ANALITICA consultoria

POLÍTICAS DE SEGURANÇA DE DADOS

1. INTRODUÇÃO

Neste documento apresentaremos um conjunto de normas, instruções e procedimentos para normatizar e melhorar nossa visão e atenção em segurança. A segurança é um dos assuntos mais importante dentre as preocupações de uma empresa.

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 Sr. comprometeu-se a respeitar-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 NÃO cumprimento dessa Política

O não cumprimento dessa política 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 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), datas e outros são extremamente fáceis de descobrir. Então aprenda a criar senha de forma coerente, observando nossa política de senhas.

2.1 Políticas de Senhas

Uma senha segura deverá conter no mínimo 8 (oito) caracteres alfanuméricos (letras e números) com maiúsculas e minúsculas. Para facilitar a memorização das senhas, utilize padrões mnemônicos. Por exemplo: eSus8C (euSEMPREuso8CARACTERES), ou qualque outra formação que seja familiar ao usuário.
As senhas terão vida útil determinada pela equipe de segurança, devendo a mesma ser respeitada, caso contrário o usuário ficará sem acesso aos sistemas.
As senhas não deverão ser repassadas a ninguém, nem mesmo à equipe de segurança. Caso desconfie que sua senha não esteja mais segura, fique 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.

2.2 Política de E-mail

Não abra anexos com as extensões .bat, .exe, .src, .lnk, .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 se não for de seu hábito recebe-los. Alguns dos vírus mais terríveis dos últimos anos tinham assuntos como ILOVEYOU, BrancadeNeve, etc.
Não reenvie e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, pague menos em alguma coisa, etc..
Não utilize o e-mail da empresa para assuntos pessoais.
Não mande e-mails para mais de 10 pessoas de uma só vez.
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-papos, apostas e assemelhados estará bloqueado e será monitorado.
Proibido o uso de Instant Messengers não homologados/autorizados pela equipe de segurança.
LEMBRANDO: 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 de trabalho acarretará em responsabilidade sua. Por isso, sempre que sair da frente de sua estação, tenha certeza que efetuou logoff ou travou a console.
Não instale nenhum tipo de software ou hardware sem autorização e/ou concordância. da equipe técnica ou da equipe 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 supérfluo 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 com fazer isso, entre em contato com a sua equipe técnica.

4. POLÍTICA SOCIAL

Como seres humanos têm 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. A 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.

5. VIRUS E CÓDIGOS MALICIOSOS

Mantenha seu antivírus atualizado sempre. 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 equipe para que a situação seja 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 à 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 técnica 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

6.2 Membros da Equipe de Segurança

NOME	E-MAIL	RAMAL	CELULAR

7. TERMO DE RESPONSABILIDADE

Concordo com as disposições descritas acima e firmo este documento ciente das responsabilidades e encargos que passo a ter responsabilidade.