Política de Segurança da Informação

Rio PREFEITURA

PREVI-RIO

PREVI-RIO

R. Afonso Cavalcanti, 455-
Cidade Nova, Rio de Janeiro - RJ

Acesse

Manual sujeito a alteração
Elaboração em 11/12/2024

ÍNDICE

I. Termos e Definições

Acesso: capacidade de usar um ativo da informação;
Ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização;
Aplicação: sistema de informação ou serviço digital desenvolvido especificamente para suporte aos processos de negócio e serviços de uma organização;
Autenticação: processo de reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte de uma transação eletrônica;
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: concessão ao usuário, após sua autenticação, de um conjunto de permissões de acesso a um ativo da informação;
Conscientização em segurança da informação: processo de iniciação educacional que visa possibilitar, a cada indivíduo, incorporar à rotina pessoal e profissional as melhores práticas de Segurança da Informação;
Confidencialidade: propriedade que garante que a informação só esteja disponível a indivíduos ou processos autorizados;
Controle de acesso/login: conjunto de controles que visam proteger as informações residentes em ativos da informação contra acessos não autorizados;
Disponibilidade: propriedade que garante que a informação só esteja disponível às pessoas e aos processos autorizados a qualquer momento em que sejam requeridas;
Equipamento ou equipamento de TIC: componente da infraestrutura de Tecnologia da Informação e Comunicação (TIC);
Integridade: propriedade que garante que informação está intacta e protegida contra perda, dano ou modificação não autorizada;
Plano de gerenciamento de incidentes: plano de ação claramente definido e documentado para ser usado quando ocorrer um incidente;
Rede corporativa: conjunto de recursos de TIC interligados onde circulam as informações corporativas da PCRJ;

I. Termos e Definições

Risco: probabilidade de ameaças explorarem vulnerabilidades, comprometendo a confidencialidade, integridade ou disponibilidade da informação, causando impactos para as atividades da Administração Pública Municipal;

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 Administração Pública Municipal;

Software: sistema operacional ou aplicativo de terceiros utilizado no suporte às atividades de uma organização

Tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

Usuário: qualquer pessoa autorizada a ler, inserir ou atualizar informações em um sistema de informação.

Malware: é um termo abreviado para "software malicioso". Refere-se a qualquer tipo de software projetado para causar danos a um computador, servidor, rede ou dispositivo móvel, comprometendo sua segurança, integridade ou disponibilidade.

Intranet: Rede interna, de uso corporativo, que utiliza a mesma tecnologia da internet, para que os funcionários possam acessar as informações internas;

Firewall: é um componente de segurança de rede que monitora e controla o tráfego de dados entre redes, tipicamente entre uma rede interna e a internet, com o objetivo de proteger os sistemas e dados contra ameaças externas;

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

II. Legislação Aplicável

Lei Geral de Proteção de Dados Pessoais;
Decreto Rio 53700 de 8 de Dezembro de 2023;
Resolução CVL N° 216 DE 15 DE Dezembro de 2023;
NBR ISSO/IEC 17799.

III. Objetivo

O objetivo desse manual é a realização de procedimentos para proteger as informações visando minimizar falhas, danos e prejuízos, além da conscientização e responsabilidade de cada usuário em segurança da informação.

IV. Diretrizes

A segurança da informação é uma preocupação fundamental para organizações de todos os tamanhos e setores. A execução de uma política de segurança da informação robusta é essencial para proteger os ativos digitais de uma organização e garantir a confiança de seus usuários.

Se baseando em três princípios fundamentais, conhecidos como a tríade CIA: Confidencialidade, Integridade e Disponibilidade. Esses princípios formam a base sobre a qual as estratégias de segurança da informação são desenvolvidas.

1. **Confidencialidade**

A confidencialidade é a garantia de que as informações são acessadas apenas por indivíduos autorizados e devidamente credenciados.

2.Integridade

A integridade refere-se à precisão e à completude das informações, garantindo que os dados não sejam alterados ou corrompidos de forma não autorizada durante seu armazenamento, processamento ou transmissão.

3.Disponibilidade

A disponibilidade diz respeito à acessibilidade das informações quando necessárias.

A IPLANRIO presta serviço na administração dos recursos de tecnologia da informação e comunicação para o município do Rio de Janeiro assim, o PREVI-RIO (Instituto de Previdência e Assistência do Município do Rio de Janeiro) dispõem, desses serviços.

O PREVI-RIO libera esse acesso aos usuários internos e externos através das aplicações desenvolvidas por nós, mediante permissão dos gestores da informação.

V. Responsabilidades

É de responsabilidade Institucional:

- Auxiliar a prática da Política de Segurança da Informação;
- Auxiliar na criação da estratégia para gerenciar os riscos de segurança da informação;
- Divulgar esta Política e suas normas adicionais;
- Tomar medidas corretivas e disciplinares, com apoio operacional da IPLANRIO, quando houver violações da Política de Segurança da Informação ou de suas normas complementares.

Assim, como é de responsabilidade de todos os usuários:

- Gerenciar os recursos de informação atribuídos a eles, garantindo que sejam usados apenas para os propósitos previstos;
- Cumprir suas funções de trabalho em conformidade com todas as políticas, normas e procedimentos de segurança da informação relevantes;
- Informar imediatamente ao seu superior direto, ou ao representante designado no caso de prestadores de serviços, sobre qualquer violação das políticas, normas e procedimentos estabelecidos, ou incidentes de segurança de que tenham conhecimento;

- Tratar a informação de acordo com sua classificação, seguindo as medidas de proteção estabelecidas para mitigar os riscos aos quais os recursos de informação sob sua responsabilidade estão sujeitos;
- Manter-se atualizados sobre esta Política e quaisquer normas complementares.

VI. Rede Corporativa

É uma infraestrutura de comunicação de dados privada utilizada para interligar seus computadores, servidores, dispositivos e sistemas. Essas redes são projetadas para facilitar a comunicação interna, o compartilhamento de recursos, como arquivos e impressoras, e o acesso a aplicativos e serviços específicos para as necessidades da organização.

Nossas redes corporativas são protegidas por medidas de segurança robustas, como firewalls, sistemas de detecção de intrusão e políticas de acesso, para garantir a confidencialidade, integridade e disponibilidade dos dados.

VII. Regras Normativas

A Politica de Segurança da Informação são elementos cruciais para o bom funcionamento estrutural, portanto, é imprescindível adotar todas as precauções e as normas, para protegê-las contra qualquer forma de manipulação, dano ou divulgação não autorizada.

As ações que violem esta Política ou suas normas complementares são passíveis de sanções administrativas, conforme a legislação em vigor.

1. **Serviço de e-mail:**

O serviço de e-mail corporativo deve ser usado exclusivamente para comunicações institucionais. Cada usuário receberá uma conta e senha única de e-mail corporativo, pessoal e intrasferível, sendo de responsabilidade única do titular da conta, que deverá ser disponibilizado pelo IPLANRIO através de um chamado com base na solicitação do superior imediato.

Todas as trocas de mensagens institucionais seguem critérios e medidas de segurança de acordo com a classificação das informações compartilhadas.

As mensagens armazenadas no serviço de e-mail corporativo estão sujeitas a auditoria a qualquer momento.

2. **Antivírus**

Cada estação de trabalho possui um software antivírus instalado, e a sua desinstalação ou alteração de configuração é bloqueada pela IPLANRIO. Qualquer arquivo proveniente de fontes externas, como CDs, discos rígidos, pen drives, ou obtidos pela internet, é verificado pelo mesmo antes de ser acessado pelo usuário.

3. **Acesso à internet**

O acesso à internet através da rede interna estará disponível em todas as estações de trabalho, sendo restrito apenas ao uso para os propósitos institucional.

As conexões podem ser monitoradas e registradas pela equipe de Tecnologia da Informação da IPLANRIO, a qualquer momento e sem aviso prévio, para identificar qualquer uso indevido, invasões ou presença de Malwares, sem a necessidade de autorização superior.

O PREVI-RIO não se responsabilizará por perdas ou danos resultantes de falhas na segurança durante o acesso de caráter pessoal.

O uso do acesso à internet disponibilizado será permitido para o uso com fins particulares pelos agentes públicos desde que o tempo e o conteúdo do acesso não prejudiquem o desempenho das responsabilidades do servidor público e não impactem negativamente no funcionamento da rede e a segurança dos sistemas do PREVI-RIO. Todas as conexões e conteúdos transmitidos estão sujeitos a monitoramento, mesmo que sejam de uso particular ou conteúdo privado.

O monitoramento e registro podem ser realizados mesmo em conexões autorizadas para fins particulares de acordo com esta política; O uso da internet de forma contrária às normas estabelecidas nesta política pode resultar em responsabilidade administrativa.

4. **Acesso aos Computadores**

- É importante garantir que todos os recursos disponíveis, sejam eles tecnológicos ou não, sejam utilizados exclusivamente para os propósitos da Instituição;
- Assegurar que os sistemas e informações sejam usados de acordo com as diretrizes estabelecidas nesta Política;
- Manusear os equipamentos com cuidado, pois são considerados patrimônio público. Qualquer anomalia ou falta de equipamentos deve ser comunicada imediatamente ao setor de TI para as devidas providências;
- A instalação de softwares ou equipamentos na rede corporativa requer autorização prévia da área responsável;
- 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.

VIII. Procedimento de Contingência

Toda administração de incidentes e riscos de segurança da informação é uma atividade do IPLANRIO, tendo assessoria da informática do PREVI-RIO quando solicitada.

O PREVI-RIO faz uso do Data Center do IPLANRIO que está situado na prefeitura do Rio de Janeiro, em local com acesso controlado e refrigerado.

Diariamente em horário noturno faz-se backups totais das bases de dados e arquivos compartilhados na rede. Os mesmos são guardados em mídias externas que ficam protegidas em cofres no próprio Data Center.

IX. Controle de acesso lógico

O acesso aos recursos de informação é feito utilizando um sistema de identificação pessoal e intransferível, responsabilizando o usuário por todas as atividades realizadas por meio desse acesso.

A concessão de permissões de acesso aos recursos de informação é limitada aos privilégios mínimos necessários para que os usuários desempenhem suas funções de trabalho.

O download de arquivos suspeitos é bloqueado.

X. Controle de acesso físico

Quanto às instalações físicas:

As medidas de proteção são proporcionais aos riscos identificados. Os recursos de informação considerados essenciais para as atividades são armazenados em áreas de acesso restrito, preferencialmente controladas por dispositivos de controle de acesso biométricos.

O acesso de visitantes às áreas que abrigam esses recursos de informação críticos é autorizado por um agente competente e supervisionado por um representante designado.

XI. Coordenadoria de Tecnologia da Informação e Comunicação

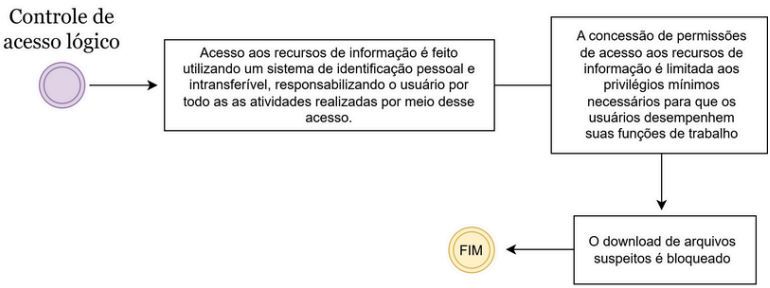
Cabe a Coordenadoria de Tecnologia da Informação e Comunicação do PREVI-RIO:

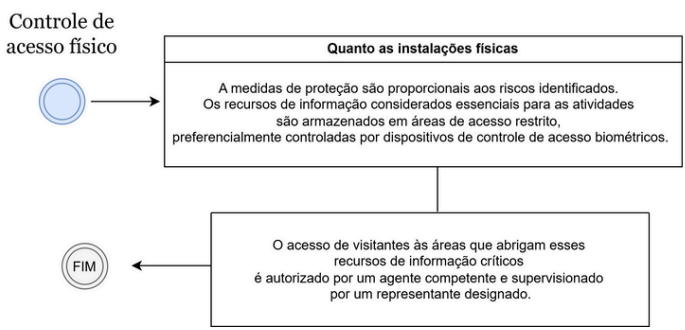
- Auxiliar na abertura de chamados junto ao IPLAN para criação de login, atribuição de direitos, solicitação de acesso ao espaço de compartilhamento na rede interna, bem como solicitação de acesso a qualquer recursos na rede;
- Criação de e-mail corporativo;

- Manutenções corretivas e atualizações nos computadores;
- Cadastro na intranet e atribuições de direito de acesso as aplicações setoriais do PREVI-RIO;
- Manutenções corretiva e evolutiva nas aplicações setoriais do PREVI-RIO;
- Desenvolvimento de novas soluções para necessidades setoriais do PREVI-RIO.

XII. Mapeamento

Controle Acesso Físico e Lógico





XII. Mapeamento

Procedimento de Contingência