Políticas de Segurança

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.

1.1 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.

1.2 O não cumprimento dessa política

O não comprimento dessas políticas acarretará em sanções administrativas em primeira instância, podendo acarretar no desligamento do funcionário de acordo com a gravidade da ocorrência.

2. 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.

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.

2.1 Política de senhas

Uma senha segura deverá conter no mínimo 6 caracteres alfanuméricos (letras e números) com diferentes caixas.

Para facilitar a memorização das senhas, utilize padrões mnemônicos. Por exemplo:

eSus6C (eu SEMPRE uso seis 6 CARACTERES)

odIamp0709 (ouviram do Ipiringa as margens plácidas 7 de Setembro)
s3Nh45 (A palavra senha onde o 3 substiui o E, o 4 o A e o 5 o S)

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 está mais segura, sinta-se à vontade para altera-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.

2.2 Política de e-mail

- Não abra anexos com as extensões .bat, .exe, .src, .lnk e .com 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 10 pessoas de uma única vez (to, cc, bcc)

- Evite anexos muito grandes

- Utilize sempre sua assinatura criptográfica para troca interna de e-mails e quando necessário para os e-mails externos também

2.3 Políticas de acesso a 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 de ferramentas P2P (kazaa, Morpheus, etc)

- É proibido o uso de IM (Instant messengers) 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.

3. 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 em responsabilidade sua. Por isso sempre que sair da frente de sua estação, tenha certeza que efetuou logoff ou travou o console.

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

- Não tenha MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria

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

4. Política Social

Como seres humanos, temos a grande vantagem de sermos sociáveis, mas muitas vezes quando descorremos 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 chego por e-mail.

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

5. Vírus e códigos maliciosos

- Mantenha seu anti-vírus 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 disquetes ou CDs 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"

6. 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.

6.1 Membros da equipe técnica

Nome	E-mail	Ramal	Celular
Fulano	fulano@empresa.com	123	9999-9991

6.2 Membros da equipe de segurança

Nome	E-mail	Ramal	Celular
Fulano	fulano@empresa.com	123	9999-9991