

POLÍTICA DE DESASTRES E BACKUP

Código 001 Versão1.00

HISTÓRICO DE REVISÃO

Número da versão	1.00
Data de implementação	29/09/2023
Próxima data de revisão	28/08/2024
Data de Aprovação	06/10/2023
Aprovado por	Leonilde Aparecida Barbaresco de Goes

Seção e detalhes	Autor	Data Alterada	Número da Versão
Versão inicial	W7BR SOLUÇÕES	setembro 2023	1.00

RESPONSABILIDADE	PUBLICAÇÃO	CLASSIFICAÇÃO
DPO-secva2000@gmail.com	[29/09/2023]	Interna

POLÍTICA DE DESASTRES E BACKUP

Código 001 Versão1.00

Sumário

1. Introdução	3
2. Objetivos	3
3. Definições	3
4. Referências.....	4
5. Responsabilidade e Atribuições	4
6. Escopo do backup e sua formalização	4
7. Prazo de retenção	5
8. Procedimentos de backup	5
9. Procedimentos de restauração.....	5
10. Teste de confiança	6
11. Disposições finais.....	6

RESPONSABILIDADE	PUBLICAÇÃO	CLASSIFICAÇÃO
DPO-secva2000@gmail.com	[29/09/2023]	Interna

1. Introdução

1.1. Para manter a continuidade do órgão CÂMARA MUNICIPAL DE VALE DO ANARI 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 seus dados eletrônicos, o presente documento apresenta a política de continuidade de negócios, recuperação de desastres e backup, assim como, a restauração, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

2. Objetivos

2.1. Regular a política de continuidade de negócios, recuperação de desastres e backup das informações eletrônicas no âmbito do órgão, com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos seus dados, visando garantir a segurança, confidencialidade, integridade e disponibilidade, em conformidade com a Política de Segurança da Informação.

3. Definições

- 3.1. Para o disposto neste documento (“Política”) considera-se:
1. Política Organizacional: política aplicável a todos os serviços do órgão, que deve garantir o cumprimento de suas diretrizes mínimas;
 2. Política de Backup (“PB”): cronograma pré-definido pelo qual dados, informações de aplicações comerciais, arquivos de usuários, em servidores locais e/ou em cloud, são copiados em uma ou mais mídias, para garantir a recuperação de dados no caso de exclusão acidental de dados, informações corrompidas ou algum tipo de interrupção do sistema.
 3. Setor de Compliance: departamento que elabora, aplica e monitora as políticas, procedimentos e regras relacionadas ao compliance digital, juntamente com o Setor de TI.
 4. Setor de TI: departamento que fornece gerenciamento e suporte de TI ao órgão é chefiado pelo Coordenador de TI;
 5. Coordenador de TI: colaborador ou terceirizada que administra a infraestrutura de TI do órgão e tem autoridade designada para tomar decisões relacionadas a essa infraestrutura;
 6. Administrador de Backup: colaborador da BETTER TECH INFORMATICA E SERVIÇOS DE AUTOMAÇÃO LTDA responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de backup e restauração;
 7. Backup Completo (full): modalidade de backup na qual os dados são copiados em sua totalidade;
 8. Backup Diferencial: modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup completo são copiados;
 9. 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.
 10. Clientes de backup: todo equipamento servidor no qual é instalado o agente de backup;
 11. Mídia: meio físico ou virtual no qual efetivamente armazenam-se os dados de um backup;
 12. Retenção: período em que o conteúdo da mídia de backup deve ser preservado;
 13. Objeto: qualquer dado passível de backup e restauração;
 14. Tarefa de Backup: mecanismo que é executado sob demanda ou de acordo com um

RESPONSABILIDADE	PUBLICAÇÃO	CLASSIFICAÇÃO
DPO-secva2000@gmail.com	[29/09/2023]	Interna

POLÍTICA DE DESASTRES E BACKUP

Código 001 Versão1.00

agendamento e vincula um ou mais objetos a uma modalidade de backup e um período de retenção; e

15. Plano de Continuidade de Negócios “(PCN)”- visa assegurar a continuidade das operações do órgão, em caso de ser afetado por diferentes níveis de desastres físicos e/ou lógicos, que podem ser de desastres de curto prazo até grandes problemas que perduram vários dias ou até mesmo uma perda permanente de um edifício.

4. Referências

4.1. A presente política tem como referências:

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

5. Responsabilidade e Atribuições

5.1. O Setor de Compliance é responsável por elaborar e/ou aprovar as diretrizes da Política de Continuidade de Negócios, Recuperação de Desastres e Política de Backup, assim como assegurar o cumprimento de suas normas.

5.2. O Setor de TI ou Empresa contratada para esse fim é o Administrador de Backup, ficando responsável pelos procedimentos relativos aos serviços de backup e restauração, bem como por guardar as mídias referentes a backup e restauração.

5.3. São atribuições do Administrador de Backup:

1. Criar e manter as tarefas de backup;
2. Configurar a ferramenta de backup e os clientes;
3. Criar e manter mídias, se o procedimento de backup as utilizar;
4. Testar o backup e a restauração;
5. Criar notificações e relatórios;
6. Verificar periodicamente os relatórios gerados pela ferramenta de backup;
7. Restaurar os backups em caso de necessidade;
8. 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;
9. Fazer manutenções periódicas dos dispositivos de backup, se forem utilizados dispositivos deste gênero;
10. Propor modificações visando o aperfeiçoamento da política em questão.

6. Escopo do backup e sua formalização

6.1. Apenas os servidores da empresa (físicos e/ou virtuais) serão incluídos na estratégia de backup.

6.1.1. O Administrador de Backup deverá definir quais diretórios e arquivos serão incluídos no backup, tendo como prioridade:

11. conteúdo de repositórios de dados associados a sistemas
12. arquivos institucionais de usuários (documentos e e-mails);
13. arquivos de aplicações desenvolvidas para a órgão ou quaisquer outros não descritos neste, mas que a perda de suas informações gere prejuízo a esta empresa.

6.2. O Administrador de Backup deverá definir quais diretórios e arquivos não serão incluídos

RESPONSABILIDADE	PUBLICAÇÃO	CLASSIFICAÇÃO
DPO-secva2000@gmail.com	[29/09/2023]	Interna

POLÍTICA DE DESASTRES E BACKUP

Código 001 Versão 1.00

narotina, tendo como referência:

14. arquivos do sistema operacional ou de aplicações que podem ser recolocados através de uma nova instalação;
15. arquivos temporários;
16. arquivos fora dos servidores da rede (ex: os salvos exclusivamente nas estações de trabalho).

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:

17. novas aplicações desenvolvidas;
18. novos locais de armazenamento de dados ou arquivos;
19. novas instalações de bancos de dados;

6.5. Outras informações que necessitem de proteção através de backups deverão ser informadas ao Administrador de Backup.

7. Prazo de retenção

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

7.1.1. Diário: 30 últimos dias (feito em cloud na BETTER);

7.1.2. Expirado o prazo de retenção dos dados armazenados, o versionamento a partir do mais antigo (30º dia) é sobrescrito iniciando o ciclo novamente.

7.2.1. Em arquivos armazenados no e-mail oficial não serão excluídos.

8. Procedimentos de backup

8.1. A criação e operação dos backups deverão obedecer às seguintes orientações:

1. criação de backups;
2. o backup deverá ser programado para execução automática fora do horário de expediente;

8.2. operação de backups:

1. O backup deverá ser monitorado pelo Administrador de Backup;
2. 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;
3. O Administrador de Backup deverá verificar diariamente os logs do software de backup para verificar se ele concluiu corretamente as tarefas agendadas;
4. Para os backups que apresentarem falhas, a ferramenta de backup, cria um incidente no órgão, onde ficará registrada a falha bem como as medidas adotadas em sua correção.

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

1. os backups diários serão executados de segunda à domingo, entre 20h e 7h do dia posterior, em modo incremental;
2. 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:

1. A solicitação de recuperação de objetos deverá sempre partir do responsável

RESPONSABILIDADE	PUBLICAÇÃO	CLASSIFICAÇÃO
DPO-secva2000@gmail.com	[29/09/2023]	Interna

POLÍTICA DE DESASTRES E BACKUP

Código 001 Versão 1.00

pelo recurso, através de chamado técnico, utilizando o e-mail para criar uma tarefa para o Setor de TI ou empresa contratada para esse fim.

2. 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), se for o caso, e a justificativa para recuperação.
3. Este chamado será encaminhado ao Setor de TI ou empresa contratada para esse fim, que após a conclusão da tarefa, realizará o fechamento do chamado indicando a restauração do(s) objeto(s).
4. A restauração de objetos somente será possível nos casos em que este seja atingido pela estratégia de backup.

10. Teste de confiança

10.1. Os backups deverão ser testados quanto à integridade e recuperabilidade dos objetos, de maneira amostra, no prazo máximo de seis meses após a sua execução.

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

10.1.2. Para todos os testes realizados deverá ser gerada uma tarefa que será criada no através de e-mail documento, com os resultados dos testes.

11. Disposições finais

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

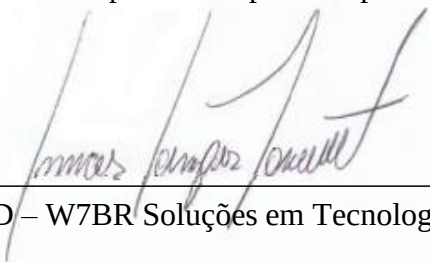
11.2. Esta política poderá ser complementada por normas e procedimentos específicos, estabelecendo obrigações mais restritivas, porém nunca mais permissivas, por meio de Apêndice.

11.3. As normas complementares devem ser aprovadas nos mesmos moldes desta política, conforme item 11.5, adiante.

11.4. Casos excepcionais ou não previstos serão tratados pelo Setor de TI, Setor de Compliance e Diretoria.

11.5. Esta política é revisada periodicamente, conforme o entendimento da diretoria do CPD e da secretária do órgão.

Esta política é aprovada pela diretora do CPD em conjunto com a Diretoria do órgão.



CPD – W7BR Soluções em Tecnologia

Controlador – Jamir Batista Ferreira

RESPONSABILIDADE	PUBLICAÇÃO	CLASSIFICAÇÃO
DPO-secva2000@gmail.com	[29/09/2023]	Interna