POLÍTICA DE SEGURANÇA

1. INTRODUÇÃO

A segurança da informação é um dos pilares de qualquer empresa. Nesse documento iremos apresentar um conjunto de instruções e procedimentos para melhorar nossa visão e aplicação na área de segurança da informação.

1.1 A empresa e a Política

Todas as normas estabelecidas serão seguidas por todos os funcionários, parceiros e colaboradores. Desta forma, quando divulgado e entregue a cópia deste documento, todos que receberem se comprometem a respeitar todos os tópicos abordados e está ciente do comprometimento perante o documento.

1.2 O não cumprimento da Política de Segurança

O não cumprimento das políticas aqui detalhadas acarretará sanções administrativas em primeiro momento, podendo na reincidência ou conforme a gravidade do ato contrário à esta política acarretar o desligamento do funcionário.

2. OBJETIVOS

Servirá esta Política de Segurança para definir normas e procedimentos de segurança da informação, alem de implementar controles e processos para atendimento. Temos ainda como objetivo preservar as informações quanto à:

• Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

• Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

• Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

3. AUTENTICAÇÃO

A autenticação nas estações de trabalho e sistemas da Attitude será através de login e senha especificas e cadastradas para cada usuário.

3.1 Políticas de Senhas (Estação de Trabalho)

As senhas deverão conter no mínimo 8 dígitos, contendo letras, numeros e caractere. As senhas terão um tempo de vida útil de 42 dias, sendo necessário a troca da mesma após esse período.

3.2 Políticas de Senha (Sistemas)

As senhas para acessar os sistemas serão passadas para cada colaborador e parceiro individualmente com as permissões necessários, considerando o cargo que representa.

3.3 Compartilhamento de Senhas

Os logins e senhas disponibilizados, jamais deverão ser compartilhados com nenhum funcionário da empresa, visto que é de responsabilidade do funcionário toda e qualquer ação suas informações.

4. POLÍTICA DE COMPARTILHAMENTO DE PASTAS DE PASTAS

As pastas de rede são compartilhadas de acordo com o cargo e gestão das áreas responsáveis. Cada área possui uma pasta compartilhada com os demais funcionários do departamento específico.

4.1 Solicitação de acesso as pastas

A solicitação de acesso as pastas deverão ser feitas pelo gerente responsável através de um e-mail ao departamento de T.I solicitando a liberação para o usuário específico.

5. POLÍTICA DE CORREIO ELETRONICOS

O uso de correio eletrônicos (e-mail) será para fins corporativos. É importante frisar, que todas as contas possuem um espelhamento de informações de até 2 dias uteis (prazo padrão) no servidor de e-mail.

O usuário deverá seguir as seguintes normas no ambiente de trabalho:

- Não abrir arquivos com extensões .bat, .exe, .src, .link e/ou qualquer arquivo que não tenha conhecimento do assunto ou do remetente.

- Não utilizar e-mail corporativo para assuntos pessoais.

- Em caso de dúvida sobre o arquivo e/ou remetente, solicitar sempre o apoio do Departamento de Tecnologia.

6. POLÍTICA DE ACESSO A INTERNET

Sabemos da importância de assegurar as informações dos nossos clientes e parceiros. Para isso, utilizamos a tecnologia de controle de filtro da SonicWall para bloquear acessos a sites maliciosos ou que contenham conteúdos não necessários para a aplicação do trabalho.

6.1 POLÍTICAS DE REGRAS DE ACESSO A SITES

Possuímos grupos específicos de regras de acesso a sites. Desta forma serão liberados somente site necessários para a aplicação do trabalho.

Possuímos relatorios com todos os acessos efetuados por cada funcionário da empresa.

7. POLÍTICA DE USO DE ESTAÇÃO DE TRABALHO

Cada estação de trabalho possui identificação que permite que ela seja identificada na rede e exceto operação, cada indivíduo possui sua própria estação de trabalho.

7.1 Gerenciamento de Diretivas

As estações de trabalho são controladas através de Gerenciamento de Diretivas. Desta forma, todos os bloqueios, liberações são feitos através desse gerenciador.

7.2 Instalação de Softwares

A instalação de novos softwares deve ser solicitada ao departamento de tecnologia, pois eles são responsáveis por manter a segurança do ambiente e estação de trabalho.

7.3 Estação de trabalho (Callcenter)

Nas estações de trabalho da operação de Callcenter, é proibido o uso de papel, celulares e/ou qualquer outro objetivo que seja possivel armazenar os dados do cliente.

8. POLÍTICA DE PROTEÇÃO AO AMBIENTE DE TRABALHO

Para mantermos o ambiente de trabalho sempre seguro será necessário

- Manter o ambiente o antivírus sempre atualizados.

- Manter bloqueado o uso de USB, CD’s e disquetes.

- Manter sempre os monitoramentos necessários para evitar vazamentos de dados dos clientes.

9. DISPOSIÇÕES FINAL

A segurança deve ser entendida como parte fundamental da cultura Attitude. Qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

10. MEMBROS DO DEPARTAMENTO TECNICO E SEGURANÇA

Nome: Paulo Henrique Cerato
Cargo: Coordenador
E-mail: pcerato@attgestao.com.br
Telefone: 11 98101-6832

Nome: Lucas Gonçalves
Cargo: Supervisor
E-mail: lgoncalves@attgestao.com.br
Telefone: 11 99818-6882