Política de Continuidade de Negócios - PCN

A Política de Continuidade de Negócios têm como objetivo principal a formalização de ações a serem tomadas para que, em momentos de crise, a recuperação, a continuidade e a retomada possam ser efetivas, evitando que os processos críticos de negócio da organização sejam afetados, o que pode acarretar em perdas financeiras.

No que diz respeito à necessidade de atualizações, o Plano de Continuidade de Negócios deve ser revisado semestralmente, pois mudanças significativas em componentes, atividades ou processos críticos de negócio podem fazer com que novas estratégias e planos de ação sejam previstos, evitando assim com que eventuais desastres desestabilizem profundamente o andamento regular do negócio da empresa.

O Plano de Continuidade de Negócios é constituído pelos seguintes planos:

I. Plano de Contingência:

A DOJO CAPITAL tem implementado o seu plano de Contingências que projeta ex-ante os potenciais riscos do negócio, e contingências, por exemplo, crises econômicas, falhas operacionais, falhas de sistemas próprios e de prestadores de serviço e /ou desastres naturais, as quais possam acarretar a interrupção do negócio.

Os colaboradores são treinados e conhecem os procedimentos de backup e salvaguarda de informações (confidenciais ou não), planos de evacuação das instalações físicas e melhores práticas de saúde e segurança no ambiente de trabalho reduzindo os principais pontos de vulnerabilidade de suas instalações e equipamentos.

Assim, pode ser definido, por exemplo, que o Grupo Executivo:

- Antes do incidente – determine o que deve ser atendido prioritariamente

  Determinar o formato da comunicação (notas de imprensa, carta, reuniões com representantes ou conferência de imprensa etc.), elaborar lista de contatos para comunicação em situação de emergência, estabelecer mecanismo de monitoração imediata em todos os meios para comprovar o alcance da crise, determinar a sequência e a coerência da comunicação (ou seja, quem liga para quem, e quem retorna informando que todos os colaboradores estão cientes da situação e dos próximos passos numa situação de contingência).

- Durante a contingência – manutenção da informação e supervisionamento de ações de contingência.

Evitar que sejam dadas declarações públicas ou internas sem preparo prévio das intervenções, registrar o contato de todos os membros dos Grupos de Comunicação/Apoio e de Administração de Crise (nome completo, cargo na companhia, endereço eletrônico – da entidade e outro que possa acessar desde uma conexão remota –, números de telefones da empresa, da residência e dos celulares), manter banco de dados de contatos com todos os interessados/afetados pela crise (bombeiros, polícia, políticos, sindicatos, fornecedores, participantes, meios de comunicação, associações civis etc.). Com relação ao sistema de telecomunicação, a entidade deve monitorar diariamente o tráfego telefônico e performance da rede, realizar análises e oferecer alternativas para solução de contingência como, por exemplo, redirecionar as ligações para um número alternativo.

- Depois da contingência – declare o encerramento da situação de contingência e o retorno operacional.

  Propor o plano de ação para a revisão ou reforço, se necessário, da imagem corporativa que contemple a todos os públicos, bem como identificar o que não aconteceu conforme planejado.

II. Plano de Administração de Crises (PAC):

Conjunto de cenários de crises previamente definidos e de respectivos procedimentos de gestão para administrar, neutralizar ou eliminar impactos até a superação da crise.

O GAC (Grupo de Administração de Crises) avaliará a situação apresentada e caso considere que todas as medidas de recuperação já foram tomadas e que houve a evolução para um cenário de crise, contemplado ou não no PCN, proporá a declaração da situação de crise ao Grupo Executivo.

Os colaboradores do Grupo Operacional têm atribuições voltadas para o apoio administrativo e à infraestrutura física e de tecnologia. No que diz respeito ao tratamento da tecnologia de informação durante a contingência, por exemplo, tão importante quanto conhecer os riscos a que o site está exposto, está a velocidade em que ele pode ser ativado. Sites próximos à sede geralmente tem um tempo de ativação relativamente rápido, quando bem estruturados, no entanto podem estar expostos aos mesmos riscos do site principal.

III. Plano de Recuperação de Desastres (PRD):

Desastre pode ser entendido como qualquer situação que afete os processos críticos do negócio de uma organização. Consequentemente, algumas ocorrências podem ser caracterizadas como sendo desastres para uma determinada empresa, mas podem não ser caracterizadas como um desastre para outra empresa. São descritas da seguinte forma:

- Treino da equipe de forma a responder de maneira eficaz a um incidente ou interrupção; adiantamento de resultado previsto, ou seja, que tenha sido antecipadamente planejado e incluído no escopo;

- Possibilitar à entidade desenvolver ações inovadoras;
- Verificação de que todas as atividades críticas da organização, suas dependências e prioridades estejam contempladas pelo PCN;
- Geração de confiança nos colaboradores envolvidos nos testes;
- Aumento da consciência do processo de continuidade de negócios pela organização por meio da publicação dos testes;
- Demonstração da competência das equipes titulares de resposta a incidentes e de seus substitutos.

IV. Plano de Continuidade Operacional (PCO).

O processo de retorno à normalidade começa durante a execução do próprio PCN, quando tiverem sido adotadas as estratégias de resposta. Após o retorno, deverão ser produzidos relatórios com informações sobre o evento, os custos incorridos, recursos utilizados, tempos de recuperação etc. Ainda que o objetivo geral de recuperação seja o retorno à normalidade o mais rápido possível, em alguns casos ou incidentes os planos de recuperação desenvolvidos pelas empresas não podem ser utilizados imediatamente.

Após os testes, do processo anterior, os usuários deverão experimentar o cenário de normalidade com tarefas inerentes a rotina sem qualquer inconsistência ou variável externa. Abaixo detalhamos algumas contingências pontuais que a gestora está preparada para enfrentar:

1. CONTINGÊNCIA ELÉTRICA

Com o objetivo de evitar uma queda da rede elétrica teremos instalados em nossa estrutura três No-Breaks conectados da seguinte forma:

No-Break 1: Servidores e servidor de internet;

No-Break 2: Máquinas dos traders e gestor;

No-Break 3: Sistemas de Back Office e Risco.

Esses No-breaks terão uma duração de 15 minutos. A capacidade desses No-Breaks será testada todas as segundas-feiras antes da abertura dos mercados.

Caso a rede elétrica não se restabeleça em 10 minutos será iniciado o processo de migração do funcionamento para o servidor espelho que fica alocado no escritório da DOJO CAPITAL também no Rio de Janeiro.

Esse processo de migração levará 2 minutos e no terceiro minuto os sistemas de gestão já estarão funcionando na nova estrutura.

2. CONTINGÊNCIA DE INTERNET

Operamos com duas internets sendo uma principal e a segunda trabalhando como back-up. Ambas possuem a mesma capacidade de banda.

Caso as duas deixem de operar, automaticamente passamos a operação para o outro escritório no Rio de Janeiro.

3. CONTIGÊNCIA DE SERVIDORES

Para suportar nossas operações possuímos um sistema gerencial proprietário.

Seu funcionamento depende das posições do dia anterior no fechamento e das operações realizados ao longo do dia.

Diariamente à noite, as posições de encerramento serrão exportadas em caso de ocorrência de falhas na internet.

Uma desconexão (intermitência) gera uma mensagem atentado a descontinuidade do sistema. Nesse caso, o servidor no Rio de Janeiro se conecta e importa automaticamente via porta 500 das corretoras às operações realizadas ao longo do dia.

Com as operações importadas em poucos minutos o funcionamento do sistema é restabelecido.

4. CONTINGÊNCIA DE LOCAL

No caso de um acidente natural (incêndio, tempestade, terremoto, etc.) temos o escritório supramencionado, que possui back-ups atualizados do sistema bem como das informações a serem utilizadas.

Nesse caso, o tempo de restabelecimento das operações é o tempo necessário somente para iniciar o sistema em posição de back-up.

A equipe anteriormente mencionada que faz parte do plano de Continuidade Operacional, exercerão papel fundamental na plena coordenação do fluxo de readaptação sistêmica operacional.