Adendo I ao ANEXO I - TERMO DE REFERÊNCIA

PREGÃO ELETRÔNICO Nº 16/2020

NUP 64222.006485/2020-75

Apêndices:
Apêndice A - Relação de Entregas, Requisitos, Testes e Critérios de Aceitação

DESCRITIVO DA SOLUÇÃO TÉCNICA

1. DESCRIÇÃO GERAL DA SOLUÇÃO

1.1. O serviço de evolução e atualização do software EBMail, será dividido em 5 (cinco) conjuntos de funcionalidades (subsistemas). Para cada conjunto de funcionalidades, serão definidos um conjunto de entregas, um conjunto de requisitos por entrega e um ou mais testes de aceitação por requisito.

Tabela 1 - Relação de Entregas por Subsistema

Subsistemas	Entregas
S1 - envio e recebimento de mensagens (EBMail)	E1 - Compilar o Software EBMail para o Sistema Operacional homologado para z/VM E2 - Escrever e Enviar Mensagem Digital Assinada para Certificados A1 e A3 E3 - Escrever e Enviar Mensagem Digital Criptografada para Certificados Tipo A1 e A3 E4 - Atualização da Interface gráfica do Zimbra E5 - Scanner de Vírus em anexos das mensagens
S2 - gerenciamento e administração de contas (EBMail Admin)	E6 - Atualização da interface de administrador E7 - Remover o acesso de todas as caixas postais para os usuários administradores, com exceção do administrador do sistema (master)
S3 - migração/backup de contas	E8 - Solução de Backup Automático das caixas postais do EBMail
S4 - criação e gestão de contas (Portal EBMail)	E9 - Criação de novas contas E10 - Recuperação de senha de conta E11 - Portal EBMail Admin
S5 - armazenamento de arquivos e administração do subsistema de armazenamento (EBDrive)	E12 - Instalar o Software EBDrive para o Sistema Operacional homologado e hardware existente na infraestrutura do CITEx E13 - Dados e usuários E14 - Nível de segurança e restrição de acesso de compartilhamento de arquivos e pastas E15 - Criação, edição e compartilhamento de documentos no formato open document format: .odt, .ods e .odp E16 - Versionamento dos arquivos salvos no EBDrive E17 - Recuperação de arquivos deletados E18 - Scanner de Vírus em arquivos armazenados E19 - Disponibilizar a movimentação de arquivos entre pastas na interface web E20 - Redundância e Alta Disponibilidade E21 - Solução de Backup Automático do EBDrive E22 - Atualização da interface do EBDrive E23 - Acesso unificado EBMail - EBDrive

	E24 - Configuração de Performance do Agente de Sincronização E25 - Monitoramento dos agentes ativos na plataforma por meio de interface WEB

1.2. O Serviço de Suporte Técnico encontra-se descrito em item específico neste documento.

1.3. Para fins de identificação, neste documento, as Entregas, Requisitos e Testes de Aceitação serão referenciadas pelo seguinte código de letras e números:

1.3.1. **Ea.**: Entrega “a”, onde “a” é um número;

1.3.2. **Ra.b.**: Requisito “b”, da Entrega “a”, onde “a” e “b” são números.

1.3.3. **Ta.b.c.**: Teste “c”, do Requisito “b”, da Entrega “a”, onde “a”, “b” e “c” são números.

2. ENTREGAS DO SUBSISTEMA 1 - envio e recebimento de mensagens (EBMail)

2.1. E1 - Compilar o Software EBMail para o Sistema Operacional homologado para z/VM

2.1.1. Compilação do software zimbra em sua versão mais recente disponível no repositório oficial da Zimbra no endereço eletrônico https://github.com/Zimbra/zm-build.

Tabela 2 - Requisitos, Testes e Critérios de Aceitação de E1

Requisitos	Testes de Aceitação	Critérios de Aceitação
R1.1. Deverá ser realizada pela CONTRATADA a adequação de todo o código fonte do Zimbra Colaboration Open Source Edition , versão 8.8.15, disponibilizado no site "www.zimbra.com", pela empresa SYNACOR, de forma a torná-lo compatível com a plataforma s390x.	T1.1.1. todas as funcionalidades presentes e disponibilizadas pela versão do Zimbra FOSS devem estar portadas e disponíveis na versão compilada para Alta Plataforma.	todas as funcionalidades referenciadas devem estar presentes
	T1.1.2. a compilação deverá ocorrer sem erros que inviabilizem a utilização de alguma funcionalidade presente na versão disponível para baixa plataforma	compilação sem erros
	T1.1.3. a equipe de testes do Exército fará uma análise estática do código fonte e da documentação entregue, não podendo apresentar falhas de segurança, erros de funcionalidade.	aprovado em relatório a ser confeccionado pelo CDS
R1.2. A CONTRATADA deverá fornecer para a CONTRATANTE sistema operacional homologado para uso na plataforma s390x, devendo ser utilizado na versão do z/VM 7.1 e superior, com licença válida por 36 meses.	T1.2.1. compilação do código fonte customizado no ambiente de homologação do 7º CTA, utilizando o sistema operacional fornecido pela contratada.	entrega da licença do sistema operacional com a respectiva instalação na versão do z/VM em uso no CITEx

2.2. E2 - Escrever e enviar mensagem digital assinada para Certificados A1 e A3

2.2.1. Consiste na funcionalidade de enviar mensagens digitalmente assinadas, por um usuário que dispõe de Certificados dos tipos A1 e A3.

2.2.2. Essa funcionalidade deve ser interoperável com a funcionalidade já existente de envio de mensagens de e-mail assinadas digitalmente com certificados dos tipos A1 e A3.

Tabela 3 - Requisitos, Testes e Critérios de Aceitação de E2

Requisitos	Testes de Aceitação	Critérios de Aceitação
R2.1. O sistema deve apresentar ao usuário, em sua interface, a opção de enviar uma mensagem de e-mail assinada digitalmente utilizando certificados do tipo A1 e A3, da ICP-Brasil.	T2.1.1. a equipe de testes do Exército realizará envios de mensagens utilizando Certificados A1 e A3 para verificar a funcionalidade de assinatura digital	Sem erros no envio das mensagens
	T2.1.2. a equipe de testes do Exército fará uma análise estática do código fonte e da documentação entregue, não podendo apresentar falhas de segurança, erros de funcionalidade e não conformidade com a Normatização de Certificado de Assinatura Digital da AC-DEFESA	aprovado em relatório a ser confeccionado pelo CDS
R2.2. O sistema deve ser compatível com qualquer certificado dos tipos A1 e A3 válido nas infraestruturas de chave pública (cartão inteligente, token criptográfico ou armazenado em nuvem) fornecidos pela AC-Defesa.	T2.2.1. a equipe de testes do Exército realizará envios de mensagens utilizando Certificados A1 e A3 para verificar a funcionalidade de assinatura digital	Sem erros no envio das mensagens
	T2.2.2. a equipe de testes do Exército fará uma análise estática do código fonte e da documentação entregue, não podendo apresentar falhas de segurança, erros de funcionalidade e não conformidade com a Normatização de Certificado de Assinatura Digital da AC-DEFESA	aprovado em relatório a ser confeccionado pelo CDS
R2.3. A funcionalidade de assinatura digital não deve aceitar a utilização de certificados auto-assinados	T2.3.1. o sistema deverá rejeitar o certificado auto-assinado gerado pela equipe de testes do Exército	rejeição do certificado auto-assinado
R2.4. A funcionalidade de assinatura digital não deve aceitar certificados revogados ou expirados	T2.4.1. o sistema deverá rejeitar os certificados revogados ou expirados, utilizados pela equipe de testes do Exército	rejeição dos certificados revogados ou expirados durante a tentativa de envio de mensagem
R2.5. A funcionalidade de assinatura digital deverá alertar ao usuário quando seu certificado estiver prestes a expirar (30 dias) ou quando estiver expirado, durante a tentativa de submissão do certificado. Ao usuário, deverá ser disponibilizada a opção de poder "ignorar" o aviso e, após esta decisão, o sistema deverá parar de exibir o aviso.	T2.5.1. a equipe de testes do Exército fará login em uma conta cujo certificado está prestes a expirar (< 30 dias) e verificará se o aviso correspondente é exibido.	o aviso deverá aparecer para o usuário com a opção "ignorar o aviso"
	T2.5.2. a equipe de testes do Exército fará login em uma conta cujo certificado está prestes a expirar (< 30 dias) e verificará se a decisão para "ignorar" é facultada ao usuário.	o aviso deverá aparecer para o usuário com a opção "ignorar o aviso"
	T2.5.3. a equipe de testes do Exército fará login em uma conta cujo certificado está expirado e verificará se o aviso correspondente é exibido.	o aviso deverá aparecer durante o teste com a opção "ignorar o aviso"
	T2.5.4. a equipe de testes do Exército fará login em uma conta cujo certificado está expirado e verificará	o aviso deverá aparecer durante o teste com a opção "ignorar o aviso"

	se a decisão para "ignorar" é facultada ao usuário.	
R2.6. O sistema deve possuir um componente para exibir as informações das chaves públicas armazenadas no servidor de chaves para o usuário	T2.6.1. a equipe de testes do Exército acessará o componente para verificar o correto armazenamento das chaves privadas para 5 usuários	o sistema deverá apresentar as chaves armazenadas para os usuários testados
R2.7. O sistema deve permitir ao usuário o cadastro da sua chave pública no servidor de chaves	T2.7.1. a equipe de testes do Exército fará o cadastro de 5 militares no servidor de chaves e, estes certificados deverão estar disponíveis nos processos de validação de assinatura.	os certificados de todos os usuários testados devem aparecer disponíveis no processo de validação de assinatura
R2.8 . O sistema de assinatura digital deve permitir a validação da assinatura e leitura de mensagens assinadas e já existentes, após a expiração do certificado digital do remetente	T2.8.1. a equipe de testes do Exército fará a validação da leitura de mensagens digitalmente assinadas após a expiração do certificado digital do remetente.	deve ser possível ler essas mensagens
R2.9. O sistema deve validar a identidade do usuário e do certificado de acordo com a "Política de Certificado de Assinatura Digital Tipos A1 e A3 da Autoridade Certificadora de Defesa (AC Defesa)" disponível na página oficial da AC Defesa.	T2.9.1. teste realizado pela AC DEFESA para a verificação do produto entregue.	ser aprovado no parecer da AC DEFESA

2.3. E3 - Escrever e enviar mensagem digital criptografada para Certificados A1 e A3

2.3.1. Consiste na funcionalidade de enviar mensagens digitais criptografadas, por um usuário que dispõe de Certificados dos tipos A1 e A3.

2.3.2. Essa funcionalidade deve ser interoperável com a funcionalidade já existente de envio de mensagens de e-mail criptografadas digitalmente com certificados dos tipo A1 e A3.

Tabela 4 - Requisitos, Testes e Critérios de Aceitação de E3

Requisitos	Testes de Aceitação	Critérios de Aceitação
R3.1. O sistema deve apresentar ao usuário, em sua interface, a opção de enviar uma mensagem de e-mail criptografada digitalmente utilizando certificados dos tipos A1 e A3.	T3.1.1. a equipe de testes do Exército realizará envios de mensagens utilizando Certificados A1 e A3 para verificar a funcionalidade de assinatura digital	Sem erros no envio das mensagens
	T3.1.2. a equipe de testes do Exército fará uma análise estática do código fonte e da documentação entregue, não podendo apresentar falhas de segurança, erros de funcionalidade e não conformidade com a Normatização de Certificado de Assinatura Digital da AC-DEFESA	aprovado em relatório a ser confeccionado pelo CDS
R3.2. As mensagens criptografadas deverão ser armazenadas criptografadas e não em texto claro.	T3.2.1. a equipe de testes do Exército fará uma análise estática do código fonte e da documentação entregue, não podendo apresentar falhas de segurança, erros de funcionalidade e não conformidade com a Normatização de Certificado de	aprovado em relatório a ser confeccionado pelo CDS

	Assinatura Digital da AC-DEFESA.	
R3.3. O certificado deve ser compatível com qualquer certificado dos tipos A1 e A3 válido nas infraestruturas de chave pública (cartão inteligente, token criptográfico ou armazenado em nuvem) fornecidos pela AC-Defesa.	T3.3.1. a equipe de testes do Exército realizará envios de mensagens utilizando Certificados A1 e A3 para verificar a funcionalidade de assinatura digital	Sem erros no envio das mensagens
	T3.3.2. a equipe de testes do Exército fará uma análise estática do código fonte e da documentação entregue, não podendo apresentar falhas de segurança, erros de funcionalidade e não conformidade com a Normatização de Certificado de Assinatura Digital da AC-DEFESA	aprovado em relatório a ser confeccionado pelo CDS
R3.4. A funcionalidade de assinatura digital não aceitará a utilização de certificados auto-assinados	T3.4.1. o sistema deverá rejeitar o certificado auto-assinado gerado pela equipe de testes do Exército	rejeição do certificado auto-assinado
R3.5. A funcionalidade de assinatura digital não aceitará certificados revogados ou expirados	T3.5.1. o sistema deverá rejeitar o certificados revogados ou expirados, utilizados pela equipe de testes do Exército	rejeição dos certificados revogados ou expirados durante a tentativa de envio de mensagem
R3.6 . A funcionalidade de assinatura digital deverá alertar ao usuário quando seu certificado está prestes a expirar (30 dias) ou quando estiver expirado, durante a tentativa de submissão do certificado. Ao usuário, deverá ser disponibilizada a decisão de poder "ignorar" o aviso e, após esta decisão, o sistema deverá parar de exibir o aviso.	T3.6.1. a equipe de testes do Exército fará login em uma conta cujo certificado está prestes a expirar (< 30 dias) e verificará se o aviso correspondente é exibido.	o aviso deverá aparecer para o usuário com a opção "ignorar o aviso"
	T3.6.2. a equipe de testes do Exército fará login em uma conta cujo certificado está prestes a expirar (< 30 dias) e verificará se a decisão para "ignorar" é facultada ao usuário.	o aviso deverá aparecer para o usuário com a opção "ignorar o aviso"
	T3.6.3. a equipe de testes do Exército fará login em uma conta cujo certificado está expirado e verificará se o aviso correspondente é exibido.	o aviso deverá aparecer para o usuário com a opção "ignorar o aviso"
	T3.6.4. a equipe de testes do Exército fará login em uma conta cujo certificado está expirado e verificará se a decisão para "ignorar" é facultada ao usuário.	o aviso deverá aparecer para o usuário com a opção "ignorar o aviso"
R3.7. O sistema deve possuir um componente para exibir as informações das chaves públicas armazenadas no servidor de chaves para o usuário	T3.7.1. a equipe de testes do Exército acessará o componente para verificar o correto armazenamento das chaves privadas	o sistema deverá apresentar as chaves armazenadas para os usuários testados
R3.8. O sistema deve permitir ao usuário o cadastro da sua chave pública no servidor de chaves	T3.8.1. a equipe de testes do Exército fará o cadastro de 5 militares no servidor de chaves e, estes certificados deverão estar disponíveis nos processos de validação de assinatura.	os certificados de todos os usuários testados devem aparecer disponíveis no processo de validação de assinatura
R3.9. o sistema de assinatura digital deve permitir a validação da assinatura e leitura de mensagens assinadas e já existentes, após a expiração do certificado digital do remetente	T.3.9.1. a equipe de testes do Exército fará a validação da leitura de mensagens digitalmente assinadas após a expiração do certificado digital do remetente.	deve ser possível ler essas mensagens

R3.10. O sistema deve validar a identidade do usuário e do certificado de acordo com a "Política de Certificado de Assinatura Digital Tipos A1 e A3 da Autoridade Certificadora de Defesa (AC Defesa)" disponível na página oficial da AC Defesa.	T.3.10.1. ser aprovado no parecer da AC DEFESA para a verificação do produto entregue, sem ressalvas, à utilização do mesmo.	ser aprovado no parecer da AD DEFESA

2.4. E4 - Atualização da Interface gráfica do Zimbra

2.4.1. Aplicação das modificações de interface da identidade visual do Zimbra, de modo compatível com a atual versão do EBMail.

Tabela 5 - Requisitos, Testes e Critérios de Aceitação de E4

Requisitos	Testes de Aceitação	Critérios de Aceitação
R4.1. adequar a exibição do nome de guerra do militar e da sua OM na interface do sistema	T4.1.1. verificação da exibição do nome de guerra e da OM de forma correta na tela de login, na lista de contatos, na identificação da conta no canto superior direito e na lista exibida durante a digitação do e-mail no campo "Para" e no campo "Cc"	exibição correta do nome de guerra e OM em todos os locais especificados

2.5. E5 - Scanner de Vírus em anexos das mensagens

2.5.1. Consiste na verificação quanto à existência de códigos maliciosos nos arquivos que são anexados às mensagens de e-mail.

Tabela 6 - Requisitos, Testes e Critérios de Aceitação de E5

Requisitos	Testes de Aceitação	Critérios de Aceitação
R5.1. O sistema deverá está configurado com a extensão para detecção de arquivos maliciosos	T5.1.1. a equipe de testes do Exército anexará um arquivo malicioso e verificará se o sistema permitirá	o sistema não deve permitir que o arquivo malicioso seja anexado

3. ENTREGAS DO SUBSISTEMA 2 - gerenciamento e administração de contas (EBMail Admin)

3.1. E6 - Atualização da interface de administrador

3.1.1. O sistema deve refletir as regras de negócio das contas do Exército em sua interface mostrando os nomes dos campos (*labels*) de acordo com a informação contida no campo.

Tabela 7 - Requisitos, Testes e Critérios de Aceitação de E6

Requisitos	Testes de Aceitação	Critérios de Aceitação
R6.1. O sistema deve refletir as regras de negócio da atual interface do administrador do EBMail	T6.1.1. será verificado se todas as customizações aplicadas à interface do administrador, interface do usuário e	todas as customizações devem estar presentes na nova versão da interface do administrador

	regras de negócio, foram portadas para a nova interface entregue.	

3.2. E7 - Remover o acesso de todas as caixas postais para os usuários administradores, com exceção do administrador do sistema (master)

3.2.1. Consiste na remoção do acesso dos administradores às caixas postais dos usuários de forma que apenas o usuário *master*, além dos próprios usuários, possa acessar o conteúdo de caixas postais.

Tabela 8 - Requisitos, Testes e Critérios de Aceitação de E7

Requisitos	Testes de Aceitação	Critérios de Aceitação
R7.1. Por padrão, o sistema Zimbra permite o acesso às caixas postais dos usuários para qualquer usuário administrador. O sistema deve remover este acesso de forma que apenas o usuário *master* possa acessar o conteúdo de todas as caixas postais.	T7.1.1. será verificado se foi removido o acesso dos usuários administradores ao conteúdo das contas do usuário.	Apenas o usuário Master poderá acessar o conteúdo das contas de usuário.

4. ENTREGAS DO SUBSISTEMA 3 - migração/backup de contas

4.1. E8 - Solução de Backup Automático das caixas postais do EBMail

4.1.1. A solução de backup é um processo automático de geração de uma cópia de segurança para os dados de usuários, assim como rotinas de migração e recuperação de dados. Devem ser criadas cópias de segurança dos dados de forma que possam ser restaurados em caso de perda dos dados originais.

Tabela 9 - Requisitos, Testes e Critérios de Aceitação de E8

Requisitos	Testes de Aceitação	Critérios de Aceitação
R8.1. O solução deverá ser entregue com o sistema de backup full do EBMail, com uma rotina que apresentará o progresso do backup de maneira a informar a quantidade de caixas processadas e a quantidade de caixas que ainda serão processadas de forma interativa, informando possíveis problemas durante a execução do backup. e o agente dessa rotina de backup confirmará todos os itens que ainda estão marcados como pendentes (ou em progresso) para realizar o Backup ou atualizar o status para "Concluído".	T8.1.1. a partir das rotinas de backup e restore fornecidas pela empresa, serão realizados backups do tipo Full, incremental e contínuo. Posteriormente, será realizada uma nova instalação do sistema de e-mail, em um ambiente de testes, para a recuperação total do ambiente de produção por meio dos arquivos de backup (Full, incremental e contínuo)	disponibilizar interface visual com o progresso do backup, onde o operador poderá verificar o real progresso do backup realizar com sucesso a execução automática e segura da rotina progresso do backup de forma visual, onde o operador poderá acompanhar o real progresso do backup
R8.2. A solução deverá dispor de gerenciamento de rotinas de backup/restore das caixas postais e dos		a criação de arquivos de backup deverá conter as novas mensagens em relação a data de realização do último

dados de usuários com confiabilidade e segurança, sendo a execução feita de forma agendada ou sob demanda.		backup
R8.3. Os procedimentos de backup devem ser executados de maneira inteligente, prevendo as sistemáticas de Backup Full, Backup Incremental e Backup Contínuo, dependendo da política adotada pelo Exército.		por meio do sistema operacional será agendado a execução das diversas rotinas desenvolvidas pela CONTRATANTE de forma a produzir arquivos de Backup Full, Backup Incremental e Backup Contínuo. Após a criação desses arquivos os mesmos serão recuperados no ambiente de homologação e devem conter o mesmo conteúdo do ambiente de produção na data do backup realizado.
R8.4. a solução deverá possuir rotinas de *restore* granular, ou seja, deve ser possível recuperar caixas postais individuais	T8.4.1. a partir dos arquivos de backup, deverá ser realizado o *restore* de uma conta de um único usuário e de sua caixa postal no ambiente de testes.	por meio dos arquivos de backup criados pelas rotinas desenvolvidas pela CONTRATANTE será resturado um determinado usuário e sua respectiva caixa postal no ambiente de homologação

5. ENTREGAS DO SUBSISTEMA 4 - criação e gestão de contas (Portal EBMail)

5.1. E9 - Criação de novas contas

5.1.1. Consiste na criação de nova conta pelo próprio usuário, de maneira automatizada.

5.1.2. Para tal, o usuário já deve ser cadastrado na base da dados corporativa do Exército.

Tabela 10 - Requisitos, Testes e Critérios de Aceitação de E9

Requisitos	Testes de Aceitação	Critérios de Aceitação
R9.1. O sistema deve autenticar um novo usuário com suas credenciais do Sistema de Cadastramento de Pessoal do Exército (SiCaPEx) para criar sua conta no EBMail.	T9.1.1. será realizado o cadastramento de 10 contas de militares registrados no SiCaPEx	após o cadastramento, os 10 militares deverão ter contas válidas no EBMail
	T9.1.2. será realizada 10 tentativas de cadatro de contas inexistentes no SiCaPEx, que não possuem EBMail	as 10 tentativas não poderão gerar conta válida no EBMail
R9.2. A autenticação do novo usuário deve ser realizada utilizando o Autenticador Geral do DGP por meio do protocolo OAuth2.	T9.2.1. A utilização do protocolo OAuth2 deverá prover a comunicação entre os servidores da aplicação e de autenticação (Autenticador Geral do DGP) de forma controlável, utilizando mecanismos de controle de acesso.	comunicação entre a aplicação e o autenticador do DGP deverá ser realizada para criação de contas
R9.3. O sistema deve, após a autenticação, extrair dados pessoais da API do Autenticador Geral do DGP ou se conectar diretamente à uma visão da base de dados corporativa do Exército, EBCorp, para obter as informações necessárias. As informações a serem extraídas serão as	T9.3.1. O sistema deverá extrair a credencial e o verificador do Autenticador Geral do DGP ou da base de dados corporativa do Exército, e de posse destas informações, as mesmas serão utilizadas no Portal EBCloud	Portal EBCloud utilizará as credencais do DGP ou da base corporativa do Exército, conforme teste de aceitação

atualmente utilizadas no Portal EBCloud.		
R9.4. Após a autenticação com as credenciais do SiCaPEx o sistema deve apresentar ao usuário as opções de endereço de e-mail existentes baseadas no nome do militar. As regras de criação de endereço de e-mail serão definidas pela CONTRATANTE.	T9.4.1. o sistema apresentará opções de email para escolha do militar de acordo com as regras definidas pela CONTRATANTE	as opções devem aparecer no formato definido pela equipe de fiscalização do contrato
R9.5. O Sistema deve ser capaz de criar contas pessoais para os militares do Exército (contas corporativas) e contas para as organizações militares para atender as contas oficiais	T9.5.1. serão criadas contas pessoais para os militares do Exército e contas corporativas para as organizações militares	tanto as contas pessoais quanto as contas corporativas devem ser criadas com êxito

5.2. E10 - Recuperação de senha de conta

5.2.1. Consiste na redefinição da senha de *login* de contas de usuários, feita pelo próprio usuário.

Tabela 11 - Requisitos, Testes e Critérios de Aceitação de E10

Requisitos	Testes de Aceitação	Critérios de Aceitação
R10.1. O sistema deve possibilitar que o usuário autenticado possa redefinir sua senha do EBMail.	T10.1.1. a equipe de testes do Exército realizará a redefinição de senha de 10 usuários	a redefinição deve ser realizada com êxito

5.3. E11 - Portal EBMail Admin

5.3.1. Consiste na evolução e atualização do Portal EBMail Admin, que é uma interface entre o administrador do sistema e as ferramentas de gestão de contas de usuários.

5.3.2. Além disso, permite que o administrador tenha acesso a dados de desempenho do sistema, permitindo o diagnóstico precoce de futuros problemas que auxiliará a tomada de decisões estratégica sobre o serviço.

Tabela 12 - Requisitos, Testes e Critérios de Aceitação de E11

Requisitos	Testes de Aceitação	Critérios de Aceitação
R11.1. O sistema deverá conter uma interface de administração exibindo dados gerenciais do EBMail com, pelo menos, as seguintes informações: quantidade total de contas, quantidade de contas criadas mês a mês e quantidade de mensagens enviadas mês a mês.	T11.1.1. será feita a identificação visual dos relatórios mínimos exigidos, na inferface de administração do Portal EBMail.	as informações constantes no requisito devem estar presentes na interface
R11.2. O sistema deverá suspender automaticamente, após 30 dias, as contas dos militares temporários licenciados do serviço ativo e militares	T11.2.1. verificar a exclusão de militar conforme descrito no requisito	as contas dos militares descritos no requisitos devem estar suspensas

demissionários, deverá suspender as onta do EBMail e EBDrive, por meio da API do Autenticador Geral do DGP ou por consulta a uma visão da Base de dados Corporativa do Exército, EBCORP, para obter as informações necessárias.		
R11.3. O sistema deverá atualizar automaticamente, na base de dados LDAP do EBMail, a graduação e o posto dos militares por ocasião de atualização dos dados cadastrais, bem como o nome de exibição na interface Web, por meio de rotinas customizadas, executadas periodicamente.	T11.3.1. verificar a atualização do dado na base LDAP conforme alteração na base do DGP	o campo deverá ser alterado, conforme o previsto no teste de aceitação

6. ENTREGAS DO SUBSISTEMA 5 - Armazenamento de arquivos e Administração do Subsistema de Armazenamento (EBDrive)

6.1. E12 - Instalar o Software EBDrive para o Sistema Operacional homologado e hardware existente na infraestrutura do CITEx

6.1.1. Consiste na instalação de solução EBDrive contendo todos os requisitos conforme definido na Tabela 13, abaixo.

Tabela 13 - Requisitos, Testes e Critérios de Aceitação de E12

Requisitos	Testes de Aceitação	Critérios de Aceitação
R12.1 Deverá ser realizada pela CONTRATADA a modernização do atual EBDrive, contendo, além dos requisitos abaixo definidos, as funcionalidades de armazenamento e compartilhamento de arquivos existentes no software NextCloud (disponível no site nextcloud.com, versão 19).	T12.1.1. todas as funcionalidades indicadas, presentes e disponibilizadas pela versão do NextCloud devem estar portadas e disponíveis na versão instalada.	todas as funcionalidades referenciadas devem estar presentes
	T12.1.2. a instalação deverá ocorrer sem erros que inviabilizem a utilização de alguma funcionalidade descrita para este subsistema	compilação sem erros
	T12.1.3. a equipe de testes do Exército fará uma análise estática do código fonte e da documentação entregue, não podendo apresentar falhas de segurança ou erros de funcionalidade.	aprovado em relatório a ser confeccionado pelo CDS
R12.2. A CONTRATADA deverá fornecer para a CONTRATANTE sistema operacional homologado para uso na plataforma x86.	T12.2.1. instalação do sistema customizado no ambiente de homologação do 7º CTA, utilizando o sistema operacional fornecido pela contratada.	entrega do sistema instalado na atual infraestrutura do EBDrive existente no CITEx

6.2. E13 - Dados e usuários

6.2.1. Consiste na migração dos dados dos usuários e na criação de uma nova conta do EBDrive, automaticamente, relacionada à criação de uma nova conta do EBMail.

Tabela 14 - Requisitos, Testes e Critérios de Aceitação de E13

Requisitos	Testes de Aceitação	Critérios de Aceitação
R13.1. Deverão ser migrados os dados dos usuários para a nova versao da solução	T13.1.1. Após a instalação do sistema e migração dos dados e usuários, será verificada a existência do usuário e de seus respectivos arquivos no novo ambiente.	todos os usuários do EBMail devem ter acesso ao EBDrive e esses usuários devem ter acesso aos seus arquivos atualmente armazenados no EBDrive
R13.2. todos os novos usuários do EBMail devem ter uma conta do EBDrive provisionada automaticamente utilizando o portal EBMail.	T13.2.1. será verificado se uma nova conta foi provisionada a partir da criação de uma nova conta no EBMail T13.2.2. esse teste será realizado nos seguintes navedores web: Mozilla Firefox, Safari, Microsoft Edge e Google Chrome.	todos os novos usuários do EBMail devem ter acesso ao EBDrive

6.3. E14 - Nível de segurança e restrição de acesso de compartilhamento de arquivos e pastas

6.3.1. Consiste na definição da maneira como arquivos e pastas podem ser compartilhados e a capacidade de manipulação de arquivos em diferentes formatos adotados pelo mercado, nas operações de *download* e *upload*.

Tabela 15 - Requisitos, Testes e Critérios de Aceitação de E14

Requisitos	Testes de Aceitação	Critérios de Aceitação
R14.1. O EBDrive deve permitir o compartilhamento de arquivos e pastas salvas, através de um link público, permitindo o download desses arquivos e do conteúdo das pastas compartilhadas.	T14.1.1. será realizado o compartilhamento de uma arquivo e de pastas, sendo verificado o acesso público aos mesmos.	compartilhando de arquivos ou pastas através do download do link gerado
R14.2. O EBDrive deve permitir compartilhamento de arquivos e pastas salvas, através de um link privado e por meio da indicação nominal da lista de usuários, permitindo o download desses arquivos e pastas compartilhados, apenas para esses usuários autorizados.	T14.2.1. Esta funcionalidade deverá restringir o acesso que o usuário terá a determinado arquivo ou pasta. O compartilhamento funcionará da seguinte forma: O usuário A concede a permissão de acesso ao arquivo/pasta ao usuário B (acesso somente leitura ou leitura/escrita), através de um link compartilhado, onde somente o usuário B poderá visualizar o arquivo ou pasta mesmo que outro usuário tenha acesso a esse link, garantindo a restrição de acesso ao conteúdo que é	O compartilhamento deverá funcionar exatamente como previsto no teste de aceitação, com a restrição de acesso sendo testada. Um link restrito não poderá ser aberto por um usuário não atribuído ao link

	compartilhado através do link.	
R14.3. Deve ser possível fazer o download e o upload de arquivos (documentos, vídeos e imagens) em diferentes formatos adotados pelo mercado.	T14.3.1. a equipe de teste do Exército fará o download e upload dos diferentes formatos, com o objetivo de testar a funcionalidade disponível para o usuário	Sem erros no download e upload dos arquivos

6.4. E15 - Criação, edição e compartilhamento de documentos no formato open document format: .odt, .ods e .odp

6.4.1. Consiste na criação e edição de documentos, em tempo real, de forma compartilhada ou não, a critério dos usuários.

Tabela 17 - Requisitos, Testes e Critérios de Aceitação de E15

Requisitos	Testes de Aceitação	Critérios de Aceitação
R15.1. Permitir a criação, a edição e o compartilhamento de documentos no formato *open document format*: .odt, .ods e .odp	T15.1.1. a equipe de testes do Exército criará novos documentos em cada um dos formatos, compartilhará esses documentos entre usuários e verificará o funcionamento da edição compartilhada de cada documento. esse teste será realizado nos seguintes navegadores web: Mozilla Firefox, Safari, Microsoft Edge e Google Chrome.	a funcionalidade de criação, edição e compartilhamento de arquivos, deverá funcionar sem problemas ou erros
R15.2. Esta funcionalidade deverá permitir a edição compartilhada de um documento, em tempo real, entre diferentes usuários do EBDrive, previamente definidos.		a edição compartilhada de um arquivo entre dois usuários será confirmada, de acordo com o teste de aceitação
R15.3. O documento a ser editado de forma compartilhada poderá ser um documento existente na conta EBDrive de um dos usuários ou ser um novo documento criado na pasta do EBDrive, sendo possível a edição desse documento por múltiplos usuários.		a edição compartilhada de um arquivo já existente entre múltiplos usuários, precisa ser realizada de acordo com o teste de aceitação
R15.4. O documento deverá ser salvo periodicamente, mantendo a versão mais atual disponível para todos os usuários que compartilhem de sua edição.		o arquivo deverá ser salvo corretamente para todos os usuários que estão usando o compartilhamento
R15.5. A funcionalidade deverá apresentar uma mensagem para confirmação de salvamento do arquivo, contendo data e hora do exato momento que o salvamento ocorre.		A mensagem de confirmação deverá ser apresentada para o usuário após o salvamento, verificar a ocorrência da mensagem

6.5. E16 - Versionamento dos arquivos salvos no EBDrive

6.5.1. Consiste no registro histórico de alterações feitas em documentos, quando editados por um ou vários usuários, com identificação do autor da modificação.

Tabela 18 - Requisitos, Testes e Critérios de Aceitação de E16

Requisitos	Testes de Aceitação	Critérios de Aceitação
R16.1. a solução deve manter um histórico com as modificações realizadas nos arquivos armazenados até 20 versões	T16.1.1. a equipe de testes do Exército fará a edição de até 20 versões de um documento e realizará o *restore* para a versão selecionada.	o histórico de modificações deverá ser criado de forma correta
	T16.1.2. esse teste será realizado nos seguintes navedores web: Mozilla Firefox, Safari, Microsoft Edge e Google Chrome.	a funcionalidade deverá ser exaustivamente testada em todos os browsers, evitando problemas de inoperabilidade

6.6. E17 - Recuperação de arquivos deletados

6.6.1. Funcionalidade que permite ao usuário recuperar um arquivo que tenha sido deletado.

Tabela 19 - Requisitos, Testes e Critérios de Aceitação de E17

Requisitos	Testes de Aceitação	Critérios de Aceitação
R17.1. a solução deverá ser capaz de recuperar arquivos deletados num período de até 15 dias	T17.1.1. será deletado um arquivo do usuário e, em até 15 dias, será realizada a recuperação do mesmo por meio da interface gráfica	o arquivo deletado deverá ser recuperado dentro do período estipulado pela operação
R17.2. após o 15º dia o arquivo deve ser definitivamente excluído do sistema de armazenamento	T17.2.1. será tentado recuperar o arquivo após o período de 15 dias por meio da interface gráfica	o arquivo deverá ser definitivamente removido dentro do período estipulado pela operação
	T17.2.2. esse teste será realizado nos seguintes navedores web: Mozilla Firefox, Safari, Microsoft Edge e Google Chrome.	O arquivo deverá ser definitivamente removido dentro do período estipulado pela operação

6.7. E18 - Scanner de Vírus em arquivos armazenados

6.7.1. Funcionalidade que inibe o *upload* de arquivos maliciosos para a solução de armazenamento.

Tabela 20 - Requisitos, Testes e Critérios de Aceitação de E18

Requisitos	Testes de Aceitação	Critérios de Aceitação
R18.1. O sistema deverá está configurado com a extensão para detecção de arquivos maliciosos	T18.1.1. a equipe de testes do Exército fará o upload de um arquivo malicioso e verificará se o sistema permitirá o seu armazenamento	o antivírus deve detectar e o sistema deve impedir o arquivo malicioso
	T18.1.2. esse teste será realizado nos seguintes navegadores web: Mozilla Firefox, Safari, Microsoft Edge e Google Chrome.	o antivírus deve detectar e o sistema deve impedir o arquivo malicioso em todos os browsers mencionados

6.8. E19 - Disponibilizar a movimentação de arquivos entre pastas na interface web

6.8.1. Funcionalidade que torna mais eficiente a maneira como os arquivos são manipulados pelos usuários na interface do sistema.

Tabela 21 - Requisitos, Testes e Critérios de Aceitação de E19

Requisitos	Testes de Aceitação	Critérios de Aceitação
R19.1. A solução deve permitir, através da interface Drag and Drop (arrastar e soltar), utilizando um mouse, a transferência de um ou mais arquivos, isto é, que os arquivos possam ser movimentados entre as pastas. A facilidade das operações acima devem ser projetadas para serem flexíveis, ou seja, independentemente do número de arquivos ou pastas selecionados, dentro do cenário de transferência de arquivos entre pastas.	T19.1.1. A operação consiste em duas partes: o arquivo de origem (drag), a partir da qual o objeto de origem é arrastado, e de um destino (drop) que recebe o objeto.	deverá funcionar conforme descrito no teste de aceitação
	T19.1.2. A fonte (drag) e o destino (drop) podem ser elementos de interface do usuário no mesmo aplicativo.	deverá funcionar conforme descrito no teste de aceitação
	T19.1.3. O arquivo de origem será movimentado da pasta A (origem) para a pasta B (destino), e o arquivo não se encontrará mais na pasta A (origem) após a operação de drag and drop.	deverá funcionar conforme descrito no teste de aceitação
	T19.1.4. esse teste será realizado nos seguintes navedores web: Mozilla Firefox, Safari, Microsoft Edge e Google Chrome.	deverá funcionar conforme descrito no teste de aceitação

6.9. E20 - Redundância e Alta Disponibilidade

6.9.1. A alta disponibilidade do serviço EBDrive permitirá que o serviço de drive esteja disponível e funcional em período contínuo, ou seja, 24x7 (24 horas por 7 dias da semana).

Tabela 22 - Requisitos, Testes e Critérios de Aceitação de E20

Requisitos	Testes de Aceitação	Critérios de Aceitação
R20.1. a nova versão do EBDRive deverá fazer uso da infraestrutura de armazenamento já disponível no DC -1 EB e sua replicação no DC-2 EB, de forma que a solução seja confgurada em *cluster* de alta disponibilidade	T20.1.1. serão copiados arquivos para o EBDrive, posteriormente será desativado a infraestrutura presente no DC - 1 e a infraestrutura do DC - 2 deverá assumir imediatamente o serviço.	a infraestrutura replicada deverá assumir o serviço, conforme o teste de aceitação

6.10. E21 - Solução de Backup Automático do EBDrive

6.10.1. A solução de backup é um processo automático de geração de uma cópia de segurança para os dados de usuários, assim como rotinas de migração e recuperação de dados. Devem ser criadas cópias de segurança dos dados de forma que possam ser restaurados em caso de perda dos dados

originais.

Tabela 23 - Requisitos, Testes e Critérios de Aceitação de E21

Requisitos	Testes de Aceitação	Critérios de Aceitação
R21.1. a solução automatizada de backup deverá interoperar com a solução existente no 7º CTA (solução VEEAM)	T21.1.1. será realizada a instalação do agente de backup do VEEAM, no servidor do EBDrive, e posteriormente será configurado a execução de scripts que farão chamadas às rotinas de backup desenvolvidas para a realização do backup	as rotinas de backup deverão ser desenvolvidas para garantir o funcionamento e a realização do backup, conforme teste de aceitação
R21.2. A solução deverá dispor de rotinas de backup/restore dos arquivos dos usuários, bem como das bases de dados e de todos os arquivos de configuração, utilizados pelo sistema de armazenamento, necessários para promover a recuperação completa da solução a partir de uma nova instalação.	T21.2.1. será realizada uma nova instalação do sistema de armazenamento, em um ambiente de testes, para a recuperação total do ambiente de produção por meio dos arquivos de backup (Full, incremental e contínuo)	A funcionalidade de backup deverá ser realizado conforme o teste de aceitação
R21.3. Os procedimentos de backup devem ser executados de maneira inteligente, prevendo as sistemáticas de Backup Full, Backup Incremental e Backup Contínuo, dependendo da política adotada pelo Exército.		A funcionalidade de backup deverá ser realizado conforme o teste de aceitação
R21.4. a solução deverá possuir rotinas de *restore* granular, ou seja, deve ser possível recuperar os arquivos por usuário.	T21.4.1. será realizado o *restore* de uma conta de usuário em particular	A funcionalidade de restore deverá ser realizado conforme o teste de aceitação
	T21.4.2. esse teste será realizado nos seguintes navegadores web: Mozilla Firefox, Safari, Microsoft Edge e Google Chrome.	

6.11. E22 - Atualização da interface do EBDrive

6.11.1. Aplicação das modificações de interface da identidade visual do atual EBDrive, de modo a atender os requisitos da Tabela 24, abaixo.

Tabela 24 - Requisitos, Testes e Critérios de Aceitação de E22

Requisitos	Testes de Aceitação	Critérios de Aceitação
R22.1. Deverá mostrar, imediatamente, o nome completo do arquivo ao passar o cursor do mouse por cima do arquivo.	T22.1.1.será passado o cursor do mouse sobre um arquivo cujo nome de exibição seja maior que o exibido na tela	o nome deverá ser apresentado de forma correta
R22.2. Ao clicar sobre o arquivo, selecionar o mesmo. Para abri-lo,	T22.2.1. será dado 1 (um) clique sobre um arquivo para selecioná-lo	a seleção do arquivo deverá ocorrer com apenas um clique

deverá clicar duas vezes.	T22.2.2. serão dados 2 (dois) cliques sobre um arquivo para abri-lo	a abertura do arquivo deverá ocorrer com duplo clique
R22.3. Deverá permitir a ordenação dos arquivos, em ordem crescente e decrescente, por data de alteração e tamanho.	T22.3.1. será ordenada uma lista de arquivos por ordem crescente e decrescente de data de alteração e de tamanho	uma lista de arquivos deverá ser apresentada de forma ordenada, conforme o teste de aceitação
R22.4. Deverá permitir a visualização dos arquivos em formato de lista ou em formato de grade.	T22.4.1 serão alternados os modos de exibição em lista e em grade de um conjunto de arquivos	visualização a ser exibida no formato exigido no teste de aceitação
R22.5. Deverá disponibilizar dados sobre a última alteração do arquivo, como data, hora, “dono” do arquivo e permissões do arquivo.	T22.5.1. será feita a identificação visual dos dados sobre a última alteração do arquivos, como data, hora, "dono" do arquivo e permissões do arquivo	confirmar e a alteração dos arquivos está com a identificação visual correta, de acordo com o exigido.
R22.6. Deverá permitir pré-visualização de arquivos em painel lateral e em ícones na forma de exibição de grade	T22.6.1. será feita a identificação visual da pré-visualização de arquivos (documentos, fotos e vídeos) em painel lateral e em ícones na forma de exibição em grade	a pré-visualização dos arquivos esta sendo gerada na exibição exigida, conforme teste de aceitação
R22.7. Atualizar a interface Web do EBDrive para a inclusão das novas funcionalidades, mantendo a identidade visual da solução atual	T22.7.1. será feita a identificação visual das novas funcionalidades na interface Web atualizada e a identificação da manutenção do padrão de cores do cliente Exército Brasileiro, tal como a versão atual	layout no formato exigido pelo Exército Brasileiro, conforme teste de aceitação
	T22.7.2. esse teste será realizado nos seguintes navedores web: Mozilla Firefox, Safari, Microsoft Edge e Google Chrome.	a Identificação visual deverá funcionar corretamente em todos os browsers mencionados, conforme teste de aceitação
	T22.7.3. a equipe de testes do Exército fará uma análise estática do código fonte e da documentação entregue, não podendo apresentar falhas de segurança, erros de funcionalidade.	realizar a analise com o intuito de procurar possiveis erros no codigo entregue pela CONTRATADA

6.12. E23 - Acesso unificado EBMail - EBDrive

6.12.1. Consiste no acesso ao serviço EBDrive sem solicitação de novo *login* para o usuário que já estava em sessão logada no EBMail.

Tabela 25 - Requisitos, Testes e Critérios de Aceitação de E23

Requisitos	Testes de Aceitação	Critérios de Aceitação
R23.1. os usuários deverão acessar o EBDrive a partir de sessão logada no EBMail	T23.1.1. será realizada o acesso ao EBMail, uma vez logado, por meio da interface gráfica do EBMail o usuário irá clicar no ícone do EBDrive e o mesmo deverá ser direcionado para a sua página do EBDrive sem a necessidade de realizar um novo *login*	a funcionalidade deverá funcionar conforme o teste de aceitação
	T23.1.2. esse teste será realizado nos seguintes navegadores web: Mozilla	funcionar corretamente em todos os browsers mencionados, conforme teste

	Firefox, Safari, Microsoft Edge e Google Chrome.	de aceitação

6.13. E24 - Configuração de Performance do Agente de Backup

6.13.1. Consiste na configuração de parâmetros de performance do agente de backup, por meio da interface WEB, para utilizar o máximo da capacidade disponível do sistema de backup.

Tabela 26 - Requisitos, Testes e Critérios de Aceitação de E24

Requisitos	Testes de Aceitação	Critérios de Aceitação
R24.1. Por meio da interface WEB, será possível trabalhar diretamente no navegador de internet. No EBDrive-Admin deverá ser possível determinar parâmetros de performance do agente de sincronização.	T24.1.1. por meio da interface web, será visualizado todos os parâmetros que serão utilizados para a melhorar a performance de sincronização dos arquivos, por meio do agente de sincronização	o parâmetro deverá melhorar a performance e que seja possível a visualização dos parâmetros utilizados.
R24.2. Com a alteração de parâmetros, deverá ser possível utilizar o máximo da capacidade disponível do agente de sincronização, na tentativa de melhorar a performance em tempo e capacidade.	T24.2.1. com os parametros configurados na interface web, deverá ser possível o acompanhamento do resultado de cada parâmetro, como tempo, capacidade disponível e melhoria na performance de sincronização.	atestar que o parâmetro utilizado melhorou o tempo e a performance de sincronização dos arquivos do usuário e garantiu a sincronização eficiente dos arquivos.

6.14. E25 - Monitoramento dos agentes ativos na plataforma através de interface WEB

6.14.1. Consiste na verificação de disponibilidade (ou não) e o status de agentes de backup na plataforma, por meio da interface WEB do EBDrive-Admin.

Tabela 27 - Requisitos, Testes e Critérios de Aceitação de E25

Requisitos	Testes de Aceitação	Critérios de Aceitação
R25.1. Por meio da interface WEB será possível, utilizando o EBDrive-Admin, verificar a disponibilidade (ou não) de um determinado agente de sincronização.	T25.1.1. será analisado pela interface o status de cada agente de sinronização, com os status running ou stopped, determinando o atual status dos agentes.	retorno do status de cada agente de sincronização, conforme teste de aceitação
R25.2. Por meio da interface WEB, será possível analisar o status de cada agente de sincronização e identificar possíveis problemas durante o sincronismo ou até mesmo apenas analisar o status do agente de sincronização naquele momento.	T25.2.1. através da interface Web será analisado o status de cada agente durante a execução, seja pela sincronização realizada ou por tempo estimado em minutos para a sincronização.	apresentar o status dos agentes e também o status de cada sincronização

6.15. FUNCIONALIDADES COMUNS A TODOS OS 5 (CINCO) SUBSISTEMAS

6.15.1. Documentação e código do sistema:

6.15.1.1. Independente da metodologia de desenvolvimento da CONTRATADA, todo serviço de contratação de software do Exército deve obedecer, também, às

normas contidas no manual EB80-MT-78.001 - Manual Técnico para Metodologia de Desenvolvimento de Software do Exército, entregando a documentação completa prescrita no manual;

6.15.1.2. Manter histórico de modificações de código em repositório git, desde o fork da versão obtida no repositório da Zimbra e incluindo todas as modificações realizadas.

6.15.1.3. Entrega de todo documentação solicitada pela CONTRATANTE:

6.15.1.3.1. Código Fonte Final da solução EBMail, EBDrive e Portal EBMail;

6.15.1.3.2. Documentação com todas as modificações e ajustes realizados no código fonte do Zimbra para torná-lo compatível com a Alta Plataforma;

6.15.1.3.3. Script de Build e deploy da solução EBMail, EBDrive e Portal EBMail;

6.15.1.3.4. Documentação de implantação;

6.15.1.3.5. Documentação prevista no manual EB80-MT-78.001 - Manual Técnico para Metodologia de Desenvolvimento de Software do Exército.

6.15.2. Migração de dados da versão atual

6.15.2.1. Fica sob responsabilidade da CONTRATADA a migração de todo e qualquer dado dos usuários na versão atual do EBMail (ambiente de produção) para o ambiente com a nova versão sendo contratada.

6.15.2.2. Essa migração de dados ocorrerá no início do período de Operação Assistida.

6.16. SUPORTE TÉCNICO

6.16.1. A CONTRATADA deverá fornecer toda mão-de-obra especializada, ferramentas e instrumentos necessários para a execução do serviço de Suporte Técnico;

6.16.2. Quaisquer problemas que venham a comprometer o alcance dos níveis de serviço estabelecidos devem ser imediatamente comunicados à CONTRATANTE;

6.16.3. Disponibilizar as versões mais atualizadas do Zimbra e Sistema Operacional ofertados para proceder à imediata substituição das versões anteriores;

6.16.4. A CONTRATADA deverá prestar o serviço de Suporte Técnico da solução entregue, durante todo o período de Suporte Técnico.

6.16.5. O atendimento da Suporte Técnico deverá ocorrer durante 24 (vinte e quatro) horas, de segunda-feira à segunda-feira. O atendimento deverá ocorrer através dos seguintes canais: telefone, e- mail, ordem de serviço, ou demais canais disponibilizados.

6.16.6. A prestação de serviços de Suporte Técnico será executada com base nos seguintes termos:

6.16.6.1. Ordens de Serviço:

6.16.6.2. Para o atendimento das solicitações de serviços de Suporte Técnico será aberta uma Ordem de Serviço (OS) emitidas pela CONTRATANTE por meio de interfaces disponibilizadas pela CONTRATADA.

6.16.6.3. A CONTRATADA imediatamente após a abertura do chamado, seja por telefone ou correio eletrônico, deverá encaminhar por correio eletrônico, ao

responsável pela sua abertura, cópia da ordem de serviço explicitando o número de registro do chamado e demanda da CONTRATANTE.

6.16.6.4. A CONTRATADA deverá possuir uma plataforma para abertura e acompanhamento de chamados por meio de acesso Web, e-mail e contato telefônico.

6.16.6.5. A CONTRATADA deverá registrar a data e hora exatos da abertura do chamado pela CONTRATANTE em sua plataforma para abertura de chamados.

6.16.6.6. O suporte deverá ser prestado pela contratada da seguinte maneira e com as condições: "Suporte Remoto", após a abertura da OS.

6.16.6.7. A empresa contratada deverá disponibilizar suporte com equipe altamente qualificada.

6.16.6.8. O "Suporte Remoto" será feito perante liberação de acesso pelo Exército Brasileiro por meio de VPN.

6.16.6.9. Os serviços serão prestados por meio de acesso remoto, com acompanhamento em tempo real por videoconferência entre os técnicos da CONTRATANTE e a equipe técnica da CONTRATADA.

6.16.7. Prazos para atendimento:

6.16.7.1. Regime de atendimento será de 24x7x365.

6.16.7.2. O tempo de resposta inicial e o tempo de resolução deverão respeitar, no mínimo, os seguintes níveis de serviço conforme as Tabelas 28 e 29, abaixo:

Tabela 28 - Níveis de Serviço

Nível de severidade	Tempo Inicial de resposta	Tempo de Resolução
Severidade 1	até 30 minutos	No máximo 4 (quatro) horas, contadas após o início do atendimento
Severidade 2	até 1 horas	No máximo 12 (doze) horas, contadas após início do atendimento
Severidade 3	até 2 horas	No máximo 24 (vinte e quatro) horas, contadas após início do atendimento
Severidade 4	até 4 horas	No máximo 48 (quarenta e oito) horas contadas após início do atendimento

Tabela 29 - Níveis de Severidade

Severidade 1	Indisponibilidade do sistema em produção sem a existência de uma solução temporária
	Quando um serviço crítico da solução não está respondendo e não pode ser reiniciado ou estabilizado. Este nível requer um profissional disponível também do lado do cliente para realizar as atividades necessárias

Severidade 2	Problema com uma funcionalidade principal, porém possui uma solução temporária ou não causa indisponibilidade do serviço
Severidade 3	Problema com uma funcionalidade complementar, porém possui uma solução temporária ou não causa indisponibilidade do serviço
Severidade 4	Questões gerais sobre utilização

6.16.7.3. As metas de resposta serão medidas em horas corridas, a partir do primeiro registro da solicitação no sistema, ou o contato telefônico direto com a equipe de suporte da contratada (para Severidade 1).

6.16.7.4. O início da contagem do prazo de atendimento será no momento em que a ordem de serviço estiver disponível na fila de atendimento da CONTRATADO.

6.17. TREINAMENTO NAS SOLUÇÕES

6.17.1. Durante o Período de Homologação do Sistema, a CONTRATADA deverá fornecer treinamento na solução desenvolvida.

6.17.2.O treinamento deverá fornecer os conhecimentos necessários à equipe técnica da CONTRATANTE visando a instalação e operação da solução desenvolvida.

6.17.3.O treinamento terá carga horária mínima de 40 horas e será realizado, preferencialmente, no formato presencial, nas instalações da CONTRATANTE.

6.17.4. O(s) instrutor(es) deve(m) ser plenamente capacitado(s) para ministrar o treinamento na solução atualizada;

6.17.5. A turma será composta, exclusivamente, por militares indicados pela CONTRATANTE.

6.17.6.A ementa do treinamento deverá ser apresentada no início do período de homologação a ser validada pela Equipe de Fiscalização do Contrato.

6.17.7.A ementa do treinamento deverá conter, no mínimo, os seguintes tópicos:

6.17.7.1. customização e ajustes do código fonte do Zimbra;

6.17.7.2. procedimentos para compilação do produto;

6.17.7.3. procedimentos de instalação do sistema;

6.17.7.4. procedimentos para a operação da solução;

6.17.7.5. procedimentos de troubleshooting da solução; e

6.17.7.6. procedimentos de backup e restore da solução.

6.17.8. O material didático utilizado no treinamento deverá estar escrito em língua portuguesa.

6.17.9. Os custos com a hospedagem e o deslocamento dos técnicos até o local do treinamento, serão de responsabilidade da CONTRATADA.

6.17.10. Após o aceite da homologação e a realização do treinamento, o Fiscal do Contrato autorizará o início do período de Operação Assistida.

7. APÊNDICES

7.1.1. Apenso a este Descritivo da Solução Técnica, encontra-se o seguinte documento:

7.1.1.1. Apêndice A - Relação de Entregas, Requisitos, Testes e Critérios de Aceitação