ORDEM DE SERVIÇO DTI Nº 007/2023

Dispõe sobre a política de realização e rotinas de backup e restauração de dados armazenados no âmbito da Fundação CASA/SP – Centro de Atendimento Socioeducativo ao Adolescente do Estado de São Paulo.

A **Divisão de Tecnologia da Informação (DTI),** no uso das atribuições conferidas a este departamento, junto com suas gerências e seções, resolvem:

Artigo 1º - As regras e diretrizes aqui estabelecidas devem ser seguidas por todos os **USUÁRIOs,** sem quaisquer exceções.

CAPÍTULO I - FUNDAMENTAÇÃO LEGAL E NORMATIVA

Artigo 2º - A presente **OS** está fundamentada nos seguintes instrumentos legais e normativos:

I. Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal, revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991, e dá outras providências;
II. Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;
III. Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;
IV. Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Marco civil da Internet;
V. Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD);
VI. DN CGGDIESP-1, de 30 de dezembro de 2021, que traz boas práticas em segurança da informação, para privacidade e proteção de dados pessoais e para a gestão de dados e informações;
VII. DO SP V132/N259, de 29 de dezembro de 2022; IN PGDI-1, de 27 de dezembro de 2022, referente ao anexo II, 3 - Tabela de Providências Complementares e Responsáveis - Ativos da Informação: Orientação Técnica e Modelo - Inventário de Dados, da Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021;
VIII. Ordens de Serviço publicadas pela Divisão de Tecnologia da Informação (Fundação CASA/SP).

CAPÍTULO II - CONCEITOS E DEFINIÇÕES

Artigo 3º - Para fins desta **OS,** considera-se que:

I. **OS:** Ordem de Serviço;
II. **Divisão de Tecnologia da Informação (DTI):** departamento com a responsabilidade de dispor, gerir e implementar todas as ações de gestão e segurança da informação e comunicações no âmbito institucional;
III. **TIC:** tecnologia da informação e comunicação;
IV. **active directory (AD):** o *Active Directory* é o serviço de diretório da *Microsoft* utilizado para armazenar diversas informações sobre objetos **USUÁRIOs,** grupos, computadores, serviços etc. de uma rede corporativa. Por meio do AD é possível estabelecer um login de acesso único, controlar acessos, imposição de políticas corporativas, distribuição de atualizações e programas etc.;
V. **backupexec:** solução de software de *backup/restore* da empresa *Veritas;*
VI. **netbackup:** solução de software de *backup/restore* da empresa *Veritas;*
VII. **shadow copy (cópia sombra):** recurso disponível em servidores que possibilitam a restauração de arquivos apagados, ou alterados indevidamente, para uma versão anterior;
VIII. **cluster (junção):** sistema onde dois ou mais computadores (nós) trabalham de maneira conjunta para realizar processamento importante, distribuindo carga entre os nós e aumentando a disponibilidade dos serviços. De modo simples, os computadores dividem as tarefas de processamento e trabalham como se fossem um único computador;
IX. **expiração:** é quando termina o prazo de validade da última imagem de backup gravada numa fita;
X. **janela de backup:** é uma quantidade predeterminada de tempo em que os dados específicos devem ser salvos ou restaurados para evitar erros nos backups subsequentes;
XI. **job (rotina):** tarefas do *NetBackup/Backupexec* como cópia, restauração, movimentação, limpeza dos drivers, entre outros;
XII. **library (biblioteca):** uma biblioteca de fitas (padrão LTO), onde as informações são armazenadas;
XIII. **LTO (linear tape-open):** modelo de fita utilizado pelos equipamentos de backup;
XIV. **master server (servidor principal):** é o servidor principal onde fica a gestão dos backups, e as configurações de suas respectivas políticas. No *Master Server* é possível visualizar o andamento dos backups de todos os clientes. As restaurações também são realizadas por meio dele. Esse servidor possui uma base de dados com todas as informações relativas aos backups;
XV. **media server (servidor de mídia):** são servidores de backup que controlam as unidades de armazenamento *(Librarys, Storages,* etc.) e interagem com os clientes;
XVI. **policies (políticas):** rotinas de backup configuradas nos softwares de backup. Nas políticas, estão todas as informações referentes as rotinas de backup, definindo qual informação será salva, quando, em qual intervalo de tempo e onde será armazenada;
XVII. **restore (restauração):** processo de restauração dos arquivos;
XVIII. **retenção:** prazo de armazenamento dos backups efetuados;
XIX. **schedule (agendamento):** configuração do agendamento dos backups;

XX. **storage (armazenamento):** dispositivo com grande capacidade de armazenamento e alta disponibilidade (recursos redundantes para evitar falhas);
XXI. **system state (estado do sistema):** o *System State* é o backup utilizado pelos Sistemas Operacionais com referências e dados críticos e indispensáveis em caso de uma restauração completa do equipamento;
XXII. **TB (terabytes):** unidade de medida utilizada para armazenamento de dados. Equivale a 1024 gigabytes (GB);
XXIII. **VM (virtual machine** ou **máquina virtual):** tem a mesma função de uma máquina física, porém é virtualizada por software em um (ou mais) servidor(es) de maior desempenho, garantindo grande economia de espaço, recursos, energia etc.;
XXIV. **vsphere:** *VMware vSphere* é a plataforma de virtualização de computação da empresa *VMware*, que permite o gerenciamento da estrutura virtualizada, garantindo alta disponibilidade e resiliência para o ambiente computacional;
XXV. **SLA** ou **ANS (service level agreement,** ou **acordo de nível de serviço):** é a formalização referente ao serviço realizado entre as duas partes envolvidas, a empresa contratada e o contratante e/ou o departamento e o colaborador etc.;
XXVI. **administradores de TIC:** são as pessoas designadas formalmente, pela autoridade máxima da **DTI,** com atribuição principal de ser o responsável técnico pelos seus recursos de **TIC;**
XXVII. **USUÁRIO:** é qualquer pessoa, física ou jurídica, com vínculo formal direto ou indireto com a **Fundação CASA/SP,** ou em condição autorizada, que utiliza, de qualquer forma, algum recurso de **TIC** da instituição.

CAPÍTULO III – OBJETIVO

Artigo 4º - Esta **OS** é um documento que engloba as políticas, normas e regras para guiar todo o ciclo do gerenciamento de dados corporativos – como a concepção, retenção e expiração. As informações são os ativos mais valiosos dos nossos tempos, portanto é de suma importância divulgar os procedimentos adotados para a realização do *backup/restore* do ambiente computacional da **Fundação CASA/SP.**

Artigo 5º - Esta **OS** engloba os seguintes itens do processo de cópia:
I. Tipos de backup;
II. Rotinas de backup gerais;
III. Backups especiais;
IV. Tempo de retenção dos backups;
V. Guarda das fitas LTO de backup;
VI. SLA de restauração.

CAPÍTULO IV – DEFINIÇÕES

Artigo 6º - Dos **serviços de backup:**
§ 1º - O serviço de backup tem por objetivo garantir a integridade e disponibilidade das informações produzidas e armazenadas dentro da estrutura computacional da **Fundação CASA/SP.** A estrutura de backup é composta por servidores com softwares específicos para *backup/restore (Netbackup/Backupexec), Storage* para armazenamento das informações e Bibliotecas de Fitas *(Librarys).*

§ 2º - A atual estrutura de backup da instituição está dividida entre as rotinas executadas pelos softwares de *backup/restore* e pelas rotinas de cópias das VMs (que executam serviços críticos) clonadas e armazenadas em uma unidade de armazenamento *(storage)*.
§ 3º - Entre os serviços computacionais salvos em backups (seja em fita LTO ou armazenado em *storage)* temos:

I. Servidores de Arquivos *(File Servers);*
II. Servidores Web (sites e aplicações/sistemas publicados de uso institucional);
III. *Active Directory* (controladores do domínio);
IV. Servidores de Aplicação (produção, homologação e desenvolvimento);
V. Servidores de Bancos de Dados (SQL, MySQL, Base de dados da folha de pagamento, entre outros);
VI. Servidores de DNS;
VII. Servidores e serviços de Impressão;
VIII. Serviços de monitoramento do ambiente;
IX. Serviços de monitoramento e imagens (CFTV).

§ 4º - Como política complementar de backup, o recurso de **cópia de sombra** está ativo nos servidores de arquivos, o que permite a recuperação de arquivos de maneira rápida e prática em situações do dia a dia.

Artigo 7º - Dos **tipos de backup:**
§ 1º - Realiza-se, basicamente, 2 (dois) tipos de backups: **backup completo** (conhecido como *backup full)* e **backups incrementais** (que salvam as alterações feitas a partir da última versão armazenada no backup completo).
§ 2º - As VMs clonadas são cópias completas das máquinas virtuais no dia da execução da rotina.

Artigo 8º - A **DTI** da **Fundação CASA/SP** deverá, a seu critério, monitorar e manter informações e demais dados, para efeito de auditoria, conformidade, diagnóstico de problemas e produção de estatísticas. Essas informações poderão ser disponibilizadas à administração mediante solicitação formal.

CAPÍTULO V – DIRETRIZES

Artigo 9º - Das **políticas de backup:**
§ 1º - As políticas de backup variam conforme o serviço, a necessidade do tempo de retenção e o tipo de armazenamento das informações.

Artigo 10 - Dos **servidores de arquivo *(File Servers):***
§ 1º - A política para os *File Servers* compreende em rotinas executadas no software de backup *Netbackup,* organizadas em um **backup completo** aos finais de semana ou enquanto durar a completa execução em todos os servidores (a fim de garantir a integridade dos dados armazenados) e **backups incrementais** executados entre terça-feira e quinta-feira.
§ 2º - Os backups dos *File Servers* são armazenados em fitas LTO 6 (1,5 TB de armazenamento, podendo chegar a 2,3 TB comprimidas) e posteriormente em fitas LTO 8 (12 TB, podendo chegar a 30TB).
§ 3º - Tempo de **retenção:**

I. Backups semanais – **2 (dois) anos;**
II. Backups mensais e anuais – **5 (cinco) anos.**

Artigo 11 - Das **máquinas virtuais (VMs):**

§ 1º - As máquinas virtuais críticas são clonadas (cópia completa) por meio de recurso disponível no *Vsphere*, com rotina de execução aos sábados. As máquinas atendidas por essa política são:

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 - Tempo de **retenção:**

I. Backups semanais – **2 (dois) anos.**

Artigo 12 - Dos **bancos de dados:**

§ 1º - Assim como nos servidores de arquivos, a política para os bancos de dados compreende em rotinas executadas em software de backup, porém realizado no *Backupexec*, organizadas em um **backup completo** aos finais de semana e **backups incrementais** executados entre segunda-feira e sexta-feira, armazenadas em fitas LTO.

§ 2º - Na rotina dos bancos de dados, são salvos os arquivos de bancos de dados e *logs* armazenados nos servidores, para cada banco armazenado.

§ 3º - Tempo de **retenção:**

I. Backups semanais – **2 (dois) anos;**
II. Backups mensais e anuais – **5 (cinco) anos.**

Artigo 13 - Dos **servidores web** e **de aplicações:**

§ 1º - A política de backup para os servidores web e de aplicações compreende a rotinas executadas no software de backup *Backupexec*, organizadas em um **backup completo** aos finais de semana e **backups incrementais** executados entre segunda-feira e sexta-feira, armazenadas em fitas LTO.

§ 2º - 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 de **retenção:**

I. Backups semanais – **2 (dois) anos;**
II. Backups mensais e anuais – **5 (cinco) anos.**

Artigo 14 - Da **guarda de fitas LTO:**

§ 1º - As fitas LTO já utilizadas são armazenadas em sala fora do *Data Center* em um outro andar no prédio sede da **Fundação CASA/SP,** com acesso restrito aos funcionários da **DTI.** As fitas LTO são armazenadas em armários específicos para essa finalidade.

Artigo 15 – Do **SLA de restauração:**

§ 1º - O atendimento das solicitações de restauração de arquivos e demais recursos devem ser solicitados por meio de chamado registrado devidamente no **Sistema Tarefas,** direcionados para a equipe de **Segurança e Acessos,** na subcategoria **Recuperar Arquivos e Pastas,** incluindo o nome do arquivo, data desejada e o caminho completo do arquivo a ser restaurado e outros detalhes, se houver.

§ 2º - O prazo dependerá do volume de dados a ser restaurado e da janela de backup disponível para a execução da atividade. Em média a execução da atividade leva cerca de 1 (uma) hora a contar do início do processo, porém outros fatores podem aumentar o tempo de execução, como o processo de catalogação das fitas LTO, entre outros.

CAPÍTULO VI – CONFORMIDADE

Artigo 16 – As políticas e projetos de backup institucionais estão em **conformidade** com a **LGPD:**

§ 1º - Transparência e livre acesso: integração do backup com todos os sistemas legados para acesso aos dados de forma rápida e sob demanda, a qualquer momento que o titular possa exigir;

§ 2º - Qualidade dos dados: como padrão, a **DTI** entrega a gestão de dados em seus projetos de backup, podendo garantir que estarão corretos e atualizados e podem ser alterados ou excluídos se o titular desejar;

§ 3º - Segurança contra destruição, perda, alteração ou divulgação: também incluso nas políticas de backup e no armazenamento evitando quebra de informações;

§ 4º - Medidas de prevenção: a **DTI,** com o auxílio de *softwares* de gestão, monitora todo o ambiente de dados e backup 24 horas por dia, 7 dias por semana, de forma proativa para evitar ataques e desastres;

§ 4º - Responsabilização e prestação de contas: as rotinas de backup criam trilhas que podem ser auditadas, bem como fornecer *logs* de uso em qualquer instância para facilitar a geração de relatórios.

CAPÍTULO VII – PRINCÍPIOS

Artigo 17 – Princípios de *compliance* que a **DTI** e a **Fundação CASA/SP** prezam em seus projetos de gestão de dados:

I. **Segurança cibernética:** infraestrutura de segurança e conectividade com análise e armazenamento de dados de acesso e tráfego, bem como revisão periódica de fabricantes e soluções do ecossistema;

II. **Redução de vulnerabilidade:** soluções de *Firewall* de borda com *Intrusion Prevention System (IPS)*, Antivírus e *Anti-botnet*, além de geolocalização para evitar acesso de países sem relações com a instituição;

III. **Controle de rastreabilidade:** ferramentas para rastrear acessos a sistemas internos, com dados criptografados e permissionamento interno para as informações;

IV. **Registro de incidentes:** todos os incidentes são analisados e monitorados 24×7, com ações proativas para solucionamento do problema e prevenção de futuros incidentes.

CAPÍTULO VIII – DISPOSIÇÕES FINAIS

Artigo 18 - A **DTI** pode alterar o teor desta **OS** a qualquer momento, conforme a finalidade ou necessidade, tal qual para adequação e conformidade legal de disposição de lei ou norma que tenha força jurídica equivalente, cabendo ao **USUÁRIO** verificá-la.

§ 1º - Ocorrendo atualizações significativas neste documento e que demandem coleta de consentimento, a instituição notificará o **USUÁRIO** pelo e-mail fornecido e canais de atendimento.

Artigo 19 - Caso haja alguma dúvida sobre as condições estabelecidas nesta **OS** ou qualquer documento, o **USUÁRIO** pode entrar em contato por meio dos canais de atendimento supramencionados.

Artigo 20 - Caso alguma disposição desta **OS** seja considerada ilegal ou ilegítima por autoridade da localidade em que o **USUÁRIO** resida ou da sua conexão à rede local e Internet, as demais condições permanecerão em pleno vigor e efeito.

Artigo 21 - O **USUÁRIO** reconhece que toda comunicação realizada por e-mail (aos endereços por ele informados), SMS, aplicativos de comunicação instantânea ou qualquer outra forma digital e/ou virtual também são válidas como prova documental, sendo eficazes e suficientes para a divulgação de qualquer assunto que se refira aos serviços prestados pela **Fundação CASA/SP,** bem como às condições de sua prestação, ressalvadas as disposições expressamente diversas previstas nesta **OS.**

Artigo 22 - Esta **OS** e a relação decorrente das ações aqui compreendidas, assim como qualquer disputa que surja em virtude disto será regulada exclusivamente pela legislação brasileira.

Artigo 23 - Fica eleita a **Assessoria Jurídica (AJ)** da **Fundação CASA/SP** para dirimir qualquer questão envolvendo o presente documento, renunciando as partes a qualquer outro, por mais privilegiado que seja ou venha a ser.

Artigo 24 - Os casos de **não conformidade** serão avaliados pela **DTI** e, caso necessário, levados a autoridade máxima da **Fundação CASA/SP.**

Artigo 25 - Esta **OS** entra em vigor na data de sua publicação.

CAPÍTULO IX – VERSIONAMENTO

VERSÃO	DATA	AUTOR	DESCRIÇÃO
1.0	10/01/2023	Odenilson dos Santos Bonfim	**Versão Inicial**
1.1	13/01/2023	Alex Christy Rogatti, Aurélio Olímpio de Souza, João Paulo Puntel Vargens, Julio Cesar Signorini, Luiz Fernando Souza Gomes da Silva, Marcelo Pereira da Silva, Márcia Ramos dos Santos, Odenilson dos Santos Bonfim, Patricia Tsutsumi Dias, Rafael Mengel Souza, Rodrigo Braoios Vilhora e Yuri Horalek e Domigues	**Revisões e Sugestões**
1.2	16/01/2023	AJ (Assessoria Jurídica), DGA (Diretoria de Gestão Administrativa), DTI (Divisão de Tecnologia da Informação) e GP (Gabinete da Presidência)	**Versão Final**

DTI, 16 de janeiro de 2023.

DOCUMENTO ASSINADO DIGITALMENTE