## Universidade Federal Rural de Pernambuco Sistemas de Informação Segurança e Auditoria de Sistemas Lhaíslla Eduarda Cavalcanti Rodrigues da Silva RECIFE-PE

2023

Política de Uso de Recursos de Tecnologia

## Objetivo

## Esta política objetiva informar o colaborador sobre a política de uso da Internet e equipamentos de tecnologia no ambiente de trabalho da empresa, para haja a proteção do acesso aos serviços fornecidos, reduzindo riscos e oferecendo orientações ao usuário, assegurando o uso apropriado da Internet e recursos de tecnologia por parte do colaborador.

## Escopo

Esta política se aplica a todos os funcionários que tenham acesso aos serviços da empresa, sendo, colaboradores, estagiários e prestadores de serviço.

## Responsorialidades

## O uso da Internet e dos recursos de tecnologia por todos os usuários(internos/externos) e gestores de serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos computacionais, sendo permitido, sugerido e incentivado, desde que seu uso esteja relacionado aos objetivos e atividades fins do negócio ou responsabilidades do colaborador.

## É de responsabilidade do colaborador, seja interno ou externo a empresa, os prejuízos ou danos que causar ou sofrer em decorrência do descumprimento das diretrizes e normas referidas na Política de Segurança de acesso a serviços de tecnologia, nas normas e procedimentos específicos da empresa. Os envolvidos devem entender os riscos associados e cumprir rigorosamente as políticas, normas e procedimentos específicos vigentes.

## A empresa poderá, a qualquer tempo, revogar credenciais de acesso concedidas a usuários em virtude do descumprimento da Política de Segurança de acesso a serviços da empresa ou das normas e procedimentos específicos dela decorrente.

## **Regras de acesso e utilização de recursos, o que é proibido e inaceitável**

## Em complemento ao descrito acima, será considerado inaceitável tanto no uso quanto no comportamento dos colaboradores:

1. Assistir vídeos ou ouvir áudios/músicas que não tenham algum tipo de relação com as responsabilidades na empresa ou comprometam a produtividade;
2. Realizar compras pessoais na internet e tão pouco definir o endereço da empresa para entrega de qualquer tipo de correspondência ou pacote pessoal;
3. Executar atividades de qualquer tipo que gerem desperdício de tempo ou comprometam o foco do colaborador, ou da equipe;
4. Realizar atividades de navegação ou download que comprometam o desempenho da internet ou da rede corporativa;
5. Fornecer para terceiros senhas de acesso aos sistemas corporativos ou qualquer tipo de dado restrito da empresa;
6. Introduzir qualquer forma de vírus de computador dentro da rede corporativa;
7. Qualquer tentativa de burlar restrições de uso da internet implementadas pela empresa;

## 

## Riscos

## Perda de acesso: Caso haja perda das credenciais do usuário (login, senha, tokens) ou sejam expostas, até mesmo roubadas, um usuário mal-intencionado poderá utilizar essas credenciais para obter acesso a informações sensíveis.

* 1. Acesso restrito: Caso haja algum programa com acesso a informações do colaborador na máquina que não condiz com sua função, pode ser uma porta de entrada a softwares maliciosos.
  2. Compartilhamento de senhas: A senha de acesso aos sistemas é única a cada colaborador e em casos de compartilhamento pode imputar responsabilidade caso ocorra acesso a informações restritas da empresa, por parte de pessoas não autorizadas.

## Conformidade

## **5.1 Monitoramento**

## O uso da tecnologia e da Internet é uma ferramenta valiosa para o desempenho das atividades e para todo o negócio. Dessa forma, o mau uso desses recursos pode ter impacto negativo sobre a produtividade dos colaboradores e os resultados do negócio.

## Portanto, A implantação sistemas de monitoramento nas estações de trabalho, servidores, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, se fazem necessários para que a informação gerada por esses sistemas possa ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado. Dando o direito a empresa de aplicar restrições de navegação definidas conforme a política de uso da internet da empresa, visando garantir maior foco e produtividade dos colaboradores. E monitorar o uso da internet na rede corporativa, de forma individual, aplicado a cada equipamento e colaborador, registrando todo e qualquer tipo de acesso à internet realizados por cada equipamento conectado à rede.

## **5.2 Sanções**

## O descumprimento das regras de uso da Internet e dos recursos de tecnologia, descritas nesse documento, acarretará sanções, como:

## Advertência verbal ou por escrito

## Suspensão

## Dispensa por Justa Causa

## Orientações Gerais

## Para o cumprimento de suas responsabilidades, o uso dos recursos de tecnologia devem corresponder com as seguintes orientações:

1. Sigam a legislação corrente (sobre pirataria, pedofilia, ações discriminatórias);
2. Usem a Internet de uma forma responsável, consciente e munidos de bom senso;
3. Utilizem smartphones para atividades pessoais somente em casos de urgência;
4. Não criem riscos desnecessários para os equipamentos, informações ou para o negócio da empresa**;**
5. Utilizar serviços de gerenciamento de e-mail (como outlook, gmail, etc);
6. Não acessar o e-mail corporativo em dispositivos pessoais;
7. Não utilizar o e-mail corporativo de forma pessoal (cadastro em redes sociais, serviços de entrega de comida, etc);
8. Utilizar senhas fortes;
9. Manter a confidencialidade das senhas;
10. Informar qualquer problema ou suspeita de comprometimento a equipe de segurança;

No caso de dúvidas ou sugestões sobre a Política de Uso da Internet e Recursos de Tecnologia, o colaborador deve entrar em contato com o gestor ou responsável direto.

**Política de uso da Internet**

1. Objetivo

Esta política tem o propósito de definir o que é permitido ou não o acesso dentro das imediações da empresa, para que se possa atender as necessidades essenciais no desempenho das funções dos colaboradores em um ambiente com qualidade.

1. Escopo

A política de uso da internet se aplica a todos os funcionários que utilizem a internet da empresa, sendo, colaboradores, estagiários e prestadores de serviço.

1. Responsabilidade

O uso da Internet pelos colaboradores da empresa é permitido e encorajado desde que seu uso seja aderente aos objetivos e atividades fins do negócio. No desempenho das funções é necessário partilhar das seguintes diretrizes:

1. Não se utilizar do acesso à internet para comprometer a segurança(integridade, confidencialidade ou disponibilidade)de computadores, sistemas ou serviços da empresa;
2. O uso das credenciais de acesso à internet devem ser usados somente pela pessoa para que foram criados, sendo proibido o uso de usuário e senhas de outras pessoas, ficando o colaborador dono do usuário e senha responsabilizado por qualquer uso indevido dos mesmos na Internet.
3. Riscos  
   1. Vírus: O acesso a informações externas a rede apresenta o risco de vários tipos de vírus, que são prejudiciais, ao computador e sistema, podendo se espalhar para outros computadores, por meio de cópias d si mesmo e com isto comprometimento da rede e de equipamentos.
   2. Ataques a segurança da rede da empresa: Em caso de invasões a rede interna da empresa através da rede externa, que podem causar, sequestro de dados(Ransowame), roubo de dados sigilosos da empresa por meio de sites falsos(phishing).
4. Conformidade

5.1 Monitoramento  
 Com base nos riscos, a empresa reafirma que o uso da Internet é uma ferramenta valiosa para seus negócios, tem o direito de aplicar restrições de navegação segundo a política de segurança, monitorando o uso dos sistemas por meio dos Logs de rede, identificando e rastreando o uso e mau uso dos meios de internet, para seja garantida a segurança e sigilo do sistema, individualmente, aplicado a cada equipamento e colaborador com objetivo de garantir maior foco e produtividade dos colaboradores. Em adição, todos os recursos tecnológicos da [Empresa] existem para o propósito exclusivo de seu negócio. Portanto, a empresa se dá ao direito de monitorar o volume de tráfico na Internet e na Rede, juntamente com os endereços web (http://) visitados.

5.2 Sanções  
  
A falha em não seguir a política irá resultar em sanções que variarão desde procedimentos disciplinares, com avisos verbais ou escritos, até a demissão com justa causa.

1. Orientações gerais

O acesso à Internet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pela empresa. Sendo

1. Cada usuário é responsável pelas ações e acessos realizados por meio da sua conta de acesso.
2. É Proibido usar o computador para executar quaisquer tipos ou formas de fraudes, ou software/música pirata, criar ou transmitir material difamatório
3. É proibido visitas a sites da internet que contenha material obsceno e/ou pornográfico, ou páginas de conteúdo considerado ofensivo, ilegal ou impróprio.
4. É proibido o uso recreativo da internet em horário de expediente e acesso a outros conteúdos notadamente fora do contexto do trabalho desenvolvido.
5. É proibido utilizar os recursos da empresa para fazer download ou distribuição de software, ou dados não legalizados de software comercial, ou qualquer outro material cujo direito pertença a terceiros (copyright), sem ter um contrato de licenciamento ou outros tipos de licencie
6. É proibido executar atividades que desperdice os esforços do pessoal técnico ou dos recursos da rede

**Política de segurança de dados**

1. Objetivo  
   Esta política tem como propósito fornecer uma estrutura de segurança que garanta a proteção de dados da empresa contra acesso não autorizado, perda ou dano. Os dados da empresa podem ser verbais, digitais e/ou impressos, controlados individualmente ou compartilhados.
2. Escopo  
   A política de segurança de dados se aplica a todos os funcionários, colaboradores, estagiários e prestadores de serviço que tenham acesso aos dados da empresa.
3. Responsabilidade  
     
   É de responsabilidade dos colaboradores, funcionários, estagiários e prestadores de serviço com acesso aos dados da empresa, tenham a compreensão dos níveis de classificação dos dados da empresa. Cada envolvido com a empresa tem o compromisso com a integridade dos dados de modo que todo prejuízo ou dano que sofrer ou causar para empresa em decorrência do descumprimento das diretrizes e normas referidas na Política de Segurança dos dados e nas normas e procedimentos específicos dela decorrentes
4. Risco  
   1. Perda ou roubo de dados
   2. Acesso não autorizado aos dados
   3. Alteração de dados
   4. Distribuição de dados sensíveis
   5. Acesso externo a informações sigilosas
5. Conformidade  
     
   **5.1 Monitoramento**

Cabe a empresa monitorar os dados, disponibilidade e capacidade que ambientes de TI permitem as equipes reagir rapidamente diante de incidentes que acarretem indisponibilidade de algum serviço essencial.

Também compete a empresa instalar sistemas de proteção, preventivos e detectáveis, para garantir segurança das informações e dos perímetros de acesso. Desinstalar sistemas, a qualquer tempo, qualquer software ou sistema que represente risco ou esteja em desconformidade com as políticas, normas e procedimentos vigentes.

**5.2 Sanções**

## O descumprimento das regras da política de segurança de dados, descritas nesse documento, acarretará sanções, como:

## Advertência verbal ou por escrito

## Suspensão

## Dispensa por Justa Causa

* 1. Processo

1. Orientação gerais  
   1. Proteger a integridade e disponibilidade dos dados.
   2. Proteger qualquer chave física, cartão de identificação, conta de computador ou conta de rede que permita acesso aos dados da empresa.
   3. Descartar mídia que contém dados da empresa de maneira consistente, isso inclui qualquer documento impresso, meio de armazenamento eletrônico, magnético ou óptico.
   4. Não divulgar, copiar, liberar, vender, emprestar, alterar ou destruir qualquer dado sem autorização.