

Processo

Gestão de TI

Código

D.DIAT.01

Folha nº

1/11

No sentido de assegurar o acesso e a proteção das informações eletrônicas deste Tribunal, por meio de uma política de backup e restore que observe criteriosamente o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais, apresentamos os seguintes itens:

Art. 1º Regular a política de backup das informações eletrônicas no âmbito do Tribunal de Justiça de Alagoas, com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos dados sob a guarda da Diretoria Adjunta de Tecnologia da Informação, visando garantir a segurança, integridade e disponibilidade.

Art. 2º Para o disposto neste ato considera-se:

I – Administrador de backup: servidor do quadro do Tribunal de Justiça de Alagoas responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de backup e restore;

II – Administrador do recurso: servidor do quadro do Tribunal de Justiça de Alagoas responsável pela operação de determinados serviços ou equipamentos da Diretoria Adjunta de Tecnologia da Informação.

III – Backup full ou completo: modalidade de backup na qual todos os dados são copiados integralmente;

IV – Backup Incremental: modalidade de backup na qual todos os dados que foram modificados desde o último backup de qualquer tipo são copiados

V – Backup Diferencial: modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup completo (full) são copiados;

VI – Backups de primeiro e segundo estágio: modalidade de backup dividida em duas etapas que são armazenados em meios diferentes (disco e fita).

VII – Clientes de backup: todo equipamento servidor no qual é instalado o agente de backup;

Esta cópia quando impressa será considerada não controlada

Processo

Gestão de TI

Código

D.DIAT.01

Folha nº

2/11

VIII – Disaster recovery: estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;

IX – File library: biblioteca de arquivos utilizada para armazenamento de backup em disco;

X – Mídia: meio físico no qual efetivamente armazenam-se os dados de um backup;

XI – Retenção: período de tempo em que o conteúdo da mídia de backup deve ser preservado;

XII – Recovery Manager (rman): ferramenta de backup e Disaster Recovery do banco de dados Oracle.

Art. 3º O Chefe de Conectividade será o Administrador do Backup, ficando responsável pela política e procedimentos relativos aos serviços de backup e restore, bem como de guardar as mídias móveis e assegurar o cumprimento das normas aplicáveis.

Art. 4º São atribuições do Administrador de Backup:

I - propor modificações visando o aperfeiçoamento da política de backup;

II - criar e manter os backups;

III - configurar a ferramenta de backup e os clientes;

IV - criar e testar scripts;

V - criar e manter mídias;

| | | | |
|----------|---------------------|------------------|-------------|
| Processo | Gestão de TI | Código | Folha nº |
| | | D.DIAT.01 | 3/11 |

VI - testar o backup e restore;

VII - criar notificações e relatórios;

VIII - verificar periodicamente os relatórios gerados pela ferramenta de backup;

IX - restaurar os backups em caso de necessidade;

X - gerenciar mensagens e logs diários dos backups, fazendo o tratamento dos erros de forma que o procedimento de backup tenha sequência e os erros na sua execução sejam eliminados;

XI - fazer manutenções periódicas dos dispositivos de backup;

XII - fazer o carregamento das mídias necessárias para os backups programados;

XIII - comunicar ao Administrador do Recurso os erros e ocorrências nos backups;

XIV - fazer o armazenamento das mídias de backup. Parágrafo único. As atribuições do Administrador de Backup poderão ser delegadas a outro servidor efetivo do Tribunal de Justiça de Alagoas lotado na DIATI, exceto a de monitoramento, que deve ser sempre o Chefe de Conectividade.

Art. 5º Todo e qualquer dispositivo que armazene dados deverão ser considerados para sua inclusão no backup.

§ 1º O responsável por cada recurso da DIATI deverá definir quais diretórios e arquivos serão incluídos no backup, tendo como prioridade:

a) arquivos de configurações de sistemas operacionais e aplicativos instalados em servidores;

Esta cópia quando impressa será considerada não controlada

| | | | |
|----------|---------------------|------------------|-------------|
| Processo | Gestão de TI | Código | Folha nº |
| | | D.DIAT.01 | 4/11 |

b) arquivos de log dos aplicativos, inclusive log da ferramenta de backup e restore;

c) informações e configurações de banco de dados;

d) arquivos de usuários (documentos e e-mails);

e) arquivos de aplicações desenvolvidas pelo Tribunal ou quaisquer outros não descritos neste, mas que a perda de suas informações gere prejuízo a esta corte.

§ 2º O administrador de backup ou o responsável pela aplicação que pleiteia o mesmo, deverá definir quais diretórios e arquivos não serão incluídos na rotina, tendo como referência:

a) arquivos do sistema operacional ou de aplicações que podem ser reconstituídos através de uma nova instalação;

b) arquivos temporários;

c) arquivos salvos nas unidades locais das estações de trabalho;

d) arquivos da área de transferência;

e) arquivos particulares dos usuários.

§ 3º Para os aplicativos e/ou bancos de dados devem ser seguidas as recomendações sugeridas pelo desenvolvedor e/ou fabricante.

Art. 6º Os procedimentos de backup deverão ser atualizados quando houver:

Esta cópia quando impressa será considerada não controlada

| | | | |
|----------|---------------------|------------------|-------------|
| Processo | Gestão de TI | Código | Folha nº |
| | | D.DIAT.01 | 5/11 |

I - novas aplicações desenvolvidas;

II - novos locais de armazenamento de dados ou arquivos;

III - novas instalações de bancos de dados;

IV - novos aplicativos instalados;

V - outras informações que necessitem de proteção através de backups deverão ser informadas ao Administrador de Backup, pelo Administrador do Recurso.

Art. 7º Para a especificação de um backup, o Administrador do Recurso deverá enviar uma solicitação de backup contendo as informações relativas ao backup, tais como: servidor e dados a serem incluídos.

§ 1º O backup deverá ser criado na ferramenta de backup, seguindo as orientações do documento de solicitação de backup;

§ 2º Todos os backups criados deverão ser testados antes de aplicar a programação solicitada. Estes testes deverão incluir uma restauração para comprovar a eficácia do backup, que deverá incluir um atestado de aprovação do Administrador do Recurso.

§ 3º O Administrador do Recurso receberá semanalmente um relatório com o resultado do backup.

Art. 8º Os backups realizados em mídias do tipo cartucho de fita e que necessitem de armazenamento para Disaster Recovery serão guardados no Tribunal, observando a sua capacidade, de forma que seja priorizado o armazenamento dos últimos 90 dias, e cinco últimos backups anuais.

Art. 9º A retenção dos backups no disco e em fita devem observar os seguintes prazos:

Esta cópia quando impressa será considerada não controlada

| | | | |
|----------|---------------------|------------------|-------------|
| Processo | Gestão de TI | Código | Folha nº |
| | | D.DIAT.01 | 6/11 |

I - 15 dias e 1 ciclo, em disco;

II - mensal: 90 dias, em fita;

III - anual: cinco últimos anos, em fita.

Parágrafo único. Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada ou destruída, observando sempre seu estado de utilização e número de leitura/gravação. A Fita não deverá ultrapassar 30 anos de armazenamento, devendo ser copiada para outra mídia, destruída e descartada em lugar destinado para tal, obedecendo às leis ambientais.

Art. 10º A criação e operação dos backups deverão obedecer às seguintes orientações:

I - criação de backups:

a) o backup deverá ser programado para execução automática em horários de menor ou nenhuma utilização dos sistemas e da rede. Entre 19:30 às 6:00 de segunda à sexta e aos sábados e domingos todo o dia.

II - operação de backups:

a) o backup deverá ser monitorado pelo Administrador de Backup;

b) para os backups que apresentarem falhas, é obrigação do administrador de backup executar ações corretivas para sanar o problema;

Art. 11 Os backups deverão ser realizados como disposto a seguir:

Esta cópia quando impressa será considerada não controlada

Processo

Gestão de TI

Código

D.DIAT.01

Folha nº

7/11

I - os backups diários serão incrementais, em dispositivos de discos e diferencial em fita.

II - os backups semanais, mensais e anuais devem ser realizados na modalidade FULL, de forma a poder recuperar integralmente todas as informações sem a necessidade de outros backups.

III - a cópia semanal ocorrerá na sexta-feira, referindo-se à semana que se encerra.

IV - a cópia mensal ocorrerá na primeira sexta-feira de cada mês, referindo-se ao mês anterior.

V - a cópia anual ocorrerá no primeiro dia 7 do mês de janeiro, referindo-se ao ano anterior.

VI - em caso de falha em algum procedimento de backup ou impossibilidade da sua execução, o Administrador de Backup deverá adotar as providências no sentido de salvaguardar as informações através de outro mecanismo, como por exemplo: cópia dos dados para outro servidor, execução do backup em horário de produção etc, sempre priorizando a segurança dos dados.

Art. 12 O backup do servidor de arquivos será efetuado da seguinte forma:

I – o backup de arquivos será armazenado em Tape Library e Disco, opcionalmente, sob a seguinte estratégia de backup:

a) Em caso de Backup em disco, será realizado Backup diário incremental e FULL mensal, com retenção de 1 ciclo em disco. Não será feito Backup Diferencial em fita;

b) Backup Diferencial diário de domingo a sábado, com retenção de 60 dias, 1 ciclo;

c) Backup FULL mensal com retenção 90 dias;

Esta cópia quando impressa será considerada não controlada

| | | | |
|----------|---------------------|------------------|-------------|
| Processo | Gestão de TI | Código | Folha nº |
| | | D.DIAT.01 | 8/11 |

d) Backup FULL anual, no dia 7 de Janeiro, com retenção de 5 anos;

Art. 13 O backup de Máquinas Virtuais será efetuado da seguinte forma:

I – o backup de arquivos será armazenado em Tape Library e Disco sob a seguinte estratégia de backup:

a) Backup em disco, será realizado Backup diário incremental e FULL mensal, com retenção de 15 dia, 1 ciclo, em disco;

b) Backup FULL mensal com retenção 90 dias.

Art. 14 A recuperação de backups deverá obedecer às seguintes orientações:

I - todo e qualquer usuário que precise recuperar arquivos deve entrar em contato com o N1 e registrar a solicitação na ferramenta de controle de atendimento ou enviar um e-mail dando a localização dos arquivos a serem recuperados;

II - a equipe responsável pelo cadastramento do chamado técnico solicitará o nome e setor do usuário, os arquivo (s) a ser (em) recuperado (s), subdiretório (s) em que se encontra (m) e a data da versão que deseja recuperar, sendo esta última informação obrigatória para viabilizar a recuperação do arquivo;

III - este chamado será encaminhado ao Administrador de Backup, que após a conclusão da tarefa, realizará o fechamento do chamado indicando a restauração do(s) arquivo(s);

IV - deverá ser mantido registro de todos os arquivos cuja restauração foi solicitada, juntamente com as informações relativas ao solicitante, nome do arquivo, data da versão restaurada e data e hora da solicitação;

V - os bancos de dados serão restaurados pelo Administrador de Banco de Dados responsável, podendo o Administrador de Backup auxiliá-lo na tarefa de restore.

Esta cópia quando impressa será considerada não controlada

| | | | |
|----------|---------------------|------------------|-------------|
| Processo | Gestão de TI | Código | Folha nº |
| | | D.DIAT.01 | 9/11 |

VI - A restauração dos arquivos de rede somente será possível nos casos em que o arquivo tenha sido atingido pela estratégia de backup que ocorre todos os dias no turno da noite, ou seja, os arquivos criados e eventualmente apagados ou alterados não serão passíveis de recuperação no mesmo dia da criação.

Art. 15 O backup do banco de dados Oracle deverá ser realizado das seguintes formas:

I – backup efetuado através do Oracle Rman, os dados serão gravados em disco e fitas, os logs apenas em disco. Deverão adotar as seguintes estratégias:

- a) backup full semanal com retenção de 15 (quinze) dias em disco; Podendo ser iniciado na Sexta à noite, Sábado ou Domingo;
- b) backup full mensal com retenção de 90 dias;
- c) backup full anual com retenção de 5 anos;
- d) backup dos arquivos de log do Oracle Rman, realizado a cada 15 minutos, com retenção de 15 (quinze) dias.

Art. 16 Os recursos disponíveis no banco de dados Oracle que visem garantir maior disponibilidade dos serviços deverão estar habilitados e serão utilizados das seguintes formas:

I – Oracle Flash Back: para recuperação dos dados a partir de um ponto específico do tempo. Será utilizado nas situações de corrupção de dados lógicos ou perda de dados. Deverá estar configurado para recuperação rápida de informações, pelo menos, dos últimos 7 (sete) dias;

II – Oracle Data Guard: para proteção dos dados contra falhas, desastres, erros e corrupção de dados. Deve ser instalado em um ambiente tecnológico separado do Data Center principal (Site backup). Deverá manter a réplica exata do banco de dados principal. Será acionado em caso de falha no ambiente principal, funcionando como o banco principal, até que o primeiro seja restaurado.

Esta cópia quando impressa será considerada não controlada

Processo

Gestão de TI

Código

D.DIAT.01

Folha nº

10/11

Art. 17 A configuração e monitoração das funcionalidades relativas ao banco de dados Oracle será de responsabilidade do Administrador de Banco de Dados.

Art. 18 Os backups do banco de dados PostgreSQL, MySQL deverá ser realizado das seguintes formas:

a) backup incremental diário com retenção de 15 (quinze) dias em disco;

a) backup full semanal com retenção de 15 (quinze) dias em disco;

b) backup full mensal com retenção de 90 dias, em fita;

c) backup full anual com retenção de 5 anos, em fita.

Art. 19 O Administrador deverá testar por amostragem os backups Full mensais.

§1º Caso seja detectada falha no backup ou se o mesmo estiver incompleto, novo backup deverá ser executado com vistas ao seu armazenamento.

§2º Os testes de restauração dos bancos de dados deverão ser auxiliados pelo Administrador do Banco de Dados.

§3º Para todos os testes realizados deverá ser gerado um relatório que será apresentado ao Diretor da DIATI.

Art. 20 Quaisquer procedimentos programados nos equipamentos “servidores” e que impliquem riscos de funcionamento ou em quaisquer dispositivos de armazenamento do Tribunal, somente deverão ser executados após a realização do backup dos seus dados.

Art. 21 O descarte das mídias de backup inservíveis ou inutilizáveis deverá ser feito mediante proposta apresentada pelo Administrador de Backup dirigido ao Diretor da DIATI.

Esta cópia quando impressa será considerada não controlada

Política de Backup e Restore

| | | | |
|----------|---------------------|------------------|--------------|
| Processo | | Código | Folha nº |
| | Gestão de TI | D.DIAT.01 | 11/11 |

Parágrafo único. As fitas a serem descartadas deverão ser destruídas de forma a impedir a sua reutilização ou acesso indevido às informações por pessoas não autorizadas.

| Histórico de Alterações | | | |
|-------------------------|---------|------------------------------------------------------------------------------------|-------------------------------|
| Data | Revisão | Descrição das alterações | Aprovação |
| 08/09/2016 | 00 | Validação pelo Gestor | José Baptista dos Santos Neto |
| 08/06/2022 | 01 | Atualizações dos artigos da Política pela Compra de Appliance de Backup em Discos. | José Baptista dos Santos Neto |
| | | | |