Alguns bons tutoriais sobre Segurança da informação, frutos de uma pesquisa com as respectivas referências.

Segurança da informação: conheça as 12 melhores práticas

Postado por **Positivo Tecnologia**em **Comentários**

Author

Segurança da informação é um tema estratégico da gestão de negócios que nunca pode ser deixado de lado. Seus desvios interferem no bom andamento das atividades rotineiras, no alcance dos resultados planejados e na sobrevivência e reputação de uma empresa.

Percebeu a grande importância deste artigo para alavancar a sua carreira em segurança da informação ou incluir ferramentas dessa área para proteger o seu negócio? Apesar de tão essencial, as diversas facetas deste tema são desconhecidas por grande parte dos gestores, que ficam focados em outros setores empresariais.

Quer saber mais sobre o universo da segurança da informação? Então, continue a leitura e confira!

Quais são os princípios da segurança da informação?

Para entender o que representa a segurança da informação, é necessário conhecer os seus princípios básicos e suas principais características. Confira:

Confidencialidade

A informação só pode ser acessada e atualizada por pessoas autorizadas e devidamente credenciadas. Dados e informações importantes de alguns setores ou clientes jamais podem ser acessados por terceiros estranhos à corporação.

Devem haver mecanismos de segurança de tecnologia da informação (TI) capazes de impedir que pessoas não autorizadas acessem informações confidenciais, seja por engano ou por má-fé.

Confiabilidade

É o caráter de fidedignidade da informação. Deve ser assegurada ao usuário a boa qualidade da informação com a qual ele estará trabalhando.

Integridade

É a garantia de que a informação estará completa, exata e preservada contra alterações indevidas, fraudes ou até mesmo contra a sua destruição.

Assim, são evitadas violações da informação, sejam elas de forma acidental ou mesmo proposital.

Disponibilidade

É a certeza de que a informação estará acessível e disponível em escala contínua para as pessoas autorizadas.

Hoje em dia, os mecanismos de acesso remoto tornam possível a disponibilidade da informação de qualquer lugar em que o usuário esteja no planeta e a qualquer hora do dia ou da noite.

Autenticidade

É saber, por meio de registro apropriado, quem realizou acessos, atualizações e exclusões de informações, de modo que haja confirmação da sua autoria e originalidade.

Como vimos, todos os aspectos da segurança da informação precisam estar em vista e serem tratados com o máximo de critério e cuidado para que os gestores e colaboradores da empresa sejam beneficiados, assim como os públicos externos — parceiros e clientes — que interagem com ela.

Qual a importância da segurança da informação para as empresas?

Todos os dados das empresas, que vão desde informações a respeito dos produtos ou serviços oferecidos, nomes e números de documentos particulares de funcionários e gestores, faturamento, contabilidade, entre outros, estão disponíveis nos sistemas utilizados.

Como são muitas informações, inúmeros empreendedores já estão salvando esses relatórios na nuvem. Assim, as informações passam a ser armazenadas na internet e, caso a empresa não tenha uma boa segurança, é possível que ela sofra ataques cibernéticos.

Uma simples falha pode causar um enorme estrago, que vai desde a exposição dos valores financeiros movimentados durante um período, até a perda de clientes — já que seus nomes e contatos estarão na base de dados e os hackers podem usá-los para beneficiar a concorrência.

Todas as informações são consideradas patrimônio do negócio. Nesse sentido, é de extrema importância que sejam preservadas e mantidas fora do alcance de pessoas que não façam parte da corporação, para evitar prejuízos e, inclusive, danos à imagem da sua empresa.

Qual a diferença entre segurança da informação e segurança de TI?

Embora os profissionais da área estejam habituados em trabalhar com segurança de dados, muitos ainda se confundem com os termos segurança da informação e segurança de TI.

Apesar da confusão que pode ocorrer por causa da semelhança dos termos, que são diferenciados apenas pela inclusão da palavra “tecnologia” no segundo caso, as duas técnicas são distintas e não devem ser tratadas como sinônimos.

Vamos apontar as diferenças a seguir, acompanhe a leitura!

Segurança de TI

A segurança de Tecnologia da Informação é usada para manter a segurança dos sistemas operacionais, tais como:

- banco de dados;
- computadores;
- provedores;
- servidores.

Ela apresenta papel estratégico nas empresas, pois é com o uso dessa técnica que toda a estrutura da tecnologia do empreendimento estará protegida.

Segurança da Informação

Já a segurança da informação fica responsável por proteger os dados corporativos de ameaças. Veja abaixo alguns de seus objetivos:

- defesa contra ataques de hackers aos sistemas da corporação;
- proteção das informações da empresa disponíveis na internet;

- prevenção do acesso de indivíduos não autorizados a acessar dados sigilosos.

Ainda tem alguma dúvida com relação aos dois termos que são referentes à segurança corporativa? Saiba que fazer a diferenciação é muito simples, pois, basta você pensar que a segurança de TI é especializada na área de computadores e máquinas do empreendimento, enquanto a segurança da informação protege a parte de software e da rede corporativa.

Quais são as qualificações necessárias para utilizar a segurança da informação?

Os profissionais da área da segurança da informação precisam ser qualificados para realizarem as tarefas necessárias. As principais certificações são:

- **CEH — Certified Ethical Hacker:** traduzido para o português, é "hacker ético certificado", cuja especialização serve para avaliar a segurança de sistema de computadores;
- **CHFI — Computer Hacking Forensic Investigation:** a certificação serve para ensinar os profissionais a detectarem os crimes virtuais;
- **CISSP — Certified Information System Security Professional:** nada mais é do que uma certificação na qual são abordadas práticas para controlar acessos;
- **CCISO — Certified Chief Information Security Officer:** é um programa que capacita os profissionais nos mais altos níveis de segurança da informação.

A profissão é nova e é muito difícil encontrar profissionais qualificados na área, por isso é importante realizar um processo seletivo específico para esse ramo.

Quais são os deveres e responsabilidades dos profissionais da área?

Os analistas que desejam ter uma boa carreira em segurança da informação têm como principais atividades encontrar vulnerabilidades nos servidores, aplicações e networking — bem como criar políticas de

proteção com o uso de processos. Dessa forma será possível manter a integridade dos dados do negócio.

Como começar a usar a técnica?

Um dos primeiros passos a ser aplicado no uso da técnica é estudar e efetuar boas práticas de desenvolvimento de sistemas de segurança de informação.

Outro ponto importante é pesquisar quais são as técnicas mais usadas para invadir os sistemas, tais como:

- SQLInjection;
- Brute force;
- DoS;
- DDoS.

O que também pode ser realizado para diminuir os danos causados por um ataque é o ato de realizar backups de tempos em tempos, o que deixará os profissionais da área mais tranquilos.

Sem contar que devem ser traçados planos de recuperação. Assim, com a ajuda da tecnologia da informação será possível recuperar dados que foram acessados pelos invasores.

Os backups de sistema também são uma ótima saída para manter os dados guardados e não perder as informações necessárias para a empresa.

É aconselhável a realização de backups semanais, e, além disso, que sejam mantidas cópias de segurança de todos os arquivos indispensáveis em outros locais. Para a proteção dos dados, os gestores devem considerar mais de um ou dois meios de garantir a acessibilidade das informações.

Como a cada dia que passa os invasores cibernéticos desenvolvem mais técnicas de atacar os sistemas, torna-se imprescindível que os analistas estejam sempre se atualizando.

Aliás, os profissionais que não buscam qualificação em breve estarão enfrentando entraves na realização das suas tarefas. Esse é o preço das inovações tecnológicas, que trouxeram inúmeros benefícios em todas as áreas do conhecimento, mas exigem capacitação constante.

Como funciona a capacitação desses profissionais?

A capacitação é adquirida por meio de cursos de boas práticas de segurança da informação e outros cursos sobre a ISO 27001 e 27002.

Devido à complexidade das áreas relacionadas à segurança da informação, é importante participar de palestras relacionadas à marca e lógica de firewall.

Outros assuntos das capacitações abordam as configurações de NAT (Network Address Translation), VPN (Virtual Private Network) e perfis de navegação, por exemplo.

Os treinamentos podem ser encontrados com facilidade na internet e já existem opções de cursos ministrados de maneira presencial, o que é muito interessante e útil. Na verdade, oportunidade para aperfeiçoamento profissional é o que não falta em nossos dias.

Basta fazer uma busca para localizar as mais variadas ofertas de cursos e treinamentos presenciais e a distância, com valores inexpressivos e muita informação colocada à disposição daqueles que desejam se aprimorar. No entanto, é preciso avaliar os conteúdos programáticos antes de efetivar uma inscrição.

Quais são as melhores práticas de segurança da informação?

As práticas de segurança vão do básico ao sofisticado, dependendo do mecanismo escolhido pelo gestor de TI. Algumas são tradicionais e conhecidas pela maioria das pessoas e outras, somente pelos especialistas da área.

Contudo, não há motivo para se preocupar. Neste post você terá acesso às 12 melhores práticas de segurança da informação, descritas de forma simples e objetiva. Vamos a elas!

1. Detectar vulnerabilidades de hardware e software

Os equipamentos de TI — hardwares — e os sistemas e aplicativos — softwares — passam por evolução tecnológica contínua e precisam ser substituídos periodicamente. E a sua aquisição tem que levar em conta os aspectos técnicos e de qualidade, não podendo se nortear apenas pelo quesito preço.

A defasagem tecnológica torna vulnerável toda a infraestrutura e a segurança de TI e gera consequências tais como:

- perda de competitividade;
- ineficiência operacional;
- insatisfação de colaboradores e clientes;
- morosidade e ineficácia do processo decisório.

Os equipamentos estão sujeitos a defeitos de fabricação, instalação ou utilização incorreta, quebra ou queima de componentes e má conservação, o que pode comprometer um ou mais dos princípios da segurança da informação.

Os softwares estão sujeitos a falhas técnicas e de configurações de segurança, mau uso ou negligência na guarda de login e senha de acesso.

Devem ser adotadas práticas de segurança específicas para cada elemento componente da infraestrutura de TI:

- servidores;
- computadores;
- rede;
- softwares;
- componentes de comunicação, dentre outros.

Também é fundamental providenciar treinamento e atualização de conhecimentos para a equipe de TI e os usuários dos recursos tecnológicos. Afinal, inabilidade técnica também gera vulnerabilidades de hardware e software.

É imprescindível detectar de forma rápida as possíveis vulnerabilidades de hardware e software, para tomar providências imediatas no sentido da sua solução.

2. Cópias de segurança

O tão conhecido backup — ou cópia de segurança — é um mecanismo fundamental para garantir a disponibilidade da informação, caso as bases onde a informação esteja armazenada sejam danificadas ou roubadas.

O backup pode ser armazenado em dispositivos físicos — servidores de backup, CD, pendrive, HD externo — ou em nuvem.

O mais importante é que haja pelo menos duas cópias das bases de dados, armazenadas em locais distintos da instalação original, ou seja, ambas guardadas em locais seguros fora do prédio da sua empresa.

A partir do backup é possível recuperar, em curtíssimo espaço de tempo, informações perdidas acidentalmente ou em consequência de sinistros (enchentes, incêndio etc.), sabotagens ou roubos.

Vale destacar que as empresas que funcionavam no World Trade Center na ocasião do fatídico atentado de 11 de setembro de 2001 tinham boas práticas de manutenção de backup. Todas sobreviveram a essa terrível catástrofe, voltando a funcionar normalmente em poucos dias.

3. Redundância de sistemas

A alta disponibilidade das informações é garantida com a redundância de sistemas, ou seja, quando a empresa dispõe de infraestrutura replicada — física ou virtualizada.

Se um servidor ou outro equipamento de TI (roteador, nobreak etc.) falhar, o seu substituto entra em operação imediatamente, permitindo a continuidade das operações, às vezes, de forma imperceptível para o usuário.

4. Eficácia no controle de acesso

Existem mecanismos físicos, lógicos ou uma combinação destes de controle de acesso à informação. Os mecanismos físicos podem ser uma sala de infraestrutura de TI com acesso restrito e com sistemas de câmeras de monitoramento.

Outra forma de restrição de acesso é o uso de travas especiais nas portas, acionadas por senha (misto físico/lógico). Já os principais mecanismos lógicos são, por exemplo, os seguintes.

4.1. Firewall

É um mecanismo de controle do tráfego de dados entre os computadores de uma rede interna e destes com outras redes externas.

Ele trabalha segundo protocolos de segurança (TCP/IP, IPSec, HTTP etc.) que garantem o correto funcionamento da comunicação entre as duas pontas, visando impedir intrusões.

4.2. Assinatura digital

É uma forma de identificação do usuário que está acessando aos recursos de TI, ela dá validade legal aos documentos digitais, assegurando a autenticidade do emissor da informação.

4.3. Biometria

O acesso às informações somente é liberado para a pessoa autorizada, levando em consideração as suas características físicas (impressão digital, voz ou padrões da íris do olho ou do rosto inteiro.).

Outra faceta importantíssima do controle de acesso é o uso de equipamentos próprios dos colaboradores para operação de sistemas e aplicativos empresariais de forma remota.

Como a empresa não tem controle sobre as configurações de segurança dos dispositivos particulares dos colaboradores, ela tem que reforçar os mecanismos de validação da autenticidade do usuário e as barreiras contra ataques cibernéticos.

5. Política de segurança da informação

É um documento que estabelece diretrizes comportamentais para os membros da organização, no que tange às regras de uso dos recursos de tecnologia da informação.

Essas regras servem para impedir invasões de cibercriminosos, que podem resultar em fraudes ou vazamento de informações, evitar a entrada de vírus na rede ou o sequestro de dados e garantir a confidencialidade, confiabilidade, integridade, autenticidade e disponibilidade das informações.

Idealmente, essa política deve ser desenvolvida de forma participativa entre a equipe de TI e os colaboradores dos demais departamentos, sendo aprovada pela alta direção da empresa. Assim, de comum acordo, fica muito mais fácil gerir a segurança da informação.

Vale pontuar que é indispensável que o texto da política seja curto e objetivo, para facilitar e estimular a leitura e tornar o processo de divulgação e treinamento das pessoas mais leve e eficaz.

6. Decisão pela estrutura de nuvem pública/privada/híbrida

Uma das formas mais avançadas de garantir a segurança da informação é a decisão pela utilização de uma estrutura de computação em nuvem. Essa estrutura tem três categorias distintas: nuvem pública, privada ou híbrida.

Na nuvem pública toda a infraestrutura de TI, a sua manutenção, os seus mecanismos de segurança e a atualização são de responsabilidade do provedor do serviço. A sua instalação é rápida e os seus recursos são escalonáveis, de acordo com o perfil de demanda da empresa contratante.

A nuvem privada é de propriedade da empresa e fica instalada em sua área física, requerendo infraestrutura de hardware, software, segurança e pessoal próprios para o seu gerenciamento.

Já a nuvem híbrida combina o melhor dos dois tipos anteriores, com isso, parte dos dados são disponibilizados na nuvem privada — aqueles que

exigem sigilo — e outra parte fica na nuvem pública — dados não confidenciais.

Todos os três tipos de serviço de computação em nuvem respeitam altos padrões de segurança da informação, basta avaliar qual é o mais adequado para as necessidades e expectativas da sua organização.

O advento da computação em nuvem viabilizou serviços como:

- IaaS — Infraestrutura como Serviço;
- PaaS — Plataforma como Serviço;
- SaaS — Software como serviço.

Essas novas modalidades permitem terceirizar importantes serviços de tecnologia da informação, reduzindo custos, assegurando agilidade e atualização permanente e elevando o patamar de segurança de hardware e software.

7. Gestão de riscos apropriada

Os principais riscos à segurança da informação estão relacionados com alguns aspectos. Adiante estão destacados os principais!

7.1. Falta de orientação

Não saber como operar equipamentos, sistemas e aplicativos, enfim, os recursos de TI, coloca em risco a segurança da informação. E o desconhecimento de técnicas de proteção, também.

Por isso, proporcionar treinamentos nas novas tecnologias e/ou recursos de TI aos usuários comuns e à equipe de informática é uma boa prática que tem o seu lugar.

Dependendo do porte da empresa — média ou grande —, vale a pena desenvolver profissionais C-Level em TI, que possam ampliar os horizontes tecnológicos da empresa, tornando a área de TI alinhada à estratégia empresarial.

Com a ajuda desses especialistas, os recursos tecnológicos serão aplicados para alavancar a produtividade das equipes e facilitar o

alcance das metas estabelecidas, sem perder de vista o aprimoramento contínuo da sistemática de segurança da informação.

7.2. Erros de procedimentos internos

Procedimentos de gestão da segurança da informação mal estruturados ou desatualizados podem acarretar vulnerabilidades e perdas de dados.

Essas vulnerabilidades podem se manifestar nos hardwares, softwares ou nas pessoas despreparadas para fazer frente às ameaças que se renovam a cada dia.

7.3. Negligência

Deixar de cumprir com as regras da política de segurança da informação ou com os procedimentos internos de TI, por mera negligência, pode custar caro — prejuízos financeiros, de imagem ou materiais.

Campanhas de conscientização dos colaboradores são fundamentais, para redobrar os cuidados e estarem sempre alertas a ciladas cibernéticas, especialmente em e-mails, sites e arquivos maliciosos, que provocam a propagação de vírus, malwares, trojans e outros na rede de informática.

7.4. Malícia

As ações mal-intencionadas de colaboradores internos insatisfeitos e de pessoas externas tornam instável a segurança da informação, especialmente, se não houver mecanismos de detecção de intrusões.

Conhecer as principais fontes de riscos é o ponto de partida para mapear os diversos cenários que podem configurar ameaças à segurança da informação e tornar possível o desenvolvimento de boas práticas de gestão de riscos.

8. Regras de negócio bem definidas

As informações críticas devem ser identificadas e as regras de negócio referentes ao acesso, manutenção — inclusão, alteração, exclusão — e tempo de guarda devem ser estabelecidas de forma criteriosa, para garantir total segurança.

As regras de negócios são indispensáveis para a configuração de permissões de acesso em softwares, hardwares e redes lógicas.

Essas regras precisam ser melhoradas continuamente, agregando novos mecanismos físicos e lógicos e práticas comportamentais atualizadas que contribuam para minimizar os riscos à segurança da informação.

9. Cultura da organização

A terceira plataforma de TI combinou tecnologias sociais, computação em nuvem, dispositivos móveis — smartphones, tablets — e tecnologias de análise de dados — business intelligence e Big Data — para promover a conectividade permanente, romper as fronteiras da mobilidade e gerar informação em tempo real sobre o comportamento dos consumidores.

Esse movimento fez com que as metodologias de gestão da segurança da informação ganhassem uma nova dinâmica de readequação e realinhamento constantes. Assim, é possível bloquear as novas rotas de ataques cibernéticos às bases de dados das empresas, proporcionadas pelas novas tecnologias.

Tudo isso impacta diretamente na cultura organizacional, que precisa se adequar a essa transformação digital, modernizando os seus processos internos, sem descuidar da segurança.

Para tanto, velhos conceitos, práticas e formas de pensar e trabalhar precisam ser revistas e até reinventadas, para que todos estejam cientes dos riscos e sobre como proteger as informações empresariais.

10. Contratos de confidencialidade

Os colaboradores internos de uma organização e os terceirizados, especialmente aqueles vinculados à área de TI, no exercício de suas atividades, muitas vezes, têm acesso a informações sigilosas, que precisam ser resguardadas.

A melhor forma de preservar a segurança da informação, nesses casos, é fazer um contrato de confidencialidade com todas as pessoas que conhecem e acessam informações sigilosas.

É importante que esse contrato de confidencialidade seja redigido considerando os requisitos legais aplicáveis à organização e eventuais acordos desse gênero pactuados com clientes, fornecedores, prestadores de serviços e parceiros de negócios.

11. Gestão de Continuidade de Negócios (GCN)

As informações de um negócio são essenciais para garantir a sua continuidade, pois se compõem de dados dos clientes, produtos, parceiros comerciais, transações financeiras e comerciais e demais assuntos pertinentes ao funcionamento de uma empresa. Logo, a sua perda pode tornar inviável o negócio.

A Gestão de Continuidade de Negócios (GCN) é uma prática que visa estabelecer planos de ação de emergência para resposta rápida a eventos adversos (desastres naturais, explosões, incêndios, fraudes financeiras, atentados, sabotagens, falhas nos sistemas informatizados ou nos equipamentos etc.).

Os planos de ação traçados pela GCN devem permitir minimizar ou evitar os impactos negativos que possam ser causados, tais como paralisações na produção e/ou prestação de serviços, perdas financeiras e danos à imagem ou credibilidade do negócio.

A GCN é uma ferramenta de ação preventiva, que deve priorizar a tomada de ações para eliminar os cenários de riscos passíveis de extinção, mediante a adoção de mudanças em processos, produtos ou serviços de TI. Pequenas mudanças podem resultar em saltos quânticos na segurança da informação.

12. Benchmarking

O benchmarking é um importante instrumento de gestão, que parte do princípio de comparação de produtos, serviços, processos e práticas empresariais próprios de uma organização com os de terceiros — concorrentes ou não.

Isso mesmo, muitos insights fantásticos surgem da análise de situações das empresas de ramos diferentes de atividade e que podem ser

replicadas — casos de sucesso — ou evitadas — casos de insucesso — com as devidas adaptações.

Há quem pense que o benchmarking foca somente nas situações de sucesso do mercado empresarial para gerar conhecimento. Muito pelo contrário, ele também obtém lições das experiências ruins que são divulgadas.

Conhecer os casos mal-sucedidos de gestão da segurança da informação serve como base para não cometer os mesmos erros e bloquear prejuízos de toda a sorte. Vejamos alguns casos que viraram manchetes de jornais.

12.1. eBay

Em maio de 2014 a base de dados de usuários do eBay sofreu a violação das senhas de 112 milhões de pessoas, que foram obrigadas a trocá-las e ocasionou a perda de dados pessoais ali armazenados. Foram preservadas apenas as informações financeiras.

Esse tipo de ocorrência gera transtornos a um contingente enorme de usuários e abala seriamente a confiança dos clientes na credibilidade da empresa.

12.2. Snapchat

O Snapchat passou por maus momentos em janeiro e outubro de 2014. No primeiro evento de ataque cibernético, foram vazados os dados pessoais de 4,6 milhões de usuários — o que gerou um pedido de desculpas por parte da empresa e a promessa de melhorias nos mecanismos de segurança.

Já o segundo evento resultou de falhas de segurança em um parceiro de negócios do Snapchat, que estava responsável por armazenar imagens compartilhadas pelo aplicativo, o que possibilitou a divulgação indevida de 13 GB de fotos dos usuários na web.

12.3. Kickstarter

A Kickstarter foi vítima da quebra de segurança dos dados pessoais e senhas de 6 milhões de usuários cadastrados, também no ano de 2014.

A reação rápida da empresa conseguiu evitar a perda dos dados dos cartões dos clientes. No entanto, os impactos não deixaram de ser imensos.

12.4. Nasdaq

Nem mesmo o sistema de segurança da Nasdaq, considerado um dos mais robustos do mercado, ficou imune à intrusão, alteração e roubo de 160 milhões de registros, no ano de 2013, gerando prejuízos financeiros de alta monta.

12.5. Heartland Payment Systems Inc.

Em 2009, um malware infectou o datacenter da Heartland, importante operadora de cartões de crédito norte-americana, e permitiu o acesso de hackers a 100 milhões de registros, causando perdas milionárias de recursos financeiros e de inúmeros clientes.

Eventos desagradáveis como estes ligam o sinal de alerta e os radares da equipe de TI para a percepção de riscos internos e externos, que podem abalar a moral dos colaboradores e dos clientes da organização e que, em alguns casos, podem decretar o fim de uma empresa.

Até aqui, trilhamos uma longa jornada de visitação às 12 melhores práticas de segurança da informação. Este post colocou também todos os holofotes nas práticas proativas de prevenção de problemas na área de tecnologia da informação.

Todo este arsenal poderá ser utilizado pela sua empresa para evitar intrusões, roubos ou sequestros de dados, fraudes, alterações ou exclusões indevidas de informações.

Dessa forma, serão prevenidas perdas de milhares de clientes, com os consequentes prejuízos de imagem e financeiros, assim como o repasse indesejado de estratégias de negócios para os concorrentes.

As atualizações tecnológicas ao mesmo tempo que produzem novos recursos para proteção da informação, também abrem gaps, que podem ser aproveitados por pessoas mal-intencionadas para realizar crimes cibernéticos, visando obter fama e/ou dinheiro.

Inúmeros casos de violação da segurança da informação são divulgados todos os anos e precisam ser tomados para estudo de caso e determinação de novas práticas de proteção tanto no campo das máquinas e aplicativos quanto nas ações das pessoas. Assim, impede-se infortúnios que afetam a vida de muita gente.

Outro ponto de atenção quando o assunto é segurança: trata-se da adoção de critérios rigorosos para seleção e monitoramento da segurança da informação nos parceiros de negócios da área de TI e outras.

Eles são solidários na responsabilidade pelo atendimento aos princípios da segurança da informação. É preciso também garantir a segurança jurídica das relações de trabalho e de parceria, por meio da aplicação de contratos de confidencialidade.

Viu como a segurança da informação tem muitas facetas? Tecnológicas, jurídicas, humanas, físicas e virtuais. Todas elas devem ser alvo de medidas que contribuam para melhorar a gestão da segurança da informação.

Agora que você já conhece as melhores práticas de segurança da informação, que tal saber mais sobre essa nova tendência na área de TI chamada de BYOD (Bring Your Own Device)? Afinal de contas ela pode fazer emergir novas ameaças no cenário tecnológico. A sua empresa está preparada?

https://www.meupositivo.com.br/panoramapositivo/seguranca-da-informacao/

Shutterstock

A Internet é um dos principais pontos por onde a informação é distribuída na forma de bits e bytes. Notícias, opiniões, tutoriais e produtos, tudo isso é espalhado na Web em uma velocidade nunca vista em outro meio de comunicação. Justamente por isso, com tantos dados disponíveis a apenas um clique, a segurança da informação é mais que necessária. Afinal de contas, espalhar informações sigilosas, falsas ou que simplesmente não deveriam ser publicadas por expor alguém, é uma prática que deve ser evitada e traz consequências. Mas afinal, o que é Segurança da Informação e como funciona?

O que é Segurança da Informação?

O termo é usado para se referir à defesa de dados e à prática que assegura que informações sigilosas possam ser acessadas somente por aqueles a quem estas se referem (em outras palavras, seus responsáveis de direito).

A segurança da informação é uma grande aliada de empresas, pois é responsável por evitar que qualquer pessoa distribua, de forma indevida, dados sobre vendas, margem de lucro, concorrentes, entre outras. Em um mundo no qual diversas tarefas são realizadas ao mesmo tempo e e-mails

confidenciais podem ser enviados em apenas um clique, é fundamental que exista proteção para eventuais erros.

Nesses casos, a Segurança da Informação permite construir políticas e métodos que são empregados na circulação de dados confidenciais e são controlados pelo departamento de Tecnologia da Informação (TI) de uma empresa.

Geralmente, programas são instalados para garantir que os computadores serão utilizados somente para fins de trabalho. Além disso, é imprescindível garantir que os funcionários não baixarão nenhum tipo de programa no computador, uma vez que um simples *bug* ou *malware* pode colocar tudo a perder. Por isso, corporações preveem punições rigorosas (e até o risco de demissão) para qualquer colaborador que quebrar as regras de uso das informações, quer estejam em um e-mail com relatórios sobre vendas, quer em planilhas sobre a porcentagem dos lucros ou em apresentações salvas no computador.

Além disso, a Segurança da Informação também pode ser utilizada por indivíduos, principalmente em redes sociais, para proteger seus dados. Para garantir sua privacidade, é imprescindível que as pessoas possuam um bom antivírus, troquem sempre suas senhas de acesso, evitem compartilhá-las com outras pessoas e também evitem acessar suas redes usando computadores ou redes públicas. Tudo isso faz parte das propriedades básicas da Segurança da Informação, que são: confidencialidade, disponibilidade, autenticidade, integridade e legalidade.

Cursos sobre Segurança da Informação

Por conta da importância da área para a proteção de dados sigilosos, existem cursos de pós-graduação, MBA e também cursos que não requerem graduação prévia e podem ser encontrados em plataforma como a Udemy. Os profissionais da área de Tecnologia da Informação já reconhecem essa disciplina como sendo uma das mais importantes.

Um bom profissional de Segurança da Informação é capaz de monitorar riscos e projetar respostas adequadas a cada um deles, protegendo as máquinas contra o acesso de *hackers* e espiões. Além disso, ele também pode evitar a apropriação de dados sigilosos por criminosos que buscam fraudar e aplicar golpes na empresa.

Casos de falhas famosas de Segurança da Informação

Pacific Bank

O caso Pacific Bank ocorreu em 1978, quando um funcionário, Stanley Mark Rifkin, aplicou um golpe no banco onde trabalhava. Para executar seu plano, tudo o que ele precisou foi obter acesso a três códigos utilizados pelos funcionários responsáveis por realizar transferências eletrônicas: o *Código Diário Secreto*, o número do escritório e o número de estabelecimento entre escritórios (que foi obtido através de uma simples ligação).

Com esses três códigos, Stanley se passou por um membro do Departamento Internacional do banco e solicitou uma transferência de 10 milhões de dólares para uma conta na Suíça. Até hoje, o caso é lembrado como uma das maiores fraudes por vazamento de informações da história.

Hewlett-Packard (HP)

Já o incidente envolvendo a popular empresa HP ocorreu em 2005, quando informações sigilosas da corporação foram espalhadas por um dos diretores mais antigos da empresa, que as vendeu para o *Wall Street Journal*.

Antes da confissão, no entanto, a empresa grampeou telefones e contratou detetives particulares para descobrir o responsável pela quebra no sigilo dos dados - o que não teve um bom resultado, uma vez que a justiça dos EUA os acusou de utilizar meios ilegais para a investigação.

Petrobrás

O caso Petrobrás é a prova de que, além de proteger os dados no meio virtual, a Segurança da Informação também deve se precaver contra imprevistos envolvendo componentes físicos. Em 2008, notebooks e discos rígidos da Petrobrás sumiram misteriosamente. Todos continham informações extremamente importantes sobre o projeto do Pré-Sal, o que resultou em uma preocupação no país inteiro.

O caso foi investigado pela Polícia Federal e resultou na prisão de quatro pessoas.

E aí, você consideraria a Segurança da Informação um dos principais investimentos de uma empresa?

https://canaltech.com.br/seguranca/seguranca-da-informacao-o-que-e-158375/

Atualmente, os dados importantes e sigilosos das empresas são armazenados digitalmente, o que faz com que a preocupação com a segurança da informação seja extrema. O risco de criminosos virtuais acessarem essas informações ou provocarem a perda dos dados faz com que muitas empresas utilizem medidas e ferramentas protetivas.

Entretanto, é preciso saber quais ferramentas utilizar, bem como quais são as mais indicadas em cada situação específica. Em razão disso, fizemos este guia completo sobre SI para que você entenda a importância de adotar essas medidas protetivas para o negócio.

Vamos mostrar também, quais os benefícios em sua utilização, os principais erros que devem ser evitados e a melhor forma de implementar a SI na sua empresa. Acompanhe a leitura!

Escrito por 01/10/201912 comentários

Importância da segurança da informação para os negócios

https://www.eveo.com.br/blog/guia-seguranca-da-informacao/

O avanço da tecnologia fez com que grande parte dos processos empresariais passassem a serem feitos por meios eletrônicos.

A última Pesquisa Global de Segurança da Informação da PwC, realizada em 2018, revela que 46% dos impactos sofridos pelas empresas por conta de ataques cibernéticos comprometeram informações sobre seus clientes.

Com base nesses dados, dá para entender o tamanho da criticidade e prejuízos que esses ataques podem proporcionar às empresas.

Gerenciamento do Firewall voltado para SI

Uma das ferramentas utilizadas para conter esse problema é o firewall, que funciona como uma barreira a fim de impedir a entrada de elementos estranhos no sistema.

Em sua configuração, é possível determinar quem pode ou não pode acessar o ambiente, o que evita o acesso indevido aos dados.

Para garantir uma proteção eficiente é preciso fazer o gerenciamento de maneira adequada, que tanto pode ser por forma de bloqueio nas entradas, quanto por meio de permissão de acesso.

Além disso, é preciso fazer um acompanhamento constante para garantir que as políticas definidas sejam mantidas.

Outro ponto importante é sempre executar testes antes de implementar alguma alteração em suas configurações.

O ideal é criar um plano de reversão para situações em que seja preciso voltar as configurações em um estado anterior.

Benefícios da segurança da informação

A utilização do firewall protege a empresa de inúmeras ameaças, como as que vamos citar a seguir.

O que é Segurança da Informação e qual sua importância?

últimos artigos

FINANÇAS

Dívida líquida/EBITDA: saiba mais sobre esse indicador

FINANÇAS

O que são commodities e como investir nesses produtos?

FINANÇAS

FGC: o que é o Fundo Garantidor de Crédito e para que serve?

FINANÇAS

O que é o PIB e como é feito o cálculo deste índice?

- Publicado em 27.7.20
- Por Denis Zeferino

Com a criação do Regulamento Geral Sobre Proteção de Dados na Europa, no ano de 2016, a segurança da informação passou a ser um ponto de grande importância e cuidado por parte das empresas que tratam dados de clientes.

A segurança da informação é crucial se uma empresa deseja proteger todos os dados da instituição, um fator indispensável para o exercício de qualquer atividade empresarial.

1. O que é segurança da informação?
2. Como a segurança da informação se aplica à LGPD?

3. Como aplicar estas medidas a fim de aprimorar a segurança de dados em empresas?
4. O que é um plano de segurança de informação?
5. Melhores práticas de medidas de segurança da informação
6. Como garantir que as medidas de segurança da informação serão aplicadas e evitar erros?
7. Qual a diferença entre sistema de segurança de informação e gestão de segurança de informação?
8. Existe algum curso ou certificação nesta área?

O que é segurança da informação?

Segurança da informação é um conjunto de ações e boas práticas que têm como finalidade proteger um grupo de dados.

De tal maneira, essas medidas de segurança podem ser aplicadas em todas as empresas que trabalham com dados, uma vez que toda organização gera informações próprias.

A segurança da informação se baseia em quatro pilares que sustentam todas as medidas tomadas para garantir a proteção dos dados, que são:

- confidencialidade;
- autenticidade;
- integridade; e
- disponibilidade.

Por que cada um destes pontos são importantes para a segurança de dados?

Para entendermos a importância dos conceitos de confidencialidade, autenticidade, integridade e disponibilidade, traremos exemplos sobre cada um deles.

Um erro na confidencialidade, por exemplo, pode acabar deixando os dados de uma organização livres para que concorrentes possam acessá-los, sejam eles destinados para estratégias ou não.

Por outro lado, pode ocorrer um ataque nos servidores por parte de hackers, fazendo com que os dados de clientes armazenados sejam vazados ou roubados.

De toda forma, para ambos os casos a empresa terá prejuízos financeiros, uma vez que ela pode ser multada ou então perder novos clientes.

E, além disso, a imagem da instituição no mercado no qual ela trabalha será manchada por causa das falhas de segurança para com os clientes, sendo um ponto que atrapalha na obtenção de clientela.

Agora, quando falamos sobre autenticidade, mencionamos principalmente garantir que as informações preservadas sejam autênticas para evitar fraudes.

Um exemplo claro disso é o uso dos dados do cartão de crédito do cliente, fator que pode levar a clonagem e que eventualmente acaba sendo mostrado ao público que, por sua vez, perde a confiança.

Já a integridade está fortemente ligada à ferramentas e mecanismos de segurança, como os backups, a fim de garantir que os dados não sejam perdidos em caso de erros no sistema adotado pela empresa.

Por fim, quando falamos de disponibilidade, estamos falando justamente da possibilidade de acessar os dados a qualquer momento.

Ou seja, é necessário que todas as informações estejam disponíveis quando requisitadas, sendo este um fator que gera agilidade em processos.

Agora, caso uma empresa não preste atenção em todos estes pontos, o prejuízo virá sobre a instituição nas mais variadas áreas.

Afinal, com o uso cada vez mais intenso da redes sociais, as informações se espalham muito mais rapidamente no ambiente virtual.

Dessa forma, caso algum cliente faça uma reclamação na internet, ou haja dados vazados nesse ambiente, a reputação e imagem da empresa será prejudicada.

Sendo assim, todas as ações devem possuir base nos quatro pilares principais aqui citados para evitar problemas.

Quais os objetivos almejados por essas medidas?

A primeiro momento, é possível entender que o principal propósito de todas as ações tomadas aqui tem como fim proteger os dados e informações.

Contudo, é preciso entender que a segurança da informação vai além de uma estratégia adotada por uma instituição. Afinal, ela é uma das principais encarregadas pelo bom funcionamento e evolução do negócio.

Isso se dá tendo em vista que, atualmente, quem detém dados e informações possui poder.

E, por outro lado, no âmbito corporativo, é válido pontuar que as informações têm sido utilizadas de forma estratégica para que as instituições cresçam e se destaquem entre concorrentes.

Um bom exemplo para ilustrar isso é o uso do Big Data, algo que tem sido cada vez mais comum.

Analisando por outra perspectiva, os crimes cibernéticos estão crescendo, o que faz com que seja cada vez mais necessário possuir consciência do cenário atual.

Por isso é preciso tomar medidas para evitar problemas como invasões e roubo de dados, evitando que a empresa possua qualquer prejuízo.

Mas, para isso, é necessário possuir um bom planejamento para implementar tais medidas de proteção aos dados.

Como a segurança da informação se aplica à LGPD?

Um dos pontos que tem sido mais comentados ao falar sobre dados é o advento da LGPD, a Lei Geral de Proteção de Dados, sancionada em agosto de 2018.

Essa nova lei terá efeito sobre todos os setores da economia para empresas de todos os tamanhos.

A lei solicita que seja adotada uma forma diferente de trabalhar com dados, então pontos como segurança, transparência e privacidade e proteção de dados pessoais se tornaram mais importantes.

Agora, para as empresas que não respeitarem as diretrizes da lei, as multas podem chegar a valores de até R$50 milhões.

De tal forma, neste momento se tornou mais forte ainda a importância de garantir que todos os pontos colocados pela LGPD sejam garantidos. E, para isso, todas as soluções de segurança devem estar em conformidade, a fim de garantir uma proteção completa dos dados de clientes.

Essas medidas, além de serem requisitadas pela lei, servem justamente para evitar que os dados sejam roubados através de invasões de hackers ou extraviados por compartilhamentos realizados incorretamente ou até mesmo má fé de colaboradores internos das empresas.

Assim, é possível analisar que o principal desafio enfrentado por todas as empresas que trabalham com dados no momento é justamente garantir a proteção de todos eles.

Quer se tornar um especialista em LGPD e GDPR certificado pela EXIN? Clique e tenha acesso às primeiras vagas e desconto exclusivo!

Com a chegada da lei, os profissionais deste ramo são prejudicados?

Agora, olhando pelo lado do profissional dessa área, o advento da lei é um ponto benéfico.

Afinal, perante a norma, devem ser utilizadas medidas técnicas e administrativas para proteger os dados, o que faz necessário existir uma Governança dos Dados.

Ou seja, serão identificados pontos como:

- onde o cliente mora;
- qual o fluxo do dado;
- classificação de nível (se é um dado pessoal, sensível ou se não);
- gerenciamento de uso e ciclo de vida dos dados.

Tudo isso possui uma finalidade comum: evitar vazamentos e a perda, total ou parcial, de informações enquanto é feito um monitoramento do uso.

Porém, o aconselhado é buscar que todas as dicas que iremos trazer sejam seguidas em conjunto.

Como aplicar estas medidas a fim de aprimorar a segurança de dados em empresas?

Após entendida a importância e tendo ciência de que a segurança da informação nas empresas é um dos pontos fundamentais para o seu bom funcionamento, a dúvida que fica é sobre como implementá-la.

Para isso, existe uma série de práticas que podem ser implementadas na área de TI para que a empresa mantenha-se alinhada à lei. Confira então as recomendações para estar adequado a lei e evitar eventuais problemas:

1. acompanhar tendências e evoluções na área de tecnologia, uma vez que as evoluções deste segmento são constantes;
2. procure sempre manter os softwares e drives atualizados;
3. tenha controle sobre o acesso que os colaboradores tem aos dados;
4. possua um bloqueio de sistema de saída, evitando que qualquer dado seja liberado sem que os funcionários de TI tenham ciência;
5. possua políticas de segurança dentro da empresa;
6. mantenha todos os processos e políticas de segurança alinhados;
7. faça treinamentos com a equipe de pessoas que trabalham na empresa para deixar todos a par das medidas de segurança;
8. invista em ferramentas para realizar o monitoramento na rede ou servidor aos quais os dados estão armazenados;
9. faça uso da criptografia de dados para impedir o acesso sem chaves privadas;
10. tenha parceria ou contato de empresas especializadas no ramo de segurança da informação;
11. possua planos de contingência a fim de saber como agir em situações que ofereçam riscos para os dados coletados; e
12. sempre realize um backup dos dados, sendo indicado principalmente em nuvem, para possuir uma alternativa em termos de recuperação de dado caso seja necessário devido algum incidente.

E tendo isso em vista, a principal recomendação ao falarmos sobre este assunto é justamente adotar uma boa política de segurança com todas estas dicas.

O que é um plano de segurança de informação?

Ao falar sobre os possíveis procedimentos de segurança da informação de uma empresa, é necessário a implementação de medidas técnicas, administrativas e organizacionais, principalmente colocando em prática o SGSI (Sistema de Gestão de Segurança da Informação).

Este, por sua vez, é um conjunto de normas específicas as quais devem ser seguidas.

Este plano foi aprovado no ano de 2012 e ele dita que os sistemas de administração de informações e dados devem seguir os seguintes critérios:

- autenticidade;
- auditoria;
- privacidade; e
- não repúdio.

Para isso são levados em conta os quatro pilares que citamos anteriormente. Ou seja, é necessário que somente as pessoas autorizadas pela empresa tenham acesso às informações e dados, gerando confidencialidade.

Além disso, todas as alterações nos dados apenas poderão ser realizadas caso exista uma autorização pela empresa, o que traz a integridade.

Por outro lado, é altamente necessário que as informações fiquem disponíveis a qualquer momento para quando as pessoas forem utiliza-las, o que traz a disponibilidade.

E por fim, mas não menos importante, este plano requer que os dados sejam autênticos de maneira a evitar fraudes ou uma eventual clonagem.

Agora, para seguir todas esses pontos imprescindíveis, os dados devem ser gerenciados e protegidos contra fraudes, roubos, espionagem ou perda de dados, além de outras ameaças.

Melhores práticas de medidas de segurança da informação

Ao analisar as medidas tomadas para garantir a segurança de informações, é possível entender que podem existir práticas básicas e sofisticadas.

O aconselhado é que todas elas sejam seguidas para que uma empresa esteja adequada em relação a Segurança da Informação e LGPD, principalmente.

Para ficar mais simples, trouxemos então uma série de práticas para garantir que tudo seja seguido corretamente, veja:

- detectar possíveis vulnerabilidades no hardware e no software utilizados;
- sempre realizar cópias de segurança dos dados, o chamado backup;
- as redundâncias de sistemas não são uma opção ruim, ou seja, possuir mais de um servidor ou equipamento para poder dar continuidade às operações do negócio pode ser interessante;
- possua alta eficácia no controle de acesso através de um firewall, assinatura digital ou por meio da biometria das pessoas que possuem autorização;
- tenha um documento que sentencie diretrizes comportamentais para os colaboradores da instituição, chamada de política de segurança da informação;
- opte por uma estrutura de nuvem, seja ela pública, privada ou híbrida;
- tome cuidado com eventuais ameaças através de uma gestão de riscos apropriada, evitando falta de orientação, erros em procedimentos internos, negligência ou malícia;
- as regras do negócio e da empresa em tudo que diz respeito aos dados devem estar bem definidas;
- organização é um ponto imprescindível;
- contratos de confidencialidade com organizações e terceirizados vinculados à área de TI são bem vindos;
- sempre possua uma boa gestão de continuidade de negócios, chamada de GCN; e
- o benchmarking é um instrumento de gestão que auxilia muito a empresa.

Como garantir que as medidas de segurança da informação serão aplicadas e evitar erros?

Uma vez colocadas todas as medidas e práticas para manter dados protegidos, é preciso considerar que de nada adianta apenas possuir mecanismos de segurança da informação, mas não garantir que os mesmos sejam colocados em prática.

Sendo assim, se torna necessário ter certeza de que tudo está tendo aplicação no dia a dia, evitando eventuais problemas relacionados a segurança da informação.

E, para isso, existe uma série de medidas as quais podem ser feitas pelo gestor de TI de uma instituição ou alguém encarregado por analisar a segurança de dados, conforme veremos a seguir:

1. Proteger a rede e o uso da internet através de um UTM (Unified Threat Management), restringindo acessos a sites específicos
2. Possuir uma preservação e atualização constante dos sistemas utilizados
3. Orientar os usuários para identificar eventuais riscos, prevenindo possíveis ataques ao sistema

1.Proteger a rede e o uso da internet através de um UTM, restringindo acessos a sites específicos

Dessa maneira é possível impedir que ocorram acidentes que podem ser prejudiciais.

O grande exemplo aqui são os malwares que sequestram os dados, conhecidos como ransomwares.

Para isso podem ser bloqueados o acesso a:

1. sites estranhos;
2. sites para download;
3. algum site de jogos;
4. locais na internet que dão espaço a violência; e
5. sites de pornografia.

Contudo, o aconselhado é ter em vista o investimento necessário para obter um UTM (Unified Threat Management).

Outros pontos importantes são a manutenção e atualizações, bem como a relação entre os benefícios que o investimento proporciona.

2. Possuir uma preservação e atualização constante dos sistemas utilizados

Atualmente existem diversas formas as quais podem ser utilizadas para o roubo e ataques a bancos de dados.

Normalmente elas são causadas por eventuais falhas e vulnerabilidades do sistema ou então através da curiosidade dos usuários.

É justamente por isso que o sistema da empresa deve estar sempre atualizado.

E a preocupação aqui se encontra em:

1. atualizar os sistemas operacionais com periodicidade;
2. revisar as políticas de segurança da empresa e atualizá-las, caso necessário;
3. configurar os roteadores de internet com constância;
4. possuir um bom antivírus;
5. deixar os navegadores dos computadores sempre atualizados; e
6. identificar possíveis falhas na rede de tempos em tempos.

Através de todas estas medidas é possível evitar problemas nos sistemas.

3. Orientar os usuários para identificar eventuais riscos, prevenindo possíveis ataques ao sistema

Este ponto possui grande relação com o que foi citado anteriormente sobre a curiosidade dos usuários.

Afinal, muitas vezes por falta de conhecimento, as pessoas podem acabar clicando em links ou e-mails que levam para sites maliciosos.

Por isso, é altamente importante e recomendado que os funcionários sejam orientados para prevenir ataques e identificar riscos.

Uma dica aqui é elaborar um manual para o uso seguro do sistema e também da internet da instituição.

E a melhor forma de colocar isso em prática é oferecendo informação aos usuários tanto sobre eventuais fraudes como o uso correto dos equipamentos.

Qual a diferença entre sistema de segurança de informação e gestão de segurança de informação?

Quando falamos em gestão de segurança de informação é necessário entender que esta é uma área de TI que possui como principal função

elaborar processos e sistemas para monitorar as informações coletadas e indicar ações no intuito de evitar incidentes de segurança da informação.
O profissional desta área é o responsável pela prevenção a possíveis ataques e furtos de dados que uma empresa pode sofrer.
Sendo assim, ele também se torna o incumbido por fazer, de maneira rápida, com que os sistemas sejam restabelecidos em casos de ameaças ou emergências.
Contudo, tanto um gestor nessa área como o sistema de segurança de informações podem trabalhar de maneira conjunta.
Afinal, no primeiro caso falamos de uma pessoa que realiza as funções, a fim de garantir a proteção dos dados, enquanto no segundo caso trata-se de um sistema que gera um local seguro para os dados.
Por isso, uma empresa pode possuir um gestor, ou uma equipe de gestores, para analisar se o sistema está funcionando corretamente e mantendo as informações protegidas.
Vale lembrar que os dois devem ser utilizados de maneira conjunta em uma empresa, fator recomendado por especialistas para que uma instituição possua boa medida de proteção a dados.
Existe algum curso ou certificação nesta área?
Existe atualmente dentro de uma equipe de TI uma alta importância para especialistas na área de segurança da informação.
E isso ocorre principalmente devido ao crescimento do volume de dados bem como o armazenamento e gerenciamento de tudo o que foi coletado de maneira segura.
De tal forma, a necessidade de um profissional especializado neste segmento se dá uma vez que o risco de ataques, seja por vírus ou hackers, e furto de dados tem sido cada vez maior.
Contudo, a dúvida que fica é sobre qual é o caminho para então poder ocupar essa vaga em uma empresa.

Para isso, o primeiro passo é se formar academicamente como profissional desta área a fim de possuir conhecimentos sobre tecnologia da informação e proteção de dados.

No entanto, isso é válido para pessoas que possuem interesse por este segmento e, para tal, pode ser feito um curso superior tecnológico.

O curso segurança da informação dura cerca de dois anos, totalizando quatro semestres, e pode ser feito em módulo EaD caso desejado.

Agora, para quem já atua na área de TI, existem outras opções para se especializar em segurança de informação.

Aqui, por sua vez, se enquadram os profissionais que já possuem bacharelado em alguma área relacionada à tecnologia como Ciência da Computação, por exemplo.

A indicação então é justamente a de realizar uma pós-graduação no segmento de proteção de dados.

Após finalizado o curso, o profissional pode atuar livremente então neste ramo devido aos conhecimentos adquiridos por ele ao longo de ambas as graduações.

Como as certificações agem dentro deste ramo da tecnologia da informação?

É notório que a área de TI possui diversas possibilidades de especialidades e certificações.

E, tendo em vista que novas tecnologias são introduzidas a cada ano, não é para menos.

Os certificados são pontos diferenciais muito valorizados no currículo, principalmente quando falamos sobre o profissional deste ramo, uma vez que são a comprovação de que o indivíduo possui domínio sobre aquele assunto.

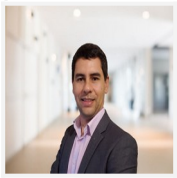
Para quem deseja ter destaque dentro do ramo de privacidade e proteção de dados, em especial, existem três certificações principais que podem credenciar o profissional, sendo:

1. Information Security Foundation (ISFS)
2. Privacy and Data Protection Foundation (PDPF)
3. Privacy and Data Protection Practitioner (PDPP)

Essas certificações são oferecidas pelo programa de formação EXIN para o DPO, profissional responsável pelas questões relativas à proteção de dados dentro de uma empresa, conforme determina a lei de proteção de dados.

No entanto, qualquer profissional que lida diretamente com dados e que deseja especializar-se está habilitado a certificar-se, sendo recomendado ainda, a quem precise, a realização do curso de nível básico PDPE – Privacy & Data Protection Essentials, que vislumbra um embasamento maior sobre o tema.

De toda maneira, o aconselhado para se tornar um bom profissional da segurança da informação é optar pelo investimento na carreira através principalmente das certificações para o ramo. Sendo assim, não perca tempo e dê um up no seu currículo agora mesmo!



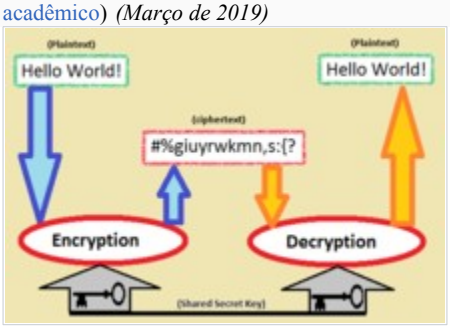
Denis Zeferino

Denis Zeferino é Data Protection Officer (DPO) certificado pela EXIN. Bacharel em Ciência da Computação e pós-graduado em Gestão de Infraestrutura de TI, Segurança da Informação e Cybersecurity. Tem mais de 15 anos de experiência, conciliando sua vida profissional entre o universo da Tecnologia e Segurança da Informação e da Educação. É membro da Associação Nacional dos Profissionais de Privacidade de Dados e dedicado a levar o entendimento da LGPD e Proteção de Dados aos alunos do Certifiquei.
https://www.certifiquei.com.br/seguranca-informacao/

Segurança da informação

Origem: Wikipédia, a enciclopédia livre.

Este artigo cita fontes, mas estas **não cobrem todo o conteúdo**. Ajude a inserir referências. Conteúdo não verificável poderá ser removido.—*Encontre fontes:* Google (notícias, livros e acadêmico) *(Março de 2019)*



A criptografia é essencial para a troca de dados pela internet.

A **segurança da informação** (SI) está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da
informação: confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

A SI não está restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. O conceito aplica-se a todos os aspectos de proteção de informações e dados. O conceito de *Segurança Informática* ou *Segurança de Computadores* está intimamente relacionado com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas em si o sistema.

Atualmente o conceito de Segurança da Informação está padronizado pela norma ISO/IEC 17799:2005, influenciada pelo padrão inglês (British Standard) BS 7799. A norma técnica de segurança da informação em vigor é: ABNT NBR ISO/IEC 27002:2013[1]

Índice

Conceitos de segurança

A maioria das definições de Segurança da Informação (SI) (Brostoff, 2004; Morris e Thompson, 1979; Sieberg, 2005; Smith, 2002) pode ser sumarizada como a proteção contra o uso ou acesso não-autorizado à informação, bem como a proteção contra a negação do serviço a usuários autorizados, enquanto a integridade e a confidencialidade dessa informação são preservadas. A SI não está confinada a sistemas de computação, nem à informação em formato eletrônico. Ela se aplica a todos os aspectos de proteção da informação ou

dados, em qualquer forma. O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer do uso impróprio da mesma. É importante lembrar que a SI também cobre toda a infraestrutura que permite o seu uso, como processos, sistemas, serviços, tecnologias, e outros.

A Segurança da informação refere-se à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto às informações corporativas quanto às pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente e, com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente. A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infraestrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação.

A tríade CIA (Confidentiality, Integrity and Availability) — Confidencialidade, Integridade e Disponibilidade — representa os principais atributos que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Outros atributos importantes são não-repúdio (irretratabilidade), autenticidade e conformidade. Com a evolução do comércio eletrônico e da sociedade da informação, a privacidade é também uma grande preocupação.

Portanto os atributos básicos da **segurança da informação**, segundo os padrões internacionais (ISO/IEC 17799:2005) são os seguintes:

- *Confidencialidade*: propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação;

- *Integridade*: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (Corrente, intermediária e permanente). O ciclo de vida da informação orgânica - criada em ambiente organizacional - segue as três fases do ciclo de vida dos documentos de arquivos; conforme preceitua os canadenses da Universidade do Quebec (Canadá): Carol Couture e Jean Yves Rousseau, no livro Os Fundamentos da Disciplina Arquivística;
- *Disponibilidade*: propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação;
- *Autenticidade*: propriedade que garante que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo;

Mecanismos de segurança

O suporte para as recomendações de segurança pode ser encontrado em:

- **Controles físicos**: são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura (que garante a existência da informação) que a suporta. Mecanismos de segurança que apoiam os controles físicos: portas, trancas, paredes, blindagem, guardas, etc.
- **Controles lógicos**: são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado. Mecanismos de segurança que apoiam os controles lógicos:
- Mecanismos de **cifração ou encriptação**: permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.
- **Assinatura digital**: Um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade e autenticidade do documento associado, mas não a sua confidencialidade.

- Mecanismos de **garantia da integridade da informação**: usando funções de "Hashing" ou de checagem, é garantida a integridade através de comparação do resultado do teste local com o divulgado pelo autor.
- Mecanismos de **controle de acesso**: palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.
- Mecanismos de **certificação**: atesta a validade de um documento.
- **Honeypot**: é uma ferramenta que tem a função de propositalmente simular falhas de segurança de um sistema e colher informações sobre o invasor enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema. É uma espécie de armadilha para invasores. O honeypot não oferece nenhum tipo de proteção.
- **Protocolos seguros**: uso de protocolos que garantem um grau de segurança e usam alguns dos mecanismos citados aqui.

  Atualmente existe uma grande variedade de ferramentas e sistemas que pretendem fornecer segurança. Alguns exemplos: antivírus, firewalls, filtros anti-spam, fuzzers, detectores de intrusões (IDS), analisadores de código, etc. [2]

Ameaças à segurança

As ameaças à segurança da informação são relacionadas diretamente à perda de uma de suas três principais características, quais sejam:

- **Perda de confidencialidade**: há uma quebra de sigilo de uma determinada informação (ex: a senha de um usuário ou administrador de sistema) permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários.
- **Perda de integridade**: determinada informação fica exposta a manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação.
- **Perda de disponibilidade**: a informação deixa de estar acessível por quem necessita dela. Seria o caso da perda de comunicação com um sistema importante para a empresa, que aconteceu com a queda de um servidor ou de uma aplicação crítica de negócio, que apresentou uma falha devido a um erro

causado por motivo interno ou externo ao equipamento ou por ação não autorizada de pessoas com ou sem má intenção.
No caso de ameaças à rede de computadores ou a um sistema, estas podem vir de agentes maliciosos, muitas vezes conhecidos como crackers, (hackers não são agentes maliciosos, pois tentam ajudar a encontrar possíveis falhas). Os crackers são motivados a fazer esta ilegalidade por vários motivos, dentre eles: notoriedade, autoestima, vingança e enriquecimento ilícito. De acordo com pesquisa elaborada pelo *Computer Security Institute*, mais de 70% dos ataques partem de usuários legítimos de sistemas de informação (*insiders*), o que motiva corporações a investir largamente em controles de segurança para seus ambientes corporativos (intranet).

Invasões na Internet

Todo sistema de computação necessita de um sistema para proteção de arquivos. Este sistema é um conjunto de regras que garantem que a informação não seja lida, ou modificada por quem não tem permissão.

A segurança é usada especificamente para referência do problema genérico do assunto, já os mecanismos de proteção são usados para salvar as informações a serem protegidas. A segurança é analisada de várias formas, sendo os principais problemas causados com a falta dela a perda de dados e as invasões de intrusos. A perda de dados na maioria das vezes é causada por algumas razões:

- Fatores naturais: incêndios, enchentes, terremotos, e vários outros problemas de causas naturais;
- Erros de hardware ou de software: falhas no processamento, erros de comunicação, ou bugs em programas;
- Erros humanos: entrada de dados incorreta, montagem errada de disco ou perda de um disco.
  Para evitar a perda destes dados é necessário manter um backup confiável, armazenado geograficamente distante dos dados originais.

Exemplos de invasões

Em 1988, um estudante colocou na internet um programa malicioso (malware), escrito em linguagem C, derrubando milhares de computadores pelo mundo, que foi identificado e removido logo após. Mas até hoje há controvérsias de que ele não foi completamente removido da rede. Até hoje não se sabe qual era seu objetivo, o que se sabe é que ele tentava descobrir todas as senhas que o usuário digitava. Mas esse programa se autocopiava em todos os computadores em que o estudante invadia. Essa “brincadeira” não durou muito, pois o estudante foi descoberto pouco tempo depois, processado e condenado a liberdade condicional, e teve que pagar uma alta multa.

Um dos casos mais recentes de invasão por meio de vírus foi o do worm Conficker (ou Downup, Downadup e Kido) que tinha como objetivo afetar computadores dotados do sistema operacional Microsoft Windows, e que foi primeiramente detectado em outubro de 2008. Uma versão anterior do malware propagou-se pela internet através de uma vulnerabilidade dos sistemas de rede do Windows (2000, XP, Vista, Server 2003, Server 2008, 7 Beta e Server 2008 R2 Beta, que tinha sido lançado anteriormente naquele mês). O worm bloqueia o acesso a websites destinados à venda, protegidos com sistemas de segurança e, portanto, é possível a qualquer usuário de internet verificar se um computador está infectado ou não, simplesmente por meio do acesso a websites destinados a venda de produtos dotados de sistemas de segurança.

Em 15 de outubro de 2008, a Microsoft liberou um bugfix de emergência para corrigir a vulnerabilidade MS08-067, através da qual o worm prevalece-se para poder se espalhar. As aplicações da atualização automática se aplicam somente para o Windows XP SP2, SP3, Windows 2000 SP4 e Windows Vista; o Windows XP SP1 e versões mais antigas não são mais suportados.

Em janeiro de 2009, o número estimado de computadores infectados variou entre 9 e 15 milhões. Em 13 de fevereiro de 2009, a Microsoft oferecia US$ 250mil em recompensa para qualquer informação que levasse à condenação e à prisão de pessoas por trás da criação e/ou distribuição do Conficker.

Os softwares antivírus não-ligados a Microsoft, tais como a BitDefender, Enigma Software, Eset, F-Secure, Symantec, Sophos, e o Kaspersky Lab liberaram atualizações com programas de detecção em seus produtos e são capazes de remover o worm. A McAfee e o AVG também são capazes de remover o vírus através de escaneamentos de discos rígidos e mídias removíveis.

Através dessas informações históricas percebemos que os antivírus devem estar cada vez mais atualizados, porque estão surgindo novos vírus rapidamente, e com a mesma velocidade deve ser lançado atualizações para os bancos de dados dos antivírus para que os mesmos sejam identificados e excluídos. Com a criação da internet essa propagação de vírus é muito rápida e muito perigosa, pois se não houver a atualização dos antivírus o computador e usuário estão vulneráveis, pois com a criação da internet várias empresas começarão a utilizar internet como exemplo empresas mais precisamente bancos, mas como é muito vulnerável esse sistema, pois existem vírus que tem a capacidade de ler o teclado (in/out), instruções privilegiadas como os keyloggers. Com esses vírus é possível ler a senha do usuário que acessa sua conta no banco, com isso é mais indicado utilizar um teclado virtual para digitar as senhas ou ir diretamente ao banco.

Nível de segurança

Depois de identificado o potencial de ataque, as organizações têm que decidir o nível de segurança a estabelecer para uma rede ou sistema os recursos físicos e lógicos a necessitar de proteção. No nível de segurança devem ser quantificados os custos associados aos ataques e os associados à implementação de mecanismos de proteção para minimizar a probabilidade de ocorrência de um ataque.

Segurança física

Considera as ameaças físicas como incêndios, desabamentos, relâmpagos, alagamento, algo que possa danificar a parte física da segurança, acesso indevido de estranhos (**controle de acesso**), forma inadequada de tratamento e manuseio dos veículos.

Segurança lógica

Atenta contra ameaças ocasionadas por vírus, acessos remotos à rede, *backup* desatualizados, violação de senhas, furtos de identidades, etc.

Segurança lógica é a forma como um sistema é protegido no nível de sistema operacional e de aplicação. Normalmente é considerada como proteção contra ataques, mas também significa proteção de sistemas contra erros não intencionais, como remoção acidental de importantes arquivos de sistema ou aplicação. É fácil manipular a informação usando palavras-chave, como nesse caso: informação; segurança; e controle.

Pontos de controle de segurança

[3]Conforme Bluephoenix(2008) apud Espírito Santo(2012), após identificar os riscos, os níveis de proteção e determinar as decorrências que os riscos podem causar, deve-se executar os pontos de controle para reduzir riscos. Os controles podem aplicar-se na seguinte forma:

1. Políticas de segurança da informação;
2. Organização da segurança da informação;
3. Gestão e controle de ativos;
4. Segurança em recursos humanos;
5. Segurança física e do ambiente;
6. Gestão das operações e comunicações;
7. Controle de acessos;
8. Aquisição, desenvolvimento e manutenção de sistemas de informação;
9. Gestão da continuidade do negócio;
10. Conformidade legal.

Políticas de segurança

De acordo com o RFC 2196 (*The Site Security Handbook*), uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização.

As políticas de segurança devem ter implementação realista, e definir claramente as áreas de responsabilidade dos utilizadores, do pessoal de gestão de sistemas e redes e da direção. Deve também adaptar-se a alterações na

organização. As políticas de segurança fornecem um enquadramento para a implementação de mecanismos de segurança, definem procedimentos de segurança adequados, processos de auditoria à segurança e estabelecem uma base para procedimentos legais na sequência de ataques.

O documento que define a política de segurança deve deixar de fora todos os aspectos técnicos de implementação dos mecanismos de segurança, pois essa implementação pode variar ao longo do tempo. Deve ser também um documento de fácil leitura e compreensão, além de resumido.

Algumas normas definem aspectos que devem ser levados em consideração ao elaborar políticas de segurança. Entre essas normas estão a BS 7799 (elaborada pela British Standards Institution) e a NBR ISO/IEC 17799 (a versão brasileira desta primeira). A ISO começou a publicar a série de normas 27000, em substituição à ISO 17799 (e por conseguinte à BS 7799), das quais a primeira, ISO 27001, foi publicada em 2005.

Existem duas filosofias por trás de qualquer política de segurança:

- a proibitiva (tudo que não é expressamente permitido é proibido) e
- a permissiva (tudo que não é proibido é permitido).

Os elementos da política de segurança devem ser considerados:

- Disponibilidade: o sistema deve estar disponível de forma que quando o usuário necessitar, possa usar. Dados críticos devem estar disponíveis ininterruptamente;
- Integridade: o sistema deve estar sempre íntegro e em condições de ser usado;
- Confidencialidade: dados privados devem ser apresentados somente aos donos dos dados ou ao grupo por ele liberado;
- Autenticidade: o sistema deve ter condições de garantir de que a informação e/ou a identidade dos usuários, são quem dizem ser;
- Legalidade: valor legal das informações dentro de um processo de comunicação.

Políticas de senhas

Dentre as políticas utilizadas pelas grandes corporações a composição da senha é a mais controversa. Por um lado profissionais com dificuldade de

memorizar várias senhas de acesso com mais de 10 caracteres diferenciados, por outro funcionários displicentes que anotam a senha sob o teclado, no fundo das gavetas e, em casos mais graves, até em post-it no monitor.

Recomenda-se a adoção das seguintes regras para minimizar o problema, mas a regra fundamental é a conscientização dos colaboradores quanto ao uso e manutenção das senhas:

- Senha com data para expiração.
  Adota-se um padrão definido onde a senha possui prazo de validade de 30 ou 45 dias, obrigando o colaborador ou usuário a renovar sua senha;

- Inibir a repetição.
  Adota-se através de regras predefinidas que uma senha não poderá ter mais que 60% dos caracteres utilizados nas últimas senhas. Por exemplo: caso a senha anterior fosse “123senha”, a nova senha deve ter mais de 60% dos caracteres diferentes, como “456**se**use”, neste caso foram repetidos somente os caracteres “s” “e” os demais diferentes;

- Obrigar a composição com número mínimo de caracteres numéricos e alfabéticos.
  Define-se obrigatoriedade de 4 caracteres alfabéticos e 4 caracteres numéricos. Por exemplo: 1432seus ou até 1s4e3u2s ;

- Criar um conjunto com possíveis senhas que não podem ser utilizadas.
  Monta-se uma base de dados com formatos conhecidos de senhas e proibir o seu uso. Exemplos: o nome da empresa ou abreviatura, caso o funcionário chame-se José da Silva, sua senha não deveria conter partes do nome como 1221jose ou 1212silv etc., nem sua data de nascimento/aniversário, número de telefone, e similares.

- Recomenda-se ainda utilizar senhas que mesclam caracteres em cAiXa aLtA e bAiXa, além da utilização de caracteres especiais como: @ # $ % & * ;
- Usar a técnica leet na composição das senhas, substituindo letras por números e símbolos; [4]

- Automaticamente gerar a senha para os usuários ou deixar que eles escolham entre um número limitado de opções exibidas.

A Gestão de riscos unida à segurança da informação

A gestão de riscos, por sua vez, fundamental para garantir o perfeito funcionamento de toda a estrutura tecnológica da empresa, engloba a Segurança da Informação, já que a quantidade de vulnerabilidades e riscos que podem comprometer as informações da empresa é cada vez maior.

Ao englobar a gestão da segurança da informação, a gestão de riscos tem como principais desafios:

- proteger um dos principais ativos da organização – a informação – assim como a reputação e a marca da empresa;
- implementar e gerir controles que tenham como foco principal os objetivos do negócio;
- promover ações corretivas e preventivas de forma eficiente;
- garantir o cumprimento de regulamentações;
- definir os processos de gestão da Segurança da Informação.

Entre as vantagens de investir na gestão de riscos voltada para a segurança da informação estão a priorização das ações de acordo com a necessidade e os objetivos da empresa e a utilização de métricas e indicadores de resultados.[5]

Referências

1. ↑ ABNT NBR ISO/IEC 27002:2013
2. ↑ 'Meu amigo foi atacado por um hacker'; sistema da Microsoft tenta evitar roubo de senhas no Hotmail, acessado em 5 de maio de 2012
3. ↑ Adrielle Fernanda Silva do Espírito Santo (2012). «Segurança da Informação» (PDF). ICE.EDU. Consultado em 28 de junho de 2015
4. ↑ Como criar senhas mais fortes, seguras e protegidas, acessado em 8 de fevereiro de 2017
5. ↑ GUEDES, MARIA HELENA (2016). *Os Mecanismos !*. [S.l.]: Clube de Autores. pp. 51–53

- Terpstra, John (2005). *Segurança para Linux*. RJ: Elsevier. ISBN 85-352-1599-9
- Melhorar a usabilidade de Gerenciamento de senha com políticas de senha padronizados
- Claudia Dias, Segurança e Auditoria da Tecnologia da Informação, 2000, Editora: Axcel Books 142, ISBN 85-7323-231-9

- Brostoff, S. (2004). *Improving password system effectiveness*. Tese de Doutorado. University College London.
- Morris, R. & Thompson, K. (1979). Password security: a case history. *Communications of the ACM,* 22, 594-597.
- Sieberg, D. (2005). Hackers shift focus to financial gain. *CNN.com - Special Reports - Online Security*. Publicado em 26 de setembro de 2005.
- Smith, R.E. (2002). The strong password dilemma. *Authentication: From Passwords to Public Keys*. Chapter 6. Addison-Wesley.

Ligações externas

A Wikipédia tem o portal:

Portal das tecnologias de informação

O Wikilivros tem um livro chamado *Segurança da Informação*

- «Computer Security Institute» (em inglês)
- «CERT.PT»
- «CERT.br»
- «Glossário de Segurança da Informação» publicado pelo Gabinete de Segurança Institucional
- «Como bloquear sites no PC»

https://pt.wikipedia.org/wiki/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o

25 de Fevereiro de 2021**POR STEFANINI**

Um tema importante na gestão de negócios, a segurança da informação

er

organização esteja seguro.

https://stefanini.com/pt-br/trends/artigos/guia-sobre-seguranca-da-informacao

O grande problema é que qualquer falha encontrada nas redes e nos sistemas pode abrir caminho para problemas maiores. Em 2015, um erro desse tipo expôs 4 milhões de servidores federais dos Estados Unidos. Isso mostra que grandes corporações e até mesmo órgãos governamentais estão suscetíveis a ciberataques e brechas de segurança.

GUIA COMPLETO SOBRE SEGURANÇA DA INFORMAÇÃO

21 de janeiro de 2021

em Disaster Recovery

Compartilhe:

- Empresas de pequeno e médio porte também podem perder seus dados para cibercriminosos, principalmente devido à maior vulnerabilidade dos seus sistemas. Por isso, é fundamental que os gestores entendam a importância do assunto, bem como todos os pontos, técnicas e informações envolvidos para aprimorar a proteção do negócio.

Neste artigo, mostraremos como aumentar a segurança digital nas empresas. Para isso, é preciso entender o conceito, seus princípios e sua importância, as penalidades legais envolvidas e o valor do investimento. Além disso, é essencial verificar a necessidade de contratar empresas especializadas e saber o que avaliar nesse momento. Vamos conferir?

O que é segurança da informação? E cibersegurança?

A área de TI das empresas trabalha com diferentes tipos de tecnologias no gerenciamento e armazenamento de dados. Muitas das informações são confidenciais e precisam estar protegidas por políticas de segurança digital. Essas diretrizes determinam as estratégias e os procedimentos mais eficazes para o tratamento dos dados.

Há pouco mais de 20 anos, ninguém imaginava que o mundo estaria como está hoje. Naquele tempo, ter um aparelho celular não era privilégio de muitos. Do mesmo modo que ter um computador com acesso à internet.

Nessas duas décadas, bastante coisa mudou. Agora as pessoas podem interagir com o mundo por meio de redes sociais, e ações bancárias se tornaram possíveis e mais ágeis em poucos cliques e

Existem diversos conceitos a respeito da área de InfoSec — Information Security —, mas utilizaremos esta: a segurança da informação compreende um conjunto de práticas, recursos, ações, habilidades e mecanismos usados ao proteger todos e quaisquer tipos de dados da empresa e sistemas contra o ataque de criminosos, o acesso indevido de usuários e o uso impróprio das informações da organização.

Essas técnicas também visam prevenir o sequestro ou a perda de dados.

documentos físicos podem ser salvos em nuvem, de forma totalmente digital.

Mas, nem tudo são flores na internet. Afinal, todas as interações, a movimentação bancária e o armazenamento na nuvem trabalham com um volume grande de informações. E, mesmo na *web*, existem riscos dos seus dados serem extraviados, roubados ou até adulterados.
Já ouviu falar em **segurança da informação**? Não sabe qual a importância de preservar os dados, nem como proteger a sua empresa contra ataques **cibernéticos**?
Então, confira esse guia completo sobre **segurança da informação** para dominar o assunto de uma vez por todas!

SEGURANÇA DA INFORMAÇÃO: O QUE É E QUAL SUA IMPORTÂNCIA PARA OS NEGÓCIOS?

A **segurança da informação** é uma prática que visa proteger as informações de um determinado indivíduo ou organização a fim de preservar a sua integridade.
No mundo dos negócios, a **segurança da informação** é extremamente importante porque garante que apenas os usuários autorizados tenham acesso aos dados e documentos. O que pode livrar a empresa de uma série de problemas.

Como hoje as organizações realizam muitas ações pela internet, investir na **segurança da informação** é uma ação necessária para se prevenir contra diversos tipos de ameaças e riscos. Por exemplo: perda e adulteração de dados e ataques cibernéticos.

Os princípios básicos da política de **segurança da informação** são divididos em **6 pilares**:

- **Integridade:** preservar a originalidade e confiabilidade dos dados;
- **Confidencialidade:** assegurar o sigilo da informação;
- **Disponibilidade:** garantir a disponibilidade dos dados;
- **Autenticidade:** confirmar que as informações vieram de fonte confiável;
- **Irretratabilidade:** atuar para que a empresa não negue a autoria de uma ação específica;
- **Conformidade:** assegurar que todos os procedimentos serão feitos dentro das leis e normas.

SOLUÇÕES DE SEGURANÇA DA INFORMAÇÃO E SEUS BENEFÍCIOS

Assim que a política de **segurança da informação** é implantada, a empresa garante mais transparência e eficiência nos negócios. Isso porque tais medidas ajudam na organização dos dados, simplificando o acesso às informações e reduzindo danos à infraestrutura de TI.

Os principais erros cometidos na **segurança da informação** geralmente estão relacionados à falta de treinamento dos usuários, de monitoramento ou de uma política de backup de dados. Isso

sem dizer da ausência de investimentos nos processos de controle de acesso e atenção em manter os sistemas atualizados.
Sua empresa já cometeu ou comete algum desses erros? Abaixo, veja 4 soluções que podem ajudar na política de segurança da sua empresa e quais são os benefícios de contar com essas ferramentas:

FIREWALL

O firewall é um dispositivo que monitora o tráfego de conexão com a internet. Ele pode ser um hardware, software ou ambos. Por meio de um firewall você pode permitir ou bloquear acessos específicos de acordo com as políticas de segurança da sua empresa.

Os principais tipos de firewall são:

- ***Packet filtering***: controla o acesso monitorando os pacotes de entrada e saída;
- ***Proxy services***: protege a rede filtrando as mensagens, mascarando o endereço IP e limitando os tipos de tráfego;
- ***Stateful inspection***: impede o tráfego não autorizado, analisando os pacotes e inspecionando o estado de cada um deles.

ANTIVÍRUS

O antivírus é um software que protege o computador contra as ações maliciosas de vírus e *worms* (*malware* mais perigoso que um vírus comum). O objetivo do programa é dar mais segurança ao usuário, como também impedir que todo tipo de arquivo mal intencionado danifique a infraestrutura de TI. Hoje existem várias **opções de antivírus** no mercado.

BACKUP

Backup, que em português significa cópia de segurança, é uma ação utilizada para armazenar documentos, imagens, vídeos ou outros tipos de arquivo no computador ou na **nuvem**.
A finalidade do ***backup*** é proteger a sua empresa contra a perda de arquivos, geralmente ocasionada por ataque de vírus e malware, danos mecânicos ou falhas elétricas.
Entre os principais **tipos de backups existentes,** destacamos:

- **Backup completo:** copia todos os arquivos do servidor para outro local de armazenamento, de preferência na nuvem;
- **Backup incremental:** copia apenas os arquivos que foram alterados desde o último backup completo;
- **Backup diferencial:** salva os dados alterados desde o último backup completo;

DISASTER RECOVERY

Disaster Recovery, também conhecido como Recuperação de Desastre, refere-se a um plano de ação para recuperação de ambientes em caso

de um eventual desastre na infraestrutura de TI. Sua principal função é garantir a segurança dos dados, mantendo alta disponibilidade da operação da sua empresa, caso ocorra possíveis imprevistos.
Feito por meio de replicação de dados, sistemas e servidores físicos ou virtuais, o Disaster Recovery as a Service, consiste em uma solução que garante à empresa um ambiente de trabalho secundário, garantindo a proteção dos principais pontos do ambiente de TI de uma empresa, mantendo a continuidade do seu negócio mesmo após possíveis falhas.

Esse tipo de solução previne do Ataque DDos, que sobrecarrega um servidor/computador até esgotar os seus recursos deixando-o indisponível para uso e do **ataque ransomware**, que infecta o equipamento e exibe mensagens exigindo a quitação de uma taxa para fazer o sistema voltar a funcionar.
O mais interessante do *Disaster Recovery* as a Service é que a solução oferece segurança de blockchain, o que torna possível a prevenção contra essas ameaças. Também o *Secure Socket Layer* (SSL), que em português significa ferramenta de encriptação de páginas e pode ser usado para criptografar e autenticar os dados enviados entre um navegador e um servidor de web.
O Disaster Recovery as a Service, serviço que oferecemos em parceria com a Veeam, assegura todas as funcionalidades necessárias para prevenir a empresa contra riscos e ameaças.

ESTRATÉGIAS PARA CRIAR UMA BOA IMPLANTAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Agora que você já sabe o que é **segurança da informação**, qual a sua importância nos negócios e as soluções que podem ser usadas pela sua empresa, veja algumas estratégias para criar uma boa implantação de **segurança da informação**.

#1. UTILIZE FERRAMENTAS DE PROTEÇÃO

Invista em ferramentas que protegem o seu computador e o acesso dos usuários na rede contra ataques de hackers, vírus ou qualquer outra ameaça.

#2. UTILIZAR COMPUTAÇÃO NA NUVEM

A **computação na nuvem** chegou para simplificar o acesso e armazenamento de dados. Para não correr o risco de perder os arquivos

por conta de problemas no computador, você pode recorrer a essa tecnologia para fazer o *backup* ou manter uma cópia dos documentos.

#3. MANTER SISTEMAS ATUALIZADOS

Os criminosos virtuais estão sempre se aprimorando para roubar informações e prejudicar a sua infraestrutura de TI. Assim sendo, para não correr o risco de cair em alguma armadilha deles, saia na frente e mantenha seus sistemas sempre atualizados.

#4. CRIE UMA POLÍTICA DE CONTROLE DE ACESSOS

Os hackers e os vírus não são as únicas ameaças. Usuários não autorizados podem alterar documentos ou até excluir dados acidentalmente, assim prejudicando a veracidade das informações. Para não correr esse risco, crie uma política de controle de acessos.

#5. CRIE POLÍTICAS DE SEGURANÇA

Estabeleça critérios para arquivar documentos, treine a equipe para utilizar as tecnologias certas, invista em ferramentas que facilitam os acessos aos dados, enfim. Crie políticas de segurança para garantir que as informações da sua empresa estão seguras, são verídicas e estão sendo manuseadas corretamente.

#6. UTILIZE FERRAMENTAS DE MONITORAMENTO

Acompanhar os sites que os funcionários estão acessando, saber como eles estão se comportando na rede e como estão fazendo uso das informações também é importante. Assim sendo, utilize ferramentas de monitoramento que permitam esse tipo de ação.

#7. UTILIZE CRIPTOGRAFIA DE DADOS

A criptografia de dados codifica e decodifica informações. Recorrer a esse tipo de prática é uma forma de você impedir que os documentos e arquivos mais importantes sejam lidos por pessoas não autorizadas.

#8. CAPACITE SEUS COLABORADORES

Por trás da tecnologia sempre vai existir interação humana. Assim, se você quer que as ferramentas sejam usadas corretamente e com isso as informações realmente fiquem protegidas, você precisa capacitar todos os seus colaboradores.

#9. TENHA UM PLANO DE DISASTER RECOVERY

Por último, tenha um plano de Disaster Recovery. O Penso Veeam Disaster Recovery as a Service que oferecemos em parceria com a Veeam, é uma excelente alternativa para uma restauração rápida de ambiente e a replicação segura baseada em imagem em caso de algum desastre.
Com essa ferramenta você consegue aumentar a segurança das informações, além de garantir a continuidade dos seus negócios em tempo recorde.

Entre os principais recursos oferecidos pelo Penso Veeam Disaster Recovery as a Service, destacamos:

- Proteção contínua dos dados corporativos;
- Menor tempo de recuperação em caso de desastres;
- Criptografia de ponta a ponta;
- Replicação contínua para restauração dos seus servidores em Cloud Privada;
- Failover flexível e rápido;
- Backup e replicação de dados dos seus servidores físicos Windows/Linux e dos seus ambientes virtualizados Vmware, Hyper-V, Cloud Azure e AWS.

Gostou do tema? Ficou curioso para saber mais sobre o **Penso** Veeam Disaster Recovery as a Service e como a solução pode aumentar ainda mais a **segurança da informação** do seu negócio? Então, **conheça mais sobre o nosso produto!**
https://www.penso.com.br/guia-completo-sobre-seguranca-da-informacao/