MINISTÉRIO PÚBLICO DA UNIÃO
MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS
Seção de Contratação de Soluções de TI - STI
Praça Municipal - Eixo Monumental - Brasília - DF

ESPECIFICAÇÃO TÉCNICA E QUANTIDADES

(Registro de preços para a contratação de empresa especializada no fornecimento de licenças e serviços Microsoft)

ANEXO I – ESPECIFICAÇÃO TÉCNICA

1. ESPECIFICAÇÃO TÉCNICA

GRUPO	ITEM	DESCRIÇÃO	PART NUMBER	ID SGD8*	QUANTIDADE / UNIDADE
1	1	Subscrição da licença Office 365 E1	T6A-00024	MS.4.0-A1723	2600 / UN
	2	Subscrição da licença Office 365 E3	AAA-10842	MS.4.0-A0871	1000 / UN
	3	Subscrição da licença Office 365 E5	SY9-00004	MS.4.0-A1698	100 / UN
	4	Subscrição do complemento de licença de Office 365 E1 (STEP UP) para Office 365 E3	AAA-10906	MS.4.0-A0877	1600 / UN
	5	Subscrição da licença Microsoft 365 E3	AAD-33204	MS.4.0-A0936	2600 / UN
	6	Subscrição do complemento de licença de Office 365 E3 (STEP UP) para Microsoft 365 E3	AAD-86538	MS.4.0-A0941	2600 / UN
	7	Subscrição do complemento de licença de Office 365 E5 (STEP UP) para Microsoft 365 E5	AAD-86532	MS.4.0-A0939	100 / UN
	8	Subscrição da licença Exchange Online Kiosk	7TC-00001	MS.4.0-A0507	1000 / UN
	9	Espaço extra de armazenamento do SharePoint Online em Gibabytes - GB	6WT-00001	MS.4.0-A0318	16000 / UN
	10	Subscrição do complemento da licença Microsoft Entra ID P1 (antigo Azure Active Directory Premium P1) para Microsoft Entra ID P2	6E6-00004	MS.4.0-A0283	2700 / UN
	11	Subscrição da licença Microsoft Entra ID P2 (antigo Azure Active Directory Premium P2)	6E6-00003	MS.4.0-A0282	2700 / UN
	12	Subscrição da licença PowerAppsPlan ShrdSvr ALNG SubsVL MVL PerUsr	SEJ-00002	MS.4.0-A1683	50 / UN
	13	Subscrição da licença Power Pages Auth Users T1 Sub (100 User/Site/Mo)	VQQ-00002	-	50 / UN

	14	Power Automate Premium Sub Per User	1O4-00001	-	50 / UN
	15	Subscrição da licença Copilot Studio Sub (Messages)	YFI-00001	-	20 / UN
	16	Subscrição da licença Power Automate Process Sub	8F5-00001	-	5 / UN
	17	Subscrição da licença Power Automate Hosted RPA Sub Add-on	WLN-00001	-	5 / UN
	18	Subscrição da licença M365 Copilot Managed Sub Add-on	83I-00001	-	700 / UN
	19	Azure prepayment(crédito)	6QK-00001	-	100 / UN
	20	Subscrição da licença SQL Server Enterprise Core ALng LSA 2L	7JQ-00341	MS.4.0-A0455	36 / UN
	21	Subscrição da licença SQL Server Standard Core ALng LSA 2L	7NQ-00302	MS.4.0-A0489	16 / UN
2	22	Serviço de Implementação de Hardening Office 365 E1	-	-	1 / UN
	23	Serviço de Implementação de Hardening Microsoft 365 E3	-	-	1 / UN
	24	Serviço de Implementação de Hardening Microsoft 365 E5	-	-	1 / UN
	25	Serviço de migração das contas AD e email para nuvem	-	-	1 / UN

*****Conforme Acordo Corporativo nº 8/2020, firmado entre a União, por intermédio da Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, doravante denominada SGD/ME, e do outro lado a empresa Microsoft do Brasil Importação e Comércio de Software e Video Games Ltda.

https://www.gov.br/governodigital/pt-br/contratacoes/catalogo-de-solucoes-de-tic

2. REQUISITOS GERAIS DO LICENCIAMENTO (ITENS 1 A 21)

2.1. Devido às particularidades desta contratação, os objetos devem ser fornecidos por um único revendedor qualificado LSP (*Large Solution Partner*) autorizado a atender contas governamentais, conforme a política do fabricante.

2.2. Os produtos devem ser licenciados de acordo com as condições estabelecidas no Acordo Corporativo Nº 8/2020, dos Catálogos de Soluções de TIC, seguindo as normas da Secretaria de Governo Digital - SGD/MGI.

2.3. Os produtos deverão ser disponibilizados na versão mais atual disponível.

2.4. A CONTRATADA precisa disponibilizar comprovante de registro que garanta o direito de atualização das licenças no site do fabricante durante o período de vigência do contrato.

2.5. O serviço de atualização das licenças será prestado dentro do período de vigência do contrato e consiste no fornecimento para a CONTRATANTE de todas as versões, *features, releases, fixes e service packs,* de forma a manter a solução permanentemente atualizada, bem como, no fornecimento de manuais e boletins técnicos com informações que assegurem a plena utilização dos produtos licenciados sem custo adicional para a CONTRATANTE.

2.6. Caso haja atualização disponível da solução e a CONTRATANTE não consiga realizar o seu download por meio da Internet, esta entrará em contato com a CONTRATADA, que deverá disponibilizá-la dentro dos prazos definidos neste documento.

2.7. A CONTRATADA deverá prestar assessoria técnica e administrativa na correta ativação de todo o licenciamento.

2.8. A solução deverá suportar no mínimo os seguintes níveis de usuários:

2.8.1. Usuário Comum, dividido em categorias de acordo com as licenças disponibilizadas: básico, intermediário e avançado;

2.8.2. Usuário Administrador: Permissão para criar, excluir e alterar dados e contas dos clientes, além de acessar o portal de operações, gerenciar os serviços e realizar pesquisas e auditorias.

2.9. As contas e-mail usarão o domínio principal @mpdft.mp.br, possibilitando a utilização de domínios secundários do @mpdft.mp.br, como por exemplo o @mpdft.gov.br, entre outros.

2.10. As interfaces e telas das soluções oferecidas devem estar disponíveis no idioma Português do Brasil.

2.11. A solução deve possuir arquitetura redundante garantindo a continuidade da prestação do serviço, exceto em interrupções programadas de serviços, que devem ser informadas à CONTRATANTE conforme prazos estabelecidos neste documento.

2.12. A solução deve possuir site de administração que permita à CONTRATANTE o gerenciamento de todo o conjunto de serviços contratados, provendo equivalência na gestão de contas, listas, grupos e outro recurso à solução on premise atualmente utilizada.

2.13. A solução deve possibilitar aos usuários finais da solução fazer logon único para acesso aos serviços disponíveis.

2.14. A solução deve oferecer serviços baseados na Internet projetados para atender à necessidade de segurança, confiabilidade e produtividade do usuário.

2.15. A solução deverá ser acessada através de criptografia TLS (*Transport Layer Security)* ou SSL (*Secure Sockets Layer*) de pelo menos 256bits.

2.16. A CONTRATADA ou fabricante deverá monitorar constantemente a solução contra qualquer atividade suspeita ou incomum.

2.17. A solução deve permitir administração remota através da console Web e/ou via linha de comando.

2.18. A solução deve permitir que os administradores possam realizar tarefas através de scripts ou processos automatizados.

2.19. A solução deve possuir interface de acesso aos serviços, compatível, no mínimo, com os seguintes navegadores: Internet Explorer 10, Mozilla Firefox 27, Google Chrome 30 e Safari 11, ou superiores.

2.20. A solução deve permitir aos administradores a configuração de diretivas de controle de acesso por usuários ou grupos específicos dentro da empresa, usando a interface gráfica baseada na web.

2.21. A solução deve dispor de serviços ou utilitários para migração de contas legadas para ambiente em nuvem.

2.22. A solução deverá estar disponível de forma integral 24 horas por dia, 07 dias por semana.

2.23. A CONTRATADA não deve analisar ou processar o conteúdo dos e-mails para qualquer finalidade que não seja a prestação do serviço contratado.

2.24. A CONTRATADA não deve analisar, processar ou indexar o conteúdo do e-mail para fins publicitários ou de criação de perfil de usuários.

2.25. A CONTRATADA não recolherá qualquer informação sobre o uso da Internet ou a localização por parte dos usuários.

2.26. A plataforma deve possibilitar, a qualquer momento, a migração de dados para nuvem ou de volta à infraestrutura local.

2.27. A plataforma deverá ter a capacidade de sincronizar com o Microsoft Active Directory, de tal forma que a criação e manutenção de usuários e listas de distribuição sejam centralizadas no data center (on premise) da CONTRATANTE.

2.28. Para autenticação do usuário, a solução deverá sincronizar a senha do Microsoft Active Directory com o serviço de nuvem ou oferecer mecanismos de autenticação federada. Os componentes usados para essa finalidade devem ser criados pelo mesmo fabricante da solução, de tal forma que não haja nenhum código de terceiros manipulando essa informação.

2.29. **SUPORTE TÉCNICO**

2.29.1. O serviço de suporte técnico à solução fornecida e implementada se destina a correção de problemas e esclarecimento de dúvidas sobre configuração, funcionamento, manutenção e atualização da solução ofertada.

2.29.2. Os serviços serão solicitados pela equipe técnica do MPDFT mediante abertura de chamado junto à CONTRATADA, caso o fabricante não reserve para si a responsabilidade pelo atendimento, via chamada telefônica local ou gratuita, e-mail ou sítio na Internet, devendo o recebimento dos chamados ocorrer em período integral (24x7x365).

2.29.3. Os atendimentos poderão ser realizados remotamente (via Internet, telefone ou e-mail) ou presencialmente, se necessário, sem custo adicional para o CONTRATANTE.

2.29.4. Não haverá limite de quantidade de chamados durante a vigência do contrato.

2.29.5. Todos chamados deverão ser tratados em língua portuguesa do Brasil.

2.29.6. O que não estiver previsto no edital deverá obedecer às regras de comercialização do fabricante, tendo como referência básica os seguintes links:

https://www.microsoft.com/pt-br/Licensing/licensing-programs/enterprise?rtc=1&activetab=enterprise-tab%3aprimaryr2

https://www.microsoft.com/pt-br/microsoft-365/enterprise/

https://learn.microsoft.com/pt-br/azure/cost-management-billing/manage/ea-portal-agreements

https://learn.microsoft.com/pt-br/azure/cost-management-billing/manage/ea-portal-enrollment-invoices

https://learn.microsoft.com/pt-br/azure/cost-management-billing/manage/ea-azure-marketplace

https://learn.microsoft.com/pt-br/azure/cost-management-billing/manage/cancel-azure-subscription

2.30. **NÍVEL MÍNIMO DE SERVIÇO (NMS)**

2.30.1. Os chamados serão classificados e deverão ser atendidos, em comum acordo pelas partes, de acordo com a SEVERIDADE do problema e prazos (em horas corridas) para início de atendimento e para o fim do atendimento com uma solução definitiva ou de contorno abaixo definidos:

NÍVEL DE SEVERIDADE	**DESCRIÇÃO**	**PRAZOS DE ATENDIMENTO**	
		Início	Término
NÍVEL 1 – Situação crítica / Sistema indisponível	Componente da Solução crítico para a CONTRATANTE indisponível; As operações de negócio foram severamente interrompidas; Um componente de software da solução está tornando serviços de rede indisponíveis; Falha em alguma interface/componente/solução crítica.	1 hora	2 horas
NÍVEL 2 – Impacto grave	Um componente da Solução tem seu uso gravemente restringido, causando impacto significativo para o ambiente da CONTRATADA; e Serviço crítico parcialmente indisponível ou com degradação de tempo de resposta.	2 horas	4 horas
NÍVEL 3 – Impacto moderado	Um componente da Solução não-crítico não está funcionando corretamente, ou apresenta desempenho degradado, causando impacto moderado para a CONTRATANTE	8 horas	16 horas
NÍVEL 4 – Impacto mínimo	Um componente da Solução não-crítico não está funcionando corretamente, causando impacto mínimo para a CONTRATANTE; Consulta sobre problemas e dúvidas gerais sobre a Solução de forma repetitiva para obtenção de resposta; Erro na documentação da Solução; e Aplicado para instalação, configuração, manutenção preventiva e esclarecimento técnico relativo à Solução.	16 horas	36 horas

3. SERVIÇOS

3.1. ITEM 22 - SERVIÇO DE IMPLEMENTAÇÃO DE HARDENING OFFICE 365 E1

3.1.1. A contratada deverá executar as atividades abaixo conforme o CIS BENCHMARK mais recente disponível para download em www.cisecurity.org . Essas atividades de melhores práticas de segurança têm por finalidade diminuir a superfície de ataque no ambiente.

3.1.2. As atividades estão separadas por tipos de licenças:

Office 365 E1 – Implementação Hardening	
Atividades	1
Configuração do MFA “Autenticação Multifator”.	
Sanitização das contas administrativas existentes. • Garantir que todas as contas administrativas estão somente na nuvem. • Garantir que não tem licenças aplicadas para essas contas. • Garantir que está ativado MFA para contas administrativas. • Configurar MFA resistente a phishing' para administradores • Segmentar funções administrativas.	
Validar e alterar política de senhas. • Nível de complexidade • 10 últimas senhas repetidas • Número de caracteres	
Configurar auditoria de contas administrativas.	
Customização do EOP “Exchange online”. • Auditoria de caixa de correio	
Manutenção do Microsoft Secure Score.	
Operação assistida “12 horas” uma vez ao mês durante 12 meses para relatório de segurança. 144 horas ano. • Certifique-se de que o relatório de uso do aplicativo seja revisado pelo menos semanalmente. • Certifique-se de que o relatório de atividades de redefinição de senha de autoatendimento seja revisado pelo menos semanalmente. • Certifique-se de que o relatório 'Inscrições arriscadas' do Azure AD seja revisado pelo menos semanalmente. • Certifique-se de que as regras de encaminhamento de correspondência sejam revisadas pelo menos semanalmente. • Verificação do Microsoft secure score	

3.2. ITEM 23 - SERVIÇO DE IMPLEMENTAÇÃO DE HARDENING MICROSOFT 365 E3

3.2.1. A contratada deverá executar as atividades abaixo conforme o CIS BENCHMARK mais recente disponível para download em www.cisecurity.org . Essas atividades de melhores práticas de segurança têm por finalidade diminuir a superfície de ataque no ambiente.

3.2.2. As atividades estão separadas por tipos de licenças:

Microsoft 365 E3 – Implementação Hardening	
Atividades	1
Configuração do MFA “Autenticação Multifator”.	
Sanitização das contas administrativas existentes. • Garantir que todas as contas administrativas estão somente na nuvem. • Garantir que não tem licenças aplicadas para essas contas. • Garantir que está ativado MFA para contas administrativas. • Configurar MFA resistente a phishing' para administradores • Segmentar funções administrativas.	
Validar e alterar política de senhas. • Nível de complexidade • 10 últimas senhas repetidas • Número de caracteres	
Configurar auditoria de contas administrativas.	
Customização do EOP “Exchange online”. • Auditoria de caixa de correio	
Manutenção do Microsoft Secure Score.	
Operação assistida “12 horas” uma vez ao mês durante 12 meses para relatório de segurança. 144 horas ano. • Certifique-se de que o relatório de uso do aplicativo seja revisado pelo menos semanalmente. • Certifique-se de que o relatório de atividades de redefinição de senha de autoatendimento seja revisado pelo menos semanalmente. • Certifique-se de que o relatório 'Inscrições arriscadas' do Azure AD seja revisado pelo menos semanalmente. • Certifique-se de que as regras de encaminhamento de correspondência sejam revisadas pelo menos semanalmente. • Verificação do Microsoft secure score	
Verificação de configuração dos grupos do Microsoft 365 “públicos” para aprovação.	
Bloquear a entrada da conta associada à caixa de correio compartilhada diretamente.	
Configurar o bloqueio automático de sessão em ativos corporativos após um período definido de inatividade.	

Configurar para que o 'compartilhamento externo' de calendários não esteja disponível.
Configurar a proibição para que os usuários instalem suplementos no Word, Excel ou PowerPoint.
Configurar a proteção interna contra phishing para Formulários “forms”.
Configurar para que 'serviços de armazenamento de terceiros' sejam restritos no 'Microsoft 365 na Web'.
Configurar o Sways para que não possa ser compartilhado com pessoas fora da organização.
Ativar o filtro de tipos de anexos comuns.
Configurar política para alertar administradores quando um malware for enviado por um usuário.
Configurar as políticas de spam do Exchange Online para notificar os administradores.
Verificar os registros SPF/DMARC/DKIM publicados para os domínios do Exchange.
Restringir usuários não administradores de criar locatários.
Desabilitar 'conexões de conta do LinkedIn' para evitar phishing.
Verificar se a sincronização de hash de senha esteja habilitada para implantações híbridas.
Habilite a frequência de login para que as sessões do navegador não sejam persistentes para usuários administrativos.
Habilitar políticas de risco de usuário do Azure AD Identity Protection.
Habilitar políticas de risco de entrada da Proteção de Identidade do Azure AD.
Habilitar listas personalizadas de senhas banidas.
Configurar as 'revisões de acesso' para usuários convidados.
Configurar as 'revisões de acesso' para funções do Azure AD com privilégios elevados.
Certifique-se de que 'AuditDisabled' organizacionalmente esteja definido como 'False.
Habilitar a auditoria de caixa de correio para usuários do E3.
Certifique-se de que 'AuditBypassEnabled' não esteja habilitado em caixas de correio.
Bloquear ou desativar todas as formas de encaminhamento de e-mail.
Desabilitar que os usuários instalem suplementos do Outlook.
Configurar a autenticação moderna do Exchange Online.
Habilitar MailTips para usuários finais.
Certifique-se de que a autenticação moderna para aplicativos do SharePoint seja necessária.
Habilitar a integração do SharePoint e do OneDrive com o Azure AD B2B.
Configurar o compartilhamento de conteúdo externo para que seja restrito.
Configurar o compartilhamento de conteúdo do OneDrive para que seja restrito.
Configurar para que os usuários convidados do SharePoint não possam compartilhar itens que não sejam de sua propriedade.
Configure para que o compartilhamento externo do SharePoint seja gerenciado por meio de lista de permissões/listas negras de domínio.
Configure para que o compartilhamento de links seja restrito no SharePoint e no OneDrive.
Configure para que o compartilhamento externo seja restrito pelo grupo de segurança.
Configure para que o acesso de convidado a um site ou OneDrive expire automaticamente.
Certifique-se de que a reautenticação com código de verificação seja restrita.
Configure para que os arquivos infectados do Office 365 SharePoint não sejam permitidos para download.
Configure para que a sincronização do OneDrive esteja restrita a dispositivos não gerenciados.
Configure para que a execução de scripts personalizados seja restrita em sites pessoais.
Configure para que a execução de scripts personalizados seja restrita em conjuntos de sites.
Configure para que o compartilhamento externo de arquivos no Teams esteja habilitado apenas para serviços de armazenamento em nuvem aprovados.
Configure para que os usuários não possam enviar e-mails para um endereço de e-mail de canal.
Configure para que o 'acesso externo' seja restrito no centro de administração do Teams.
Configure as políticas de permissão de aplicativos.
Configure pera que usuários anônimos não possam participar de uma reunião.
Configure para que usuários anônimos e chamadores não possam iniciar uma reunião.
Configurar que apenas as pessoas da minha organização possam ignorar o lobby.
Configure para que os usuários que discam não possam ignorar o lobby.
Configurar para que o bate-papo da reunião não permita usuários anônimos.
Configurar para que o acesso do usuário convidado seja restrito.
Configurar para que os convites de usuários externos sejam restritos.
Configure para que o acesso de convidados ao conteúdo seja restrito.
Configurar para que 'Publicar na web' esteja restrito.
Configurar para que 'Permitir que os usuários apliquem rótulos de confidencialidade ao conteúdo' esteja 'Ativado.
Configurar para que os links compartilháveis sejam restritos.
Configurar para que a ativação do compartilhamento externo de dados seja restrita.

Configurar para 'Bloquear autenticação ResourceKey'.	

3.3. **ITEM 24 - SERVIÇO DE IMPLEMENTAÇÃO DE HARDENING MICROSOFT 365 E5**

3.3.1. A contratada deverá executar as atividades abaixo conforme o CIS BENCHMARK mais recente disponível para download em www.cisecurity.org . Essas atividades de melhores práticas de segurança têm por finalidade diminuir a superfície de ataque no ambiente.

3.3.2. As atividades estão separadas por tipos de licenças:

Microsoft 365 E5 – Implementação Hardening	
Configurar o recurso de lockbox do cliente.	1
Ativar links seguros para aplicativos do Office.	
Habilitar política de anexos seguros.	
Habilitar os anexos seguros para SharePoint, OneDrive e Microsoft Teams.	
Criar uma política anti-phishing.	
Configurar e habilitar a proteção da conta prioritária.	
Configura e habilitar o Microsoft Defender para aplicativos em nuvem.	

3.4. **ITEM 25 - SERVIÇO DE MIGRAÇÃO DAS CONTAS AD E EMAIL PARA NUVEM**

3.4.1. O serviço consiste em atribuir as licenças adquiridas de AzureAD, Office365 e Microsoft 365 e Exchange Kioski aos usuários e caixa de correios indicados pelo contratante, e migração para a nuvem e ativação dos serviços AzureAD Premium P2. No final teremos um ambiente de gerenciamento de usuários local e na nuvem totalmente integrado com os serviços AzureAD Premium P2 e caixas de correios migradas;

3.5. **AMBIENTE DO MPDFT**

3.5.1. Descrição do ambiente atual: o ambiente atual do MPDFT é formado por 3 controladores de domínio locais com sistema operacional Windows Server 2019, com nível funcional de domínio e floresta Windows Server 2016. O serviço de email local é formado por 2 servidores Exchange Enterprise 2016 configurado com Grupo de disponibilidade de banco de dados. O nosso Active Directory está integrado com a AzureAD e nosso Exchange está integrado com o Exchange Online em modo híbrido;

3.6. **EXECUÇÃO DO SERVIÇO**

3.6.1. A execução será acompanhada por pontos de controle acordados previamente;

3.6.2. A solução deve seguir a recomendação do fabricante, implementando técnicas de segurança atuais;

3.6.3. A execução deve levar em conta a continuidade do negócio, evitando interrupções durante horário comercial;

3.6.4. Na conclusão do serviço deve ser entregue documentação técnica e apresentação do novo ambiente, detalhando os serviços que foram criados para a integração e noções de configuração e verificação de funcionamento;

3.7. **DOCUMENTAÇÃO TÉCNICA**

3.7.1. Deverá ser entregue pela CONTRATADA a "Documentação Técnica" (DT) de toda a solução implementada no ambiente da CONTRATANTE, composta de:

3.7.2. Plano de Projeto, contendo o passo a passo para execução de todos os serviços contidos nesse Termo de Referência.

3.7.3. Plano de Implantação, contendo as configurações específicas, arquiteturas e suas topologias e diagramas lógicos da solução;

3.7.4. Plano de Testes;

3.7.5. Plano de ações de rollback;

3.7.6. Essa documentação fica sujeita à análise e à aprovação da equipe técnica da CONTRATANTE;

3.7.7. Toda a DT deverá ser entregue em mídia digital, devendo as topologias da solução serem entregues em formato a ser definido pela CONTRATANTE;

3.7.8. Toda a DT fornecida pela CONTRATADA referente às ferramentas e solução implantadas no ambiente da CONTRATANTE é de propriedade da CONTRATANTE.

3.7.9. Toda a DT fornecida pela CONTRATADA deverá estar em português do Brasil.

3.8. **NÍVEIS MÍNIMOS DE SERVIÇOS EXIGIDOS (NMSE)**

3.8.1. Os chamados técnicos serão categorizados nas severidades descritas abaixo, devendo ser atendidos nos prazos especificados (tabelas I e II):

TABELA I - Severidade dos chamados técnicos	
Severidade	**Descrição**
ALTA	Serviços totalmente indisponíveis ou comprometimento de performance ou funcionalidade da solução.
MÉDIA	Quando há um alerta na solução, mas a mesma ainda se encontra operacional.
BAIXA	Solicitação de configuração, manutenções preventivas, esclarecimentos técnicos relativos ao uso e aprimoramento do serviço. Não haverá abertura de chamado com esta severidade em sábados, domingos e feriados.

TABELA II - Prazos para a solução do chamado

Severidades	ALTA	MÉDIA	BAIXA
Prazo para término do atendimento	4 (quatro) horas	24 (vinte e quatro) horas	3 (três) dias úteis

3.8.2. Para efeitos dos níveis de serviço exigidos, serão considerados os seguintes critérios:

3.8.2.1. Término do atendimento: o tempo decorrido entre a abertura do chamado pela CONTRATANTE e a solução definitiva da demanda pela CONTRATADA.

3.8.2.2. O atendimento da demanda só será considerado concluído após o aceite formal da equipe técnica da CONTRATANTE. Caso a CONTRATANTE não confirme a conclusão do atendimento, este permanecerá em aberto. Nesse caso, a CONTRATANTE fornecerá informações sobre as pendências a serem resolvidas.

3.8.2.3. A severidade do chamado será informada pela CONTRATANTE no momento da sua abertura e seguirá o que está disposto na Tabela I.

3.8.2.4. A severidade poderá ser reclassificada pela CONTRATANTE. Caso isso ocorra, haverá uma nova contagem de prazo, conforme a nova severidade, e os prazos seguirão o que está disposto na Tabela II.

3.8.2.5. À CONTRATADA é vedado interromper o atendimento de severidade ALTA até que a solução esteja plenamente funcional, mesmo que isso envolva períodos noturnos, sábados, domingos e feriados. Não haverá custos adicionais à CONTRATANTE nessas situações.

4. REUNIÃO DE ALINHAMENTO DE EXPECTATIVAS

4.1. Deverá ser realizada uma reunião de alinhamento com o objetivo de identificar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus Anexos, e esclarecer possíveis dúvidas acerca da infraestrutura de TI da CONTRATANTE;

4.2. Deverão participar dessa reunião, no mínimo, o Gestor do Contrato, o Fiscal Técnico do Contrato, o Preposto e membro da equipe técnica da CONTRATADA;

4.3. A reunião realizar-se-á na sede da CONTRATANTE em prazo especificado neste documento;

4.4. Na reunião de Alinhamento de Expectativas a CONTRATADA deverá apresentar:

4.4.1. Sugestão de conjunto de configuração e topologia para implantação da solução contratada;

4.4.2. As sugestões deverão ser apresentadas para discussão durante a reunião e as configurações definitivas devem ser apresentadas no Plano de Implantação e Plano de Projeto.

5. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

5.1. A CONTRATADA obriga-se por si, seus empregados, sócios, diretores e mandatários, manter total sigilo e confidencialidade dos serviços prestados ao CONTRATANTE no que se refere à não divulgação, por qualquer forma, de toda ou parte das informações ou documentos a ele relativos, e aos quais venha a ter acesso, em decorrência da prestação dos serviços executados por força deste contrato. Também se compromete a respeitar as imposições relativas ao sigilo bancário as quais o CONTRATANTE está sujeito.

5.2. A CONTRATADA poderá revelar as informações decorrentes deste contrato, exclusivamente, a seus prepostos e funcionários diretamente envolvidos nas atividades que fazem uso ou tenham acesso permanente ou eventual às mesmas.

5.3. A CONTRATADA se obriga, ainda, a respeitar integralmente as normas de segurança estabelecidas pelo CONTRATANTE e atender os padrões de segurança e controle para acesso e uso das instalações e equipamentos do CONTRATANTE, zelando por sua integridade, mantendo sigilo e considerando confidenciais todos os dados e informações pertinentes aos serviços prestados.

5.4. Não serão considerados confidenciais quaisquer documentos, dados ou informações do presente contrato, informações de domínio público, que a CONTRATADA venha ter conhecimento lícito através de terceiros e aqueles que o CONTRATANTE vier a tornar públicos.

5.5. A obrigação das partes de não divulgação das informações tidas como sigilosas e confidenciais sobreviverá à rescisão do contrato, até que ocorra a liberação pela parte proprietária das informações, por determinação judicial ou pela ocorrência dos eventos indicados neste contrato com liberadores dessa obrigação.

5.6. O CONTRATANTE analisará a liberação dos acessos às dependências, equipamentos, softwares e sistemas que forem necessários ao cumprimento do objeto nos termos desta especificação.

5.7. Para tanto, a CONTRATADA deverá disponibilizar previamente as informações necessárias para acesso aos ambientes e atender às normas e políticas de segurança utilizadas pelo CONTRATANTE.

5.8. A CONTRATADA deverá assegurar que seus empregados estejam cientes e que devem obedecer às políticas de segurança de informações do CONTRATANTE e de garantir adequação às políticas estabelecidas.

5.9. A CONTRATADA irá gerenciar a segurança das informações e dados com os esforços necessários para restringir o acesso não autorizado. A CONTRATADA fará os esforços necessários para garantir que seus empregados e representantes estejam inteiramente cientes dos riscos associados com problemas e riscos inerentes à segurança da informação.

Documento assinado eletronicamente por **PAULO LUIZ ALMEIDA DOS REIS**, **Chefe de Seção**, em 16/02/2024, às 18:25, conforme § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site https://sei.mpdft.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0885788** e o código CRC **6132F97E**.