POLITICA DE CONTROLE DE ACESSO

1- OBJETIVO DA POLÍTICA

A Política de Controle de Acesso objetiva estabelecer controles de identificação, autenticação e autorização para salvaguardar as informações da Secretaria Municipal de Saúde do Rio de Janeiro (SMS-Rio) estejam elas em qualquer meio, seja digital ou físico, a fim de evitar a quebra da segurança da informação e quaisquer acessos não autorizados que implique em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Sem controles de autorização, identificação e autenticação, existe o risco potencial de que os sistemas de informação possam ser acessados ilicitamente e que a segurança desses sistemas de informação seja comprometida.

Considera-se, portanto, que as credenciais: crachá de identificação funcional e logins de acesso dos sistemas de informações, são pessoais e intransferíveis e são o único método legítimo pelo qual o direito de acesso físico e/ou lógico podem ser exercidos.

Os controles de autorização, identificação e autenticação garantem que apenas usuários autorizados tenham acesso físico ou façam uso dos sistemas de informação da SMS-Rio.

2- ESCOPO

Esta Política se aplica a todas as informações, cuja SMS-Rio seja o agente de tratamento, ao meio utilizado para este tratamento, seja digital ou físico, e as dependências físicas desta organização, incluidas todas unidades de saúde do Municipio do Rio do Janeiro, bem como a qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento.

Especificamente, inclui:

- Todos os funcionários, sejam servidores efetivos ou temporários, da SMS-Rio.
- Todos os contratados e terceiros que trabalham para a SMS-Rio.

- Todos os funcionários de parceiros que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação da SMS-Rio.

Essa Política se refere à rede Iplan de uso interno da SMS-Rio. Demais sistemas que são ou forem utilizados pela SMS-Rio, serão objeto de politicas de acesso apartadas.

3- TERMOS DE DEFINIÇÕES

ACESSO - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

ADMINISTRADOR DE PERFIL INSTITUCIONAL - agentes públicos que detenham autorização de responsável pela área interessada para administrar perfis institucionais de órgão ou entidade da administração pública federal, direta e indireta, nas redes sociais;

ADMINISTRADOR DE REDE - pessoa física que administra o segmento de rede correspondente à área de abrangência da respectiva unidade;

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 federal, direta e indireta;

AGENTES DE TRATAMENTO - o controlador ou o operador;

AMBIENTE CIBERNÉTICO - inclui usuários, redes, dispositivos, *software*, processos, informação armazenada ou em trânsito, serviços e sistemas que possam ser conectados direta ou indiretamente a redes de computadores;

ARQUIVO: agrupamento de registros que, geralmente, seguem uma regra estrutural e que possuem informações (dados).

AUTENTICIDADE: garantia de que uma informação, produto ou documento é do autor a quem se atribui.

CONFIDENCIALIDADE: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

CONTA DE SERVIÇO - conta de acesso à rede corporativa de computadores, necessária a um procedimento automático (aplicação, script, entre outros) sem qualquer intervenção humana no seu uso;

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. Via de regra, requer procedimentos de autenticação;

CREDENCIAIS DE ACESSO: conjunto composto pelo nome de conta e respectiva senha, utilizado para o ingresso ou acesso (login) em equipamentos, rede ou sistema.

CRIPTOGRAFIA: arte e ciência de esconder o significado de uma informação de receptores não desejados.

ESTAÇÕES DE TRABALHO: computador pessoal utilizado para trabalho nas Unidades Organizacionais.

INTEGRIDADE: propriedade de salvaguarda da exatidão e completeza da informação contra alterações, intencionais ou acidentais, em seu estado e atividades.

PRIVILÉGIO MÍNIMO: conceito que define que uma pessoa só precisa acessar os sistemas e recursos mínimos necessários para realizar suas atividades.

RECURSOS DE TI: todo equipamento ou dispositivo que utiliza tecnologia da informação, bem como qualquer recurso ou informação que seja acessível por meio desses equipamentos ou dispositivos tecnológicos, tais como impressoras, sistemas, programas, softwares, acessos à rede local, internet, VPN (rede particular virtual), pendrives, smartcards, tokens, smartphones, modens sem fio, desktops, pastas compartilhadas em rede, entre outros.

SISTEMA DE INFORMAÇÃO: aplicação da tecnologia da informação que dá apoio às atividades de determinada área de conhecimento, visando otimizar as operações, o gerenciamento e a decisão, trabalhando os dados e transformando-os em informação.

TI: Tecnologia da Informação.

UNIDADE ORGANIZACIONAL: unidade em que está lotado o empregado, assessor, terceirizado, estagiário ou aprendiz.

USUÁRIO: pessoa física ou jurídica que opera algum sistema informatizado da SMS-Rio.

WEB: Rede Mundial de Computadores.

WEBCONFERÊNCIA: reunião ou encontro virtual realizado pela internet por meio de aplicativos ou serviço com possibilidade de compartilhamento de apresentações, voz, vídeos, textos e arquivos por meio da web.

Para outras definições, acessar o link https://www.gov.br/gsi/pt-br/dsic/glossario-de-seguranca-da-informacao-1

4- REFERÊNCIAS LEGAIS E DE BOAS PRÁTICAS

Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados
ABNT NBR ISO/IEC 27002: 2013. Código de Prática para controles de Segurança da Informação
CIS V8 – Capítulo 6: Gestão de Controle de Acesso

5- ACESSO LÓGICO

O acesso lógico aos recursos da Rede Local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela IplanRio – Empresa Pública de Informática do Municipio do Rio de Janeiro e pela àrea de Tecnologia da Informação da Secretaria Municipal de Saúde do Rio de Janeiro, baseado nas responsabilidades e tarefas de cada usuário.

I. Terão direito a acesso lógico aos recursos da Rede Local os usuários de recursos de tecnologia da informação.

II. Para fins desta Política, consideram-se usuários de recursos de tecnologia da informação servidores ocupantes de cargo efetivo ou cargo em comissão, ocupantes de emprego público em exercício, assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade na área de Tecnologia da Informação da Secretaria Municipal de Saúde do Rio de Janeiro.

III. O acesso remoto deve ser realizado por meio de VPN – Rede Virtual Privada, após as devidas autorizações.

IV. Deve ser utilizado os sistemas homologados e autorizados de acesso remoto.

V. O acesso a todas as aplicações corporativas ou de terceiros que estejam hospedados em fornecedores deve utilizar a politica de segurança vigente.

A SMS-Rio junto com os setores responsáveis de Tecnologia da Informação, deveram estabelecer e manter um inventário de todas as contas gerenciadas, este deve incluir contas de usuário, administrativas, testes e serviço. Em caso de contas de serviço, o inventário deve conter no mínimo informações de:

a. Departamento/Setor proprietário.

b. Data de criação/última autorização de renovação de acesso;

A área de Tecnologia da Informação da SMS-Rio deve estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, tal inventário deve ser revisado periodicamente.

A área de Tecnologia da Informação da SMS-Rio deve definir e manter o controle de acesso dos usuários baseado em funções.

I. Deve ser elaborada a documentação dos direitos dos acessos para cada função dentro da organização.

II. Deverão ser realizadas análises de controle de acesso aos ativos institucionais para validar se todos os privilégios estão autorizados para a execução de atividades de cada função, este processo deve ser repetido de forma periódica ou quando novas funções e ativos de informação forem inseridos na organização.

6- CONTA DE ACESSO LÓGICO E SENHA

Para utilização das estações de trabalho na Secretaria Municipal do Rio de Janeiro e suas unidades de saúde, será obrigatório o uso de uma única identificação (*login*) e de senha de acesso, fornecidos pela SMS-Rio ou pela entidade parceira, mediante solicitação formal pelo responsável da unidade do requisitante.

O *login* e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pela área de Tecnologia da Informação da SMS-Rio quando constatada qualquer irregularidade.

No caso de bloqueio para retomar o acesso à rede, deverá ser formalizada nova requisição pelo titular da unidade do requisitante à sua Coordenação e a área de Tecnologia da Informação da SMS-Rio.

O padrão adotado para o formato da conta de acesso do usuário é a sequência primeiro nome + ponto + último nome do usuário ou a matricula do usuário, como por exemplo, João.silva ou 0333555.

Nos casos de já existência de conta de acesso para outro usuário, a área de Tecnologia da Informação da SMS-Rio realizará outra combinação utilizando o nome completo do usuário para o qual a conta está sendo criada.

O padrão adotado para o formato da senha é o definido pela área de Tecnologia da Informação da SMS-Rio e pela IplanRio, que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores.

I. A formação da senha da identificação (*login*) de acesso à Rede Local deve seguir as regras de:

a) Possuir tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras e números, para contas que utilizam MFA e 14 caracteres para contas que não utilizam MFA;

b) Recomenda-se a utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &,...);

c) Não ser formada por sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações;

d) Não utilizar termos óbvios, tais como: Brasil, senha, usuário, *password* ou *system*.

e) Não reutilizar as últimas [05 (cinco)] senhas.

II. A área de Tecnologia da Informação da SMS-Rio e a IplanRio fornecerá uma senha temporária para cada conta de acesso criada no momento da liberação dessa conta e a mesma deverá ser alterada pelo usuário quando do primeiro acesso à Rede Local.

As senhas de acesso serão renovadas a cada 60 (sessenta) dias, devendo o usuário ser informado antecipadamente a fim de que ele próprio efetue a mudança. Caso não efetue a troca no prazo estabelecido, será bloqueado seu acesso à Rede Local até que a nova senha seja configurada.

7- BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

A conta de acesso será bloqueada nos seguintes casos:

I. Após 5 (cinco) tentativas consecutivas de acesso errado;

II. Solicitação do superior imediato do usuário com a devida justificativa;

III. Quando da suspeita de mau uso dos serviços disponibilizados pela SMS-Rio ou descumprimento da Política de Segurança da Informação e normas correlatas em vigência.

IV. Após 45 (quarenta e cinco) dias consecutivos sem movimentação pelo usuário.

O desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do superior imediato do usuário ao área de Tecnologia da Informação da SMS-Rio.

Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato ou do Coordenação de Gestão de Pessoas – CGP.

A conta de acesso não utilizada há mais de 180 (cento e oitenta) dias poderá ser cancelada.

A área de Tecnologia da Informação da SMS-Rio, deve configurar o bloqueio automático de sessão nos ativos após um período de inatividade preestabelecido. Tal prazo pode ser específico para cada tipo de ativo.

A área de Tecnologia da Informação da SMS-Rio deve, sempre que possível, priorizar a revogação/desativação de contas com o objetivo de manter dados e logs para possíveis auditorias.

8- MOVIMENTAÇÃO INTERNA

Quando houver mudança do usuário para outro setor ou o usuário ocupar uma nova função, os direitos de acesso à Rede Local devem ser revogados.

I. O novo superior imediato ou a Coordenção de Gestão de Pessoas deve realizar a solicitação de novos acessos de acordo com novo setor / função do usuário.

II. Os direitos de acesso antigos devem ser imediatamente cancelados conforme solicitação do antigo superior imediato ou da Coordenação de Gestão de Pessoas.

9- ADMINISTRADORES

A utilização de identificação (*login*) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

I. Somente os técnicos da área de Tecnologia da Informação da SMS-Rio, devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede.

II. Na necessidade de utilização de *login* com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para o área de Tecnologia da Informação da SMS-Rio, que poderá negar os casos em que entender desnecessária a utilização.

III. Se concedida a permissão ao usuário como administrador local na estação de trabalho, esse será responsável por manter a integridade da máquina, não podendo instalar, desinstalar ou remover qualquer programa sem autorização formal área de Tecnologia da Informação da SMS-Rio

IV. Caso constatada a irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão.

V. A identificação (*login*) com privilégio de administrador nos equipamentos locais será fornecida em caráter provisório, podendo ser renovada por solicitação formal do titular da unidade requisitante.

VI. Salvo para atividades específicas da área responsável pela gestão da tecnologia da informação do órgão, não será concedida, para um mesmo usuário, identificação (login) com privilégio de administrador para mais de uma estação de trabalho, ou para acesso a equipamentos servidores e a dispositivos de rede.

VII. Excepcionalmente, poderão ser concedidas identificações (login) de acesso à rede de comunicação de dados a visitante em caráter

temporário após apreciação da Coordenação responsável por meio da área de Tecnologia da Informação da SMS-Rio

VIII. A área de Tecnologia da Informação da SMS-Rio deve restringir os privilégios de administrador a contas de administrador dedicados nos ativos de informação, para que o usuário com privilégio de administrador não consiga realizar atividades gerais de computação, como navegação na Internet, e-mail e uso do pacote de produtividade, estas atividades deverão ser realizadas preferencialmente a partir da conta primária não privilegiada do usuário.

10- RESPONSABILIDADES

É de responsabilidade do superior imediato do usuário comunicar formalmente à Coordenação de Gestão de Pessoas e à área de Tecnologia da Informação da SMS-Rio o desligamento ou saída do usuário da Secretaria Municipal de Saúde do Rio de Janeiro para que as permissões de acesso à Rede Local sejam canceladas.

Caberá à Coordenação de Gestão de Pessoas da Secretaria Municipal de Saúde do Rio de Janeiro a comunicação imediata ao área de Tecnologia da Informação da SMS-Rio sobre desligamentos, férias e licenças de servidores e estagiários, para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos.

É responsabilidade da Coordenação de Gestão de Pessoas da Secretaria Municipal de Saúde do Rio de Janeiro a comunicação imediata à área de Tecnologia da Informação da SMS-Rio da Informação sobre desligamentos, férias e licenças de funcionários de empresas prestadoras de serviços terceirizados, para que seja efetuado o bloqueio momentâneo ou revogação definitiva da permissão de acesso aos recursos.

I. Os serviços serão filtrados por programas de *antivírus*, *anti-phishing* e *anti-spam* e, caso violem alguma regra de configuração, serão bloqueados ou excluídos automaticamente.

II. Nenhum técnico do fora da àrea de Tecnologia da informação da Secretaria de Saúde do Rio de Janeiro terá acesso ao conteúdo das informações armazenadas nos equipamentos servidores da Secretaria Municipal de Saúde do Rio de Janeiro .

É de responsabilidade da área de Tecnologia da Informação da SMS-Rio o monitoramento da utilização de serviços de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como bloquear, temporariamente, sem aviso prévio, a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica do [Nome do órgão ou entidade].

O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à Rede Local e a recursos de tecnologia custodiados ou de propriedade da Secretaria Municipal de Saúde do Rio de Janeiro.

I. O usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos.

II. A utilização simultânea da conta de acesso à Rede Local em mais de uma estação de trabalho ou notebook deve ser evitada, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica.

III. O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à Rede Local.

É dever de o usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a Instituição, a saber:

I. Não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;

II. Evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;

III. Interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;

IV. Não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;

V. Não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

VI. Utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;

VII. Não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo- as como pessoais e intransferíveis;

VIII. Assinar o Termo de Responsabilidade (Modelo – Anexo I) quanto a utilização da respectiva conta de acesso.

11- DA UTILIZAÇÃO DO CORREIO ELETRÔNICO CORPORATIVO

O correio eletrônico é o recurso corporativo para comunicação a ser utilizado de modo compatível com o exercício da função, sem comprometer a imagem da SMS-Rio nem o tráfego de dados na rede de computadores da instituição.

Todas as mensagens eletrônicas enviadas e recebidas nos domínios da SMS-Rio terão registrados os dados: data e hora do envio ou recebimento, remetente e destinatário.

A SMS-Rio junto com os setores responsáveis, deverão implantar mecanismos que evitem o envio e a recepção de mensagens que possam comprometer a segurança do serviço de correio eletrônico.

A área de Tecnologia da Informação da SMS-Rio poderá estabelecer cotas para limitar o espaço de armazenamento das caixas postais, por Unidade Organizacional e por usuário.

A área de Tecnologia da Informação da SMS-Rio não acessará mensagens individuais de caixas de e-mail, salvo para atender aos seguintes objetivos:

I. verificar a obtenção, retenção, uso e divulgação de informações por meio ou com fins ilícitos, ou em desacordo com as normas regulamentares sobre segurança da informação, mediante autorização da autoridade gestora da Subsecretaria ou Coordenação;

II. recuperar conteúdo de interesse da SMS-Rio, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização da autoridade gestora da Subsecretaria ou Coordenação;

III. atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização da autoridade gestora da Subsecretaria ou Coordenação;

IV. atender à determinação judicial; e

V. realizar a recuperação de mensagens do backup, a pedido do próprio usuário.

O envio de mensagens a componentes da lista de endereços e grupos de e-mails da SMS-Rio restringir-se-á a assuntos de interesse geral da instituição ou do Sistema Processo.rio.

A exclusão de caixas postais ocorrerá com o desligamento do usuário.

São vedadas as seguintes ações relacionadas à utilização do correio eletrônico:

I. acesso ou tentativa de acesso à caixa postal em desacordo com o previsto no § 4º do Art. 50;

II. envio ou armazenamento de mensagem de conteúdo incompatível com as atribuições do usuário, incluindo as que contém ofensas, comentários discriminatórios e pornografia; e

III. adulteração de dados referentes à origem da mensagem nos campos de controle e cabeçalho.

Para os fins deste artigo, considera-se armazenado o e-mail aberto e mantido na caixa postal do usuário.

A área de Tecnologia da Informação da SMS-Rio prestará suporte para a configuração e utilização da tecnologia adotada para o serviço de correio eletrônico corporativo.

12- DA UTILIZAÇÃO DO SISTEMA DE ARQUIVOS

O sistema de arquivos compreende um conjunto de pastas armazenadas em servidor de arquivos e compartilhadas em rede, que podem ser compartilhadas

entre todos os usuários ou restrito a usuários de determinada Unidade Organizacional ou de determinado projeto.

A SMS-Rio junto com os setores responsáveis, deverão realizar o backup dos arquivos armazenados no servidor de arquivos, conforme discriminado na Política de Segurança da Informação.

O backup de arquivos de pastas de usuário armazenadas nas estações de trabalho é de responsabilidade do usuário.

A área de Tecnologia da Informação da SMS-Rio poderá limitar o tipo de extensão dos arquivos a serem armazenados nas pastas das Unidades Organizacionais.

A área de Tecnologia da Informação da SMS-Rio não acessará os arquivos armazenados nas pastas das Unidades Organizacionais e dos usuários, salvo nas seguintes situações:

I. verificar a obtenção, retenção, uso e divulgação de informações por meio ou com fins ilícitos, ou em desacordo com as normas regulamentares sobre segurança da informação, mediante autorização da autoridade gestora da Subsecretaria ou Coordenação;

II. recuperar conteúdo de interesse do CFC, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização da autoridade gestora da Subsecretaria ou Coordenação;

III. atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização da autoridade gestora da Subsecretaria ou Coordenação;

IV. atender à solicitação judicial; e

V. realizar a recuperação de arquivos do backup, a pedido do usuário.

13- DISPOSIÇÕES GERAIS

Os incidentes que afetem a Segurança das Informações, assim como o descumprimento da Política de Segurança da Informação e Normas de Segurança devem ser obrigatoriamente comunicados pelos usuários à área de

Tecnologia da Informação da SMS-Rio e aos respectivos Encarregados de Dados Pessoais.

Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a área de Tecnologia da Informação da SMS-Rio fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

I. Nos casos em que o ator da quebra de segurança for um usuário, a área de Tecnologia da Informação da SMS-Rio comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis.

II. Ações que violem o Programa de Privacidade e Proteção de Dados Pessoais da SMS-Rio ou que quebrem os controles de Segurança da Informação serão passíveis de sansões civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

III. Processo administrativo disciplinar específico deverá ser instaurado para apurar as ações que constituem em quebra das diretrizes impostas por esta Norma e pelo Decreto Rio Nº 53700 de 8 de dezembro de 2023, que Institui a Política de Segurança da Informação – PSI, no âmbito do Poder Executivo Municipal do Rio de Janeiro/RJ, e dá outras providências.

IV. A resolução de casos de violação/transgressões omissos nas legislações correlatas será resolvida pelo Comitê de Governança Proteção de Dados da Secretaria Municipal de Saúde do Rio de Janeiro.

14- MUDANÇAS:

A presente versão 1.0 deste instrumento foi atualizada pela última vez em: Agosto de 2024.

O editor se reserva o direito de modificar no site, a qualquer momento, as presentes normas, especialmente para adaptá-las às evoluções das medidas de segurança da informação da SMS-Rio, seja pela disponibilização de novas funcionalidades, determinações ou responsabilidades, seja pela supressão ou modificação daquelas já existentes.

Qualquer alteração e/ou atualização neste instrumento passará a vigorar a partir da data de sua publicação no sítio do serviço e deverá ser integralmente observada pelos usuários.