**Política de Backup e Restauração**

Sumário



**1.Introdução**

1.1. Para manter a continuidade dos negócios do Cartório do 1º Ofício Registro de Imóveis Títulos e Documentos de Alta Floresta a ON LINE ENGENHARIA DE SISTEMAS LTDA, através do seu software estabelece mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de perdas por erro humano, ataques externos, catástrofes naturais ou outras ameaças. No sentido de assegurar a proteção dos seus dados eletrônicos, o presente documento apresenta a política de backup e restauração, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

***Este documento faz parte do programa de compliance do cartório 1º Oficio à Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - "LGPD")***

**2. Objetivos**

2.1. Art. 1º Regulamentar a política de backup das informações eletrônicas no âmbito do Cartório do 1º Ofício, com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos seus dados, visando garantir a segurança, integridade e disponibilidade, em conformidade com a Política de Segurança da Informação.

**3. Definições**

3.1. Para o disposto neste documento considera-se:

I – **Administrador de Backup**: colaborador do quadro do Cartório do 1º Ofício responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de backup e restauração;

II – **Administrador de Recurso**: colaborador do quadro do Cartório do 1º Ofício responsável pela administração de ativo de TIC, físico ou virtual, sob responsabilidade da empresa ON LINE ENGENHARIA DE SISTEMAS LTDA.

III – **Backup Completo (full):** modalidade de backup na qual os dados são copiados em sua totalidade;

IV – **Backup Diferencial**: modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup completo são copiados;

V – **Backup Incremental**: modalidade de backup na qual somente os arquivos novos ou modificados
desde o último backup - seja ele completo, diferencial ou incremental - são copiados.
VI – **Clientes de backup**: todo equipamento servidor no qual é instalado o agente de backup;
VII – **Recuperação de Desastre**: estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;
VIII – **Mídia**: meio físico ou virtual no qual efetivamente armazenam-se os dados de um backup;
IX – **Retenção:** período de tempo em que o conteúdo da mídia de backup deve ser preservado;
X – **Objeto**: qualquer dado passível de backup e restauração;
XI – **Tarefa de Backup**: mecanismo que é executado sob demanda ou de acordo com um agendamento e vincula um ou mais objetos a uma modalidade de backup e um período de retenção.

**4. Referências**

4.1. A presente política tem como referências:

I – Política de Segurança da Informação;
II – Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos;
III – Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;
IV – Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais.

**5. Responsabilidade e Atribuições**

5.1. O Departamento de TI será o Administrador de Backup, ficando responsável pela política e procedimentos relativos aos serviços de backup e restauração, bem como de guardar as mídias móveis e assegurar o cumprimento das normas aplicáveis.

5.2. São atribuições do Administrador de Backup:

I – propor modificações visando o aperfeiçoamento da política de backup;
II – criar e manter as tarefas de backup;
III – configurar a ferramenta de backup e os clientes;
IV – criar e manter mídias, se o procedimento de backup as utilizar;
V – testar o backup e a restauração;
VI – criar notificações e relatórios;
VII – verificar periodicamente os relatórios gerados pela ferramenta de backup;
VIII – restaurar os backups em caso de necessidade;
IX – 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;
X – fazer manutenções periódicas dos dispositivos de backup, se forem utilizados dispositivos deste gênero;
XI – fazer o carregamento das mídias necessárias para os backups programados;
XII – comunicar ao Administrador do Recurso os erros e ocorrências nos backups;
XIII – fazer o armazenamento das mídias de backup em cofre apropriado, caso o backup se utilize de mídias físicas.

**6. Escopo do backup e sua formalização**

6.1. Todo e qualquer ativo de TIC que armazene dados deverá ser considerado para avaliação de inclusão no processo de backup.
6.1.1. O responsável por cada recurso 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;
b) arquivos de log dos aplicativos, inclusive log da ferramenta de backup e restauração;
c) informações e configurações de banco de dados;
d) conteúdo de repositórios de dados associados a sistemas
e) arquivos institucionais de usuários (documentos e e-mails);
e) arquivos de aplicações desenvolvidas pelo Cartório do 1º Ofício ou quaisquer outros não descritos neste, mas que a perda de suas informações gere prejuízo a esta empresa.

6.2. O Administrador de Backup ou o Administrador de Recurso que pleiteia a inclusão de um Cliente de Backup 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 recolocados através de uma nova instalação;
b) arquivos temporários.

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

6.4. Os procedimentos de backup deverão ser atualizados quando houver:

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 de Recurso.

6.5. Para a especificação de um backup, o Administrador de Recurso deverá formalizar chamado técnico através da ferramenta de controle de atendimentos. O chamado deverá conter as informações relativas ao backup, tais como: identificação do servidor e dados a serem incluídos.

6.5.1. Os procedimentos de backup deverão ser configurados na ferramenta de backup, seguindo as orientações do documento de solicitação de backup;

**7. Prazo de retenção**

7.1. A retenção dos backups deve observar os seguintes prazos:

I – diário: dez últimos dias;
II – semanal: seis últimas semanas;
III – mensal: sessenta últimos meses;
IV – semestral: permanente;

7.1.1. 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 mídia não deverá ultrapassar 30 anos de armazenamento, devendo, nesse caso, ser copiada para outra mídia, destruída de forma segura e descartada em lugar destinado para tal, obedecendo as leis ambientais.

7.2. Sempre que necessário deverá ser realizada a atualização das mídias de backup com a finalidade de preservar o acesso aos dados nelas contidas.

**8. Procedimentos de backup**

8.1. 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 utilização dos
sistemas;

II – operação de backups:

a) o backup deverá ser monitorado pelo Operador NOC;

b) para todos os backups realizados, deve ser gerado um extrato automatizado pela própria ferramenta de backup. Tal extrato deverá ser enviado por e-mail para o Administrador de Backup;

c) para os backups que apresentarem falhas, o Operador NOC deverá criar uma entrada em relatório citando os clientes de backup e se houve ação corretiva adotada. Competirá ao Administrador de Backup tratar falhas remanescentes.

8.2. Os backups deverão ser realizados preferencialmente como disposto a seguir:

I – os backups diários serão executados de segunda à sexta-feira, entre 18h e 6h do dia posterior, em modo incremental;

II – os backups semanais serão executados nos finais de semana, iniciando aos sábados, em modo incremental. Não haverá execução de backup semanal quando coincidir com o backup mensal ou semestral;

III – os backups mensais serão executados no primeiro sábado do mês, em modo incremental. Não haverá execução de backup mensal quando coincidir com o backup semestral;

IV – os backups semestrais serão executados no primeiro sábado dos meses de Janeiro e Julho, em modo completo.

V – em caso de falha em algum procedimento de backup ou impossibilidade da sua execução, o Administrador de Backup deverá adotar as providências necessárias para promover a salvaguarda das informações através de outro mecanismo, como por exemplo: nova execução do backup em horário comercial ou cópia dos dados para outro servidor.

**9. Procedimentos de restauração**

9.1. A recuperação de backups deverá obedecer às seguintes orientações:

I – A solicitação de recuperação de objetos deverá sempre partir do responsável pelo recurso, através de chamado técnico, utilizando a ferramenta de controle de atendimentos.

II – o chamado técnico deve conter, ao menos, o nome e setor do usuário, o(s) objeto(s) a ser(em) recuperado(s), localização em que se encontra(m), a data da versão que deseja recuperar, local alternativo para o armazenamento do(s) objeto(s) recuperado(s), se for o caso, e a justificativa para recuperação.

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) objeto(s).

IV – A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup.

**10. Teste de confiança**

10.1. Os backups mensais e semestrais deverão ser testados quanto à integridade e recuperabilidade dos objetos, de maneira amostral, no prazo máximo de uma semana após a sua execução.

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

10.1.2. Para todos os testes realizados deverá ser gerado um relatório que ficará sob guarda do DSU.

**11. Recuperação de desastre**

11.1 As cópias do tipo Recuperação de Desastres serão feitas com base na replicação das mídias do backup semestral e serão armazenadas em cofre de segurança do CPD e que esteja, preferencialmente, localizado em local remoto.

11.1.1. A geração das mídias de Recuperação de Desastres ocorrerá após a realização do teste do backup semestral e terá retenção de um semestre.

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

**12. Descarte das mídias**

12.1. O descarte das mídias de backup inservíveis ou inutilizáveis deverá ser feito pelo Departamento de TI mediante solicitação do Administrador de Backup.

12.1.1. As mídias de backup a serem descartadas deverão ser destruídas de forma a impedir a sua reutilização ou acesso indevido aos dados por pessoas não autorizadas conforme preconiza a Política de Segurança da Informação.

**13. Disposições finais**

13.1 Esta política será reavaliada a cada 2 (dois) anos ou sempre que surgirem novos requisitos tecnológicos, corporativos e/ou legais.
13.2. Esta política poderá ser complementada por normas e procedimentos específicos.
13.3. Casos excepcionais ou não previstos serão tratados pela Direção do Centro de Processamento de Dados.