo o processo de migração e aprendizado, sem a necessidade de manutenção do sistema legado até o final do ciclo de vida dos dados backupeados
4. O uso de novas facilidades não disponíveis na versão “*Community*” sejam incorporadas ao processo de proteção dos dados de forma a facilitar o processo de recuperação dos dados quando da necessidade de recuperação de desastres quer sejam ocasionados por falha ou por resultado de ataques cibernéticos a exemplo dos danos já causados por “*ransomware*” em diversas instituições públicas.
5. A possibilidade de realizar backups full e incrementais das máquinas virtuais Xen (base tecnológica utilizada no TRE/AC), sem necessidade de instalação de agentes nas referidas máquinas virtuais, utilizando de mecanismo moderno como Change Block Tracking, ou tecnicamente conhecido como CBT, o que torna o backup incrivelmente rápido, capaz de atender nossas exigências de RPO e RTO.
6. A compatibilidade com as máquinas virtuais *Xenserver*, com envio diretamente para fita, utilizando CBT, inexistente na solução 01, dessa forma, tal solução não atende aos requisitos do Regional, restando a Solução 3, como a solução que melhor se adequa as necessidades do TRE/AC.

2. Análise final do custo da solução escolhida

1. Considerando a ata de registro de preços em que nosso Regional é partícipe (0564995), os valores estimados da contratação ficam assim detalhados:

ITEM	DESCRIÇÃO	QTD	VALOR DA LICENÇA (1 ANO)	RENOVAÇÃO SEGUNDO ANO	RENOVAÇÃO TERCEIRO ANO	VALOR TOTAL
1	Licença perpétua do bacula enterprise Bronze + Bweb	1	R\$ 142.490,50	R\$ 28.498,10	R\$ 28.498,10	R\$ 199.486,70
7	Licença perpétua do plugin Bare metal Linux	1	R\$ 39.976,00	R\$ 7.995,00	R\$ 7.995,00	R\$ 55.966,00
10	Licença perpétua do plugin VSS (exchange)	1	R\$ 39.976,00	R\$ 7.995,00	R\$ 7.995,00	R\$ 55.966,00
8	Licença perpétua do plugin Bare metal Windows	1	R\$ 39.976,00	R\$ 7.995,00	R\$ 7.995,00	R\$ 55.966,00
11	Licença perpétua do plugin Xen	1	R\$ 39.976,00	R\$ 7.995,00	R\$ 7.995,00	R\$ 55.966,00
9	Licença perpétua do plugin AD/LDAP	1	R\$ 39.976,00	R\$ 7.995,00	R\$ 7.995,00	R\$ 55.966,00
6	Licença perpétua do plugin Oracle Db	1	R\$ 39.976,00	R\$ 7.995,00	R\$ 7.995,00	R\$ 55.966,00
13	Serviço de Implantação com Repasse Tecnológico - Turma de até 6 (seis) participantes	1	R\$ 19.900,00			R\$ 19.900,00
CUSTO TOTAL						R\$ 555.182,70

-
- Os valores estimados de uma solução de mercado, como o Veeam backup (0564964), estão, em valores estimativos, quase o dobro do valor da solução escolhida, conforme detalhamento abaixo:**

ITEM	QTDE	VALOR UNITÁRIO	VALOR TOTAL
Veeam Backup & Replication Universal Perpetual License. Includes Enterprise Plus Edition features. 10 instance pack. 3 years of Production (24/7) Support is included. Public Sector	22	R\$ 42.791,00	R\$ 941.402,00
Serviço de implementação SEPROL	01	R\$ 24.000,00	R\$ 24.000,00
TOTAL			R\$ 965.402,00

-
-
- Fica demonstrado então que tanto tecnicamente quanto economicamente, a solução 03, aquisição da ferramenta Bacula Enterprise, é mais vantajosa para o Tribunal, pois além de manter compatibilidade com o backup legado do Regional, ainda possui funcionalidades que melhor se adequam ao nosso parque tecnológico, como a possibilidade de realizar backup de máquinas virtuais xen, sem a necessidade de instalação de agente, bem como possui um menor custo de aquisição.

3. Descrição da solução de TI

- A presente solução consiste na aquisição de software Bacula Enterprise Backup Server com garantia de 03 (três) anos.
- Serão adquiridas licenças de softwares que proporcionarão a cópia de segurança dos dados (backup) de forma segura e em conformidade com as **boas práticas da norma ISO 27000 - Segurança da informação, e com a LGPD.**

3. Justificativa para o não parcelamento

- A presente solução não poderá ser parcelada por tratar-se de solução integrada a qual dependerá de todos os componentes para o funcionamento de forma satisfatória.

4. Adequação do ambiente:

- Não há necessidades de adequação do ambiente

5. Logística de implantação:

- Primeira Fase: Inventário do ambiente a ser backupeado
- Segunda Fase: Análise do ambiente de backup atualmente utilizado
- Terceira Fase: Implantação da nova solução, integrando-a com a solução atualmente utilizada, envolvendo nesse caso softwares e hardwares, como os appliances de backup e a Biblioteca de Fitas
- Quarta Fase: Testes de backup e restauração

6. Impacto ambiental:

- Quanto aos requisitos ambientais, deve-se seguir a seguinte diretriz de sustentabilidade ambiental, estabelecida na IN. 01/2010 SLTI/MPOG, qual seja: o equipamento não deve conter substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenilpolibromados (PBDEs)

2. ESTRATÉGIA DA CONTRATAÇÃO:

1. Descrição da solução de Tecnologia da informação

1. Descrição da solução

- Aquisição de licença de uso perpétuo do software bacula backup enterprise server e plugins para compor o processo e cópias de segurança no datacenter do Tribunal regional Eleitoral do Acre, em substituição a versão '*Free*' (comunitária) hoje utilizada

2. Detalhamento dos bens e serviços que compõem a solução:

- Software bacula backup enterprise server e plugins
- Serviço de instalação
- Treinamento presencial/repasse de conhecimento

3. Definição da solução:

-

Critério	Atendimento
É possível especificar o serviço usando parâmetros usuais de mercado	SIM
É possível medir o desempenho da qualidade usando parâmetros usuais de mercado	SIM
O objeto da contratação se estende necessariamente por mais de 01 ano	SIM
O objeto da contratação é essencial para o negócio	SIM

2. Responsabilidades da Contratante e da Contratada

1. Deveres e Responsabilidades da Contratante:

- Exigir o cumprimento de todas as obrigações assumidas pela contratada, de acordo com o edital do pregão eletrônico, termo de referência e seus anexos, as cláusulas contratuais, e da proposta da CONTRATADA;
- Permitir o acesso, quando necessário de funcionários da CONTRATADA, devidamente identificados para solução de qualquer anormalidade, desde que solicitado pela contratada ao Fiscal do contrato, o qual acompanhará toda atividade a ser desenvolvida;
- Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, hora, mês e ano, bem como os demais detalhes envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;
- Notificar a contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;
- Prestar as informações e esclarecimentos relativos ao objeto desta contratação que venham a ser solicitados pela CONTRATADA
- Comunicar à CONTRATADA toda e qualquer ocorrência relacionada ao contrato e demais elementos constitutivos;
- Exigir que a CONTRATADA execute os serviços de forma conveniente e compatível com o exercício das funções que lhe forem atribuídas sem causar embaraço e desconfiância à fiscalização.
- Fiscalizar a entrega dos serviços podendo sustar, recusar, mandar fazer ou desfazer qualquer material que não esteja de acordo com as condições e exigências especificadas no edital, termo de referência ou eventual ata de registro de preços;
- Proporcionar as facilidades necessárias ao bom andamento para a execução dos serviços;
- Efetuar os pagamentos nas condições e preços pactuados pela prestação dos serviços mediante apresentação, aceitação e atesto do Fiscal nos documentos hábeis de cobrança;
- Receber por meio de Fiscal, acompanhado pelo responsável da execução do contrato, os serviços, a fim de que se evitem desarmonias entre serviços entregues;
- Efetuar as retenções tributárias devidas sobre o valor da nota fiscal fornecida pela contratada em conformidade com a legislação aplicável;

2. Deveres e Responsabilidades da Contratada:

- Cumprir fielmente o que estabelece o Edital de Licitação, Termo de referência, anexos e ou Ata de Registro de Preços;
- Garantir o compromisso de executar o objeto, nas condições estabelecidas na proposta;
- Garantir o cumprimento dos prazos e demais exigências constantes no Edital, Termo de Referência, anexos e Ata de Registro de Preço;
- Tomar conhecimento de todas as cláusulas e condições da contratação, constantes do edital, não sendo admitida posterior alegação de desconhecimento;
- Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.
- Repassar ao TRE/AC, durante todo o período de vigência do contrato, todos os preços e vantagens ofertadas pelo mercado, inclusive os de preço reduzido, sempre que esses forem mais vantajosos que os ofertados na licitação;
- Durante o tempo em que a garantia estiver em vigor, disponibilizar o suporte na modalidade 8x5, resolvendo os problemas no próximo dia útil, desde que exista algum fato que impeça a sua resolução no mesmo dia;
- Manter durante toda vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
- Apresentar, sempre que solicitado pela Contratante no prazo estipulado no pedido, documentação referente às condições exigidas neste instrumento contratual;

3. Termos Contratuais

1. procedimentos e critérios de aceitação

-

ID Etapa / Fase / Item	Indicador	Valor Mínimo Aceitável
01 Recebimento do software:	Entrega e aceite pela Seção de Infraestrutura e Comunicação	100%
01.01 - Licenças.		
01.02 - Serviço de instalação.		
01.03 - Testes de funcionamento.		
02 Treinamento		

02.01 - Realização do treinamento / repasse de conhecimento	Entrega e aceite pela Seção de Infraestrutura e Comunicação	100%
---	---	------

2. **Modalidade e tipo de licitação**
1. Para a presente licitação recomenda-se a modalidade Pregão Eletrônico, através do Sistema de Ata de Registro de Preços.
3. **Classificação monetária**
1. Orçamento ordinário do Tribunal
4. **Vigência da Contratação**
1. O prazo de vigência da contratação será de 36 (trinta e seis) meses.
5. **Garantia**
1. A garantia será de 36 (trinta e seis) meses On-Site. O atendimento se dará no horário comercial, na modalidade de 8x5 (oito horas, cinco dias por semana).
4. **Equipe de Contratação**
1. **Integrante Demandante: Edcley da Silva Firmino - SEREDE**
2. **Integrante Técnico, Bruno Samuel Pereira Gomes Silva - CIE**
3. **Integrante Técnico, João Batista Bento da Silva - COMAP**
5. **Gestão da Contratação**
1. **Gestor do Contrato: Bruno Samuel Pereira Gomes Silva - CIE**
2. **Fiscal do Contrato: Edcley Da Silva Firmino - SEREDE**
3. **PLANO DE SUSTENTAÇÃO**
1. **Introdução**
1. O plano de sustentação tem por objetivo propor ações para manter a continuidade do negócio da instituição com a aquisição da contratação.
2. **Recursos Necessários à Continuidade do Negócio Durante e Após a Execução do Contrato**
1. Recursos Materiais
1. Manutenção da rede elétrica e lógica
1. Ações Para Obtenção do Recurso e Seus Respectivos Responsáveis:
1.

Ação	Responsável
Propor ações na proposta orçamentária	Secretário de TI
Propor ações para o Comitê Diretivo de Tecnologia da Informação	Secretário de TI
2. Recursos Humanos
1. Seção de Redes
1. Atribuições:
1. Manter o controle das licenças
2. Manter o controle das garantias e das atualizações
3. **Estratégia de Continuidade Contratual**
1. Fim do contrato
1. Ações de contingência:
1. Utilizar a versão comunitária do software, ação que tem como responsável o titular da SEREDE
4. **Estratégia de independência:**
1. Documentação e transferência de Conhecimento
2. Manter pelo menos 02 (dois) servidores capacitados para eventuais iterações na infraestrutura, de forma a garantir que o negócio não seja prejudicado em decorrências de ausências devidamente justificada pelo técnico principal.
4. **ANÁLISE DE RISCOS**
1. A análise de riscos permite a identificação, avaliação e gerenciamentos dos riscos relacionados à contratação. Os riscos analisados foram organizados em duas categorias:
1. Riscos que possam comprometer o sucesso dos processos de contratação e de gestão contratual;
2. Riscos que possam fazer com que a Solução de TI não alcance os resultados que atendam às necessidades do TRE/AC.
2. Para cada risco identificado, define-se a probabilidade de ocorrência dos eventos, os possíveis danos potenciais em caso de acontecimento, possíveis ações preventivas e contingências, bem como a identificação de responsáveis por ação.
3. Após a identificação e classificação, deve-se executar uma análise qualitativa dos riscos, sendo esta realizada por meio da classificação escalar dos níveis de probabilidade e de impacto, conforme a tabela de referência a seguir:

Probabilidade	Impacto
Baixa	Baixo
Média	Médio
Alta	Alto

1.
4. A análise qualitativa dos riscos consiste na classificação conforme a relação entre a probabilidade e o impacto, resultando assim no nível do risco e direcionando as ações relacionadas aos riscos durante a fase de contratação e gestão do contrato, bem como da solução de TI. A tabela a seguir apresenta a Matriz Probabilidade x Impacto, instrumento responsável pela definição dos critérios qualitativos de classificação do nível de risco.

Probabilidade	Alta	Média	Baixa
	Alta	Média	Baixa
	Média	Baixa	Baixa
	Baixa	Baixa	Baixa
	Insignificante	Moderado	Catastrófico
	Impacto		

1.
5. O produto da Probabilidade pelo Impacto de cada risco gera nove combinações possíveis no contexto da Matriz e, a partir destas combinações, define-se a(s) ação(ões) adequada(s) para o tratamento de cada risco gerado. A tabela a seguir apresenta uma síntese dos riscos identificados e classificados relacionados a esta contratação

Id	Risco	Categoria	P	I	Nível Risco (P x I)
1	Especificação do objeto aquém/além da real necessidade do negócio	Contratação	Médio	Alto	Alto
2	Contratação deserta/fracassada	Contratação	Baixa	Alto	Médio
3	Valor ofertado acima da média de mercado	Contratação	Baixa	Médio	Baixo
4	Impugnação do processo licitatório	Contratação	Baixa	Alto	Médio
5	Requisitos de negócios incompletos ou inexistentes para o planejamento	Contratação	Médio	Alto	Alto
6	Não aprovação dos artefatos do Planejamento da Contratação	Contratação	Baixa	Médio	Baixo
7	Atraso na entrega do objeto	Gestão	Baixa	Médio	Baixo

6.

ID	TIPO DE RISCO	RISCO	PROBABILIDADE	IMPACTO	DANO POTENCIAL	ACAO PREVENTIVA	AÇÃO DE CONTINGÊNCIA	RESPONSÁVEL
1	RISCOS DO PROCESSO DE CONTRATAÇÃO	Especificação do objeto aquém/além da real necessidade do negócio	MÉDIA	ALTO	- Atraso na execução dos projetos que dependem da contratação dos serviços de TI - Recursos públicos utilizados com baixa eficiência	- Revisar cuidadosamente o Termo de Referência quando o objeto possuir especificações técnicas ou condições de fornecimento/prestações detalhadas - Pesquisar contratações similares e verificar juntos aos CONTRATANTES as principais dificuldades	Executar aditivo ou supressão contratual para ajustar à necessidade real	- Equipe de planejamento da contratação - Gestor do Contrato
2	RISCOS DO PROCESSO DE CONTRATAÇÃO	Contratação deserta/fracassada	BAIXA	ALTO	Atraso na execução dos projetos que dependem da contratação dos serviços de TI	Revisar cuidadosamente o Termo de Referência quando o objeto possuir especificações técnicas ou condições de fornecimento/prestações detalhadas	- Agendar e realizar nova sessão de lances - Executar a contratação direta, após o Pregão fracassado/deserto desde que devidamente justificado	- Equipe de planejamento da contratação - pregoeiro - SAO
3	RISCOS DO PROCESSO DE CONTRATAÇÃO	Valor ofertado acima da média de mercado	BAIXA	MÉDIO	Comprometimento da economicidade da contratação	- Elaborar pesquisa de preço o mais realista possível - Negociar junto ao vencedor dos lances valores mais vantajosos à Administração	Agendar e realizar nova sessão de lances.	- Equipe de planejamento da contratação - Pregoeiro
4	RISCOS DO PROCESSO DE CONTRATAÇÃO	Impugnação do processo licitatório	BAIXA	ALTO	Atraso na execução dos projetos que dependem da contratação dos serviços de TI.	- Revisar cuidadosamente o Termo de Referência quando o objeto possuir especificações técnicas ou condições de fornecimento/prestação detalhadas - Pesquisar em Pregões similares as principais causas de questionamentos administrativos e jurídicos - Responder todos os questionamentos administrativos de forma efetiva e eficaz	Determinar a criação de um novo processo licitatório	- Equipe de planejamento da contratação - DG
5	RISCOS DO PROCESSO DE CONTRATAÇÃO	Requisitos de negócios incompletos ou inexistentes para o planejamento	MÉDIO	ALTO	- Atraso no planejamento da contratação. - Aquisição de bens diferentes da real necessidade	- Revisar cuidadosamente o Termo de Referência quando o objeto possuir especificações técnicas ou condições de fornecimento/prestação detalhadas - Pesquisar em Pregões similares as principais causas de questionamentos administrativos e jurídicos - Responder todos os questionamentos administrativos de forma efetiva e eficaz - Informar os requisitos de negócio que atendam a real necessidade	Determinar a criação de um novo processo licitatório	- Equipe de Planejamento da Contratação - SEREDDE - DG
6	RISCOS DO PROCESSO DE CONTRATAÇÃO	Não aprovação dos artefatos do Planejamento da Contratação	BAIXO	MÉDIO	Atraso no planejamento da contratação	- Reuniões com autoridades superiores para alinhamento e aprovação dos artefatos - Estabelecer procedimentos para que a área administrativa acompanhe a elaboração dos artefatos	Determinar a criação de um novo processo licitatório	- Equipe de Planejamento da Contratação - SAO

						evitando envios e devoluções do processo		▪ DG
7	RISCOS DO PROCESSO DE GESTÃO CONTRATUAL E DA SOLUÇÃO DE TI	Atraso na entrega do objeto.	BAIXO	MÉDIO	▪ Atraso ou ausência dos projetos/atividades que dependem da contratação para seu prosseguimento.	▪ Estabelecer no Termo de Referência prazo adequado para entrega do objeto ▪ Estabelecer no Termo de Referência o atraso máximo tolerado antes da rescisão contratual ▪ Prever sanções proporcionais ao dano causado pelo atraso ▪ Manter regularmente comunicação com a empresa desde a assinatura do contrato ▪ Demandar explicações detalhadas e documentadas à empresa sobre alertas de atraso pelo IBAMA ▪ Aplicar sanções	▪ Rescindir o contrato e convocar a colocada seguinte no Pregão.	▪ Equipe de Planejamento da Contratação ▪ Gestor do Contrato ▪ DG

1.

EDCLEY DA SILVA FIRMNO

TITULAR DA SEÇÃO DE REDES
INTEGRANTE DEMANDANTE

BRUNO SAMUEL PEREIRA GOMES

TITULAR DA COORDENADORIA DE INFRAESTRUTURA
INTEGRANTE TÉCNICO

JOÃO BATISTA BENTO DA SILVA

TITULAR DA COORDENADORIA DE MATERIAL E PATRIMÔNIO
INTEGRANTE ADMINISTRATIVO

 Documento assinado eletronicamente por **BRUNO SAMUEL PEREIRA GOMES SILVA, Coordenador(a)**, em 08/02/2023, às 14:11, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

 Documento assinado eletronicamente por **JOÃO BATISTA BENTO DA SILVA, Coordenador(a)**, em 08/02/2023, às 14:21, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

 Documento assinado eletronicamente por **EDCLEY DA SILVA FIRMINO, Chefe de Seção**, em 08/02/2023, às 14:31, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

 A autenticidade do documento pode ser conferida no site https://sei.tre-ac.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0565232** e o código CRC **FFC5CB0F**.