PORTOSRIO
DIRETORIA ADMINISTRATIVO FINANCEIRA
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO
GERÊNCIA DE OPERAÇÃO DE SOLUÇÕES

Documento nº 9548656/2025/GERSOL-PORTOSRIO/SUPTIN-PORTOSRIO/DIRAFI-PORTOSRIO

Rio de Janeiro, na data da assinatura.

Processo nº 50905.000514/2020-00

Interessado: Gerência de Operação de Soluções

POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS

1. OBJETIVO

1.1. Estabelecer diretrizes para o processo de armazenamento, backup e restauração das informações relevantes na rede corporativa da PortosRio, visando garantir a sua integridade, disponibilidade e autenticidade.

2. ABRANGÊNCIA

2.1. Esta política aplica-se a todos os dados críticos da PortosRio, incluindo aqueles armazenados em serviços externos de nuvem pública ou privada, bem como aos agentes públicos e terceiros que criam, processam, acessam ou armazenam esses dados por meio dos sistemas e equipamentos de TI da Instituição.

2.2. A proteção dos dados digitais pertencentes aos serviços de TI da PortosRio, mas gerenciados ou armazenados por entidades externas, sejam públicas ou privadas, como nos casos de serviços em nuvem, deve ser garantida por meio de cláusulas específicas nos acordos ou contratos que formalizam a relação entre as partes envolvidas.

2.3. Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora do centro de processamento de dados mantido pela GERSOL, ficando sob a responsabilidade do indivíduo que usa esses dispositivos.

2.4. Os serviços de armazenamento e backup da PortosRio são destinados exclusivamente ao uso corporativo, sendo passíveis de auditoria. Dados pessoais ou não relacionados às atividades institucionais não devem ser armazenados nos repositórios disponibilizados pela Companhia. Caso sejam identificados, esses dados poderão ser removidos sem aviso prévio.

3. TERMOS E DEFINIÇÕES

3.1. No âmbito do presente normativo, considera-se:

3.1.1. **Ativo crítico**: Equipamento físico, unidade de armazenamento e dados que possuem elevada importância para a continuidade das atividades e serviços e concretização dos objetivos da organização.

3.1.2. **Backup**: 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.

3.1.3. **Backup completo:** Modalidade de backup em que todos os dados a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de

armazenamento, independentemente de terem sido ou não alterados desde o último backup.

3.1.4. **Backup incremental:** Modalidade de backup em que são salvaguardados apenas os dados novos ou modificados desde o último backup de qualquer modalidade efetuado.

3.1.5. **Backup diferencial:** Modalidade de backup em que são salvaguardados apenas dados novos ou modificados desde o último backup completo efetuado;

3.1.6. **Caminho na rede:** Especifica uma localização única em um sistema de arquivos.

3.1.7. **Cloud server:** Servidor de dados e/ou aplicações executado a partir de um ambiente virtual, instalado nas dependências de um provedor desse tipo de serviço e acessado a partir da internet.

3.1.8. **Criticidade**: Grau de importância dos dados para a continuidade das atividades e serviços da organização.

3.1.9. **Dado Pessoal:** Informação relacionada à pessoa natural identificada ou identificável.

3.1.10. **Descarte**: Eliminação correta de dados, documentos, unidades de armazenamento e acervos digitais.

3.1.11. **Diretório ou pasta:** Estrutura lógica utilizada para organizar arquivos em um computador.

3.1.12. **Disco Rígido:** Chamado também de HD, é a parte do computador onde são armazenados os dados.

3.1.13. **Disponibilidade**: Propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados.

3.1.14. **Esquema de backup:** Conjunto de procedimentos que incluem metodologias, softwares e equipamentos integrados de modo a garantir o armazenamento de cópias de segurança dos servidores, arquivos e aplicações.

3.1.15. **Gestor da informação:** Agente público formalmente responsável pela administração de serviço de TI e pelas informações produzidas em seu processo de trabalho.

3.1.16. **Imagem de backup:** Arquivo gerado pela solução de backup, não necessariamente no formato original dos arquivos que contêm os dados salvaguardados.

3.1.17. **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.

3.1.18. **Janela de backup:** Período de tempo durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas.

3.1.19. **Mídia**: Mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação - inclui discos ópticos, magnéticos, CDs, fitas e papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos.

3.1.20. **Plano de Continuidade de Negócios (PCN):** Documentação dos procedimentos e das informações necessárias para que os órgãos ou entidades da administração pública federal mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, em um nível previamente definido, em caso de incidente.

3.1.21. **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.

3.1.22. **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.

3.1.23. **Restauração ou Restore:** É o procedimento de recuperação de dados e aplicações a partir de uma cópia de segurança previamente armazenada.

3.1.24. **Retenção**: Período de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração.

3.1.25. **Rotina de backup:** Procedimento utilizado para se realizar um backup.

3.1.26. **Serviço de TI:** Provimento de serviços de desenvolvimento, de implantação, de manutenção, de armazenamento e de recuperação de dados e de operação de sistemas de informação, projeto de infraestrutura de redes de comunicação de dados, modelagem de processos e assessoramento técnico necessários à gestão da informação

3.1.27. **Servidor:** Sistema de computação centralizada que fornece serviços a uma rede de computadores.

3.1.28. **Storage**: Equipamento composto por conjuntos de discos magnéticos, especializado no armazenamento e disponibilização de grandes volumes de dados.

3.1.29. **Tempo de retenção:** Período de tempo em que o conteúdo da mídia de backup deve ser preservado.

3.1.30. **Unidade de armazenamento:** Dispositivo para armazenamento de dados em suporte digital.

3.1.31. **Unidade de armazenamento de backup**: Unidade de armazenamento com características específicas para retenção de cópia de segurança de dados digitais.

4. REFERÊNCIAS LEGAIS E NORMATIVAS

4.1. O presente normativo fundamenta-se nas seguintes referências legais e normativas:

4.1.1. Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos;

4.1.2. Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;

4.1.3. Lei Nº 13.709, de 14 de agosto 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);

4.1.4. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação e Comunicações na Administração Pública Federal;

4.1.5. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

4.1.6. Decreto nº 11.856, de 26 de dezembro de 2023;

4.1.7. Portaria SGD/MGI nº 852, de 28 de março de 2023;

4.1.8. Lei nº 12.527, de 18 de novembro de 2011; e

4.1.9. Ferramentas do Framework do PPSI: Modelo de Política de Backup Versão 2.0.

5. DIRETRIZES

5.1. **Dos princípios gerais:**

5.1.1. A Política de Backup e Restauração de Dados deve estar alinhada com à Política de Segurança da Informação da PortosRio e com uma gestão de continuidade de negócios em nível organizacional.

5.1.2. As rotinas de backup devem:

I - Ser orientadas para a restauração dos dados no menor tempo possível, sobretudo, quando da indisponibilidade de serviços de TI;

II - Utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada; e

III - Possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da Organização.

5.1.3. Os serviços e ativos de TIC críticos da PortosRio devem ser formalmente elencados pelo Comitê de Gestão de Tecnologia da Informação e Comunicação (CGTIC) da Companhia.

5.1.4. As seguintes soluções e suas respectivas bases de dados são previamente classificadas como ativos críticos na PortosRio:

I - Sistema de Gestão Portuária;

II - Sistema de Gestão de Pessoal e de Gestão Empresarial/Financeira;

III - Site Institucional; e

IV - Portal de Intranet.

5.1.5. Os sistemas desenvolvidos ou fornecidos à PortosRio devem ser entregues com documentação detalhada que descreva as melhores práticas de backup aplicáveis, assegurando sua conformidade com as diretrizes de segurança e continuidade operacional da organização.

5.2. **Das ferramentas de backup:**

5.2.1. As ferramentas de backup devem ser compatíveis com os sistemas operacionais, aplicações e dispositivos existentes no ambiente organizacional.

5.2.2. Os ativos envolvidos no processo de backup são considerados ativos críticos para a Organização.

5.2.3. As ferramentas devem ser avaliadas periodicamente para assegurar o atendimento aos requisitos organizacionais.

5.3. **Da frequência e retenção dos dados:**

5.3.1. Os backups dos serviços de TI críticos da PortosRio devem ser realizados utilizando-se as seguintes frequências temporais:

I - Diária;

II - Semanal;

III - Mensal; e

IV - Anual.

5.3.2. Os backups dos serviços de TI críticos e não críticos da PortosRio devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/ retenção de dados estabelecida a seguir:

I - Diária: Retenção de 7 dias.

II - Semanal: Retenção de 4 semanas.

III - Mensal: Retenção de 12 meses.

IV - Anual: Retenção de 2 anos.

5.3.3. Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.

5.3.4. A solicitação de salvaguarda dos dados referentes aos serviços de TI, críticos e não críticos, deve ser realizada pelo gestor das informação, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

I - Escopo ou abrangência (dados digitais a serem salvaguardados);

II - Tipo de backup (completo, incremental, diferencial);

III - Frequência temporal de realização do backup (diária, semanal, mensal, anual);

IV - Retenção;

V - RPO - Objetivo do Ponto de Recuperação; e

VI - RTO - Objetivo de tempo de recuperação.

5.3.5. A alteração das frequências e tempos de retenção pré-estabelecidos para os serviços de TI deverá ser precedida de solicitação e justificativa formais encaminhadas à Superintendência de Tecnologia da Informação - SUPTIN. A execução da alteração estará condicionada à aprovação prévia do CGTI.

5.3.6. Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

5.3.7. A GERSOL deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados da PortosRio, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da organização.

5.3.8. Salvo indicação em contrário, o backup dos dados será feito de acordo com o Plano de backup disposto no **Anexo I (9222589)** para minimizar interferências nas operações da PortosRio.

5.4. **Das unidades de armazenamento de backups:**

5.4.1. As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:

I - A criticidade do dado salvaguardado;

II - O requisito de segurança da informação;

III - O tempo de retenção do dado;

IV - A probabilidade de necessidade de restauração;

V - O tempo esperado para restauração;

VI - O custo de aquisição da unidade de armazenamento de backup;

VII - A vida útil da unidade de armazenamento de backup.

5.4.2. A GERSOL deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

5.4.3. Podem ser utilizadas técnicas de compressão de dados, desde que o acréscimo no tempo de recuperação dos dados seja considerado aceitável pelos gestores das informações.

5.4.4. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

5.4.5. As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade e temperatura, uso de criptografia e com acesso restrito a pessoas autorizadas pela GERSOL.

5.4.6. Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

5.5. **Da recuperação de dados (restauração):**

5.5.1. A solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através de abertura de chamado técnico.

5.5.2. O chamado técnico deve conter, ao menos, a identificação do usuário, dos dados a serem recuperados, sua localização, a data da versão que deseja recuperar, o local alternativo para o armazenamento (quando couber) e a justificativa para recuperação.

5.5.3. A recuperação de dados não será viabilizada em caso de perdas anteriores à conclusão

da cópia de segurança. Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de backup.

5.5.4. A GERSOL terá a prerrogativa de recusar a restauração de dados cujo conteúdo não esteja alinhado às atividades institucionais da PortosRio, sendo assegurado ao demandante o direito de recorrer da negativa junto ao gestor da respectiva unidade.

5.5.5. O prazo estimado para recuperação dependerá do volume e da complexidade dos dados.

5.6. **Dos testes de backup:**

5.6.1. Os backups devem ser testados semestralmente para garantir sua confiabilidade e a integridade dos dados armazenados.

5.6.2. Os testes de restauração do backup devem ser realizados, por amostragem, em equipamentos servidores diferentes dos equipamentos que atendam os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis em cada unidade da PortosRio.

5.6.3. Testes adicionais poderão ser realizados, de forma eventual, em resposta a alterações significativas no ambiente de TIC, como a inclusão de novos servidores, sistemas ou aplicações.

5.6.4. Todos os testes de backup devem ser devidamente documentados, incluindo, no mínimo, as seguintes informações:

I - O tipo de sistema/serviço que teve o seu reestabelecimento testado;

II - A data da realização do teste;

III - O tempo gasto para o retorno do backup; e

IV - Se o procedimento foi concluído com sucesso.

6. PAPÉIS E RESPONSABILIDADES

6.1. **São atribuições da GERSOL:**

6.1.1. Prover, administrar e atualizar continuamente as ferramentas de hardware e software necessárias à realização do backup e restauração, garantindo seu funcionamento ininterrupto.

6.1.2. Criar e manter as tarefas de backup em conformidade com os requisitos legais e operacionais, considerando aspectos de criticidade e tempos de retenção.

6.1.3. Manter as unidades e dispositivos de backup preservados, funcionais, seguros e sujeitos a verificações regulares e manutenções periódicas.

6.1.4. Atualizar as tarefas de backup sempre que houver inclusão ou exclusão de servidores e/ou aplicações, conforme solicitação formal do Gestor da Informação.

6.1.5. Realizar a restauração de backups mediante abertura de chamado, seguindo prazos e procedimentos estabelecidos.

6.1.6. Estabelecer e revisar periodicamente os procedimentos de backup e restauração, incluindo a execução regular de testes de recuperação.

6.1.7. Gerenciar e auditar os registros de logs dos backups, com análise diária e geração de relatórios.

6.1.8. Reportar imediatamente à SUPTIN e a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR quaisquer incidentes que causem indisponibilidade ou falhas nos processos de backup ou restauração.

6.2. **São atribuições do Gestor da Informação:**

6.2.1. Solicitar, formalmente, a salvaguarda das informações geridas e dar anuência à solicitação feita pela área técnica para recuperação de dados;

6.2.2. Validar, negocialmente, o resultado das restaurações eventualmente solicitadas; e

6.2.3. Validar, negocialmente, o resultado dos testes de restauração dos backups.

6.3. **São responsabilidades de todos os empregados da PortosRio:**

6.3.1. Garantir que todos os arquivos relevantes ao desenvolvimento de suas atividades laborais sejam armazenados exclusivamente nos diretórios designados para o seu respectivo setor.

6.3.2. Solicitar, mediante abertura de chamado técnico, a restauração de arquivos danificados ou que foram equivocadamente apagados.

6.3.3. Responsabilizar-se pelo backup de dados pessoais, eventualmente, armazenados nas estações de trabalho da PortosRio.

7. VIOLAÇÃO DA POLÍTICA, ADVERTÊNCIA E PUNIÇÕES

7.1. O descumprimento da POSIC poderá acarretar responsabilização, nos termos do IN ASSIND 01.012 e demais regulamentos da PortosRio e nos termos dos contratos ou convênios para estagiários, menores aprendizes, empresas prestadoras de serviço e seus empregados, sem prejuízo das responsabilidades civis e penais eventualmente cabíveis.

8. CONSIDERAÇÕES FINAIS

8.1. A Política de Backup e Restauração de dados deverá ser aprovada pela Diretoria Executiva da PortosRio.

8.2. A Política de Backup e Restauração de dados deverá ser formalmente publicada por Resolução e aplicada a todos os usuários de recursos informatizados da PortosRio.

8.3. A Política de Backup e Restauração de dados deverá ser atualizada a cada três anos, objetivando refletir os avanços tecnológicos e as alterações dos ambientes interno e externo.

9. ANEXOS

9.1. Anexo I - Plano de Backup (9546582).

Rua Dom Gerardo 35, 10º andar - Edifício Sede - Bairro Centro
Rio de Janeiro/RJ, CEP 20090-905
Telefone: 2122198600 - www.portosrio.gov.br