**GOVERNO DO DISTRITO FEDERAL**

INSTITUTO DE GESTÃO ESTRATÉGICA DE SAÚDE DO DISTRITO FEDERAL

Gerência de Infraestrutura de Tecnologia da Informação

Núcleo de Rede

**ELEMENTO TÉCNICO** Nº 3/2020 - IGESDF/DIADM/SUTIC/GEINF/NURED

| | |
|---|---|
| **Unidade:** | IGESDF/DIAPO/SUTIN/GEINF |
| **Solicitante:** | Edilmara Albino Dato |
| **Interessado/Responsável:** | Marcos Flávio de Souza |
| **E-mail:** | infraestrutura@igesdf.org.br |
| **Contato:** | (61) 3550-8900 R:1806 |

## 1. DO OBJETO

1.1. O objeto deste Elemento Técnico é a contratação, na modalidade registro de preços, de serviços e fornecimento de solução de proteção contra ameaças internas e auditoria para ambiente computacional não estruturado, do Instituto de Gestão de Saúde do Distrito Federal - IGSDF.

## 2. JUSTIFICATIVA DA AQUISIÇÃO

2.1. A presente contratação busca atender os objetivos estratégicos no que diz respeito a viabilizar a disponibilidade, integridade e a confidencialidade dos sistemas de informação proporcionando segurança da informação e promover continuamente ações estratégias de governança de TIC.

2.2. Com o intuito de atender a essas necessidades, o presente documento tem por objetivo a contratação de empresa especializada para o fornecimento da solução de proteção contra ameaças internas e auditoria para ambiente computacional não estruturado.

2.3. A solução visa controlar, auditar e monitorar proativamente os dados e deve permitir gerenciar o risco operacional envolvido e avaliar a adequação das tecnologias e sistemas de informação utilizados na organização através da revisão e classificação dos controles, procedimentos de TI, infraestrutura, operação, desempenho e segurança da informação, que envolve o processamento de informações críticas, para a tomada de decisão. Permite, ainda, reunir, agrupar e mensurar evidências para determinar se um sistema de informação suporta adequadamente um ativo de negócio, mantendo a integridade dos dados, utilizando eficientemente os recursos e cumprindo com as regulamentações e leis estabelecidas.

2.4. A maioria das informações acessadas por usuários locais estão armazenada em repositórios de dados não estruturados na rede do Instituto. Este é mais um fato que cria a necessidade da contratação de uma solução - baseada em software para auditoria e controle de

acessos -para melhor gestão do ambiente computacional do Instituto. Esta solução possibilitará auditoria, controle e gerencia sob as ações dos usuários, nas plataformas, tais como: diretório de usuários (Microsoft Active Directory), servidor de arquivos (Microsoft File Server), correio eletrônico (Microsoft Exchange Server) assim como monitorar e prevenir comportamentos suspeitos em tempo real e gerir de forma automática e segura todas as permissões dos usuários.

2.5. O Instituto não possui nenhuma solução de auditoria na forma proposta, sendo necessária para que o IGSDF possa verificar de forma eficiente e proativa o comportamento de seus usuários e as ameaças ao seu ambiente computacional. Deste modo, aumentando a qualidade da entrega de seus serviços, uma vez que a sua infraestrutura de tecnologia da informação necessita de melhorias continuas, modernas e seguras.

2.6. Considerando a importância e o grande volume de informações eletrônicas do Instituto, faz-se necessário preservar a integridade dessas informações, com vistas a manter o máximo possível a sua segurança. E também, assim, minimizando o risco de perda de informação sensível através de usuários descontentes com esta empresa.

2.7. Um grande risco para as atividades desenvolvidas por qualquer instituição é tornar os sistemas computacionais indisponíveis e colocar em dúvida a confidencialidade e a integridade dos dados armazenados. Com os sistemas cada vez mais 'online' e usuários acessando uma infinidade de aplicativos Web ou remotos, faz-se necessária a implementação de controles e políticas de segurança da informação que garantam a disponibilidade, confidencialidade e integridade das informações corporativas.

2.8. O elevado volume de informações eletrônicas dá ao IGESDF importância estratégica nos serviços de saúde do DF, e isso traz consigo a necessidade da preservação destas informações e equipamentos (por seus valores financeiro, informativo, probatório e histórico) com a devida segurança e qualidade de um ambiente adequado à sua destinação. Segundo o instituto de pesquisas técnicas e análises de tendências de TI - o GARTNER GROUP, cerca de 80% dos dados estratégicos estão armazenados em base de dados não estruturadas ou semi-estruturadas. Esses dados estão distribuídos em pastas (departamentais, setoriais e individuais), acessadas entre os diversos usuários de rede e gerenciadas por Sistemas Operacionais que proporcionam o registro de eventos (logs).

2.9. Outro estudo do GARTNER GROUP aponta que, em média, para cada 1 TeraByte de arquivos, existem 50.000 (cinquenta mil) pastas. Em cada uma dessas pastas existem arquivos que podem conter informação de cunho crítico ao funcionamento da instituição. Da mesma forma, uma extensa quantidade de arquivos sensíveis também é armazenada e usada durante o dia-a-dia no Instituto.

2.10. Com o grande número de arquivos sigilosos e estratégicos de pacientes existentes dentro do IGSDF é comum que um funcionário/servidor seja apontado como o dono de uma determinada pasta contendo esses arquivos. Devido a mudanças frequentes de cargos internos que não são devidamente avisadas a Gerência de TI, essas pastas podem estar sendo gerenciadas por um funcionário/servidor que não está mais em posição para isso, comprometendo estes dados, e infringindo por vezes a Norma Complementar n° 20/IN01/DSIC/GSIPR.

2.11. Além disso, uma vez que os eventos são registrados, a busca por informação destes em arquivos de log's é lenta, com interface ineficiente para consultas e pesquisas, além de não fazer monitoramento e análise crítica de eventos proativamente, visando detecção antecipada de situações indevidas, assim, tornando inviável qualquer tipo de gerenciamento e a auditoria de acesso aos dados de forma real e imediata, sem geração de tráfego de rede.

2.12. Diante do exposto, faz-se necessário a implementação no ambiente de uma solução de auditoria, controle e gerência de permissionamento dos serviços de AD e de solução de análise de comportamento e alarme em tempo real, os quais são responsáveis pela comunicação e armazenamento dos dados não estruturados ou semi-estruturados do Instituto.

2.13. O volume de usuários na rede de dados do Instituto torna a atividade de gestão inexequível para os Analistas e Administradores da TI as atividades de auditar, controlar e gerenciar as ações dos usuários nas plataformas de TI, tais como: diretório de usuários (Microsoft Active Directory), servidor de arquivos (Microsoft File Server), correio eletrônico (Microsoft Exchange Server), Onedrive, monitorar e prevenir comportamentos suspeitos em tempo real e gerir todas as permissões dos usuários de forma segura exigem sistemas eficientes que possibilitem essa tarefa.

2.13.1. São desafios que hoje esses Analistas e Administradores da TI enfrentam:

a) Identificar os proprietários dos dados;

b) Controle e auditoria dos eventos (quem acessou o que e como);

c) Excesso de demanda com falta de mão de obra para executar as tarefas;

d) Assegurar que as autorizações sejam baseadas em necessidades de negócios.

2.14. Desta maneira, espera-se a adequação contínua das capacidades de controle e monitoramento necessárias aos serviços alocados no ambiente, de modo que, após implantação, aumentaremos a gestão, a eficiência e a proteção das informações, simplificando tarefas complexas e permitindo uma fácil adaptação dos analistas e administradores da TI às alterações de emergência ou imprevistas. Desta forma, permite-se significativa melhora na garantia de disponibilidade, confiabilidade, rapidez e segurança aos dados do IGESDF.

2.15. O Instituto de Gestão Estratégica de Saúde do Distrito Federal- IGESDF foi instituído por meio do Decreto n° 38.332, de 13 de julho de 2017, obedecendo às cláusulas do contrato de Gestão com a Secretaria de Estado de Saúde do DF, e deverá observar os seguintes pontos:

2.16. Informatizar o IGESDF na sua totalidade, contemplando toda a infraestrutura tecnológica em equipamentos, sistemas informatizados, migração do legado da Secretaria de Estado da Saúde - SES, suporte técnico, até que se consiga total independência de infraestrutura tecnologia da SES.

2.17. Manter e aperfeiçoar sistemas de coletas e analises de dados relativos à qualidade e aos custos dos serviços prestados, desenvolvendo igualmente modelos estatísticos com base na análise destes dados e estudos comparativos de avaliação de desempenho das atividades profissionais desenvolvidas;

2.18. Atender às demandas relativas à realização de estudos específicos e de incorporação tecnológica e propostas de normas técnicas, elaboração de protocolos e procedimentos, coleta e análise de dados, avaliação de tecnologias e técnicas terapêuticas, e formação de pessoal;

2.19. Alimentar o Sistema de Informações ou qualquer sistema que venha a substituir os anteriores nos prazos previstos pela sua regulamentação, sem gerar créditos ou onerar o teto físico-financeiro de assistência distrital;

2.20. Com tal prerrogativa, faz-se necessária a contratação de serviços tecnológicos, através de uma solução abrangente, onde as disponibilizações dos serviços serão sob demandas flexíveis e a forma de pagamento será balizada pelo efetivo serviço realizado.

## 3. JUSTIFICATIVA DO QUANTITATIVO A SER ADQUIRIDO

3.1. Os quantitativos a serem adquiridos foram estimados para atender as necessidades do IGSDF e atuais unidades por ele assistida. Os números finais, foram calculados com base no relatório 29893365 com as evidências retiradas da ferramenta de administração de rede. A saber os números são:

3.2.

| **Quantitativo de usuários no IGESDF** |
|---|

| | |
|---|---|
| Total de contas = 8.915 Contas ativas, valor consolidado com os dados abaixo: | |
| **Local** | **Quantitativo de contas ativas** |
| HB | 5.745 |
| HRSM | 2777 |
| UPA-Bandeirante | 63 |
| UPA-Ceilândia | 73 |
| UPA-Recanto | 114 |
| UPA-Samambaia | 32 |
| UPA-São Sebastião | 56 |
| UPA-Sobradinho | 55 |
| **Quantitativo de usuários com acesso ao servidor de arquivos** | |
| Total de contas = 6.457 Contas ativas (dados obtidos através das contas de usuários contidas em grupos de segurança com acesso ao servidor de arquivos). | |
| Quantitativo de usuários com acesso ao onedrive. | |
| Contas com licença atribuída E1 e E3 | 597 |
| | |
| Contas de E-mail no exchange online total = 707 contas consolidados com os dados abaixo: | |
| Contas setoriais compartilhadas entre usuários | 82 |
| Particulares | 581 |
| Contas de usuários grupos de distribuição | 44 |

3.2.1. Sendo assim, entende-se por necessário o quantitativo abaixo para atender ao IGSDF:

| Itens | Bem/Serviço | Quantidade |
|---|---|---|
| | | |

| | | |
|---|---|---|
| 01 | Licença de subscrição de software para solução de auditoria em Windows File Server pelo período de 12 meses | 7.500 |
| 02 | Licença de subscrição de software para solução de auditoria em Microsoft Active Directory pelo período de 12 meses | 10.250 |
| 03 | Licença de subscrição de software para solução de auditoria em Exchange Online pelo período de 12 meses | 810 |
| 04 | Licença de subscrição de software para solução de auditoria em OneDrive pelo período de 12 meses | 700 |
| 05 | Licença de subscrição de software para solução de análise em tempo real e prevenção de comportamentos suspeitos pelo período de 12 meses | 10.250 |
| 06 | Operação Assistida (horas) | 50 |

## 4. ESPECIFICAÇÃO DO OBJETO

4.1. Para a prestação dos serviços, objeto do presente Elemento Técnico a CONTRATADA deverá atender às necessidades do Instituto de Gestão Estratégica de Saúde do Distrito Federal - IGESDF, considerando o custo dos ativos e recursos a serem suportados, conforme volumetria, arquitetura, serviços e necessidades que por ventura surgirem.

4.2. A solução deverá ser de um único fabricante e permitir que seus módulos sejam todos integrados, do modo que preserve a interoperabilidade e a harmonia entre todos os elementos;

4.3. Através de acessos autorizados a solução deverá disponibilizar console nativa, a qual poderá ser acessada através dos servidores e das estações de trabalho;

4.4. A solução deve fornecer todas as funcionalidades citadas abaixo sem a necessidade de retenção dos logs nativos do Windows. Caso a solução ofertada necessite habilitar o log de auditoria do Windows File Server, o hardware sem ponto único de falha necessário para o armazenamento destes logs por 12 (doze) meses deverá ser contemplado na proposta;

4.5. O processo de instalação de agentes nos servidores a serem monitorados, caso se faça necessário, não poderá impactar na disponibilidade dos mesmos e de seus serviços;

4.6. Possibilitar a configuração de credencial diferente para cada servidor/serviço a ser monitorado;

4.7. Deve suportar a utilização de servidores virtualizados para todos os seus componentes;

4.8. Deve oferecer a possibilidade de configurações de diferentes níveis de segurança às suas funcionalidades, de modo que diferentes equipes com papéis diferentes e com acesso restrito a diferentes funções possam utilizá-la;

4.9. A solução não poderá permitir que o nível de consumo dos recursos ultrapasse limites definidos e configurados onde houver um agente instalado e monitorando o desempenho;

4.10. Com o intuito de garantir a integridade e a confiabilidade jurídica, contratual e regulatória, esta solução deve ter certificação utilizada pela administração pública como parâmetro para definição de requisitos de sistema de gerenciamento de segurança da informação como a ISO/IEC 27001 ou similares;

4.11. Deve permitir associar ou assinalar um ou mais usuários como "proprietário(s)" de uma

pasta ou grupo;

4.12. Deve permitir monitorar diferentes domínios, independente da existência de relação de confiança;

4.13. A solução deverá realizar a análise comportamental dos usuários e fazer recomendações de alteração, revogação de acesso, trocas de grupos e permissões aos dados não estruturados dos servidores monitorados;

4.14. Realizar a descoberta automática de contas privilegiadas de usuários administrativos, contas executivas e de serviço; Identificar de forma automática usuários com acesso a pastas indevidas, sugerindo a revogação de impactos das mudanças pretendidas nos usuários e grupos em relação à suas permissões nos diretórios monitorados, de modo que seja possível analisar quais acessos os usuários ou grupos ganharão ou perderão antes que as alterações sejam aplicadas;

4.15. Deve fornecer a visão das permissões efetivas, informando permissões de Share e NTFS;

4.16. Possibilitar a visibilidade total sobre o serviço de diretório Azure, possibilitando diferenciar e consultar os objetos do Azure Active Directory e do Active Directory on-premise;

4.17. Fornecer visibilidade sobre aplicações de alterações que estão pendentes e o histórico das alterações aplicadas através da console;

4.18. Deve oferecer a opção de aplicação imediata ou agendada das permissões no Active Directory e demais servidores monitorados, assim como aplicação parcial ou completa destas permissões;

4.19. Deve apresentar as permissões excessivas baseadas na análise dos eventos de auditoria; Deve permitir alterações das permissões dos diretórios monitorados através de sua interface gráfica;

4.20. A visualização gráfica e interativa das listas de controle de acesso incluindo grupos, subgrupos e seus respectivos membros, deverá ser exibida para cada pasta dos recursos monitorados;

4.21. Deve gerar relatórios nos formatos CSV, HTML, XLS, XLSX e PDF;

4.22. Permitir que relatórios sejam extraídos sob demanda e que possam ser agendados e enviados, com frequência definida, para correio eletrônico ou para um compartilhamento no servidor de arquivos;

4.23. Fornecer relatórios de permissões concedidas a grupos globais;

4.24. Fornecer relatórios de usuários desabilitados que ainda fazem parte de grupos de segurança;

4.25. Fornecer relatórios de SID's não resolvidos e usuários com permissão direta em pastas;

4.26. Fornecer relatórios de dados e usuários inativos;

4.27. Deve fornecer relatório de histórico de permissões;

4.28. Deve fornecer relatório de histórico de membros de grupos de segurança;

4.29. Deve oferecer relatórios de estatísticas, métricas e gráficos com informações sobre usuários, grupos, pastas e permissões ao longo de determinado período;

4.30. A funcionalidade de envio de relatórios por e-mail deve ser nativa da ferramenta, sem a utilização de softwares terceiros, e deve suportar o protocolo SSL sobre SMTP;

4.31. Fornecer relatórios de todas as permissões de qualquer usuário nos repositórios e pastas monitorados e seus respectivos acessos;

4.32. Fornecer relatório sobre as alterações, versão alterada e quais foram as mudanças realizadas em GPO;

4.33. Fornecer relatório de auditoria das ações dos usuários na console;

4.34. Deve oferecer relatório de estatística de acesso, utilização por tipo de arquivos, eventos por usuários e distribuição por tipos de eventos;

4.35. Deve fornecer relatórios com as recomendações de revogação de permissão geradas pela análise comportamental realizada sobre os usuários e recursos monitorados;

4.36. Deve oferecer relatórios de estatísticas de autenticação e falha de autenticação;

4.37. Deve oferecer relatórios comparativos dos sistemas de arquivos monitorados;

4.38. Fornecer relatório de lista de usuários administradores em grupos não administrativos;

4.39. Fornecer relatório de lista de permissões de usuários desabilitados;

4.40. Fornecer relatório de pastas sem administradores;

4.41. Fornecer relatório dos alertas de comportamento anômalo identificados;

4.42. Deve coletar os logs serviços/servidores monitorados de forma continua e automática e normatizá-los em banco de dados;

4.43. Deverá contabilizar a quantidade de vezes que um mesmo evento ocorreu em um mesmo dia e informar a primeira e última vez que aquele determinado evento ocorreu;

4.44. Permitir filtragem gráfica, ordenação e agrupamento dos logs;

4.45. Deve apresentar os logs de todos os serviços/servidores monitorados na console de visualização de permissionamentos e apresentar as informações completas de cada uma das operações com data e horário, nome do servidor, tipo do objeto, caminho (path) dos dados, domínio, arquivo impactado e nome do usuário;

4.46. Possibilitar a alteração do conjunto de dados (colunas) retornados da consulta aos logs de acordo com a necessidade da informação;

4.47. Deve fornecer resumo gráfico das atividades auditadas; Permitir que os usuários realizem pesquisas baseados em critérios como: data do evento, servidor ou plataforma em que ocorreu o evento, tipo de evento, arquivos ou diretórios acessados;

4.48. Deve oferecer, através da interface de monitoração, as funcionalidades de permissionamento, log, relatórios e análise comportamental dos usuários nos servidores de diretórios de usuários Microsoft Active Directory;

4.49. Deve suportar a auditoria do Directory Service nos seguintes eventos: criação de deleção de objetos; membros adicionados e removidos de grupos de segurança; alteração nas propriedades do objeto do AD; requisição de acesso; autenticação de conta; reset de senhas; bloqueio e desbloqueio de conta; criação de deleção de conta; habilitação e desabilitação de conta; permissão adicionada a objeto do AD; permissão removida de objetos do AD; proprietário alterado; modificação de configuração de GPO; criação de link de GPO; deleção de link de GPO; modificação de link de GPO;

4.50. Deve realizar, de uma só vez e através de seleção de múltiplos usuários, as seguintes ações: deleção; reset de senha; desbloqueio da conta; habilitação e desabilitação;

4.51. Deve oferecer, através da interface gráfica, visibilidade da hierarquia de diretórios de usuários, todos os domínios, unidades organizacionais, computadores, grupos e demais objetos do domínio;

4.52. Permitir, através de interface gráfica, rastrear no Active Directory quem fez alterações, qual foi a alteração e quando foi executada;

4.53. Permitir auditar diferentes domínios em uma única instalação;

4.54. Permitir que os administradores, ao gerenciar os objetos no AD, sejam capazes de realizar, através da interface gráfica, as seguintes ações: criar novos usuários; criar novos grupos de segurança; excluir usuários; excluir computadores; alterar parâmetros de usuários já existentes; alterar membros de grupos de segurança; reconfigurar senhas; desbloquear usuários; habilitar e desabilitar usuários;

4.55. Permitir, através de relatórios e interface gráfica, trilhas de auditoria classificável e pesquisável de todas as atividades do Active Directory;

4.56. Possibilitar a criação de pastas que sejam automaticamente reconhecidas na interface gráfica e que possam ser automaticamente usadas pelos usuários;

4.57. Oferecer funcionalidade de ajuste aos diretórios com herança de permissões quebradas;

4.58. Deve manter logs sobre as operações de abrir, criar, apagar, modificar, copiar, renomear e acesso negado;

4.59. Deverá suportar em todas as versões os Sistemas Operacionais Windows Server 2016, Windows 7, Windows 10;

4.60. Deve oferecer, através da interface gráfica, as funcionalidades de permissionamento, log, relatórios e análise comportamental dos usuários nos servidores de diretórios de usuários Microsoft Exchange Online;

4.61. Deverá suportar os seguintes comandos PowerShell: Add-MailboxPermission; Remove-MailBoxPermission; Add-MailboxFolderPermission; Remove-MailboxFolderPermission; Set MailboxFolderPermission; Add-ADPermission; Remove-ADPermission;

4.62. Deverá coletar os seguintes eventos de auditoria do Exchange Online: logon; pasta aberta; pasta criada; pasta deletada; pasta renomeada; permissão adicionada à pasta; permissão removida de pasta; permissões de pasta alteradas; pasta movida; mensagem criada; mensagem apagada; mensagem editada; mensagem movida; mensagem copiada; mensagem enviada em (on behalf of); mensagem enviada como (send as);

4.63. Deverá coletar ao menos os seguintes eventos de auditoria do OneDrive: Permissão removida; permissão adicionada; pasta renomeada; pasta deletada; arquivo renomeado; link compartilhado usado; link compartilhado atualizado; link compartilhado removido; link compartilhado criado; convite a pasta/arquivo atualizado; convite a pasta/arquivo cancelado; convite a pasta/arquivo aceito; requisição de acesso a pasta/arquivo aprovado; pasta movida; pasta restaurada; download de arquivo; arquivo movido; arquivo restaurado; arquivo copiado; upload de arquivo; arquivo deletado; arquivo aberto; arquivo modificado; arquivo criado;

4.64. Deve oferecer, através da interface gráfica, as funcionalidades de permissionamento, log, relatórios e análise comportamental para a plataforma OneDrive;

4.65. Estes serviços serão realizados sob demanda de acordo com cada Ordem de Serviço a ser emitida pela CONTRATANTE.

## 5. PROPOSTA COMERCIAL

5.1. A proposta deverá ser apresentada em planilha discriminativa, que deverá conter no mínimo:

a) nome do representante legal da empresa e dados;

b) detalhamento do objeto;

c) as quantidades;

d) valores unitários e totais por unidade, em moeda nacional, em algarismo e por extenso;

e) prazo de validade da proposta não inferior a 90 (noventa) dias;

f) prazo para entrega;

g) dados bancários da empresa, tais como conta corrente número agência e banco

h) CNPJ, telefone/fac-símile, endereço e e-mail;

i) marca e modelo do objeto

j) garantia do objeto; e nos preços já deverão estar consideradas todas as despesas com tributos, fretes, transportes,seguros

k) e demais despesas que incidam direta ou indiretamente no fornecimento desse Elemento técnico.

5.2. Na proposta deverá ser apresentada conforme quadro demonstrativo abaixo:

| Item | Bem/Serviço | Quantidade | Preço Unitário | Preço Total |
|---|---|---|---|---|
| 01 | Licença de subscrição de software para solução de auditoria em Windows File Server pelo período de 12 meses | 7.500 | | |
| 02 | Licença de subscrição de software para solução de auditoria em Microsoft Active Directory pelo período de 12 meses | 10.250 | | |
| 03 | Licença de subscrição de software para solução de auditoria em Exchange Online pelo período de 12 meses | 810 | | |
| 04 | Licença de subscrição de software para solução de auditoria em OneDrive pelo período de 12 meses | 700 | | |
| 05 | Licença de subscrição de software para solução de análise em tempo real e prevenção de comportamentos suspeitos pelo período de 12 meses | 10.250 | | |
| 06 | Operação Assistida (horas) | 50 | | |

## 6. PROVA DE CONCEITO

6.1. A Empresa participante do Ato Convocatório, classificada com a melhor oferta poderá ser convocada pela comissão de compras do Instituto de Gestão Estratégica de Saúde do Distrito Federal para realização da Prova de Conceito - POC, no prazo de até 2 (dois) dias úteis, após abertura das propostas, obedecendo ao seguinte rito:

6.2. O IGESDF irá constituir uma comissão para avaliação da POC e será composta por colaboradores da área técnica da SUTIC;

6.3. A empresa convocada para a POC deverá demonstrar na prova de conceito 100 % (cem por cento) das funcionalidades descritas no Item 4 - Especificações do Objeto;

6.4. Caso a empresa convocada para a POC não demonstre qualquer funcionalidade da solução, será automaticamente desclassificada. A comissão de compras do IGESDF convocará a empresa classificada em segundo lugar e sucessivamente até a comprovação das funcionalidades;

6.5. A comissão julgadora do IGSDF seguirá um roteiro como parâmetro do Ato Convocatório para conferir todas as funcionalidades requeridas;

6.6. Será disponibilizado um local com estrutura adequada para a realização da prova de conceito;

6.7. A prova de conceito terá duração máxima de até 2 (dois) dias, nos horários de 08:00 às 12:00 e 14:00 às 17:00h;

6.8. A comissão de compras, subsidiada pela área técnica da SUTIC, emitirá um laudo da(s) POC (s) realizadas.

6.9. **Roteiro da prova de conceito**

6.9.1. Para fins de verificação de adequação da solução ofertada às especificações técnicas detalhadas apresentadas neste Elemento Técnico, a Empresa participante convocada deverá apresentar a documentação comprobatória das especificações técnicas da solução, composta por:

6.9.2. Documentações originais do fabricante (disponíveis em links de URL's públicos na Internet oficiais do fabricante) e MATRIZ PONTO-A-PONTO contendo, de forma organizada, o item do Elemento Técnico, a indicação do número da página e trecho das documentações originais do fabricante entregues que comprove o atendimento pontual pela solução ofertada de todos os itens da especificação técnica;

6.9.3. A empresa participante detentora do melhor lance poderá ser convocada pela CONTRATANTE para entregar e instalar a solução apresentada na proposta de preços no ambiente computacional da CONTRATANTE no prazo de até 2 dias úteis;

6.9.4. Findo o prazo de entrega e instalação da solução em todo o ambiente computacional da CONTRATANTE, será dado prazo de 5 (cinco) dias úteis para que a solução realize a coleta de dados/informações necessárias à posterior demonstração das funcionalidades da solução exigidas nos itens/subitens do Roteiro de Teste de Conformidade destacados diretamente das especificações técnicas detalhadas deste Elemento Técnico;

6.9.5. Findo o prazo determinado para coleta de dados/informações do ambiente pela solução ofertada, a empresa participante deverá, no prazo de até 2 (dois) dias úteis, demonstrar à contratante o atendimento pontual dos itens contidos no Roteiro de Teste de Conformidade destacados diretamente das especificações técnicas detalhadas deste Elemento Técnico;

6.9.6. O software da solução a ser utilizado no teste não poderá ser diferente do apresentado na proposta de preço e também não poderá ser alterado ou customizado durante o período do teste, sob pena de reprovação;

6.9.7. No decorrer do teste, caso a solução ofertada pela empresa participante não demonstre à equipe técnica da contratante o atendimento de item constante no

6.9.8. **Roteiro de Teste de Conformidade**

6.9.9. o teste poderá ser finalizado para fins de economia processual e a solução ofertada será considerada reprovada;

6.9.10. Além dos representantes da empresa participante responsável pela execução do teste sob supervisão da equipe técnica da contratante, o teste poderá ser observado por somente 1 (um) representante das demais

6.9.11. Empresas participantes do certame,indicados por seus representantes via e-mail, com

nome, cargo, CPF e declaração de vínculo com a empresa;

6.9.12. Durante o período do teste, os observadores somente poderão fazer considerações relativas ao teste à equipe técnica da contratante responsável pelo acompanhamento por escrito e devidamente justificadas em conformidade às especificações deste Elemento Técnico e contidas no escopo do Roteiro de Teste de Conformidade;

6.9.13. Ao final do teste será lavrada a ata do teste a ser assinada pela equipe técnica da contratante, pelos representantes da empresa participante e os observadores, se houverem, com a indicação de atendimento ou não aos itens e a devida indicação de classificação ou desclassificação da empresa participante;

6.9.14. A comprovação dos itens descritos no Roteiro de Teste de Conformidade não desobriga a empresa participante de atender todos os outros itens previstos nas especificações técnicas detalhadas deste Elemento Técnico por meio da comprovação documental prevista no item de matriz ponto-a-ponto;

6.9.15. Caso a solução seja reprovada, a contratante procederá com a convocação da próxima empresa participante no certame em até 3 (três) dias úteis.

6.10. **Roteiro de Teste de Conformidade**

6.10.1. Visando preservar harmonia entre todos os elementos da solução, a total interoperabilidade de componentes e a facilidade de uso e operação, a solução fornecida deverá ser de um único fabricante em que seus módulos e ou programas sejam totalmente integrados e disponibilizados em uma única interface gráfica;

6.10.2. A solução deve fornecer todas as funcionalidades citadas abaixo sem a necessidade de retenção dos logs nativos do Windows. Caso a solução ofertada necessite habilitar o log de auditoria do Windows File Server, o hardware sem ponto único de falha necessário para o armazenamento destes logs por no mínimo 12 (doze) meses deverá ser contemplado na proposta;

6.10.3. Caso a solução ofertada necessite reter o log nativo de auditoria do Active Directory, o hardware sem ponto único de falha necessário para o armazenamento destes logs por 12 (doze) meses deverá ser contemplado na proposta;

6.10.4. Deve ser possível, também, monitorar diferentes domínios independentemente da existência de relação de confiança;

6.10.5. Devido às características e criticidade das informações coletadas, armazenadas e processadas, com o intuito de garantir integridade e confiabilidade jurídica, contratual e regulatória, e pela possibilidade das informações serem utilizadas para perícia forense inclusive como provas judiciais, a solução deverá ter certificação utilizada pela administração pública como parâmetro para definição de requisitos de sistema de gerenciamento de segurança da informação como a ISO/IEC 27001 ou similares;

6.10.6. A solução deverá exibir para cada pasta dos recursos monitorados a visualização gráfica e interativa das listas de controle de acesso incluindo grupos, subgrupos e seus respectivos membros;

6.10.7. A interface gráfica deverá permitir a busca por um usuário ou grupo e apresentar graficamente seus níveis de permissão nos diretórios dos recursos monitorados. Esta visibilidade deve incluir herança de permissão ativa/desativada e indicação de compartilhamento;

6.10.8. A solução deve permitir a modelagem de permissionamento de maneira gráfica antes da aplicação em produção. Esta modelagem deve demonstrar os impactos das mudanças pretendidas nos grupos e usuários em relação a suas permissões nos diretórios monitorados, ou seja, deve ser possível analisar quais acessos os usuários ganharão ou perderão antes que essas alterações sejam efetuadas em produção;

6.10.9. A solução deve oferecer a opção de aplicação completa ou parcial das alterações pretendidas nos grupos, usuários e permissões assim como oferecer a opção de efetivação imediata ou agendada no Active Directory e servidores monitorados;

6.10.10. A solução deve oferecer a opção de aplicação das alterações utilizando uma credencial diferente da credencial do usuário logado na interface gráfica assim, a modelagem pode ser feita por um usuário e efetivada por outro usuário, este último, com permissões de alterações no Active Directory;

6.10.11. A solução deve fornecer a visibilidade sobre aplicações de alteração que estão pendentes e o histórico das alterações aplicadas através da console;

6.10.12. A solução deve apresentar todos os logs de todos os usuários e de todas as plataformas monitoradas na mesma console de visibilidade de permissionamento;

6.10.13. A solução ofertada deve manter o log das operações de abrir, criar, apagar, modificar, copiar, renomear e acesso negado;

6.10.14. Os logs apresentados pela solução ofertada devem conter informações completas de cada uma das operações com data e horário, nome do servidor, tipo do objeto, caminho (path) dos dados, domínio, arquivo impactado e nome do usuário;

6.10.15. A solução deverá permitir filtragem gráfica, ordenação e agrupamento dos logs;

6.10.16. Fornecer resumo gráfico das atividades auditadas, incluindo (visualização dos usuários mais e menos ativos; visualização dos diretórios mais e menos acessados; visualização dos diretórios onde um usuário ou um grupo de usuários estejam acessando; visualização dos usuários que estejam acessando um diretório);

6.10.17. A solução deverá permitir que os usuários realizem pesquisas baseados em critérios como: data do evento, servidor ou plataforma em que o evento ocorreu, tipo de evento, arquivos ou diretórios acessados;

6.10.18. Deve ser possível alterar o conjunto de dados (colunas) retornados da consulta aos logs de acordo com a necessidade da informação;

6.10.19. A ferramenta deve permitir o agendamento para envio de relatórios pelo correio eletrônico ou para um compartilhamento no servidor de arquivos;

6.10.20. A ferramenta deve fornecer relatório de todas as permissões de determinado usuário nos repositórios monitorados;

6.10.21. A ferramenta deve fornecer relatório de todos os usuários com permissões em determinada pasta;

6.10.22. A ferramenta deve fornecer relatório dos acessos aos arquivos;

6.10.23. Fornecer relatório de onde há permissões concedidas a grupos globais (Everyone, Domain Users, Users, AuthenticatedUsers);

6.10.24. Fornecer relatórios de SIDs não resolvidos e usuários com permissão direta em pastas;

6.10.25. Fornecer relatórios de dados e usuários inativos;

6.10.26. Fornecer relatórios de usuários desabilitados que ainda fazem parte de grupos de segurança;

6.10.27. Fornecer relatório de lista de usuários administradores em grupos não administrativos;

6.10.28. Fornecer relatório de lista de permissões de usuários desabilitados;

6.10.29. Fornecer relatório de pastas sem administradores;

6.10.30. A solução deve fornecer relatório de auditoria das ações dos usuários na console;

6.10.31. A solução deve oferecer relatório sobre as alterações, versão alterada e quais foram as mudanças realizadas em GPOs;

6.10.32. A solução deve identificar, de forma automática, usuários com acesso a pastas e\ou arquivos indevidos sugerindo a revogação de acesso;

6.10.33. A solução deverá fornecer em modo gráfico recomendações sobre permissionamento excessivo, baseado na análise de atividade de acesso;

6.10.34. A solução ofertada deve manter o log das operações de abrir, criar, apagar, modificar, copiar, renomear e acesso negado;

6.10.35. A solução deve fornecer funcionalidade de ajuste aos diretórios com herança de permissões quebradas;

6.10.36. A solução deve possibilitar a criação de pastas que sejam automaticamente reconhecidas na interface gráfica e que possam ser automaticamente usadas pelos usuários;

6.10.37. A solução deve possuir visibilidade da hierarquia do serviço de Diretórios de Usuários através de interface gráfica;

6.10.38. A solução deve suportar a auditoria dos seguintes eventos do Directory Service: Criação de deleção de dos objetos; Membros adicionados e removidos de grupos de segurança; Alteração nas propriedades do objeto do AD; Requisição de acesso; Autenticação de conta; Reset de senhas; Bloqueio e desbloqueio de conta; Criação e deleção de conta; Habilitação e desabilitação de conta; Permissão adicionada a objeto do AD, Permissão removida de objeto do AD, Proprietário alterado; Modificação de configuração de GPO; Criação de link de GPO; Deleção de link de GPO; Modificação de link de GPO;

6.10.39. Deverá ser possível o gerenciamento de objetos do AD.

6.10.40. É necessário que os usuários administradores sejam capazes de realizar as seguintes ações através da interface gráfica da solução: Criar novos usuários; Criar novos grupos de segurança; Alterar parâmetros de usuários já existentes; Alterar membros de grupos de segurança; Excluir usuários; Excluir computadores; Reconfigurar senhas; Desbloquear usuários; Habilitar e desabilitar usuários;

6.10.41. A solução deve possuir as funcionalidades de visibilidade de permissionamento, log, relatórios, análise comportamental e alertas no Microsoft Exchange Online e deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios de dados;

6.10.42. Possuir as funcionalidades de Permissionamento, Registro de Eventos, Relatórios e Análise Comportamental para a plataforma OneDrive e deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios de dados;

6.10.43. Nos alertas em tempo real, deve ser possível configurar para que, um usuário, uma pasta, um período ou uma ação específica seja alertada caso ocorra ação que os envolva;

6.10.44. Os alertas poderão ser iniciados com base nos dados da auditoria, tais como usuário, ação, data e hora, ação realizada;

6.10.45. Os alertas devem ser apresentados também em dashboard web que apresente: quantidade de alertas e suas severidades em determinado período, usuários mais alertados em determinado período, tipos de alertas que mais ocorreram, máquinas que foram mais utilizadas para as ações suspeitas, classificação dos alertas dentro de um cenário de ataque cibernético;

6.10.46. O dashboard deve apresentar os eventos que motivaram o alerta para que o time de segurança possa fazer investigação forense.

## 7. HABILITAÇÕES DA EMPRESA

7.1. O Fornecedor deverá apresentar os documentos referentes à regularidade fiscal, jurídica e técnica, conforme relacionados abaixo:

7.2. **Referentes às Regularidades Fiscais:**

a) CNPJ - Comprovante de inscrição e de situação cadastral no Cadastro Nacional de Pessoa Jurídica;

b) União - Certidão Negativa de regularidade com a Fazenda Federal, mediante certidão conjunta negativa de débitos, ou positiva com efeitos de negativa, relativos aos tributos federais e à Dívida Ativa da União;

c) CNDT - Certidão Negativa de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante Certidão Negativa de Débitos Trabalhistas, ou certidão positiva com efeitos de negativa;

d) FGTS - Certidão Negativa de regularidade relativa ao Fundo de Garantia do Tempo de Serviço, mediante Certificado de Regularidade;

e) Certidão Negativa de regularidade perante as Fazendas Municipal, Estadual ou Distrital da sede do fornecedor;

f) CEIS - Cadastro Nacional de Empresas Inidôneas e Suspensas, mantido pela Controladoria Geral da União;

g) CNJ - Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça;

h) TCU - Lista de Inidôneos, mantida pelo Tribunal de Contas da União; e

i) Certidão Negativa de Falência ou Concordata (art.192, Lei n°11.101/2005), Recuperação Judicial ou Extrajudicial e Execução patrimonial, expedidas pelo setor de distribuição da Justiça Comum, Justiça Federal e Justiça do Trabalho do domicílio ou domicílios da pessoa física ou jurídica.

7.3. **Referentes à Habilitação Jurídica:**

a) Cópia da Cédula de identidade, quando se tratar de empresa Pessoa Física;

b) No caso de empresa individual: registro empresarial na junta comercial;

c) No caso de sociedades comerciais: Ato Constitutivo, Estatuto ou Contrato Social em vigor, devidamente registrado na junta comercial. Os documentos deverão estar acompanhados de todas as alterações ou da consolidação respectiva;

d) Documento comprobatório autenticado de seus administradores reconhecido nacionalmente (CNH, carteira de identidade, registro profissional ou outro);

e) No caso de sociedades por ações: Ato Constitutivo, Estatuto ou Contrato Social em vigor,

f) devidamente registrado, acompanhado de documentos de eleição de seus administradores, em exercício;

g) No caso de sociedades civis: inscrição do Ato constitutivo e alterações subsequentes no Registro civil das Pessoas Jurídicas, prova de diretoria em exercício; acompanhada de prova de diretoria em exercício;

h) No caso de empresa ou sociedade estrangeira em funcionamento no país: decreto de autorização e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir; e

i) Para todos os efeitos, considera-se como Ato Constitutivo, Estatuto ou Contrato Social em vigor, o documento de constituição da empresa, acompanhado da (s) última (s) alteração (ões)

j) Referente (s) à natureza da atividade comercial e à administração da empresa, ou a última alteração consolidada.

7.4. **Quanto à Representação:**

a) Se representante legal apresentar procuração por instrumento particular ou público, com poderes para praticar os atos pertinentes da Seleção de Fornecedores;

b) Na hipótese de procuração por instrumento particular, deverá vir acompanhada do documento constitutivo do proponente ou de outro documento em que esteja expressa a capacidade/competência do outorgante para constituir mandatário; e

c) O representante legal constante na procuração deverá apresentar documento comprobatório autenticado reconhecido nacionalmente(CNH, carteira de identidade, registro profissional ou outro), assim como do sócio outorgante.

d) A qualquer momento durante o processo ou no prazo de vigência do instrumento contratual, o IGESDF poderá solicitar, para fins de comprovação, as cópias autenticadas ou os originais da documentação exigida neste elemento técnico.

## 8. CONDIÇÕES DE ENTREGA

8.1. Os produtos deverão ser entregues no IGESDF no endereço SHMS - ÁREA ESPECIAL - QUADRA 101 - BLOCO A, Brasília - DF, CEP: 70.335-900, no horário de 09h00min as 17h00min horas, conforme local indicado na ordem de fornecimento. O Fornecedor dirigir-se-á ao local da entrega munido da(s) Nota Fiscal(is) e da Ordem de Fornecimento;

8.2. Durante a vigência do instrumento contratual ou/até o recebimento definitivo do objeto, o local de entrega para fornecimento poderá sofrer modificações, a critério do IGESDF. Neste caso, o novo endereço para entrega constará na Ordem de Fornecimento.

8.3. O prazo para entrega dos produtos será de 30 (trinta) dias corridos, contados do recebimento pelo detentor da Ordem de Fornecimento, exceto quando, a critério do IGESDF, for estabelecido prazo superior na Ordem de Fornecimento.

8.3.1. Os produtos deverão ser entregues da seguinte forma:

a) O fornecedor deverá indicar na(s) nota(s) fiscal(is),além de outras informações exigidas de acordo com a legislação específica:

b) Número da ordem de fornecimento;

c) O nome do material;

d) A marca e o nome comercial;

e) Deverá conter o tipo de instrumento contratual ou número Seleção de Fornecedores;

8.4. Em caso de descumprimento, a empresa estará sujeita às penalidades previstas no item 15 deste Elemento Técnico, além das previstas no Regulamento Próprio de Compras e Contratações do IGESDF.

## 9. VIGÊNCIA

9.1. O instrumento contratual decorrente do presente Elemento Técnico terá vigência a partir da data de sua assinatura até o recebimento definitivo do objeto, que deverá ocorrer no prazo fixado no item 8.4.

9.2. O prazo de vigência da contratação é de 12 (doze) meses corridos, havendo a possibilidade de ser prorrogado posteriormente, mediante Termo Aditivo nos termos do Art. 29 do

## 10. OBRIGAÇÕES DA CONTRATADA

10.1. Cumprir o objeto deste elemento técnico, dentro do prazo fixado, em conformidade com a proposta apresentada, ficando ao seu cargo todos os ônus e encargos decorrentes do fornecimento.

10.2. Ao emitir a nota fiscal o Fornecedor deverá seguir fielmente a descrição do produto, conforme descrição do item 3.

10.3. Acusar o recebimento da Ordem de Fornecimento encaminhada por meio do endereço eletrônico correspondente ao seu envio.

10.4. Manter atualizados os dados cadastrais, comunicando ao IGESDF toda e qualquer alteração.

10.5. Fornecer o(s) produto(s), rigorosamente, de acordo com as especificações constantes no item 4, não se admitindo procrastinação em função de pedido de revisão de preço ou substituição de marca.

10.6. Responsabilizar-se pelo transporte do(s) produto(s) de seu estabelecimento até o local determinado, bem como pelo seu descarregamento até o interior do local de entrega, observando as regras para manutenção da sua qualidade.

10.7. Garantir a boa qualidade do(s) produto(s) fornecido(s), respondendo por qualquer deterioração, substituindo sempre que for o caso.

10.8. Arcar com todas as despesas pertinentes ao fornecimento registrado, tais como tributos, fretes, embalagem e demais encargos.

10.9. Responder, integralmente, pelos danos causados ao IGESDF ou a terceiros, decorrentes de sua culpa ou dolo, quando da execução dos serviços.

10.10. Os produtos deverão ser entregues conforme as exigências deste instrumento.

## 11. PARCELAMENTO DO OBJETO.

11.1. Objeto não será parcelado, uma vez que todos os produtos e serviços a serem prestados são componentes de uma única solução, a qual não pode ser desmembrada sem que haja perda de produtividade e economia de escala, já que a especificidade do objeto demanda um tratamento que inviabiliza a realização de suas etapas por diferentes participantes.

11.2. Não-parcelamento destes serviços e produtos está amparado na legislação específica, conforme acórdão no que manifestou o entendimento de que, havendo dependência entre os serviços e produtos que compõem o objeto, a opção pelo não parcelamento mostra-se adequada, no mínimo do ponto de vista técnico, permitindo a composição, em um único grupo (lote);

11.3. Não serão aceitos consórcios e terceirizações.

## 12. OBRIGAÇÕES DA CONTRATANTE

12.1. Indicar os locais e horários em que deverá ser entregue o produto.

12.2. Autorizar o pessoal da Contratada, acesso ao local da entrega desde que observadas às normas de segurança do IGESDF;

12.3. Rejeitar no todo ou em parte, o produto entregue em desacordo com as obrigações assumidas pelo fornecedor;

12.4. Garantir o contraditório e ampla defesa;

12.5. Efetuar o pagamento à Contratada nas condições estabelecidas deste Elemento Técnico;

12.6. Acompanhar e fiscalizar a execução do instrumento contratual, bem como atestar na nota fiscal/fatura a efetiva execução do objeto.

12.7. Notificar a Contratada, por escrito, sobre imperfeições, falhas ou irregularidades constatadas na execução da entrega deste Elemento Técnico, para que sejam adotadas as medidas corretivas necessárias.

## 13. FISCALIZAÇÃO

13.1. A fiscalização e atesto das Nota (s) Fiscal (is) será realizado pela Gerência de Gestão de Infraestrutura de Tecnologia da Informação da Superintendência de Tecnologia da Informação do IGESDF.

## 14. PAGAMENTO

14.1. O pagamento do serviço será realizado conforme abaixo através de Ordens de Serviços:

| Item | Descrição do item |
|---|---|
| 1 a 5 | Licenciamento tipo subscrição - Pagamento em parcela única em até 30 (trinta) dias úteis após a disponibilização do quantitativo das licenças demandadas em cada Ordem de Serviço. |
| 6 | Operação assistida - Pagamento realizado até 30 (trinta) dias úteis após o termo de aceite do serviço |

14.2. Será por meio de depósito bancário em conta corrente, contados do recebimento da Nota Fiscal devidamente atestada pela Unidade responsável.

14.3. Sendo o pagamento realizado mediante depósito em conta corrente, o Fornecedor não deverá fazer a emissão de boleto bancário, sob pena de haver cobrança indevida.

## 15. PENALIDADES

15.1. O atraso injustificado na entrega do(s) serviço(s) e produto(s), objeto do presente Elemento Técnico, sujeitará o fornecedor, sem prejuízo das sanções previstas nos artigos 35, 41, 42 e 43 do Regulamento Próprio de Compras e Contratações do IGESDF, às seguintes multas:

15.2. 0,1% (um décimo por cento) ao dia, sobre o valor total da aquisição, até o limite de 30 (trinta) dias;

15.3. 10% (dez por cento), cumulativamente, sobre o valor total da aquisição, após 30 (trinta) dias, podendo ainda o IGESDF, a seu critério, impedir o fornecedor de participar de novas cotações com este Instituto.

15.4. O atraso injustificado de entrega dos itens superior a 30 (trinta) dias corridos, será considerado como inexecução total do objeto, devendo o instrumento respectivo ser rescindido, salvo razões de interesse público devidamente explicitadas no ato da autoridade competente do HB ou IGESDF.

## 16. DOS CRITÉRIOS PARA ACEITAÇÃO DAS PROPOSTAS

16.1. A proposta de preços deverá conter o prazo de validade e planilha de custo, discriminando o custo unitário por item e o valor total dos serviços a serem executados no IGESDF.

16.2. Nos preços apresentados deverão estar incluídas todas as despesas com materiais, mão de obra, deslocamentos, hospedagens, ferramentas, equipamentos, seguros, taxas, tributos, incidências fiscais e contribuições de qualquer natureza ou espécie, encargos sociais, custos diretos e indiretos e quaisquer outros encargos, quando necessários à perfeita execução do objeto da presente solicitação.

## 17. DO CRITÉRIO DE JULGAMENTO DAS PROPOSTAS:

17.1. Atendidos todos os requisitos estabelecidos neste documento, será contratada a empresa que apresentar o MENOR PREÇO GLOBAL, e atenda as qualificações desta Especificação Técnica, nos termos do Regulamento de Compras e Contratações do IGES-DF.

## 18. LOCAL E DATA

Brasília/DF, 17/fevereiro/2020.

Identificação do Responsável pela elaboração do Elemento Técnico nº 3/2020:

Thiago de Lacerda Chaves

Chefe de Núcleo de Redes

00004166

Identificação do Responsável da área técnica:

Edilmara Albino Dato

Gerente de Infraestrutura de Tecnologia da Informação

00004274

Na atribuição de autoridade imediata superior responsável pela Superintendência de Tecnologia da Informação e Comunicação, APROVO e AUTORIZO o presente Elemento Técnico, em observância ao Art. 2º, §1º do Regulamento Próprio de Compras e Contratações do IGESDF.

Marcos Flávio de Souza

Superintendente de Tecnologia da Informação e Comunicação

00003074

Documento assinado eletronicamente por **THIAGO DE LACERDA CHAVES - Matr.0000416-6**, **Chefe de Núcleo**, em 18/02/2020, às 13:59, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **EDILMARA ALBINO DATO - Matr.0000427-4**, **Gerente**, em 18/02/2020, às 14:02, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **MARCOS FLAVIO DE SOUZA - Matr. 0000304-7**, **Superintendente**, em 18/02/2020, às 14:03, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **35737092** código CRC= **7C623C95**.