ÍNDICE DE REVISÕES

REVISÃO	STATUS	DESCRIÇÃO
0	AP	Elaboração inicial do documento.
A	AP	Atualização dos prazos de backup.

PA - PARA APROVAÇÃO	CA - CANCELADO	PR - PRELIMINAR
PI - PARA INFORMAÇÃO	AP - APROVADO	LI - LIBERADO

REVISÃO	REV. 0	REV. A	REV. B	REV. C	REV. D	REV. E	REV. F	REV. G
DATA	07/06/2022	01/08/2023						
ELABORAÇÃO	CARLOS C.	MARIANA O.						
ANÁLISE CRÍTICA	ADRIANA S	ADRIANA S.						
PADRONIZAÇÃO	ADRIANA S.	ADRIANA S.						
APROVAÇÃO	PAULO M.	BRUNO D.						

Sumário

1. ATA DE APROVAÇÃO 3
2. ABRANGÊNCIA 3
3. POLÍTICA 3
   - 3.1 Introdução 3
   - 3.2 Escopo do backup e sua formalização 3
   - 3.3 Prazo de retenção 3
   - 3.4 Procedimentos de backup 4
   - 3.5 Procedimentos de restauração 4
   - 3.6 Teste de confiança 5
   - 3.7 Recuperação de desastre 5
   - 3.8 Auditorias internas 5
   - 3.9 Casos omissos 5
   - 3.10 Glossário 5
   - 3.11 Revisões 5
   - 3.12 Gestão da política 6
4. DIRETRIZES 6
   - 4.1 Objetivo 6
   - 4.2 Atribuições e responsabilidades 6

1. ATA DE APROVAÇÃO

A ata de aprovação desta política encontra-se devidamente assinada e arquivada na plataforma UniVoce, no Curso Adequações LGPD, acessível a todos os colaboradores da empresa.

URL de Acesso: https://univoce.com.br/enrol/index.php?id=46

2. ABRANGÊNCIA

Abrangência interna e externa, para todos os colaboradores, clientes, fornecedores, parceiros e demais utentes que queiram conhecer esta Política.

3. POLÍTICA

3.1 Introdução

3.1.1 Para manter a continuidade do negócio 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 de Dados, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

3.2 Escopo do backup e sua formalização

3.2.1 Todo e qualquer ativo que armazene dados e que esteja sob responsabilidade da empresa deverá ser considerado para avaliação de inclusão no processo de backup.

- O responsável por cada recurso deverá definir quais diretórios e arquivos serão incluídos no backup;
- Para os aplicativos e/ou bancos de dados devem ser seguidas as recomendações sugeridas pelo desenvolvedor e/ou fabricante.

3.2.2 Os procedimentos de backup deverão ser atualizados e informados ao Administrador de Backup quando houver:

- Novas aplicações desenvolvidas;
- Novos locais de armazenamento de dados ou arquivos;
- Novas instalações de bancos de dados;
- Novos aplicativos instalados;
- Outras informações que necessitem de proteção através de backups.

3.2.3 Para a especificação de um backup, o interessado deverá formalizar chamado técnico através da ferramenta de abertura de chamados MeuHelpDesk. O chamado deverá conter as informações relativas ao backup, tais como: identificação do servidor e dados a serem incluídos;

3.3 Prazo de retenção

3.3.1 A retenção dos backups deve observar os seguintes prazos:

- Diário: dez últimos dias;
- Mensal: doze últimos meses;
- Semestral: Enquanto cliente;
- Anual: No encerramento do contrato.

3.4 Procedimentos de backup

3.4.1 A criação dos backups deverá obedecer às seguintes orientações:

- O backup deverá ser programado para execução automática em horários de menor utilização dos sistemas;
- O backup, preferencialmente, deverá ser realizado através da rede de backup.

3.4.2 A operação dos backups deverá obedecer às seguintes orientações:

- O backup deverá ser monitorado pelo Setor de Infraestrutura Corporativa e pelo DBA;
- Para todos os backups realizados, deve ser gerado um extrato automatizado pela própria ferramenta de backup. Tal extrato deverá ser enviado para o Administrador de Backup.

3.4.3 Os backups deverão ser realizados, preferencialmente, como disposto a seguir:

- Os backups diários serão executados de segunda à domingo, em modo completo;
- Os backups diários serão executados de segunda à sexta-feira, entre 18h e 6h do dia posterior, em modo completo;
- Os backups semanais serão executados nos finais de semana, iniciando aos sábados, em modo completo. Não haverá execução de backup semanal quando coincidir com o backup mensal ou semestral;
- Os backups mensais serão executados no primeiro sábado do mês, em modo completo. Não haverá execução de backup mensal quando coincidir com o backup semestral;
- Os backups semestrais serão executados no primeiro sábado dos meses de janeiro e julho, em modo completo.

3.4.4 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.

3.5 Procedimentos de restauração

3.5.1 A recuperação de backups deverá obedecer às seguintes orientações:

- A solicitação de recuperação de objetos deverá sempre partir do responsável pelo recurso, através de chamado técnico, utilizando a ferramenta de abertura de chamados MeuHelpDesk;
- 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;
- 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) solicitado(s);

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

3.6 Teste de confiança

3.6.1 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;

3.6.2 Caso seja detectada falha no backup ou se o backup estiver incompleto, um novo backup deverá ser executado com vistas ao seu armazenamento;

3.6.3 Para todos os testes realizados deverá ser gerado um relatório que ficará sob guarda do Administrador de Backup.

3.6.4 O DBA deverá realizar teste mensal quanto ao tamanho e qualidade dos backups gerados para garantir que não haja arquivos corrompidos.

3.7 Recuperação de desastre

3.7.1 As cópias do tipo Recuperação de Desastres serão feitas com base na replicação do backup semestral e serão armazenadas em nuvem.

3.8 Auditorias internas

3.8.1 Para verificação do cumprimento das normas definidas nessa e nas demais políticas internas, será responsável o setor de Auditoria Interna, que poderá implementar rotinas, eventuais ou programadas, de auditoria.

3.8.2 Será de responsabilidade dos gestores de setor contribuir para a realização das auditorias citadas no item anterior fornecendo todos os dados necessários aos responsáveis pela sua realização.

3.9 Casos omissos

Os casos omissos serão avaliados pelo Comitê Gestor de Proteção de Dados Pessoais para posterior deliberação.

3.10 Glossário

3.10.1 **Administrador de Backup:** colaborador responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de backup e restauração;

3.10.2 **Backup Completo (Full):** modalidade de backup na qual os dados são copiados em sua totalidade;

3.10.3 **Clientes de Backup:** todo equipamento servidor no qual é instalado o agente de backup;

3.10.4 **Database Administrator (DBA):** profissional da área de tecnologia responsável pela criação, instalação, monitoramento, reparos e análise de estruturas de um banco de dados ou sistemas de bancos de dados;

3.10.5 **Recuperação de Desastre:** estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;

3.10.6 **Retenção:** período de tempo em que o conteúdo do backup deve ser preservado;

3.10.7 **Objeto:** qualquer dado passível de backup e restauração;

3.10.8 **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.

3.11 Revisões

Esta política será reavaliada sempre que surgirem novos requisitos tecnológicos, corporativos e/ou legais conforme o entendimento do Comitê Gestor de Proteção de Dados Pessoais ou a cada 02 (dois) anos.

3.12 Gestão da política

3.12.1 A Política de Backup e Restauração de Dados é aprovada pela Diretoria da empresa, em conjunto com o Comitê Gestor de Proteção de Dados Pessoais.

3.12.2 Essa Política precisa estar atualizada em sua última versão na plataforma UniVoce, no Curso Treinamentos Corporativos – Normas e Políticas Internas, conforme acesso anteriormente citado.

4. DIRETRIZES

4.1 Objetivo

Regulamentar a Política de Backup e Restauração de Dados das informações eletrônicas no âmbito da empresa, com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos dados sob a guarda da empresa, visando garantir a segurança, integridade e disponibilidade, em conformidade com a Política de Segurança da Informação.

4.2 Atribuições e responsabilidades

4.2.1 O Setor de Infraestrutura Corporativa, em atuação conjunta com o DBA, desempenhará o papel de Administrador de Backup, ficando responsáveis pela política e procedimentos relativos aos serviços de backup e restauração de dados, assegurando o cumprimento das normas aplicáveis.

4.2.2 São atribuições do Administrador de Backup:

- Propor modificações visando o aperfeiçoamento da Política de Backup e Restauração de Dados;
- Criar e manter as tarefas de backup;
- Configurar a ferramenta de backup e os devidos clientes;
- Testar o backup e a restauração;
- Criar notificações e relatórios;
- Verificar periodicamente os relatórios gerados pela ferramenta de backup;
- Restaurar os backups em caso de necessidade;
- Gerenciar mensagens e logs diários dos backups, tratando os erros de forma que o procedimento de backup tenha sequência e os erros na sua execução sejam eliminados;
- Fazer manutenções periódicas dos dispositivos de backup;
- Comunicar aos solicitantes os erros e ocorrências nos backups.

4.2.3 Presidência, Diretoria Executiva e o Comitê Gestor de Proteção de Dados Pessoais estão comprometidos com uma gestão efetiva da proteção de dados pessoais na empresa. Desta forma, adotam todas as medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua atualização e adequação às necessidades da empresa.