

Número do Documento de Formalização da Demanda: 95/2023

1. Informações Básicas

Área requisitante	Data da conclusão da contratação	UASG	Editado por
CGTI/SPTI/SEXEC/MCOM	31/12/2023 00:00	410003	MARCELO DA SILVA COSTA
Descrição sucinta do objeto			
Gerenciamento de Acesso Lógico Privilegiado			

2. Justificativa de necessidade

Controlar, monitorar e auditar o acesso a sistemas, dados e recursos privilegiados dentro de uma organização. Reduzir os riscos associados a esses privilégios, garantindo que apenas as pessoas autorizadas tenham acesso a eles e que suas atividades sejam monitoradas e registradas adequadamente.

3. Materiais/Serviços

3.1 Materiais

Nenhum material incluído.

3.2 Serviços

Nº do item	Grupo	Descrição	Qtd	Val. unit. (R\$)	Val. total (R\$)
1	SERVICOS PARA A INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃOE COMUNICAÇÃO (TIC), NAO CLASSIFICADOS EM OUTROS TÓPICOS	OUTROS SERVIÇOS PARA A INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (TIC)	1,00	1.400.000,00	1.400.000,00

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

MARCELO DA SILVA COSTA

Agente de contratação

5. Acompanhamento

Id Acompanhamento	Responsável	Data
1 A área demandante justificou inclusão extemporânea tendo em vista a recente reestruturação organizacional do Ministério das Comunicações, bem como as mudanças ocorridas no âmbito da SPTI, o que impactou na priorização de determinados projetos de TIC.	MARCELO DA SILVA COSTA	21/07 /2023 12:08

6. Relacionamentos

Nenhum relacionamento encontrado.



MINISTÉRIO DAS COMUNICAÇÕES

ANEXO I - INFORMAÇÕES COMPLEMENTARES AO DOCUMENTO DE FORMALIZAÇÃO DA DEMANDA Nº 95/2023 (11068424)

Anexo complementar ao Documento de Formalização da Demanda - DFD (11068424) cadastrados previamente no Sistema de Planejamento e Gerenciamento de Contratações (PGC), visando atender ao conteúdo mínimo exigido no parágrafo 1º do art. 10 da IN SGD/ME nº 94/2022.

1- INFORMAÇÕES GERAIS

1.1- Data prevista para conclusão do processo

A data estimada para a conclusão desta contratação é 31/12/2023.

1.2- Descrição sucinta do objeto

Solução de Gerenciamento de Acesso Lógico Privilegiado.

1.3- Grau de prioridade da compra ou da contratação

Baixa prioridade.

2- JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO

2.1- Justificativa da necessidade da contratação

Controlar, monitorar e auditar o acesso a sistemas, dados e recursos privilegiados dentro de uma organização. Reduzir os riscos associados a esses privilégios, garantindo que apenas as pessoas autorizadas tenham acesso a eles e que suas atividades sejam monitoradas e registradas adequadamente.

O MCOM lida diariamente com uma grande diversidade de informações, das quais muitas são protegidas por lei. A presente proposta de contratação tem por objetivo atender demandas relacionadas à proteção dessas informações, somada a outros esforços, utilizando como referência os padrões ABNT NBR ISO/IEC 27002:2005 - Código de Prática para a Gestão da Segurança da Informação e ABNT NBR ISO/IEC 27001:2006 – Sistema de Gestão de Segurança da Informação.

O Ministério das Comunicações é um órgão da administração federal direta que foi criado em junho de 2020, a partir do desmembramento do Ministério da Ciência, Tecnologia e Inovações. A pasta foi criada com o objetivo de fortalecer as áreas de política nacional de telecomunicações, política nacional de radiodifusão; e, serviços postais, telecomunicações e radiodifusão.

Além disso, é de competência do Ministério atuar na política de comunicação e divulgação do Governo Federal; no relacionamento do Governo Federal com a imprensa regional, nacional e internacional; convocação de redes obrigatórias de rádio e televisão; bem como na pesquisa de opinião pública; e no sistema brasileiro de televisão pública.

Nesse contexto, de acordo com sua importância estratégica, para prover todos os serviços prestados por meio de suas políticas e recursos de TIC para a sociedade.

Para isso foram realizados vários investimentos na concepção e adoção de vários sistemas e aplicações internas estruturantes, sistemas de troca e armazenamento de informações (storages) como e-mail, aplicações em nuvem, documentos gerados por suíte de aplicativos de escritório (documentos, planilhas, apresentações e outros), além de vários bancos de dados lógicos que mantêm informações sigilosas e extremamente importantes para o MCOM. Os acessos remotos e a quantidade dessas informações crescem a cada dia de maneira exponencial, e como consequência, torna-se imprescindível aumentar o nível de segurança dos acessos remotos privilegiados e da proteção de todo este arcabouço, em especial com o advento da LGPD – Lei Geral de Proteção de Dados, que passou a estabelecer regras para uso, proteção e transparência de qualquer informação considerada pessoal de qualquer cidadão, o que requer um maior investimento no controle de acessos e proteção de todas as informações pessoais que o MCOM mantém sob sua guarda.

Esta solução visa possibilitar também o controle, o gerenciamento e a execução de trilhas de auditoria dos acessos remotos privilegiados a equipamentos e em manutenções remotas nos computadores dos servidores do Ministério, incluindo smartphones.

A implantação da solução ainda traz como benefício: permitir a adequação contínua das capacidades de controle e monitoramento necessárias aos serviços alocados, aumentando o gerenciamento, eficiência e proteção das informações. Desta forma, simplifica tarefas complexas e permite uma fácil adaptação dos analistas e administradores da TI a alterações de emergência e imprevistas.

Motivação

De acordo com o último levantamento realizado o MCOM possui hoje um total de 1.640 dispositivos, sendo 1.140 estações de trabalho (desktop e notebook), 246 servidores físicos e virtuais e 26 aplicações web, onde o atendimento a todo esse parque é realizado por telefone ou presencialmente, e quando realizado de maneira remota, acabam muitas vezes acontecendo sem uma conexão segura ou criptografada, sem a geração de uma trilha de auditoria para averiguação futura das ações dos técnicos internos e/ou terceirizados externos, dentro do ambiente computacional do MCOM, pois não há um mecanismo lógico que gerencie de forma efetiva e segura todos os acessos remotos, onde por meio da aquisição pretendida, além de otimizar a utilização dos recursos humanos disponíveis, pois não haverá a necessidade de locomoção até o espaço físico destino e cada atendente poderá atender vários chamados ao mesmo tempo utilizando a nova opção tecnológica, além de implementar uma comunicação mais eficiente e segura entre os técnicos e os usuários finais, elevando o nível de disponibilidade, integridade e confiabilidade das informações custodiadas pelo MCOM, criando regras de segurança e rastreabilidade das conexões de acesso remoto.

Necessidade de proteção para os servidores em teletrabalho

As soluções de gerenciamento de acesso lógico privilegiado geralmente precisam oferecer suporte a vários objetivos de segurança. Isso pode ser realizado por meio de uma combinação de recursos de segurança incorporados às soluções de acesso remoto e controles de segurança adicionais aplicados aos dispositivos de teletrabalho e outros componentes da solução de acesso remoto. Os objetivos de segurança mais comuns para as tecnologias de teletrabalho e acesso remoto são os seguintes:

- a) **Confidencialidade** – garanta que as comunicações de acesso remoto e os dados armazenados do usuário não possam ser lidos por terceiros não autorizados;
- b) **Integridade** – detecte quaisquer alterações intencionais ou não intencionais nas comunicações de acesso remoto que ocorrem em trânsito; e
- c) **Disponibilidade** – garanta que os usuários possam acessar recursos por acesso remoto sempre que necessário.

Portanto, o objeto desta contratação pretendida constitui tecnologia de gerenciamento de acesso lógico privilegiado amplamente necessária para o MCOM. Onde a falta de sua adoção, impactará fortemente no controle e auditoria do uso de credenciais privilegiadas por meio dos acessos remotos realizados e na proteção das informações e no aumento da segurança e agilidade nos serviços prestados ao cidadão por meio de suas políticas públicas. Por outro lado, sua adoção elevará a disponibilidade dos técnicos promovendo um melhor atendimento a todos os usuários independente dos locais físicos em que se encontrem, ademais, todos os acessos lógicos remotos passarão a ser auditados, possibilitando que todas as ações realizadas possam ser consultadas até mesmo pelo

FUNÇÃO	TITULAR	SUBSTITUTO
INTEGRANTE REQUISITANTE	Nome: VICTOR HENRIQUE HISAO TAIRA IAPE: 2270979 Lotação: COINS/CGTI/SPTI/SEXEC	Nome: ILLO ALBERTO QUEIROZ WEBER IAPE: 2730994 Lotação: DIATU/COINS/CGTI/SPTI/SEXEC
INTEGRANTE TÉCNICO	Nome: MICHEL GULARTE RECONDO	Nome: LEANDRO BOLZAN BÉRIA

Ressalta-se que, nos termos do parágrafo 2º do artigo 10 da Instrução Normativa SGD/ME nº 94/2022, os servidores elencados na tabela acima, subscrevem o presente e declaram expressamente ter ciência de sua indicação para compor a equipe de planejamento da contratação, bem como das atribuições a serem exercidas na qualidade de membro da equipe.

ASSINATURA - CIÊNCIA DOS INTEGRANTES DA EQUIPE DE PLANEJAMENTO

(assinado eletronicamente)
VICTOR HENRIQUE HISAO TAIRA
Integrante Requisitante

(assinado eletronicamente)
ILLO ALBERTO QUEIROZ WEBER
Integrante Requisitante Substituto

(assinado eletronicamente)
MICHEL GULARTE RECONDO
Integrante Técnico

(assinado eletronicamente)
LEANDRO BOLZAN BÉRIA
Integrante Técnico Substituto

ASSINATURA - CIÊNCIA DO RESPONSÁVEL DA ÁREA TÉCNICA

(assinado eletronicamente)
FELIPE LINHARES LUSTOSA DA COSTA
Coordenador-Geral de Gestão da Informação, substituto

ASSINATURA - RESPONSÁVEL DA ÁREA REQUISITANTE

(assinado eletronicamente)
HELDER MOTA GOMES
Coordenador Geral de Tecnologia da Informação e Comunicação



Documento assinado eletronicamente por **Helder Mota Gomes**, **Coordenador-Geral de Tecnologia da Informação e Comunicação**, em 24/08/2023, às 18:00 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Felipe Linhares Lustosa da Costa**, **Coordenador-Geral de Gestão da Informação substituto**, em 25/08/2023, às 13:22 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Michel Gualarte Recondo**, **Coordenador de Segurança da Informação**, em 25/08/2023, às 14:56 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Leandro Bolzan Béria**, **Assessor Técnico Especializado**, em 25/08/2023, às 15:14 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Illo Alberto Queiroz Weber**, **Chefe da Divisão de Atendimento aos Usuários**, em 25/08/2023, às 16:37 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Victor Henrique Hisao Taira**, **Coordenador de Infraestrutura e Serviços de Tecnologia da Informação**, em 28/08/2023, às 10:06 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site <https://sei.mcom.gov.br/sei/verifica>, informando o código verificador **11068424** e o código CRC **6E51AC63**.