ATOS DO EXECUTIVO

GABINETE DO PREFEITO

DECRETO Nº 4132/2024.

DISPÕE SOBRE A APROVAÇÃO DA NORMA COMPLEMENTAR PARA CONTROLE DE ACESSO LÓGICO 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;

D E C R E T A:

CAPÍTULO I
DA NORMA COMPLEMENTAR PARA CONTROLE DE ACESSO LÓGICO

Seção I
Da Introdução
Art. 1º Esta Norma Complementar tem por objetivo estabelecer as normas relativas ao controle do acesso lógico aos ativos de tecnologia da informação no âmbito do Município de Rio das Ostras.

CAPÍTULO II
DO PROPÓSITO

Art. 2º Esta Norma complementar se aplica a todos os usuários de serviços de tecnologia da informação institucionais, tais como: servidores do quadro permanente, comissionados, cedidos, requisitados, terceirizados, discentes, estagiários, prestadores de serviços, usuário de unidade/setor e pessoal de associação temporária que usam serviços de tecnologia da informação do Município de Rio das Ostras com acesso restrito, ou acesso autenticado.
Art. 3º Esta Norma complementar tem o objetivo de estabelecer normas para minimizar riscos à gestão de credenciais de acesso lógico, tendo como objetivos específicos:
I- especificar um modelo mínimo de controle de acesso lógico para proteger os ativos de tecnologia da informação de acessos não autorizados;
II- legitimar o processo de definição de responsabilidades para usuários;
III- especificar procedimentos mínimos para o controle de acesso lógico aos ativos de tecnologia da informação.

CAPÍTULO III
DOS TERMOS E DEFINIÇÕES

Art. 4º Esta Norma complementar tem o objetivo de estabelecer os termos e definições, da seguinte forma:
I- ACESSO: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;
II- AGENTE PÚBLICO: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Municipal, direta e indireta;
III- ATIVOS DE INFORMAÇÃO: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
IV- CONTROLE DE ACESSO: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais;
V- CREDENCIAMENTO: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;
VI- CREDENCIAIS OU CONTAS DE ACESSO: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física, como crachá, cartão e selo ou lógica como identificação usuário e senha;
VII- ACESSO AUTENTICADO: acesso restrito que exige a identificação da pessoa, por meio do usuário e passe, para acessar um serviço de tecnologia da informação;
VIII- ACESSO LÓGICO: direito de acesso na modalidade virtual a um ativo de tecnologia da informação;
IX- ACESSO LÓGICO PRIVILEGIADO: acesso lógico privilegiado é um tipo específico de acesso à aplicação de infraestrutura computacional ou de configuração de serviços em ativos de tecnologia da informação sob responsabilidade da Gestão de Tecnologia, incluindo, mas não se limitando a: sistema operacional, servidor, sistema gerenciador de banco de dados, acesso remoto a servidores, configuração de micro serviços e acesso à serviço que trata dados pessoais;
X- CANCELAMENTO DE USUÁRIO: processo para desabilitar a credencial de um usuário para que o mesmo não possa mais se autenticar como usuário válido;
XI- CONTROLE DE ACESSO LÓGICO: operação de conceder, alterar, analisar e revogar direito de acesso a um ativo de tecnologia da informação;
XII- REVOGAÇÃO DE ACESSO: cancelamento do direito de acesso lógico do usuário a um ativo de tecnologia de informação;
XIII- DADO: é um elemento informativo concreto e sua forma plural expressa uma informação, é o registro do atributo de um ente objeto ou fenômeno onde registro indica o ato de registrar, ou seja, é a gravação ou a impressão de caracteres ou símbolos que tenham um significado em algum documento ou suporte físico;
XIV- DOMÍNIO: agrupamento lógico de computadores em rede que compartilham recursos em um banco de dados de segurança, comum, onde a administração e autenticação são centralizadas. Desta forma um usuário precisa de uma conta para ter acesso ao domínio e aos recursos compartilhados;
XV- ESTAGIÁRIO: educando que esteja frequentando o ensino regular, em instituições de educação superior, de educação profissional, de ensino médio, de educação especial e dos anos finais do ensino fundamental, na modalidade profissional da educação de jovens e adultos, que desenvolve as atividades relacionadas à sua área de formação profissional junto as pessoas Jurídicas de Direito Privado, órgãos da Administração Pública e Instituições de Ensino, que tenham condições de proporcionar experiência prática na sua linha de formação;
XVI- GESTOR DA INFORMAÇÃO: usuário que gerou a informação, que responde pelo seu conteúdo ou que foi formalmente designado para definir, alterar a sua classificação nos graus de sigilo e perfil de acesso dos demais usuários e processos;
XVII- INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
XVIII- LOG OU REGISTRO DE AUDITORIA: registro de eventos relevantes em um dispositivo ou sistema computacional;
XIX- PERFIL DE ACESSO DO USUÁRIO: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

XX- RECURSOS DE REDE: dispositivos (impressoras, scanners, multifuncionais, e outros) ou serviços (sistemas, portais, e outros) disponibilizados para os usuários por meio de uma rede de dados;
XXI- SERVIÇO DE DIRETÓRIO: serviço que armazena e organiza informações relativas a recursos disponíveis e usuários de uma rede de dados. Permite que o administrador da rede gerencie o acesso de usuários e sistemas aos recursos disponíveis;
XXII- USUÁRIO: servidores, terceirizados, colaboradores, procuradores, advogados da união, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da Administração Pública Municipal, formalizada por meio da assinatura de Termo de Responsabilidade.

CAPÍTULO IV
DA REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

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

Orientação	Seção
Decreto Municipal Nº 4060/2024 – Política de Segurança da Informação - PSI	Em sua íntegra
Norma NBR ISO/IEC 17799 - Tecnologia da Informação	Controle de acessos
Norma NBR ISO/IEC 27000 - Tecnologia da Informação	Sistemas de Gestão de Segurança da Informação
CIS - Center for Internet Security	Em sua íntegra
MITRE ATT&CK	Em sua íntegra

CAPÍTULO V
DAS DISPOSIÇÕES GERAIS

Seção I
Dos Princípios
Art. 6º O controle de acesso lógico a ativos de tecnologia da informação no âmbito do Município de Rio das Ostras busca atender aos seguintes princípios:
I- PRIVACIDADE: respeito à privacidade dos usuários e a finalidade de tratamento dos dados pessoais;
II- CONFIDENCIALIDADE: garante que somente o usuário autorizado possa acessar o ativo de informação;
III- SEGURANÇA: previne os riscos de acessos indesejáveis e vazamento de informações tratadas pelo Município;
IV- AUTENTICIDADE: garante que usuários anônimos acessem somente os ativos de tecnologia da informação considerados públicos;
V- INTEROPERABILIDADE E OTIMIZAÇÃO DE RECURSOS: uso de tecnologias ou processos que atendam o maior número de ativos de tecnologia da informação, quando for viável;
VI- NÃO REPÚDIO: acurácia e precisão na identificação das atividades do usuário.

Seção II
Da Solicitação de Conta de Acesso
Art. 7º As solicitações de contas de acesso a recursos computacionais, deverá ser realizada por meio de ferramenta informatizada definida pela Gestão de Tecnologia do Município.
Art. 8º Os formulários de solicitação deverão ser preenchidos com todos os dados solicitados.
Art. 9º Somente solicitações de contas devidamente assinadas e carimbadas pelo solicitante e, pelo menos pela chefia imediata, serão aceitas.

Seção III
Da Política de Senha
Art. 10. Com relação às senhas de acesso, deve-se observar que:
I- deverão ter no mínimo 08 (oito) caracteres e conter, obrigatoriamente, caracteres alfanuméricos (combinação de letras e números) e caracteres especiais (espaços em branco, símbolos, sinais de pontuação e outros);
II- é vedada a reutilização das últimas 05 (cinco) senhas utilizadas pelo usuário;
III- terão validade de 01 (um) ano;
IV- podem ser alteradas sempre que preciso ou quando o usuário achar necessário.

Seção IV
Da Gestão de Acesso Lógico
Art. 11. A concessão de acesso lógico deve ser efetivada mediante autorização ou consentimento do respectivo responsável pelo processo de negócio que gerencia o ativo de tecnologia de informação a ser acessado.
Art. 12. A concessão de acesso lógico deve estar em conformidade com os normativos e procedimentos institucionais relativos à segurança da informação e privacidade de dados.
Art. 13. Uma pessoa deve ter somente 01 (uma) identificação de usuário ativa no serviço de tecnologia da informação.
Art. 14. Todo usuário deve atestar conhecimento sobre suas responsabilidades em relação aos normativos de segurança da informação e privacidade, no 1º (primeiro acesso), anualmente e sempre que houver alterações nestes normativos.
Art. 15. O uso compartilhado de usuário não é permitido.
Art. 16. São obrigações do usuário, dentre outras:
I- não divulgar, nem mesmo compartilhar, os códigos de segurança que lhe forem atribuídos (credenciais de acesso), os quais são pessoais e intransferíveis;
II- não utilizar as credenciais para acessar os recursos disponíveis em mais de uma estação de trabalho simultaneamente;
III- não solicitar credenciais de acesso customizadas;
IV- não fazer uso das credenciais de acesso de outros usuários;
V- comunicar à chefia imediata ou responsável pela administração do sistema ou rede corporativas quaisquer violações ou incidentes referentes à proteção do equipamento utilizado, do software ou de outros ativos da informação;
VI- sempre que for necessário, afastar-se da estação de trabalho, certificar-se de que a sessão de rede ou acesso ao sistema corporativo esteja encerrado ou bloqueado;
VII- efetuar processo de alteração da sua senha em seu 1º (primeiro) acesso à rede de dados corporativa.
Art. 17. O cancelamento de todos os direitos de acesso vigentes do usuário deve ocorrer de forma imediata, e geral em todos os ativos de tecnologia da informação, quando a pessoa encerrar o vínculo institucional, através de solicitação da chefia imediata ou do próprio usuário.
Art. 18. É dever da chefia imediata comunicar formalmente a mudança de lotação ou desligamento de usuário(a) aos responsáveis pela gestão do direito de acesso lógico, bem como os direitos de acesso lógico a serem cancelados em decorrência da respectiva mudança da pessoa na unidade.

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;