CENTRO DE ESTUDOS OCTAVIO DIAS DE OLIVEIRA

CNPJ: 06.152.582/0001-08

FACULDADE UNIÃO DE GOYAZES

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TRINDADE – GO

Sumário

1. Apresentação

Com o avanço tecnológico, o uso de computadores conectados em redes exigiu uma estrutura de segurança mais sofisticada nas empresas, englobando controles lógicos e equipes especializadas, para garantir a guarda segura das informações das empresas.

Essa expansão tecnológica mostrou para empresas a necessidade de criar regras e procedimentos para o uso dos computadores afim de manter o controle e o monitoramento, visando otimizar o investimento em tecnologia e evitar gastos desnecessários devido ao uso indevido dos ativos de TI e acesso não autorizado a informação.

A política de segurança é um mecanismo preventivo de proteção dos dados e processos importantes para empresa. Neste documento definimos diretrizes, normas e procedimentos que devem ser seguidos por todos os colaboradores, parceiros e fornecedores que fazem uso do ambiente computacional, são estabelecidos princípios institucionais de como a organização deverá proteger, controlar e monitorar seus recursos computacionais e informações manipuladas. O não cumprimento desta política implica em falta grave e poderá resultar em uma ação disciplinar, demissão e/ou processo civil ou criminal.

2. Abrangência

Esta política se aplica aos funcionários, prestadores de serviços, consultores, temporários e demais colaboradores que estejam a serviço da empresa, incluindo toda mão-de-obra terceirizada ou disponibilizada mediante convênio, parcerias ou quaisquer outras formas de atuação conjunta com outras empresas e abrange todos os sistemas e equipamentos de propriedade da empresa, bem como aqueles de propriedade de terceiros que lhe sejam confiados a qualquer título ou cedidos pela mesma a terceiros.

3. Missão do Departamento de Tecnologia da Informação

Garantir a disponibilidade, integridade, confiabilidade, legalidade, autenticidade e audibilidade da informação necessária para a realização do

negócio da empresa. Proteger as informações, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

4. É Dever de Todos na Empresa

Considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para empresa e deve sempre ser tratado profissionalmente.

Com o intuito de proteger as informações da empresa, 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. Nem deixe-a escrita em lugar visível ou fácil de ser descoberta;
- Não digite sua senha ou usuário em máquinas de terceiros, especialmente fora da empresa;
- Somente aceite ajuda técnica de um membro da nossa equipe técnica previamente apresentado e identificado;
- Somente execute procedimentos técnicos cujas instruções tenham chegado por e-mail da equipe técnica da empresa.

É recomendado que todos os funcionários leiam a política de segurança da informação e tire suas dúvidas junto à equipe técnica da empresa.

5. Política

5.1. Política de Senha

Dentre as políticas utilizadas pelas grandes corporações a composição da senha ou password é a mais controversa. Por um lado profissionais com dificuldade de memorizar várias senhas de acesso, por outro, funcionários displicentes que anotam a senha sob o teclado no fundo da gaveta, em casos mais graves o colaborador anota a senha no monitor.

A adoção das seguintes regras tende a minimizar o problema, mas a regra fundamental é a conscientização dos colaboradores quanto ao uso e manutenção das senhas.

- Prazo de validade da senha é de 90 dias;
- Não é permitido o uso das últimas 3 senhas digitadas anteriormente;
- Não é permitido o uso de senhas com caracteres repetidos;
- A senha deve ser composta no mínimo de 7 caracteres, contendo números, letras alfabéticas e caracteres especiais;
- Não é permitido o uso de senha de terceiro;

As senhas de acesso são de uso individual e restrito. O compartilhamento de senha é terminantemente proibido. O usuário possuidor da senha será responsável por todas as ações realizadas com sua senha.

Guarde sua senha em local seguro, de preferência memorizada. Nunca deixe a senha por escrito sob o teclado, na gaveta, ou mesmo colada junto ao monitor.

5.2. Política de E-mail

Grande parte de nossa comunicação do dia-a-dia passa através de e-mails. Mas é importante lembrar que grande parte das pragas eletrônicas chegam por esse meio. Devemos lembrar que os vírus atuais são mandados automaticamente.

Alertamos a todos que ao receber um e-mail, verifique sua procedência. **Nunca abra e-mail de conteúdo duvidoso, mesmo que seja de alguém conhecido.** Grande parte das mensagens que circulam na Internet é: ***spam, virus, trojans e worm***. Essas mensagens assumem disfarce com o objetivo de iludir e induzir o destinatário a fazer alguma coisa, solicitando que envie dados confidenciais (preencher um formulário, executar um programa **<<click aqui>>,**

assista algum vídeo, etc) para algum endereço eletrônico ou que se cadastre em uma página da Internet, que na verdade é uma cópia de alguma outra página.

Na maioria dos casos, essas armadilhas são criadas para obter informações pessoais e senhas para que possam ser usadas em algum tipo de fraude ou para transferência bancária e compras pela Internet.

O servidor de email da Google, que utilizamos, já faz um pré-filtragem de alguns e-mails marcando-os Spam. Lembramos que este trabalho é preventivo e que algumas atitudes do usuário final são requeridas:

- Não abra anexos com as extensões: .bat, .exe, .com .src, .lnk e vídeos;
- Desconfie de todos os e-mails com assuntos estranhos e/ou em inglês;
- 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. Isso consome recurso da rede, do servidor e banda da Internet, prejudicando quem realmente precisa utilizar.
- 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 anexo muito grande, tamanho máximo ideal de 5 MByte por e-mail;

5.3. Política de Internet

A Internet é indiscutivelmente nossa mais poderosa ferramenta de trabalho, devemos encará-la dessa forma dentro da empresa. O uso recreativo da mesma não deverá ocorrer em momento algum, mesmo por que, qualquer acesso a Internet fica registrado em nosso banco de dados para fins de auditoria.

Regra Geral:

- 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 assistir e/ou baixar vídeos;
- É proibido ouvir rádio;
- É proibido o uso de MSN/Skype ou outro tipo de Chat dentro da empresa para fins particulares;
- É proibido o uso de e-mails particulares dentro da empresa.

5.4. Política de Estação de Trabalho

Cada estação de trabalho tem códigos internos que permitem que ela seja identificada na rede e cada pessoa possui sua própria estação de trabalho. Isso significa que tudo que venha a ser executado na estação de trabalho é de inteira responsabilidade do usuário. Por isso, orientamos, sempre que sair de frente da estação de trabalho, tenha certeza que sua estação de trabalho está com o acesso bloqueado (proteção de tela), impossibilitando que outra pessoa utlize enquanto você está ausente.

Lembramos que a estação de trabalho é uma ferramenta de trabalho, mas também é um importante componente de segurança. Por isso observe as seguintes recomendações:

- 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 estação de trabalho somente os dados pessoais e 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.

5.5. Política de Utilização da Rede Local

Rodovia GO 060, Km 19, 3.184,
Laguna Park • Trindade • Goiás • 75.380-000
62.3506.9300 • contato@fug.edu.br • www.fug.edu.br

Esse tópico visa definir as normas de utilização da rede que abrange o login, manutenção de arquivos no servidor e tentativas não autorizadas de acesso. Estes itens estarão sendo abordados para todos os usuários dos sistemas e da rede de computadores.

Regras Gerais

- Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta (também conhecido como "*cracking*"). Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se ao servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes;
- Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques, tentativas de provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor;
- Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas em uso, evitando, desta maneira, o acesso por pessoas não autorizadas, se possível efetuar o logout/logoff da rede ou bloqueio do computador através de senha;
- O usuário deve fazer manutenção no diretório do departamento localizado no servidor, evitando acúmulo de arquivos desnecessários;
- Material de natureza pornográfica e racista não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede;
- Jogos ou qualquer tipo de software/aplicativo não pode ser gravado ou instalado no diretório pessoal do usuário, no computador local e em qualquer outro diretório da rede, podem ser utilizados apenas os softwares previamente instalados no computador autorizado pela equipe técnica;

- Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas.
- É obrigatório armazenar os arquivos inerentes à empresa no servidor de arquivos para garantir a cópia de segurança dos mesmos;
- É proibido a instalação ou remoção de softwares que não forem devidamente acompanhadas pela equipe técnica;
- Não são permitidas alterações das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro;
- Quanto à utilização de equipamentos de informática particulares, computadores, impressoras, entre outros, a empresa não fornecerá acessórios, software ou suporte técnico para computadores pessoais de particulares, incluindo assistência para recuperar perda de dados, decorrentes de falha humana, ou pelo mau funcionamento do equipamento ou do software;
- É proibida a abertura de computadores para qualquer tipo de reparo, caso seja necessário o reparo deverá ocorrer pela equipe técnica de informática;
- Quando um funcionário é transferido entre departamentos, o gerente que transferiu deve certificar-se de que todos os direitos de acesso aos sistemas e outros controles de segurança ainda serão necessários na sua nova função e informar a equipe de TI qualquer modificação necessária;
- Quando ocorrer a demissão do funcionário, o gerente responsável e o departamento de RH, devem informar a equipe técnica para providenciar a desativação dos acessos do usuário a qualquer recurso da rede. Deve-se verificar a necessidade de troca de senhas de contas de uso comum ao departamento, evitando o acesso às informações.

6. Violação da Política de Segurança

Rodovia GO 060, Km 19, 3.184,
Laguna Park • Trindade • Goiás • 75.380-000
62.3506.9300 • contato@fug.edu.br • www.fug.edu.br

Ao ser detectado uma violação à política de segurança, será feito um processo de investigação para determinar a sua razão, ou seja, a violação pode ter ocorrido por negligência, acidente ou erro, por desconhecimento da política ou por ação previamente determinada, ignorando a política estabelecida.

Um processo de investigação deve determinar as circunstâncias da violação, como e porque ela correu. Dependendo do tipo de violação e de quem a cometeu, a punição pode variar desde uma advertência verbal até um processo judicial.

Regras Gerais

- Caso seja necessário advertir o funcionário, será informado à gerência do departamento para interagir e manter-se informado da situação.
- O não cumprimento, pelo funcionário, das normas estabelecidas neste documento seja isolada ou acumulativamente, poderá causar, de acordo com a infração cometida, as seguintes punições: Comunicação de descumprimento, Advertência ou suspensão, Demissão por justa causa.
- As infrações identificadas serão reportadas ao Gerente imediato, ao Departamento de RH e a Diretoria para aplicação da punição necessária.