Serviço Notarial e Registro de Imóveis

Política de Backup e Restauração

Sumário

Introdução

Para manter a continuidade do negócio da Cartcom Sistemas, em sua missão como fornecer alta tecnologia aos Cartórios, com produtos originais, de fácil compreensão e que estejam de acordo com Códigos e Normas, é fundamental estabelecer 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 dados eletrônicos desta Empresa, 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.

Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas.
Para garantir a privacidade e a proteção dos seus dados pessoais, é muito importante que você conheça e respeite as diretrizes da Política de Backup e Restauração.

Este documento faz parte do programa de compliance do cartório Sexto Oficio à Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – "LGPD")

Orientações Gerais

I - As diretrizes desta instrução normativa devem considerar, prioritariamente, os requisitos legais, os objetivosestratégicos, a estrutura e finalidade da Instituição.
II - Cabem aos administradores preverem a realização de testes periódicos de restauração, no intuito deaveriguar os processos de backup e estabelecer melhorias.
III - A administração dos backups também deve ser orientada para que seus trabalhos respeitem as janelas para execução, inclusive realizando previsão para a ampliação da capacidade dos dispositivos envolvidos no armazenamento.
IV – Em caso de mídias físicas as mesmas que estiverem defeituosas ou inservíveis serão encaminhadas para picotamento, incineração, procedimentos de sobrescrita de dados remanescentes (disco rígido) ou outro procedimento que impossibilite a recuperação dos dados por terceiros.
V - Todo e qualquer ativo que armazene dados e que esteja sob responsabilidade do cartório Sexto Oficio deverá ser considerado para avaliação de inclusão no processo de backup.

Conceitos e Definições

Administrador de backup: responsável pelos procedimentos de configuração, execução e monitoramento de backup e pelo acompanhamento dos testes nos procedimentos de restore;

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentesao tratamento de dados pessoais;

Encarregado de Dados (DPO – Data Protection Officer): pessoa indicada pelo Controlador e Operador para atuarcomo canal de comunicação entre o Controlador, os Titulares dos Dados e a Autoridade Nacional de Proteção deDados (ANPD).

Auditor: Pessoa ou empresa nomeada por uma empresa para executar uma auditoria.

Backup full: cópia de segurança de dados computacionais;

Backup total: backup em que todos os dados são copiados integralmente (cópia de segurança completa);

Backup incremental: backup em que somente os arquivos novos ou modificados são copiados;

Backup diferencial: backup em que os arquivos novos ou modificados da base de dados incremental sãocopiados;

Clientes de backup: todo equipamento servidor no qual é instalado o cliente de backup;

Disaster Recovery: estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;

IX. Mídia: meio físico no qual se armazenam os dados de um backup;
X. Retenção: período de tempo em que o conteúdo da mídia de backup deve ser preservado;
XI. Restore: restauração de arquivos computacionais

Papéis e Responsabilidades

Será nomeado o **"Administrador de 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.

São atribuições do administrador de backup:

I – Providenciar a criação e manutenção dos backups;
II – Configurar a ferramenta de backup;
III – Manter as mídias preservadas, funcionais e seguras;
IV – Efetuar testes de backup e auxiliar nos procedimentos de restore;
V – Verificar diariamente os eventos gerados pela ferramenta de backup, tomando as providências necessáriaspara remediação de falhas;
VI – Restaurar os backups em caso de necessidade; VII – Gerenciar mensagens e logs diários dos backups;
VII – Comunicar ao Controlador os erros e as ocorrências nos backups e
VIII – Propor modificações visando o aperfeiçoamento da política de backup.
Observação – O serviço de backup deve ser orientado para a restauração das informações no menor tempo possível, principalmente havendo indisponibilidade de serviços que dependam da operação de restore.

Será nomeado o **"Auditor"**, ficando responsável pela auditoria relativo aos serviços de backup e restore, assegurar o cumprimento das normas aplicáveis.

É atribuição do Auditor:

I – Validar o resultado dos Backup e restore, levando em consideração os principios de Segurança da Informação(Integridade, disponibilidade e Confidencialidade).
II – Informar o Controlador os resultados obtido nas auditoria.

É atribuição do Controlador:

I - Deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. (Art 48 – LGPD)

Procedimentos de Backup

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;
b) o backup, preferencialmente, deverá ser realizado através da rede de
backup.
II – operação de backups:
a) o backup deverá ser monitorado pelo **Administrador de Backup**;
b) para todos os backups realizados, deve ser gerado um extrato automatizado pela própria ferramenta debackup. Tal extrato deverá ser enviado ao **Auditor** que prestará conta ao **Controlador**;
c) para os backups que apresentarem falhas, o **Administrador de Backup** deverá criar uma entrada no **Sistemade Controle interno** citando os clientes de backup e se houve ação corretiva adotada. Competirá ao **Administrador de Backup** tratar falhas remanescentes.

Os backups deverão ser realizados preferencialmente como disposto a seguir:
I – para os Backups de Clientes "Backup em Nuvem", serão executados obedecendo o Provimento nº 74/2018 Dispõe sobre padrões mínimos de tecnologia da informação
II – os backups internos no cartório Sexto Oficio serão executados de segunda à sexta-feira, entre 17:30 e 6h do diaposterior, em modo incremental;
III – 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;
IV – os backups mensais serão executados no primeiro sábado do mês, em modo incremental. Não haveráexecução de backup mensal quando coincidir com o backup semestral;
V – os backups semestrais serão executados no primeiro sábado dos meses de Janeiro e Julho, em modocompleto.
VI – 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 de comercial ou cópia dos dados para outro servidor.

VI – Em caso de Backup do Cliente com finalidade única e exclusiva de "Debug"(Correção de procedimentos internos ao Banco de Dados) o **Administrador de Backup** deverá criar uma entrada no **Sistema de Controle interno** citando o motivo do "Debug" e data, para finalidade de auditoria de Segurança.

Procedimentos de Restauração

A recuperação de backups deverá obedecer às seguintes orientações:

I - para os Backups de Clientes "Backup em Nuvem", a solicitação de recuperação de objetos deverá sempre partir do responsável pelo recurso (Cliente), através de chamado, utilizando a ferramenta de controle de atendimentos.
II – os backups internos a solicitação de recuperação de objetos deverá sempre partir do responsável pelo recurso (Interno), através do **Sistema de Controle interno**.

III – 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.
IV – 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).
V – A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup
VI – Em caso de Restauração de Backup do Cliente com finalidade unica e exclusiva de "Debug"(Correção de procedimentos internos ao Banco de Dados) o **Administrador de Backup** deverá criar uma entrada no **Sistema de Controle interno** citando o motivo do "Debug" e data, para finalidade de auditoria de Segurança.

Auditoria

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

I - Caso seja detectada falha no backup ou se o mesmo estiver incompleto, novo backup deverá ser executadocom vistas ao seu armazenamento.
II - Para todos os testes realizados deverá criar uma entrada no **Sistema de Controle interno** com informaçõesdo teste realizado, constando data e o status do teste realizado.
III – O **Auditor** deverá confirmar o descarte dos Backups com finalidade unica e exclusiva de "Debug"(Correção

de procedimentos internos ao Banco de Dados)

Recuperação de desastre

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

Observação: A geração das mídias de Recuperação de Desastres ocorrerá após a realização do teste do backupsemestral e terá retenção de um semestre.

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

Descarte de mídias

I - O descarte das mídias de backup inservíveis ou inutilizáveis deverá ser feito pelo Departamento de Segurançada Informação mediante solicitação **do Administrador de Backup**.

Observação: 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.

II - Após a correção dos procedimentos de desenvolvimento dos Bancos de dados de Cliente com finalidade unica e exclusiva de "Debug"(Correção de procedimentos internos ao Banco de Dados) o **Administrador de Backup** deverá descartar o Banco de dados como o Backup de forma que possa impedir a sua reutilização ou

acesso indevido aos dados por pessoas não autorizadas e após criar uma entrada no **Sistema de Controleinterno** citando o descarte, data para finalidade de auditoria de Segurança.

Disposições finais

I - Esta política será reavaliada a cada 2 (dois) anos ou sempre que surgirem novos requisitos tecnológicos, corporativos e/ou legais.
II - A implementação dessa política está sujeita a disponibilidade de recursos financeiros e humanos.III - Esta política poderá ser complementada por normas e procedimentos específicos.

IV - Casos excepcionais ou não previstos serão tratados com o Controlador.

Documento	Política de Backup e Restauração
Tipo de Instrumento Normativo	Política
Categoria do Assunto	Controle e Conformidade
Versão	1.0/2021
Identificação	PBK.01.001.2021

Elaborado por	Henrique J. Haveroth
Posição Elaborador	Gerente T.I
Aprovado por	Maria Auxiliadora Assis Asckar Rabaneda
Posição Aprovador:	DPO

Conclusão

O Cartório Sexto Oficio assume o compromisso em sua Política em empregar medidas técnicas e organizacionais adequadas no trato com dados pessoais, e esforçar-se para proteção dos dados pessoais dos titulares de dados pessoais contra acessos não autorizados, perda, destruição, compartilhamento não autorizado, entre outras hipóteses.