

UM GUIA PARA EDUCAR OS FUNCIONÁRIOS PARA MAIOR SEGURANÇA DA TI



03

Introdução

18

Colhendo frutos

06

A importância da segurança na TI

21

Conclusão

09

Educando os funcionários

23

Sobre a Digitrix



INTRODUÇÃO



Já faz algum tempo que a utilização dos recursos de tecnologia da informação deixou de ser uma escolha, se convertendo em elemento essencial para o desempenho das atividades de qualquer empresa, independentemente de seu porte ou setor. Desde o uso de planilhas eletrônicas até a implantação de sofisticados sistemas de gestão corporativa, as ferramentas tecnológicas estão por toda parte, sendo itens imprescindíveis para a sobrevivência das organizações.

Nesse contexto, em que a informação se transformou em um dos ativos mais importantes para a empresa, a segurança dos dados e do parque tecnológico passou a ser uma preocupação constante dos gestores.



Como os recursos estão à disposição de praticamente todos os funcionários, não há como realizar um controle totalmente centralizado que garanta a segurança absoluta dos dados.

“

Assim como o acesso às ferramentas é disseminado por toda a organização, também devem ser as responsabilidades com a segurança e privacidade das informações corporativas.

Mais uma vez, não importa o tamanho da empresa, é necessário investir em dispositivos que possam prover a proteção desejada. Mais que isso, entretanto, é essencial dispensar recursos para a educação dos colaboradores — em geral, o elo mais fraco da corrente quando se fala em segurança da informação.

Neste material, vamos mostrar a importância de um programa contínuo de educação dos funcionários da empresa sobre o uso da tecnologia da informação, destacando a importância do tema e apresentando sugestões para sua implantação. Por fim, vamos apresentar as vantagens que a empresa pode angariar com esses cuidados básicos, de modo que possa se dedicar plenamente ao seu negócio.



A IMPORTÂNCIA DA SEGURANÇA NA TI





Conforme já destacado, a informação se transformou em um dos bens mais importantes das organizações. Essa afirmação nada tem de retórica, mas é revestida de uma importância ímpar para as empresas de qualquer tamanho e segmento.

Não é concebível, nos dias atuais, que uma empresa ainda mantenha seus registros somente em meio "físico", com anotações em papel e sem suporte tecnológico. Por menor que seja o emprego da tecnologia e a respectiva integração dos dados, ao menos os principais documentos e planilhas devem estar armazenados em meio digital.

Com tamanha importância, é natural que as ameaças à informação também cresçam de forma exponencial.

Seja por defeito em equipamentos ou pela ação de pessoas mal-intencionadas, a verdade é que os riscos estão por toda parte. Nesse sentido, é importante que a empresa possua um programa que inclua políticas de segurança e planos de contingência que permitam prevenir e reduzir eventuais prejuízos causados por falhas de qualquer natureza.

“

Investir em segurança de TI, mais do que garantir a continuidade do negócio, amplia a reputação da organização perante o mercado, o que se traduz em retorno financeiro direto. Mas não é suficiente apenas aplicar recursos em equipamentos modernos e softwares de proteção.

Como já apontamos na introdução desse material, uma política de segurança da informação deve necessariamente envolver os funcionários da empresa, de forma a completar a proteção oferecida pelos demais recursos. Vamos entender um pouco mais sobre o assunto no próximo tópico.



EDUCANDO OS FUNCIONÁRIOS



Aqui, passamos a caminhar em um terreno mais instável. Enquanto um computador ou sistema não possui vontade própria e se limita a obedecer a programação que lhe é atribuída, um funcionário nem sempre consegue fazê-lo de forma tão precisa. Por estar sujeito a influências das mais diversas, o comportamento humano não é tão previsível quanto gostaríamos.

Grande parte dos prejuízos causados por perda ou violação de informações corporativas são originados por falha humana. A boa notícia é que, quase sempre, isso é causado por desconhecimento e não má-fé, o que pode ser facilmente solucionado com um programa de educação dos colaboradores.



Você já deve estar convencido de que a proibição de acesso aos recursos não é o melhor caminho. Ainda que seja recomendável a criação de algumas barreiras de acesso a determinados equipamentos e informações, limitar totalmente o uso do sistema pode trazer problemas para o próprio negócio. Assim, educar sobre as formas corretas de usufruir das ferramentas é a solução mais indicada.

CONSCIENTIZANDO SOBRE A IMPORTÂNCIA DA SEGURANÇA

Em um mundo ideal, seus funcionários deveriam estar naturalmente preocupados com os dados da empresa, não sendo preciso convencê-los sobre a necessidade de zelar por isso. No entanto, ainda que boa parte das pessoas “vista a camisa” da organização, há exceções que precisam ser tratadas com atenção.

Assim, uma boa ideia é mostrar aos funcionários que as recomendações não se aplicam apenas ao mundo corporativo, mas às suas próprias vidas. Como todos fazem uso de redes sociais, sites e aplicativos no cotidiano, ao perceber que as dicas de conscientização podem ajudar também nesse aspecto, é natural que passem a segui-las e criem hábitos que ajudarão nos dois ambientes — pessoal e profissional.



Uma das boas práticas nesse processo é a criação de uma “cartilha” ou manual com dicas básicas — e práticas — de segurança, que podem ser executadas imediatamente e não exigem maior investimento.

Veja algumas dicas de conteúdo para esse material ou para qualquer outra forma de divulgação que entender conveniente para sua empresa:

Usar software original e atualizado

Apesar de todos os cuidados, é quase inevitável que algum funcionário deseje instalar um aplicativo para ajudar em determinada tarefa e conclua que não vale a pena pagar pela respectiva licença. Afinal, o link está ali à mão, basta fazer o download e, em poucos minutos, ter a nova ferramenta à disposição sem qualquer investimento.

Para além das questões éticas e legais desse comportamento, vamos nos ater aos aspectos de segurança: é comum que softwares disponibilizados “de graça” tragam consigo elementos indesejáveis. Podem ser desde singelos programas que tornam o processamento mais lento até – e aqui o grande risco – espiões digitais, códigos maliciosos que roubam informações sigilosas ou “sequestram” os dados da empresa, só liberando o acesso mediante pagamento.

“

A orientação é utilizar apenas aplicações originais — que, com planejamento, podem ser adquiridas em lote e de forma mais barata junto aos fabricantes. Assim, você obtém o benefício adicional de mantê-las sempre atualizadas, pois os fornecedores investem constantemente em melhorias para combater novas ameaças e falhas de segurança.



Não clicar em links suspeitos

Essa dica tem relação direta com o item anterior e vale tanto para o download de aplicações quanto para os links de páginas de jogos e transmissões online – e até mesmo no acesso a imagens. Aqui, o risco também reside nos códigos escondidos por trás dos recursos prometidos.

Ao mesmo tempo em que proporcionam o serviço, os links instalam os espões de forma silenciosa, sem que o usuário perceba. Quando notar algo diferente no comportamento de seu computador, pode ser tarde demais.

Suspeitar de mensagens de origem desconhecida

O e-mail, enquanto uma das principais ferramentas de produtividade nas empresas, pode trazer consigo alguns inconvenientes. Não estamos falando apenas das constantes propagandas, mas especialmente das fraudes e golpes cada vez mais comuns por meio dessa ferramenta. Assim, a sugestão é que se desconfie de qualquer mensagem recebida de remetentes desconhecidos ou com promessas e ofertas tentadoras.

Embora os softwares de análise de mensagens já filtrem quase a totalidade dos e-mails fraudulentos, eles não são infalíveis e, por vezes, deixam passar algum "falso negativo", isto é, uma mensagem que deveria ter sido bloqueada, mas foi entendida como legítima. Por isso, a ação humana passa a ser essencial no complemento da proteção oferecida pela ferramenta.

Dar valor a senhas e identificações pessoais

Não é um caso incomum, especialmente entre pessoas que trabalham juntas há algum tempo: um funcionário sai de férias e deixa sua senha para que os outros possam realizar algumas atividades ou fornece a senha para que outro acesse determinada função que, em tese, não deveria estar autorizado a fazer.

É curioso verificar como as pessoas dão pouca importância às credenciais de acesso que recebem da empresa. Senhas e qualquer outro dispositivo de identificação são essenciais para garantir a segurança e devem ser tratadas com zelo e discrição. Ninguém fornece a senha de seu cartão de banco a outrem, mas muitos não têm o mesmo cuidado com os dados corporativos.



Ensine aos funcionários que as senhas garantem a identificação de quem realizou determinada tarefa e que permitem rastrear o comportamento dentro da organização. Além disso, estimule a criação de senhas fortes e sua troca periódica, de modo a aumentar a proteção oferecida.

Não compartilhar informações demasiadas nas redes sociais

Essa sugestão vale tanto para a vida pessoal quanto profissional dos funcionários. As redes sociais, não obstante sejam uma ferramenta absolutamente fantástica de comunicação e integração, não possuem recursos muito eficientes para identificação de seus usuários. Assim, é fácil que pessoas mal-intencionadas se escondam atrás de perfis falsos ou, o que pode ser ainda pior, que naveguem silenciosamente em busca de informações de seu interesse.

Nesse sentido, é recomendável usar os recursos de privacidade oferecidos pelas redes sociais, limitando o acesso apenas a perfis de pessoas conhecidas, assim como reduzir a quantidade e qualidade das informações disponibilizadas. Isso vale tanto para dados sobre família/filhos e hábitos pessoais, como para informações da empresa.

Ter atenção aos dispositivos móveis

De simples dispositivos de comunicação pessoal, os smartphones passaram a ter importância também no campo profissional. Relatórios, informações sobre produtos, aplicativos diversos — tudo está bem ali, ao alcance da mão. E, ao mesmo tempo em que a mobilidade traz consigo a vantagem de possibilitar o acesso a tudo de qualquer lugar, desperta a necessidade de dispensar um cuidado maior com a segurança.



A dica é proteger os dispositivos com senhas e usar aplicativos para sua localização em caso de perda, além de, naturalmente, mantê-los consigo sempre que possível.

Realizar cópias de segurança

Seja por comodidade ou falta de conhecimento, os funcionários costumam trabalhar em arquivos localizados apenas em seus próprios computadores, quando a estrutura de rede da empresa assim permite.

Com isso, novas informações vão sendo acrescentadas ou atualizadas e permanecem ali, apenas em um equipamento. Em caso de falha nesse dispositivo, os transtornos podem ser muito grandes.



Além do backup corporativo, que já deve ser feito rotineiramente, crie discos departamentais para que os funcionários façam cópias dos arquivos em que estão trabalhando, caso seja mesmo inevitável que o façam apenas em seus computadores. Por fim, incentive essa prática, explicando as vantagens de possuir cópias de segurança dos dados.

Contar com o suporte técnico

Por menor que seja a empresa, sempre existe pelo menos uma pessoa responsável por fornecer suporte às atividades de TI. Se não for um funcionário efetivo, será uma empresa contratada. Incentive seus colaboradores a confiar e contar com o apoio dessas pessoas. Em caso de qualquer dúvida sobre a utilização dos recursos, é sempre preferível acionar o pessoal especializado do que correr riscos desnecessários.

Claro, instrua também o responsável pelo atendimento a agir de maneira didática, orientando e educando os funcionários sobre o uso dos recursos. Esse comportamento vai aumentar a segurança da empresa e, ao mesmo tempo, reduzir a necessidade de intervenção por parte do suporte.



COLHENDO FRUTOS





Até aqui, mostramos a importância de educar os funcionários da empresa sobre o bom uso dos recursos e os cuidados com a segurança da informação. Mas quais os benefícios que esse procedimento pode gerar para a empresa?

Em primeiro lugar, vamos falar da confiabilidade das informações armazenadas. Cuidados básicos como os descritos permitem que os dados corporativos estejam sempre disponíveis e consistentes, o que garante que os negócios sejam realizados com base em dados atualizados e corretos. Com o tempo, os próprios funcionários passam a confiar mais nas informações fornecidas pelos sistemas e, por consequência, a realizar suas atividades de maneira mais rápida e eficiente.

Outra vantagem diz respeito à garantia de continuidade do negócio. Com a implantação de políticas de segurança é natural que o risco de perda de dados seja praticamente eliminado, assim como a necessidade de intervenção ou parada do negócio para correção de problemas e recuperação de informações.

Por fim, todas as vantagens auferidas se traduzem basicamente em melhoria na reputação da empresa. A imagem de uma organização confiável e consistente reflete em vantagem competitiva perante um mercado cada vez mais acirrado e exigente em relação a padrões e políticas de segurança. Afinal, os clientes preferem que suas informações estejam sob a guarda de empresas que as valorizam e as tratam com a devida importância.





CONCLUSÃO



Nesse material, procuramos mostrar a importância da segurança da informação e da educação dos funcionários da empresa sobre o tema. Ainda que a instituição possa – e deva – investir em recursos automatizados que reduzam os riscos, como firewall e antivírus, deve estar ciente que isso não é suficiente. É essencial, cada vez mais, despendar esforços no treinamento e na educação de seu corpo de colaboradores.

Ainda assim, tenha em mente que não basta ensinar uma única vez, de forma isolada. A educação para o uso dos recursos de TI precisa ser um programa contínuo, assim como é a evolução dos dispositivos e equipamentos.

Agindo de forma proativa e frequente, a utilização correta da tecnologia passa a ser um hábito incorporado pela organização, o que traz consequências positivas tanto para o ambiente corporativo quanto para a vida pessoal de seus funcionários.





A **DIGITRIX** é uma empresa especializada em Serviços e Soluções de TI. Desde 2003 ajudamos empresários e gestores a vencer seus desafios através da Tecnologia da Informação.

Nossa missão: Implantar e Gerenciar Serviços de TI que possibilitem as empresas a serem mais produtivas, seguras e estratégicas em seus negócios.

Somos especialistas em serviços gerenciados de TI. Nosso objetivo é fornecer suporte estratégico para o seu negócio.

www.digitrix.com.br