2. POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS DIGITAIS

Responsável: ALMIR BEZERRA LEITE
Políticas Relacionadas: Relacione outras políticas corporativas relacionadas dentro ou externas a este modelo, por exemplo, Política de Gestão de Riscos \ Política de Retenção de Dados\ POSIN
Localização de armazenamento: Descreva a localização física ou digital das cópias desta política.

Data de revisão : 20/12/2025

PROPÓSITO :

A Política de Backup e Restauração de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pela(s) empresa de servidor de hospedagem do site, empresa servidora do sistema de gestão, e formalmente definidos como de necessária salvaguarda nessa empresa, para se manter a continuidade do negócio.

No sentido de assegurar sua missão é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças. O presente documento apresenta a Política de Backup e Restauração de Dados Digitais, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

Escopo

A quem se aplica:
Colaboradores ou Terceiros Responsáveis pelo BKP:

Esta política se aplica a todos os dados no âmbito dessa empresa incluindo dados fora armazenados em um serviço de nuvem Pública ou Privada. “Dados críticos”, neste contexto, incluem e-mail, arquivos pessoais e compartilhados,

bancos de dados e conteúdo da web específicos e sistemas operacionais. A definição de dados críticos e o escopo desta política de backup serão revisados anualmente pelo CONTROLADOR.

Os serviços de TI críticos devem ser formalmente elencados pelo CONTROLADOR.

- Já ficam previamente estabelecidos SITE E SISTEMA DE GESTÃO, como serviços críticos da empresa.

- Esta política se aplica a todos os agentes que podem ser criadores e/ou usuários de tais dados. A política também se aplica a terceiros que acessam e usam nessa empresa sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade dessa empresa.

- Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s).

- A salvaguarda dos dados em formato digital pertencentes a serviços de TI dessa empresa mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

Termos e Definições

BACKUP OU CÓPIA DE SEGURANÇA - Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

CUSTODIANTE DA INFORMAÇÃO - Qualquer indivíduo ou estrutura de órgão ou entidade da Administração Pública Federal, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles

de segurança em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação;

ELIMINAÇÃO - Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado; MÍDIA - Mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação - inclui discos ópticos, magnéticos, rígidos, CDs, fitas e papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos;

INFRAESTRUTURA CRÍTICA – instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança;

Recovery Point Objective (RPO): ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente;

Recovery Time Objective (RTO): tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados, após um incidente;

REFERENCIA LEGAL E BOAS PRÁTICAS:

Orientação	Seção
Acórdão 1.109/2021-TCU-Plenário	Em sua íntegra
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo, art.3, Inciso I, II e V
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art.15
Framework Control Objectives for Information and Related Technology – Cobit, conjunto de boas práticas a serem aplicadas à governança da TI;	v4.1: DS11: Gerenciar Dados v5: DSS01.01, DSS04.08; DSS06.04, DSS04.08, DSS05.06; DSS06.05-06, DSS04.08, DSS001.01; DSS05.02-05; DSS06.03; DSS06.06
Guia do Framework de Privacidade e Segurança da Informação	Controle 11
Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI;	Gestão da Segurança da Informação
Instrução Normativa 01/GSI/PR	Art.12, Inciso IV, alínea g, h
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo IV
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos;	A.12.3 Cópias de segurança
Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;	12.3 Cópias de segurança
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra

DECLARAÇÕES DA POLÍTICA

POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS DIGITAIS

Empresa: BINÁRIA

Versão: 1.0

Data de emissão: 11/02/2025

---

1. OBJETIVO

Esta Política tem como objetivo estabelecer diretrizes para o **backup (cópia de segurança)** e a **restauração dos dados digitais** tratados pela empresa BINÁRIA, com o intuito de preservar a **integridade, disponibilidade e continuidade das informações**, especialmente aquelas relacionadas a clientes, atendimentos espirituais e transações realizadas por meio da loja virtual e do sistema de gestão.

---

2. ABRANGÊNCIA

Esta política se aplica a todos os dados digitais gerados, coletados, armazenados ou tratados nos ambientes e plataformas utilizadas pela empresa, incluindo:

- Sistema de gestão;
- Loja virtual;

- WhatsApp Business;
- Redes sociais (Instagram, Facebook, etc.);
- Documentos e planilhas locais;
- Dispositivos da equipe (notebooks e celulares pessoais).

---

3. RESPONSABILIDADE

- O titular **e encarregado de dados**, ALMIR BEZERRA LEITE, é responsável por garantir a execução desta política.
- A colaboradora de apoio deve seguir as orientações estabelecidas e comunicar quaisquer falhas ou riscos identificados.

---

4. DIRETRIZES GERAIS DE BACKUP

4.1. Frequência dos backups

- **Diariamente**: backups automáticos do sistema de gestão e da loja virtual, quando esses recursos estiverem habilitados pelas plataformas.
- **Semanalmente**: backup manual dos arquivos locais (planilhas de agendamentos, registros de atendimentos, documentos sensíveis) para nuvem segura (ex: Google Drive, OneDrive) com autenticação em duas etapas.
- **Mensalmente**: backup completo dos dispositivos (notebook e celular principal), com cópia externa armazenada em unidade USB criptografada e protegida por senha.

4.2. Local de armazenamento

- Cópias são armazenadas em **ambientes de nuvem seguros**, vinculados a contas oficiais da empresa, com controle de acesso;
- Backups externos são mantidos em local físico seguro, de acesso exclusivo da titular.

4.3. Dados incluídos no backup

- Registros de atendimentos;
- Fichas de clientes;
- Planilhas e documentos financeiros e administrativos;
- Arquivos de campanhas, conteúdos personalizados e kits energéticos;
- Mensagens importantes do WhatsApp exportadas em PDF (quando necessário para histórico);

- Dados de cadastro e pedidos extraídos da loja virtual.

---

5. RESTAURAÇÃO DE DADOS

5.1. Procedimento de restauração

- Em caso de perda, exclusão acidental, falha técnica ou incidente de segurança, o backup mais recente será utilizado para restauração.
- A restauração será feita **de forma prioritária e imediata** nos casos que afetem diretamente o atendimento ao cliente ou a continuidade das operações.

5.2. Tempo de resposta

- O tempo de resposta estimado para restaurar os dados críticos é de **até 24 horas**, salvo em caso de falhas graves nos sistemas terceirizados.

---

6. POLÍTICA DE RETENÇÃO

- Os backups semanais serão mantidos por **6 meses**;
- Os backups mensais serão armazenados por **até 1 ano**;
- Após esse período, os dados serão excluídos de forma segura, salvo quando houver obrigação legal de retenção por prazo superior.

---

7. SEGURANÇA

- Todos os backups devem estar protegidos por **senha forte**, preferencialmente com **autenticação em duas etapas**;
- Não é permitido o armazenamento de cópias em mídias ou locais compartilhados ou públicos;
- Dispositivos de backup devem permanecer com **acesso restrito e sob responsabilidade direta da titular**.

---

8. AUDITORIA E REVISÃO

- Esta política será revisada **anualmente** ou sempre que houver alteração significativa nos sistemas, plataformas ou estrutura da empresa;
- O titularmanterá registro das execuções de backup e das restaurações realizadas, para fins de conformidade com a LGPD.

---

9. DISPOSIÇÕES FINAIS

O cumprimento desta política é essencial para garantir a **continuidade das atividades da empresa**, bem como a **proteção dos dados pessoais e sensíveis tratados nos atendimentos e transações**. Eventuais dúvidas ou sugestões de melhoria devem ser direcionadas à Encarregado de Dados.

E, por estarem de pleno acordo, firmam o presente instrumento .

Caruaru– PE, ____ de _____ de 2025.

_____

ALMIR BEZERRA LEITE

Titular e Encarregado de Dados

_____

[Nome do(a) Colaborador(a)]

CPF: [preencher]