PLANOS

CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

Resumo

Foco para Companhia Securitizadora ou Consultoria de Crédito.

victorrodrigo@girubank.com.br

Versão	Data	Editor	Descrição da Alteração
1.0	28/11/2023	GIRUBANK Securitizadora S.A.	Versão Inicial
2.0	30/11/2023	GIRUBANK Securitizadora S.A.	Modificações no procedimento de exclusão de acesso
3.0	04/12/2023	GIRUBANK Securitizadora S.A.	Modificações no procedimento de exclusão de acesso e glossário
4.0	04/12/2023	GIRUBANK Securitizadora S.A.	Alteração na descrição do item Abrangência.
5.0	18/12/2023	GIRUBANK Securitizadora S.A.	Inclusão das solicitações no fluxo.
6.0	18/12/2023	GIRUBANK Securitizadora S.A.	Alteração no processo operacional.
7.0	08/01/2024	GIRUBANK Securitizadora S.A.	Alteração no processo de envio.
8.0	08/01/2024	GIRUBANK Securitizadora S.A.	Revisão do procedimento, dos fluxos e ajustes no processo. Alteração no Documento nº. 3 (Anexo)
9.0	22/01/2024	GIRUBANK Securitizadora S.A.	Revisão do procedimento, dos fluxos e ajustes no processo de exclusão de usuários para atender ao novo fluxo do sistema de RH.
10.0	05/02/2024	GIRUBANK Securitizadora S.A.	Revisão do procedimento e ajuste no processo.
11.0	19/02/2024	GIRUBANK Securitizadora S.A.	Modificar o processo de inclusão na rede e no notes para incluir o Aceite Eletrônico

Aprovação do Documento	
Aprovado por:	Victor Rodrigo de Lima
Assinado por:	Victor Rodrigo de Lima

Sumário

Esboço

1.1. Introdução

Este documento apresenta a estrutura das aplicações e equipamentos para orientar os procedimentos de contingência da **GIRUBANK Securitizadora S.A**.

1.2. Objetivos

Os principais objetivos deste plano são:

- ✓ Detalhar as atividades dos grupos funcionais e suas atividades;
- ✓ Apresentar os recursos mínimos necessários para contingência;
- ✓ Apresentar os procedimentos de contingência.

1.3. Abrangência

Este documento abrange todas as unidades da **GIRUBANK**.

1.4. Leitor Alvo

Este documento abrange todos os funcionários, colaboradores e prestadores de serviços da **GIRUBANK** que estejam, direta ou indiretamente, envolvidos no processo de continuidade dos processos vitais da companhia.

Apresentação

O **Plano de Contingência** visa assegurar, no tempo máximo estabelecido, o restabelecimento dos serviços de processamento de dados que suportam os processos e sistemas vitais da empresa, minimizando perdas e garantindo a continuidade dos seus negócios, quando da ocorrência de um evento que impossibilite a utilização do ambiente produtivo de TI, por um período que cause impacto aos negócios.

Neste documento constam as orientações para assegurar a existência dos dados e recursos necessários, bem como os procedimentos que orientam o processo de restauração e disponibilização dos serviços de processamento de dados em um local alternativo, “Backup Site”.

Nesse contexto, o “Backup Site” pode ser mantido tal como a configuração usual, uma vez que é suportado em contrato (sugerir extensão do modelo proposto).

Considerando a extrema importância do plano, é fundamental que seu conteúdo seja revisado, atualizado, e testado periodicamente, garantindo integridade, eficiência e a correta utilização quando da sua necessidade.

Grupos Funcionais

As atividades para a execução do Plano de Contingência estão distribuídas pelos Grupos Funcionais, de acordo com atribuições e responsabilidades específicas.

Segue a descrição das atividades e responsabilidades para cada Grupo Funcional, em relação ao: antes, durante e depois do acionamento do Plano de Contingência.

2. Grupo de Administração do Plano

2.1. Responsabilidades:

- ✓ Garantir a operacionalização e exequibilidade do Plano, assegurando a preparação dos recursos e a disponibilidade de serviços administrativos e de comunicações necessários para a operação de emergência;
- ✓ Ativar a execução do plano em situação de contingência;
- ✓ Coordenar o comando da operação de emergência;
- ✓ Supervisionar as ações dos demais grupos;
- ✓ Solucionar conflitos;
- ✓ Atuar como elo entre o Grupo Executivo e demais grupos, no tocante ao Plano de Contingência.

2.2. Atividades antes da operação de contingência:

a. Definir reuniões periódicas para coordenar testes de mesa[1], antes dos testes no "Backup Site", visando à análise do Plano como um todo e proceder aos ajustes necessários.
b. Manter e atualizar cadastro (localização, número de telefone, nome etc.) dos participantes dos Grupos Funcionais e dos principais usuários.
c. Manter e atualizar cadastro de fornecedores e atualizar dados cadastrais de acordos / contratos para serviços gerais, para equipamentos de comunicação e para recursos humanos terceirizados.
d. Elaborar relatórios dos testes e das operacionalizações do Plano e das propostas dos ajustes que venham a ser necessários.
e. Manter atualizados todos os membros do grupo através de reuniões periódicas.

2.3. Atividades no retorno da operação de contingência:

a. Orientar a desativação das operações no "Backup Site" e o início da transferência do processamento para a instalação definitiva (ambiente TI de origem ou reconstruído).
b. Providenciar transporte para pessoas, equipamentos e suprimentos, bem como promover desativação, devolução e pagamentos dos recursos adicionais utilizados durante a operação de emergência.
c. Manter informados os demais Grupos sobre a desativação da contingência.
d. Avaliar ações de retorno, com base no protocolo de ocorrências e corrigir falhas atualizando este Plano de Contingência.

[1] Teste de mesa é uma **simulação da execução de um programa ou de uma operação** de forma manual, geralmente feita no papel. Não há regras rígidas para criar um teste de mesa, geralmente é feito de duas formas. Uma sem as rotinas informatizadas, seguindo as normas e procedimentos sem ferramentas tecnológicas e sem projeção de resultados, a outra segue o mesmo modelo, porém "define" o resultado esperado.

3. Grupo de Servidores

3.1. Responsabilidades:

- ✓ Garantir que esteja adequada e preparada a configuração de “hardware” e “software” necessária para a continuidade da operação nos serviços de informática no “Backup Site”;
- ✓ Assegurar a continuidade dos serviços de processamento das aplicações.

3.2. Atividades antes da operação de contingência:

a. Manter controle do ambiente/configuração de “hardware” e de “software” da instalação necessária para o processamento e definir as alternativas operacionais de recursos computacionais junto ao “Backup Site” para uso em contingência (grandes emergências), e na própria instalação de produção para emergências gerais.
b. Elaborar e manter processos de “Backup” de contingência para o ambiente de “software” e de dados da instalação.
c. Documentar e manter atualizadas as informações e os procedimentos relativos ao “hardware” e “software”.
d. Manter mapeamento de alocações e distribuição de arquivos considerando a disponibilidade dos recursos para “hardware e software” do “Backup Site”.
e. Manter atualizadas as configurações de “hardware” e “software” na instalação “Backup Site” sempre que versões de “softwares” ou equipamentos forem incorporadas ou alteradas no ambiente de produção.
f. Assegurar a disponibilidade dos manuais técnicos, bem como das autorizações de “*passwords*” para “softwares” com verificação de “*Serial Number* da CPU”, para uso no “Backup Site”.
g. Planejar e preparar rotinas para verificação contínua e teste do funcionamento dos recursos de “hardware” e “software” instalados no “Backup Site”.
h. Manter permanentemente atualizadas as informações e os procedimentos operacionais estabelecidos no Plano de Contingência e relacionadas à restauração / reativação para o retorno do ambiente operacional.
i. Executar o Plano de Testes de recuperação para “Backup Site” em conjunto com os demais Grupos, protocolando os passos, corrigindo falhas, atualizando documentação e informando as alterações realizadas ao Grupo de Administração do Plano.

3.3. Atividades no retorno da operação de contingência:

a. Assegurar a atualização ou carga (identificada como necessária) de dados provenientes do “Backup Site”, quando do retorno para a instalação original ou reconstruída, em conformidade aos procedimentos estabelecidos no Procedimento Operacional de Retorno.
b. Liberar as atividades para a continuidade dos trabalhos.
c. Avaliar o funcionamento durante a operação de retorno.
d. Elaborar relatório de avaliação, com base no protocolo de ocorrências, identificando distorções, e estabelecendo ações para correções de falhas e atualização dos procedimentos do Plano de Contingência.

4. Grupo de Telecom

4.1. Responsabilidades:

✓ Garantir que esteja adequada e preparada a configuração de “hardware” e “software”, bem como os recursos da Rede de Comunicação de Dados, necessários para continuidade da operação e dos serviços de informática no “Backup Site”, para assegurar a continuidade dos serviços de processamento a partir daquele local.

4.2. Atividades antes da operação de contingência:

a. Manter controle do ambiente/configuração de “hardware” e “software” da rede e definir as alternativas operacionais de recursos computacionais para uso no “Backup Site” em contingência (grandes emergências), e na própria instalação para emergências menores.
b. Elaborar e manter a documentação e processos de “backup” da configuração da rede (endereçamento IP, rotas e roteadores, DNS, switches etc.) do ambiente de produção e do ambiente no “Backup Site”.
c. Assegurar a disponibilidade das mídias de instalação e dos manuais técnicos, para uso no “Backup Site”.
d. Planejar e preparar rotinas para verificação contínua e teste do funcionamento dos recursos “hardware” e “software” da rede instalados no “Backup Site”.
e. Preparar rotinas que forem necessárias para o ambiente produtivo da rede no “Backup Site”.
f. Manter atualizadas as configurações de “hardware” e “software” da rede no “Backup Site” sempre que versões de “softwares” ou equipamentos forem incorporadas ou alteradas no ambiente de produção.
g. Manter atualizadas as informações e os procedimentos estabelecidos no Plano de Contingência relacionados ao “hardware” e “software” da rede de comunicação de dados e à reativação do ambiente.
h. Executar o Plano de Testes de recuperação para “Backup Site” em conjunto com os demais Grupos, protocolando os passos, corrigindo falhas, atualizando documentação e informando as alterações realizadas ao Grupo de Administração do Plano.

4.3. Atividades no retorno da operação de contingência:

a. Assegurar a operacionalização do retorno para o ambiente original ou reconstruído, em conformidade aos procedimentos estabelecidos no Procedimento Operacional de Retorno, e eventuais procedimentos especiais que forem necessários para o retorno à normalidade.
b. Elaborar relatório de avaliação, com base no protocolo de ocorrências, identificando distorções, e estabelecendo ações para correções de falhas e atualização dos procedimentos do Plano de Contingência.

5. Grupo de Sistemas

5.1. Responsabilidades:

✓ Garantir que as aplicações do ambiente sejam recuperadas sem perda dos dados vitais;
✓ Continuidade do processamento das aplicações.

5.2. Atividades antes da operação de contingência:

a. Manter-se informado do ambiente e da configuração do “Backup Site”.
b. Definir os requisitos mínimos para processamento das aplicações críticas e alternativas para processamento das aplicações em caso de contingência.
c. Orientar para que no desenvolvimento de aplicações sejam consideradas adequações que viabilizem ou facilitem a utilização dos recursos de “hardware” e “software” no ambiente do “Backup Site”.
d. Manter atualizada a política de retenção dos arquivos básicos para recuperação integral dos sistemas de aplicações, considerando os aspectos legais e funcionais que regem o assunto.
e. Planejar, definir, testar e assegurar a existência dos “backups” necessários junto ao Suporte Técnico.
f. Planejar, identificar, definir e testar procedimentos que sejam necessários em função da contingência ou das características do “Backup Site”. (Exemplo: processamento modificado; inicialização, reinicialização e sincronização de arquivos; retorno ao ambiente de TI original; etc.).
g. Identificar e definir instruções específicas para produção e para usuários, com relação ao uso das aplicações na ocorrência de contingência, caso seja diferente do normal.
h. Identificar e estabelecer procedimentos alternativos ou de controle para processos que foram disponibilizados para execução e controle direto por usuários, e que possam interferir na obtenção de resultados corretos das aplicações quando em contingência.
i. Participar no planejamento e execução de testes de recuperação no “Backup Site”.

5.3. Atividades durante a operação de contingência:

✓ Prover suporte à produção para a retomada e continuidade do processamento dos aplicativos.
✓ Realizar as correções e adequações nos programas e rotinas que forem necessárias.

5.4. Atividades no retorno da operação de contingência:

a. Acompanhar e fornecer suporte no retorno à normalidade, bem como para a execução de procedimentos especiais que forem necessários.
b. Elaborar relatório de avaliação, com base no protocolo de ocorrências, identificando distorções, e estabelecendo ações para correções de falhas e atualização dos procedimentos do Plano de Contingência.

Alternativas de Processamento

A **GIRUBANK** utiliza cloud server. A empresa Finanblue que fornece o sistema LiveWork utiliza os serviços da empresa Amazon Web Services (AWS), que é uma plataforma de computação em nuvem bastante abrangente, desenvolvida e fornecida pela gigante mundial Amazon.

Recursos Necessários - Contingência

A **GIRUBANK** utiliza um sistema específico e operacional de Gestão de Recebíveis Cadastro e Motor de Crédito, para a gestão dos recebíveis adquiridos, juntamente com os sistemas de informação de crédito da SERASA. Está em processo de contratação de plataforma de BIG DATA integrada a inteligência artificial – IA, para auxílio no processamento da operação.

Quando ocorre a ativação do Plano de Contingência há a necessidade de recorrer a diversos recursos para minimizar os efeitos da contingência, esses dependem dos dados que deverão ser recuperados e a definição dos recursos que serão disponibilizados nessa fase.

6. Recursos

6.1. Hardware:

A configuração de hardware apresentada para cada servidor é a mínima aceitável para retorno do sistema em termos de contingência, a solução definida para a contingência das aplicações no ambiente atual será o compartilhamento de um servidor por mais de um processo.

Nem todos os equipamentos utilizados comumente nas operações precisam ser consignados como referência para contingenciamento, somente os críticos. Este plano define a criticidade, a necessidade e a configuração de cada servidor e/ou equipamento necessário para pronto atendimento na contingência de TI.

Para recuperação dos servidores a configuração de hardware mínima que deverá ser disponibilizada será (configuração válida para todas as unidades):

a. Desktops:

✓ Equipamento com as seguintes características mínimas: processador AMD Ryzen 3 ou superior (ou equivalente), memória /RAM de 8gb, unidade de armazenamento com 120 GB tipo SSD, Windows 10 PRO.

b. Servidores:

✓ Servidor de aplicação e web: processador Xeon, memória RAM de no mínimo 14 Gb, unidade de armazenamento de 500 GB tipo SSD.

✓ Servidor banco de dados: processador Xeon, memória RAM de no mínimo 14 Gb, unidade de armazenamento com no mínimo 500 GB tipo SSD

6.2. Software:

Os recursos de software são os correspondentes aos que existem instalados nos servidores da **GIRUBANK**. Para recuperação deverão ser instalados conforme o licenciamento do fabricante. Além disso deverá ser disponibilizada uma licença do software para gerenciamento de mais de uma aplicação no servidor de contingência.

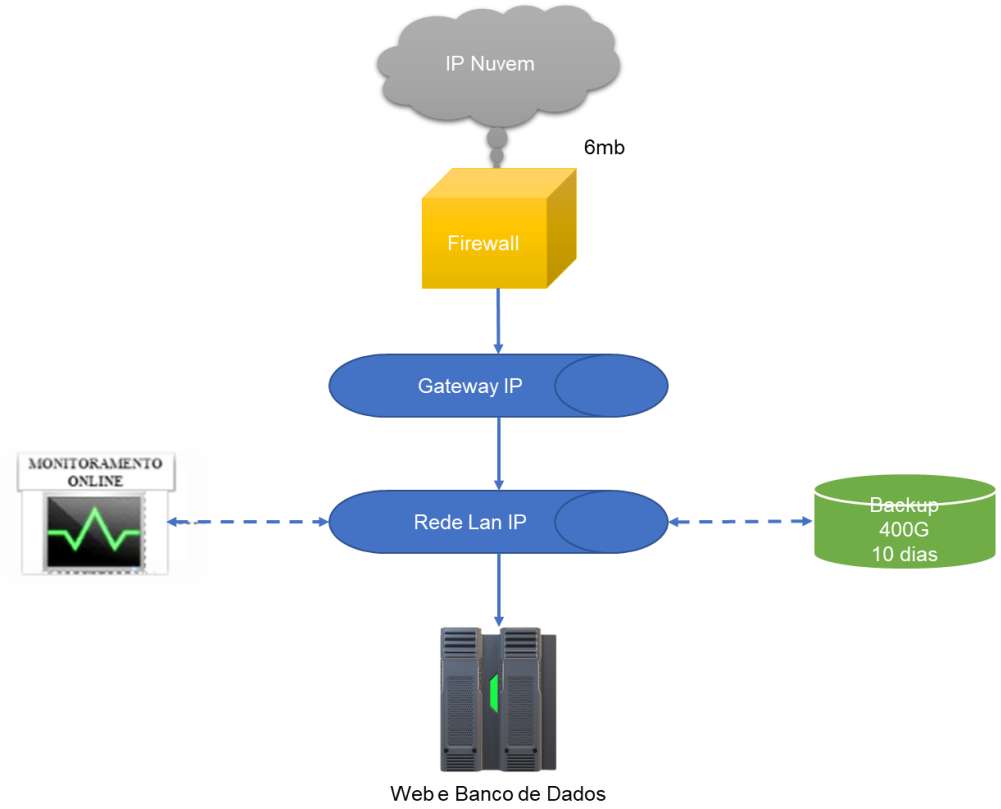
Para recuperação dos serviços a configuração de softwares que deverá ser disponibilizada deve conter:

- ✓ Windows Server 2019 Standard – servidores;
- ✓ Active Directory instalado e ativado – servidores;
- ✓ SQL Server Standard para o banco de dados (sistema) – servidores;
- ✓ Antivírus Kaspersky Total Security – servidores e estações de trabalho;
- ✓ Firewall ou versão equivalente – servidores;
- ✓ Browser para acesso à internet – servidores e estações de trabalho;
- ✓ Versão do Office – estações de trabalho.

6.3. Comunicação de Dados:

Os recursos de comunicação de dados **GIRUBANK** que estão implantados atendem as seguintes localidades (veja diagrama abaixo)

Hospedagem de servidores:



6.4. Postos de trabalho:

Os postos de trabalho devem ser definidos pelo Diretor de Operações e GRC, sendo o mínimo necessário para a continuidade dos negócios da **GIRUBANK**.

Deverá ser definido projeto para implantação das contingências nas localidades e transferência das atividades diárias para localidades alternativas, conforme exemplo abaixo:

a. Localidade A;
b. Localidade B; e etc.

6.5. Configuração padrão para workstation de usuários:

Configuração padrão da **GIRUBANK**:

✓ Processador AMD Ryzen 3 ou superior (ou equivalente), memória /RAM de 8gb, unidade de armazenamento com 120 Gb tipo SSD, Windows 10 PRO, placa de rede 10/100, sem unidade de CD, sem multimídia, sem floppy, monitor 15 “.

Estratégia de Backup

Para viabilizar o processo de restauração definido no plano de contingência, o processo de cópias de segurança (backup) deve ser estruturado de acordo com o seguinte processo:

a. Realizar cópia do banco do servidor MODELO-BD01.
b. Enviar cópia de segurança para pasta da nuvem (confirmar local de cópia).
c. Testar periodicamente as cópias geradas.

7. Listagens, documentos e mídias:

a. Cópia do banco de dados do servidor MODELO-BD01 (com identificação sequencial de data do backup) deverá ser mantida em pasta segregada com duas cópias, sendo uma em máquina local a ser designada por norma interna e outra em nuvem.
b. Envelope lacrado contendo as user id/senhas de acesso especial autorizado (logins de usuários suporte do Administrador do Sistema, Administrador do SGBD, Administrador da rede e configuração de roteadores) e Senhas de Boot de servidores. O envelope deverá ser trocado a cada alteração de senhas que ocorrer no ambiente dos servidores. Periodicamente deve ser efetuada verificação do lacre.
c. Cópia de documentação de controle de direitos de acesso de usuários e grupos, deverá ser mantida no “Backup Site”.
d. Cópia das mídias de instalação e dos documentos de configuração dos softwares utilizados nos servidores. As cópias deverão ser mantidas no diretório e replicadas no servidor de contingência.
e. Cópia das documentações da configuração da rede (LAN, WAN, ROUTERS) e arquivos de senhas dos roteadores, gravada em pen drive e armazenada no “Backup Site”.
f. Cópia dos manuais dos sistemas e aplicativos instalados nos servidores e das instruções para instalação e configuração no ambiente (Server e Client).
g. Enquanto não houver definição / contratação do serviço de “Backup Site” todos os documentos e cópias serão guardados com o Diretor de Operações e GRC da MODELO em ambiente definido por ele.

NOTA: todas os documentos referenciados devem ser mantidos atualizados e em cofre externo, bem como sempre que ocorrerem alterações no ambiente produtivo.

Arquivo de Segurança

As mídias de dados e respectiva listagem de controle, necessários ao plano de contingência são armazenadas no “Backup Site”. As cópias das demais informações e documentos do ambiente dos servidores, bem como dos roteadores da **GIRUBANK**, também deverão ser mantidos armazenados no Backup Site.

Enquanto não houver definição / contratação do serviço de “Backup Site” todos os documentos e mídias de cópia de segurança (backup) serão armazenados de acordo com os contratos vigentes com os prestadores de serviços de tecnologia da informação e comunicação sob responsabilidade do Diretor de Operações e GRC.

Testes

A habilidade para recuperação, após a ocorrência de uma contingência, em tempo compatível com as necessidades da **GIRUBANK**, constitui um dos fatores determinantes para a continuidade dos negócios. Fatores que contribuem para a obtenção da necessária habilidade para a recuperação são:

a. O treinamento das pessoas envolvidas no processo; e
b. A consistência e a integridade dos Procedimentos Operacionais do Plano de Contingência.

Portanto, é essencial que, além de manter o Plano de Contingência constantemente revisado e atualizado, também sejam realizadas sessões de teste do funcionamento do “Backup Site” (interno e externo quando for definida sua contratação), a cada doze meses.

Durante a sessão de teste, devem ser registrados os problemas ou dificuldades encontradas, para que após a realização da reunião de avaliação, sejam providenciadas as devidas correções e/ou adequações que visem acrescentar melhorias para a utilização do Plano de Contingência.

É importante salientar que a sessão de teste permite a verificação não apenas dos procedimentos operacionais de recuperação contidos no Plano de Contingência, como também se os procedimentos determinados para serem executados em tempos normais (anteriores à ocorrência de uma contingência), no dia a dia, estão sendo executados, e são consistentes com as necessidades. Exemplos de procedimentos que devem ser executados no dia a dia:

- ✓ A atualização das documentações de configuração dos softwares e da rede; a realização dos backups na forma e na periodicidade estabelecida;
- ✓ O controle dos recursos necessários no “Backup Site” em função de atualizações no ambiente de produção;
- ✓ A atualização dos procedimentos de recuperação em função de alterações ou novas implantações de sistemas.

O exercício de teste permite também tornar o Plano de Contingência um documento vivo, já que será frequentemente avaliado. No tópico “Preparação para Teste de Contingência”, abaixo, encontram-se um conjunto de procedimentos que orientam os preparativos para execução do teste prático de contingência no “Backup Site”.

Além da sessão de teste de contingência no “Backup Site”, deverão ser realizados testes contínuos de verificação de funcionamento dos equipamentos e dos respectivos “softwares” destinados a serem utilizados durante a contingência.

Estes testes permitirão assegurar que o ambiente de “backup” está pronto para utilização a qualquer momento que for exigido. Adicionalmente, devem ser conduzidas sessões de teste de “mesa” (teste teórico dos procedimentos operacionais do Plano de Contingência, sem utilização prática do “Backup Site”).

Para este tipo de teste, os participantes dos Grupos Funcionais de contingência deverão ser convocados e alocados em uma sala de reunião, onde deverão executar o ensaio das ações que cada um deverá executar no caso de uma emergência, em conformidade ao descrito nos procedimentos operacionais.

A sequência de atividades abaixo define em linhas gerais o roteiro de testes.

Atividade: 1 - Programar os testes do Plano
Grupo: ADMINISTRAÇÃO DO PLANO
Responsável: Administrador do Plano

Procedimento:

a. Anualmente, programar as datas para a realização dos testes anuais ou em conformidade com necessidades especiais da **GIRUBANK**.
b. Divulgar aos líderes dos Grupos de Contingência, as datas programadas para os testes, para que possa estabelecer com antecedência adequada os preparativos necessários.

Atividade: 2 - Preparar plano de teste
Grupo: ADMINISTRAÇÃO DO PLANO
Responsável: Administrador do Plano
Dependências: 1 Programar os testes do Plano

Procedimento:

a. Com pelo menos 01 (um) mês de antecedência às datas programadas, deverão ser executados os procedimentos.
b. Convocar reunião com os líderes de grupos de contingência para preparar o plano de testes, considerando:
    i. Tipo de teste planejado sem comunicação externa, apenas restauração dos servidores, ou com comunicação externa (filiais e /ou terceiros);
    ii. Quais sistemas e rotinas serão testados;
    iii. A participação ou envolvimento de usuários e/ou terceiros para realização de testes de aplicativos;
    iv. A necessidade de preparação de “backups” especiais para testes que envolvam repetição de processamentos de rotinas no “Backup Site” (por exemplo: salva de movimentos, salvas de bancos de dados, salvas de logs etc.);

v. A necessidade de executar, em momento imediatamente anterior ao início do teste, "backups full" de segurança da configuração de roteadores e dos servidores da localidade que será utilizada como “Backup Site” (estes backups deverão ser utilizados para retornar as configurações e dados à situação normal de produção, desfazendo assim as alterações executadas durante o teste de contingência);
vi. Verificar a necessidade de que durante o teste não ocorra utilização produtiva do ambiente que será utilizado como “Backup Site” (os usuários da localidade não deverão utilizar produtivamente o ambiente durante o teste de contingência);
vii. A necessidade de configuração da rede de TP para conexão com as localidades / terceiras;
viii. O tempo previsto de duração dos testes;
ix. A alocação de pessoal dos grupos de contingência no “Backup Site”;
x. Os materiais adicionais necessários (pen drive, formulários, equipamentos etc.);
xi. Os tipos de evidências de realização do teste a serem coletadas (exemplo: cópias de arquivos, cópias de logs, cópias de telas etc.);
xii. A necessidade de suporte técnico dos fornecedores durante os testes.

c. Caso os testes envolvam conexões de TP, verificar:
    i. A existência e a adequação dos recursos físicos necessários no “Backup Site” e nas localidades / instituições abrangidas pelo teste (links, routers);
    ii. Recursos de pessoal para o plantão nas localidades / terceiros;
    iii. A necessidade de envolvimento ou de informações dos fornecedores de Telecom, para redirecionamento e/ou configuração de comunicação ao “Backup Site”;
    iv. Notificar o pessoal necessário, informática e usuários para a execução dos testes, indicando as respectivas atividades a serem previamente preparadas, e incluir também o cronograma de datas, horários previstos e locais para sua realização.

Atividade: 3 - Execução dos testes
Grupo: ADMINISTRAÇÃO DO PLANO
Responsável: Administrador do Plano

Procedimento:

a. O Grupo de Administração do Plano convoca, pelos meios disponíveis, os membros dos demais Grupos Funcionais para comparecerem com a documentação do Plano de Contingência ao local do Posto de Comando.
b. Verifica em conjunto com os líderes dos Grupos Funcionais para a Contingência, a disponibilidade de técnicos, estabelece com os mesmos a escala de pessoal para execução dos trabalhos e informa as instalações que serão utilizadas como “Backup Site”.
c. Havendo falta de recursos de pessoal, verificar a possibilidade de suprir as necessidades, realocando funções para o atendimento emergencial e/ou contatar fornecedores de serviços e providenciar recursos de acordo com o perfil técnico necessário.