ARTIGO #02 - FEV/2018 - TOP TIER INFRASTRUCTURE

PREPARAÇÃO E RESPOSTAS A EMERGÊNCIAS EM DATA CENTERS

Os Data Centers e demais Ambientes de Missão Crítica são idealizados para operar em regime 7x24, mas independentemente de quão bom sejam o projeto e os recursos implantados de infraestrutura, é impossível eliminar todos os riscos de interrupção inesperada do sistema. Estar adequadamente preparado para agir de forma eficaz e efetiva em caso de qualquer incidente é fundamental para manutenção da disponibilidade e minimizar ou evitar qualquer impacto na organização. Esta preparação demanda um conjunto de processos para antecipar, prevenir e atenuar os efeitos da ocorrência de incidentes e eventos de emergência.

Neste artigo abordamos os principais elementos que compõem essa importante disciplina na maturidade da operação e manutenção de facilites de Data Centers.

EOP (Emergency Operating Procedures) – Para garantir que as respostas sejam oportunas, eficazes e sem erros, uma boa preparação começa com o desenvolvimento de Procedimentos Operacionais de Emergência (EOPs) para todos os cenários possíveis de falha e ou de alto risco. Alguns exemplos são: falha na partida de um grupo gerador, falha de uma central de água gelada, a perda de uma unidade UPS e assim por diante. Os EOPs estabelecem um plano de ação detalhado para isolar com segurança falhas e restaurar serviços ou redundância, quando possível. Esses procedimentos devem ser desenvolvidos, aprovados e publicados. Também é importante que simulações desses procedimentos sejam conduzidas regularmente para treinar e avaliar a eficácia da resposta à emergência para a equipe e os indivíduos.

CMP (Crisis Management Plan) – No ambiente de Data Center muitos cenários de emergência estão previstos e os respectivos procedimentos de emergência (EOPs) definidos, mas não é incomum experimentar eventos imprevistos ou avarias. Uma crise é definida como uma situação de extrema dificuldade que está fora do escopo das respostas preparadas. As crises podem ser prolongadas e têm o potencial para se tornarem mais graves quando não tratadas de forma coordenada por todos os colaboradores envolvidos. A fim de minimizar o seu impacto, um Plano de Gestão de Crises (CMP) deve ser desenvolvido pela equipe de operações, em coordenação com a área de gestão de clientes e as ações devem ser detalhadas passo a passo sobre o que fazer nesses casos. Atenção especial deve ser dada a políticas de aquisição de combustível durante desastres naturais, bem como os procedimentos de manutenção do gerador e políticas durante os períodos de operação estendida em geradores.

BC/DR (Business Continuity/Disaster Recovery) Procedures – Os Procedimentos de Continuidade de Negócios / Recuperação de Desastres (BC/DR) fazem parte do Plano de Resposta a Emergência que será utilizado para responder a emergências e devem ser de conhecimento obrigatório para todos os coordenadores e gestores de um Data Center. Ele tem como objetivos, proteger a vida, a saúde e a segurança, limitar e conter danos para a instalação e equipamentos, estabilizar as operações e serviços e gerir eficazmente as comunicações durante todo o incidente. Os Procedimentos de BC/DR destinam-se a fornecer orientações para a recuperação rápida e eficaz de funções críticas de negócios após qualquer evento que provoque uma perda ou uso limitado de serviços e instalações do Data Center. O Plano de Continuidade de Negócios visa minimizar o impacto financeiro e operacional resultante de uma perda nas instalações, tecnologia ou equipamentos, priorizar as funções de missão crítica que exigem imediata restauração, identificar os principais recursos e dependências para funções críticas e servir como documento guia para os planos de continuidade de cada unidade de negócios individualmente.

Gerenciamento de Incidentes – Para uma adequada resposta a emergência é necessário um protocolo que garanta que qualquer evento envolvendo segurança ou missão crítica seja conhecido pelo pessoal apropriado, sejam eles funcionários, contratados ou fornecedores. Todos os incidentes devem ser relatados imediatamente após a estabilização da situação. Um breve resumo do incidente deve ser enviado para uma lista de distribuição definida pela gravidade de cada incidente. Dentro de 24 horas do incidente, um relatório completo deve ser arquivado, contendo uma descrição cronológica detalhada, passo a passo e que identifique claramente os fatos. Isto será importante para a **Análise de Falhas** (um programa abrangente para determinar a causa raiz, necessário para qualquer incidente que implique em, ou tenha a probabilidade de causar, uma lesão ou tempo de inatividade do sistema) e para **Lições Aprendidas** (um programa que ajudará a prevenir ocorrências futuras, sendo usado como uma ferramenta de treinamento e referência para todos os locais geridos).

Para responderem eficazmente a todos os diferentes tipos de riscos e crises nos Data Centers, as organizações devem agir rapidamente e de forma coordenada, além de saberem como proceder em situações inesperadas. Uma metodologia operacional correta evitará erros comuns e o agravamento da situação. O Plano de Preparação e Respostas a Emergências é o elemento chave dessa metodologia e inclui a integração de pessoas, processos e sistemas que leva os operadores de missão crítica a executarem ações de forma previsível e eficaz.

José Roberto da Silva
Luís V. R. Dória
Diretores da Top Tier Infrastructure