MANUAL DE REFERÊNCIA

TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

PREFEITURA RIO | Administração Previ-Rio

PREVI-RIO

AUTARQUIA GESTORA DO FUNPREVI

PRESIDENTE

BERNARDO EGAS LIMA FONSECA

COORDENADORA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

FERNANDA NUNES LEIROZ

EQUIPE DA COORDENAÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (PRE/CTIC)

ALEXANDRE FERREIRA TAVARES

CESAR AUGUSTO PEREIRA PEIXOTO

DENISE MARIANO CORRÊA

FABIO LUIZ LOPES FERREIRA

GILSON VAGUINER DOS SANTOS JUNIOR

JACKELINE FERNANDA DE OLIVEIRA

MARCELO MOTA DAS VIRGENS

PAULO ROBERTO RODRIGUES MARIM JUNIOR

PAULO ROBERTO XAVIER DE CARVALHO

Índice

1. INTRODUÇÃO E OBJETIVOS

A informação é um dos bens mais valiosos de uma instituição. Proteger esses dados é uma responsabilidade de todos.

Este manual tem como objetivo orientar os usuários sobre como adotar boas práticas de segurança da informação, ajudando a prevenir falhas, danos e prejuízos. Também busca reforçar a conscientização e o compromisso de cada pessoa com o uso seguro e responsável das informações.

A segurança da informação não depende apenas de sistemas e equipamentos, mas também de atitudes corretas no dia a dia. Cada servidor, ao seguir as orientações aqui descritas, contribui para um ambiente de trabalho mais seguro, confiável e eficiente.

Com este material, o PREVI-RIO reafirma seu compromisso com a transparência, a integridade e a proteção dos dados institucionais e pessoais sob sua responsabilidade.

2. APLICAÇÃO E ABRANGÊNCIA

Este manual é dirigido às seguintes pessoas:

• Agente Público (independentemente de sua função, cargo ou vínculo empregatício).

• Prestador de Serviço.

• Estagiário.

• Qualquer pessoa física ou jurídica autorizada a tratar informações do PREVI-RIO, FUNPREVI e FASS em quaisquer meios (físicos ou digitais).

3. TERMOS E DEFINIÇÕES

• **Acesso**: capacidade de utilizar um ativo da informação.

• **Ameaça**: evento com potencial para comprometer os objetivos da organização.

• **Aplicação**: sistema de informação ou serviço digital desenvolvido especificamente para dar suporte aos processos de negócio e aos serviços de uma organização.

• **Autenticação**: processo de reconhecimento formal da identidade dos elementos que se comunicam ou participam de uma transação eletrônica.

• **Autorização**: concessão, ao usuário devidamente autenticado, de um conjunto de permissões de acesso a um ativo da informação.

• **Conscientização em Segurança da Informação**: processo educacional que visa capacitar cada indivíduo a incorporar, em sua rotina pessoal e profissional, as melhores práticas de Segurança da Informação.

• **Controle de acesso (login)**: conjunto de mecanismos destinados a proteger as informações armazenadas em ativos da informação contra acessos não autorizados.

• **Data Center**: instalação física projetada para abrigar grande quantidade de equipamentos de computação, armazenamento de dados e sistemas de rede.

• **Disponibilidade**: propriedade que garante que a informação esteja acessível a pessoas e processos autorizados sempre que necessária.

• **Disponibilidade**: propriedade que garante que a informação esteja acessível a pessoas e processos autorizados sempre que necessária.

• **Equipamento ou Equipamento de TIC**: componente integrante da infraestrutura de Tecnologia da Informação e Comunicação (TIC).

• **Firewall:** componente de segurança de rede que monitora e controla o tráfego de dados entre redes — geralmente entre uma rede interna e a internet — com o objetivo de proteger sistemas e dados contra ameaças externas.

• **Intranet**: rede interna de uso corporativo que utiliza a mesma tecnologia da internet para permitir que os servidores acessem informações e sistemas internos.

• **Malware**: abreviação de "malicious software" (software malicioso). Refere-se a qualquer tipo de programa desenvolvido para causar danos a computadores, servidores, redes ou dispositivos móveis, comprometendo sua segurança, integridade ou disponibilidade.

• **Plano de Gerenciamento de Incidentes**: documento que define, de forma clara, as ações a serem executadas quando ocorrer um incidente de segurança.

• **Risco**: probabilidade de uma ameaça explorar vulnerabilidades, comprometendo a confidencialidade, a integridade ou a disponibilidade da informação, com impactos nas atividades da Administração Pública Municipal.

• **Sistema de Informação**: conjunto de ativos da informação voltado ao armazenamento, transporte e processamento de dados, com o objetivo de dar suporte a funções, serviços ou processos da Administração Pública Municipal.

• **Software**: sistema operacional ou aplicativo de terceiros utilizado para apoiar as atividades de uma organização.

• **Tratamento da Informação**: conjunto de ações relacionadas à produção, recepção, classificação, uso, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento,

4. REDE CORPORATIVA

A rede corporativa é uma infraestrutura privada de comunicação de dados criada para interligar computadores, servidores, dispositivos e sistemas da Prefeitura da Cidade do Rio de Janeiro (PCRJ), inclusive o PREVI-RIO.

Essa rede viabiliza a comunicação interna, o compartilhamento de recursos — como arquivos, impressoras e sistemas — e o acesso a aplicativos e serviços voltados às necessidades operacionais da Autarquia.

Para garantir a confidencialidade, integridade e disponibilidade das informações, a rede é protegida por medidas robustas de segurança, como firewalls, sistemas de detecção de intrusão e políticas de controle de acesso.

A administração dos recursos de Tecnologia da Informação e Comunicação (TIC) do Município do Rio de Janeiro, incluindo os do PREVI-RIO, é de responsabilidade da Empresa Municipal de Informática – IPLANRIO.

5. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

A Política de Segurança da Informação é o conjunto de regras e orientações que ajudam a proteger os dados e sistemas de uma instituição. Garante que as informações sejam usadas de forma correta, segura e responsável por todos os usuários.

Seguir essa política é fundamental para o bom funcionamento da estrutura organizacional.

Por isso, é importante adotar todas as precauções e cumprir as normas definidas, evitando qualquer tipo de manipulação indevida, dano ou divulgação não autorizada de informações.

Qualquer ação que viole esta Política ou suas normas complementares pode resultar em sanções administrativas, conforme a legislação vigente.

5.1. PRINCÍPIOS E PROPRIEDADES

A segurança da informação fundamenta-se nos seguintes princípios (artigo 5.º do Decreto Rio n.º 53.700, de 8 de dezembro de 2023):

I. Publicidade: garantir a ampla divulgação das medidas de gestão de riscos em Segurança da Informação, observados os critérios legais de sigilo aplicáveis.

II. Proporcionalidade: assegurar que as medidas adotadas sejam compatíveis com o valor da informação e com o nível de risco ao qual estiver exposta.

III. Completude: abranger todo o ciclo de vida da informação, considerando todos os ativo.

III. Privacidade: assegurar o direito individual e coletivo à inviolabilidade da intimidade e ao sigilo dos dados pessoais, nos termos da legislação vigente.

IV. Privacidade: assegurar o direito individual e coleti - vo à inviolabilidade da intimidade e ao sigilo dos dados pessoais, nos termos da legislação vigente.

São também 4 (quatro) suas **propriedades** (art. 6.º):

I. Confidencialidade: garantir que a informação só esteja disponível a indivíduos ou processos autorizados;

II. Integridade: garantir que a informação esteja intacta e protegida contra perda, dano ou modificação não autorizada;

III. Disponibilidade: assegurar que a informação só esteja disponível às pessoas e aos processos autorizados a qualquer momento em que sejam requeridas; e

IV. Autenticidade: garantir 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.

6. DIRETRIZES DA PSI

6.1. TRATAMENTO DA INFORMAÇÃO

I. As informações são ativos vitais da organização e devem ser protegidas contra alteração, destruição, perda ou divulgação não autorizada.

II. As informações devem ser classificadas conforme os requisitos de confidencialidade, integridade e disponibilidade. Essa classificação define o grau de sensibilidade da informação diante de uma possível quebra de segurança.

I**II.** Cada informação deve ser tratada de acordo com sua classificação, adotando-se as medidas de proteção correspondentes para mitigar os riscos identificados.

I**V.** Qualquer tratamento de informação que extrapole as atribuições funcionais do usuário exige autorização formal prévia do gestor da informação.

6.2. CONTROLE DE ACESSO

I. Identificação Pessoal e Intransferível: o acesso deve ocorrer através de um mecanismo de identificação de uso pessoal e intransferível.

II. Responsabilidade Pessoal: o usuário será qualificado como responsável por quaisquer ações realizadas por meio de sua identificação.

III. Princípio do Mínimo Privilégio: a autorização de acesso deve se restringir aos privilégios mínimos necessários para que o usuário desenvolva suas competências funcionais.

IV. Prazo Limitado: A duração do acesso deve ter prazo limitado à execução de sua finalidade.

6.3. USO DA INTERNET PELA REDE INTERNA

I. O acesso à internet por meio da rede interna estará disponível em todas as estações de trabalho, sendo restrito ao uso para fins institucionais.

II. As conexões poderão ser monitoradas e registradas, a qualquer momento e sem aviso prévio, pela equipe de Tecnologia da Informação da IPLANRIO, com o objetivo de identificar uso indevido, tentativas de invasão ou presença de malwares, dispensando autorização superior.

III. O PREVI-RIO não se responsabiliza por perdas ou danos decorrentes de falhas de segurança ocorridas durante acessos de caráter pessoal.

IV. O uso da internet disponibilizada poderá ser tolerado para fins particulares, desde que o tempo e o conteúdo do acesso não prejudiquem o desempenho

das atividades funcionais, nem comprometam o funcionamento da rede ou a segurança dos sistemas do PREVI-RIO.

V. Todas as conexões e conteúdos transmitidos estão sujeitos a monitoramento, mesmo quando se referirem a acessos de uso particular ou conteúdo de natureza privada.

VI. O monitoramento e o registro das conexões poderão ocorrer também em acessos previamente.

6.4. USO DO E-MAIL CORPORATIVO

I. Uso Institucional Exclusivo: O e-mail corporativo deve ser utilizado exclusivamente para fins institucionais. Uma mensagem de cunho institucional contém informações que suportam a atuação dos agentes públicos na execução de suas competências.

II. Auditoria: As mensagens nas bases de dados do serviço de e-mail corporativo estão sujeitas à auditoria a qualquer tempo.

II. Compartilhamento Seguro: Em todas as trocas de mensagens, o usuário deve observar os critérios e medidas de segurança em conformidade com a classificação das informações compartilhadas.

6.5. CUIDADOS COM ATIVOS E EQUIPAMENTOS

I. Foco Institucional: O usuário deve utilizar os ativos da informação sob sua custódia exclusivamente para os fins previstos.

II. Descarte: Em casos de alienação ou descarte de equipamentos, procedimentos adequados à classificação das informações devem ser seguidos, para que não haja risco de vazamento ou perda de informações sensíveis.

II. Local de Trabalho: Se o usuário trabalha com ativos da informação considerados críticos, estes podem estar armazenados em áreas com acesso restrito;

III. Anomalias: Qualquer anomalia ou falta de equipamentos deve ser comunicada imediatamente ao setor de TI para as devidas providências;

IV. Softwares e Equipamentos: A instalação de softwares ou equipamentos na rede corporativa requer autorização prévia da área responsável;

V. Downloads e Armazenamento: É proibido fazer download ou armazenar, em computador local ou na rede, qualquer material protegido por direitos autorais sem um contrato de licença, a menos que seja disponibilizado gratuitamente para uso profissional. Arquivos que não estejam em conformidade com as normas desta Política serão removidos da rede sem aviso prévio.

6.6. ANTIVÍRUS

I. Proteção de Rede e de Equipamentos: Cada estação de trabalho possui um software antivírus instalado, e a sua desinstalação ou alteração de configuração é bloqueada pela IPLANRIO.

II. Fontes Externas de Informação: Qualquer arquivo proveniente de fontes externas, como CDs, discos rígidos, pen drives, ou obtidos pela internet, é verificado pelo antivírus antes de ser acessado pelo usuário.

7. INCIDENTES

Um incidente de segurança ocorre quando uma ameaça (evento com potencial de causar dano, como falha de equipamento, furto ou indisponibilidade) explora uma vulnerabilidade (fragilidade em sistemas, processos ou equipamentos), comprometendo a

confidencialidade, integridade ou disponibilidade das informações.

7.1 COMO PROCEDER EM INCIDENTES?

I. Comunicação Imediata: é responsabilidade do usuário comunicar imediatamente ao seu chefe imediato — ou ao preposto responsável, no caso de prestadores de serviço — qualquer desvio das políticas, normas ou procedimentos estabelecidos, bem como qualquer incidente de segurança do qual tenha conhecimento.

II. Apoio Operacional: em caso de descumprimento da Política de Segurança da Informação, a Empresa Municipal de Informática (IPLANRIO) prestará apoio operacional nas ações corretivas necessárias.

A gestão de incidentes será conduzida por meio de um processo formal, que compreende as fases de detecção, triagem, análise e resposta, sob a coordenação do Grupo de Prevenção, Tratamento e Resposta a Incidentes, liderado pela IPLANRIO.

8. RESPONSABILIDADES

8.1. DO PREVI-RIO

I. Promover a aplicação da Política de Segurança da Informação no âmbito da Autarquia.

II. Contribuir para a definição e implementação de estratégias voltadas ao gerenciamento dos riscos de segurança da informação.

III. Divulgar esta Política e suas normas complementares, assegurando sua ampla compreensão pelos servidores e colaboradores; e

IV. Adotar medidas corretivas e disciplinares, com o apoio operacional da IPLANRIO, sempre que ocorrerem violações desta Política ou de suas normas complementares.

8.2. DO USUÁRIO

I. Gerenciar os ativos da informação sob sua responsabilidade, garantindo seu uso exclusivo para os fins institucionais previstos;

II. Executar suas atribuições funcionais em conformidade com todas as políticas, normas e procedimentos de segurança da informação;

III. Manter-se atualizado quanto ao conteúdo desta Política e de suas normas complementares;

IV. Comunicar imediatamente ao superior hierárquico — ou ao representante designado, no caso de prestadores de serviço — qualquer violação das políticas, normas e procedimentos estabelecidos, bem como qualquer incidente de segurança de que tenha conhecimento; e

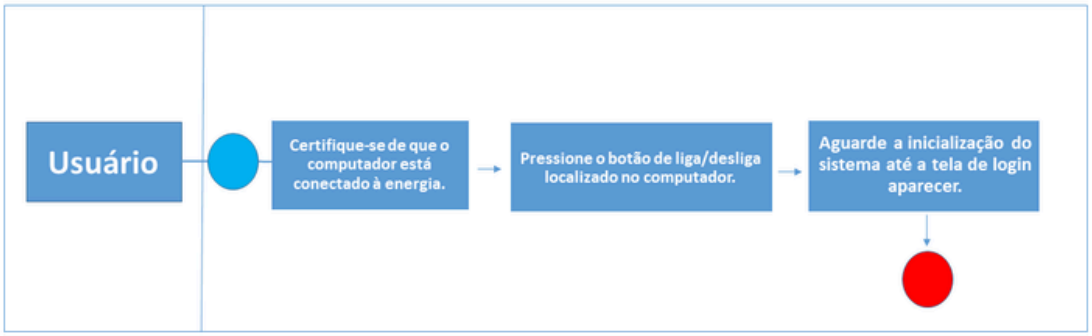
V. Tratar as informações de acordo com sua classificação, observando as medidas de proteção necessárias para mitigar os riscos a que os recursos de informação sob sua responsabilidade estejam expostos.

9. LEGISLAÇÃO APLICÁVEL

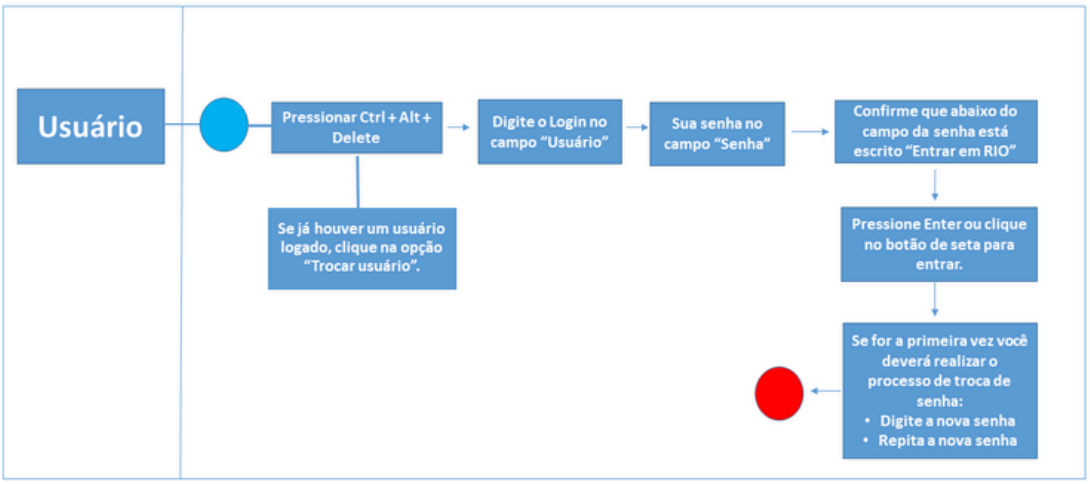
- Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais (LGPD).
- Decreto Rio n.º 53.700, de 8 de dezembro de 2023.
- Resolução CVL n.º 216, de 15 de dezembro de 2023.
- NBR ISO/IEC 17799

10. MAPEAMENTO

10.1. LIGAR O COMPUTADOR

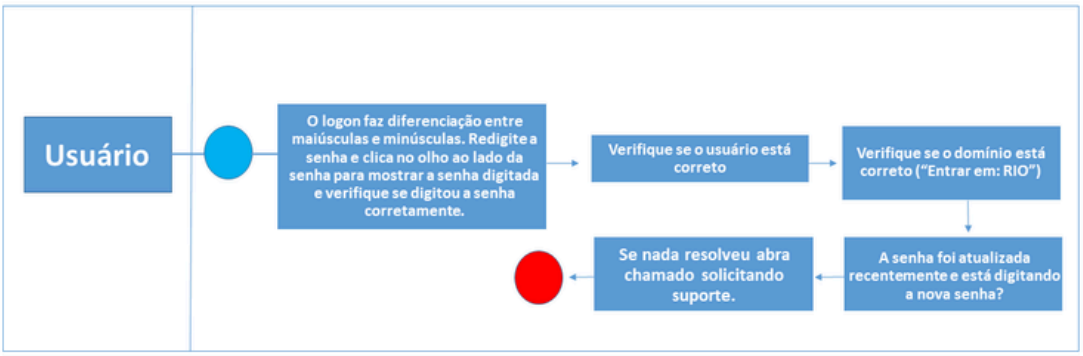


10.2. ACESSAR A TELA DE LOGIN

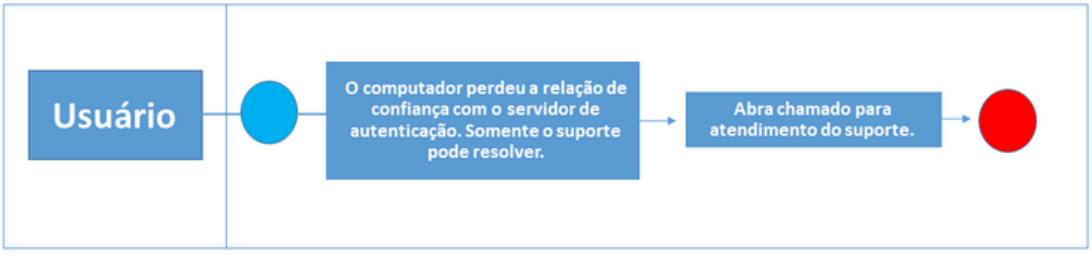


10.3. LOGON: FALHAS

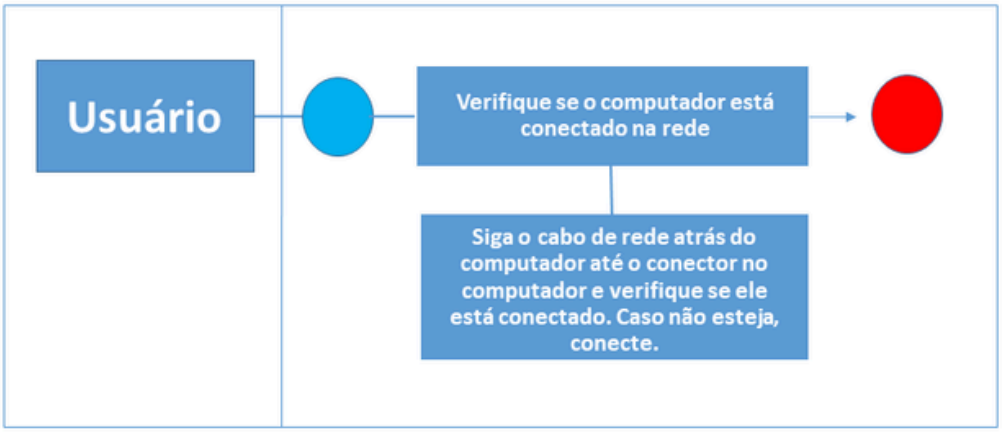
10.3.1. Senha Incorreta

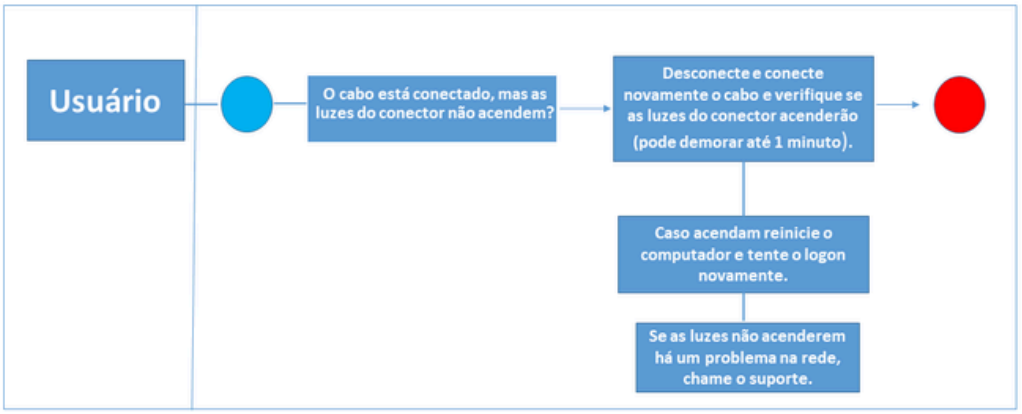


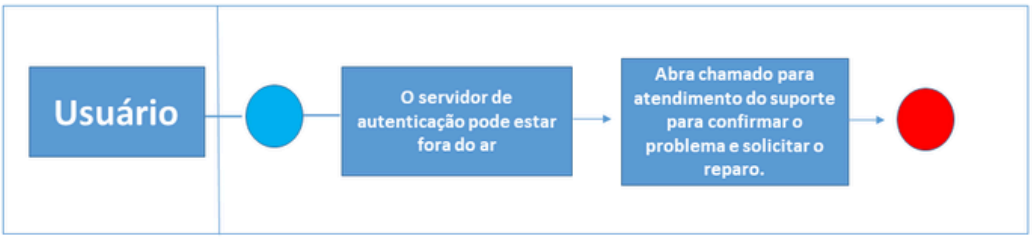
10.3.2. Falha na Relação de Confiança



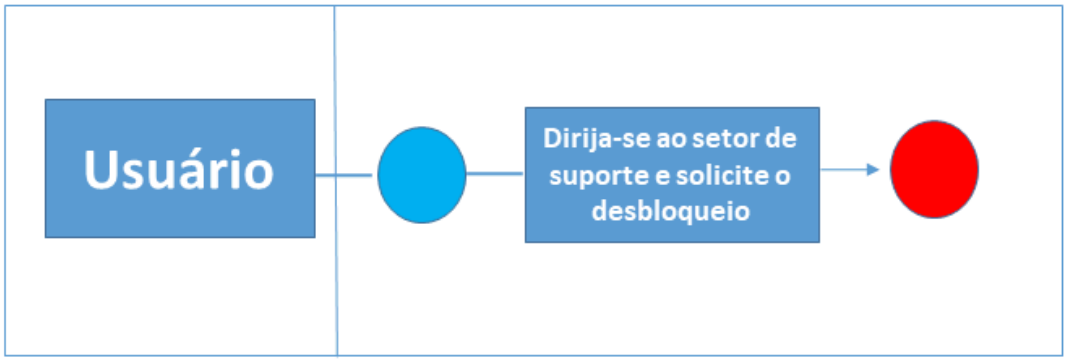
10.3.3. Servidor de Domínio Indisponível





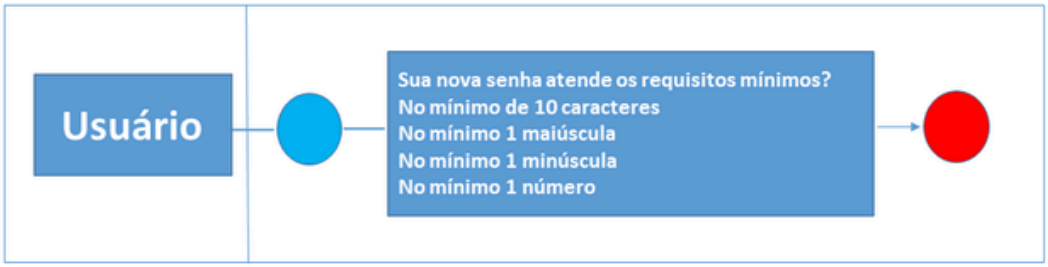


10.3.4. Usuário Bloqueado

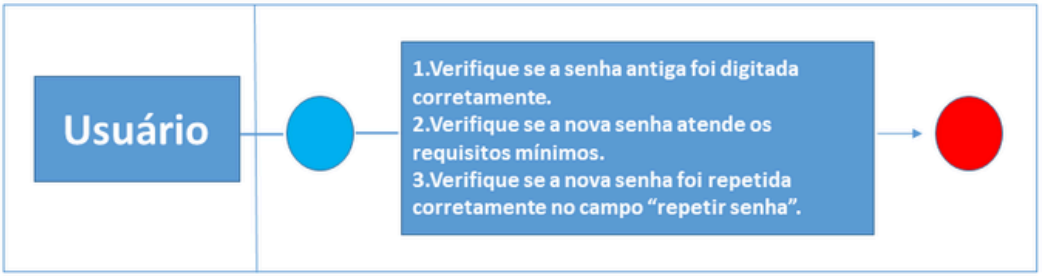


10.4. ALTERAÇÃO DE SENHA

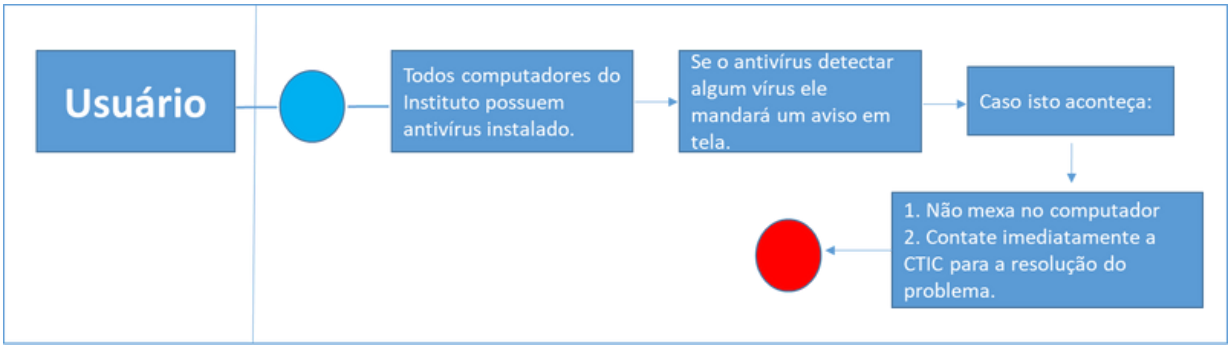
10.4.1. Requisitos Mínimos



10.4.2. Mensagem “Não foi possível alterar a senha.”



10.5. ATAQUE DE VÍRUS: PROCEDIMENTO



ANEXOS

ANEXO 1: COMPETÊNCIAS PSI - DECRETO RIO N.º 53.700/2023

1. Secretaria Municipla da Casa Civil (CVL)

• Consolidar e coordenar as ações de gestão de riscos em Segurança da Informação (SI) no âmbito da Administração Pública Municipal.

• Deliberar, analisar e revisar as normas complementares à Política de Segurança da Informação.

• Definir as metodologias referentes à gestão de riscos em SI.

• Promover a divulgação das políticas, normas e melhores práticas de gestão de riscos no tema de SI para todos os órgãos e entidades municipais.

• Definir as estratégias para a implementação da PSI e de suas normas complementares.

• Receber, analisar e consolidar os resultados relativos às auditorias de nível de conformidade dos órgãos e entidades municipais às políticas e normas de SI.

• Atualizar periodicamente, mediante ato regulamentar, a Política de Segurança da Informação.

• É também responsável por regulamentar a PSI por meio de atos.

2. Empresa Municipal de Informática (IPLANRIO)*

• Instituir e coordenar o Grupo de Prevenção, Tratamento e Resposta a Incidentes.

• Elaborar, implantar e gerenciar o programa de continuidade de negócios dos serviços corporativos.

• Planejar, coordenar, supervisionar e controlar as atividades de Tecnologia da Informação e Comunicação (TIC) visando garantir conformidade com a PSI e suas normas complementares.

• Prever orçamento específico para as ações de SI.

• Oferecer apoio operacional nas ações corretivas em casos de descumprimento da PSI ou de suas normas complementares, nos órgãos e entidades da PCRJ.

* A IPLANRIO presta serviço na administração dos recursos de TIC para o município do Rio de Janeiro, incluindo o PREVI-RIO.

3. Grupo de Prevenção, Tratamento e Resposta a Incidentes

• Executar as atividades de prevenção, tratamento e resposta a incidentes de segurança.

• Elaborar o plano de gerenciamento de incidentes no Datacenter.

• Executar as atividades de recuperação dos sistemas e serviços comprometidos por incidentes de segurança de forma integrada com as respectivas equipes de administração dos ativos.

4. PREVI-RIO

• Implementar a Política de Segurança da Informação.

• Apoiar a elaboração da estratégia de gestão de riscos de SI.

• Implementar o programa de gestão de riscos de SI.

• Disseminar esta Política e suas normas complementares.

• Aplicar as ações corretivas, com apoio operacional da IPLANRIO, e disciplinares nos casos de descumprimento da PSI ou de suas normas complementares.

5. Controladoria Geral do Município do Rio de Janeiro (CGM)

• Auditar periodicamente o cumprimento da PSI e de suas normas complementares, analisando e avaliando a eficácia das suas medidas de implementação.

6. Responsabilidades dos Usuários dos Ativos da Informação

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

• Realizar suas competências funcionais em aderência a todas as políticas, normas e procedimentos de segurança da informação.

• Comunicar prontamente ao seu chefe imediato, ou ao preposto em caso de prestadores de serviço, quaisquer desvios das políticas, normas e procedimentos estabelecidos, ou incidentes de segurança que tenha conhecimento.

• 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.

• Manter-se atualizado quanto à PSI e normas complementares.

7. Responsabilidades dos Custodiantes da Informação

• Zelar pela disponibilidade, integridade e confidencialidade das informações sob sua custódia.

• Utilizar os ativos da informação sob sua custódia exclusivamente para os fins previstos.

• Comunicar prontamente ao seu chefe imediato, ou ao preposto em caso de prestadores de serviço, quaisquer desvios ou incidentes de segurança.

• Preservar a classificação dos ativos da informação aos quais tiver acesso, adotando as medidas de proteção previstas.

ANEXO 2: BOAS PRÁTICAS

1. Recomendações Gerais

I. Utilize senhas fortes (com letras maiúsculas, minúsculas, números e símbolos) e nunca as compartilhe.

II. Troque suas senhas regularmente e evite usar a mesma em vários sistemas.

III. Bloqueie o computador ao se afastar da mesa, mesmo por pouco tempo.

IV. Use o e-mail institucional apenas para atividades de trabalho.

V. Evite abrir links ou anexos de remetentes desconhecidos.

2. Proteção de Dados e Sigilo Funcional

As informações tratadas no ambiente de trabalho podem envolver dados pessoais e institucionais sigilosos.

Cada servidor deve:

- Manter sigilo sobre informações sensíveis obtidas no exercício de suas funções.
- Evitar o compartilhamento indevido de documentos e dados.
- Verificar a necessidade e a autorização antes de enviar informações a terceiros.
- Guardar e descartar documentos físicos com segurança, triturando papéis quando necessário.

O descumprimento dessas orientações pode gerar responsabilidade administrativa e legal.

3. Comportamento no Ambiente de Trabalho

I. Bloqueie o computador sempre que se ausentar.

II. Guarde documentos confidenciais em armários ou gavetas com chave.

III.Não deixe papéis com informações pessoais sobre a mesa.

IV. Evite comentar dados institucionais em locais públicos ou redes sociais.

V. Tenha cuidado com impressões: retire imediatamente os documentos da impressora e evite imprimir desnecessariamente.

4. Uso Responsável de Sistemas e Redes

I. Use apenas acessos autorizados. Nunca utilize credenciais de outro servidor.

II. Não compartilhe senhas nem salve-as em planilhas ou anotações visíveis.

III. Fique atento a e-mails falsos (phishing): desconfie de mensagens com erros de escrita, links estranhos ou pedidos de urgência.

IV. Acesse sistemas apenas por canais oficiais.

V. Evite o uso de redes Wi-Fi públicas para acessar sistemas institucionais.

5. Procedimentos em Caso de Incidentes

Se ocorrer algum problema de segurança, avise imediatamente à Coordenação de Tecnologia da Informação e Comunicação (CTIC).

Exemplos de incidentes:

- Acesso indevido a informações.
- E-mails suspeitos ou com links estranhos.
- Vazamento de dados.
- Travamentos ou comportamentos anormais no sistema.

Não tente resolver sozinho. A comunicação rápida ajuda a evitar maiores prejuízos.

6. Responsabilidades do Usuário

Cada servidor é responsável por:

- Cumprir as normas de segurança da informação.
- Zelar pela confidencialidade e integridade dos dados.
- Utilizar os recursos tecnológicos para fins de trabalho.
- Evitar práticas que possam por em risco os sistemas ou as informações do PREVI-RIO.

O uso inadequado pode gerar responsabilização administrativa e legal.

7. Dicas de Segurança

- ✓ Desconfie de e-mails pedindo senhas ou dados pessoais.
- ✓ Bloqueie seu computador ao se afastar.
- ✓ Não use senhas fáceis (como datas de nascimento).
- ✓ Mantenha antivírus e sistema atualizados.
- ✓ Evite pendrives desconhecidos.
- ✓ Tenha cuidado com o que compartilha em grupos e redes sociais.

8. Contatos e Suporte

Em caso de dúvidas, incidentes ou orientações adicionais, procure a CTIC (11.º Andar, Ala B, Sala 1144).