Art. 19. A gestão de usuário deve considerar que:
I- o usuário não pode ser excluído, ele deve ser inativado ou desabilitado, salvo exceções previstas em normativo ou procedimento específico para o respectivo ativo onde o usuário está registrado;
II- a inativação pode fundamentar-se, também, em análise crítica que apresenta o risco do usuário ativo à segurança da informação ou desconformidade com algum normativo vigente;
III- a inativação automatizada de usuário deve existir quando houver regras de negócio bem definidas e implementação viável em programa de computador;
IV- o processo de autenticação de usuários deve ser definido pela área responsável pela gestão de Tecnologia da Informação e poderá ser baseada em autenticação simples (nome de usuário e senha) e agregada a autenticação multifator (certificação digital ou outros meios disponíveis).
Art. 20. O controle de acesso lógico deve utilizar uma base centralizada para autenticação dos usuários, exceto quanto o ativo não permitir a interoperabilidade com a base central de autenticação institucional.
Art. 21. O usuário deve utilizar os serviços e as informações obtidas, por meio do perfil de acesso, única e exclusivamente em razão do exercício da função pública e para os fins que lhe foi designado, cumprindo os procedimentos dispostos nesta norma, sem prejuízo das demais normatizações vigentes na Administração Pública Municipal.
Art. 22. O usuário que tiver algum dado da conta institucional envolvido em vazamento de dados terá a conta institucional suspensa até que seja feito troca das credenciais de acessos.
Art. 23. A Rede de Dados Corporativa compõe a infraestrutura de rede, que é disponibilizada para uso institucional, logo, apenas equipamentos de propriedade do Município de Rio das Ostras são autorizados e devem ser conectados à rede corporativa.
Art. 24. Em casos excepcionais, a conexão de equipamentos particulares à rede corporativa deve ser feita em razão do interesse do Município e sob prévia autorização do responsável pela gestão da unidade em que o equipamento estiver localizado.

Seção V
Das Vedações
Art. 25. É vedado o uso da rede corporativa para:
I- acesso por meio de equipamento não homologado pela ANATEL ou não autorizado pela Gestão de Tecnologia;
II- fazer download, instalar e/ou utilizar sistemas ou aplicativos não homologados pela área responsável pela gestão de TIC do Município;
III- a utilização de softwares particulares em equipamentos do Município sem autorização expressa;
IV- a instalação e conexão de equipamentos particulares à rede corporativa do Ministério sem a prévia autorização do gestor responsável pela unidade ou da área responsável pela gestão de TI do Município;
V- o uso dos recursos de rede para fins particulares ou de terceiros alheios aos interesses do Município, em especial, quando tal procedimento prejudique o tráfego da rede de dados;
VI- o uso para fins de divulgação ou distribuição de material que não possua vínculo com as atividades desenvolvidas pelo Município;
VII- a instalação ou utilização de ferramentas de monitoramento de rede computacional sem a anuência e autorização expressa da área responsável pela gestão de TIC do Município;
VIII- a instalação de dispositivos de comunicação ou de compartilhamento de dados sem fio, particulares, à rede corporativa do Município, sem autorização expressa da área responsável pela gestão de TIC;
IX- burlar as regras de acesso à internet configuradas em proxy ou ferramenta similar de gerenciamento de conteúdo web.

Seção VI
Dos Tratamentos de Incidentes
Art. 26. O processo de tratamento de incidentes de segurança deve considerar eventual violação deste normativo de controle de acesso lógico.
Art. 27. A permissão de acesso lógico que não implementar padrão de controle a partir de 01 (um) dispositivo criptográfico, biometria ou senha deve ser tratada como incidente de segurança.
Art. 28. Pedido de análise de operação de um comportamento de usuário deve ser registrado pela área de negócio responsável pelo serviço ou por um grupo de trabalho que foi formalmente designado para investigar um incidente envolvendo o respectivo usuário.

Seção VII
Das Violações, Penalidades e Sanções
Art. 29. Cabe a área responsável pela gestão de TIC no âmbito do Município definir os aspectos relacionados à plataforma tecnológica, gestão operacional, forma de autenticação e sustentação do domínio de rede corporativa.
Art. 30. As ocorrências de mau uso do acesso aos recursos disponíveis na rede e sistemas corporativos não previstas nesta norma e os casos omissos serão encaminhados para a área responsável pela gestão de TIC no âmbito do Município para análise e pronunciamento.
Art. 31. O descumprimento dessa Norma poderá resultar em sanções administrativas, civis e criminais, na forma da Lei.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 32. Orientações e devidas documentações técnicas a respeito do controle de acesso lógico estão disponíveis no Portal GovTIC: https://www.riodasostras.rj.gov.br/govtic/.
Art. 33. Este Decreto entra em vigor na data de sua publicação, aprovando a Norma Complementar para Controle de Acesso Lógico.

Rio das Ostras, 22 de novembro de 2024.

MARCELINO CARLOS DIAS BORBA
Prefeito do Município de Rio das Ostras

DECRETO Nº 4133/2024.

DISPÕE SOBRE A APROVAÇÃO DA NORMA COMPLEMENTAR PARA CÓPIA DE SEGURANÇA E RESTAURAÇÃO DE DADOS DO MUNICÍPIO DE RIO DAS OSTRAS.
O PREFEITO DO MUNICÍPIO DE RIO DAS OSTRAS, Estado do Rio de Janeiro, no uso de suas atribuições legais, em consonância ao Processo Administrativo nº 44568/2024;

DECRETA:

CAPÍTULO I
DA NORMA COMPLEMENTAR PARA CÓPIA DE SEGURANÇA E RESTAURAÇÃO DE DADOS

Seção I
Da Introdução

Art. 1º Esta Norma Complementar tem por objetivo estabelecer a política de cópia de segurança e restauração de dados com as diretrizes para o processo de cópia e armazenamento dos dados sob a guarda da Gestão de Tecnologia da Informação, visando garantir a segurança, integridade e disponibilidade no âmbito do Município de Rio das Ostras.

CAPÍTULO II
DO PROPÓSITO

Art. 2º 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(s) Gestões de Tecnologia da Informação e formalmente definidos como de necessária salvaguarda no Município de Rio das Ostras, 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.

CAPÍTULO III
DO ESCOPO

Art. 3º Esta normativa se aplica a todos os dados no âmbito do Município, incluindo dados armazenados no Datacenter ou em um serviço de nuvem Pública ou Privada, assim como:

I- os serviços de TIC considerados críticos devem ser formalmente elencados pela Gestão de TIC no Município;
II- já ficam previamente estabelecidos os documentos administrativos e base de dados de sistemas próprios, como serviços críticos do Município;
III- 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 sistemas e equipamentos de TIC ou que criam, processam ou armazenam dados de propriedade do Município de Rio das Ostras;
IV- 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 TIC, ficando sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s);
V- obrigatoriamente, salvo em ocasiões justificadas onde não existe acesso lógico ao Datacenter, todos os dados devem ser armazenados nos Servidores de Armazenamento da TIC;
VI- a salvaguarda dos dados em formato digital pertencentes a serviços de TIC 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.

CAPÍTULO IV
DOS TERMOS E DEFINIÇÕES

Art. 4º Esta Norma Complementar tem por objetivo estabelecer os termos e definições, da seguinte forma:

I- 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;
II- PLANO DE BACKUP: documento formal onde são definidos os responsáveis pela cópia dos dados, o que será armazenado, periodicidade de execução da cópia e tempo de retenção, de acordo com as orientações da Política de Backup;
III- BACKUP COMPLETO (FULL): modalidade de backup em que todos os dados a serem guardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último backup;
IV- BACKUP DIFERENCIAL: modalidade de backup em que são guardados apenas dados novos ou modificados desde o último backup completo efetuado;
V- BACKUP INCREMENTAL: modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup - seja ele completo, diferencial ou incremental - são guardados;
VI- SHADOW COPY: uma tecnologia incluída no Microsoft Windows que pode criar cópias de backup ou instantâneos de arquivos ou volumes de computador, mesmo quando estão em uso;
VII- RETENÇÃO: intervalo de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração;
VIII- ROTINA DE BACKUP: procedimentos de realização de cópias de segurança;
IX- BASE DE DADOS OU BANCO DE DADOS: coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;
X- ADMINISTRADOR DE BACKUP: agente público responsável pelos procedimentos de configuração, execução, monitoramento, elaboração de padrões, atendimentos avançados, resolução de incidentes, testes dos procedimentos de backup e restauração;
XI- GESTOR DA INFORMAÇÃO: agente público formalmente responsável pela administração do serviço de TIC e/ou sistema e pelas informações produzidas em seu processo de trabalho. Preferencialmente, deve ser um gestor da área negocial. O respectivo substituto deve ser, preferencialmente, da área negocial;
XII- 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;
XIII- ELIMINAÇÃO: exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
XIV- 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;
XV- INTEGRIDADE: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
XVI- JANELA DE BACKUP: intervalo de tempo durante o qual as cópias de segurança sob execução agendada ou manual poderão ser executadas;
XVII- LOG OU REGISTRO DE AUDITORIA: registro de eventos relevantes em um dispositivo ou sistema computacional;
XVIII- 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;
XIX- RECOVERY POINT OBJECTIVE (RPO): ponto no tempo em que os dados dos serviços de TIC 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;
XX- RECOVERY TIME OBJECTIVE (RTO): tempo estimado para restaurar os dados e tornar os serviços de TIC novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TIC inoperantes até a restauração de seus dados, após um incidente;
XXI- STORAGE: Equipamento especializado para armazenamento de dados na rede.

CAPÍTULO V
DA REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

Art. 5º Esta Norma apresenta a referência legal e de boas práticas, no quadro seguinte:

Orientação	Seção
Decreto Municipal Nº 4060/2024 – Política de Segurança da Informação	Capítulo backup
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art.15
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 VI
DAS DISPOSIÇÕES GERAIS

Seção I
Do Backup e da Restauração de Dados

Art. 6º Esta Norma Complementar aplica-se a todos sistemas, bases de dados, máquinas físicas ou virtuais e repositórios de arquivos institucionais, em formato digital, em uso e de propriedade do Município de Rio das Ostras.
Art. 7º A Política de Backup e Restauração de Dados deve estar alinhada com à Política de Segurança da Informação.
Art. 8º A Política de Backup e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.
Art. 9º As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TIC.
Art. 10. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
Art. 11. As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TIC ou dado salvaguardado, dando prioridade aos serviços de TIC críticos da organização.
Art. 12. O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica.
Art. 13. 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.
Art. 14. A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.
Art. 15. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.
Art. 16. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.
Art. 17. Deverá ser elaborado um Plano de Backup, conforme requisitos presentes no Art. 24º desta Norma, para todos os sistemas, bases de dados, máquinas físicas ou virtuais e repositórios de arquivos institucionais do Município de Rio das Ostras que serão objeto de cópias de segurança, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização.
Art. 18. Todos os dados elaborados são de propriedade intelectual do Município, portanto deverão obrigatoriamente ser armazenados nos storages, a fim de preservar a integridade e continuidade dos serviços prestados.
Art. 19. Os dados armazenados localmente, em microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos repositórios de dados mantido pelas Gestões de Tecnologia da Informação, ou que não façam parte de um plano de backup formalmente definido não terão backup e não haverá garantia de recuperação.

Seção II
Das Atribuições do Administrador do Backup

Art. 20. São atribuições do administrador de backup:
I- propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela Gestão de Tecnologia da Informação;
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;
VI- verificar os eventos gerados pela solução de backup, tomando as providências necessárias para remediação de eventuais falhas;
VII- tomar medidas preventivas para evitar falhas;
VIII- gerenciar mensagens e registros de auditoria (LOGs) de execução dos backups;
XIV- disponibilizar informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos backups;
XV- solicitar restaurações de dados, com anuência do gestor da informação;
XVI- propor modificações visando ao aperfeiçoamento desta Norma;
XVII- providenciar a execução dos testes de restauração.

Seção III
Das Atribuições do Gestor da Informação

Art. 21. São atribuições dos gestores da informação:

I- solicitar, formalmente, a guarda das informações geridas;
II- solicitar, formalmente, a recuperação dos dados;
III- autorizar a solicitação de recuperação de dados feitas pela Gestão de Tecnologia da Informação;
IV- validar, negocialmente, o resultado das restaurações eventualmente solicitadas;
V- validar, negocialmente, o resultado dos testes de restauração dos backups.

Seção IV
Da Solicitação de Backup

Art. 22. As solicitações de backup devem ser realizadas pelo gestor da informação, utilizando sistema de controle eletrônico de atendimentos e enviados ao administrador de backup.
Art. 23. O administrador de backup analisará a solicitação.
Art. 24. Não sendo viável o atendimento da solicitação, o administrador de backup encaminhará, pelo Sistema de Processo Eletrônico, resposta ao gestor da informação.
Art. 25. Sendo viável o atendimento, o administrador de backup deverá elaborar o Plano de Backup em conjunto com o gestor da informação, de modo a atender as necessidades específicas de negócio.
Art. 26. O administrador de backup, caso identifique a necessidade de guarda de informação, pode entrar em contato com o gestor da informação para a elaboração, em conjunto, do Plano de Backup.
Art. 27. O Plano de Backup, assinado pelo gestor da informação e pelo administrador do backup, deverá conter, no mínimo, as seguintes informações:

I- ESCOPO: dados digitais a serem salvaguardados, com apontamento do local, tais como:
a) código fonte;
b) banco de dados;
c) repositório de arquivos;
d) arquivos de configuração de servidores e ativos de rede;
e) máquinas virtuais.

II- TIPO DE BACKUP: completo, incremental, diferencial, podendo ser uma associação destes;
III- FREQUÊNCIA TEMPORAL DE REALIZAÇÃO DO BACKUP: diária, semanal, mensal, anual, podendo ser uma associação destes;
IV- RETENÇÃO: período em que o dado copiado no backup ficará retido e disponível para uso numa eventual recuperação antes de ser substituído por uma versão mais nova). Deverá ser definido com base na criticidade, frequência da atualização dos dados e características específicas de cada sistema;
V- UNIDADE DE ARMAZENAMENTO: indicação da unidade de armazenamento a ser utilizada, podendo ser storage, fita ou outras unidades em uso;
VI- LOCAL DE ARMAZENAMENTO: indicação da localização de armazenamento do backup, incluindo se o backup é acessível por meio da rede, se não é acessível pela rede ou se a unidade de armazenamento se encontra em outra localidade remota, sendo em serviço de nuvem ou em edifício distinto;
VII- TESTES PREVISTOS: devem ser previstos a periodicidade, a abrangência e os procedimentos relativos aos testes que serão realizados;
VIII- PROCEDIMENTO DE RECUPERAÇÃO: documentar o procedimento para recuperar o backup quando necessário;
IX- LOGS: previsão de criação e armazenamento de registros sobre a execução dos testes e das recuperações realizadas, a fim de detectar eventuais falhas e assegurar que houve a realização integral do backup;
X- RPO (RECOVERY POINT OBJECTIVE): indicador que mensura o prazo máximo de perda dados em caso de incidentes;
XI- RTO (RECOVERY TIME OBJECTIVE): indicador que mensura o tempo máximo em que um sistema ou uma informação pode ficar indisponível após um incidente.

Art. 28. Os backups devem ter, sempre que possível, duas cópias realizadas em unidades de armazenamento distintos, sendo um online e outro offline ou disposto em outra localidade.
Art. 29. Os Planos de Backup devem ser criados e executados conforme os dispositivos desta Norma.

Seção V
Da Frequência e Retenção dos dados

Art. 30. Os backups dos serviços de TIC do Município devem ser realizados utilizando-se as seguintes frequências temporais:
I- diária;
II- quinzenal;
III- anual.

Art. 31. Os serviços de TIC do Município devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:
I- diária: 30 (trinta) dias;
II- quinzenal: 45 (quarenta e cinco) dias;
III- anual: 20 (vinte) anos.

Art. 32. Especificidades dos serviços de TIC críticos e dos serviços de TIC não críticos podem demandar frequência e tempo de retenção diferenciados.

Seção VI
Dos Tipos de Backup

Art. 33. Os tipos de backup são:
I- completo (full);
II- incremental;
III- diferencial;
IV- shadow copy

Art. 34. O tipo de backup Shadow Copy será feito de acordo com a seguinte programação padrão:
I- cópias integrais dos dados, dispostos em 4 (quatro) horários durante o dia.

Seção VII
Do Uso da Rede

Art. 35. 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 do Município de Rio das Ostras.
Art. 36. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.
Art. 37. 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.

Seção VIII
Do armazenamento

Art. 38. 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.

Art. 39. 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.
Art. 40. 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.
Art. 41. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.
Art. 42. 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.
Art. 43. 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.

Seção IX
Dos Testes de Backup

Art. 44. Os backups serão verificados periodicamente:
I- pelo menos a cada 15 (quinze) dias, 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- a TI manterá registros de backups e testes de restauração para demonstrar conformidade com esta política;
IV- os testes devem ser realizados em todos os backups produzidos independente do ambiente.

Art. 45. Os testes de restauração dos backups devem ser realizados, por amostragem, pelo menos 1 (uma) vez a cada 45 (quarenta e cinco) dias, 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 X
Do Procedimento de Restauração

Art. 46. 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 de Controle de Atendimentos;
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 XI
Do Descarte de Mídia

Art. 47. A mídia de backup será retirada e descartada conforme descrito neste documento:
I- a TIC 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 TIC garantirá a destruição física da mídia antes do descarte.

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS

Art. 48. Orientações e devidas documentações técnicas a respeito da cópia de segurança e restauração de dados estão disponíveis no Portal GovTIC: https://www.riodasostras.rj.gov.br/govtic/.
Art. 49. Este Decreto entra em vigor na data de sua publicação, aprovando a Norma Complementar para Cópia de Segurança e Restauração de Dados.

Rio das Ostras, 22 de novembro de 2024.

MARCELINO CARLOS DIAS BORBA
Prefeito do Município de Rio das Ostras