

## 1. Introdução

A segurança é um dos assuntos mais importantes dentre as preocupações de qualquer empresa. Nesse documento apresentaremos um conjunto de instruções e procedimentos para normatizar e melhorar nossa visão e atuação em segurança.

## 2. A empresa e a política de segurança.

Todas as normas aqui estabelecidas serão seguidas à risca por todos os funcionários, parceiros e prestadores de serviços. Ao receber essa cópia da Política de Segurança, o/a Sr/Sra comprometeu-se a respeitar todos os tópicos aqui abordados e está ciente de que seus e-mails e navegação na internet/intranet podem estar sendo monitorados. A equipe de segurança encontra-se a total disposição para saneamento de dúvidas e auxílio técnico.

### 2.1 O não cumprimento dessa política.

O não cumprimento dessas políticas acarretará sanções administrativas em primeira instância, podendo acarretar o desligamento do funcionário de acordo com a gravidade da ocorrência.

## 3. Autenticação

A autenticação nos sistemas de informática será baseada 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. Senhas como nome do usuário, combinações simples (abc123), substantivos (casa, meia, cadeira, Brasil), datas (11092001) e outros são extremamente fáceis de descobrir. Então aprenda a criar senha de forma coerente, observando nossa política de senhas.

### 3.1 Política de senhas:

Uma senha segura deverá conter no mínimo 8 caracteres alfanuméricos (letras Minúscula e Maiúscula, números e Caracteres especiais) com diferentes caixas. As senhas deverão ser trocadas no primeiro acesso. As senhas terão um tempo de vida útil determinado pela equipe de segurança, devendo o mesmo ser respeitado, caso contrário o usuário ficará sem acesso aos sistemas.

- Sua senha não deve ser jamais passada a ninguém, nem mesmo da equipe de segurança. Caso desconfie que sua senha não esteja mais segura, sinta-se à vontade para alterá-la, mesmo antes do prazo determinado de validade. - 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.

#### **4. Política de e-mail:**

Não abra anexos com as extensões .bat, .exe, .src, .lnk dentre outras extensões, se não tiver certeza absoluta de que solicitou esse e-mail. - Desconfie de todos os e-mails com assuntos estranhos e/ou em inglês. Alguns dos vírus mais terríveis dos últimos anos tinham assuntos como: ILOVEYOU, Branca de neve pornô, etc. - Não reenvie e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, criança doente, pague menos em alguma coisa, não pague alguma coisa, etc. - Não utilize o e-mail da empresa para assuntos pessoais. - Não mande e-mails para mais de 20 pessoas de uma única vez (to, cc, bcc) - Evite anexos muito grandes – Sempre use sua assinatura para troca de e-mails.

#### **5. Políticas de acesso à Internet:**

- O uso recreativo da internet não deverá se dar no horário de expediente. - Somente navegação de sites é permitida. Casos específicos que exijam outros protocolos deverão ser solicitados diretamente a equipe de segurança com prévia autorização do supervisor do departamento local. - Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados estará bloqueado e monitorado. É proibido o uso Messenger/Chat não homologados/autorizados 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.


#### **6. Política de uso de estação de trabalho:**

Cada estação de trabalho tem códigos internos que permitem que ela seja identificada na rede, e cada indivíduo possui sua própria estação de trabalho. Isso significa que tudo que venha a ser executado de sua estação acarretará responsabilidade sua. Por isso sempre que sair da frente de sua estação, tenha certeza que efetuou logoff ou travou o console, Salve os documentos e desliguem suas estações de trabalho no fim do expediente - Não instale/conectem nenhum tipo de software / hardware sem autorização da equipe técnica ou de segurança - Não tenha MP3, MP4, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria - Mantenha na sua estação somente o que for supérfluo ou pessoal. Todos os dados relativos à empresa devem ser mantidos no servidor ou pasta do departamento, onde existe um sistema de backup diário e confiável. Caso não saiba como fazer isso, entre em contato com a equipe técnica.

#### **7. Política Social:**

Como seres humanos, temos a grande vantagem de sermos sociáveis, mas muitas vezes quando discorremos sobre segurança, isso é uma desvantagem. Por isso observe os seguintes tópicos: - Não fale sobre a política de segurança da empresa com terceiros ou em locais públicos. - Não diga sua senha para ninguém. Nossa equipe técnica jamais irá pedir sua senha. - Não digite suas senhas ou usuários em máquinas de terceiros, especialmente fora da empresa. - Somente aceite ajuda técnica de um membro de nossa equipe técnica previamente apresentado e identificado. - Nunca execute procedimentos técnicos cujas instruções tenham chegado por e-mail. - Relate a equipe de segurança pedidos externos ou internos que venham a discordar dos tópicos anteriores.

<b>Data:</b> 03/08/2020	<b>Elaborado por:</b> Claudio Ferreira Analista de TI		<b>Aprovado por:</b> Rodrigo Gonçalves Diretor. Adm/Financ	
-------------------------	---	--	--	--

	Política	PC 07.03
	Segurança da Informação	Rev 01
		Página 3 de 3

## 8. Política de Antivírus:

Mantenha seu antivírus atualizado. Provavelmente nossa equipe técnica irá se encarregar disso, mas caso não tenha sido feito ou você perceba que a atualização não está funcional, entre em contato com a mesma para que a situação possa ser corrigida. - Não traga pendrives, CDs, ou qualquer tipo de mídia de fora da empresa. Caso isso seja extremamente necessário, encaminhe o mesmo para a equipe técnica, onde passará por uma verificação antes de ser liberado para 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"

Temos um antivírus em todos os computadores e notebooks para segurança chamado Bitdefender, este antivírus é ativo na máquina, em qualquer momento este antivírus pode bloquear/excluir um arquivo ou aplicativo. Semanalmente é feito um escaneamento mais profundo nas máquinas, em caso de arquivo suspeito, é levado para quarentena, podendo se deletado ou não, arquivos considerados perigosos são excluídos automaticamente do computador. A equipe Responsável pela segurança da informação tem autonomia para caso julguem necessário, tomar medidas pró-ativas para combater ou prevenir qualquer ameaça à segurança da informação.

## 9. Continuidade de negócios:

De nada adianta uma informação segura se a mesma estiver indisponível para quem necessita dela. Por isso nossas equipes técnicas e de segurança contam com a sua colaboração para manter nossa empresa como líder de mercado. Entre em contato conosco sempre que julgar necessário.

### 9.1 Membros da equipe técnica

Claudio Ferreira, [claudio.ferreira@viaexpressa.com](mailto:claudio.ferreira@viaexpressa.com) 11 95127-5064

Thiago Pupo, [suporte.viaexpressa@viaexpressa.com](mailto:suporte.viaexpressa@viaexpressa.com) 11 95916 7032

Data: 03/08/2020	Elaborado por: Claudio Ferreira Analista de TI		Aprovado por: Rodrigo Gonçalves Diretor. Adm/Financ	
------------------	--	--	---	--