Rio PREFEITURA | RIOSAÚDE

POLÍTICA

SEGURANÇA DA INFORMAÇÃO

RIO DE JANEIRO
2023

Rio PREFEITURA | RIOSAÚDE

POLÍTICA

SEGURANÇA DA INFORMAÇÃO

RIO DE JANEIRO
2023

SUMÁRIO

MENSAGEM DO **DIRETOR PRESIDENTE**

A gestão de segurança da informação deve ser suportada por ações e métodos que visem à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento das informações e dados, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional dos processos institucionais estratégicos, operacionais e táticos.

A Política de Segurança da Informação (PSI) faz parte de um conjunto de ações, políticas ou boas práticas para o emprego seguro de informações de empresas.

Para simplificar ainda mais, a PSI é composta por regras que limitam o acesso e a transmissão da informação. É como uma espécie de manual para guiar e determinar quais parâmetros garantem a segurança da informação em uma empresa.

Esse documento exige que suas informações sejam atualizadas constantemente e conta com a participação da Alta Administração, colaboradores e equipe de Tecnologia da Informação da empresa.

Sendo assim, a RioSaúde, em atenção às boas práticas de Governança Corporativa, e pelo Programa de Compliance, produziu a presente Política, em atendimento às normas e dispositivos que regem o tema, além de ter sido desenvolvida com base três princípios básicos da segurança da informação: confidencialidade, integridade e disponibilidade.

Roberto Rangel
Presidente - RioSaúde

INTRODUÇÃO

A Empresa Pública de Saúde do Rio de Janeiro - RioSaúde é uma sociedade anônima de capital fechado, no entanto, preza pela transparência de uma instituição que oferece serviços públicos. Por meio da contratação de profissionais em concurso público e processos seletivos – somam-se, aproximadamente, 16 mil colaboradores que se dedicam diariamente nas unidades de saúde espalhadas pela cidade do Rio – esta empresa tem por objetivo oferecer um atendimento acolhedor e cuidadoso a milhares de pacientes e suas famílias.

Com a missão de atuar na execução de políticas públicas de saúde, realiza uma gestão transparente, íntegra, eficiente e ágil, com profissionais capacitados, garantindo acesso, segurança e qualidade nos serviços prestados à população.

A importância em ter uma Política de Segurança da Informação por parte desta Empresa Pública decorre do avanço tecnológico na área da saúde, onde se tornou necessário a adoção dos padrões de segurança e privacidade dos dados. Garantir o sigilo e integridade dessas informações se torna fundamental, uma vez que a sua manipulação implica em questões de princípios éticos, médicos, sociais e legais.

Esta Política tem por objetivo definir diretrizes, responsabilidades, competências e princípios de Segurança da Informação no âmbito da Empresa Pública de Saúde do Rio de Janeiro – RioSaúde, em atendimento ao disposto nos Decretos do Município do Rio de Janeiro – n.º 44.276, de 01 de março de 2018 e n.º 53700 de 8 de dezembro de 2023.

Na RioSaúde seus colaboradores deverão respeitar todas as normas, regras e legislações pertinentes e em conformidade às boas práticas da Segurança da Informação, dentre estas:

- Lei n.º 8.159, de 8 de janeiro de 1991: dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências e a Lei Municipal n.º 3.404, de 5 de junho de 2002, cujo dispositivo dispõe sobre a política municipal de arquivos Públicos privados, o acesso aos documentos Públicos municipais e dá outras providências.

- Lei n.º 9.983, de 14 de julho de 2000: dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

- Lei n.º 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação (LAI): Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei n.º 8.112, de 11 de dezembro de 1990; revoga a Lei n.º 11.111, de 5 de maio de 2005, e dispositivos da Lei n.º 8.159, de 8 de janeiro de 1991; e dá outras providências e Decreto RIO n.º 44.745/2018 que regula a legislação no âmbito do Município.

- Decreto RIO nº 44.745 de 19 de julho de 2018, regulamenta a Lei de Acesso à Informação (LAI) em âmbito municipal;

- Lei n.º 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD): dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público, ou privado, visando proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

- Decreto Municipal n.º 44.276, de 1 de março de 2018: Estabelece a Política de Segurança da Informação da prefeitura da Cidade do Rio de janeiro;

- Norma ABNT NBR ISO/IEC 27005:2023: estabelece diretrizes para o processo de gestão de riscos de segurança da informação;

- Norma ABNT NBR ISO/IEC 27001:2023 estabelece os elementos de um Sistema de Gestão de Segurança da Informação e Comunicações;

- Norma ABNT NBR ISO/IEC 27002:2023 institui o código de melhores práticas para Gestão de Segurança da Informação e da Comunicação;

ABRANGÊNCIA

A Política deverá ser cumprida por todos os agentes públicos, colaboradores, empregados, terceirizados, diretores, coordenadores, gerentes, estagiários, membros de Comitês e membros dos Conselhos Fiscal e Administração, bem como a quaisquer outras pessoas ligadas a RioSaúde como terceiros, fornecedores ou parceiros, que em função do seu cargo, posição ou que de forma contratual, atuem em nome da empresa.

OBJETIVOS

A presente Política de Segurança da Informação foi desenvolvida com o compromisso de:

a. Definir princípios, diretrizes, responsabilidades e competências relacionadas à Governança de dados e Gestão de Segurança da Informação para salvaguardar ativos de

informação e garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações que suportam as atividades e os objetivos estratégicos da companhia.

b. Estabelecimento de metas claras, incluindo a proteção de ativos, a garantia de confidencialidade e integridade dos dados, a manutenção da disponibilidade de sistemas e informações, bem como a regulamentação do acesso com base em princípios de identificação e autenticação sólidos.

c. Definição de diretrizes rigorosas para senhas seguras e a gestão de acesso responsável.

d. Compromisso com a conformidade legal e com a avaliação constante de riscos, garantindo a melhoria contínua das práticas de segurança da informação.

e. Por fim, fomento do comprometimento dos agentes públicos na implantação e melhoria contínua de uma cultura de Segurança da Informação através da conscientização, educação e fornecimento de treinamento contínuo para os colaboradores.

A presente Política serve como base sólida para a criação de uma cultura de segurança da informação que deve se estender por toda a empresa, protegendo não só ativos críticos, como, por exemplo, servidores, backups, dentre outros ativos que são essenciais para as operações da Empresa, mas também todo e qualquer tipo de informação.

DEFINIÇÕES

Ameaça: qualquer evento que tenha potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos seus ativos ou prejuízos decorrentes de situações inesperadas (por exemplo: incêndio, falha de equipamentos, indisponibilidade de sistemas ou serviços, destruição de informações sensíveis, dentre outros); fornecedores e prestadores de serviços da empresa, que não sejam partes relacionadas;

Ativos críticos: elementos, recursos ou processos que desempenham um papel fundamental na operação, desempenho e sucesso contínuo da organização. Esses ativos são considerados críticos porque sua interrupção, perda ou comprometimento significativo pode ter um impacto significativo nas operações da empresa, na sua capacidade de atender aos objetivos estratégicos e até mesmo na sua sobrevivência.

Ativos de Informação: elementos que transformam, transportam, guardam e descartam dados ou informações, incluindo a própria informação e que se dividem em 6 (seis) grupos: equipamentos, aplicações, usuários, ambientes, informações e processos.

Ativo tecnológico: equipamento de TIC, software ou aplicação que suporta as atividades, processos de negócio e serviços de uma organização;

Autenticidade: garantia de que os ativos da informação identificados em um processo de comunicação como remetentes ou destinatários sejam realmente quem dizem ser, ou seja, diz respeito à veracidade das identidades dos ativos envolvidos em um processo de comunicação;

Autorização: a concessão de permissões específicas a usuários ou sistemas para acessar recursos ou informações.

Classificação da Informação: é o grau de sensibilidade de uma informação para o negócio diante de uma possível quebra de segurança, ou seja, do comprometimento dos princípios básicos de segurança da informação: confidencialidade, integridade e disponibilidade.

Confidencialidade: o princípio de proteger informações contra acesso ou divulgação não autorizados, garantindo que apenas pessoas autorizadas tenham acesso.

Continuidade de negócios: capacidade estratégica e tática da companhia de se planejar e responder a incidentes que gerem interrupções em suas atividades ou serviços, visando minimizar impactos e manter suas operações em um nível aceitável de disponibilidade previamente definido;

Conscientização em Segurança: programas de treinamento e educação para funcionários sobre práticas seguras de segurança da informação.

Criptografia: o processo de codificar informações para torná-las ilegíveis para qualquer pessoa que não possua a chave de descriptografia.

Dados: trata-se da informação não processada.

Disponibilidade: o princípio de garantir que as informações estejam disponíveis quando necessário para os usuários autorizados, minimizando interrupções.

Firewall: um dispositivo de segurança que controla o tráfego de rede e protege a rede contra ameaças externas.

Gestão de acessos: um conjunto de diretrizes e requisitos para criar senhas seguras e proteger contas de acesso.

Incidente de Segurança: qualquer evento que viole ou ameace violar a segurança da informação, exigindo investigação e resposta.

Informação: resultado do processamento, manipulação e organização de dados de tal forma que represente um acréscimo ao conhecimento da pessoa que a recebe, podendo se apresentar de diversas formas, como texto, imagem, áudio, etc.

Integridade: o princípio de manter a precisão e a confiabilidade das informações, protegendo-as contra alterações não autorizadas.

LOG: Os arquivos de *log* são usados para registrar ações dos usuários e servem de fontes de informação para auditorias futuras. Eles registram quem acessou os recursos computacionais, aplicativos, arquivos de dados e utilitários, quando foi feito o acesso e que tipo de operações foram efetuadas. O registro de *logs* tem como objetivo principal a detecção de ações impróprias nos sistemas de informação.

Malware: software malicioso projetado para danificar, comprometer ou roubar informações, como vírus, *spyware* e *ransomware*.

Phishing: uma técnica de ataque em que os atacantes tentam enganar os usuários para que revelem informações confidenciais, geralmente por e-mail ou sites falsos.

Plano de Resposta a Incidentes: procedimentos documentados para lidar com incidentes de segurança, incluindo comunicação, contenção e recuperação.

Recurso de TIC (Tecnologia da Informação e da Comunicação): são os ativos da informação tecnológicos que transformam, transportam, guardam e descartam dados ou informações, por exemplo: computadores, celulares, notebooks, roteadores de wi-fi.

Risco: probabilidade de ameaças explorarem vulnerabilidades, comprometendo a confidencialidade, integridade ou disponibilidade da informação, causando impactos para as atividades da companhia.

Sistema de informação: sistema composto por um conjunto de ativos da informação que tem por objetivo armazenar, transportar e processar informações visando suportar funções, serviços ou processos da companhia.

Vulnerabilidade: uma fraqueza ou falha em um sistema, aplicativo ou procedimento que pode ser explorada por ameaças para comprometer a segurança da informação.

PRINCÍPIOS

Visando as melhores práticas de governança corporativa, e com finalidade de criar um ambiente organizacional que promova a integridade pública, transparência, ética, a conformidade legal e a prevenção da corrupção em todas as suas formas, a fim de inibir atos de corrupção e suas variáveis, a empresa também adota princípios. No âmbito da Empresa, também adota princípios éticos que inspiram e justificam condutas alinhadas com valores morais e a busca pela validade universal das ações. Esses princípios são essenciais para promover uma cultura de integridade, transparência e ética dentro da organização.

A segurança da informação deve ser tratada como um aspecto crítico para a missão da organização, uma vez que as informações suportam as atividades e os objetivos estratégicos desta Empresa Pública de Saúde.

Assim, as ações de Segurança da Informação devem observar os seguintes princípios:

Confidencialidade: garantir que as informações sejam acessíveis apenas por pessoas autorizadas e que tenham necessidade de conhecê-las.

Integridade e Ética: Compromisso com a mais alta integridade e ética, garantindo que todas as ações e decisões sejam pautadas pela honestidade, transparência e retidão.

Disponibilidade: garantir que as informações estejam disponíveis sempre que necessário para as pessoas autorizadas.

Autenticidade: garantir que as informações sejam provenientes de fontes confiáveis e que sejam verdadeiras.

Publicidade: garantir a divulgação de todas as medidas de gestão de riscos de Segurança da Informação, observando os critérios legais de sigilo aplicáveis;

Privacidade: assegurar que as informações pessoais e confidenciais sejam protegidas de uso ou acesso não autorizado.

Proporcionalidade: ser proporcionais ao valor da informação e ao nível de risco ao qual estiverem expostas;

Completude: cobrir todo o ciclo de vida da informação levando em conta todos os ativos que a suportam, sejam eles físicos, tecnológicos ou humanos;

Conformidade: cumprimento todas as leis, regulamentos e normas aplicáveis ao presente tema da política, inclusive as mencionadas na introdução.

DIRETRIZES

A segurança da informação deve ser tratada como uma atividade contínua e integrada aos processos de trabalho.

Deve ser garantida a conformidade com as leis, normas e regulamentos aplicáveis à segurança da informação.

Adicionalmente aos conceitos e as definições referidas, para efeitos desta Política, considera-se:

1. Tratamento das Informações

1.2. As informações são ativos de propriedade do Município, devendo ser tomadas todas as medidas necessárias para protegê-las de alteração, destruição e divulgação não autorizadas.

1.3. As informações devem ser identificadas e classificadas quanto à confidencialidade, integridade, autenticidade e disponibilidade de forma a serem adequadamente acessadas, manipuladas, armazenadas, transportadas e descartadas.

1.4. Os controles de segurança da informação devem ser proporcionais à sua classificação e ao nível de risco ao qual esteja exposto.

1.5. Funcionários públicos, prestadores de serviço e estagiários devem garantir o sigilo das informações a que tiverem acesso em função de suas competências funcionais, tomando o cuidado necessário quanto a sua divulgação interna e externa, de acordo com sua classificação.

a. Classificação da Informação

O gestor de cada área é responsável por estabelecer os critérios relativos ao nível de confidencialidade da informação gerada por sua área e classificá-las em quatro categorias: Pública, Confidencial, Restrita ou Interna. Os Dados de Pacientes, por sua vez, sempre serão categorizados como confidenciais e restritos, recebendo tratamento especial de proteção à confidencialidade.

O processo de classificação da informação começa com a definição do grau de proteção necessário, com base nos quatro níveis de sigilo a seguir definidos:

CONFIDENCIAL: Refere-se a informações sensíveis que devem ser mantidas em estrito sigilo e manuseadas exclusivamente por pessoas autorizadas. A divulgação inadequada de informações com essa classificação pode acarretar impactos significativos para a empresa e seus negócios como um todo.

RESTRITA: Refere-se a informações cujo acesso e manuseio são restritos a indivíduos autorizados. Qualquer divulgação indevida dessas informações pode afetar a continuidade de um ou mais processos de negócios da empresa, gerando impacto em uma ou mais áreas.

INTERNA: Envolve informações de baixa sensibilidade, mas que devem ser circuladas apenas internamente, não estando disponíveis ao público em geral.

PÚBLICA: Refere-se a informações que podem ser de conhecimento público e não possuem restrições significativas quanto à sua divulgação.

2. Gestão de Recursos de TIC

2.1. Os recursos de TIC de propriedade da RioSaúde são de gestão da Diretoria de Governança e Tecnologia da Informação - DGOVI e são fornecidos para uso corporativo, sendo proibido seu uso para fins pessoais.

2.2. Todos os recursos de TIC devem ser identificados de forma individual, controlados, preservados, protegidos contra acessos indevidos, submetidos à manutenção preventiva periódica e estar com a documentação atualizada e aprovada pelos setores competentes.

2.3. A disponibilização de recursos de TIC somente deve ser permitida após o atendimento às determinações desta Política e de suas normas complementares, a homologação pela área local de Gestão de TIC e a autorização dos setores responsáveis.

2.4. A utilização de recursos de TIC a termo de empréstimo, para realização de atividades de trabalho dentro ou fora da sede da empresa, deve ser precedida de assinatura de Termo de Responsabilidade específico pelo colaborador solicitante do empréstimo, bem como pelo gestor responsável pelos recursos de TIC da Diretoria de Governança e Tecnologia da Informação - DGOVI.

2.5. Em caso de algum equipamento apresentar eventual problema técnico, deverá ser aberto chamado junto à equipe de suporte Service Desk, entre 8h e 17h.

2.6. A movimentação dos recursos de TIC deve ser precedida de registro e devida autorização.

2.7. Em casos de descarte de algum recurso, devem ser seguidos procedimentos adequados à classificação das informações residentes no recurso, para que não haja risco de vazamento ou perda de informações

2.8. Qualquer intervenção do colaborador para realizar manutenção física ou lógica, instalação, desinstalação, configuração ou modificação de software, programas

ou instruções de computador, bem como a transferência ou divulgação a terceiros (pirataria), é expressamente proibida.

2.9. Todos os computadores em desuso devem ser encaminhados ao setor de TI para a devida remoção de informações, descarte ou possível reutilização.

3. Uso de logins e senhas

3.1. Ao solicitar acesso à rede da empresa, o colaborador deve requisitar a criação de suas credenciais (login e senha) à equipe de Infraestrutura de T.I. Essa solicitação deve ser realizada por meio do envio de um e-mail para [inserir endereço de e-mail], incluindo seu nome completo, matrícula ou CPF, com o responsável direto em cópia.

3.2. Após a criação, as credenciais (login e senha) são enviadas ao usuário por e-mail, contendo uma senha padrão. É imprescindível que o usuário realize a troca dessa senha no primeiro acesso. A nova senha deve conter no mínimo 10 dígitos, sendo obrigatória a inclusão de pelo menos uma letra minúscula, uma letra maiúscula, um número e um caractere especial.

3.3. Para um controle efetivo sobre as senhas, os usuários deverão ter o pleno conhecimento das diretivas e políticas de senha da empresa, todos da mesma forma devem ser orientados e estimulados a segui-las:

- Manter a confidencialidade;
- Não compartilhar;
- Evitar anotações das senhas em papel, cadernos ou blocos de papel adesivado (*post it*);
- Selecionar senha de boa qualidade, seguindo o padrão imposto, evitando o uso de senhas muito curtas ou muito longas que obriguem a escrevê las para não esquecer (recomenda-se entre 10 (dez) a 12 (doze) caracteres);
- Alterar a senha sempre que existir qualquer indicação do sistema;
- Alterar a senha em intervalos regulares ou com base no número de acessos (senhas para usuários privilegiados devem ser alteradas com maior frequência que senhas normais);
- Não reutilizar as senhas, nem gerar sequências para as alteradas: Exemplo: (*#E58%oBz13)* para (*#E58%oBz14*);
- Não incluir senhas em processos automáticos de acesso ao sistema (por exemplo, armazenadas em macros);

Deve-se considerar que utilizar a mesma senha para diversos sistemas não se torna uma boa prática, pois a vulnerabilidade poderá ser explorada em um possível vazamento de senha.

a. Que tipo de senha deve ser evitada?

Evitar senhas compostas de elementos facilmente identificáveis.

- Nome do usuário;
- Identificador do login, mesmo que de forma embaralhada;
- Nome de membros da família ou pessoas próximas;
- Nome de pessoas e lugares em geral;
- Nome do sistema operacional, da máquina ou terminal de acesso que está utilizando;
- Nomes próximos;
- Datas, números de telefone, cartões ou identidade e outros documentos pessoais;
- Letras e números repetidos;
- Letras e números repetidos ou seguidas do teclado (ASDFG, YUIOP);

b. Como escolher uma boa senha?

Em geral, são consideradas, boas senhas, aquelas que utilizam composições com letras (maiúsculas e minúsculas) com números e símbolos de forma embaralhada. Porém elas devem possuir um critério de complexidade para dificultar deduções e, ao mesmo tempo, de fácil memorização ao proprietário da conta, sem a necessidade da anotação em qualquer local.

Torna-se também eficaz a escolha de senhas que possam ser digitadas rapidamente, dificultando que outras pessoas, a dada distância, identifiquem a sequência de caracteres.

Outra forma de geração de senha é por associação a frases que signifiquem algo para o usuário, o uso dos primeiros caracteres de cada palavra somado aos caracteres especiais podem compor uma combinação favorável para uma senha de fácil assimilação.

Por regra, na política de segurança de senha dos sistemas operacionais de rede (SOR), como exemplo: configurações de política de segurança/Windows. A troca obrigatória por um período igual ou menor aos 30 dias, recomenda-se aos demais sistemas a mesma medida.

c. Medidas de segurança

• Garantir ao usuário o fornecimento de uma senha de caráter temporário para inicialização do acesso ao ambiente corporativo, onde esta deverá ser alterada na primeira autenticação.

• As senhas temporárias, em casos de esquecimento por parte dos proprietários da conta, deverão ser reinicializadas somente após a identificação positiva do respectivo usuário, este encaminhamento terá que seguir um protocolo, evitando o uso de terceiros ou troca de mensagens em sistemas com baixa segurança (Não criptografados).

Os mecanismos de controle de senhas, devem ser configurados para trazer uma proteção ao banco de armazenamento das credenciais de acesso, contra acessos não autorizados, a exemplo disso, os campos usuário e senha não devem ser apresentados em tela e todas as contas terão data de expiração entre 30 ou 60 dias após renovação da senha.

Será necessário também um *log* de armazenamento das últimas senhas utilizadas pelos usuários.

Em relação ao controle de contas, as credenciais de ex-colaboradores devem ser bloqueadas, para isso, será necessária a comunicação prévia ao administrador da rede e dos sistemas, na ocorrência de demissões ou desligamentos de funcionários das suas funções pertinentes.

Também devem ser bloqueadas contas de usuários após um determinado número de tentativas de acesso sem sucesso. Esse procedimento diminui os riscos de acesso indevido. Atingido esse limite, só o administrador do sistema poderá desbloquear a conta do usuário.

d. Acesso restrito e controlado dos recursos informacionais

Ao se autenticar em um ambiente, os usuários terão acesso às aplicações e conteúdos conforme o seu perfil e competência, sempre atendendo ao parâmetro do menor privilégio, sem impossibilitar o desempenho de suas funções.

Os controles de acesso, sejam estes por menu ou perfil de rede, deverão ser providos pelas aplicações adquiridas e/ou desenvolvidas na instituição. Em casos de aplicações corporativas onde o controle de acesso ou de perfil esteja a cargo do detentor da licença, a exemplo disso, aplicações desenvolvidas para os órgãos das esferas: municipais, Estaduais e Federais, deve-se optar ao menos pela auditoria das contas onde serão observadas as suas modificações e as datas de vigência.

O Monitoramento dos sistemas informacionais, será por registros de *log*, trilhas

de auditoria ou qualquer outro mecanismo com a capacidade de identificação de violações de acesso.

Com a eventual falha do sistema, acesso não autorizado torna-se obrigatória a apuração e a reunião das evidências para serem tomadas as medidas corretivas necessárias ao restabelecimento do serviço e as suas condições normais, juntamente com os procedimentos administrativos e/ou judiciais como parte de apurações e investigações para aplicação de sanções pertinentes.

Os registros de *log* a princípio deverão contemplar:

- Identificação do(s) usuário(s);
- Datas e horas de entrada (logon) e saída do sistema (logoff);
- Identificação da estação de trabalho quando possível assim como sua localização;
- Registro de tentativas de acesso ao sistema ou outro(s) recurso(s) (permitidas ou negadas);

Deve-se entender que o armazenamento de tais princípios sem o devido acompanhamento pode tornar inviável o acompanhamento, dada a gama de informações que serão registradas. Para tanto, recomenda-se criar uma rotina envolvendo trilhas de auditorias por softwares de inspeção do tipo open source (código aberto).

Outros recursos podem ser utilizados para um monitoramento mais efetivo, como exemplo disso, os controles de acesso lógicos que seguem algumas práticas:

- Encerramento das sessões ativas, a menos que elas possam ser protegidas por mecanismos de bloqueio (telas com senha de logon);
- Em sessões em terminais conectados a computadores de grande porte e/ou servidores, efetuar a desconexão da sessão finalizada;
- Desabilitar o acesso remoto de determinadas contas fora dos dias e horários úteis;
- Limitar a quantidade de sessões concorrentes, impossibilitando ao usuário ou login o acesso via mais de um terminal, ou computador simultaneamente.

Resumem-se as regras de acesso nesta política, as recomendações a seguir, cabendo o gestor a viabilização e o cumprimento das mesmas:

- A adoção de um identificador de usuário (ID) único, de forma que Cada usuário possa ser identificado e responsabilizado por suas ações;

- A validação e verificação se o usuário obteve autorização do proprietário do sistema de Informação ou serviço para sua utilização;

- A inspeção se o nível de acesso concedido ao usuário está adequado aos propósitos da Missão e Valores e consistente com a política de segurança da RioSaúde;

- Fornecimento, aos usuários, de documento escrito com seus direitos de acesso. Os usuários deverão assinar esse documento, indicando que entenderam as condições dos direitos de acesso;

- A Manutenção de um registro formal de todas as pessoas cadastradas para usar cada sistema de informações;

- A remoção imediata dos direitos de acesso de usuários que mudarem de função ou saírem da instituição;

- A verificação periódica da lista de usuários, com intuito de remover usuários inexistentes e (IDs) em duplicidade;

- A inclusão de cláusulas nos contratos de funcionários e prestadores de serviço, que especifiquem as sanções a que estarão sujeitos em caso de tentativa de acesso não autorizado.

- O estudo de viabilidade de novos métodos de acesso por credenciais que envolvam a segurança e proteção de dados: autenticação por dois fatores que condiciona uma camada extra de segurança, exigindo o fornecimento de informações adicionais além da senha de acesso, o uso de assinaturas digitais, trazendo um caráter individualizado para determinados documentos de cunho restrito, a serem adotados pelo gestor de infraestrutura.

e. Revogação de acesso

A revogação do acesso de usuários desligados da RioSaúde deve ser efetuada de forma imediata no momento em que o desligamento for comunicado.

As credenciais de acesso dos usuários que concluíram suas atividades na empresa não devem ser removidas das bases de dados, mas sim bloqueadas para impedir sua utilização. Deve haver um sistema de registro mantido para possibilitar a identificação dos usuários responsáveis por ações realizadas por meio das credenciais de acesso, mesmo após o bloqueio ter sido aplicado.

3.4. Tela Limpa e Mesa Limpa

3.4.1. A configuração do papel de parede e da proteção de tela de todos os computadores deve estar em conformidade com a padronização estabelecida pela RioSaúde.

3.4.2. É responsabilidade do colaborador garantir que papéis de parede, mídias e imagens exibidas nos monitores não fiquem acessíveis a pessoas não autorizadas.

3.4.3. Os computadores devem ser bloqueados com senha sempre que não estiverem sendo utilizados. É recomendável utilizar o atalho no teclado: Windows Key+L.

3.4.4. É responsabilidade do colaborador garantir que sua mesa de trabalho mantenha-se organizada, sem acúmulos de papéis desnecessários e que documentos que possam conter informações importantes não fiquem expostos e acessíveis a outras pessoas. O ideal é que documentos/papéis importantes sejam guardados em arquivos ou pastas designadas.

3.5. Antivírus

3.5.1. A RioSaúde, por intermédio da IPLANRIO, disponibiliza software corporativo de antivírus instalado para todos os usuários.

3.5.2. O antivírus é atualizado automaticamente na estação de trabalho do usuário sempre que uma nova versão é disponibilizada pelo fabricante através do aplicativo servidor.

3.5.3. A área de TI da empresa não recomenda que o usuário remova ou altere as configurações do antivírus a fim de não comprometer a segurança que o fabricante do software proporciona.

3.6. Descarte de Mídias

Mídias contendo informações referentes à RioSaúde deverão seguir o padrão de avaliação abaixo descrito, antes de serem descartadas.

3.6.1. Descarte de Bancos de Dados

O descarte de um banco de dados deve ser realizado com cautela e seguindo diretrizes específicas para garantir a segurança das informações e o cumprimento das regulamentações. Abaixo estão algumas diretrizes gerais que devem ser consideradas ao realizar o descarte de um banco de dados de uma empresa:

a. Análise da necessidade do descarte:

Antes de iniciar o processo de descarte, deve ser realizada uma avaliação completa para determinar se o banco de dados precisa ser descartado. Isso inclui considerar se os dados ainda são relevantes, necessários e se não há obrigações legais ou

regulamentares para mantê-los.

b. Política de retenção de dados, legislações pertinentes e tabela de temporalidade:

A área responsável pelo descarte, antes de fazê-lo, deve providenciar consulta a regulamentações aplicáveis, Política de retenção de dados, se esta existir e a Tabela de temporalidade da empresa, onde devem estar claramente definidos os prazos para manutenção de informações e os critérios para descarte.

c. Classificação de dados:

É recomendável classificar os dados no banco de dados em termos de sensibilidade e importância. Dados sensíveis devem ser tratados com maior cuidado e rigor no processo de descarte.

d. Processo de descarte seguro

Se legalmente possível, o descarte deve ser feito de maneira segura e completa, incluindo a eliminação de cópias de backup, arquivos de *log* e qualquer outra instância dos dados. Isso pode incluir a destruição física de discos rígidos ou a utilização de software especializado para garantir que os dados sejam irrecuperáveis.

e. Conformidade legal e regulatória

O processo de descarte deve estar em conformidade com todas as leis e regulamentações aplicáveis, incluindo regulamentos de privacidade de dados e regras de retenção de registros.

f. Documentação e registro

Deve ser mantido um registro detalhado do processo de descarte, incluindo datas, métodos utilizados e responsáveis envolvidos. Isso pode ser necessário para comprovar o cumprimento das regulamentações.

g. Aprovação adequada

Garantir que o processo de descarte seja aprovado por autoridades competentes dentro da empresa, como o departamento de TI, a equipe de segurança da informação e a equipe jurídica.

h. Avaliação pós-descarte

Após o descarte, é recomendável realização de uma avaliação para garantir que todos os dados foram realmente eliminados e que não houve vazamento de informações.

3.7. Utilização da Internet

3.7.1. O uso indevido do acesso à Internet é de inteira responsabilidade do colaborador, podendo o mesmo ser responsabilizado legalmente pelos danos causados.

3.7.2. Downloads de arquivos, programas ou anexos de e-mails de fontes não confiáveis e não relacionadas ao trabalho devem ser evitados.

3.7.3. Havendo permissão para utilização de redes sociais, as mesmas devem ser utilizadas com responsabilidade durante o horário de trabalho, evitando-se o compartilhamento de informações sensíveis da empresa.

3.7.4. Qualquer incidente de segurança, como suspeita de malware ou phishing, deve ser imediatamente comunicado à equipe de TI da empresa.

3.8. E-mails e Mensagens Instantâneas

3.8.1. É proibido utilizar e-mails, correios eletrônicos ou mensagens instantâneas de maneira que viole a lei, a moral, os bons costumes ou a ordem pública, bem como que infrinja os direitos de propriedade intelectual ou industrial de terceiros.

3.8.2. O e-mail corporativo deve ser utilizado apenas para fins relacionados ao trabalho e de acordo com as políticas da empresa. O uso inadequado do respectivo e-mail ou para fins pessoais é de total responsabilidade do colaborador, que pode ser responsabilizado pelos danos causados.

3.8.3. A atenção deve ser redobrada com e-mails de phishing e mensagens suspeitas. Links ou anexos de remetentes desconhecidos não devem ser abertos.

3.8.4. Dispositivos móveis que acessam e-mails corporativos devem ser protegidos com senha e, se possível, recursos de bloqueio remoto em caso de perda ou roubo.

3.8.5. Qualquer tipo de comunicação em massa, propaganda, informativos, imagens, etc., deve ser previamente aprovado pelo Diretor da área para evitar ser considerado spam ou afetar o funcionamento do trabalho.

3.9. Backup

3.9.1. A política de Backup da empresa contempla a realização de 5 (cinco) backups incrementais semanais diários (seg., qua., qui. e sex) e 01 backup full mensal de todo ambiente com retenção de 60 (sessenta) dias.

3.9.2. Havendo qualquer necessidade de solicitação de informações recuperadas,

será necessário envio de e-mail para a equipe de Infraestrutura de TI pelo solicitante formalizando a solicitação, com o respectivo responsável direto da área em cópia.

3.10. Salvaguarda de Arquivos

3.10.1. Compete à equipe de Infraestrutura de TI criar e manter cópias de segurança (backups) apenas dos dados armazenados nos servidores de rede.

3.10.2. Os colaboradores devem manter obrigatoriamente os documentos, planilhas, e-mails, apresentações e outros dados/documentos que considerarem importantes para as atividades de trabalho nas pastas departamentais dos servidores de rede.

3.10.3. É de responsabilidade exclusiva de cada colaborador manter documentos de trabalho nas pastas departamentais dos servidores de rede, pois apenas os documentos que estiverem armazenados neste local serão contemplados pelo backup, não havendo responsabilização da equipe de Infraestrutura de TI por perda de material que esteja armazenado em outro local.

3.11. Softwares Piratas

3.11.1. Nos softwares homologados e instalados nos computadores e servidores de rede são proibidas as cópias integrais, ou mesmo as parciais, bem como a instalação de softwares piratas.

3.11.2. Pirataria é considerada crime e softwares piratas geram prejuízos tanto materiais como funcionais além de ocasionar problemas a imagem da Instituição. Por esta razão, estão terminantemente proibidos.

3.11.3. A instalação de softwares não autorizados (“Pirataria”) constitui crime contra apropriedade intelectual, de acordo com o art. 12 da Lei 9.609 Lei 9.609 de 19/02/98, e o infrator está sujeito à pena de detenção e multa.

PROTEÇÃO DE DADOS PESSOAIS

Em atenção à Lei Geral de Proteção de Dados Pessoais – LGPD (Lei 13.709/2018), a RioSaúde deverá garantir a disponibilidade, integridade, autenticidade e confidencialidade dos dados pessoais, em todo seu ciclo de vida. Sendo assim, deverá apresentar, em seu Programa de Governança em Privacidade e Proteção dos Dados Pessoais (PGPPDP) diretrizes claras para a coleta, processamento, armazenamento e compartilhamento de dados pessoais, garantindo que tais dados sejam tratados

com base na lei vigente e respeito à privacidade e direito dos titulares. Para isso, serão disponibilizados documentos específicos com regras detalhadas para o tratamento de dados pessoais, onde todos os colaboradores e prestadores de serviços, tomarão ciência e serão sensibilizados sobre o tema.

Em atendimento ao Decreto Municipal n.º 49.558/2021, foi instituído em março/2022, o Comitê de Privacidade e Proteção de Dados da RioSaúde, posteriormente alterado pela Portaria "P" RIOSAÚDE/PRE n.º 358/2022, de 09/08/2022, para se adequar à Resolução SEGOVI n.º 91/2022.

O Comitê é uma estrutura multissetorial formada por alguns funcionários da RIOSAÚDE com a atribuição de apoiar o trabalho dos encarregados de dados na implantação do Programa de Governança em Privacidade e Proteção dos Dados Pessoais (PGPPDP) do Município do Rio.

Atribuições do Comitê (art. 4º, Resolução SEGOVI n.º 91/2022):

I. Apoiar o trabalho dos encarregados de dados na implantação do PGPPDP - Programa de Governança em Privacidade e Proteção dos Dados Pessoais;

II. Auxiliar na elaboração dos instrumentos do Programa;

III. Fornecer informações acerca dos tratamentos de dados pessoais realizados no âmbito da RioSaúde;

IV. Tirar dúvidas e prestar esclarecimentos acerca das atividades realizadas pelas suas áreas e demais setores;

V. Reavaliar, em conjunto com os responsáveis pelos sistemas, processos de negócio, serviços e políticas públicas, a efetiva necessidade dos tratamentos de dados pessoais realizados;

VI. Implementar o Programa no âmbito da RioSaúde;

VII. Analisar o nível de criticidade em caso de incidente de segurança com dados pessoais e acionar o profissional da tecnologia da informação, se for o caso;

VIII. Documentar as respostas aos incidentes relacionados a recursos computacionais ou físicos.

IX. Mapear os processos de trabalho em que há tratamento de dados pessoais no âmbito da RioSaúde;

X. Conscientizar e divulgar a LGPD, visando estimular a mudança de cultura necessária, em razão da vigência da norma;

XI. Realizar as demais ações que se mostrem necessárias ao cumprimento da LGPD, sempre em conformidade com o PGPPDP.

RECUPERAÇÃO DE DESASTRES

1. Visando assegurar que a empresa possa lidar eficazmente com eventos adversos que possam comprometer a integridade, disponibilidade e confidencialidade de seus dados e sistemas. Abaixo estão os elementos chave a serem considerados ao integrar a Recuperação de Desastres:

a. Avaliação de Riscos e Impactos:

Identificação e avaliação de riscos relacionados a desastres naturais, falhas de sistemas, ciberataques e outros eventos que podem afetar a infraestrutura de TI. Análise do impacto potencial desses eventos nas operações críticas e nos ativos de informação

b. Backup e Recuperação de Dados:

Deve haver implementação de práticas regulares de backup por parte da equipe de infraestrutura de T.I. para garantir a preservação de dados críticos, bem como o estabelecimento de procedimentos claros para a rápida recuperação de dados em caso de perda.

c. Infraestrutura Redundante:

Implementação de redundâncias na infraestrutura de TI para garantir a continuidade operacional em caso de falhas em um local específico.

2. Em caso de ocorrência de eventos adversos que venham a comprometer a segurança da informação da empresa, a organização poderá contar com o apoio operacional da Empresa Municipal de Informática - IPLANRIO em ações de respostas a incidentes.

CONFORMIDADE

1. O colaborador deve estar ciente e seguir as recomendações da presente Política, interpretando a classificação atribuída às informações e Dados, e assegurando que recebam tratamento adequado.

2. Caso algum colaborador da RioSaúde receba consulta ou pedido oficial oriundo de qualquer entidade ou órgão de controle, deverá, em respeito às diretrizes condicionais na

presente política, bem como na utilização e divulgação das informações, observar quais dados e informações podem ser disponibilizadas, e a forma de disponibilização, respeitando, ainda, a legislação vigente, como a LGPD, a Lei de Acesso à Informação e qualquer outra legislação aplicável. A divulgação de informações deve ser autorizada pela autoridade competente.

3. A utilização inadequada dos recursos de tecnologia e comunicação oferecidos pela empresa configura um incidente de segurança da informação e pode resultar na imposição de penalidades legais e/ou administrativas, de acordo com a gravidade e o impacto do incidente para a empresa.

4. O desrespeito às disposições estabelecidas nesta Política, devidamente investigado, pode resultar em:

- Aplicação das penalidades especificadas na legislação trabalhista;
- Aplicação das penalidades estabelecidas na LGPD;
- Aplicação das penalidades conforme os contratos com prestadores de serviços e estagiários;
- Aplicação dos procedimentos legais cabíveis.

RESPONSABILIDADE E COMPETÊNCIAS

1. A Diretoria de Governança da Tecnologia da Informação – DGOVI é a instância estratégica responsável por tratar e deliberar sobre o tema.

2. Compete a esta Diretoria:

a. regulamentar, planejar, coordenar e promover a cultura da Segurança da Informação por meio de ações de sensibilização e conscientização.

b. Tomar as medidas administrativas necessárias para que sejam adotadas ações corretivas, em tempo hábil, em caso de comprometimento da Segurança da Informação.

c. Atuar junto a seus colaboradores na construção e implantação de processos de trabalho que promovam a Segurança da Informação.

3. É de responsabilidade dos colaboradores que têm acesso aos ativos da informação da RioSaúde:

a. Manter níveis de segurança da informação adequados, segundo os preceitos desta política e de suas normas complementares;

b. Gerenciar os ativos da informação sob sua responsabilidade e garantir que sejam utilizados exclusivamente para os fins previstos;

c. Tratar a informação de acordo com a sua classificação, adotando as medidas de proteção previstas para o tratamento dos riscos a que estão sujeitos os ativos de informação sob sua custódia;

d. Observar desvios das políticas, normas e procedimentos estabelecidos e informá-los ao responsável imediato;

e. Observar a presente política inclusive quando estiver em devido cumprimento legal ao responder questionamentos e ofícios enviados pelas entidade ou órgão de controle.

4. Deverá ser mantido o alinhamento constante com qualquer Entidade ou Órgãos de Controle para o cumprimento efetivo desta Política de Segurança da Informação.

PENALIDADES

Violações da Política de Segurança da Informação podem submeter o violador e a RioSaúde a penalidades civis e/ou criminais, por isso, a RioSaúde leva esses riscos extremamente a sério e exige que todos os relacionados com a Empresa façam o mesmo.

Seguindo o Código de Conduta e Integridade da RioSaúde, serão consideradas transgressões passíveis de sanção qualquer desvio de conduta em relação aos dispositivos das políticas implementadas na RioSaúde, além dos definidos na legislação vigente.

Cabe ao Núcleo de Integridade, em conjunto com a Área de Governança e Compliance, avaliar casos de transgressões identificados, propondo as sanções a serem adotadas, sem prejuízo da adoção de medidas administrativas e/ou judiciais.

Internamente, o não cumprimento das diretrizes desta Política enseja a aplicação de medidas de responsabilização dos agentes que a descumprirem, conforme a respectiva gravidade do descumprimento, sendo aplicáveis a todas as pessoas descritas no item “Abrangência” desta Política.

Serão levados em consideração na aplicação das sanções

I. a gravidade da infração;

II. a vantagem auferida ou pretendida pelo infrator;

III. a consumação ou não da infração;

IV. o grau de lesão ou perigo de lesão;

V. o efeito negativo produzido pela infração;

VI. a situação econômica do infrator;

VII. a cooperação da pessoa jurídica para a apuração das infrações;

VIII. a existência de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica;

IX. o valor dos contratos mantidos pela pessoa jurídica com o órgão ou entidade pública lesados.

Os agentes públicos que comprovadamente descumprirem ou não observarem as disposições das políticas, regimentos, códigos, decretos, portarias e demais instrumentos normativos da RioSaúde, estarão sujeitos às medidas disciplinares, previstas em lei, assegurados os direitos constitucionais do devido processo legal, da ampla defesa e do contraditório, observando os itens anteriores e eventual reincidência na violação da Política:

- Advertência verbal;
- Advertência escrita;
- Suspensão;
- Exoneração;
- Rompimento do vínculo existente entre a empresa e o infrator;
- Demissão por justa causa, a depender do modelo de contratação do agente público;
- Rompimento do Contrato, a depender do caso, ou inclusão do terceiro em lista de impedimento de licitação, de acordo com o Manual de Procedimentos para Aplicação de Sanções e ao Código de Conduta e Integridade.

A omissão em manifestar-se internamente em questões que envolvam possíveis práticas de corrupção na Empresa será analisada à luz do fato e evidenciada a infração funcional, estará sujeita às sanções disciplinares previstas em lei, podendo se constituir em falta grave.

IMPLEMENTAÇÃO, ACOMPANHAMENTO E REVISÃO

A Política de Segurança da Informação da Riosaúde é essencial para proteger ativos de informação e promover uma cultura de segurança em toda a organização. Para garantir a eficácia e a conformidade com os objetivos desta política, serão implementados procedimentos de implementação, acompanhamento e revisão contínua.

Implementação: A Riosaúde irá implementar programas de treinamento e conscientização para todos os agentes públicos, colaboradores, empregados, terceirizados, diretores, gerentes, coordenadores, estagiários, membros de Comitês e membros dos Conselhos Fiscal e Administração. Esses programas visam educar os funcionários sobre as práticas seguras de segurança da informação e garantir que compreendam suas responsabilidades.

A organização irá estabelecer procedimentos para classificar informações com base em seu nível de sensibilidade, o que ajudará a determinar o nível apropriado de proteção. Isso envolve identificar quais informações são confidenciais, quais podem ser compartilhadas e quais têm requisitos especiais de segurança.

Serão estabelecidos procedimentos rigorosos para conceder e gerenciar autorizações de acesso a recursos de tecnologia da informação. A identificação e autenticação adequadas dos usuários serão fundamentais para garantir a confidencialidade e a integridade dos dados.

Acompanhamento: A Riosaúde estabelecerá sistemas de monitoramento contínuo da segurança da informação para identificar e responder a possíveis ameaças ou vulnerabilidades. Isso envolverá a supervisão da rede, dos sistemas e do tráfego de informações.

A Empresa criará procedimentos para relatar e responder a incidentes de segurança, incluindo malware, phishing, violações de dados e outros eventos de segurança. Um plano de resposta a incidentes documentados garantirá que as ações apropriadas sejam tomadas em caso de problemas de segurança.

Revisão: A empresa realizará avaliações regulares de riscos de Segurança da Informação para identificar novas ameaças e vulnerabilidades. Essas avaliações ajudarão a ajustar as medidas de segurança conforme necessário.

A Empresa se compromete a garantir a melhoria contínua das práticas de Segurança da Informação. Isso envolverá a revisão periódica da política e de seus procedimentos à medida que as melhores práticas evoluem e a legislação pertinente é atualizada.

DISPOSIÇÕES FINAIS

Esta Política deve ser observada em conjunto com outras políticas, normas e procedimentos adotados pela RioSaúde.

O descumprimento dos dispositivos desta Política implicará na apuração de responsabilidade e aplicação de sanções administrativas nos termos dos normativos internos da RioSaúde.

Com o objetivo de assegurar a transparência e o tratamento adequado das informações geradas no âmbito da empresa, esta Política será revisada quando necessário e apreciada pela Alta Administração, área responsável por sua aprovação e alteração.

Qualquer revisão ou atualização será comunicada internamente aos colaboradores e divulgada publicamente, conforme necessário.

As dúvidas acerca das disposições da presente Política deverão ser dirimidas pela área de Segurança de Dados da empresa.

REFERÊNCIAS

Lei Federal nº 13.303, de 30 de junho de 2016 – Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, Estados, do Distrito Federal e dos Municípios - Lei das Estatais;

Decreto Municipal nº 44.698, de 29 de junho de 2018 - Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito do Município do Rio de Janeiro, nos termos da Lei Federal nº 13.303, de 30 de junho de 2016 e dá outras providências.

Decreto Federal nº 8.945, de 27 de dezembro de 2016 - Regulamenta, no âmbito da União, a Lei nº 13.303, de 30 de junho de 2016, que dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios

Lei n.º 8.159, de 8 de janeiro de 1991 - Dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências e a Lei Municipal n.º 3.404, de 5 de junho de 2002, cujo dispositivo dispõe sobre a política municipal de arquivos Públicos privados, o acesso aos documentos Públicos municipais e dá outras providências.

Lei n.º 9.983, de 14 de julho de 2000: Dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

Lei n.º 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação (LAI): Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei n.º 8.112, de 11 de dezembro de 1990; revoga a Lei n.º 11.111, de 5 de maio de 2005, e dispositivos da Lei n.º 8.159, de 8 de janeiro de 1991; e dá outras providências e Decreto RIO n.º 44.745/2018 que regula a legislação no âmbito do Município.

Decreto RIO nº 44.745 de 19 de julho de 2018, regulamenta a Lei de Acesso à Informação (LAI) em âmbito municipal;

Lei n.º 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD): dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público, ou privado, visando proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

Decreto n.º 44.276, de 1 de março de 2018: Estabelece a Política de Segurança da Informação da Prefeitura da Cidade do Rio de janeiro;

Decreto n.º 53700 de 8 de dezembro de 2023: Institui a Política de Segurança da Informação - PSI no âmbito do Poder Executivo Municipal, e dá outras providências.

Norma ABNT NBR ISO/IEC 27001:2023 Estabelece os elementos de um Sistema de Gestão de Segurança da Informação e Comunicações;

Norma ABNT NBR ISO/IEC 27002:2023 Institui o código de melhores práticas para Gestão de Segurança da Informação e da Comunicação;

Norma ABNT NBR ISO/IEC 27005:2023: Estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação;

ANEXO I

TERMO DE CIÊNCIA

Termo de Ciência

Declaro, que recebi e li a presente Política de Segurança da Informação da empresa RioSaúde.

Declaro também que compreendi as diretrizes, obrigações e responsabilidades contidas na referida Política de Segurança da Informação e que estou ciente da importância do tema para a proteção dos ativos de informação da empresa, bem como para a preservação da confidencialidade, integridade e disponibilidade das informações.

Comprometo-me a cumprir todas as disposições estabelecidas na presente Política e a adotar as práticas recomendadas para proteger os dados e informações da empresa.

Estou ciente de que o não cumprimento das diretrizes de segurança da informação pode resultar em medidas disciplinares, conforme as políticas e procedimentos da empresa.

Data: __/__/_____

Assinatura: _____

Rio
PREFEITURA

RIOSAÚDE