GESTÃO TÍTULO	Política de Backup Hosting/Cloud PREVIDÊNCIA BRB
CLASSIFICAÇÃO	Documento Executivo
REFERENCIAL NORMATIVO	Lei Geral de Proteção de Dados - Lei nº 13.709, de 14 de agosto de 2018 - LGPD Política de Segurança da Informação Manual de Segurança da PREVIDÊNCIA BRB
ASSUNTO	Estabelecer as diretrizes, os princípios e os requisitos para assegurar a proteção de dados eletrônicos.
ELABORADOR	Área de Tecnologia da Informação.
APROVAÇÃO	**Revisão 00** Aprovada na reunião 1180ª da Diretoria Executiva, de 14/07/2022 Aprovada na reunião 620ª do Conselho Deliberativo, de 26/07/2022
	Revisão 01 Aprovada na reunião 1277ª da Diretoria Executiva, de 11/01/2024 Aprovada na reunião 662ª do Conselho Deliberativo, de 30/01/2024

SUMÁRIO

1. CONSIDERAÇÕES INICIAIS

Uma política de Backup ao ser construída leva em consideração três variáveis, sendo elas: Tipos de Dados, Categoria do Backup e Retenção do Backup. Cada uma dessas variáveiscombinadas as outras, formam as diretrizes determinadas nesta Política de Backup, que entrega um **RPO**[1] e **RTO**[2] específico.

[01] Nesse contexto, para manter a continuidade do negócio da PREVIDÊNCIA BRB, em sua missão como instituição, é fundamental estabelecer mecanismos que permitam a proteção 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 desses dados eletrônicos, o presente documento, apresenta a política de backup e restauração, onde se estabelece também o novo serviço contratado com a Sonda Ativas (Datacenter), que utilizará a Tecnologia Enterprise de proteção dos dados baseado em point-in- time snapshot de alta velocidade. Podemos destacar como característica dessa solução:

- **Tecnologia Enterprise de proteção dos dados baseado em point- in-time snapshot** define forma eficaz de fazer backup dos dados com altíssimo desempenho e otimizando a utilização dos recursos tecnológicos.

[01] - **Otimização das políticas de backup,** destaca-se como a rotina baseada na necessidade de recuperação dos dados da PREVIDÊNCIA BRB e seguindo as melhores práticas do mercado atualmente predefinidas, garantindo a continuidade operacional e alinhamento aos requisitos estratégicose regulamentares do negócio da PREVIDÊNCIA BRB.

2. OBJETIVOS / BENEFÍCIOS.

[01] Informar a política de backup das informações eletrônicas, no âmbito da PREVIDÊNCIA BRB/DATACENTER, com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos dados, visando garantir a segurança, integridade e disponibilidade, em conformidade com a Política de Segurança da Informação.

Esta política almeja que o serviço possua os seguintes objetivos e benefícios:

- Assegurar um serviço de backup e recuperação de dados ágil e eficiente;
- Rápida recuperação de dados recentes por meio de restore desnapshot;
- Processo rápido e automatizado de implementação de políticas de backup no ambiente;
- Janela de Backup menores;
- Custos mais baixos com backup e recuperação eficaz;
- Recursos avançados de recuperação para Vms e aplicativos;
- Gerenciamento de backup e recuperação unificado;
- Backups sem interrupções e sem utilização de dispositivos lentos (fita);;
- Backup escalável de forma ininterrupta;
- Armazenamento de dados de backup em ambientes distribuídos com garantia de rapidez na

[1] **RPO**[1] (Recovery Point Objective): Indicador utilizado para que a empresa saiba a quantidade de recursos mínimos a serem recuperados em caso de falhas ou perda de dados.

[2] **RTO**[2] (Recovery Time Objective): Indicador que mensura o tempo máximo em que um sistema ou uma informação pode ficar indisponível após uma falha.

recuperação dos dados.

3. TIPOS DE BACKUP E RETENÇÃO

Para o disposto neste documento considera-se:

Cada dado e aplicação deve ser tratada de forma diferente, de acordo com suas características e necessidade, e os tipos de dados são:

Backup Servidor Virtual (VMWare, Citrix e Hyper-V) Windows e Linux

Backup Servidor Físico (Windows, Linux),File ServerPadrão (exceto vídeos e imagens), EPM e Sharepoint

Backup SGBD Oracle, SQL Server, DB2, MySQL, PostgreSQL, Sybase e ERPs ENT (SAP, ORACLE EBS, entre outras) com backup de LOG

Backup Servidores Virtuais S.O Windows

Tipo de Dados	Retenção	Política	RPO	RTO	Solicitação de restore	Replicado
Backup Servidores Virtuais S.O. Windows e Linux	Longa	- Full diário com retenção de 30 Dias - Full mensal com retenção de 12 Meses - 2 X Full Anual (semestral) com retenção de 5 anos ou tempo de contrato	24 horas	- 800,00 GB/hora para dados backup.	Até 3 restores mensais por ítem Backupeado	Sim
	Média	- Full diário com retenção de 30 Dias - Full mensal com retenção de 12 Meses	24 horas	- 600,00 GB/hora para dados backup.	Até 2 restores mensais por item Backupeado	Sim
	Baixa	- Full Semanal com retenção de 30 dias	24 horas	- 400,00 GB/hora para dados backup.	1 restore mensal por item backupeado	Sim

Backup Servidores físico, File Server, EPM e Sharepoint

Tipo de Dados	Retenção	Política	RPO	RTO	Solicitação de restore	Replicado
Backup Servidor Físico (Windows, Linux ou Unix), File Server Padrão (exceto vídeos e imagens), EPM e Sharepoint	Longa	- Full diário com retenção de 30 Dias - Full mensal com retenção de 12 Meses - 2 X Full Anual (semestral) com retenção de 5 anos ou tempo de contrato	24 horas	- 800,00 GB/hora para dados backup.	Até 3 restores mensais por item backupeado	Sim
	Média	- Full diário com retenção de 30 Dias - Full mensal retenção de 12 Meses	24 horas	- 600,00 GB/hora para dados backup.	Até 2 restores mensais por item backupeado	Sim
	Baixa	- Full diário com retenção de 30 dias	24 horas	- 400,00 GB/hora para dados backup.	1 restore mensal por item backupeado	Sim

Backup para Banco de dados

Tipo de Dados	Retenção	Política	RPO	RTO	Solicitação de restore	Replicado
Backup SGBD Oracle, SQL Server, DB2, MySQL, PostgreSQL, Sybase	Longa	- LOG de 1 em 1 hora com Retenção de 30 dias - Full diário com retenção de 30 dias - Full Mensal com retenção de 12 Meses e 2 X Full Anual (semestral) com retenção de 5 anos ou tempo de contrato	24 Horas Full 1 Hora para Log	- 400GB/hora para dados backup.	Até 3 restores mensais por item backupeado	Sim
	Média	- LOG de 1 em 1 hora com Retenção de 30 dias - Full diário com retenção de 30 dias - Full Mensal com retenção de 12 Meses	24 Horas Full 1 Hora para Log	- 400GB/hora para dados backup.	Até 2 restoresmensais por item backupeado	Sim
	Baixa	- LOG de 1 em 1 hora com Retenção de 30 dias - Full diário com retenção de 30 dias	24 Horas Full 1 Hora para Log	- 400GB/hora para dados backup.	1 restore mensal por item backupeado	Sim

As retenções do Backup devem levar em consideração o período em que determinada informação (por legislação ou melhores práticas) deve ficar armazenada dentro do dispositivo de armazenamento de dados.

Conforme abaixo, um exemplo a ser considerado:

- **Baixa**: com períodos de curto prazo normalmente até 30 dias –(Armazenamento realizado em backup para disco – object storage);

- **Média**: retenções de médio prazo com até 12 meses (Armazenamento realizado em ambiente object storage);**Longa**: Retenções de longo prazo de até 5 anos ou durante o período de contrato (armazenamento realizado em ambiente object storage).

4. RESPONSABILIDADE E ATRIBUIÇÕES

Para um melhor entendimento a matriz de responsabilidade será classificada com base na metodologia RASIC, onde:

[01] A PREVIDÊNCIA BRB, será a solitante para a realização de Restore, Relatórios, Backups eventuais e cabendo a contratada realizar tais procedimentos.

A empresa contratada, será a Administradora de Backup, ficando responsável pelo procedimentos relativos aos serviços de backup e restauração, bem como a retenção, conforme contratado e assegurar o cumprimento das normas aplicáveis.

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 – testar o backup e a estauração;

V – criar notificações e relatórios;

VI – verificar periodicamente os relatórios gerados pela ferramenta de backup;

VII – restaurar os backups em caso de necessidade;

VIII– 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;

IX– fazer manutenções periódicas dos dispositivos de backup;

X – fazer o carregamento das mídias necessárias para os backups programados;

XI –**[01]** comunicar a PREVIDÊNCIA BRB e ao Administrador do Recursos (GECAT) os erros e ocorrências nos backups;

A recuperação de backups deverá obedecer às seguintes orientações:

I – A solicitação de recuperação de objetos deverá sempre partir do responsável pelo recurso, através dechamado 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 (item de configuração pré-definido).

[01] Todo ativo da PREVIDÊNCIA BRB que armazene dados e que esteja sob responsabilidade da prestadora de serviços (Datacenter), deverá ser considerado para avaliação de inclusão no processo de backup.

[01] O Produto de Backup deverá garantir um serviço de proteção, aos dados da PREVIDÊNCIA BRB, com garantia de níveis de serviço, eficiência na proteção aos dados e a sua reutilização em caso de desastres e segurança completa aos dados armazenados.

Deverá também, atentar para os procedimentos em que aplicativos e/ou bancos de dados devem ser seguidas as recomendações sugeridas pelo desenvolvedor e/ou fabricante.

Os procedimentos de backup deverão ser atualizados, quando houver novas solicitações de serviço, por informações ou recomendações, ou ainda quando houver uma alteração de um item de configuração (IC).

5. TESTE DE CONFIANÇA DE BACKUP/RESTAURAÇÃO

[01] Esta política de Backup tem por finalidade buscar segurança e continuidade de negócios. Para tanto, exige a realização de testes de restauração que poderão ser auditadas pela equipe técinca da PREVIDÊNCIA BRB ou Auditoria externa.

[01] A equipe técnica da PREVIDÊNCIA BRB deverá solicitar esse serviço sob demanda.

6. DISPOSIÇÕES FINAIS

Esta política será reavaliada a cada 1 (ano) ano ou sempre que surgirem novos requisitos tecnológicos, corporativos e/ou legais.

A implementação dessa política está sujeita a disponibilidade de recursos financeiros e humanos.

Esta política poderá ser complementada por normas e procedimentos específicos.

[01] Casos excepcionais ou não previstos serão tratados pela Gerência de Tecnologia (GECAT da PREVIDÊNCIA BRB).