ESTUDO TÉCNICO PRELIMINAR

CONTRATAÇÃO DE SOLUÇÃO PARA MONITORAMENTO E AUDITORIA DE *ACTIVE DIRECTORY* E SERVIDORES DE ARQUIVOS

OBJETO A CONTRATAR

Solução para monitoramento e auditoria de Active Directory e servidores de arquivos, incluindo software, hardware, suporte técnico e treinamento.

DESCRIÇÃO DA NECESSIDADE

O Active Directory Domain Services, mais conhecido por Active Directory ou simplesmente AD, é um serviço de diretórios, desenvolvido e mantido pela Microsoft Corporation, para gerenciamento de usuários, grupos e computadores em uma rede Windows. Quando um funcionário insere suas credenciais para utilizar um equipamento em uma rede corporativa, um controlador de domínio do Active Directory é o responsável pela conferência e concessão (ou negação) do acesso, bem como pelo registro dessa operação (quem fez o acesso e em que data e horário) no gerenciador de eventos do Windows. Além de prover uma estrutura de autenticação, esse programa também armazena diversas informações de usuários, grupos e computadores, como nomes, cargo, números de telefone, gerente, endereço de e-mail, entre outros, servindo como um catálogo para consulta dos dados armazenados.

Além dos controladores de domínio, uma rede Windows também é composta por diversos servidores de arquivos, que são computadores – geralmente construídos com peças e componentes físicos (*hardware*) especiais, feitos para funcionar quase que ininterruptamente por vários anos e, consequentemente, mais robustos que computadores pessoais – destinados a armazenar informações que serão acessadas de forma centralizada por meio de uma rede digital. Numa organização, se diversos funcionários precisarem preencher e consultar uma planilha

de dados, é mais funcional e producente que todos acessem o mesmo arquivo gravado em um servidor central, ao invés de cada um possuir uma cópia em seu computador pessoal, o que pode levar a dados divergentes e conflitantes.

Em uma rede segura, os recursos para registro das operações realizadas nos objetos do Active Directory, arquivos, diretórios e pastas compartilhadas são imprescindíveis. Ou seja, deve ser capaz de rastrear, quando necessário, todas as operações realizadas nos objetos do Active Directory e nos arquivos, diretórios e pastas compartilhadas dos servidores, bem como ser capaz de verificar tentativas de acesso, bem-sucedidas ou não, às contas dos seus usuários. Além disso, como os arquivos podem conter dados pessoais, a rastreabilidade dessas operações é necessária por conta das responsabilidades geradas pela LGPD – Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018).

A plataforma Windows possui um sistema gerenciador de eventos nativo, entretanto, esse recurso apresenta as seguintes limitações:

- Impossibilidade de armazenar os registros por um período longo;
- Produção de registros bastante resumidos e codificados, o que se justifica por questões de desempenho (poupar o poder de processamento do computador) e espaço (armazenar menos dados). Esses registros brutos, embora possuam informações suficientes para seu tratamento, não podem ser interpretados de forma prática e célere por um profissional humano, exigindo a consulta frequente a manuais de referência. Igualmente, há limitações para pesquisas nos registros e para a geração de relatórios. A imagem 1 mostra um exemplo de registro criado pelo AD:

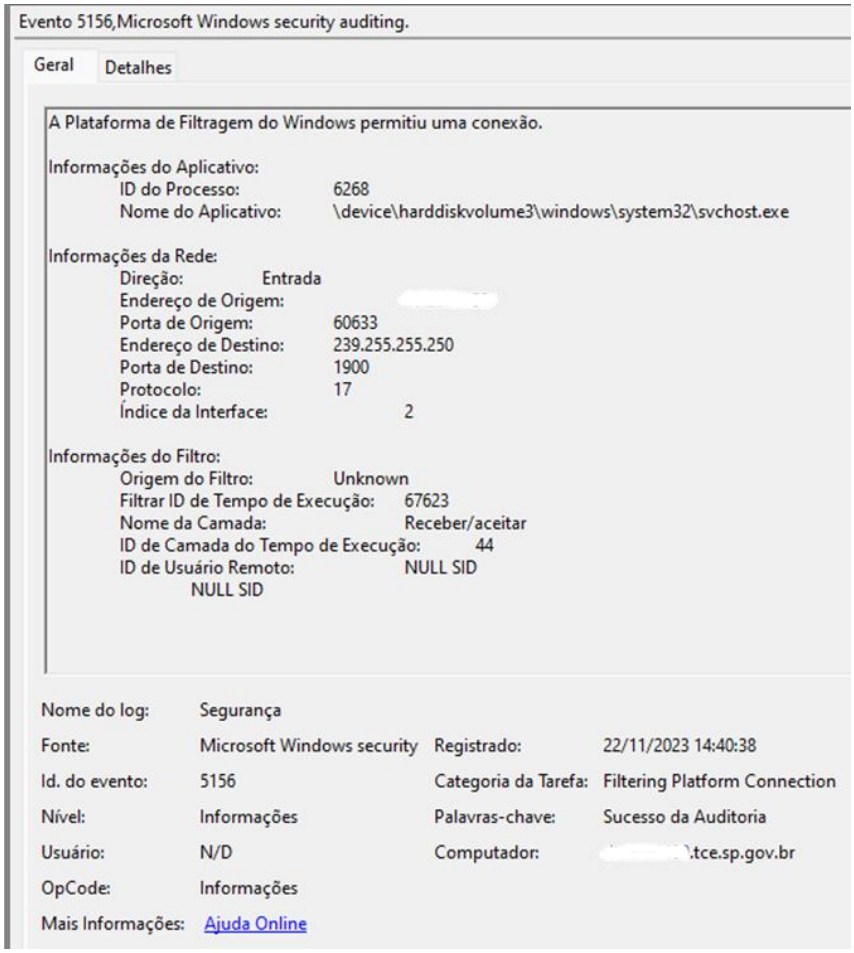

Imagem 1: Exemplo de registro de evento de auditoria criado pelo AD

Esses entraves podem ser superados com o uso de ferramentas específicas de monitoramento e auditoria que, uma vez instaladas em um servidor e trabalhando em conjunto com o Active Directory e servidores de arquivos, permitem a busca e visualização de registros e a geração de relatórios de forma prática, rápida e intuitiva. Enquanto o gerenciador de eventos do Windows gera algo como o mostrado na Imagem 1, um programa focado em auditoria mostraria informações mais claras e objetivas, como, num exemplo hipotético:

Usuário:	*fulano*
Ação efetuada:	*apagar*
Caminho:	*\\servidor\relatorios*
Arquivo:	*relatoriofinanceiro.pdf*
Data:	*22/11/2023*
Hora:	*14:46*

Tabela 1: Exemplo de registro de log.

Adicionalmente, a ferramenta permitiria a busca e emissão de relatórios de forma simples; e.g.: usuários que fizeram alterações no documento *planilha-financeira.xls* entre 01/01/2023 e 01/01/2024, ou, arquivos que foram apagados na pasta \\servidor\relatorios em 10/11/2023.

Em virtude do grande número de servidores de arquivos e dados em uso pelo TCESP, é premente que a Casa tenha uma ferramenta de auditoria do Active Directory e servidores de arquivos que permita o monitoramento de eventos, bem como produção de relatórios sobre eles, de forma intuitiva, prática e rápida.

Ademais, o contrato de suporte e manutenção da solução de auditoria atual (Contrato nº 30/2019 e SEI 1680/2019-05), termina em 04 de junho de 2024 e não pode ser mais renovado.

DEMONSTRAÇÃO DA PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAL

Esta contratação não está prevista no plano de contratações anual, uma vez que esse plano ainda está em desenvolvimento, conforme os termos da resolução 10/2023.

REQUISITOS DA CONTRATAÇÃO

A solução necessita atender os seguintes requisitos técnicos:

- Realizar auditoria de servidores locais (*on-premises*);
- Realizar a tradução de valores SID (Securiy Identifier), máscaras de acesso e linguagem de definição de descritores de segurança (SDDL) contidos nos logs de auditoria;
- Realizar a tradução dos logs de eventos do Windows em ações realizadas sobre os objetos.

ESTIMATIVA DA QUANTIDADE

QUANTIDADE	DESCRIÇÃO
1	Solução para monitoramento auditoria de *Active Directory* e servidores de arquivos, incluindo software, hardware, suporte técnico e treinamento.

Tabela 2: Quantitativo da solução

Trata-se de uma solução composta de software e hardware para atender um cenário com 02 controladores de domínio Active Directory, 32 servidores de arquivos, 2276 usuários ativos no Active Directory, 1353 grupos do Active Directory e quantidade aproximada de 150 milhões de registros de auditoria gerados semanalmente.

Essas informações foram coletadas da seguinte forma:

ITEM	FORMA DE OBTENÇÃO
Quantidade de controladores de domínio e servidores de arquivos	Valor informado pela seção técnica DTEC-1 em 12/12/2023
Quantidade de usuários	Obtida de relatório da ferramenta de auditoria atual (imagem 2)
Quantidade de grupos	Obtida a partir do seguinte comando powershell (imagem 3): (Get-ADGroup -Filter '*').Count
Quantidade aproximada de registros	Valor obtido a partir de amostra semanal das informações do sistema de auditoria em uso atualmente, considerando que, devido a filtros, aproximadamente metade dos registros são gravados (imagem 4)

Tabela 3: Levantamento do volume atual.

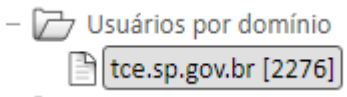

Imagem 2: Total de usuários ativos no Active Directory

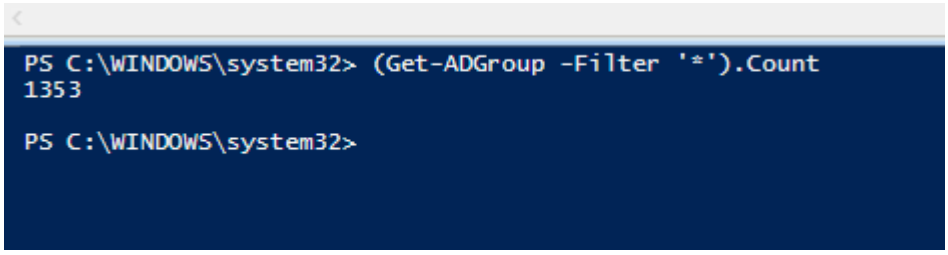

Imagem 3: Total de grupos cadastrados no Active Directory

source	count()
[redacted].tce.sp.gov.br	11,197,820
[redacted]-01.tce.sp.gov.br	19,147
[redacted]alf.tce.sp.gov.br	22,203,610
[redacted]svc.tce.sp.gov.br	13,242
[redacted]vc3.tce.sp.gov.br	15,611
[redacted].tce.sp.gov.br	74,728
[redacted]1.tce.sp.gov.br	217,581
[redacted]2.tce.sp.gov.br	282,982
[redacted]3.tce.sp.gov.br	319,713
[redacted].tce.sp.gov.br	766,406
[redacted].tce.sp.gov.br	339,375
[redacted].tce.sp.gov.br	375,885
[redacted].tce.sp.gov.br	219,235
[redacted].tce.sp.gov.br	344,752
[redacted].tce.sp.gov.br	537,055
[redacted].tce.sp.gov.br	400,032
[redacted].tce.sp.gov.br	489,332
[redacted].tce.sp.gov.br	286,854
[redacted].tce.sp.gov.br	233,552
[redacted].tce.sp.gov.br	302,724
[redacted].tce.sp.gov.br	181,344
[redacted].tce.sp.gov.br	14,182
[redacted].tce.sp.gov.br	128,445
[redacted].tce.sp.gov.br	2,615,036
[redacted].tce.sp.gov.br	227,609
[redacted].tce.sp.gov.br	328,279
[redacted].tce.sp.gov.br	131,312
[redacted].tce.sp.gov.br	575,334
[redacted].tce.sp.gov.br	185,260
[redacted].tce.sp.gov.br	32,986,412
[redacted].tce.sp.gov.br	4,314,826

Imagem 4: Amostra de quantidade de registros de auditoria gerados semanalmente.

LEVANTAMENTO DE MERCADO

Há diversas soluções de auditoria disponíveis no mercado, e o TCESP possui o Microsoft Purview, integrante do serviço Microsoft 365 (SEI 2602/2023-04), a auditoria nativa do Windows e o Graylog (solução gratuita e *opensource*). Porém, é necessário avaliar se essas ferramentas atendem os seguintes requisitos técnicos:

- Realizar auditoria de servidores locais (*on-premises*);
- Realizar a tradução de valores SID (*Security Identifier*), máscaras de acesso e linguagem de definição de descritores de segurança (SDDL) contidos nos logs de auditoria;
- Realizar a tradução dos logs de eventos do Windows em ações realizadas sobre os objetos.

Assim, foi realizado um levantamento comparativo com outras soluções de auditoria que o TCESP já possui (tabela 01), que demonstrou que somente a solução de auditoria proposta possuirá as características técnicas necessárias:

CARACTERÍSTICA	**AUDITORIA NATIVA DO WINDOWS**	**MICROSOFT PURVIEW**	**GRAYLOG**	**SOLUÇÃO PROPOSTA**
Auditoria de servidores locais	SIM	NÃO	SIM	SIM
Tradução de SID	NÃO	SIM	NÃO	SIM
Tradução de logs	NÃO	SIM	NÃO	SIM
Gerenciamento centralizado	NÃO	SIM	SIM	SIM
Emissão de relatórios	NÃO	SIM	NÃO	SIM
Visibilidade das permissões aplicadas nos arquivos, diretórios e pastas compartilhadas locais	NÃO	NÃO	NÃO	SIM
Visibilidade dos arquivos, diretórios e pastas compartilhadas locais que estão sem auditoria	NÃO	NÃO	NÃO	SIM
Visibilidade dos usuários inativos do domínio AD	NÃO	NÃO	NÃO	SIM
Visibilidade dos usuários com perfil de administrador	NÃO	NÃO	NÃO	SIM

CARACTERÍSTICA	AUDITORIA NATIVA DO WINDOWS	MICROSOFT PURVIEW	GRAYLOG	SOLUÇÃO PROPOSTA
Visibilidade dos diretórios e pastas compartilhadas com permissões inseguras	NÃO	NÃO	NÃO	SIM
Histórico de operações realizadas	NÃO	NÃO	NÃO	SIM
Visibilidade das permissões associadas a um usuário bloqueado	NÃO	NÃO	NÃO	SIM

Tabela 4: Comparação das ferramentas.

ESTIMATIVA DO VALOR DA CONTRATAÇÃO

DESCRIÇÃO	VALOR MENSAL	VALOR TOTAL
Solução de auditoria do *Active Directory* e servidores de arquivos	R$ 25.000,00	R$ 900.0000,00

Tabela 5: Orçamento estimado.

Esta estimativa foi realizada com base em pesquisa na Internet, sendo necessária a atualização deste estudo técnico preliminar quando a área responsável realizar a pesquisa de preços. Por se tratar de uma solução, que possui diferenças em cada ambiente em que for instalada, principalmente com relação ao total de usuários e capacidade de armazenamento, não foram encontradas muitas licitações semelhantes. A que mais se aproxima, em termos de quantidade de usuários, é a do Governo do Estado de Rondônia de dezembro de 2022. Entretanto, naquela licitação, não há fornecimento de hardware:

ÓRGÃO	PREGÃO	DATA	DESCRIÇÃO	ITENS	VALOR ESTIMADO
Governo do Estado de Rondônia	00701/2022	27/12/2022	Solução de Auditoria e Monitoramento para 2000 usuários (https://rondonia.ro.gov.br/wp-content/uploads/2023/01/ATA.pdf)	Item 1: SOFTWARE AUDITORIA NO AD (MICROSOFT ACTIVE DIRECTORY)	350.020,00
				Item 2: SOFTWARE AUDITORIA NO SERVIDOR DE ARQUIVOS (MICROSOFT FILE SERVER)	345.820,00
				Item 4: INSTALAÇÃO E CONFIGURAÇÃO	16.000,00
				Item 5: HANDS -ON	20.000,00
Valor total estimado (somente software)					731.840,00

Tabela 6: Informações do pregão 00701/2022

O valor do hardware foi estimado com base no equipamento utilizado pela solução de auditoria utilizada atualmente. Estima-se que o valor de um servidor com capacidade semelhante é de R$ 92.000,00, conforme indicado na tabela a seguir referente ao pregão 125/2022 do Tribunal de Justiça do Estado do Acre:

Órgão	Pregão	Data	Descrição	Itens	Quantidade	Valor total
Tribunal de Justiça do Estado do Acre	125/2022	21/12/2022	Equipamentos de informática (https://www.tjac.jus.br/licit/equipamentos-de-informatica-pe-125-2022/)	Item 1: SERVIDORES DE RACK	20	1.840.000,00
Valor estimado (1 servidor)						92.000,00

Tabela 7: Informações do pregão 125/2022

O valor estimado para os 36 meses de suporte é R$ 56.202,84, calculado com base no valor mensal pago atualmente pelo TCESP à empresa fornecedora da solução de auditoria NetAdmin no contrato 30/2019 (R$ 1.561,19).

A soma desses valores é R$ 880.042,84, que para fins de estimativa foi arredondado para R$ 900.000,00.

DESCRIÇÃO DA SOLUÇÃO

A solução para monitoramento e auditoria de Active Directory e servidores de arquivos, dentre outras funcionalidades, permitirá monitorar os acessos e alterações nos recursos críticos da rede, como usuários, grupos, computadores, registros DNS, arquivos, diretórios, compartilhamentos e diretivas de grupo (GPO).

Essa aquisição tem como objetivo complementar o *software* gratuito Graylog, utilizado atualmente pelo TCESP para essa finalidade, que não possui alguns recursos necessários para a realização de uma auditoria mais completa, tais como:

- Tradução automática de nomes de objetos e máscaras de acesso;
- Histórico de alterações realizadas;
- Visibilidade das permissões atribuídas aos usuários e grupos no Active Directory, arquivos, diretórios ou pastas compartilhadas;
- Visibilidade de permissões consideradas inseguras, como atribuição de permissão de acesso total para o grupo todos em arquivos, diretórios ou pastas compartilhadas;
- Identificação de arquivos, diretórios e pastas que estão com auditoria desabilitada;
- Identificação de usuário inativos, que estão há um certo período sem realizar *login*;
- Emissão de relatórios com:
  - Arquivos e diretórios com permissões diretas;
  - Diretórios sem administradores;
  - Arquivos e diretórios com usuários desabilitados;
  - Alterações realizadas em diretivas de grupo (GPO);
  - Histórico de membros de grupos de segurança;
  - Histórico de permissões em arquivos e diretórios;
  - Grupos vazios ou não utilizados;
  - Usuários inativos.

Também servirá para complementar a solução Microsoft Purview, que realiza auditoria apenas do ambiente de nuvem (Microsoft 365), conforme respondido por e-mail pelo suporte da Microsoft (imagem 5).

De: [redacted] <support@mail.support.microsoft.com>
Enviado em: quinta-feira, 9 de novembro de 2023 13:57
Para: [redacted]; support@mail.support.microsoft.com
Assunto: RE: O Microsoft Purview Audit (Premium) é capaz... - TrackingID# 2311080040011713

Você não costuma receber emails de support@mail.support.microsoft.com. Saiba por que isso é importante

ATENÇÃO: Esta mensagem não foi originada no TCESP. Por segurança, não clique em links ou anexos a menos que saiba que o conteúdo é seguro.

Dear [redacted],

I trust you are doing great.

Thank you for contacting Microsoft Support. My name is Chikezie. I am the Support Professional who will be working with you on this Service Request: ticket #2311080040011713.

Apologies for the delay and any inconveniences experienced.

From the service request you raised, I understand that you would like to know if Microsoft 365 Audit log could provide information on file access to File share hosted in Windows Server on-prem.

Please be advised that Microsoft Purview Solutions can only audit log for resources access in Microsoft 365 environment.

Auditoria (Premium)

ⓘ **Importante**

A partir de 30 de novembro de 2023, a Pesquisa Clássica será removida no lugar de N
inclui aprimoramentos, como tempos de pesquisa mais rápidos, opções de pesquisa a
pesquisas e muito mais.

A auditoria (Premium) baseia-se nos recursos de Auditoria (Standard) fornecendo polític
auditoria, retenção mais longa de registros de auditoria, insights inteligentes de alto valc
banda à API de Atividade de Gerenciamento Office 365.

- Soluções de auditoria no Microsoft Purview | Microsoft Learn

Please let me know if you require further assistance on this issue or if that would be all.

If you do not have any further concerns, I would then proceed to archive the service request.

Imagem 5: Resposta da Microsoft sobre a auditoria do Purview

SUBCONTRATAÇÃO

Não será admitida a subcontratação do objeto contratual.

SEGURANÇA DA INFORMAÇÃO

Os requisitos de segurança estipulados neste documento têm por objetivo reduzir a exposição do TCESP aos riscos de perda de confidencialidade, integridade e disponibilidade dos sistemas de informação e demais soluções computacionais do Tribunal. Eventual divulgação pela CONTRATADA ou prepostos de qualquer informação a que tenham acesso em virtude da prestação dos serviços tais como, por exemplo, referentes à topologia de rede, a senhas, ao modelo operacional da infraestrutura de TI do Tribunal, a arquivos, a processos ou qualquer outro tipo, poderá representar acesso irregular às informações classificadas e recursos computacionais restritos do TCESP, podendo ocasionar severos prejuízos à instituição.

Então, juntamente com o contrato, a CONTRATADA deverá assinar, por meio de seu preposto, o documento denominado Termo de Confidencialidade cujo modelo encontra-se no Anexo I – Modelo de termo de confidencialidade.

O Termo de Confidencialidade determina que a propriedade intelectual de todos os produtos ou conhecimentos gerados ou advindos da prestação dos serviços pertencem ao TCESP. Será exigida a assinatura apenas pela CONTRATADA e visa proteger o TCESP de eventuais divulgações não autorizadas de informações privilegiadas relativamente ao seu ambiente computacional.

A CONTRATADA será obrigada a também providenciar a adesão ao Termo de Confidencialidade de todas as pessoas que venham a executar serviços e fazem parte do objeto a ser contratado e que, em virtude da prestação desses serviços, tenham acesso a informações classificadas do TCESP.

A CONTRATADA será, dessa forma, caso necessário, responsável por obter as assinaturas de Termos de Confidencialidade de todo e qualquer profissional que venha a prestar serviços sob suas responsabilidades, integrantes do objeto desta contratação.

Tal procedimento busca não somente reprimir a divulgação não autorizada dos dados da instituição, como garantir que a propriedade intelectual dos produtos e conhecimentos oriundos ou gerados a partir da prestação dos serviços seja integralmente do TCESP.

Por fim, toda informação referente ao Tribunal que a CONTRATADA vier a tomar conhecimento em função da execução dos serviços contratados, não poderá ser divulgada a terceiros sem autorização expressa do TCESP.

JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

O objeto é constituído por apenas um item. Portanto, não se aplica o parcelamento do objeto.

DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS EM TERMOS DE ECONOMICIDADE E DE MELHOR APROVEITAMENTO DOS RECURSOS HUMANOS, MATERIAIS E FINANCEIROS DISPONÍVEIS

Sem uma solução de auditoria e monitoramento, a extração de informações a partir de um *log* bruto precisaria ser feita manualmente pela equipe técnica.

Para a identificação de uma ação em um servidor de arquivos, por exemplo, primeiramente deve-se buscar e filtrar os dados relacionados. Cada ação pode gerar entre dez e vinte registros. Depois disso é necessário interpretar qual a ação que gerou a ocorrência. Após encontrar o registro desejado, é preciso realizar

uma tradução manual do SID (*security identifier*) e da máscara de acesso. Para realizar a tradução é necessário identificar o objeto e relacioná-los ao registro.

Para identificar uma permissão em diretório, ou se a auditoria está aplicada a ele, é necessário visualizar a configuração diretamente no objeto, de forma manual. Caso seja preciso identificar essas informações em múltiplos diretórios, teria que ser realizado manualmente, um a um.

Todos esses levantamentos, feitos de forma manual, exigiriam demasiado tempo da equipe técnica, sendo inclusive sujeitos a erros. Todavia, caso seja usada a solução que é objeto deste estudo técnico, a busca seria rápida e precisa, gastando menos tempo da equipe técnica, o que aproveitaria melhor os recursos humanos da área de segurança da informação do Tribunal, assim como os materiais e financeiros, indiretamente.

PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

Não há.

REQUISITOS DE HABILITAÇÃO

São necessários atestados e/ou declarações de serviços prestados, com características e porte semelhantes aos que serão prestados ao TCESP, em outras empresas, órgãos ou entidades públicas ou privadas para que a licitante comprove, de forma objetiva, sua capacidade técnica para prover os serviços.

Portanto, deverá ser exigido um atestado de capacidade técnica que comprove a instalação, configuração e suporte em solução de auditoria e monitoramento do serviço Active Directory e servidores de arquivos em um ambiente com, pelo menos, 1000 usuários.

Além disso, o licitante vencedor deverá apresentar as comprovações solicitadas no item REQUISITOS DA CONTRATAÇÃO.

ANÁLISE DE RISCO

Nº	DESCRIÇÃO DO RISCO	PROBABILIDADE DE OCORRÊNCIA	IMPACTO	AÇÕES DE MITIGAÇÃO OU CONTINGÊNCIA	RESPONSÁVEIS PELAS AÇÕES	PERÍODO DE EXECUÇÃO
1	Atraso no processo de contratação	Média	Médio	Auditoria realizada pelo Graylog, porém sem tradução dos eventos e demais recursos relacionados na tabela 1	DTEC	Planejamento da contratação
2	Finalização antecipada do contrato	Baixa	Médio	Auditoria realizada pelo Graylog, porém sem tradução dos eventos e demais recursos relacionados na tabela 1	DTEC	Imediatamente após o conhecimento do fato
3	Reiteradas violações de níveis mínimos de serviço	Baixa	Médio	1. Aplicação das sanções contratuais previstas; 2. Notificação da empresa; 3. Rescisão antecipada do contrato; 4. Início de outro processo licitatório	Comissão de fiscalização	Durante a execução contratual

Tabela 07: Análise de riscos.

CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

Não há.

DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS

IMPACTO	MEDIDAS MITIGADORAS
Impactos ambientais causados pelo descarte inadequado de resíduos	Previsão de logística reversa para descarte dos resíduos gerados pela contratação

POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA

Diante da ausência de uma ferramenta capaz de auditar e monitorar os acessos e operações realizadas no Active Directory, arquivos, diretórios e pastas compartilhadas para atendimento aos requisitos de segurança da Instituição, por conta do encerramento do contrato da solução de auditoria atual, bem como para cumprimento das demandas da Lei Geral de Proteção de Dados, considera-se que esta contratação é conveniente e necessária.

ANEXO I

Modelo de Termo de Confidencialidade

O TRIBUNAL DE CONTAS DO ESTADO DE SÃO PAULO, inscrito no **CNPJ 50.290.931/0001-40**, sediado na Avenida Rangel Pestana, 315, Centro, São Paulo/SP, neste ato representado por _____, e a empresa _____, **CNPJ** _____, neste ato, representada por seu_____, _____, portador da **Cédula de Identidade** _____ e do **CPF** _____, respectivamente denominados como CONTRATANTE e CONTRATADA, firmam o presente termo no qual a CONTRATADA se obriga a:

● manter o sigilo de quaisquer informações que venham a ser fornecidas pelo **CONTRATANTE** e obtidas durante a prestação do serviço;

● cientificar todos os envolvidos na prestação do serviço a respeito da existência deste termo;

● não revelar, reproduzir, utilizar ou dar conhecimento a terceiros das informações do **CONTRATANTE**;

● informar imediatamente o **CONTRATANTE** sobre qualquer violação das regras estabelecidas neste termo;

● não copiar ou reproduzir quaisquer informações sem o consentimento do **CONTRATANTE**, exceto quando essas cópias ou reproduções forem necessárias para a prestação do serviço;

● tomar as medidas necessárias para a proteção das informações do **CONTRATANTE**, bem como prevenir sua revelação a terceiros, exceto se autorizado, formalmente, pelo **CONTRATANTE**;

● destruir quaisquer documentos por ela produzidos que contenham informações do **CONTRATANTE**, quando não for mais necessária a manutenção dessas informações.

Este termo é irrevogável e irretratável, devendo permanecer em vigor desde a data de sua assinatura até 5 anos após o término do contrato.

A quebra do sigilo das informações, devidamente comprovada, possibilitará a aplicação de penalidades previstas na legislação em vigor que trata desse assunto, podendo até resultar na RESCISÃO DO CONTRATO firmado entre as partes.