GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DE FAZENDA
SUBSECRETARIA ADJUNTA DE TECNOLOGIA DA INFORMAÇÃO

Política de Segurança da Informação
Norma 005-N1: Gestão de Backup

1. Introdução

A disponibilidade é considerada um dos pilares da segurança da informação. Sendo assim, visando assegurá-las e, por conseguinte, garantir a continuidade das atividades da Secretaria de Estado de Fazenda e Planejamento do Estado do Rio de Janeiro, a SATI tem buscado cercar-se de recursos tecnológicos capazes de suportar as atividades desta secretaria, bem como prover a recuperação das informações geradas (dados e informações) em caso de incidentes.

2. Objetivo

O principal objetivo deste documento é prover orientações e diretrizes de segurança, visando assegurar a disponibilidade da informação, através de cópias de segurança, nomeadas por backup corporativo, para que, nos casos de perda de dados, desastre, erro de arquivos, falhas de mídia, entre outros incidentes, estes arquivos e/ou sistemas possam ser recuperados e disponibilizados aos usuários.

3. Abrangência

Esta política se aplica a todos os colaboradores da SEFAZ, quais sejam: servidores, estagiários, menor aprendiz, terceirizados ou indivíduos que, direta ou indiretamente, utilizam ou suportam os sistemas, infraestrutura ou informações da SEFAZ-RJ. Todos esses colaboradores serão tratados nesta política como usuários.

A Norma de Gestão de Backup deve ser utilizada como referência para todos os procedimentos relativos a backup e recuperação de dados armazenados nos servidores da empresa.

4. Princípios Gerais

A norma de Gestão de Backup da SEFAZ-RJ deve ser utilizada como referencia para todos os procedimentos relativos a backup e recuperação de dados armazenados nos servidores da Secretaria, o que a torna de grande importância para a organização.

A norma de Gestão de Backup contém definições de todos os itens, como calendário de backups e frequência, onde as cópias devem ser armazenadas, seu transporte e por quanto tempo.

Um backup abrangente e consistente deve ser o melhor caminho para garantir que os dados possam ser recuperados em caso de incidentes que afetam o servidor.

A área de produção/banco de dados deve realizar cópia de segurança – *backup* – de todos os servidores de dados e de aplicações sob sua responsabilidade de acordo com a política estabelecida para os dados e sua necessidade.

A Superintendência de Infraestrutura da SATI deve estabelecer, em conjunto com os Gestores da Informação, o tempo de retenção das mídias e prazo para revisões, a fim de testar a restauração e a integridade dos backups, assim como definir as rotinas de backup dos bancos de dados, de modo que sejam garantidas as necessidades de recuperação dos dados.

Toda a informação considerada crítica deve possuir cópia de segurança, sendo a área de produção e de banco de dados da SATI as responsáveis pela geração e manuseio das cópias de segurança das informações da SEFAZ-RJ.

Toda geração de cópias de segurança devem atender aos requisitos operacionais, legais, históricos e de auditoria estabelecidos para cada tipo de dado ou informação.

Os dispositivos utilizados para gravação de volumes de dados somente devem ser compartilhados pela rede interna da SEFAZ, mediante a utilização de senha de acesso segura.

O segredo do cofre, chaves, controles de acesso ou semelhantes, onde estão armazenadas as cópias de segurança devem ser trocados sempre que algum dos funcionários e/ou empresas prestadoras de serviço, que tenha permissão de acesso seja desligado da SEFAZ-RJ.

5. Diretrizes de Cópias de Segurança

I. Diretrizes e Infraestrutura

a. As cópias de segurança na SEFAZ-RJ contemplam arquivos (dados e informações), sistemas digitais, de máquinas virtuais e banco de dados, armazenados e/ou hospedados nos data centers da SEFAZ-RJ, não sendo contemplados os equipamentos de mesa – *desktop* e portáteis – *notebooks.*

b. De acordo com a presente norma, devem ser estabelecidos procedimentos que considerem:

I. Cópia de segurança – Escopo, periodicidade, tempo de permanência e descarte;

II. Recuperação – Disponibilidade da informação, capacidade de armazenamento de destino, tempo de restauração e tempo de retenção pré-estabelecido.

c. O planejamento das cópias de segurança deve levar em consideração a importância dos dados e relacionar a abrangência (ex.: completa ou incremental), a frequência (ex.: diária, semanal, mensal, semestral, anual), o período de retenção, versionamento, local de armazenamento, substituição de mídias, transporte de mídias de dados e requisitos de segurança em relação à criticidade dos dados da SEFAZ-RJ;

d. As solicitações de cópias de segurança – *backup* - devem ser realizadas através de formulário especifico, contendo as informações necessárias para operacionalização. Devem ser autorizadas pelo gestor da informação, levando-se em consideração os níveis de sensibilidade da informação para o negócio;

e. O procedimento deve considerar que as cópias sejam efetuadas e testadas regularmente, de maneira que os dados copiados estejam em condições de uso quando houver necessidade de recupera-los;

f. O procedimento deve definir e disponibilizar requisitos técnicos e operacionais adequados na geração e restauração de cópias de segurança, assim como, para testes de análise e validação;

g. As solicitações de recuperação de informações devem ser realizadas através de uma requisição de mudança e autorizadas pelo gestor;

h. As ferramentas de cópia de segurança – *backup/restore* – devem ser mantidas e atualizadas de acordo com a disponibilização e recomendação do fornecedor, com licenças ativas e de acordo com o contrato;

i. As documentações relativas às configurações da ferramenta de cópia de segurança, inventários e procedimentos, devem ser mantidas atualizadas e disponíveis pela equipe técnica da SEFAZ-RJ.

6. Armazenamento, Retenção E Transporte.

I. A periodicidade com a qual são realizadas as cópias de segurança deve ser definida de acordo com o grau de importância da mesma, do sistema operacional ou aplicativo;

II. O período de retenção das cópias de segurança deve ser acordado com o Gestor da Informação, respeitados os preceitos legais para o tipo de dado envolvido;

III. A cópia de segurança completa será composta pelo *backup full*, mais seus complementos, realizados nos períodos definidos com o Gestor da Informação;

IV. O backup dos servidores deve ser iniciado conforme políticas de backups acordadas, salvos casos especiais;

V. A cópia de segurança específica para uma recuperação de desastre deve levar em consideração os sistemas operacionais, aplicações e dados que possibilitem uma completa recuperação da aplicação;

VI. Em caso de desastre, faz-se necessário que a infraestrutura disponibilizada em local de contingencia tenha as mesmas característica e configurações que o local original;

VII. Regularmente, o backup deve ser testado e analisado para garantir a confiabilidade, integridade e disponibilidade nos casos de uso emergencial e aderente aos requisitos necessários à recuperação.

VIII. A área de produção e banco de dados devem assegurar que as cópias de segurança das informações estarão disponíveis quando solicitadas, conforme os prazos definidos nos procedimentos previamente acordados com os Gestores da Informação.

IX. Toda restauração das cópias de segurança deve ser feita somente mediante aprovação do respectivo Gestor da Informação;

X. A operação de backup deve estar ciente da periodicidade de mudança de dados ou de sistemas, a fim de que seja feito um backup emergencial antes de qualquer mudança;

XI. Os novos projetos ou novas aquisições devem seguir os padrões estabelecidos nesta politica;

XII. As implementações para o ambiente tecnológico existente deverão ser adequadas a esta política no prazo de 01 (um) ano, a partir de sua publicação;

XIII. Caso não seja possível a adequação do recurso técnico ou do processo, o comitê de TI da SEFAZ-RJ deve documentar essa informação, bem como seus motivos, para fins de auditoria;

XIV. A periodicidade com que são realizadas as cópias de segurança deve ser definida de acordo com o grau de importância da mesma, do sistema operacional ou aplicativo;

XV. O backup dos servidores deve ser executado sempre às 19h00, salvo casos especiais;

XVI. A periodicidade normal do backup deve seguir a seguinte tabela:

Diário – de 2ª a 5ª-Feira a partir das 19h00.

Semanal – 6ª a partir das 22h00.

Mensal – antes do fechamento mensal da empresa, a partir das 22h00.

Anual – antes do último fechamento mensal do ano.