*Clube Naval*

# BOAS PRÁTICAS

# SEGURANÇA INFORMAÇÃO

## SUMÁRIO

## I. INTRODUÇÃO

Fazer uma boa gestão de segurança de redes não implica em altos custos, como muitos pensam. Algumas práticas são fundamentais e simples para evitar perdas financeiras e de dados, bem como manter uma boa reputação da marca frente ao mercado.

Portanto, ao pensar que o investimento em tecnologia é caro, imagine o alto preço que a empresa pode pagar se for negligente e não cuidar de seu maior ativo — a informação.

Para implementar boas práticas de segurança da informação em uma empresa, primeiro é importante definir uma estrutura de gestão de forma adequada. Para isso, essas atividades são coordenadas por representantes da organização, que possuem responsabilidades bem definidas e pratiquem algumas ações fundamentais como será apresentado nessa cartilha.

## II. OBJETIVO

A informação é um ativo muito relevante para qualquer tipo de empresa, sendo considerada, nos dias de hoje, um dos recursos patrimoniais mais importantes para a manutenção do negócio. Informações confidenciais em posse de concorrentes ou pessoas de má-fé podem prejudicar seriamente, não apenas a reputação e imagem da empresa, mas também inviabilizar processos operacionais cotidianos.

A continuidade de um negócio pode ser agravada se segurança das suas informações não receber a devida atenção. Nesse sentido entra em destaque o conceito de segurança da informação que se trata da proteção de sistemas e dados da empresa, sendo o nível de segurança definido conforme o valor das informações e os possíveis prejuízos originados pelo seu uso indevido.

Para isso, a segurança da informação implementa mecanismos, ferramentas e boas práticas que buscam proteger a empresa de diversas falhas.

## III. EXEMPLOS DE BOAS PRÁTICAS DA SEGURANÇA DA INFORMAÇÃO

Para nós, a segurança da informação já é um cuidado muito presente em todos os processos e atividades, por isso preparamos esta cartilha com as seguintes sugestões:

### MANTENHA OS SOFTWARES ATUALIZADOS

Mantenha os sistemas operacionais originais e atualizados, os fabricantes estão sempre em busca de correções e atualizações contra ataques cibernéticos.

As atualizações de software são importantes porque a maioria dos malwares por aí não tem exatamente como alvo vulnerabilidades de segurança novas e desconhecidas. Em vez disso, exploram aplicações conhecidas que já foram

corrigidas nas versões mais recentes, na esperança de que as empresas não tenham sido atualizadas.

## TENHA CONTROLE SOBRE OS ACESSOS

Comece por registrar todos os níveis e controles de acesso atuais em vigor. Após, verifique as funções das pessoas na empresa para definir o acesso a uma funcionalidade específica.

Deve ser assegurado o acesso de usuário autorizado aos locais estritamente necessários ao desenvolvimento de suas tarefas.

Isso pode reduzir os riscos associados a senhas roubadas, já que um hacker mal-intencionado tem menos chances de obter acesso a tudo.

## FAÇA CÓPIAS DE SEGURANÇA

O backup ou cópia de segurança é um mecanismo fundamental para assegurar a disponibilidade da informação, caso as bases de dados em que a informação esteja armazenada sejam roubadas ou danificadas.

Uma das etapas mais importantes do backup é descobrir com que frequência os dados precisam ser armazenados em backup. Idealmente, as empresas devem fazer o backup dos dados com a frequência que seus recursos permitirem.
Embora muitas empresas possam se contentar com um backup diário, as que lidam com dados em constante mudança, como

organizações financeiras, devem fazer backup com uma frequência ainda maior, várias vezes ao dia.

As empresas podem pesquisar softwares que fazem backup de dados automaticamente em intervalos selecionados para facilitar o gerenciamento do processo.

## INVISTA EM SERVIÇOS E EQUIPAMENTOS VOLTADOS À SEGURANÇA

Grande parte da proteção de dados em uma empresa está na capacidade de sua infraestrutura tecnológica.

Investir em uma solução de segurança que não apenas detectem o software desatualizado em execução nos dispositivos de propriedade do usuário, mas também notifica que ele pode economizar tempo dos administradores, permitindo que os usuários resolvam rapidamente seus próprios dispositivos vulneráveis.

## CRIE UMA CULTURA DE SEGURANÇA DA INFORMAÇÃO

Os programas de treinamento de segurança mais bem-sucedidos não têm apenas a participação dos funcionários operacionais, mas sim de todos os níveis da organização.

Isso ocorre simplesmente porque uma abordagem total é a melhor maneira de construir uma cultura de segurança em toda a empresa na qual a boa tomada de decisões e a aplicação das melhores práticas de segurança da informação se tornem atividades diárias.

Hoje, a principal brecha na segurança das empresas é o fator humano. É por isso que os principais ataques focam engenharia social para induzir comportamentos que fujam das boas práticas.

As táticas de engenharia social estão baseadas essencialmente na confiança. Tudo o que um criminoso precisa para começar é um pouco de informação que pode ser de conhecimento público ou que a vítima pode inocentemente compartilhar em sua rede social. Um criminoso pode precisar de nada mais do que uma postagem do Facebook identificando sua localização e membros da família ou uma senha fraca.

A engenharia social acontece quando as pessoas confiam demais ou quando não pensam nas consequências de serem descuidadas com as informações. Existem infinitas maneiras de um ladrão de identidade usar a engenharia social para roubar suas informações pessoais, seja por telefone, mensagem, SMS ou e-mail.

Os hackers, nesse caso, exploram a única fraqueza encontrada em toda e qualquer organização: a psicologia humana. Usando uma variedade de mídias, incluindo chamadas telefônicas e mídias sociais, esses invasores induzem as pessoas a oferecerem informações confidenciais.

Portanto, mesmo com as mais avançadas tecnologias, existe o risco de um funcionário ser enganado e passar os dados da empresa via engenharia social e, assim, perder

informações importantes para o mercado, como dados de clientes.

Assim, para evitar o roubo de dados por meio da engenharia social em sua empresa:

- Eduque os funcionários. Se as pessoas não são educadas para os tipos de ataques que estão sendo usados, então elas não podem se defender contra eles;

- Esteja ciente das informações que estão sendo transmitidas;

- Defina quais dos seus ativos são mais valiosos para proteger;

- Faça um bom treinamento de conscientização;

- Quando for solicitada alguma informação, busque compreender se a pessoa com quem você está falando precisa realmente da informação solicitada;

- Preste atenção às perguntas que não se encaixam no contexto.

## IV. EXEMPLOS DE POLÍTICAS E RECOMENDAÇÕES

Sabemos que cada empresa possui seus processos e sai especificidade, razão pela qual deve ser criada uma

política que se adeque ao seu dia a dia e que seja possível de se implementar e fácil de ser seguida por seus empregados, os quais são as principais figuras, conforme falado acima.

Assim, podemos mencionar algumas atitudes simples que podem ser adotadas por todas as empresas que já começam a criar a cultura da segurança da informação:

## PREVENÇÕES NA INTERNET

- Navegue conscientemente na Web;

- Evite sites que pareça, suspeitos e não clique em links de janelas Pop-ups;

- Utilize sites seguros ao enviar dados confidenciais;

## SENHAS DE ACESSO

- Utilize senhas fortes em qualquer tipo de cadastro, incluindo números, letras maiúsculas e minúsculas e caracteres especiais;

- Evite repetir a mesma senha para diferentes cadastros ou anotá-las em papel/caderno;

- Evite utilizar nomes próprios, sobrenomes, datas de nascimento, parte do CPF, nomes dos filhos, pais, parentes, ou de animais de estimação ou qualquer informação que pode ser obtida publicamente;

- Altere as senhas regularmente;

- Siga corretamente as políticas de senha da plataforma ou da sua instituição;

- Jamais salve senhas em computadores públicos ou de terceiros;

- Não forneça sua senha para outra pessoa;

## E-MAILS

- Nunca use seu e-mail corporativo para tratar assuntos pessoais;

- Da mesma forma nunca use seu e-mail particular para tratar assuntos profissionais;

- Não realize cadastros utilizando o seu e-mail corporativo em sites de compras, redes sociais, entre outros que não tenham qualquer relacionamento com as atividades da empresa;

- Não clique em links suspeitos recebidos por e-mail, na dúvida, sempre procure o TI;

- Não execute arquivos anexados aos e-mails sem antes examiná-los;

- Desconfie sempre que receber um e-mail de caráter duvidoso oferecendo vantagem ou dinheiro rápido, promoções, alterações de senha de banco, fotos, cobranças, boletos bancários etc.

- Verifique se o remetente é realmente quem ele diz ser, de maneira simples, passe o mouse no cabeçalho do e-mail e veja se o e-mail condiz com o usuário.

## COMPUTADORES CORPORATIVOS

- Evite ao máximo baixar arquivos pessoais, tais como fotos, dentro do computador corporativo;

- Nunca baixe programas sem autorização do departamento de TI.

- Bloqueie a tela da sua estação de trabalho sempre que for se ausentar da mesa, mesmo que por um curto período;

- Caso seja necessário o acesso da rede privada da empresa, que seja feito utilizando-se equipamento fornecido e chancelado pela empresa para essa finalidade.

## DISPOSITIVOS EXTERNOS E PORTAS USB (PEN DRIVES E HDS EXTERNOS)

- Evite utilizar tais dispositivos.

- Evite conectar qualquer dispositivo ou componente estranho a estação de trabalho, tal como celular;

- Informe imediatamente ao TI caso identifique dispositivo estranho conectado ao seu computador;

- Caso necessário solicite ao TI autorização para o seu uso tempo limitado para execução do trabalho.

### CELULARES CORPORATIVOS

- Utilize senhas para desbloquear a tela do celular corporativo;

- Não bloqueie o acesso remoto do TI da empresa;

- Comunique imediatamente ao TI caso o dispositivo móvel seja perdido, furtado ou roubado;

## V. POLÍTICA DA MESA LIMPA

A segurança da informação não é única e exclusivamente direcionada aos arquivos eletrônicos ou ambientes virtuais, todo tipo de informação e dado deve ter igual atenção, inclusive as informações em meio físico.

Muitas empresas adotam a política de mesa limpa, prática recomendada para o local de trabalho a fim de se evitar a exposição desnecessária de informações/dados.

Para se reduzir os riscos de acesso não autorizado, perda ou danos às informações/dados durante e fora do horário de expediente é recomendado que nenhuma informação/dado seja deixada à vista, visto que informações deixadas sobre as mesas de trabalhos ou *scanners* são passíveis de serem danificas, destruídas ou furtadas.

Assim, a fim de se reduzir o risco de violação de segurança, fraudes e roubo de informações/dados causados por documentos deixados ou guardados de forma inadequada no ambiente de trabalho ou até mesmo no sistema de *home office* recomenda-se:

- Evite documentos em papeis sobre a mesa de maneira desnecessárias, devendo ser armazenados em armários ou gavetas trancaras quando não estiverem em uso, especialmente fora do horário do expediente;

- Evite deixar anotações, recados e lembretes amostra sobre a mesa ou colados em paredes, divisórias ou monitor do computador;

- Evite anotar informações/dados sensíveis em quadros a vista;

- Destrua os documentes impressos antes de jogá-los fora, sempre que possível utilize máquinas desfragmentadoras;

- Evite imprimir documentos apenas para lê-los;

- Retire a impressão de forma imediata de informações/dados sensíveis e/ou confidenciais impressos em local coletivo;

- Guarde agendas e cadernos de anotações em uma gaveta trancada;

- Mantenha seus pertences pessoais em gavetas ou armários trancados;

- Nunca deixei seu crachá de identificação ou chaves em qualquer lugar, mantenha-os junto a você;

- Limpe a mesa de trabalho, guarde os documentos, tranque as gavetas e armários ao final do expediente, ou em caso de ausência prolongada;

- Não deixe as chaves de gavetas e armários na fechadura;