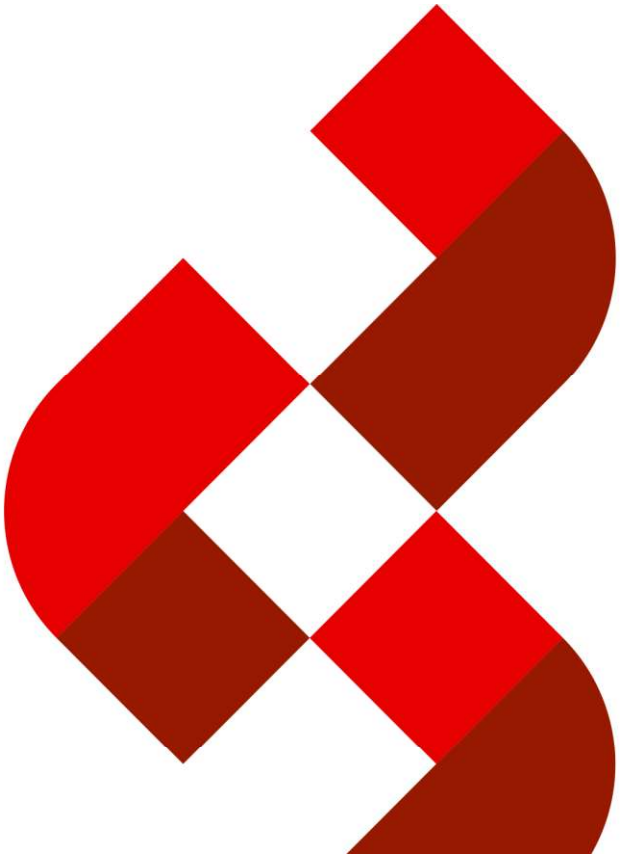
Política de Gestão de Backup



POLÍTICA CORPORATIVA

V1.0

SUMÁRIO

SIGLAS, ABREVIAÇÕES E DEFINIÇÕES

TERMO	DESCRIÇÃO
Ambiente de Produção	Ambiente de uso real que os usuários finais utilizam
Backup	Cópia de segurança
Backup Completo	Tipo de backup em que todos os dados são copiados de forma integral
Backup Diferencial	Tipo de backup em que só são copiados dados novos ou alterados após o último backup completo
Backup Incremental	Tipo de backup em que só são copiados dados novos ou alterados após o último backup realizado, não importando o tipo de backup executado anteriormente
Continuidade de Negócios	Capacidade estratégica e tática da organização de se planejar e responder a incidentes e interrupções de negócios, para conseguir continuar suas operações em um nível aceitável previamente definido
Criptografia	Técnica utilizada para codificar os dados, sendo apenas decifráveis para aqueles que possuem sua decodificação. Evitando o livre acesso aos dados
Custodiante	Pessoa ou grupo que tem a custódia, com o intuito de proteger e guardar
Demandante	Aquele que apresenta a demanda, podendo ser o próprio responsável pelos dados ou um representante
Integridade	Garantia que os dados foram preservados (sem alteração, sem perda)
Janela de Backup	Período de tempo que o backup pode ser executado
Organização	Grupo de pessoas e instalações com uma série de responsabilidades, autoridades e relacionamentos. Exemplo: Companhia, corporação, firma, empresa, instituição de caridade, profissional liberal ou associação, ou partes ou combinações destas
Partes interessadas	Aqueles que possuem algum interesse nos resultados de uma organização
Processo	Atividade ou conjunto de atividades executados por uma organização que produzem ou suportem um ou mais produtos ou serviços
Restore	Restauração do backup realizado (restauração das cópias de segurança)

RPO - *Recovery Point Objective*	Significa *Recovery Point Objective* ou objetivo de ponto de recuperação, em português. Esse indicador define a janela de perda aceitável do ponto em que um evento crítico ocorre até o último processo de backup anterior realizado com sucesso. Ou seja, o RPO acaba medindo, então, a frequência com que o setor realiza as cópias de segurança.
RTO - *Recovery Time Objective*	Significa *Recovery Time Objective* ou objetivo de tempo de recuperação, em português. O indicador mede o período máximo em que um sistema ou uma informação pode ficar indisponível após uma falha sem causar danos significativos para o negócio, além disso, mede o intervalo necessário para restaurar os dados e a operação normal dos sistemas.
Sanitização	Aplicação de técnicas físicas e lógicas para realizar a limpeza dos dados que tornam a recuperação inviável
TIC	Tecnologia da Informação e Comunicação

1. INTRODUÇÃO

1.1. RESUMO

O documento Política de Gestão de Backup visa descrever as diretrizes necessárias para prover o suporte aos requisitos da RTM em relação ao ciclo de vida das cópias de segurança.

1.2. APLICAÇÃO

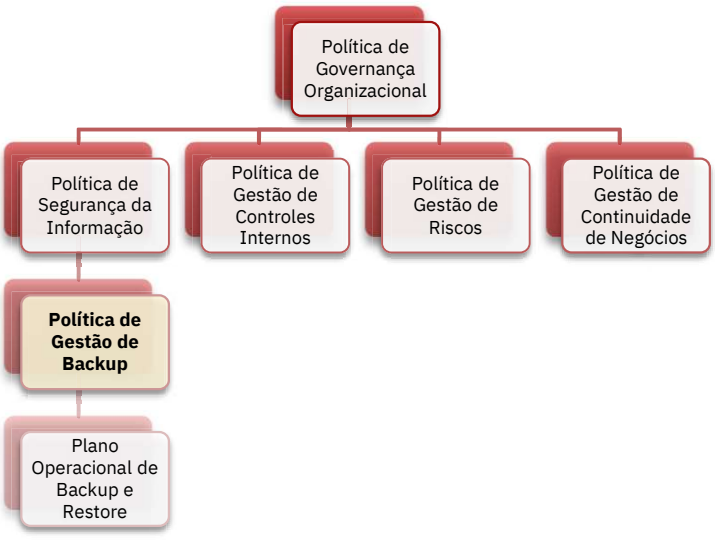
Em todo Grupo RTM.

1.3. REQUISITOS ESTATUTÁRIOS E REGULAMENTARES

- ABNT NBR **ISO/IEC 27.002** (Código de prática para controles de segurança da informação)
- ABNT **NBR 16167** (Diretrizes para classificação, rotulação, tratamento e gestão da informação)
- **COBIT 2019** (Objetivos de controle de informação e tecnologia relacionada)
- BACEN **Resolução 4893** (Política de segurança cibernética para instituições autorizadas pelo Banco Central)
- **LEI 13.709/18** (Lei geral de proteção de dados - LGPD)
- **NIST SP 800-53** (Controles de segurança e privacidade para sistemas de informação)
- **NIST SP 800-61** (Guia de tratamento de incidentes de segurança)
- **NIST SP 800-209** (Diretrizes de segurança para infraestrutura de armazenamento)
- **PCI DSS v3.2.1** (Padrão de segurança de dados da indústria de cartões de pagamento)
- **SWIFT SIP v3** (Programa de segurança do cliente da Sociedade de Telecomunicações Financeiras Interbancárias Mundiais)

1.4. DOCUMENTAÇÃO NORMATIVA DE REFERÊNCIA

A Política de Gestão de Backup está alinhada às demais políticas da organização, dentre as quais destacamos as seguintes:



2. PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades definidos nessa Política de Gestão de Backup descrevem as funções exercidas pelos colaboradores da RTM que atuam diretamente neste processo.

2.1. Diretoria de Operações

Compete a Diretoria de Operações a função de **direcionadora estratégica**, além das seguintes atribuições:

- Estabelecer as diretrizes para a gestão do backup;
- Estabelecer e comunicar formalmente os papéis, responsabilidades e níveis de autoridades da estrutura de gestão do backup.

2.2. Comitê Executivo de TIC

Compete ao Comitê Executivo de TIC a função de **aprovador**, além das seguintes atribuições:

- Definir os serviços críticos onde o backup deve ser executado, de acordo com o GCN – Gestão de Continuidade de Negócios;
- Aprovar a Política de Backup.

2.3. Gerência de Infraestrutura de TI

Compete a Gerência de Infraestrutura de TI as funções de **proprietária e gestora do processo**, além das seguintes atribuições:

- Assegurar o envolvimento de colaboradores qualificados no estabelecimento, implementação e manutenção dos procedimentos e processos de backup e recuperação de dados;
- Definir ferramentas e tecnologias que serão usadas na gestão do backup;
- Elaborar e manter os Planos e Procedimentos Operacionais de Backup e Restore;
- Definir estratégia de backup;
- Gerenciar todo o ciclo de vida do backup.

2.4. Gerência de Governança de TIC

- Identificar e analisar os requisitos legais e regulatórios;
- Identificar gap's de qualidade do processo de backup;
- Identificar e analisar atividades de controles internos de TIC;
- Garantir a revisão periódica dos serviços críticos.

2.5. Gerência de Segurança da Informação

- Especificar os requisitos para proteção e retenção dos dados;
- Definir os mecanismos de segurança da informação para serem implementados.

2.6. Administrador de Backup

Compete ao colaborador ou equipe técnica, parte integrante da Gerência de Infraestrutura de TI, a responsabilidade pela política e asseguração do cumprimento das normas complementares aplicáveis, além das seguintes atribuições:

- Execução dos procedimentos relativos aos serviços de backup e restauração;
- Armazenamento e monitoramento das mídias;
- Configuração da ferramenta de backup;
- Criação de notificações e relatórios.

2.7. Demandante

- Informar os dados a serem copiados;
- Informar os dados a serem recuperados;
- Aprovar estratégia de backup.

3. OBJETIVOS

A Política de Gestão de Backup estabelece e descreve as diretrizes para o gerenciamento do backup, segurança, integridade, proteção e disponibilidade dos dados sob a guarda da RTM, visando também o alinhamento com o GCN – Processo de Gestão de Continuidade de Negócios.

4. METODOLOGIA

A metodologia de Gestão de Backup implantada na RTM baseia-se nos princípios apresentados no item 1.3 – requisitos estatutários e regulamentares – e tem como objetivo garantir a continuidade do negócio em casos na ocorrência de eventos que possam impactar os dados do ambiente operacional.

Figura 1 - Ciclo de vida da gestão de backup

5. ESCOPO

Esta Política de Gestão de Backup engloba os sistemas, aplicativos e dados críticos sob a responsabilidade da RTM, mas não limitando-se a estes:

- Serviços corporativos;
- Sistemas que suportam as mensagens SWIFT;
- Arquivos de trilha de auditoria;
- Serviços fornecidos aos clientes em que a responsabilidade pelo backup é da RTM;
- Serviços e informações internas da RTM em que o backup é necessário.

6. DIRETRIZES GERAIS

6.1. Processo de Backup

6.1.1. Planejamento

- Os Planos Operacionais de Backup e Restore devem ser elaborados em conformidade com as leis vigentes envolvidas e com o contrato do serviço solicitado;
- Devem ser elaborados os Planos Operacionais de Backup e Restore para, no mínimo, os serviços classificados como críticos pela RTM;
- Os Planos Operacionais de Backup e Restore devem possuir, no mínimo, os seguintes itens:
  - Escopo;
  - Papéis e responsabilidades definidos;
  - Locais de armazenamento (principal e alternativo);
  - Requisitos de segurança da informação;
  - Estratégia de backup.
- A estratégia deve contemplar os requisitos abaixo:
  - Tipo de backup (completo e incremental);
  - Frequência;
  - Tipos de mídias a serem utilizadas;
  - Número de cópias;
  - Tempo de retenção.
- O período de execução do backup (janela) deve ser acordado entre as partes interessadas;
- O tipo de backup (completo e incremental) deve ser acordado entre as partes, além de respeitar os limites funcionais das ferramentas e tecnologias;
- O tipo de criptografia a ser implementada deve estar em conformidade com as leis vigentes envolvidas e com o contrato de serviço solicitado;
- No Plano Operacional de Backup e Restore deve estar definido a retenção do backup em conformidade com as leis vigentes envolvidas e com o contrato de serviço;
- No Plano Operacional de Backup e Restore deve estar definido a periodicidade dos testes, conforme acordado com o responsável pelos dados;
- A Gerência de Infraestrutura de TI será a responsável por definir, manter e utilizar as ferramentas e tecnologias envolvidas na execução do backup e da recuperação de dados;
- As ferramentas e tecnologias, implantadas e mantidas pela Gerência de Infraestrutura de TI, devem gerar log's para trilha de auditoria, no mínimo:
  - Na finalização da execução do backup;

- Na falha da execução do backup;
- Na finalização da execução da recuperação de dados;
- Na falha da execução da recuperação de dados.

- As ferramentas e tecnologias devem, preferencialmente, ser de funcionamento automatizado;
- Os Planos Operacionais de Backup e Restore devem ser aprovados pelos responsáveis dos dados;
- Todos os Planos Operacionais e Procedimentos de Backup devem ser revisados anualmente.

6.1.2. Execução das Rotinas

- Deve-se executar as rotinas conforme estratégia de backup definida;
- A execução do backup não deve impactar operacionalmente na produção;
- O backup deve ser protegido utilizando meios de segurança, como por exemplo a criptografia;
- Deve-se implementar criptografia nos arquivos de backup que contenha dados que necessitem de confidencialidade e/ou que sejam críticos;
- O backup deve ser classificado para melhor determinar sua proteção;
- A execução das rotinas deve atender às metas de recuperação do negócio;
- Pode ocorrer execução de backup fora de sua programação pré-definida, caso seja necessário e a solicitação seja aprovada, ou em casos de eventos de gatilhos pré-definidos.

6.1.3. Armazenamento

- Devem ser definidos os locais de armazenamento, tanto o local principal como o alternativo;
- Os locais de armazenamento devem estar em conformidade com as leis vigentes envolvidas e com o contrato de serviço solicitado;
- A escolha, dos locais de armazenamento, deve levar em consideração o prazo de recuperação de dados;
- Os locais de armazenamento devem seguir, minimamente, os seguintes requisitos para proteção física e ambiental:
  - Controles de acesso físico;
  - Proteção contra incêndio;
  - Proteção contra enchentes;
  - Controle de umidade e temperatura;

- Outros requisitos devem ser definidos no Plano Operacional de Backup e Restore, em conformidade com as leis vigentes envolvidas e com o contrato do serviço solicitado.

- O local de armazenamento alternativo deve possuir uma distância suficiente para evitar ser atingido por um desastre que possa acontecer no local principal;
- Os locais de armazenamento devem ser acessíveis;
- Deve-se listar o pessoal autorizado a ser custodiante das mídias de backup
  - Considerar no ambiente da RTM e, também, no percurso até ao local de armazenamento.
- As mídias devem ser classificadas e rotuladas de acordo com o seu grau de criticidade;
- Deve-se implementar mecanismos de rastreabilidade do backup:
  - Rótulos;
  - Catálogo de backup;
  - Monitoramento do trajeto da mídia;
  - Relatório de transporte;
  - Entre outros.
- Deve-se testar a segurança dos locais de armazenamento.

6.1.4. Monitoramento

- As rotinas de backup devem ser monitoradas periodicamente e o status de realização do monitoramento deve ser registrado (log's de eventos de backup);
- Em caso de falhas, rotinas de backup malsucedidas, deve-se:
  - Gerar um alerta para verificação do evento (registro de incidente na ferramenta de chamados técnicos), onde cada situação deve ser analisada e as tomadas de decisões devem ser baseadas nos requisitos definidos entre a equipe de backup e o responsável pelos dados;
  - Executar um novo backup.

6.1.5. Testes

- Os arquivos de backup devem ser testados periodicamente, conforme definido no Plano Operacional de Backup e Restore, para garantir a confiabilidade e integridade dos dados armazenados;
- Deve-se realizar os seguintes tipos de testes:
  - Testes de restauração em ambiente distinto do ambiente de produção;
  - Testes de confiabilidade e integridade;
  - Ao realizar os testes, o tempo de restauração deve ser identificado e registrado.

6.1.6. Recuperação dos Dados

- A recuperação de dados deve ser solicitada pelo responsável dos dados ou por outros com a aprovação dele;
- Toda execução de recuperação de dados deve ser registrada e mantida;
- O serviço de backup deve ser orientado para a restauração das informações no menor tempo possível, principalmente em casos de indisponibilidade de serviços que dependam dessa operação;
- O tempo máximo de restauração dos serviços ofertados e hospedados será definido no Plano de Backup juntamente com os administradores de backup e responsáveis pelos dados;
- A restauração deverá ocorrer em local diferente do ambiente original, sempre que possível, de modo a evitar falhas no processo.

6.2. Procedimentos

- Os procedimentos operacionais de backup devem ser:
  - Elaborados, atualizados, mantidos e disponibilizados;
  - Descritos de forma detalhada (execução, armazenamento, transporte, testes e restauração);
  - Disponibilizados para os principais envolvidos na operação.
- Convém que os procedimentos de backup sejam atualizados quando houver:
  - Novos produtos ou serviços corporativos desenvolvidos;
  - Novas aplicações desenvolvidas;
  - Novos módulos de ERP instalados;
  - Novos locais de armazenamento de dados ou arquivos;
  - Novas instalações de bancos de dados;
  - Outras informações que necessitem de proteção através de backups deverão ser informadas ao Administrador de Backup.

6.3. Treinamento e Conscientização

- Todos os colaboradores intervenientes devem estar cientes da relevância e importância de suas atividades dentro do processo de Gerenciamento do Backup;
- Deverão ser realizados treinamentos para toda equipe de backup, de acordo com suas responsabilidades dentro do processo.

ANEXOS

I. Matriz de papéis e responsabilidades (RACI)