ANEXO VII

PLANO DE CONTINGÊNCIA E RECUPERAÇÃO DE DESASTRE

1 INTRODUÇÃO

1.1 Objetivo

A M Square Investimentos Ltda. ("**Empresa**" ou "**M Square**") elaborou este plano de contingência e recuperação de desastre (o "**Plano de Contingência**") com o objetivo de estabelecer os procedimentos adequados ao gerenciamento de situações de contingência, cenários de incidentes, desastres ou falhas que causem impacto nas rotinas operacionais da empresa como um todo ("**Eventos de Contingência ou Desastre**") com vistas a assegurar à M Square e seus colaboradores a plena continuidade operacional das atividades da empresa, a todo tempo e sob qualquer circunstância.

São exemplos de Eventos de Contingência ou Desastre: suspensão total ou interrupção temporária na prestação de serviços por provedores de energia, acesso à internet, serviços de telefonia, etc., catástrofes naturais que impeçam o acesso ao prédio, interdição do prédio onde funciona a sede da M Square por qualquer motivo, inclusive em cenários de greves, pane nos sistemas e softwares utilizados pelos Colaboradores da Empresa, perda de arquivos por qualquer motivo, dentre outros.

Dentre as funcionalidades críticas à M Square a que este Plano de Contingência se propõe a cobrir incluem-se (i) a contínua execução de trades (com a respectiva manutenção das regras de *compliance* aplicáveis), (ii) o desempenho das rotinas operacionais, (iii) a possibilidade de recebimento e troca regular de e-mails (sejam internos ou com contrapartes externas) e atendimento telefônico via PABX além de (iv) acesso/uso ininterrupto aos sistemas, funcionalidades e arquivos utilizados pela Empresa, conforme descritos no item 1.2 abaixo ("**Sistemas Cobertos**"), mesmo em caso de total impossibilidade de acesso ao escritório físico da Empresa.

1.2 Funcionalidades e Sistemas Cobertos

São funcionalidades e sistemas cobertos para fins deste Plano de Contingência:

- E-mails & Intranet;
- Sistema de passivo, *Phibra*;
- Sistema de carteiras – Phibra;
- *Bloomberg*; e
- Fileserver.

2 MEDIDAS PREVENTIVAS

A M Square adota as seguintes medidas preventivas visando a mitigação de eventuais riscos de ocorrências de Eventos de Contingência ou Desastre:

A. Rota de fuga, sinalização de emergência e simulações de incêndio: a sinalização das rotas de fuga e colocação da sinalização de emergência é feita em locais estratégicos do escritório da Empresa e facilmente identificáveis. Os colaboradores são ainda, instruídos à se portarem com um padrão de conduta adequado em caso de incidentes com fogo. Neste caso, os colaboradores são obrigados a participar das simulações periódicas de incêndio realizadas pelo condomínio de modo a se familiarizarem com os procedimentos mínimos exigidos para o caso de uma ocorrência que demande a evacuação do prédio.

B. Identificação de visitantes / Circulação de terceiros: com vistas a assegurar um nível de segurança mínimo nas suas premissas, os visitantes são identificados pelo condomínio, e somente permitidos a subir ao escritório da M Square mediante prévia aprovação de um dos colaboradores. Neste mesmo sentido, os visitantes e prestadores de serviços são instruídos a observar o procedimento padrão para circulação dentro do escritório, não sendo permitida sua entrada no salão principal exceto se acompanhado de um colaborador. Ademais, a entrada de colaboradores no escritório é controlada por sistema de biometria.

C. Monitoramento do Ambiente Corporativo: o monitoramento do ambiente corporativo se dá através da instalação de câmeras em locais estratégicos do escritório, permitindo a identificação de quem acessa o escritório, com a respectiva retenção das gravações.

D. Avaliação Periódica dos Circuitos Elétricos e Instalações Hidráulicas: a Empresa, através de prestadores de serviços terceirizados, realiza anualmente a reavaliação dos circuitos elétricos e do sistema hidráulico de seu escritório com vistas a mitigar riscos de curto-circuito e rompimento e/ou defeito das instalações hidráulicas (registros, válvulas e pontos de infiltração).

E. Telefones de Colaboradores: a Empresa disponibiliza aos seus colaboradores - em sua intranet - o acesso à lista de telefones celulares pessoais de cada um dos demais colaboradores, inclusive para os casos de emergência, facilitando assim a comunicação em cenários de estresse ou emergenciais.

3 INFRAESTRUTURA TECNOLÓGICA

A M Square é detentora de uma infraestrutura tecnológica robusta. A Empresa opera com 1 *datacenter* próprio onde ficam localizados seus servidores físicos e virtuais e 1 *datacenter* virtual de *Disaster Recovery,* hospedado na Microsoft. Todos os sistemas de produção e arquivos rodam nos servidores e todos eles têm redundância interna completa (discos e fontes de energia).

Sistemas: Os servidores responsáveis pelos sistemas de produção (Phibra) e bancos de dados da Empresa estão localizados em *datacenter* próprio, com equipamentos totalmente redundantes (Storage EMC, Servidores Dell operando em modo Virtual através de VmWare), de tal maneira que nenhuma falha única cause indisponibilidade sistêmica (No Single Point of Failure). O uptime médio está acima de 99.9% ao longo dos últimos 4 anos. Além disso, diariamente é feito um back-up dos arquivos em nuvem (Microsoft Azure) e criptografado.

Arquivos: Os servidores responsáveis pelo sistema de arquivos (*File Server*) da M Square estão localizados em *datacenter* próprio localizado no escritório da M Square – em um ambiente com servidores, *storage* e rede totalmente redundantes (CPD) – e todos os dados desse sistema de arquivos são sincronizados em tempo real, com o ambiente de *Disaster Recovery*. Além disso, diariamente é feito um back-up dos arquivos em nuvem (Microsoft Azure), criptografados e com política de retenção de 10 anos.

E-mail: O sistema de e-mail também está localizado fora do escritório (Microsoft Office 365), com retenção/armazenamento automático de todos os e-mails por 5 anos. Sendo assim, em caso de um Evento de Contingência ou Desastre, todo o histórico de e-mails estará disponível via *webmail* e o fluxo de entrada e saída de e-mails não será afetado.

Acesso à rede: Todas as permissões de rede/login/senha são sincronizadas online com o ambiente de *Disaster Recovery,* tendo em vista a existência de um *domain controller* da rede. Ou seja, uma alteração de senha no ambiente de produção é replicada no ambiente de *Disaster Recovery* em questão de segundos, viabilizando desta forma, o acesso remoto à rede com o mesmo login e senha de acesso utilizados no escritório físico.

PABX: Nossa telefonia (PABX e troncos) está na nuvem, em modo de alta disponibilidade. Adicionalmente, vale ressaltar que todas as ligações são gravadas e as mesmas ficam disponíveis por 5 anos.

Escritório: O escritório da M Square possui redundância no acesso à internet (3 links), backup de eletricidade (2 nobreaks com 2 horas de autonomia e 4 geradores no prédio, que entram em serviço em média 19 segundos após uma falta de luz) e 2 fornecedores de telefonia, pois caso um deles falhe, o outro será ativado, permitindo a continuidade dos negócios sem interrupções. Este Plano de Contingência foi estruturado de forma a garantir a manutenção do maior tempo de atividade possível ao nosso escritório.

Provedores de Serviço de TI: A M Square conta um fornecedor externo (Atual - IT) que fica disponível 24/7. Este fornecedor consegue trabalhar remotamente sobre a quase totalidade dos problemas e, caso necessário, está comprometido em mandar um técnico ao escritório em menos de uma hora para suporte.

Disaster Recovery: A estrutura externa de *Disaster Recovery* (ver abaixo "Estrutura e Plano de *Disaster Recovery*") é sincronizada automaticamente e pode ser acessada em Eventos de Contingência ou Desastre, observados os critérios e procedimentos abaixo definidos.

Sumário da Infraestrutura:

Sistemas e Bancos de dados	Localizados em d*atacenter* próprio e sincronizados diariamente com um *datacenter* externo de *Disaster Recovery*, além de backup em nuvem
Arquivos	Localizados em d*atacenter* próprio e sincronizados em tempo real com um *datacenter* externo de *Disaster Recovery*, além de backup em nuvem.
E-mails	Armazenados e fluem através de uma solução em nuvem da Microsoft (Office365), com retenção dos últimos 5 anos.
PABX/ Telefonia	Produção Nuvem e contingência no local.
Desktops Virtuais	Disponível o serviço de Terminal Service no *datacenter* da Microsoft, que se encontra sempre atualizado e em total compatibilidade com os sistemas operacionais utilizados nas rotinas diárias da Empresa, permitindo a plena continuidade das funções críticas inerentes ao negócio no caso de um Evento de Contingência ou Desastre. Para acesso ao serviço de Terminal Service, é necessário tão somente que o colaborador possua um computador (Windows ou Mac) com acesso à Internet.

4 ESTRUTURA E PLANO DE *DISASTER RECOVERY*

A M Square possui uma estratégia para cenários de desastre composta por (i) back-ups de seus sistemas e (ii) estrutura de acesso remoto aos seus desktops, com sincronismo diário e completamente disponíveis para uso tanto em caso de um desastre físico envolvendo seu escritório quanto em caso de contingencia envolvendo o ambiente de *Disaster Recovery*.

(i) Back-up de Sistemas: com relação aos sistemas, todos os sistemas de produção da Empresa estão localizados em um *datacenter* próprio, com sincronismo diário para um *datacenter* externo hospedado na Microsoft. Além disso, é feito diariamente backup em nuvem e criptografado, para garantir a capacidade de restaurar o ambiente caso algum evento afete o escritório.

(ii) Acesso remoto a desktops: com relação ao acesso remoto por colaboradores da Empresa a seus desktops, a Empresa conta com um contrato com a Microsoft com back-up de Sistemas, bancos de Dados, *File Server* e um Terminal Service para cenários de contingência. Este Terminal Service destina-se a atender as 4 áreas críticas da Empresa, com funções que são *time sensitive* e não podem parar. Os Sistemas Cobertos ficam atualizados neste Terminal Service, a todo o tempo, formando um ambiente de *Disaster Recovery* ("**DR**"). Sempre que instalado um novo sistema ou uma versão de sistema atualizada no ambiente de produção, o mesmo procedimento é replicado no ambiente de DR mantendo, desta forma, os desktops de uso diário e o Terminal Service simultaneamente sincronizados.

O acesso ao ambiente de DR é feito através da utilização de mesmo usuário e senha da rede adotados no acesso ordinário de dentro da Empresa.

Por questões de segurança, neste ambiente foi desabilitado funções de transferência de arquivos entre a estação do usuário e o Terminal Service.

Para mais detalhes sobre como proceder para o acesso ao ambiente de DR, vide Anexo A do presente Plano de Contingência.

5 PROCEDIMENTOS

5.1 Procedimentos durante um Evento de Contingência ou Desastre

- **Falha de Sistemas:**

No caso de um Evento de Contingência ou Desastre que implique na descontinuidade na prestação de serviço atrelados aos sistemas operacionais considerados críticos – Sistemas Cobertos, e/ou em seus servidores e rede, a Atual-IT atuará para reestabelecer o acesso aos referidos sistemas de forma emergencial, além de ativar imediatamente e disponibilizar na rede em modo redundante. Caso tal falha seja decorrente de um Evento de Contingência ou Desastre na qual fique inviabilizado o acesso ao escritório físico da M Square, os colaboradores devem se orientar para que o acesso seja feito remotamente e conforme guia de acesso remoto disponível na sede da Empresa.

- **Falha de Infraestrutura:**

(a) Energia Elétrica: caso haja falha no fornecimento de energia, a M Square conta com os seguintes recursos: (i) 2 sistemas de alimentação secundária de energia elétrica (nobreaks) com 2 horas de autonomia de bateria; e (ii) 4 geradores no prédio inicializados automaticamente que levam em média 19 segundos para ativação após a ocorrência de queda de energia e possuem autonomia de mais 36 horas até que seja necessário seu reabastecimento.

- ✓ Principais Ações e Responsáveis: Caso os back-ups de eletricidade elencados acima não funcionem ou sejam insuficientes, a Atual-IT orientará os *Key Users* para que se desloquem até suas casas e deem continuidade operacional aos trabalhos via acesso aos Desktops Virtuais (Terminal Service) localizados no *datacenter* externo.

(b) Comunicações: a M Square conta com 3 links de acesso à internet (redundância) para a eventualidade de uma falha na prestação do serviço do provedor de internet e/ou no link de dados.

Da mesma forma, a Empresa possui back-up de telefonia.

(c) Controle Ambiental CPD: o ambiente do CPD situado no escritório da M Square é monitorado regularmente para garantir o seu correto funcionamento e a manutenção de temperatura (aproximadamente 21° C) e umidade (aproximadamente 22%).

- ✓ Principais Ações e Responsáveis: A Atual-IT é responsável por monitorar diariamente, inclusive via acesso remoto, as condições mínimas de funcionamento do CPD. Caso haja qualquer intercorrência no ambiente do CPD gerando falha nos mecanismos de controle e/ou alteração de tais condições, a Atual-IT atuará para mitigação das falhas e reestabelecimento de suas funcionalidades, inclusive comunicará à Diretora de Gestão de Risco da M Square (nomeada nos termos do seu contrato social) caso verifique que um problema no CPD pode causar falhas acessórias sistêmicas. Neste sentido, a Atual-IT e a Diretora de Gestão de Risco atuarão, conjuntamente, para desenvolver um plano imediato de ação. Dependendo do grau de complexidade da falha e por medida de segurança, caberá a Diretora de Gestão de Risco orientar os demais colaboradores a procederem à evacuação do escritório, e subsequente acesso remoto aos desktops virtuais. Caso isso aconteça, a Atual-IT solicitará à administradora do escritório que proceda à imediata comunicação dos fatos ao condomínio.

(d) Desastres (Incêndio, inundação, assalto, etc): Eventos de Contingência ou Desastre que impliquem na evacuação e/ou inacessibilidade do escritório físico onde está localizada a sede social da Empresa, impossibilitando o acesso aos sistemas de operação da empresa.

- ✓ Principais Ações e Responsáveis: Além dos procedimentos padrão de evacuação do edifício e atuação ativa dos brigadistas para salvaguardar a vida dos colaboradores da M Square, ficará a cargo da Atual-IT e em sua ausência, da Diretora de Gestão de Risco da M Square, atuar para viabilizar a ativação do site de contingência, permitindo às 4 áreas críticas e aos colaboradores designados para seu acesso, nos termos acima, acesso seguro e integral à rede, aos Sistemas Cobertos, aos seus e-mails e demais recursos mínimos necessários para restabelecimento operacional, sem maiores rupturas.

  Para tanto, a orientação aos colaboradores é de procederem às suas residências ou a um local seguro em que possam, através de qualquer computador, acessar os computadores virtuais que ficam disponíveis no site da Microsoft Azure seguindo os procedimentos descritos no item 5.2 abaixo.
- ✓ Tempo de Ação: Imediato - quanto antes for a atuação da Empresa e de seus colaboradores, menor será o prejuízo. A Atual-IT ficará a inteira disposição dos *Key-Users* para viabilizar os acessos aos Sistemas Cobertos em Eventos de Contingência ou Desastre.

5.2 Acesso ao Ambiente DR

Os procedimentos para acesso ao TERMINAL SERVICE encontram-se detalhados abaixo:

Neste cenário, os colaboradores permanecem com acesso full aos e-mails (incluindo nos aparelhos celulares). Os sistemas de arquivos estão com a última versão de contato com o site, já que a replicação é em tempo real. Os bancos de dados e sistemas serão restaurados para D-1 na ocasião do evento, sendo necessário refazer as rotinas do dia do desastre.

A Empresa disponibiliza o acesso ao ambiente DR para dois grupos segregados de Colaboradores, quais sejam:

(1) Key Users – áreas consideradas críticas para fins de continuidade do negócio em um Evento de Contingência ou Desastre, são elas: *Trading, Back-office, Compliance* e Relações com Investidores.

(II) Demais Colaboradores

A prioridade de atendimento é para os *Key Users*, seguida de restauração do ambiente de produção e posteriormente, atendimento e acesso aos demais usuários. Em caso de problemas no acesso durante um Evento de Contingência ou Desastre, os colaboradores são orientados a ligar ou contatar um dos contatos listados na lista de emergência disposta na intranet da Empresa.

5.3 Procedimentos após Evento de Contingência ou Desastre

Na ocorrência de um Evento de Contingência ou Desastre, será estabelecido um comitê de gerenciamento de crise ("**Comitê de Gerenciamento de Crise**"), composto essencialmente pela Atual- IT, Diretora de Gestão de Risco e um colaborador nomeado em conjunto por ambos, os quais ficarão responsáveis por:

- avaliar os impactos diretos e indiretos sofridos;
- elaborar e implementar um plano de ação para recuperação dos serviços impactados, em especial com vistas a restabelecer as 4 funções críticas à Empresa, com a maior brevidade possível;
- comunicar aos demais Colaboradores acerca do referido plano de ação e se necessário, convocá-los para reunião presencial para esclarecimento de dúvidas e ponderações acerca das medidas que foram e serão adotadas em tal cenário; e
- atuar para a reparação da estrutura afetada, incluindo, mas não se limitando, conforme o caso, ao reestabelecimento do ambiente, dos sistemas de rede e operacionais, bem como estabelecer metodologias de prevenção à ocorrência de novos eventos de contingência ou desastre com características similares (se e quando possível) mitigando, desta forma, o risco de recorrências.

O Comitê de Gerenciamento de Crise será instaurado e permanecerá atuante até que sanados todos problemas decorrentes do Evento de Contingência ou Desastre e restabelecidas, em sua integralidade, as funções e atividades da Empresa.

6 REGISTROS, TREINAMENTOS & REVISÕES PERIÓDICAS

6.1 Registros de Ocorrências

Caberá ao Comitê de Gerenciamento de Crise o registro em pauta de toda e qualquer incidência que implique na ativação dos procedimentos de contingência descritos neste plano. Constará de tal registro, no mínimo:

- Descrição dos fatos;
- Data e hora (quando aplicável) da ocorrência;
- Descrição das medidas adotadas;
- Data e hora (quando aplicável) do reestabelecimento das condições normais de trabalho;
- Informações adicionais (eventualidades, estragos e afins); e
- Assinaturas do Diretor de Gestão de Risco e da Atual-IT.

As pautas de registro ficarão armazenadas com a Diretora de Gestão de Risco pelo prazo de cinco anos.

6.2 Treinamentos Periódicos

Todos os Colaboradores comparecerão a um treinamento anual sobre o presente Plano de Contingência (e quando necessário, a reuniões adicionais sobre o tema), que se dará conjuntamente com a reunião anual de treinamento de *Compliance*. Tal treinamento será elaborado e apresentado pela Atual-IT sob supervisão do Diretor de Gestão de Risco.

6.3 Revisões Periódicas

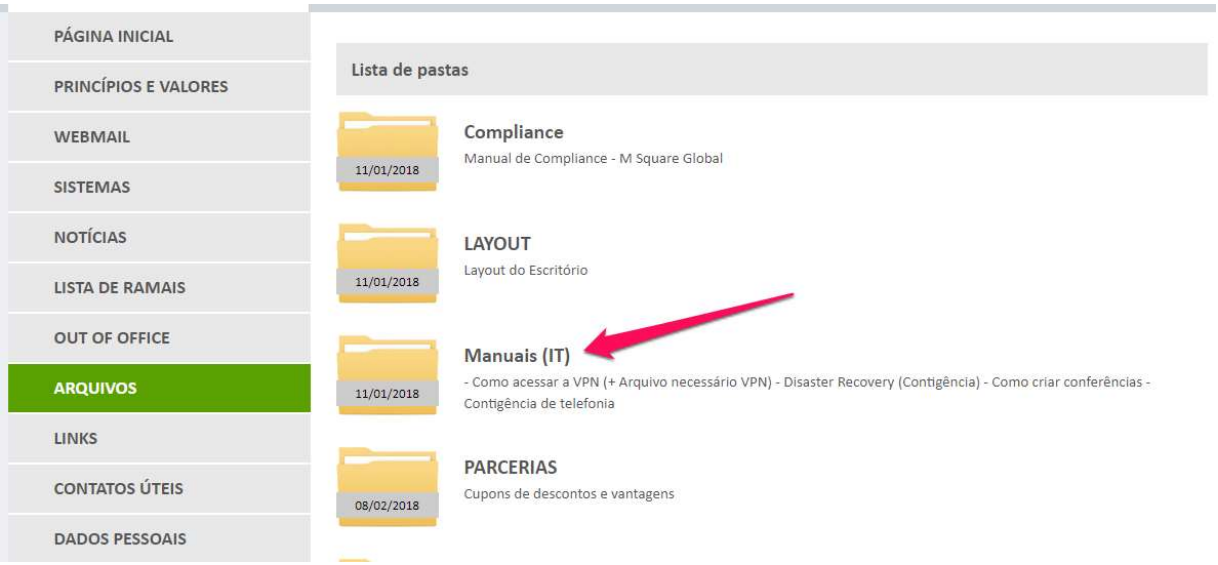
O presente Plano de Contingência será revisado anualmente pela Atual-IT ou, quando necessário, na ocorrência de alterações nos processos ou na estrutura adotados pela M Square (seja por otimização, adequações, ou introdução de novas tecnologias) e estará sujeito à validação pelo Diretor de Gestão de Risco da M Square. O Plano de Contingência será também testado, conforme a regulação aplicável, com o objetivo de avaliar se o Plano é capaz de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios da M Square e de manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotada, e se pode ser ativado tempestivamente.

Todos os Colaboradores receberão uma cópia do presente Plano de Contingência, além do treinamento anual mencionado acima, e poderão acessá-lo, em sua versão mais atual, a qualquer tempo, no website da Empresa.

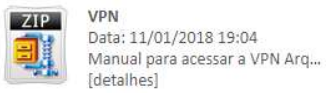
ANEXO A

Acesso ao ambiente de DR

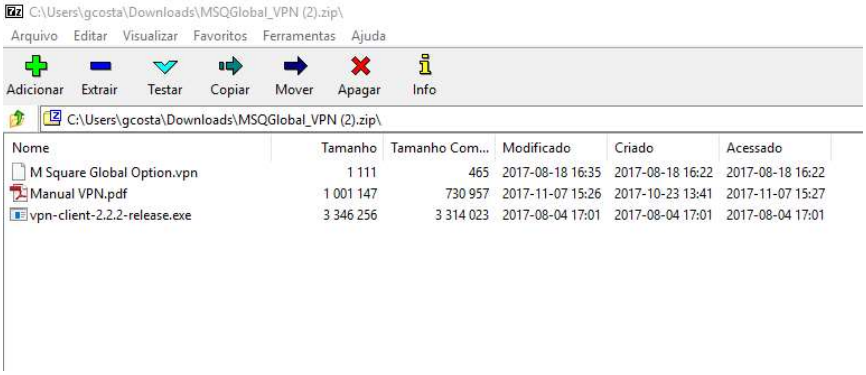
1. Acessar a página https://intranet.msquareglobal.com.br/
2. Logar no Perfil da Intranet com login e senha pessoal;
3. Na sessão "Arquivos" > "Manuais (IT)



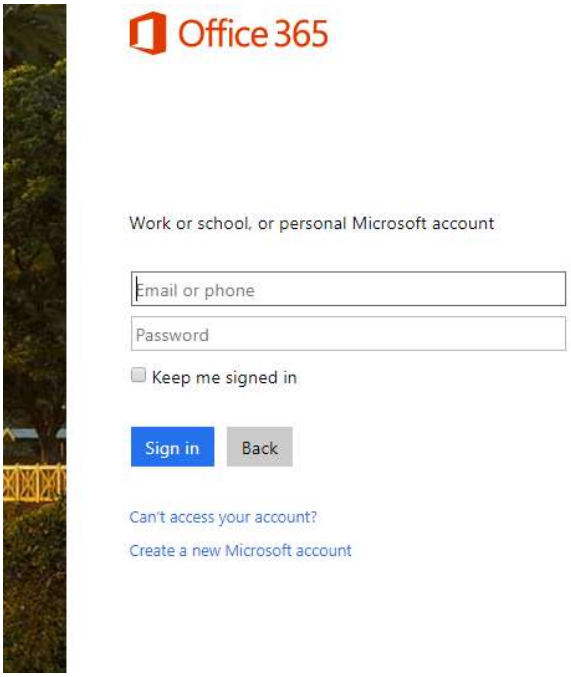
4. Clique no Link "VPN"



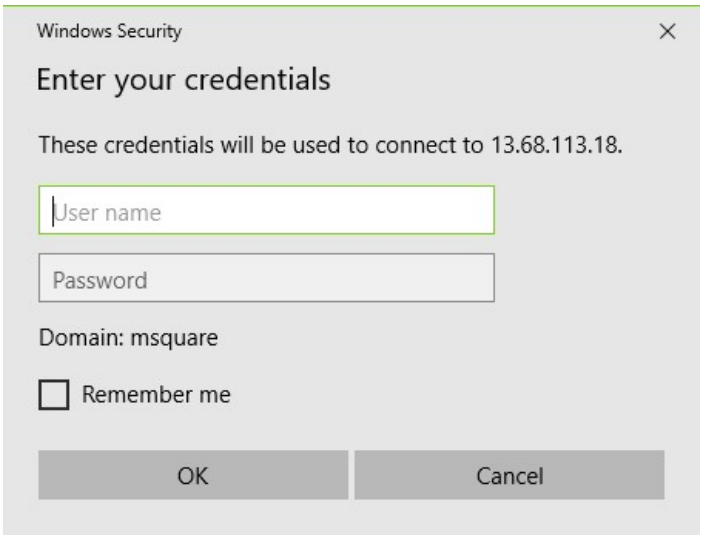
5. Extraia os 3 arquivos:



6. Será solicitado o login e senha de acesso ao Office365

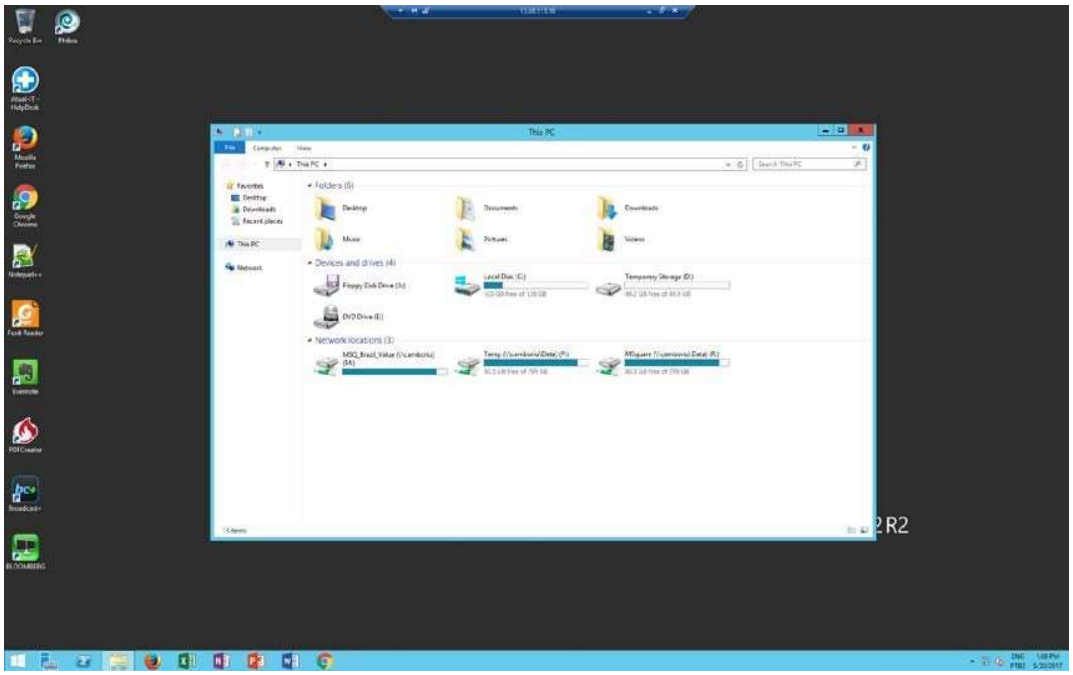


7. Execute o arquivo quando finalizar o download.
8. Será solicitado a credencial para acesso ao TERMINAL SERVICE



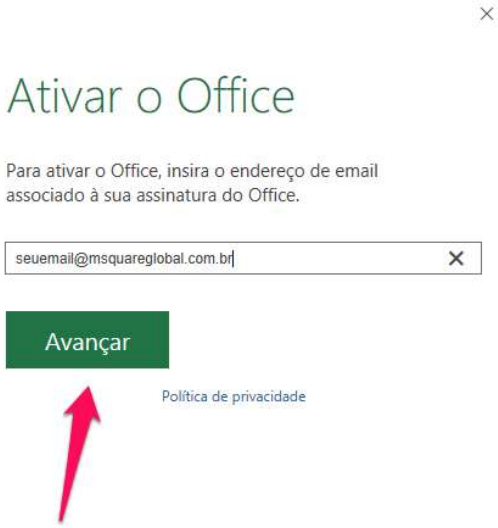
9. Digite o seu usuário e senha de acesso (o mesmo utilizado para acessar os desktops físicos)
10. Você receberá um aviso sobre a identidade do computador remoto. Marque a opção "Don´t ask me again..." e clique em "Yes"

11. Após finalizada a etapa de login você terá acesso ao TERMINAL SERVICE com os aplicativos e sistemas instalados e atualizados.

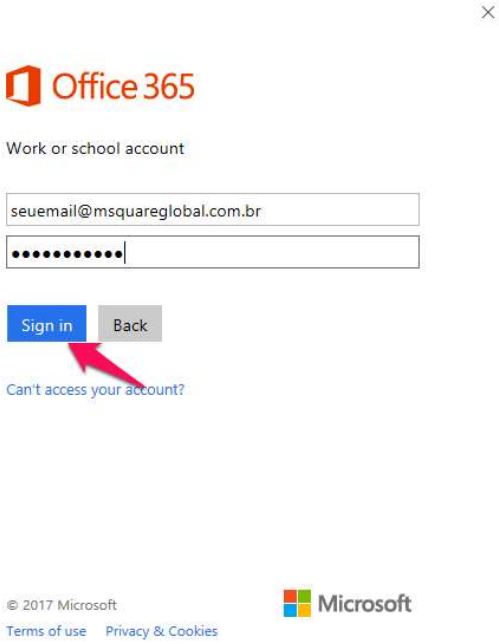


12. Para utilizar o pacote office no ambiente de DR será necessário ativar.

13. Ao clicar a primeira vez sobre o qualquer produto do office aparecerá a tela abaixo. Digite seu e-mail e clique em "Avançar"



14. Na próxima tela será solicitado a senha do seu e-mail. Digite-a e clique em "Sign in" Após isso todos os produtos do office estarão ativados.



Observações

1. Transferência de arquivos entre estação cliente / terminal service foi desabilitada por segurança da informação
2. Sugerimos ao usuário a utilização do WEBMAIL como alternativa ao Microsoft Outlook durante o DR
3. Para acesso ao webmail entrar no site http://portal.office.com
4. A quantidade de usuários conectados simultaneamente no terminal service está vinculado ao limite de licenças disponíveis. Caso você receba a mensagem que não há licença disponível tente novamente mais tarde