Protocolo: 927405
Data: 06/10/2023
Título: PORTARIA - Política de Controle de Acessos - RIOLUZ Nº 278 DE 04 DE SETEMBRO DE 2023
Página(s): a

ATOS DO DIRETOR PRESIDENTE

PORTARIA "N" RIOLUZ Nº 278 DE 04 DE SETEMBRO DE 2023.

INSTITUI A POLÍTICA DE CONTROLE DE ACESSOS NO ÂMBITO DA COMPANHIA MUNICIPAL DE ENERGIA E ILUMINAÇÃO - RIOLUZ.

A **COMPANHIA MUNICIPAL DE ENERGIA E ILUMINAÇÃO**- **RIOLUZ**, no exercício de suas atribuições legais e regimentais,

Considerando o Decreto n.º 9.637 de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, em especial o inciso II do Art.15;

Considerando o Decreto n.º 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

Considerando o Decreto RIO nº 44.276 de 1 de março de 2018, que estabelece a Política de Segurança da Informação da Prefeitura da Cidade do Rio de Janeiro - PCRJ;

Considerando as normas técnicas ABNTNBRISO/IEC 27001:2013 e 27001:2022 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos, ABNTNBRISO/IEC 27002:2013 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação e ABNTNBRISO/IEC 27003:2020 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Orientações;

Considerando o Decreto RIO nº 30.648/2009, que redefine o funcionamento do sistema municipal de informática e a política de informática no âmbito do poder executivo municipal e o Decreto Rio nº 26.487/2006;

Considerando a Lei 13.709 de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

Considerando a Resolução CD/ANPD Nº 4/2023, publicada no DOU em 27/02/2023, que aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas;

Considerando a RESOLUÇÃO SEGOVI 91 DE 2022; que regulamenta o Programa de Governança em Privacidade e Proteção dos Dados Pessoais - PGPPDP no âmbito da Administração Pública Municipal, em conformidade com o art. 50, § 2º da Lei Geral de Proteção de Dados Pessoais - LGPD.

RESOLVE:

CAPÍTULO - I
DA INSTITUIÇÃO, APLICAÇÃO E CONTROLES DE ACESSOS

Art. 1º Fica instituída a Política de Controle de Acesso aos ativos e aos sistemas de informação, para possibilitar o controle de acesso à rede, aos sistemas e às informações produzidas pela Companhia Municipal de Energia e Iluminação - RIOLUZ.

Art. 2º Esta Política de Controle de Acesso aplica-se aos funcionários, terceirizados, estagiários, aprendizes, colaboradores, e parceiros e/ou empresas contratadas pela RIOLUZ.

Art. 3º A elaboração e atualização deste documento são de responsabilidade do Comitê de Privacidade e Proteção de Dados - LGPD da RIOLUZ.

Art. 4º O acesso a informações rotuladas como públicas e de uso interno não é restringido com controles de acesso que discriminam o usuário.

Art. 5º O acesso às informações confidenciais e restritas serão permitidas apenas quando uma necessidade de trabalho tiver sido identificada e tal acesso aprovado pela Assessoria de Informática da RIOLUZ responsável.

Art. 6º O acesso a alguns equipamentos de hardware e/ou software especiais (tais como equipamentos de diagnóstico de rede) é restrito aos profissionais da Assessoria de Informática, com uso registrado, baseado nas necessidades da RIOLUZ.

Art. 7º Será dado mediante necessidade dos usuários da RIOLUZ, o acesso aos serviços básicos como correio eletrônico (*e-mails* e *browser WEB*), mediante autorização do superior hierárquico.

CAPÍTULO - II
DOS TERMOS E DEFINIÇÕES

Art. 8º Os seguintes termos são utilizados nesta Política de Controle de Acesso aos ativos e aos sistemas de informação da RIOLUZ com os significados específicos que se seguem:

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

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

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

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

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

VI. Disponibilidade: propriedade de estar acessível e utilizável sob demanda por um usuário autorizado.

VII. Estações de trabalho: computador pessoal utilizado para trabalho nos Departamentos do CRCMS.

VIII. Gestor de Sistema: empregado oficialmente designado como gestor de determinado sistema de informação.

IX. Integridade: propriedade de salvaguarda da exatidão e completeza da informação contra alterações, intencional ou acidental, em seu estado e atividades.

X. Ponto de acesso sem fio: equipamento que compõe uma rede sem fio (wireless), concentrando as conexões de um ou mais equipamentos.

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

XII. Programa: coleção de instruções que descrevem uma tarefa a ser realizada por um computador.

XIII. Recursos de armazenamento de dados corporativos: armazenamento de massa projetado para ambientes de grande escala e alta tecnologia.

XIV. 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.

XV. Rede local da RIOLUZ: conjunto de recursos compartilhados por meio dos servidores de rede, *switches* e computadores clientes, por onde circulam as informações corporativas da RIOLUZ.

XVI. Rede sem fio (*wireless*): sistema que interliga equipamentos utilizando o ar como via de transmissão por meio de ondas eletromagnéticas.

XVII. 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.

XVIII. Sistemas de mensageria: sistemas que permitem o envio e a recepção de mensagens de correio eletrônico ou de mensagens instantâneas entre usuários, dentro e fora da instituição.

XIX. TI: Tecnologia da Informação.

XX. TIC: Tecnologia da Informação e Comunicação são um conjunto de recursos tecnológicos utilizados de forma integrada com um objetivo comum.

XXI. Setor da RIOLUZ: Setor em que está lotado o funcionário, terceirizado, estagiário ou aprendiz.

XXII. Usuário: pessoa física ou jurídica que opera algum sistema informatizado da RIOLUZ.

XXIII. *Web*: Rede Mundial de Computadores.

XXIV. 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*.

CAPÍTULO - III
DO CADASTRAMENTO DE USUÁRIOS

Art. 9º A criação de novas contas de acesso à rede se dará da seguinte forma:

I. Para funcionários: após a abertura de chamado pela Gerência de Recursos Humanos da RIOLUZ informando o nome completo, a lotação e a matrícula do empregado;

II. Para estagiários e menores aprendizes: após a abertura de chamado pela Gerência de Recursos Humanos da RIOLUZ informando a lotação, matrícula do estagiário e a vigência do contrato; e

III. Para prestadores de serviço: após a abertura de chamado pelo gestor do contrato, informando o nome completo, Setor de lotação, nome da empresa contratada e matrícula na empresa contratada (ou outro documento legalmente válido).

Parágrafo único. Nas eventuais substituições, caberá ao responsável informar o período para a configuração adequada da conta de acesso do empregado, assessor ou prestador de serviço.

Art. 10 As contas dos estagiários, menores aprendizes e prestadores de serviço serão configuradas para expiração automática, concomitantemente à vigência do contrato.

Art. 11 Caberá ao titular do setor solicitar à Assessoria de Informática a liberação ou restrição de privilégios de acesso aos documentos de seu departamento.

Art. 12 Para evitar a expiração automática da conta de estagiários, menores aprendizes ou de prestadores de serviços, deverá ser aberto chamado pelo superior hierárquico imediato do estagiário ou do menor aprendiz, ou pelo gestor do contrato do prestador de serviços, com antecedência mínima de 72 (setenta e duas) horas à expiração da conta.

Art. 13 Todos os usuários que utilizam aplicações e sistemas da RIOLUZ, funcionário, estagiário ou menor aprendiz, devem assinar o Termo de Responsabilidade sobre o conhecimento da Política de Controle de Acesso da RIOLUZ, conforme o Anexo l.

Art. 14 A assinatura do documento de que trata o artigo anterior indica que o usuário em questão entende e concorda com as políticas, padrões, normas e procedimentos da RIOLUZ relacionados ao ambiente de TI, incluindo as instruções contidas nesta portaria, bem como as implicações legais de correntes do não cumprimento do disposto no termo.

Art. 15 A Gerência de Recursos Humanos ficará responsável por recolher a assinatura desses no Termo de Responsabilidade sobre o conhecimento da Política de Controle de Acesso da RIOLUZ, conforme o Anexo I, que ficará arquivada na respectiva gerência.

Art. 16 É de responsabilidade da Gerência de Recursos Humanos solicitar o cancelamento da conta de acesso quando do desligamento ou afastamento do prestador de serviço.

Art. 17 A Gerência de Recursos Humanos deverá informar à Assessoria de Informática, o desligamento e a movimentação permanente de lotação de funcionários, terceirizados, estagiários e de menores aprendizes para as providências de bloqueio e posterior eliminação da conta, se for o caso.

Parágrafo Único - As movimentações temporárias de funcionários, terceirizados, estagiários e de menores aprendizes entre os setores deverão ser formalizadas ao setor de Informática, devendo especificar o tempo que irá durar tal movimentação, bem como eventual alteração de privilégio de acesso ao Sistema, caso seja necessário.

Art. 18 Não haverá identificação genérica e de uso compartilhado para acesso aos recursos de rede, excetuando-se os casos de necessidade, justificada e acompanhada de parecer do TI, acerca da possibilidade de aceitação dos riscos associados.

Art. 19 As novas contas de acesso à rede serão compostas por nome e sobrenome, sendo a forma padrão o nome e o último sobrenome, separados por underline.

Art. 20 Após a criação da conta solicitada, o TI deverá informar ao solicitante a criação da conta e a senha de acesso inicial, juntamente com as instruções para a sua alteração.

Art. 21 Em nenhuma hipótese será admitido o empréstimo ou o compartilhamento de credenciais de acesso.

Parágrafo único. No descumprimento dos casos tratados neste item, os atos praticados serão de responsabilidade de todos os envolvidos, estando sujeitos às sanções administrativas e penais cabíveis, tanto o titular das credenciais quanto aquele que as utilizar indevidamente.

CAPÍTULO - IV
DA POLÍTICA DE SENHAS

Art. 22 A identificação de usuários que operam a rede local da RIOLUZ deve ser feita mediante a autenticação usuário-senha.

Art. 23 A senha cadastrada é pessoal, intransferível e confidencial.

Art. 24 A senha deverá observar as seguintes regras de formação:

l. Não pode conter o nome da conta do usuário ou partes do nome completo do usuário que excedam dois caracteres consecutivos;

II. Deve conter, no mínimo, 08 (oito) caracteres; e

III. Deve conter caracteres de três das quatro categorias seguintes:

a) Caracteres alfabéticos maiúsculos;

b) Caracteres alfabéticos minúsculos;

c) Caracteres numéricos; e

d) Caracteres especiais, não alfabéticos (por exemplo: *,$,#,%).

Art. 25 A senha cadastrada terá prazo de validade de 45 (quarenta e cinco) dias, ao fim do qual o usuário deverá cadastrar nova senha.

Parágrafo único. A nova senha não poderá ser igual às últimas 02 (duas) senhas anteriormente utilizadas no período de 12 (doze) meses.

Art. 26 Após 05 (cinco) tentativas erradas, o usuário ficará bloqueado, necessitando recadastrar nova senha.

Art. 27 Em caso de suspeita de exposição indevida do ambiente de TI, todas as senhas de acesso devem ser imediatamente alteradas.

Art. 28 Em caso de comprometimento comprovado de segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas.

Art. 29 Em caso de esquecimento da senha o usuário entrará em contato com a Assessoria de Informática pelo portal: http://preainrioluz.rio.rj.gov.br/glpi/ ou pelo telefone do setor para abertura do chamado de *reset* de senha.

Art. 30 Independentemente das circunstâncias, as senhas de acesso não devem ser compartilhadas ou reveladas para outras pessoas que não o usuário autorizado, ficando o proprietário da senha responsável legal por qualquer prática indevida cometida.

CAPÍTULO - V
DOS ACESSOS

Seção I
DO ACESSO À REDE

Art. 31 Apenas poderão ser conectadas à rede cabeada da RIOLUZ microcomputadores e *notebooks* previamente autorizados pela Assessoria de Informática.

§ **1º** Exceções devem ser comunicadas à Assessoria de Informática, justificando a necessidade e o prazo de utilização.

§ **2º** As exceções autorizadas deverão, obrigatoriamente, adotar os padrões definidos pela Política de Segurança da Informação regulamentada pela Deliberação nº 001 de 28 de março de 2018 da Prefeitura e pela IPLANRIO, sendo o proprietário do equipamento responsável pelo licenciamento dos produtos nele instalados, uma vez que a RIOLUZ não fornecerá licenças para o funcionamento de microcomputadores particulares e *notebooks*.

Art. 32 Microcomputadores e dispositivos portáteis poderão acessar a rede sem fio específica para esse fim.

Parágrafo único. O usuário, antes de acessar a rede visitante, deverá se identificar e concordar com o termo de uso da rede sem fio.

Art. 33 O TI poderá desconectar das redes cabeadas e sem fio qualquer dispositivo que constitua ameaça à segurança da informação.

Art. 34 Dispositivos com acesso à rede deverão ser desligados ou bloqueados na ausência do usuário.

Seção II
DO ACESSO À INTERNET

Art. 35 Os acessos aos portais da internet da RIOLUZ serão efetuados, preferencialmente, por meio da rede local e deverão ser identificados por usuário.

§ **1º** Os rastros de acesso deverão, no mínimo, identificar usuários, endereço IP, URL acessada, data e hora.

Art. 36 É proibido o acesso a sítios que tratem de pornografia, pedofilia, erotismo e correlatos; de racismo; de ferramentas para invasão e evasão de sistemas; de compartilhamento de arquivos; e de apologia e incitação a crimes.

Parágrafo único. O TI poderá utilizar *software* específico que realizará o bloqueio automático desses sítios.

Art. 37 Os acessos a *sites* e serviços disponíveis na internet serão controlados por filtros de conteúdo e reguladores de tráfego implementados nos dispositivos de segurança da rede da RIOLUZ, cuja operacionalização é de responsabilidade do TI.

Art. 38 Os Setores da RIOLUZ devem definir, com base nas categorias de conteúdo fornecidas pelo TI, os perfis de filtro de conteúdo a serem aplicados a cada uma de suas unidades.

§ **1º** As solicitações de criação ou alteração nas permissões de acesso deverão ser formalizadas e aprovadas pela Assessoria de Informática, juntadas em processo próprio.

§ **2º** Os Chefes dos setores da RIOLUZ devem fiscalizar o bom uso dos acessos à internet e solicitar ajustes e restrições, em caso de má utilização.

Art. 39 O TI poderá, eventualmente e quando necessário, fazer ajustes temporários no controle de banda para viabilizar eventos específicos como vídeo conferências e acesso a visitantes.

Art.40 Todas as operações de acesso realizadas serão registradas para fins de auditoria.

Art. 41 Não será admitido burlar ou tentar burlar os filtros de conteúdo ou restrições de acesso à internet, sob pena de responsabilização dos envolvidos, que estarão sujeitos às sanções administrativas e penais cabíveis.

Seção III
DO ACESSO REMOTO A SISTEMAS DE INFORMAÇÃO

Art. 42 O acesso remoto à rede corporativa da RIOLUZ deve ser realizado somente para atender aos interesses de trabalho.

Art. 43 Compete ao TI definir os perfis de acesso, aplicando técnicas de autenticação e de segurança.

I. O acesso remoto, no âmbito da rede corporativa, deve ser provido por meio de canal criptografado, preferencialmente utilizando as recomendações da ICP-Brasil;

II. O acesso remoto à rede corporativa terá privilégios diferenciados do acesso local, de acordo com o perfil de acesso, com serviços explicitamente controlados;

III. A permissão para se realizar acesso remoto à rede corporativa deve ser solicitada à área de administração da rede pela Coordenação ou área superior a que o usuário da rede está subordinado, com definição do prazo de validade e horários para se realizar o acesso; e

IV. O acesso remoto à rede corporativa será gravado, para posterior auditoria, em *logs* contendo data e hora, serviço utilizado, usuário e informações específicas que facilitem o rastreamento da ação tomada.

Art. 44 Quaisquer computadores que tenham comunicação remota em tempo real com os sistemas da RIOLUZ devem se submeter ao mecanismo de controle de acesso, levando-se em consideração os privilégios necessários ao acesso a cada tipo de informação.

Art. 45 Os usuários da rede devem reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação ao Encarregado de Dados e ao Comitê de Privacidade e Dados Pessoais da RIOLUZ

Art. 46 Em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação, a Assessoria de Informática da RIOLUZ deverá, imediatamente, dar ciência ao Encarregado de Dados, e tomar as providências necessárias a sanar as causas, podendo até mesmo determinar a restrição temporária do acesso às informações e/ou ao uso dos recursos de tecnologia da informação da RIOLUZ.

Art. 47 Os casos omissos serão resolvidos pelo Comitê de Privacidade e Dados Pessoais da RIOLUZ.

CAPÍTULO - VI
DA UTILIZAÇÃO DO CORREIO ELETRÔNICO CORPORATIVO

Art. 48 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 RIOLUZ nem o tráfego de dados na rede de computadores da instituição. As regras e normas da utilização são de competência do IPLANRIO - Empresa Municipal de Informática.

CAPÍTULO- VII
DA UTILIZAÇÃO DO SISTEMA DE ARQUIVOS

Art. 49 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.

Art. 50 O TI realizará o backup dos arquivos armazenados no servidor de arquivos, conforme discriminado na Política de Backup.

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

Art.51 O TI poderá limitar o tipo de extensão dos arquivos a serem armazenados nas pastas dos departamentos da RIOLUZ.

Art. 52 O TI não acessará os arquivos armazenados nas pastas dos departamentos 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 Presidência da RIOLUZ;

II. Recuperar conteúdo de interesse da RIOLUZ, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização da Presidência da RIOLUZ;

III. Atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização da Presidência da RIOLUZ;

IV. Atender à solicitação judicial; e

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

Art. 53 Os casos omissos serão dirimidos pelo Comitê de Privacidade e Dados Pessoais da RIOLUZ.

CAPÍTULO - VIII
CONTROLE DE ACESSO FÍSICO

Art. 54 Dispõe sobre a importância da prevenção contra o acesso físico não autorizado em setores da RIOLUZ que realizam tratamento de dados pessoais visando garantir a segurança e privacidade dos dados.

§ 1º Fica instituído procedimentos para garantir a política de mesa limpa e tela limpa:

I. Fica estabelecida a política de mesa limpa para documentos e mídia de armazenagens removíveis;

II. Fica instituída a política de tela limpa para os recursos de processamento da informação que contenham dados pessoais, de forma a reduzir riscos de acesso não autorizado, perda e danos à informação classificada em qualquer grau de sigilo, durante e fora do horário normal de trabalho.

§**2º** As seguintes regras devem ser observadas no que diz respeito à adoção da mesa limpa e tela limpa:

I. Não expor em cima de mesas documentos e mídias contendo informações classificadas em qualquer grau de sigilo, que possam ser danificadas, furtadas, ou destruídas em caso de catástrofes, como incêndios, inundações ou explosões.

II. Armazenar documentos e mídia de computador em armários e estantes apropriadas e trancadas ou em outras formas de mobília de segurança, quando não estiverem em uso, principalmente fora do horário de expediente.

III. Proteger computadores pessoais e terminais de computador, bem como as impressoras por bloqueios de teclas, senhas ou outros controles, quando não estiverem em uso.

IV. Proteger copiadoras contra o uso não autorizado fora do horário normal de expediente.

V. Retirar informações sensíveis ou confidenciais, quando impressas, das impressoras imediatamente após a impressão.

Art. 55 Coleta de informações pessoais no setor de Recepção da RIOLUZ:

§1º A Coleta de dados pessoais na recepção será realizada conforme disposições previstas na LGPD.

§**2º** Os responsáveis pela coleta, controle e armazenamento dos dados pessoais coletados na recepção da empresa, deverão:

a) Registrar as informações no sistema informatizado de recepção. Caso não seja possível a utilização do sistema, de forma temporária, o registro poderá ser realizado manualmente em formulário específico. Os dados pessoais coletados, o tratamento e a finalidade constam do Termo de Uso da Recepção da RIOLUZ.

b) O acesso ao sistema será definido por perfil de acesso específico para esta finalidade.
c) Os formulários deverão ser armazenados em compartimentos fechados com chave sob a guarda do Setor de Infraestrutura e Logística da RIOLUZ.

d) O tempo de armazenamento e descarte será de dois anos.

e) O descarte será feito por meio de delével ou fragmentadora.

§ **3º** Os Avisos e Políticas de Privacidade deverão estar disponíveis por meio físico no mural da recepção e por código QR, para acesso dos titulares dos dados.

Art. 56 Segurança das informações e dados pessoais contidos nos processo físicos:

§ **1º** Os setores da RIOLUZ que armazenam dados pessoais deverão:

I. Manter fechada com chave as portas das salas que contenham arquivos com os processos que contenham dados pessoais, com ambiente controlado e acesso restrito às pessoas autorizadas.

II. Todos os setores que mantenham as portas fechadas devem disponibilizar as chaves reservas no claviculário da companhia.

III. O Setor de Recepção deverá manter o controle de movimentação das chaves reservas.

Aprovada na 14ª Reunião do Comitê de Proteção Privacidade e Proteção de Dados Pessoais da RIOLUZ, realizada em 24 de agosto de 2023.

Art. 57 Esta portaria entra em vigor na data de sua publicação.

ANEXO - I

Termo de Responsabilidade

Pelo presente termo, eu, _____, declaro ter conhecimento da Política de Controle de Acesso da Companhia Municipal de Energia e Iluminação - RIOLUZ, disponível para consulta na Internet (link.).

Declaro que estou recebendo uma conta com privilégios adequados ao exercício das atividades que executo, a qual será utilizada somente para tal fim.

Comprometo manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas.

Comprometo não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador (browser), bloquear estação de trabalho, bem como encerrar a seção do cliente de correio, garantindo assim a impossibilidade de acesso indevido por terceiros.

Declaro estar ciente que minhas ações serão monitoradas nos termos da Política de Controle de Acesso da RIOLUZ, e que qualquer alteração será de minha responsabilidade, feita a partir de minha identificação, autenticação e autorização.

Estou ciente, ainda, que serei responsável pelo dano que possa causar em descumprimento da Política de Controle de Acesso da RIOLUZ, ao realizar uma ação de iniciativa própria de tentativa quanto à modificação da configuração, física ou lógica, dos recursos computacionais sem a permissão da área competente.

Rio de Janeiro, _____ de _____ de 202____.

Nome:
Matrícula:
Setor:

Nome:
Setor:

(titular da unidade, para o caso dos terceirizados)