Governo do Estado de São Paulo
Fundação Centro de Atendimento Socioeducativo ao Adolescente
ATI - Assessoria de Tecnologia da Informação

INSTRUÇÃO

Nº do Processo: 161.00062941/2025-13

Interessado: FUNDAÇÃO CASA, ATI - Assessoria de Tecnologia da Informação

Assunto: Política de Backup e Recuperação de Dados

Responsável	Assessoria de Tecnologia da Informação - ATI
Aprovado por:	Gabinete da Presidência.
Políticas Relacionadas	Política de Governança de TI, Política de Segurança da Informação, Política de Uso Aceitável de TI, Política de Serviços de Mensageria e Telefonia, Política de Gestão de Acessos, Política de Continuidade Operacional de TI
Localização de armazenamento	Processo SEI 161.00062941/2025-13
Data da Aprovação	Data da Assinatura
Data de revisão	
Versão	1.0

1- INTRODUÇÃO

1.1 - 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 Assessoria de Tecnologia da Informação (ATI) e formalmente definidos como de necessária salvaguarda na Fundação CASA-SP, 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.

2 - ESCOPO

2.2 Esta política se aplica a todos os dados no âmbito da Fundação CASA-SP, incluindo dados fora da Fundação CASA-SP armazenados em um serviço de nuvem Pública ou Privada.

2.3 Esta política se aplica a todos que podem ser criadores e/ou usuários de tais dados. A política

também se aplica a terceiros que acessam e usam na Fundação CASA-SP sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade da Fundação CASA-SP.

2.4 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).

2.5 A salvaguarda dos dados em formato digital pertencentes a serviços de TI da Fundação CASA-SP, 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.

3- TERMOS E DEFINIÇÕES

3.1 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;

3.2 CUSTO DIANTE 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;

3.3 ELIMINAÇÃO - Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

3.4 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;

3.5 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;

3.6 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;

3.7 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.

4- REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

Orientação	Seção

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
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

CAPÍTULO I - DECLARAÇÕES DA POLÍTICA

Artigo 1º A Política de Backup e Restauração de Dados deve estar alinhada com à **Política de Segurança da Informação** e à **Política de Continuidade Operacional de TI** da Fundação CASA-SP.

CAPÍTULO II - DAS ROTINAS DE BACKUP

Artigo 2º As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

Artigo 3º As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

Artigo 4º As rotinas de backup devem 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.

CAPÍTULO III - DO ARMAZENAMENTO DE BACKUP

Artigo 5º O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um sítio de backup em um local remoto ao da sede da Fundação CASA-SP para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.

Artigo 6º A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.

Artigo 7º Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup, conforme disponibilidade.

CAPÍTULO IV - DA FREQUÊNCIA E RETENÇÃO DOS DADOS

Artigo 8º O recurso de cópia de sombra de ser ativado pela ATI nos servidores de arquivos, permitindo o salvamento das versões anteriores dos arquivos no mínimo em três horários distintos do dia.

Artigo 9º Devem ser realizados dois tipos de backup: backup completo (conhecido como backup full) e backups incrementais (que salvam as alterações feitas a partir da última versão armazenada no backup completo).

Seção I - Dos servidores de arquivo (File Servers)

Artigo 10 Devem ser realizados backups dos servidores de arquivo (file servers).

§ 1º - A política para os File Servers compreende rotinas executadas no software de backup:

I. um backup completo aos finais de semana ou enquanto durar a execução em todos os servidores.

II. backups incrementais executados entre terça-feira e quinta-feira.

§ 2º - Os backups dos File Servers devem ser armazenados em fitas LTO.

§ 3º - Tempo mínimo de retenção:

I. Backups semanais – 4 meses.

II. Backups mensais – 1 ano.

III. Backups anuais – 5 anos.

Seção II - Das máquinas virtuais (VMs)

Artigo 11 Devem ser realizados backups das máquinas virtuais.

§ 1º - As máquinas virtuais críticas deverão ser clonadas (cópia completa) por meio de recurso disponível, com rotina de execução durante o final de semana:

I. Controladores do Domínio;

II. Servidores de DNS;

III. Servidores de Aplicação;

IV. Servidores de Impressão;

V. Servidores Web;

VI. Servidores de Banco de Dados;

VII. Serviços de monitoramento do ambiente.

§ 2º - Os backups das máquinas virtuais devem ser armazenados em storage de backup.

§ 3º - Tempo mínimo de retenção:

I. Backups semanais – 3 semanas.

Seção III- Dos bancos de dados.

Artigo 12 Devem ser realizados backups dos bancos de dados.

§ 1º - A política para os Bancos de Dados compreende rotinas executadas no software de backup:

I. um backup completo aos finais de semana ou enquanto durar a execução em todos os servidores.

II. backups incrementais executados entre segunda-feira e sexta-feira.

§ 2º - Os backups dos Bancos de Dados devem ser armazenados em fitas LTO.

§ 3º - Na rotina dos bancos de dados, são salvos os arquivos de bancos de dados e logs armazenados nos servidores.

§ 3º - Tempo mínimo de retenção:

I. Backups semanais – 4 meses.

II. Backups mensais – 1 ano.

III. Backups anuais – 5 anos.

Seção IV - Dos servidores web e de aplicações

Artigo 13 Devem ser realizados backups dos servidores web e de aplicações.

§ 1º - A política para os servidores web e de aplicações compreende rotinas executadas no software de backup:

I. um backup completo aos finais de semana ou enquanto durar a execução em todos os servidores.

II. backups incrementais executados entre segunda-feira e sexta-feira.

§ 2º - Os backups dos servidores web e de aplicações devem ser armazenados em fitas LTO.

§ 3º - Na rotina estão inclusos arquivos e recursos críticos que possibilitem a restauração do serviço ou a recuperação de informações relevantes para as áreas responsáveis.

§ 3º - Tempo mínimo de retenção:

III. Backups semanais – 4 meses.

IV. Backups mensais – 1 ano.

V. Backups anuais – 5 anos.

Artigo 14 Os ativos envolvidos no processo de backup são considerados ativos críticos para a Fundação CASA-SP.

Artigo 15 A solicitação de salvaguarda dos dados, alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas à ATI. A aprovação para execução da alteração depende da anuência do Gabinete da Presidência.

Artigo 16 A solicitação de salvaguarda dos dados referentes aos serviços de TI deve ser realizada pelo gestor, com a anuência prévia e formal da Executiva vinculada (DGA, DGAR, AEPS ou Gabinete da Presidência), refletindo os requisitos de negócio da Fundação CASA-SP, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da Fundação CASA-SP, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

I – Escopo (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;

VI – RTO.

Artigo 17 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.

Seção V - Do uso da rede

Artigo 18 Fica definido como administrador de backup a Seção de Segurança da Informação.

Artigo 19 O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados da Fundação CASA-SP, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da Fundação CASA-SP.

Artigo 20 A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.

Artigo 21 O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com a Gerência de Infraestrutura e Segurança da Informação.

Seção VI - Do transporte e armazenamento

Artigo 22 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 tempo de retenção do dado;

III - A probabilidade de necessidade de restauração;

IV – O tempo esperado para restauração;

V – O custo de aquisição da unidade de armazenamento de backup;

VI – A vida útil da unidade de armazenamento de backup.

Artigo 23 O administrador de backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

Artigo 24 Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelos gestores das informações.

Artigo 25 A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

Artigo 26 No caso de contas de e-mail de gestores comissionados, após o desligamento do usuário, transferência ou descomissionamento, será realizado o backup do conteúdo de e-mail o qual deverá ser mantido por, no mínimo, 30 dias, sendo necessária solicitação de disponibilização para a ATI durante esse período.

§1º Após esse período a conta e os arquivos poderão ser excluídos a qualquer tempo.

§2º O backup será salvo no computador local do gestor da área.

§3º A solicitação de backup será submetida para aprovação do Gabinete da Presidência.

Artigo 27 Não será realizado backup de conta de e-mails departamentais que extrapolarem o limite de 100% da capacidade de armazenamento.

Artigo 28 Não será realizado no servidor backup de conta de e-mails pessoais que extrapolarem o limite de 100% da capacidade de armazenamento, sendo armazenado o backup apenas no computador local.

Artigo 29 As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas pelo administrador de backup. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

Artigo 30 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.

Artigo 31 As fitas de backup serão transportadas e armazenadas conforme descrito:

I. Todos os novos backups serão gravados em fitas LTO.

II. A mídia será claramente identificada e armazenada em uma área segura acessível apenas para a equipe da ATI.

III. A mídia não será deixada sem supervisão durante o transporte.

Seção VII - Dos testes de backup

Artigo 32 Os backups serão verificados periodicamente:

I - Os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.

II - Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha.

III- Os testes de restauração dos backups devem ser realizados, por amostragem, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar backups bem-sucedidos.

Seção VIII -Procedimento de restauração de backup

Artigo 33 O atendimento de solicitações de restauração de arquivos, e-mails e demais formas de dados deverá obedecer às seguintes orientações:

I. A solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através do Sistema Tarefas, direcionados para Segurança da Informação e Acesso, na subcategoria Recuperação de Arquivos, serviço “Arquivos e Pastas”, incluindo o nome do arquivo, data desejada e o caminho completo do arquivo a ser restaurado e outros detalhes, se houver.

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

III- A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações.

IV O operador de backup terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.

Seção IX- O cronograma de restauração de dados:

Artigo 35 O tempo de restauração, preferencialmente definido em Acordo de Nível de Serviço entre as áreas de negócio e de TIC, é proporcional ao volume de dados necessários para o restore e dependerá janela de backup disponível para a execução da atividade. A cada 100GB de dados, o tempo de restauração é de uma hora. Esta estimativa é do tempo de atendimento da Seção de Segurança da Informação, não contemplando o tempo antes ou após o pedido a equipe.

Seção X - Descarte da Mídia

Artigo 36 A mídia de backup será retirada e descartada conforme descrito neste documento:

I - A Gerência de Infraestrutura e Segurança da Informação garantirá que a mídia não contenha mais imagens de backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados.

II- A Gerência de Infraestrutura e Segurança da Informação garantirá a destruição física da mídia antes do descarte.

CAPÍTULO V - DAS RESPONSABILIDADES

Artigo 37 O administrador de backup e o operador de backup devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.

Artigo 38 São atribuições do administrador de backup:

I. Propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela organização;

II. Providenciar a criação e manutenção dos backups;

III. Configurar as soluções de backup;

IV. Manter as unidades de armazenamento de backups preservadas, funcionais e seguras;

V. Definir os procedimentos de restauração e neles auxiliar.

CAPÍTULO VI - DISPOSIÇÕES GERAIS

Artigo 39 Esta política será revisada periodicamente, conforme a necessidade e evolução das melhores práticas de governança de TI, segurança da informação e mudanças na legislação aplicável.

Artigo 40 Alterações na Política deverão ser submetidas à aprovação do Gabinete da Presidência.

São Paulo, na data da assinatura digital.

Raelen Bego Luiz
Chefe de Gabinete

Leandro Timossi de Almeida
Assessor da Presidência

Documento assinado eletronicamente por **Leandro Timossi de Almeida**, **Assessor da Presidência II**, em 13/03/2025, às 16:25, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Raelen Bego Luiz**, **Chefe de Gabinete**, em 18/03/2025, às 22:30, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0059061990** e o código CRC **E30862CE**.