**CENTRO PAULA SOUZA**

**ESCOLA TÉCNICA ESTADUAL DE PERUÍBE**

**Ensino Técnico em Informática Integrado ao Ensino Médio**

**Guilherme Jose Santos Da Silva**

**João Victor Pereira da Silva**

**Jorge Mauricio dos Santos**

**Luís Carlos de Oliveira Junior**

**Valter Muniz dos Santos**

**Políticas de Segurança:** Projeto ElderApp - Aplicativo de auxílio aos idosos e Casas de Repouso

**Peruíbe**

**2020**

**Guilherme José Santos Da Silva**

**João Victor Pereira da Silva**

**Jorge Mauricio dos Santos**

**Luís Carlos de Oliveira Junior**

**Valter Muniz Santos**

**Políticas de Segurança:** Projeto ElderApp - Aplicativo de auxílio aos idosos e Casas de Repouso

**Peruíbe**

**2020**

**SUMÁRIO**

**INTRODUÇÃO** 3

**1. POLÍTICAS DE SEGURANÇA** 4

**1.1 Autenticação** 4

**1.2 Políticas de Senhas** 4

**1.3 Políticas de Acesso à Internet** 5

**1.4 Políticas de uso de estação de trabalho** 5

**1.5 Política Social** 6

**1.6 Vírus e códigos de segurança** 7

**REFERÊNCIAS BIBLIOGRÁFICAS** 8

**INTRODUÇÃO**

A segurança é um das questões mais importantes e principal preocupação de qualquer empresa. Nesse documento apresentaremos um conjunto de instruções e procedimentos para normatizar e melhorar nossa visão e atuação em segurança do projeto ElderApp, aplicativo de auxílio aos idosos e casas de repouso.

Inicialmente, a Segurança da Informação deve conter três princípios simples:

- **Confidencialidade**: Propriedade que determina que a informação deva estar disponível apenas para pessoas autorizadas;

- **Integridade**: Propriedade que prevalece que a informação esteja certa, confiável, sem que ocorra mudanças não autorizadas;

- **Disponibilidade**: Propriedade que estabelece que a informação esteja sempre disponível para a utilização legítima de pessoas autorizadas.

Todas as normas aqui definidas deverão ser seguidas à risca por todos os funcionários, parceiros e prestadores de serviços. Ao receber uma cópia da Política de Segurança, todos estão comprometidos a respeitar todos os tópicos aqui apresentados e está consiso de que seus e-mails e navegação na internet poderão estar sendo monitorados. A equipe de segurança encontra-se a total disposição para saneamento de dúvidas e auxílio técnico.

O não cumprimento dessas regras acarretará em sanções administrativas em primeira instância, podendo acarretar no desligamento do funcionário de acordo com a gravidade da ocorrência e cancelamento temporário ou permanente de sua conta.

**1. POLÍTICAS DE SEGURANÇA**

**1.1 Autenticação**

A autenticação nos sistemas de informática serão baseados em uma senha. Esse meio é muito utilizado por sua facilidade de implantação e manutenção e por seu baixo custo. Infelizmente esse meio também é o mais inseguro. Então aprenda a criar senha de forma coerente, observando nossa política de senhas.

**1.2 Políticas de senhas**

- A senha deverá conter no mínimo 6 caracteres alfanuméricos, podendo contér também simbolos, recomendado uma vez que deixa a conta ainda mais segura.

- Tente não separar numéros e letras, pois ficam mais fáceis de serem decifrados. Senhas como nome do usuário, combinações simples (xyz890), substantivos (casa, filmes, nomes, brasil), datas (25082020) e outros são bem fáceis de decifrar. Procure misturar letras maiúsculas e minúsculas com números e símbolos pra melhorar a segurança da sua conta.

- Para facilitar a memorização das senhas, pode optar pelo uso de mnemônios. Por exemplo: eSam3f (eu SEMPRE amarei meus 3 filhos) m1Nh4s3Nh45 (A palavra minhasenha onde o 1, 3, 4 e 5 substituem respectivamente o I, E, A e S).

- Para garantir a segurança dos dados do usuário, o login será limitado a 3 tentativas. Após isso será efetuado um bloqueio temporário da conta do usuário, e será mandado uma mensagem sugerindo a troca da senha, que deverá ser refeita através do email ou número de telefone do usuário.

- Sua senha não deve ser jamais passada a ninguém, nem mesmo a equipe de segurança. Lembrando que a equipe também não pode solicitar a senha do usuário.

- É aconselhado que não abra sua conta conectado a uma rede pública, mas se necessário lembre-se sempre de sair da conta após o uso.

- Caso desconfie que sua senha não está mais segura, sinta-se à vontade para altera-la ou notifique a empresa pedindo uma alteração da senha.

- Tudo que for executado com a sua senha será de sua inteira responsabilidade, por isso tome todas as precauções possíveis para manter sua senha secreta.

**1.3 Políticas de Acesso à Internet**

Além da empresa de segurança, os Lares de Idosos que possuem acesso a rede também poderão acessar a internet. Mas, sempre lembrando que é melhor haver regras quanto ao uso dessa rede. No caso das casas de repouso e lares de idosos fica a critério seguir ou não as recomendações à seguir. Lembrando que elas são de extrema importância para garantir a segurança dos dados e a privacidade do usuário.

- O uso recreativo da internet não poderá ser em horário de expediente.

- Durante o expediente, somente navegação de sites é permitida, para fins de necessidades ou emergências, mais para uma fonte de consulta. Exemplo: pesquisar por atividades físicas para idosos, lazer, bem-estar, saúde, sintomas de doenças, problemas socio-emocionais, etc.

- É proibido o acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados, que estarão sendo monitorados e poderão ser bloqueados.

- É proibido o uso de IM (Instant messengers) nãoautorizados pela equipe de segurança. Lembrando novamente que o uso da internet estará sendo auditado constantemente e o usuário poderá vir a prestar contas de seu uso e ter sua conta bloqueada.

**1.4 Política de uso de estação de trabalho**

Essa parte pode se referir tanto para os funcionários da empresa, membros e administrados, quanto para os funcionários das casas de repouso e similares que acessam a rede através de máquinas locais.

- Cada estação de trabalho tem códigos internos que permitem sua identificação na rede, sendo que cada indivíduo possui sua própria estação de trabalho. Isso significa que tudo que venha a ser compilado de sua estação será de sua responsabilidade. Por isso sempre que abandonar sua estação, tenha certeza de que efetuou logoff ou travou o console.

- Não instale nenhum tipo de software / hardware sem autorização da equipe técnica ou de segurança.

- Não baixe arquivos MP3, vídeos, filmes, jogos, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria nas máquinas locais.

- Não consuma nenhum tipo de comida ou bebida perto das maquinas, para evitar acidentes ou danos aos aparelhos.

- Nunca tente dar manutenção no computador por conta própria. Sempre que houver algum problema, notifique a equipe técnica autorizada para que ela possa solucionar o problema.

- Não danifique nenhum dos componentes dos computadores ou periféricos. Sempre manuseie com cuidado ao utilizar os computadores.

- Mantenha na sua estação somente o que for supérfulo ou pessoal. Todos os dados relativos à empresa devem ser armazenados no servidor, onde existe um sistema de backup diário confiável. Caso não saiba como fazer isso, entre em contato com a equipe técnica.

**1.5 Política Social**

Sendo seres humanos, temos a grande vantagem de sermos sociáveis, mas muitas vezes quando esquecemos o conceito de segurança, isso se torna uma desvantagem. Por isso preste atenção nos seguintes tópicos:

- Não diga sobre a política de segurança da empresa com terceiros ou em locais públicos.

- Nunca diga sua senha para ninguém. A equipe técnica jamais poderá pedir sua senha.

- Evite digitar suas senhas ou usuários em máquinas de terceiros, especialmente fora da empresa, pois estará mais vulnerável a ataques.

- Não aceite a ajuda de ninguém que não seja um membro da equipe técnica previamente apresentado e identificado pela empresa.

- Nunca execute procedimentos técnicos cujas instruções tenham chego por e-mail ou via redes socias. A empresa só se comunica através de um canal oficial, seja ele um e-mail oficial ou telefone fixo.

- Relate a equipe de segurança pedidos externos ou internos que venham a discordar dos tópicos anteriores.

- Evite gravar suas senhas em arquivos guardados no computador (pessoal ou empresarial), pois isso deixa a conta vulnerável se por acaso o PC for invadido. Tente criar senhas que sejam fáceis de lembrar, mas que ainda assim sejam complexas.

**1.6 Vírus e Códigos Maliciosos**

- Mantenha seu anti-vírus atualizado. Provavelmente a equipe técnica se encarregará de cuidar disso, mas, em caso de não tiver sido feito ou você perceba que a atualização não é funcional, comunique a mesma para que a situação seja corrigida.

- Não traga CDs, Pen Drives, HD’s ou Cartões SD de fora da empresa. Caso seja extremamente necessário, leve os mesmos para a equipe técnica, onde serão verificados antes de haver a liberação para o uso.

- Reporte atitudes suspeitas em seu sistema a equipe técnica, para que possíveis vírus possam ser identificados no menor espaço de tempo possível.

- Suspeite de softwares que "você clica e não acontece nada", o propagandas ou anúncios, mandados por e-mail.

**REFERÊNCIAS BIBLIOGRÁFICAS**

FERREIRA, Rafael. **Soluções de Segurança da Informação para o mundo corporativo (Atualidade e projeção de mercado)**. Disponível em: <https://pt.slideshare.net/clavissecurity/palestra-semana-estaciosiv01>. Acesso em: 25 ago. 2020.