PREFEITURA DE SOROCABA

CEPOTI – COMISSÃO DE EXECUÇÃO DE POLÍTICAS DE TECNOLOGIA DA INFORMAÇÃO

POLÍTICA DE BACKUP

Novembro/2024

Responsável	Willian Moreira Finamore
Aprovado por:	Órgão Central do SIGESTI
Políticas Relacionadas	Plano de Gestão de Continuidade de Serviços de TIC, Política de Segurança da Informação
Data de Aprovação	21/11/2024-3552205.404.00029442/2024-61

Índice

INTRODUÇÃO

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 **Coordenadoria Geral de Tecnologia da Informação** e formalmente definidos como de necessária salvaguarda na **Prefeitura de Sorocaba**, para efetivar o Plano de Continuidade de Serviços de TI.

No sentido de assegurar a efetividade do Plano de Continuidade de Serviços de TI, 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.

Escopo

Esta política se aplica a todos os dados no âmbito da Prefeitura de Sorocaba, incluindo dados fora da Prefeitura de Sorocaba armazenados em um serviço de nuvem Pública ou Privada. “Dados críticos”, neste contexto, incluem e-mail (Exchange), arquivos armazenados em file system e compartilhados, bancos de dados e conteúdo web específicos, software e código-fonte, e sistemas operacionais (snapshot). A definição de dados críticos e escopo desta política de backup serão revisados anualmente.

Os serviços de TI críticos da Prefeitura de Sorocaba, devem ser formalmente elencados pela Comissão de Execução de Políticas de Tecnologia da Informação-CEPOTI, avalizados pelo Órgão Central do SIGESTI e demais setores da Coordenadoria Geral de Tecnologia da Informação.

Ficam previamente estabelecidos os sistemas de saúde, educação, assistência social, tributário, contabilidade, RH(Recursos Humanos), CRM (156), portal institucional e os serviços de e-mail, AD(Active Directory), storage, SEI(Sistema Eletrônico de Informações), como serviços críticos da Prefeitura de Sorocaba.

Esta política é aplicável a todos os agentes públicos que podem ser criadores e/ou usuários de tais dados. A política também se estende a terceiros que acessam e utilizam sistemas e equipamentos de TI da Prefeitura de Sorocaba ou que criam, processam ou armazenam dados de propriedade da Prefeitura de Sorocaba.

Não serão salvaguardados nem recuperados, dados armazenados localmente nos microcomputadores patrimoniados dos usuários ou em quaisquer outros dispositivos fora da **Rede de Comunicação Interna da TI**, ficando sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s).

A salvaguarda dos dados em formato digital pertencentes aos serviços de TI da Prefeitura de Sorocaba, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem ou hospedados por terceiros, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

Termos e Definições

ADMINISTRADOR DE BACKUP: agente responsável pelo planejamento de soluções de backup, definição de padrões, configurações e atendimento avançado de resolução de incidentes e problemas.

ARQUIVOS DE LOG: arquivo digital onde se encontra armazenado o processo de registro de eventos relevantes num sistema computacional, utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado.

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;

GESTOR DA INFORMAÇÃO: Qualquer indivíduo ou estrutura de órgão ou entidade da Administração Pública Direta Municipal, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controle de segurança em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação;

CRITICIDADE: grau de importância dos dados para a continuidade das atividades e serviços da organização.

DESCARTE: eliminação correta de dados, documentos, unidades de armazenamento e acervos digitais.

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

JANELA DE BACKUP: período de tempo durante o qual as cópias de segurança sob execução agendada ou manual poderão ser executadas.

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;

OPERADOR DE BACKUP: profissional responsável por procedimentos de atendimento de primeiro nível, acompanhamento de execução de rotinas de backup, realização de restaurações de arquivos de usuários e manutenção nos sistemas de backup e recuperação.

RESTAURAÇÃO: processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de backup.

RETENÇÃO: período de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração.

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 ou à segurança;

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;

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.

ROTINA DE BACKUP: procedimento utilizado para se realizar um backup.

SERVIÇO DE TI: sistema de informação ou qualquer solução de tecnologia da informação que armazene informações em formato digital

UNIDADE DE ARMAZENAMENTO: dispositivo para armazenamento de dados em suporte digital.

UNIDADE DE ARMAZENAMENTO DE BACKUP: unidade de armazenamento com características específicas para retenção de cópia de segurança de dados digitais

Referência Legal e Boas Práticas

Orientação	Seção
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
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
Decreto Municipal 22.194 de 29 de fevereiro de 2016	Institui a política de segurança da informação no âmbito da administração direta e indireta do município de Sorocaba
Decreto Municipal 22.984 de 9 de fevereiro de 2024	Atualização da Tabela de Temporalidade de Documentos da Administração Pública do Município de Sorocaba, instituída pelo Decreto 22.419 de 29 de setembro de 2016.

DECLARAÇÕES DA POLÍTICA

Dos princípios gerais

1. A política de Backup e Restauração de Dados deve estar alinhada com a Política de Segurança da Informação da Prefeitura de Sorocaba.
2. A Política de Backup e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.
3. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.
4. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
    a. A solução utilizada para realização das cópias de segurança deve gerar logs das rotinas de backup, incluindo as etapas bem-sucedidas e erros do processo de backup, além de permitir integração com um servidor operador de serviço de Syslog.
5. 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.**
6. 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 local remoto ao da sede da organização para armazenar cópias extras dos principais backups, a exemplo de dados de serviços críticos.
7. A infraestrutura de rede de backup deve ser apartada logicamente dos sistemas críticos da organização.
8. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.
9. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Da frequência e retenção dos dados

10. Os backups dos serviços de TI críticos da Prefeitura de Sorocaba devem ser realizados utilizando-se as seguintes frequências temporais:
    a. Diária;
    b. Semanal;
    c. Mensal;
    d. Anual.
11. Os serviços de TI críticos da Prefeitura de Sorocaba devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:
    a. Diária: 01 semana;
    b. Semanal: 03 semanas;
    c. Mensal: 01 ano;
    d. Anual: 07 anos.

12. Os serviços de TI NÃO críticos da Prefeitura de Sorocaba devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados a seguir:
    a. Diária: 01 semana;
    b. Semanal: 03 semanas;
    c. Mensal: 01 ano;
    d. Anual: 2 anos.
13. Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.
14. Os ativos envolvidos no processo de backup são considerados ativos críticos para a Prefeitura de Sorocaba.
15. A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pelo (s) responsável (s) dos dados, com a anuência prévia e formal do superior hierárquico, refletindo os requisitos de negócio da organização da informação para a continuidade da operação, e deve explicitar, no mínimo, os seguintes requisitos:
    a. Escopo (dados digitais a serem salvaguardados);
    b. Tipo de backup (completo, incremental, diferencial);
    c. Frequência temporal de realização do backup (diária, semanal, mensal, anual);
    d. Retenção;
    e. POR;
    f. RTO.
16. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao Administrador de Backup. A aprovação para execução da alteração depende da anuência do Gestor da Informação.
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.
18. Todos os pedidos de realização de backup/recuperação deverão ser encaminhados para o administrador de backups, que emitirá decisão sobre o pedido.

Tipos de backup

I – Completo (full): Um backup completo copia todos os dados de um sistema ou conjunto de dados específico. Inclui todos os arquivos e pastas, independentemente de terem sido modificados. Fornece uma cópia integral dos dados, facilitando a restauração completa. No entanto, pode levar mais tempo e exigir mais armazenamento.

II – Incremental: Um backup incremental só armazena as alterações feitas desde o último backup. É mais rápido e usa menos espaço de armazenamento, mas a restauração pode ser mais complexa porque depende do último backup completo e de todos os incrementais subsequentes.

III – Diferencial: Um backup diferencial armazena todas as alterações feitas desde o último backup completo. Ele é mais rápido que um backup completo e usa menos espaço de armazenamento. No entanto, ao contrário do backup incremental, ele não depende de todos

os backups incrementais realizados desde o último backup completo, o que torna a restauração mais simples e rápida.

Salvo indicação em contrário, o backup dos dados do sistema será feito de acordo com a seguinte programação padrão:

19. Backup incremental diário (segunda a sábado), armazenado no local.
    a. Poderão ser estabelecidas frequências maiores de acordo com a necessidade específica, por exemplo, backup incremental de hora em hora para log de transações de banco de dados.
20. Backup completo semanal (sábado a domingo), armazenado externamente. Sempre que possível, os backups devem ser iniciados às 00h00 da manhã de sábado para permitir mais tempo durante o fim de semana para realizar o backup e tempo suficiente para lidar com quaisquer problemas que possam surgir durante o processo de backup.

Do uso da rede

21. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados da Prefeitura de Sorocaba, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da Prefeitura de Sorocaba.
22. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.
23. O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com a Divisão de Infraestrutura, responsável pela administração da rede de dados da Prefeitura de Sorocaba.

Do transporte e armazenamento

24. As unidades de armazenamento utilizadas na salvaguarda dos dados devem considerar as seguintes características dos dados resguardados:
    a. A criticidade do dado salvaguardado;
    b. O tempo de retenção do dado;
    c. A probabilidade de necessidade de restauração;
    d. O tempo esperado para restauração;
    e. O custo de aquisição da unidade de armazenamento de backup;
    f. A vida útil da unidade de armazenamento de backup.
25. 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.
26. Podem ser utilizadas técnicas de compressão de dados, contando que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelos gestores das informações.
27. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

28. No caso de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos na Rede de Comunicação Interna (RCI) deverá ser mantido por, no mínimo, 90 dias. Após esse período os arquivos poderão ser excluídos a qualquer tempo.
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.
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.
    a. As mídias de backup serão armazenadas conforme descrito neste documento:
        i. Todos os backups serão gravados em unidades com capacidade e taxa de transferência de acordo com os recursos disponíveis à época da execução desta política.
        ii. Backups devem seguir os prazos e frequências definidos nos itens 11 e 12 desta política.

Dos testes de backup

31. Os backups serão verificados periodicamente:
    a. Diariamente, os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.
    b. Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha.
    c. A CGTI manterá registros de backups e testes de restauração para demonstrar conformidade com esta política.
    d. Os testes devem ser realizados em todos os backups produzidos independente do ambiente.
32. Os testes de restauração dos backups devem ser realizados, por amostragem uma vez por semana, 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.
33. Verificar se foram atendidos os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs.
34. Os registros deverão conter, no mínimo, o tipo/serviço que teve o seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do backup e se o procedimento foi concluído com sucesso.
35. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pela Comissão de Segurança da Informação.

Procedimentos de restauração de backup

36. O atendimento de solicitações de restauração de arquivos, e-mails e demais formas de dados deverá obedecer às seguintes orientações:
    a. A solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através de chamado técnico pelo e-mail informatica@sorocaba.sp.gov.br
    b. A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup.
    c. A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações.
    d. O administrador 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.
37. O cronograma de restauração de dados:
    a. O tempo de restauração, preferencialmente definido em Acordo de Nível de Serviço, entre as áreas de negócio e a CGTI, é proporcional ao volume de dados necessários para o restore.
    b. Backups externos serão disponibilizados em no máximo 48 horas corridas de uma falha catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um.
    c. Backups externos, serão disponibilizados em no máximo 5 dias de uma falha não catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um.
38. Diretrizes para restauração de dados:
    a. Críticos:
        i. O processo de restauração deve ser iniciado imediatamente após a identificação de um problema pela Prefeitura;
        ii. O processo deve seguir um cronograma previamente definido no Acordo de Nível de Serviço (SLA);
        iii. A equipe de TI deve registrar a data e hora do início e término do processo, bem como qualquer anomalia ou desafio enfrentado durante a restauração;
        iv. Qualquer falha no cumprimento do cronograma precisa ser reportada imediatamente aos gestores, e um plano de ação corretiva deve ser implementado para evitar recorrências.

Do Descarte da Mídia

39. A mídia de backup será retirada e descartada conforme descrito neste documento:
    a. A CGTI 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.
    b. A CGTI garantirá a destruição lógica e física da mídia antes do descarte
    c. As mídias a serem descartadas (devido à obsolescência tecnológica, ou defeito irrecuperável) devem ser eliminadas de forma segura e protegida, por meio

de procedimento que impossibilite a recuperação dos dados por terceiros, observadas as orientações para o descarte ou eliminação desse tipo de bem.

Das Responsabilidades

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

41. São atribuições do **Administrador de Backup**:
    a. Propor soluções de cópia de segurança das informações digitais corporativas produzidas ou customizadas pela organização;
    b. Providenciar a criação e manutenção dos backups;
    c. Configurar as soluções de backup;
    d. Manter as unidades de armazenamento de backups preservadas, funcionais e seguras;
    e. Definir os procedimentos de restauração e neles auxiliar;

42. São atribuições do **Operador de Backup**:

    a. Restaurar ou recuperar os backups em caso de necessidade;
    b. Operar e manusear as unidades de armazenamento de backups;
    c. Informar ao administrador de backup qualquer problema que impossibilite a criação ou restauração de um backup; e
    d. Executar os testes de restauração de backup.

43. São atribuições da **Coordenadoria Geral de Tecnologia da Informação**:
    a. Manter as unidades de armazenamento de backups preservadas, funcionais e seguras;
    b. Solicitar as restaurações de dados, com anuência do gestor da informação;
    c. Sanar dúvidas técnicas do administrador de backup acerca das informações salvaguardadas;
    d. Validar, tecnicamente, o resultado das restaurações eventualmente solicitadas; e
    e. Validar, tecnicamente, o resultado dos testes de restauração dos backups.

44. São atribuições dos **Gestores da Informação**:
    a. Solicitar, formalmente, a salvaguarda das informações geridas e dar anuência à solicitação feita pela área técnica para recuperação de dados;
    b. Validar, tecnicamente, o resultado das restaurações eventualmente solicitadas; e
    c. Validar, tecnicamente, o resultado dos testes de restauração dos backups.