ANEXO I – DECRETO Nº 8109 DE 29 DE NOVEMBRO DE 2024

TERMO DE RESPONSABILIDADE

POLÍTICA MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO

Eu, _____,
Registro Funcional nº_____, CPF nº _____,
lotado na Secretaria de_____, declaro estar ciente:

1. Da POLÍTICA DE SEGURANÇA DA INFORMAÇÃO do Município da Estância Balneária de Praia Grande – inclusive do conteúdo de suas NORMAS;

2. Do uso de assinaturas eletrônicas conforme regras vigentes;

3. Da possibilidade de auditoria, sem prévio aviso, nos recursos por mim utilizados, assumindo que estes estão disponíveis para execução de minhas funções junto à Prefeitura de Praia Grande;

4. De que todas as informações tratadas, recebidas, enviadas e armazenadas pela Prefeitura de Praia Grande, sob minha responsabilidade, serão tratadas de forma sigilosa e confidencial;

5. De que devo zelar pelo sigilo absoluto de minhas senhas;

6. De não revelar, fora do serviço público municipal, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

7. De que devo manter a absoluta cautela quando da exibição de informação e imagens em tela, a fim de evitar que pessoas não autorizadas tenham acesso;

8. De não me ausentar do terminal sem encerrar ou bloquear a sessão de uso do sistema, garantindo assim a impossibilidade de acesso indevido por pessoas não autorizadas; e

9. De responder, em todas as instâncias, cível, penal e administrativa, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento das minhas senhas ou das transações as quais esteja habilitado.

Praia Grande, ___ de _____ de 20____

_____
ASSINATURA

ANEXO II – DECRETO Nº 8109 DE 29 DE NOVEMBRO DE 2024

TERMO DE RESPONSABILIDADE - PREPOSTO

POLÍTICA MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO

Eu,_____

_____, **CPF** nº_____, preposto da empresa

_____,

inscrita no CNPJ sob o nº_____, declaro estar ciente:

a) Da POLÍTICA MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO da Administração Pública Direta do Município da Estância Balneária de Praia Grande – inclusive do conteúdo de suas NORMAS;

b) De que todas as informações tratadas, recebidas, enviadas e armazenadas pela Administração Direta Municipal, sob minha responsabilidade, serão tratadas de forma sigilosa e confidencial;

c) De não utilizar as informações restritas a que tiver acesso para gerar benefício próprio, exclusivo e/ou unilateral, presente ou futuro, ou para o benefício de terceiros;

d) De que não devo fazer apropriação, reproduzir ou dar conhecimento a terceiros, sem a anuência formal e expressa da Administração Direta Municipal, de material ou informação restrita;

e) De que devo cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao Poder Executivo Municipal, devendo cientificá-los da existência deste termo e da natureza confidencial das informações restritas;

f) De não utilizar, bem como a não permitir que diretores, consultores, prestadores de serviços, colegas de trabalho e/ou prepostos utilizem as informações restritas de forma diversa da prevista no contrato de prestação de serviços com a Administração Pública Direta do Município de Praia Grande;

g) De não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

h) De que devo informar imediatamente o Poder Executivo Municipal sobre qualquer violação das regras de sigilo estabelecidas neste termo que tenha tomado conhecimento ou ocorrido por ação ou omissão, independentemente da existência de dolo.

ANEXO II – DECRETO Nº 8109 DE 29 DE NOVEMBRO DE 2024

A quebra do sigilo das informações restritas, devidamente comprovada, sem autorização expressa da Administração Direta do Município da Estância Balneária de Praia Grande, acarretará na aplicação das sanções administrativas previstas no contrato, bem como, possibilitará a dispensa dos serviços prestados ao município. O prestador de serviço estará sujeito, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo município, inclusive os de ordem moral, bem como as responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo administrativo e judicial.

E, por estar ciente de todas as condições e obrigações constantes neste termo, bem como, na Política Municipal de Segurança da Informação e seus respectivos Anexos, segue o aceite com o abaixo assinado.

Praia Grande, ____ de _____de 20____

_____

ASSINATURA

ANEXO III – DECRETO Nº 8109 DE 29 DE NOVEMBRO DE 2024

TERMO DE RESPONSABILIDADE PARA UTILIZAÇÃO DE ACESSO REMOTO

POLÍTICA MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO

Eu,_____, Registro Funcional nº _____, CPF nº _____, lotado na Secretaria de_____,

Declaro ter ciência da Política de Segurança da Informação e que devo observar suas regras bem como devo seguir rigorosamente os procedimentos de segurança estabelecidos abaixo para o acesso remoto aos recursos da Rede Institucional da Administração Direta do Município da Estância Balneária de Praia Grande, pelo qual me responsabilizo a partir da disponibilização das chaves de acesso para permissão de uso:

1. De zelar pelo sigilo e privacidade das minhas credenciais de acesso, uma vez que a permissão é estritamente pessoal, sendo proibida a sua transferência ou o seu compartilhamento;

2. De utilizar o acesso exclusivamente para fins institucionais relacionados às minhas atribuições;

3. De responsabilizar-me pelo pedido de cancelamento da chave de acesso quando da não utilização ou desnecessidade dela;

4. De dispor de infraestrutura física e tecnológica necessárias e adequadas à realização de acesso remoto que permita o tráfego de informações de maneira segura e tempestiva, evitando qualquer tipo de incidente de segurança, voluntário ou involuntário, na Rede Institucional da Administração Direta do Município, conforme orientação dada pelo Departamento de Informática.

5. De que o acesso poderá ser realizado por meio de VPN (Rede Virtual Privada), RDP (Área de Trabalho Remota) ou outra ferramenta aprovada pelo Departamento de Informática do Município.

Confirmo o entendimento de que toda comunicação entre o computador e a Rede Institucional da Administração Direta do Município de Praia Grande será monitorada durante a conexão e declaro, ainda, estar ciente dos procedimentos de segurança acima descritos e que em caso de descumprimento de quaisquer determinações, minhas credenciais serão revogadas.

Praia Grande, ___ de _____ de 20____

_____

ASSINATURA

ANEXO IV – DECRETO Nº 8109 DE 29 DE NOVEMBRO DE 2024

TERMO DE RESPONSABILIDADE PARA UTILIZAÇÃO DE ACESSO REMOTO - PREPOSTO

POLÍTICA MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO

Eu, _____, CPF nº_____,

preposto da empresa _____,

inscrita no CNPJ sob o nº_____

Declaro ter ciência da Política de Segurança da Informação e que devo observar suas regras bem como devo seguir rigorosamente os procedimentos de segurança estabelecidos abaixo para o acesso remoto aos recursos da Rede Institucional da Administração Direta do Município da Estância Balneária de Praia Grande, pelo qual me responsabilizo a partir da disponibilização das chaves de acesso para permissão de uso:

1. De zelar pelo sigilo e privacidade das minhas credenciais de acesso, uma vez que a permissão é estritamente pessoal, sendo proibida a sua transferência ou o seu compartilhamento;

2. De utilizar o acesso exclusivamente para fins institucionais relacionados às atribuições da empresa contratada;

3. De responsabilizar-me pelo pedido de cancelamento da chave de acesso quando da não utilização ou desnecessidade dela;

4. De dispor de infraestrutura física e tecnológica necessárias e adequadas à realização de acesso remoto que permita o tráfego de informações de maneira segura e tempestiva, evitando qualquer tipo de incidente de segurança, voluntário ou involuntário, na Rede Institucional da Administração Direta do Município, conforme orientação dada pelo Departamento de Informática.

5. De que o acesso poderá ser realizado por meio de VPN (Rede Virtual Privada), RDP (Área de Trabalho Remota) ou outra ferramenta aprovada pelo Departamento de Informática do Município.

Confirmo o entendimento de que toda comunicação entre o computador e a Rede Institucional da Administração Direta do Município de Praia Grande será monitorada durante a conexão e declaro, ainda, estar ciente dos procedimentos de segurança acima descritos e que em caso de descumprimento de quaisquer determinações, minhas credenciais serão revogadas.

Praia Grande, ___ de _____ de 20____

_____

ASSINATURA

ANEXO V – DECRETO Nº 8109 DE 29 DE NOVEMBRO DE 2024

POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS DIGITAIS

Responsável	Divisão de Infraestrutura e Segurança de Dados, Departamento de Informática e Divisão de Suporte ao Monitoramento e Projetos
Aprovado por:	Comissão Municipal de Tecnologia da Informação – CMTI Comitê de Segurança da Informação - CSI
Políticas Relacionadas	Política de Segurança da Informação, Plano de Continuidade de Serviços de TI
Data da Aprovação	29 de dezembro de 2022

PROPÓSITO

A Política de Backup e Restauração de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam a segurança, proteção e disponibilidade dos dados digitais custodiados pelas unidades de Tecnologia da Informação (TI) e formalmente definidos como de necessária salvaguarda na Administração Direta do Município da Estância Balneária de Praia Grande para se manter a continuidade dos serviços. No sentido de assegurar este objetivo, 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 do Poder Executivo Municipal, incluindo dados fora da instituição, armazenados em serviços de nuvem Pública ou Privada.

Os serviços de TI críticos devem ser formalmente elencados pelo Comitê de Segurança da Informação.

Ficam previamente estabelecidos como serviços críticos os sistemas cuja finalidade seja o atendimento, a segurança ou a prestação de serviços ao cidadão.

Esta política se aplica a agentes públicos que podem ser criadores e/ou usuários de tais dados. A política também se aplica a terceiros que acessam e usam na instituição

sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade do Município da Estância Balneária de Praia Grande.

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 sob a responsabilidade do indivíduo que usa o(s) dispositivo(s).

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

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

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.

CÓPIA LOCAL: corresponde aos dados originais que são utilizados pelo usuário para acesso primário.

BACKUP LOCAL: corresponde a uma cópia de backup armazenada de forma a permitir o acesso imediato havendo a necessidade de restauração dos dados originais que tenham sido deletados, alterados ou perdidos.

BACKUP REMOTO: corresponde a uma segunda cópia de backup armazenada em local remoto para possibilitar a restauração dos dados caso o datacenter primário seja danificado em ocasião de desastre ou qualquer situação que cause dano irreparável aos equipamentos originais.

DADOS CRÍTICOS: neste contexto, incluem: e-mail, arquivos pessoais e compartilhados, bancos de dados, conteúdos da web específicos e sistemas operacionais.

ANEXO V – DECRETO Nº 8109 DE 29 DE NOVEMBRO DE 2024

Orientação	Secção
Acórdão 1.889/2020-TCU-Plenário	Relatório de Levantamento de Auditoria Páginas 30-32
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
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
Framework de segurança cibernética do CIS 8	Salvaguardas do controle 11 (Data Recovery Capabilities)
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
Guias Operacionais SGD	Todos
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
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
Política de Segurança da Informação da Prefeitura de Praia Grande	Em sua íntegra
Norma de Controle e Acesso ao Data Center da Prefeitura de Praia Grande	Em sua íntegra

ANEXO V – DECRETO Nº 8109 DE 29 DE NOVEMBRO DE 2024

DECLARAÇÕES DA POLÍTICA
DOS PRINCÍPIOS GERAIS

1. A Política de Backup e Restauração de Dados deve estar alinhada com à Política de Segurança da Informação do Município da Estância Balneária de Praia Grande.

2. É recomendado que as rotinas de backup sigam as diretrizes que regem a existência de três cópias dos dados: Cópia local, Backup local e Backup remoto.

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.

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 do Município

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 do paço municipal para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.

7. A infraestrutura de rede de backup deve preferencialmente ser apartada, lógica e fisicamente, dos sistemas críticos do Município.

8. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.

9. Os backups, assim como os dados originais, necessitam de medidas de segurança que previnam o acesso indevido e não autorizado. Para tanto, deve ser empregado o uso de recursos como criptografia, senhas e controles de acesso lógico ou físico quando aplicável.

10. É importante que os backups possuam identificação da data de criação para controle de manutenção ou descarte, bem como possibilitar a catalogação dos backups disponíveis de maneira organizada.

DA FREQUÊNCIA E RETENÇÃO DOS DADOS

11. Os backups dos serviços de TI críticos devem ser realizados utilizando-se as seguintes frequências temporais:
11.1. Diário

11.2. Semanal

11.3. Mensal

11.4. Anual

12. Os serviços de TI críticos devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:
12.1. Diário: 1 mês;

12.2. Semanal: 2 meses;

12.3. Mensal: 6 meses e;

12.4. Anual: 2 anos.

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

13.1. Diário: 2 semanas;

13.2. Semanal: 1 mês;

13.3. Mensal: 3 meses e;

13.4. Anual: 1 ano.

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

15. Os ativos envolvidos no processo de backup são considerados ativos críticos.

16. A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pelos responsáveis pelos dados, com a anuência prévia e formal dos responsáveis por essa Política de Backup e Restauração de Dados Digitais e refletindo os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação, e deve explicitar, no mínimo, os seguintes requisitos técnicos:
16.1. Escopo (dados digitais a serem salvaguardados);

16.2. Tipo de backup (completo, incremental, diferencial);

16.3. Frequência temporal de realização do backup (diária, semanal, mensal, anual);

16.4. Retenção;

16.5. RPO e;

16.6. RTO.

17. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas aos responsáveis pelo backup. A aprovação para execução da alteração depende da anuência do setor responsável na secretaria.

18. 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.

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

19.1. Backup incremental diário (segunda a sábado), armazenado no local.

19.2. Backup completo semanal (sábado e domingo), armazenado externamente. Sempre que possível, os backups devem ser iniciados às 12h 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

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

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

22. 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 Poder Executivo Municipal.

DO TRANSPORTE E ARMAZENAMENTO

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

23.1. A criticidade do dado salvaguardado;

23.2. O tempo de retenção do dado;

23.3. A probabilidade de necessidade de restauração;

23.4. O tempo esperado para restauração;

23.5. O custo de aquisição da unidade de armazenamento de backup e;

23.6. A vida útil da unidade de armazenamento de backup.

24. Os backups devem existir em pelo menos duas mídias diferentes para aumento da segurança. Exemplo: uma cópia em disco e uma cópia em fita, ou uma cópia em disco e uma cópia em nuvem.

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, contanto 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 deverá ser mantido por, no mínimo, 30 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, e com acesso restrito a pessoas autorizadas pelo administrador de backup. Além disso, as condições de temperatura, umidade 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.

DOS TESTES DE BACKUP

31. Os backups deverão ser verificados periodicamente, conforme estipulado por esta política.

31.1. Diariamente, os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.

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

31.3. A TI manterá registros de backups e testes de restauração para demonstrar conformidade com esta política.

31.4. 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, semanalmente, em 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. Os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs, deverão ser verificados para garantir seu devido atendimento.

34. 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.

35. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pelo Comitê de Segurança da Informação.

ANEXO V – DECRETO Nº 8109 DE 29 DE NOVEMBRO DE 2024

PROCEDIMENTO DE RESTAURAÇÃO DE BACKUP

36. Planos de ação devem ser elaborados para orientação do procedimento a ser adotado em caso de necessidade de restauração de backups ou, em casos mais graves, recuperação de desastres.

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

37.1. A solicitação de restauração de objetos deverá sempre partir do responsável pelo dado, através de sistema para atendimento ao usuário (S.A.U.) em até 5 dias corridos.

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

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

37.4. 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.

DO DESCARTE DA MÍDIA

38. A mídia de backup será retirada e descartada conforme descrito neste documento:

38.1. A equipe de TI deverá assegurar que, antes do descarte, a mídia não contenha mais imagens de backup ativas, garantindo que quaisquer dados anteriormente armazenados na mídia não possam ser lidos ou recuperados.

38.2. Sempre que possível, a equipe de TI deverá promover a destruição física da mídia antes de seu descarte.

DAS RESPONSABILIDADES

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

40. São atribuições do administrador de backup:

40.1. Propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pelo Poder Executivo Municipal;

40.2. Providenciar a criação e manutenção dos backups;

40.3. Configurar as soluções de backup;

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

40.5. Definir os procedimentos de restauração e realizar os devidos auxílios necessários;