UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

INSTRUÇÃO NORMATIVA STI/POSIN 08 – GESTÃO DE CONTINUIDADE

A Gestão de Continuidade é um processo abrangente de gestão que identifica ameaças potenciais aos ativos de informação da Ufes e possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente aos incidentes de Segurança da Informação (SI) e minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades da Universidade, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

Os setores da Ufes deverão manter processo de gestão de continuidade de negócios, visando não permitir que as atividades sejam interrompidas e, também, assegurar a sua retomada em tempo hábil, quando for o caso.

Todos os titulares das unidades administrativas da Ufes deverão atuar de forma proativa para aumentar a resiliência contra possíveis interrupções dos serviços, protegendo, assim, a reputação e imagem institucional da Ufes.

Todos os setores da Ufes deverão formalizar, no Plano de Gestão de Riscos, as estratégias e procedimentos que serão adotados em situações que comprometam o andamento normal dos processos e a consequente prestação dos serviços. Essas medidas deverão assegurar a disponibilidade dos ativos de informação e a recuperação de atividades críticas, com o objetivo de minimizar o impacto sofrido diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.

Deve-se evitar que pessoas externas à Ufes respondam por ativos de informação importantes uma vez que a suspensão das atividades e falta de documentação são fatores que colocam em risco a gestão de continuidade.

1. PARADA DE SISTEMAS CRÍTICOS

As modificações nos recursos de processamento da informação e sistemas devem ser gerenciadas, uma vez que o controle inadequado dessas modificações nos sistemas e nos recursos de processamento da informação é uma causa comum de falhas de segurança ou

de sistema.

Mudanças em ambientes operacionais, especialmente quando da transferência de um sistema em desenvolvimento para o estágio operacional, podem trazer impactos à confiabilidade de aplicações.

Os sistemas operacionais e aplicativos devem estar sujeitos a rígido controle de gestão de mudanças. Quando mudanças forem realizadas, é conveniente que seja mantido um registro de auditoria contendo todas as informações relevantes.

As mudanças em sistemas operacionais devem ser realizadas apenas quando houver uma razão de negócio válida para tal, como um aumento no risco do sistema. A atualização de sistemas às versões mais atuais de sistemas operacionais ou aplicativos nem sempre é do interesse do negócio, pois pode introduzir mais vulnerabilidades e instabilidades ao ambiente do que a versão corrente. Pode haver ainda a necessidade de treinamento adicional, custos de licenciamento, suporte, manutenção e sobrecarga de administração, bem como a necessidade de novos equipamentos, especialmente durante a fase de migração.