(16)3711-9000
Rua Frederico Moura, 1.517 - Cidade Nova
Franca/SP - Cep: 14401-150
CNPJ: 47.970.769/0001-04 - I.E: isento

POLÍTICA DE CÓPIAS DE SEGURANÇA (BACKUP)

Versão 1.0

(16)3711-9000
Rua Frederico Moura, 1.517 - Cidade Nova
Franca/SP - Cep: 14401-150
CNPJ: 47.970.769/0001-04 - I.E: isento

SUMÁRIO

(16)3711-9000
Rua Frederico Moura, 1.517 - Cidade Nova
Franca/SP - Cep: 14401-150
CNPJ: 47.970.769/0001-04 - I.E: isento

OBJETIVO

A Política de Cópias de Segurança objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pelo Departamento de Tecnologia da Informação e formalmente definidos como de necessária salvaguarda no Município de Franca, para se manter a continuidade da prestação do serviço público. 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 Cópias de segurança (Backup), 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 Administração Pública Municipal, incluindo dados fora da Prefeitura de Franca armazenados em um serviço de nuvem Pública ou Privada. “Dados críticos”, neste contexto, incluem e-mail, arquivos pessoais e compartilhados, bancos de dados e conteúdo da web específicos e sistemas operacionais. A definição de dados críticos e o escopo desta política de backup serão revisados anualmente.
- Os serviços de TI críticos do Município de Franca devem ser formalmente elencados pelo Departamento de Tecnologia da Informação.
- Esta política se aplica a servidores públicos municipais que podem ser criadores e/ou usuários de tais dados. A política também se aplica a terceiros que acessam e usam sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade do Município de Franca.

(16)3711-9000
Rua Frederico Moura, 1.517 - Cidade Nova
Franca/SP - Cep: 14401-150
CNPJ: 47.970.769/0001-04 - I.E: isento

- 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).
- A salvaguarda dos dados em formato digital pertencentes a serviços de TI do Município de Franca, 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.

TERMOS E DEFINIÇÕES

- 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;
- CUSTODIANTE 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;
- ELIMINAÇÃO - Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
- 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;
- INFRAESTRUTURA CRÍTICA – instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem

(16)3711-9000
Rua Frederico Moura, 1.517 - Cidade Nova
Franca/SP - Cep: 14401-150
CNPJ: 47.970.769/0001-04 - I.E: isento

desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional 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.

REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

LEGISLAÇÃO / ORIENTAÇÃO	SEÇÃO
Lei Municipal nº 9.538, de 15 de agosto de 2024	Na íntegra

PROCEDIMENTOS PRÁTICOS DA POLÍTICA

Dos princípios gerais

1. A Política de Cópias de Segurança (backup) deve estar alinhada com à Política de Segurança da Informação do Município de Franca.
2. A Política de Cópias de Segurança (backup) 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.

(16)3711-9000
Rua Frederico Moura, 1.517 - Cidade Nova
Franca/SP - Cep: 14401-150
CNPJ: 47.970.769/0001-04 - I.E: isento

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 um local remoto ao da sede da organização para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.
7. A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, 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 do Município de Franca devem ser realizados utilizando-se as seguintes frequências temporais:
    I – Diária;
    II – Semanal;
    III – Mensal;
    IV – Anual.
11. Os serviços de TI críticos do Município de Franca devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:
    I – Diária: 1 semana;
    II – Semanal: 4 semanas;
    III – Mensal: 6 meses;
    IV – Anual: 2 anos.

(16)3711-9000
Rua Frederico Moura, 1.517 - Cidade Nova
Franca/SP - Cep: 14401-150
CNPJ: 47.970.769/0001-04 - I.E: isento

12. Os serviços de TI NÃO críticos dom Município de Franca devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

    I – Diária: 1 semana;

    II – Semanal: 4 semanas;

    III – Mensal: 6 meses;

    IV – 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 o Município de Franca.

15. A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pela chefia imediata de cada setor, 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 (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.

16. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao Departamento de Tecnologia da Informação (infra@franca.sp.gov.br). A

(16)3711-9000
Rua Frederico Moura, 1.517 - Cidade Nova
Franca/SP - Cep: 14401-150
CNPJ: 47.970.769/0001-04 - I.E: isento

aprovação para execução da alteração depende da anuência da chefia imediata do setor.

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.

Tipo de backup

18. São os tipos de backup:
    I – Completo (full);
    II – Incremental;
    III – Diferencial.

Do uso da rede

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

Do transporte e armazenamento

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;

(16)3711-9000
Rua Frederico Moura, 1.517 - Cidade Nova
Franca/SP - Cep: 14401-150
CNPJ: 47.970.769/0001-04 - I.E: isento

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.

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.
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.
25. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.
26. No caso de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos em nuvem deverá ser mantido por, no mínimo, 07 (sete) dias. Após esse período os arquivos poderão ser excluídos a qualquer tempo.
27. 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.
28. 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.

Dos testes de backup

29. Os backups serão verificados periodicamente:

(16)3711-9000
Rua Frederico Moura, 1.517 - Cidade Nova
Franca/SP - Cep: 14401-150
CNPJ: 47.970.769/0001-04 - I.E: isento

- Diariamente, os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.
- Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha.
- A TI manterá registros de backups e testes de restauração para demonstrar conformidade com esta política.
- Os testes devem ser realizados em todos os backups produzidos independente do ambiente.

30. 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.
31. Verificar se foi atendido os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs.
32. Os registros deverão conter, no mínimo, o tipo de sistema/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.
33. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pelo Departamento de Tecnologia da Informação, juntamente com a Secretaria de Administração e Recursos Humanos.

Procedimento de restauração de backup

34. 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 do e-mail infra@franca.sp.gov.br.
    b. A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup.

(16)3711-9000
Rua Frederico Moura, 1.517 - Cidade Nova
Franca/SP - Cep: 14401-150
CNPJ: 47.970.769/0001-04 - I.E: isento

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

d. 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.

RESPONSABILIDADES

Em caso de violação desta política poderão ser aplicadas sanções previstas no Decreto nº 11.234, de 08 de abril de 2021 e outras legislações cabíveis.

Pedro Silva Garcia

Diretor do Departamento de Tecnologia da Informação

Petersson Alves Faciroli

Secretário Municipal de Administração e Recursos Humanos