Segurança das Informações

As pessoas são o elo mais fraco

Cláudio dos Santos Moretti

Segurança das informações: as pessoas são o elo mais fraco

Cláudio dos Santos Moretti
CES - ASE

Moretti, Cláudio dos Santos.

Segurança das informações: as pessoas são o elo mais fraco. USA. Monee, Illinois. Editora: Independently published. 2020.

ISBN: 9798677594359

Sumário

Prefácio

Este compendio foi elaborado a partir de diversas publicações de minha autoria nas mídias especializadas em Segurança Empresarial, como por exemplo, o Jornal da Segurança e a revista Gestão de Riscos.

O tema refere-se a importância das informações no contexto empresarial e pessoal com foco no desenvolvimento da cultura organizacional e conscientização das pessoas.

Apesar de fazer algumas referências a intrusão no sistema computacional ou invasão realizada por hackers, o ponto focal desta obra são as formas de atuação dos engenheiros sociais e as vulnerabilidades que são expostas através do elo mais fraco neste processo – as pessoas.

Portanto, não se trata de softwares, antivírus ou firewall e sim de educação nos procedimentos básicos de segurança das informações que residem na falta de cultura de proteção das pessoas.

Além disso, introduzi dois capítulos sobre o avanço tecnológico no setor de segurança privada.

Boa leitura!

Sobre o autor

Ex-sargento do Exército (1980-1987); Graduado em Gestão Empresarial – UNIMONTE – Santos (2003) e Tecnólogo em Processos Gerenciais - FAEL. Especializado em Gestão da Segurança Empresarial – MBA - FECAP/Brasiliano; Pós-graduado em Gestão de Crises Corporativa, - Universidade Gama Filho; Pós-graduado em Inteligência Estratégica - AVM; MBA em Gestão da Qualidade; MBA Executivo em Gestão de Pessoas; Gestión de Seguraridad Empresarial Internacional pela Universidad Pontificia Comillas, realizado em Madri, ES; Especialista em Gestón del Riesgo pelo IUGM – Instituto Universitário General Gutiérrez Mellado de la UNED Centor de Estudios de Seguridad (GET). Diversos cursos de extensão universitária. Professor da FAPI/FESP-SP/Brasiliano INTERISK no Curso Avançado em Segurança Empresarial – MBS, (2005 – 2019); foi professor do Curso de Gestão em Segurança da Universidade Monte Serrat (2005 – 2008) – UNIMONTE; foi professor do Curso Graduação Tecnológica de Gestão em Segurança Privada - UNIP/Santos (2009 – 2016); Autor de sete DVDs sobre segurança, editados pelo Jornal da Segurança; Articulista em diversas revistas

especializadas com mais de 100 artigos publicados. Trabalhou na Petrobras, (1987 – 2016) no setor de Inteligência e Segurança Corporativa (aposentado - 10/2016); Foi Coordenador da Escola Falcão – Centro de Formação e Treinamento de Segurança – Santos – SP (1999 – 2008); Membro da Associação dos Diplomados da Escola Superior de Guerra (ADESG); Perito judicial em gestão empresarial. Autor de **dois livros** didáticos da **KROTON Educacional** para cursos presenciais e EAD de Gestão de Segurança Privada nas universidades: Segurança bancária e transporte de valores, 2017. - Negociação e gestão de conflitos de segurança, 2018. Certificado de Administrador de Segurança Empresarial (**ASE**) pela Associação Brasileira dos Profissionais de Segurança Empresarial – ABSEG; Certificado de Especialista em Segurança Empresarial (**CES**) pela Associação Brasileira de Segurança Orgânica – ABSO; Professor em diversos cursos do **SESVESP** – (2013 – 2019). Autor de 12 cursos EAD para **IBRAGESP**; 03 para **Senhora Segurança**; 01 para **KROTON** e 01 para **ABSEG**.

A importância da informação

Na era da economia agrícola, prevalecia a atuação do homem e da natureza, na era da industrialização prevaleciam as máquinas e o trabalho manual do homem, porém isso mudou na chamada era da informação (economia intangível), onde o que vemos é que a informação sobre determinados assuntos é muito mais relevante do que as máquinas e os equipamentos. O homem continua sendo a chave mestra para o desenvolvimento, porém os bens de maior valor são as suas ideias, seu conhecimento.

Ainda hoje o modelo de gestão de pessoas que vigora em várias empresas é o modelo da era da revolução industrial, onde grande parte dos empregados não eram qualificados ou então semiqualificados. As hierarquias administrativas eram rígidas e os funcionários seguiam-nas sem questionar. Na era da informação, trabalhadores educados e habilitados, organizados em grupos, necessitam apenas de informações e de autoridade para agir em benefício do sucesso da empresa, motivo que faz com que o empowerment seja tão difundido nos dias de hoje onde os aspectos intangíveis passaram a ter um valor maior, ganhando mais importância do que os aspectos tangíveis.

Neste caso podemos citar como exemplos de aspectos intangíveis, as marcas, a imagem de uma empresa, o conhecimento pessoal, os recursos humanos, a reputação da empresa, etc.

A informação sempre teve um grande valor para a humanidade, e desde o início elas foram importantes em toda a sua história.

A informação é um ativo, que como qualquer outro ativo importante para os negócios, tem um valor para a organização.

Ela pode existir em muitas formas. Pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas.

A informação representa a inteligência competitiva dos negócios e é um ativo crítico para a continuidade operacional da empresa.

CONCEITOS:

Existem muitos conceitos sobre dados, informe, informação e conhecimento, que variam de acordo com o autor.
Apenas para exemplificar veremos alguns conceitos de diferentes autores:

De acordo com Marcos Sêmola, em seu livro **Gestão da Segurança da Informação** de 2003.

Conceito: Informação – conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos (isto é, baseados em troca de mensagens) ou transacionais (isto é, processos em que sejam realizadas operações que envolvam, por exemplo, a transferência de valores monetários).

Conceito: Ativo – todo elemento que compõe os processos que manipulam e processam a informação, o meio em que é armazenada, os equipamentos em que ela é manuseada, transportada e descartada.

O termo ativo possui esta denominação, oriunda da área financeira, por ser considerado um elemento de valor para um indivíduo ou organização, e que, por esse motivo, necessita de proteção adequada (NBR ISO/IEC-27002:2005).
O ativo pode ser dividido em diversas formas para facilitar o tratamento, mas o modelo mais comum é: equipamentos, usuários, ambientes, aplicações, processos e informações.

Para Adriana Beal m seu livro **Gestão estratégica da Informação**, os conceitos são:

Conceito: Dados – Registros ou fatos em “estado bruto”; facilmente estruturados; facilmente transferíveis; facilmente armazenados em computadores.

Conceito: Informação – Dados dotados de relevância e propósito; exige consenso em relação ao significado.

Conceito: Conhecimento – Combinação de informação contextual; experiência, insight; inclui reflexão, síntese e contexto;
De difícil estruturação; de difícil captura em máquinas; de difícil transferência.

De acordo com a NBR ISO/IEC-27002:2005 - **Tecnologia da informação - Código de prática para a gestão da segurança da informação**, o conceito é:
Informação - É um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e consequentemente necessita ser adequadamente protegida

Beal afirma que apesar das diferenças, há um certo entendimento comum: um conjunto de dados não produz necessariamente uma informação, nem um conjunto de informações representa necessariamente um conhecimento.

Alguns dados importantes sobre a informação:

Valor – a informação é um fator de apoio à decisão, pois com ela, a informação, é muito mais fácil você decidir sobre qualquer aspecto.
Ela é um fator de produção, pois com ela podemos produzir muito mais.
Também é um fator de sinergia, onde podemos juntar informações e com isso obter um resultado ainda melhor do nosso trabalho ou negócio.
Além disso, um valor importante que se refere à informação é que ela é um fator determinante de comportamento. Com a informação correta seu comportamento muda.

O valor da informação é resultado de três aspectos:

- O seu conteúdo;
- O contexto no qual está inserida;
- O tempo em que é disponibilizada.

Sun Tzu já sabia disso há mais de 2.500 anos atrás, onde, nos seus escritos de **A Arte da Guerra** diz: ”que o alto comando é bem-sucedido em situações onde as pessoas comuns fracassam, porque conseguem mais informações na hora certa e a utilizam mais rapidamente”.

LEIS DA INFORMAÇÃO:

Leis da informação – A informação é infinitamente compartilhável, ela não acaba a cada vez que você a usa. Nunca.
O valor da informação aumenta a cada uso que você faz dela, quanto mais você usa a informação mais ela tem valor.
Porém a informação é perecível (tem prazo de validade), caso não seja usada na época certa perderá seu valor de importância.
Quanto mais precisa for a informação mais valor ela terá para aqueles que necessitam dela.

Uma informação isolada tem um valor, porém quando combinada com outras informações seu valor aumenta significativamente.

Aqui também devemos fazer uma ressalva. Mais informação não quer dizer que seja necessariamente melhor, pois elas podem se perder no meio de tantas outras, sem ser devidamente usada. Paradoxalmente a isto, informação se multiplica, e torna-se interminável.

A INFORMAÇÃO COMO FONTE DE PODER.

Mais do que nunca conhecimento é poder, e a empresa que liderar a chamada “era da informação” ou “era do conhecimento” estará à frente das outras. Isto significa estar atento ao avanço das tecnologias de informação e comunicação e desenvolver a habilidade em coletar, processar e disseminar informações.

Em um mundo de rápidas transformações, informação sobre o que está acontecendo no mercado, nos gostos e preferências dos clientes, sobre desenvolvimento tecnológico, e principalmente sobre concorrentes é crucial.

Com a globalização, o desafio das empresas, hoje, está em conhecer as exigências dos diferentes segmentos de mercado. Para isso a informação é matéria prima, fazendo com que a empresa possa reagir rapidamente às mudanças de seu ambiente.

De acordo com a NBR ISO/IEC-27002:2013 “O valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos. ”

As informações podem ser classificadas, quanto a forma encontrada, do seguinte modo:
Basicamente elas podem ser oriundas de Fontes abertas é o termo utilizado para designar as informações que se encontram disponíveis para serem acessadas por qualquer pessoa, contrariamente são as informações fechadas que possuem classificação de segurança (secreto, ultrassecreto, confidencial ou reservado).

Também podem estar divididas conforme os tipos abaixo relacionados:

- **Literatura cinza** – literatura que não é classificada, pois não sofreu nenhum processo de avaliação para atribuição de graus de sigilo, porém é produzida em quantidade limitada e com propósito específico.
- **Informações eletrônicas abertas** – é a informação disponível na internet.
- **Informação empresarial aberta** – é a informação adquirida através de um processo de engenharia reversa de produtos adquiridos legalmente. Neste caso são amplamente aceitos os esforços de um competidor em estudar a organização e os produtos do seu competidor.
- I**nformação empresarial fechada ou informação classificada** – são os segredos das empresas, aos quais é negado o acesso de pessoas estranhas. Essas informações só podem ser obtidas por meio de espionagem industrial.

TIPOLOGIA DA INFORMAÇÃO

As informações podem ser encontradas nas seguintes formas:

40% - Textual ou Formal – são oriundas de banco de dados, publicações, patentes, revistas, etc.

40% - Informal – são oriundas de rumores, clientes, empresas, pessoas, intuição, etc.

10% - Especialistas – dependem da memória e know-how do especialista
10% - Exposições e Feiras.

Hoje em dia, o problema não é a falta de informação, mas o excesso.
A internet trouxe uma gama enorme de informações disponíveis e isso também é parte do problema. Fazer a análise dessas informações, filtrá-las de forma adequada para uso prático é um desafio diário para qualquer gestor. Lembrando uma frase do professor Cortella que diz, mais ou menos assim “muitos navegam na internet, enquanto outros naufragam” essa frase é a síntese do excesso de informação e a facilidade de se perder o foco.

A proteção das informações está nas pessoas

Em uma empresa, a conscientização de todos os colaboradores é fundamental para garantir a proteção de dados importantes, o que pode exige, muitas vezes, a atuação de uma equipe multidisciplinar.

Muito já se falou sobre a segurança das informações, mesmo assim os casos de fuga involuntária de dados continuam acontecendo diariamente. Inúmeras empresas se preocupam em instalar bons softwares para evitar a intrusão, criam políticas de segurança (o que é fundamental), porém não conseguem evitar a fuga de informação. A razão é a falta de conscientização e também de treinamento aos colaboradores.

Um pequeno exemplo: não adianta estabelecer senhas com números e letras maiúsculas e minúsculas, se o usuário as escreve num papel e cola em seu microcomputador. A forma como foi elaborada a senha estava correta, porém não há eficácia na segurança das informações.
Outro exemplo: o acesso às informações é restrito e segmentado, porém o usuário imprime os documentos para ler e os deixa sobre a mesa ou os joga no lixo sem nenhum tratamento. Da mesma forma que ocorreu no primeiro caso, houve a preocupação em segmentar e restringir as informações, porém não houve eficácia na segurança das informações.

Para comprovar que a informação não pode ser desprezada ou simplesmente jogada no lixo, em junho de 2001 uma empresa de investigação foi contratada pela Oracle Corporation para espionar o lixo da Microsoft, seu concorrente direto. Ora, então não há como proteger as informações? É claro que há. No entanto, isso não pode ficar apenas nas mãos dos técnicos – que usam as ferramentas adequadas. A chave está e sempre estará nas mãos das pessoas.
É bom lembrar que não existe segurança 100% infalível, já que ela sempre dependerá das pessoas. Mas deixar toda a proteção das informações apenas nas mãos dos especialistas em TI é um grande equívoco. Muitas vezes eles não possuem ferramentas para trabalhar com as pessoas, não têm meios

para fazer um trabalho de conscientização, estão preocupados com a proteção do sistema de informações, evitando que ele seja invadido, interrompido ou que estas informações sejam alteradas ou destruídas. Daí a necessidade de uma equipe multidisciplinar para trabalhar com a segurança das informações.

A segurança da informação deve ser pensada de maneira holística. É comum tentar proteger tudo e, desse modo, acabar perdendo o foco do negócio. O mais importante não é a segurança, é o negócio. Conhecer os fatores críticos de sucesso é fundamental, pois daí sairão políticas e as prioridades de proteção.

É difícil fazer com que as pessoas tenham consciência de que a informação a que elas têm acesso é valiosa, que pode causar danos à empresa e que existem pessoas interessadas nestas informações. Geralmente, quando falamos em segurança das informações, as pessoas logo imaginam documentos ultrassecretos que nunca viram. Mas não é isso: as informações que devem ser protegidas são aquelas que, muitas vezes não foram classificadas quanto à sua segurança (secretas, confidencial, restrita, rotineira, corporativa, pública, etc.). Isso ocorre, principalmente, quando a empresa não tem políticas de segurança das informações.

Os dados que devem ser protegidos são aqueles que, nas mãos da concorrência, podem trazer prejuízos à empresa. E não é só isso. Imagine informações sobre o caso de corrupção de um funcionário da sua empresa e que seja divulgada na mídia de maneira indevida ou distorcida. Quanto essa notícia poderá prejudicar a imagem dessa corporação?

O projeto de um produto ou campanha de marketing no qual foram investidos muito tempo e dinheiro e que acaba “vazando” na mídia, faz com que se perca o “time” do lançamento. Quanto isso custaria?

Então, o que as empresas têm que fazer é treinar seus colaboradores. Uma boa iniciativa é começar mostrando às pessoas porque a informação é importante. Esse treinamento deve ser seguido de uma prática de procedimentos e atitudes para fortalecer as teorias, pois o adulto aprende muito mais quando consegue colocar em prática os novos ensinamentos.

Abaixo, alguns pequenos exemplos de boas práticas de segurança:

Mesa limpa: orientar o usuário a não deixar nenhum documento sobre a mesa quando estiver ausente, mesmo que seja por alguns minutos.

Cuidados com o lixo: o lixo é uma fonte de informações. Todo documento ou rascunho jogado no cesto de lixo poderá cair em mão erradas e causar prejuízos à empresa.

Papéis adesivos: ainda existem pessoas que anotam senhas nestes papéis e os deixam colados no monitor, ou seja, de nada adianta a senha conter oito dígitos, mesclar letras maiúsculas e minúsculas e ainda números, se o usuário, para não a esquecer, deixa tudo anotado junto ao monitor ou em sua mesa.

Impressoras: esquecer documentos impressos é muito comum, principalmente quando a impressora faz parte de uma rede, de modo que os documentos acabam esquecidos e à mercê de qualquer pessoa.

Auditoria comportamental para orientação e correção: muita gente teme esta palavra auditoria, porém a ideia é fazer uma verificação no seu posto de trabalho e poder orientá-lo sobre os riscos existentes e como evitá-los.

Classificação das informações: serve para informar as pessoas que manuseiam estes documentos que têm alguma ou muita importância para a empresa e que não devem ser divulgados, e devem ser armazenados ou arquivados em local seguro, assim como seu descarte deve seguir os procedimentos de acordo com a classificação do documento.

Esses são apenas alguns exemplos que podem ser implantados na empresa com o objetivo de desenvolver uma cultura de segurança da informação.

A Informação como ativo mais importante do negócio

Kevin Mitnik, considerado o maior hacker dos EUA nos anos 90, que hoje é consultor de segurança, escreveu no livro **A Arte de Invadir**: "*Qual é o ativo mais valioso do mundo em qualquer organização? Não é o hardware de computador, não são os escritórios nem a fábrica, nem mesmo o que é proclamado no tão conhecido clichê da corporação: "Nosso ativo mais valioso é nosso pessoal". O fato óbvio é que qualquer um deles pode ser substituído. Tudo bem, não tão facilmente, não sem luta, mas muitas empresas sobreviveram depois que sua fábrica foi queimada ou que alguns funcionários-chave saíram. Sobreviver à perda da propriedade intelectual, entretanto, é uma história totalmente*

diferente. Se alguém rouba seus designs de produto, sua lista de clientes, seus planos de novos produtos, seus dados de P&D - esse seria um golpe que poderia fazer sua empresa desaparecer". Mitnick e Simon (2006).

A informação sempre foi um ativo de grande valor para as empresas e às pessoas, de modo geral, mas ganhou mais importância devido ao avanço tecnológico e a dinâmica das mudanças nos mercados de produtos e serviços.

Este avanço é inevitável, a cada dia novas tecnologias são desenvolvidas para dar suporte à segurança pública e privada.

Hoje em dia, seria impossível pensarmos num projeto de segurança sem a interface com a segurança eletrônica.

Grande parte deste avanço tecnológico teve sua base ampliada a partir do uso da internet.

Para identificarmos o desenvolvimento e a rapidez do avanço da internet e suas implicações nos diversos modais ligados à segurança eletrônica, a segurança pública e privada basta observarmos o seu uso crescente.

Nas décadas de 1970 e 1980, além de ser utilizada para fins militares, a Internet também foi um importante meio de comunicação acadêmico.

O número de dispositivos conectados em 1984 era 1.000 e com a difusão do uso da internet a partir de 1990 começou a alcançar a população em geral, obtendo o número espantoso de 1 milhão de dispositivos conectados em 1992, já em 2008 era 1 bilhão e que em 2014 eram 10 bilhões.

De acordo com a 12ª edição da pesquisa TIC Domicílios (2017), divulgada pelo **Comitê Gestor da Internet no Brasil** – CGI.br, apesar da desigualdade no Brasil, 36,7 milhões de domicílios (54% do total) possuem acesso à internet.

O relatório (2017) sobre economia digital divulgado pela **Conferência da Nações Unidas sobre Comércio e Desenvolvimento** (UNCTAD – United Nations Conference on Trade And Development) colocou o Brasil em 4º lugar no ranking mundial de usuários de internet, com 120 milhões de brasileiros conectados.

Agora, com a chamada "**4ª revolução industrial**", a qual já está alterando e ainda vai alterar muito mais os nossos processos de desenvolvimento com mais velocidade, maior alcance das tecnologias e maior impacto nos sistemas, trarão ainda mais mudanças.

A "**internet das coisas**" (Internet of Things - IoT) trará mais integração, do mundo físico com o mundo digital, através de um processo de Inteligência, com coleta, processamento e análise de dados gerados através da conectividade e integração dos diversos meios tecnológicos.

Na pratica estamos vendo a crescente demanda pela **portaria remota** (que prefiro chamar de portaria inteligente), que, a pouquíssimo tempo, era inimaginável e está revolucionando a forma de atendimento, principalmente nos condomínios residenciais.

Outro exemplo, é o projeto **City Câmeras** da prefeitura de São Paulo, com a integração entre a tecnologia e a participação da sociedade na prevenção e reação contra a criminalidade.

Com isso, cada vez mais, a segurança das informações terá mais espaço na agenda, não só dos empresários, mas de todas as pessoas.

O ativo intangível, hoje, em muitas empresas, já é maior do que o valor de qualquer empreendimento físico (fábricas, máquinas, móveis, etc.).

Para essas empresas, a imagem e as ideias dos homens têm muito mais valor do que qualquer produto tangível. Tome como exemplo a Microsoft, o Google, a Coca-Cola, etc.

As grandes empresas têm se preocupado mais com a segurança das informações do que as pequenas e médias, onde muitas ainda não possuem uma precaução mínima a respeito do assunto e serão surpreendidas com esta necessidade, cada vez mais emergente.

Neste contexto, observamos que as grandes empresas ainda falham no desenvolvimento da cultura de segurança, deixando de lado o ponto frágil de qualquer estrutura que possamos pensar em relação à segurança – as pessoas.

Quando os sistemas computacionais são mais bem protegidos, as pessoas tendem a não se preocupar com a segurança, acreditando que o setor de TIC cuidará de tudo, que haverá programas para impedir qualquer acesso indevido aos arquivos.

Além disso, nem todos os firewalls e protocolos de criptografia do mundo nunca serão suficientes para deter um hacker decidido a atacar um ativo intangível de uma empresa.

O treinamento dos colaboradores é essencial. Para demonstrar isso, basta vermos as ações dos engenheiros sociais, que atuam na parte mais sensível de qualquer sistema – as pessoas.

Kevin Mitnik definiu em outro livro **A Arte de Enganar** como sendo: **"***A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia*". Mitnik e Simon, (2003).

Um dos precursores deste conceito é o ex-fraudador americano, Frank W. Abagnale. Seu livro, **Prenda-me se for capaz** (1980), virou filme. O filme dirigido por, nada menos que, Stven Spilberg que foi protagonizado pelos atores não menos famosos, Leonardo DiCaprio e Tom Hanks, em 2002.

No Brasil nós também temos pessoas que conseguiram notoriedade com seus golpes de engenharia social. Um deles é Marcelo Nascimento da Rocha.

Sua extensa lista de mentiras e trapaças, das mais diversas possíveis, demonstradas no livro "**VIP's – HISTÓRIAS REAIS DE UM MENTIROSO**" (2005), também virou filme com o mesmo nome, protagonizado pelo ator Wagner Moura em 2011.

Outro exemplo foi Carlos da Cruz Sampaio Júnior, o falso Coronel Sampaio, que atuou na Polícia Militar do Rio de Janeiro, sendo desmascarado e preso em 2010.

São vários os exemplos de como as pessoas conseguem ludibriar para conseguirem o que querem e usar o conhecimento de maneira criminosa.

Só o treinamento sistemático pode mitigar os riscos da ação de um engenheiro social. E para demonstrar a importância do treinamento, deixo um recado: "*Há um ditado popular que diz que um computador seguro é aquele que está desligado. Isso é inteligente, mas é falso: o hacker convence alguém a entrar no escritório e ligar aquele computador*". Mitnik (2003).

A importância da segurança da informação

Na era da economia agrícola, prevalecia a atuação do homem e da natureza, na era da industrialização prevaleciam as máquinas e o trabalho manual do homem, porém isso mudou na chamada era da informação (economia intangível), onde o que vemos é que a informação sobre determinados assuntos é muito mais relevante do que as máquinas e os equipamentos.

O homem continua sendo a chave mestra para o desenvolvimento, porém os bens de maior valor são as suas ideias, seu conhecimento.

Ainda hoje o modelo de gestão de pessoas que vigora em várias empresas é o modelo da era da revolução industrial, onde grande parte dos empregados não eram qualificados ou então semiqualificados. As hierarquias administrativas eram rígidas e os funcionários seguiam-nas sem questionar. Na era da informação, trabalhadores educados e habilitados, organizados em grupos, necessitam apenas de informações e de autoridade para agir em benefício do sucesso da empresa, motivo que faz com que o *empowerment* seja tão difundido nos dias de hoje onde os aspectos intangíveis passaram a ter um valor maior, ganhando mais importância do que os aspectos tangíveis.

Neste caso podemos citar como exemplos de aspectos intangíveis, as marcas, a imagem de uma empresa, o conhecimento pessoal, os recursos humanos, a reputação, etc.

Um exemplo bem conhecido é sobre a marca COCA-COLA. Já na informação anual de 1996, o valor de mercado da COCA-COLA era de US$ 131 bilhões, sendo que US$ 117 eram referentes ao ativo intangível, a marca. Tudo o mais (equipamentos, máquinas, imóveis, enfim a todos os bens materiais) teria um valor de mercado de US$ 14 bilhões.

A informação sempre teve um grande valor para a humanidade, e desde o início elas foram importantes em toda a história da humanidade.

A informação é um ativo, que como qualquer outro ativo importante para os negócios, tem um valor para a organização.

Ela pode existir em muitas formas. Pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas.

A informação representa a inteligência competitiva dos negócios e é um ativo crítico para a continuidade operacional da empresa.

O valor da informação é resultado de três aspectos:

- O seu conteúdo;
- O contexto no qual está inserida;
- O tempo em que é disponibilizada.

Sun Tzu *já sabia disso há mais de 2.500 anos atrás, onde, em seus escritos diz: "o alto comando é bem-sucedido em situações onde as pessoas comuns fracassam, porque conseguem mais informações na hora certa e a utilizam mais rapidamente"* (**Arte da Guerra**, século IV a. C.).

Dessa forma, a informação mostra-se como um dos ativos mais importantes para a organização, pois baseadas nestas informações é que as decisões são tomadas em benefício da empresa.

Com a mesma preocupação que o empresário deve ter com a busca das informações necessárias para suas decisões, a organização também deve ter para proteger as informações da empresa.

Neste ponto surgem as ferramentas da segurança das informações, colocando-se como uma das ferramentas mais importantes para a manutenção da competitividade da empresa.

Basicamente, o objetivo da segurança da informação é manter a confidencialidade, a integridade e a disponibilidade da informação, onde:

A confidencialidade é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso.

A integridade refere-se a salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

A disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Além das características essências da segurança da informação, ainda podemos acrescentar outros objetivos relacionados à segurança da informação. São eles:

Autenticidade - Trata-se de possibilidade de identificar e autenticar usuários, entidades, sistemas ou processos. Esta propriedade indica que o acesso aos serviços oferecidos pelo sistema deveria ser concedido apenas a usuários, entidades, sistemas ou processos autorizados e aprovados.

Irrevogabilidade - Trata-se de possibilidade de evitar o repúdio ou a negativa de autoria posterior de transações legítimas por parte de usuários. Esta propriedade indica que quaisquer transações legítimas, efetuadas por usuários, entidades, sistemas ou processos autorizados e aprovados, não deveriam ser passíveis de cancelamento posterior.

Legalidade - Esta propriedade indica que transações e informações devem estar em conformidade com necessidades legais, normativas, contratuais e estatutárias.

Devemos lembrar a segurança da informação não é uma função, ela é um processo que passa por todos os departamentos e setores da empresa, que deve ser constantemente realimentada.

As ameaças externas e internas sempre atuarão nas vulnerabilidades da empresa, para ficar mais claro, vamos mostrar alguns conceitos.

Ameaça - Trata-se de elementos (pessoa, processo, evento ou ideia) que levam algum risco a algum bem, explorando vulnerabilidades no sistema, comprometendo um ou mais dos seguintes requisitos: confidencialidade, a integridade e/ou a disponibilidade.

A ameaça pode ter origem acidental ou intencional.

Ameaças acidentais ou involuntárias - podem ser decorrentes de erro do usuário, falhas do equipamento, falhas do software ou de desastres naturais (incêndio, enchente, vendaval, raios, etc.).

Ameaças intencionais - pode ser fruto de roubo ou furto de equipamentos, engenharia social, ação do usuário (uso indevido, burlando o sistema), ação do pessoal da manutenção (sabotagem do sistema), ação de invasores do sistema, acesso remoto não autorizado, falsificação de documentos e registros, etc. São ameaças propositais, de ocorrência humana.

Vulnerabilidade - São fraquezas do sistema de proteção ou a ausência de proteção, que se traduzem em oportunidades para ocorrência ou concretização de ameaças.

As vulnerabilidades podem ser:

Físicas – salas mal planejadas, estruturas físicas de segurança fora dos padrões exigidos, falta de controle de acesso físico, etc.

Naturais – equipamentos propensos a ação da natureza, como raios, enchentes, incêndios, falta de energia elétrica, aumento da umidade e da temperatura ambiente.

Hardware – desgaste do equipamento ou máquinas obsoletas ou ainda sua má utilização.

Software – má instalação, erros de configuração, etc.

Mídias – CDs, DVDs ou pen drives danificados.

Humanas – vulnerabilidades ligadas aos fatores humanos, como a falta de treinamento e de conscientização, desrespeito as políticas de segurança, etc.

Comunicação – perda de comunicação ou acessos não autorizados.

São muitas as formas de ter suas informações perdidas ou vazadas para o concorrente e são muitas as formas de se proteger as informações, que vão desde a elaboração de políticas de segurança até a aquisição de softwares específicos, ou ainda seguindo todos os processos para a certificação ISO/IEC 27001:2013 **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**, porém, o que vemos hoje é que, algumas empresas, gastam muito dinheiro com tecnologias novas, criam uma série de procedimentos de segurança e acabam esquecendo do elo mais fraco nesta corrente de segurança – o ser humano.

Milhões empregados em sofisticados sistemas de segurança, porém poucos reais gastos em treinamento e na conscientização dos funcionários.

Dependem deles, grande parte das fugas de informações privilegiadas, sendo involuntárias ou não.

Ainda hoje pessoas guardam a senha sob o teclado, ainda emprestam sua senha para um colega, ainda divulgam informações pessoais a pessoas estranhas.

Um pequeno exemplo hipotético:

Um funcionário deixa sobre a mesa ou joga no lixo (sem tratamento) uma listagem contendo a qualificação dos empregados do seu setor (nome completo, RG, CPF, endereço, matrícula e setor em que trabalha) que é apanhada por alguém mal-intencionado.

Esta pessoa, através da lista telefônica interna da empresa, vê o ID (chave ou nome do usuário da rede interna) e liga para o Help Desk. Diz que esqueceu a senha. Eles pedem alguns dados para a confirmação do usuário (RG, CPF ou endereço) e lhe fornece uma nova senha provisória.

Pronto, ele já pode acessar a rede interna da empresa.

Este pequeno exemplo mostra como somos frágeis, como pequenos detalhes, podem trazer grandes prejuízos.

Poderia citar diversas formas de proteção das informações como, senhas seguras, formas de identificação positivas, políticas de segurança, controles de acesso físico e lógico, classificação das informações, boas práticas, mas tudo isso só tem validade a partir da conscientização das pessoas. Elas devem dar o verdadeiro valor as informações que estão em suas mãos e ter uma ideia de como podem ser usadas para o mal ou pelo menos contra seus interesses e os interesses da empresa.

De qualquer forma, a segurança da informação sempre começará e terminará nas pessoas, independentemente das ferramentas que a empresa use para implementá-la. E é justamente quando **NÃO** se dá a devida atenção às pessoas que o investimento em segurança se transforma em custo.

A segurança da informação

Quando se fala em segurança da informação a maioria das pessoas relaciona este tema com a área de TI, porém não é bem assim. Ou alguém acha que quando não existiam computadores não havia preocupação com a segurança da informação?

Em 1900 a.C. os Faraós faziam escritas em tabletes de argila para proteger suas informações contra outras civilizações.

Desde a descoberta da escrita, há mais de cinco mil anos, as pessoas procuraram proteger suas informações, seja através das formas de escritas seja através da forma com que elas eram armazenadas ou ainda de como se evitava o acesso a elas.

Sempre haverá alguém interessa do nas suas informações. Imagine o seu concorrente que teve acesso a sua proposta de negócio; o que você oferece; quanto você cobra; qual seu prazo de entrega; quais as formas de pagamento; que diferencial você pode oferecer; quais são seus potenciais compradores, parceiros e fornecedores; qual sua margem de lucro; quais seus projetos de curto, médio ou longo prazo; em que você está investindo; quais suas áreas de pesquisa, etc.
Com essas informações ele terá muito mais chances de vencer uma concorrência contra a sua empresa.

Porém, somente na sociedade moderna, com o surgimento dos primeiros computadores, as informações passaram a receber uma atenção especial em relação a sua segurança.
Imagine um banco que você precise ir ao caixa para ver o saldo da sua conta corrente. Imagine fazer compras no supermercado sem cartão de credito, cartão bancário ou o próprio celular.
Hoje você não é mais cliente de uma determinada agência bancária, você é cliente do banco.
Com o advento dos computadores, e da internet, a informação passou a ser muito mais compartilhada.

E com isso aumentou muito o risco de que estas informações sofressem algum tipo de alteração ou que fosse copiada por estranhos, ou ainda que ela fosse bloqueada, impedindo que você tivesse acesso a ela, assim você não teria como fazer seu trabalho. Mas não é só de segurança computacional que nós precisamos, pois muitas vezes a informação “vaza” por outros meios e, principalmente, através das pessoas, que na verdade são o elo mais forte e, ao mesmo tempo, o elo mais fraco desta corrente da segurança.

Para Brasiliano, em seu livro **A (IN) Segurança nas Redes Empresariais** (2002), não entender que a segurança da informação não faz parte da apenas da segurança computacional, é um erro grave, para ele, “a segurança da informação deve ser interpretada como a segurança física dos meios de comunicação – cabos, linhas de transmissão, ondas de radiofrequência, links com satélites; segurança física dos meios computacionais; a segurança lógica dos sistemas de tecnologia da informação; segurança do fluxo da informação – formal ou informal e por último a segurança de quem lida – as pessoas – com informações estratégicas e críticas no que concerne ao desempenho da empresa”.

Para falarmos em segurança da informação devemos definir o que é isto.

Também neste caso existem vários conceitos para segurança da informação, mas o que foi adotada pela **ABNT NBR ISO/IEC 27002:2005** é “A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades”.

A segurança da informação pode ser obtida através da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, treinamentos, estruturas organizacionais e funções de software, porém, por mais controles que existam, a segurança nunca será de 100%.

Pensar em segurança 100% é utopia, mesmo assim não dá para ficar parado, sem tomar as medidas cabíveis de segurança, achando que nada irá acontecer, pois acreditar que a nossa empresa não possui informações que sejam do interesse dos nossos concorrentes seria ingênuo demais.

A **ABNT NBR ISO/IEC 27002:2005** também define a segurança da informação como “a preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como, autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.
A integridade refere-se a salvaguarda da exatidão e completeza da informação e dos métodos de processamento”.

A confidencialidade é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso.
A integridade é a garantia de que o ativo não foi alterado, ou seja, que permanece da forma e com o conteúdo que foi criado.
A disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
Além das características essências da segurança da informação, ainda podemos acrescentar outros objetivos relacionados à segurança da informação. São eles:

Autenticidade - Trata-se de possibilidade de identificar e autenticar usuários, entidades, sistemas ou processos. Esta propriedade indica que o acesso aos serviços oferecidos pelo sistema deveria ser concedido apenas a usuários, entidades, sistemas ou processos autorizados e aprovados.

Irrevogabilidade - Trata-se de possibilidade de evitar o repúdio ou a negativa de autoria posterior de transações legítimas por parte de usuários. Esta propriedade indica que quaisquer transações legítimas, efetuadas por usuários, entidades, sistemas ou processos autorizados e aprovados, não deveriam ser passíveis de cancelamento posterior.

Legalidade - Esta propriedade indica que transações e informações devem estar em conformidade com necessidades legais, normativas, contratuais e estatutárias.

AS FORMAS DE ATAQUE ÀS INFORMAÇÕES SÃO:

Interrupção - é a obstrução a prestação dos serviços pelo sistema de informações - obstrução do fluxo normal dos dados e informações entre a fonte e o destino destes (afeta principalmente a disponibilidade dos dados e informações)

Modificação – é a alteração dos dados e informações, ocorrida entre a fonte e o destino destes - alteração do destino original dos dados e informações (afeta principalmente a confidencialidade e a disponibilidade (destino errado) e a integridade (alteração) dos dados e informações).

Fabricação – é a alteração da fonte original dos dados e informações - criação de dados fictícios ou alteração do conteúdo dos dados e informações na fonte ou no destino destes (afeta principalmente a confidencialidade e a disponibilidade (destino errado) e a integridade (alteração) dos dados e informações.

Interceptação – é a captura ou cópia de dados e informações, após estes haverem deixado a fonte emissora, fazendo com que estes não atinjam seu destino original (afeta principalmente a confidencialidade (cópia) e disponibilidade (captura) dos dados e informações).

Neste breve espaço é possível demonstrar algumas das características necessárias à segurança das informações e sua importância para qualquer tipo de negócio, inclusive quando pensamos em nossas necessidades pessoais para a garantia da nossa privacidade.

Cuidados com as informações e as ações do engenheiro social

Normalmente, quando se fala em sigilo profissional as pessoas pensam em informações ultrassecretas que, se divulgadas, podem acabar com a empresa.

Gostaria de falar sobre as informações mais comuns e na prevenção de crimes mais comuns também além da forma como atuam os engenheiros sociais, pessoas que, sem o uso da força, conseguem obter informações sigilosas para utilizá-las em extorsões.

Primeiramente, vamos entender o que é engenharia social.

Podemos conceituar a engenharia social como uma maneira de se obter informações confidenciais sobre determinada pessoa, equipamento, campanha ou empresa, sem o uso da força, apenas com inteligência, técnica, perspicácia e persuasão. Muitas pessoas associam este termo à informática, acreditando que apenas os que têm acesso a determinados programas e documentos em formato digital está sujeito a este tipo de ataque. Ledo engano.

Frank W. Abagnale, um ex-fraudador americano, conceituou engenharia social como “a arte e a ciência de induzir pessoas a agirem de acordo com seus desejos”. Seus feitos foram tão impressionantes que seu livro deu origem ao filme de mesmo nome: “**Prenda-me se for capaz**” (2002), dirigido por Steven Spilberg, protagonizado por Leonardo DiCaprio e Tom Hanks.

Apesar de todo treinamento, o ser humano muitas vezes responde aos seus instintos sociais de camaradagem, confiança ou mesmo por pura distração, revela informações sigilosas, respondendo perguntas simples e diretas, que o fazem fornecer dados confidenciais. Isso é o que acontece quando as pessoas são vítimas da engenharia social,

É o caso da empregada doméstica, por exemplo, que dá informações sobre onde as pessoas da casa trabalham, onde ela presta seus serviços, se eles estão viajando e quando retornam, onde as crianças estudam, como vão ao colégio, quem leva e quem vai buscar e que, com estas e outras informações acabam dando subsídios - sem a intenção - para uma quadrilha concretizar um sequestro planejado ou um pseudo-sequestro.

É o caso, por exemplo, do porteiro que dá informações sobre horários de chegada e saída de determinados condôminos, que informa onde eles trabalham, se possuem outros imóveis, se são empresários, se viajam com frequência, se existe algum sistema de segurança no prédio, qual o efetivo de funcionários trabalhando, etc. Estas informações, que são passadas de maneira involuntária ou sem a intenção de prejudicar alguém, mas que vão ajudar os criminosos a realizarem um roubo ou até um arrastão no prédio.

O mesmo ocorre quando a pessoa posta nas redes sociais informações que, somadas a outras, habilmente conseguidas através de ligações telefônicas com pessoas próximas ou na empresa, dão subsídios suficientes para que o marginal faça a sua investida.

Ele pode estar buscando mais informações sobre sua família ou sua empresa ou pode usar estas informações para aplicar golpes, como por exemplo, o do falso sequestro, onde o marginal, ao ligar para a vítima, já tem uma grande quantidade de informações que a vítima acaba caindo no golpe, pela quantidade de detalhes apresentados.

De nada adiantam grandes investimentos em tecnologia e equipamentos se as pessoas não estiverem preparadas para enfrentar os engenheiros sociais. Como escreveu Kevin Mitnick, no livro "**A Arte de Enganar**", a verdade é que não existe uma tecnologia no mundo que evite o ataque de um engenheiro social.

Mitinick é o hacker mais conhecido no mundo e usava a maior parte do tempo, cerca de 85%, tirando informações através dos métodos de engenharia social e apenas 15% usando o computador.

Um estudo divulgado pelo instituto norte-americano Gartner prevê que a engenharia social será a principal ameaça para os sistemas tecnológicos de defesas das grandes corporações e usuários de internet daqui a dez anos. Todos são vítimas em potencial.

Infelizmente, estas histórias não são frutos da minha imaginação elas acontecem com muito mais frequência do que possamos imaginar e muitas vezes nós tomamos conhecimento delas através dos jornais.

Portanto, a informação sempre foi e será um bem valioso, não só para as empresas, mas para a segurança das pessoas. Desprezar isso é aumentar o risco de ser surpreendido, de sofrer um duro golpe e até de perder a vida.

Deixar de dar a devida importância aos treinamentos e a conscientização dos funcionários, de todos os escalões, é arriscar-se desnecessariamente.

Acreditar que os sistemas eletrônicos farão tudo sozinho, infelizmente, não dará certo. Todo sistema tem um usuário (humano) que é falho.

A parte mais difícil é conseguir conscientizar as pessoas de que tudo o que ela diz pode ser usado de maneira indevida e agressiva por outras pessoas, podendo acarretar uma perda irreparável.

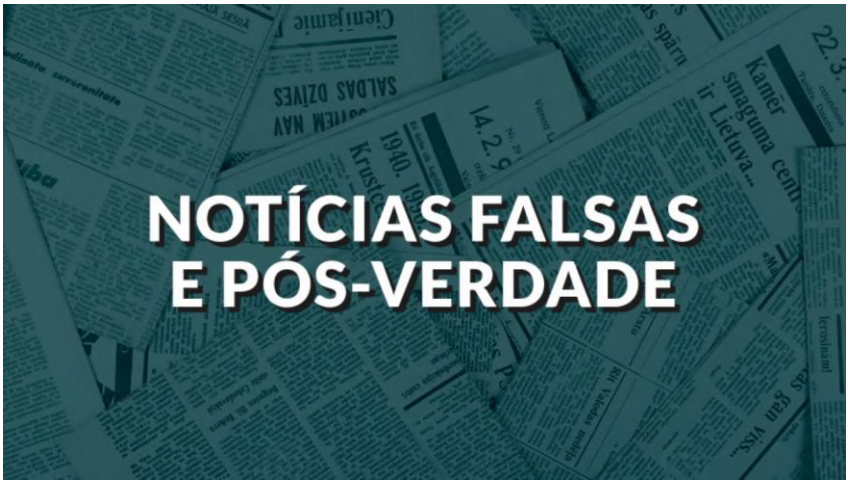
O trabalho de conscientização deve ser realizado de maneira ininterrupta, mantendo as pessoas alertas porque os marginais agem sempre com pessoas desatentas, procuram tirar informações de pessoas faladeiras, que não conseguem ver a importância das informações que eles possuem a respeito de outras pessoas e do sistema de segurança da empresa em que eles trabalham.

Não quero dizer que a pessoa deva viver num estado de paranoia, achando que todos querem tirar informações para prejudicá-lo ou qualquer coisa assim, mas algumas medidas simples devem ser tomadas. Cito aqui apenas alguns exemplos práticos.

- Não dê informações pessoais para alguém que ligou para sua casa ou trabalho, apenas porque disse que era da empresa de telefonia ou do seu banco. Nesse caso é melhor solicitar o telefone da empresa e você ligar para ele.
- Oriente as pessoas de sua família sobre os riscos de passar informações pessoais aos outros, principalmente para estranhos ou de pouca convivência.
- Mantenha os funcionários alertas para que não sejam vítimas dos engenheiros sociais (que tiram informações das pessoas de maneira, aparentemente, despretensiosas).
- Realize trabalhos constantes de conscientização, que pode ser através de palestras, DDS (diálogo diário de segurança), panfletos, pequenas notas no rodapé de algum documento de circulação interna.
- Não comente assuntos relacionados ao trabalho ou sistema de segurança da empresa em locais públicos ou com pessoas que não tenham envolvimento com a segurança.
- Cuidado com as postagens em redes sociais. Hoje em dia elas se tornaram uma ferramenta para garimpar informações de todos os tipos e para todos os fins.

De qualquer forma, a segurança da informação sempre começará e terminará nas pessoas, independentemente das ferramentas que a empresa use para implementá-la. E é justamente quando não se dá à devida atenção às pessoas que o investimento em segurança se transforma em custo.

Lembrem-se alguns exemplos de informações citadas aqui foram tiradas de ocorrência reais. Toda informação é importante, seja no nível estratégico, tático ou operacional da empresa e até as informações domésticas podem ser usadas contra você.



A era da pós-verdade

A internet é a grande difusora de informações e mentiras. Não foi à toa que a palavra pós-verdade foi considerada a palavra do ano (2016) na **Universidade de Oxford.**

Editado pela universidade britânica, anualmente a *Oxford Dictionaries*, departamento da universidade de Oxford, responsável pela elaboração de dicionários, elege uma palavra de maior destaque da língua inglesa.

A de 2016 é “pós-verdade” (“*post-truth*”).

Pós-verdade pode ser conceituada como afirmações, sentenças, ideologias sem qualquer lógica ou até mesmo conexão com a realidade.

Os fatos objetivos têm menor influência que os aspectos emocionais e às crenças pessoais.

As pessoas adotam essa ideologia e as repetem como um mantra sem prestarem atenção nos argumentos contrários por mais válidos, lógicos e fundamentados que sejam, simplesmente ignoram.

Também não se preocupam em checar as fontes, repassando quase que instantaneamente e difundindo uma mentira que pode prejudicar uma pessoa ou uma empresa, tanto faz.

Algumas características da pós-verdade são:

Traz alguma esperança, oferece consolo, resolve problemas complexos com soluções simplistas, juntando-se a isso:

a) uma população que cada vez mais se informa por meio de redes sociais sem contato com as fontes originais;

b) a acirrada polarização política;

c) a rapidez da propagação; e

d) o interesse ideológico e, sobretudo, econômico em maximizar a distribuição e pronto, estão fornecidas as condições para engrossar o caldo da desinformação.

É bom lembrar o conceito de Desinformação, que é uma ação ativa, com a finalidade de confundir, de enganar. Foi criada para este fim.

Pode ser utilizada para aproveitar o estereótipo já existente, especificamente na cultura de um povo com a finalidade de influenciar a opinião das pessoas.

Joseph Goebbels foi ministro da propaganda nazista e é atribuída a ele a frase “Uma mentira repetida mil vezes torna-se verdade”.

Romeu Tuma Junior, ex-secretário nacional de Justiça, publicou em seu livro – **Assassinato de Reputações** (2013), alguns métodos utilizados no Brasil para manchar o nome de empresários ou adversários políticos que se opõem ao governo.

O livro, entre outras denúncias, conta a história de uma maleta francesa, capaz de interceptar ligações telefônicas e os casos de "vazamentos" de informações de maneira proposital e seletiva de escutas arranjadas.

Assim como os vazamentos de informações são realizados com propósitos específicos.

O **Google** e o **Facebook** estão trabalhando já há algum tempo para identificar e bloquear sites com notícias falsas, mas ainda não apresentou os resultados esperados.

Em entrevista ao **Jornal Diário Catarinense** de 08/04/2017, o professor de Jornalismo da Universidade Federal de Santa Catarina (UFSC) e pesquisador de mídia **Rogério Christofoletti** disse que: "Não é à toa, Facebook e outras partes interessadas criaram um fundo de US$ 14 milhões para ajudar as pessoas a distinguir informações falsas.

O sistema corre perigo, referindo-se ao programa que se propõe a melhorar a confiança no jornalismo".

Boatos mentirosos já foram utilizados inúmeras vezes na história mundial. No **jornal Folha de São Paulo**, de 29/04/2017 foi publicado a tradução de um artigo do jornal inglês, ***Financial Times***, no qual cita um memorando interno infame da empresa de cigarros Brown & Williamson, redigido no verão de 1969, apresenta o pensamento do setor muito claramente: "A dúvida é nosso produto". Por que? Porque semear a dúvida "é a melhor maneira de competir com o 'conjunto de fatos' existente na cabeça do grande público. É também o jeito de se criar uma controvérsia." O mantra do "Big Tobacco" (a indústria de cigarros): alimentar a controvérsia.

Esse memorando mostra de forma bastante esclarecedora como se comportam determinados segmentos e hoje observamos estes fatos no meio político nacional, com diversas frases ou ações atribuídas a políticos que são difundidas de maneira inconsequente trazendo prejuízos às suas vítimas.

O pior é que se não fizermos uma checagem, nós também estaríamos sendo enganados por notícias absolutamente falsas, independente da sua ideologia e, por vezes, difundindo-as.

Deputados estão analisando um projeto de lei que pretende tornar crime o compartilhamento ou divulgação de informações falsas ou “prejudicialmente incompletas”. A proposta é do **deputado Luiz Carlos Hauly** (PSDB-PR) que apresentou o projeto de lei 6.812/2017, no qual prevê detenção de 2 a 8 meses e pagamento de multa para quem “divulgar ou compartilhar, por qualquer meio, na rede mundial de computadores, informação falsa ou prejudicialmente incompleta em detrimento de pessoa física ou jurídica”, pois, de acordo com o PL, será considerado crime.

A grande mídia já faz as checagens antes da publicação, mas sabemos que também usam a desinformação para casos de seus interesses.

Alguns sites, como o **www.aosfatos.org www.e-farsas.com** e **www.boatos.org** trabalham para desmascarar as mais absurdas mentiras ou comprovar a veracidade de diversas notícias que rodam pelas mídias sociais.

É certo que ainda estamos longe da responsabilização por notícias falsas, se é que isso ainda poderá existir, pois muitas dessas notícias dependem das crenças e ideologias pessoais.

A responsabilidade é de todos nós que no dia-a-dia compartilhamos notícias sem os mínimos cuidados, pois as notícias podem ser falsas, mas o efeito é real.

Boatos comprometendo a marca ou a reputação de pessoas ou empresas se espalham na internet

Com o crescente uso das mídias sociais, é cada vez mais comum encontrarmos boatos absolutamente falsos denegrindo a imagem de pessoas ou empresas.

O caso mais grave ocorreu no Guarujá (03/05/2014), quando uma mulher foi morta após ter seu nome relacionado a sequestros de crianças e magia negra. O boato foi postado no facebook e a mulher foi espancada e morta por moradores.

As mídias sociais têm causado grandes problemas, não só para as pessoas citadas nestes boatos, mas para grandes empresas também.

Veja o caso noticiado onde a polícia havia fechado um laboratório clandestino de Coca-Cola no Brasil no qual era usada água de bateria na composição da bebida. O boato, de acordo com o site e-farsas.com é falso.

Outro boato falso circulou a pouco tempo sobre Donald Trump, onde ele havia dito que imigrantes brasileiros são porcos latinos. Outra notícia que o site diz ser falsa.

Outro boato bastante difundido foi o do encosto de cabeça, dos bancos dos carros, onde ele poderia ser usado para quebrar o vidro em caso de emergência. Puro boato, segundo o site boatos.org

No livro de Romeu Tuma Junior: Assassinato de Reputações – um crime de Estado (2013) ele demonstra como são tratados os desafetos políticos e os empresários incômodos ao governo Lula e a forma de abalar a reputação destes.

Outro livro que retratou o quanto boatos falsos podem atingir pessoas famosas foi o de Mário Rosa, A Era do Escândalo (2003) sobre a atriz Glória Pires, seu marido Orlando de Moraes e a filha, também atriz, Cléo Pires.

Na área política, o campo é fértil.

A polarização que vemos, desde as eleições de 2014, até agora, não faltaram notícias falsas e tendenciosas de ambos os lados.

Com certeza, eu e você, caro leitor, poderíamos citar outras inúmeras situações de difusão de boatos falsos onde causaram problemas às pessoas envolvidas.

O que há por trás de muitos desses relatos são as características humanas ligadas a interesses financeiros, políticos, de audiência, etc.

Muitas vezes todos nós participamos desses boatos, ainda que seja de maneira absolutamente inocente, como no caso do encosto de cabeça dos bancos dos carros.

De acordo com Carlos Tholt, no livro: Decida com Inteligência (2006) as pessoas possuem predisposições cognitivas, que envolve fatores diversos como o pensamento, a linguagem, a percepção, a memória, o raciocínio e nem sempre as pessoas estão interessadas na verdade.

Essas “notícias” são amplamente divulgas pelo twitter, facebook e WhatsApp e por isso devemos tomar alguns cuidados para não sermos propagadores de boatos falsos que podem causar danos à imagem das pessoas ou até a morte, como no caso da mulher no Guarujá.

Como se prevenir, caso você não queira participar desta rede de boatos falsos.

Uma das maneiras mais rápidas e eficazes é o uso de sites especializados em desmascarar boatos falsos.

Os mais conhecidos são: **www.boatos.org, www.aosfatos.org** e o **www.e-farsas.com**.

Cruzar as informações também traz um bom resultado. Veja se a notícia aparece em outros sites, outras fontes para poder dar credibilidade às notícias recebidas.

A análise de quem está transmitindo a notícia também é muito importante e, por vezes, pode identificar um boato falso.

Veja o caso de pessoas que divulgam notícias sobre políticas, principalmente quando elas são de um determinado partido e está criticando outro, que é oposição ao seu partido preferencial.

Observe que nesses casos o excesso de palavras que agridem o outro é muito grande, acrescentando adjetivos ofensivos. Este detalhe já demonstra possíveis falsidades ou exageros, portanto devemos manter sempre a vigilância epistêmica (ligar o desconfiômetro).

É comum encontrarmos notícias em que o título diz uma coisa e o texto outra, completamente diferente.

Isso mostra que não podemos ficar apenas com a impressão que o título da matéria nos traz. Percebam que isto é muito comum.

No caso das imagens ocorre a mesma coisa, imagens montadas para circular nas mídias sociais são muito comuns também.

Uma forma de analisar as fotografias, por exemplo, é utilizando o próprio google na aba de imagens, onde você pode inserir a imagem suspeita, através do ícone de uma câmera fotográfica e encontrar a mesma imagem com datas antigas, demonstrando que aquela informação recebida é falsa ou ainda encontra-se segmentada, mostrando que ela foi obra de uma montagem a fim de denegrir a imagem de alguém, por exemplo.

A internet é uma tecnologia maravilhosa para quem busca informação e entretenimento, mas também pode trazer grandes transtornos às vidas das pessoas ou às organizações.

No livro Não nascemos prontos – Provocações filosóficas (2006), o professor Cortella escreveu:

“Sem critérios seletivos, muitos ficam sufocados por uma ânsia precária de ler tudo, acessar tudo, ouvir tudo, assistir tudo. É por isso que a maior parte dessas pessoas, em vez de navegar na internet, naufraga....”

Poderíamos acrescentar também – compartilhar tudo.

Esta mesma ideia pode ser usada para disseminar uma “falsa verdade”, criando dificuldades na hora de decidir ou encontrar as fontes originais.

Basta lembrarmos o alemão Paul Joseph Goebbels, que foi o ministro da propaganda nazista e sua célebre frase “***Uma mentira repetida mil vezes torna-se verdade***”.

Para concluir, é sempre bom observarmos algumas pequenas regras, mínimas que sejam, antes de divulgar boatos que podem afetar de maneira negativa as pessoas ou organizações.

Muitas vezes a pratica da empatia é o suficiente.

Vigilância epistêmica

O economista americano, Alvin Toffler dividiu as principais fases do desenvolvimento humano em sociedade de uma forma que ficou bastante conhecida como as três ondas da vida ou do conhecimento. Isto está em seu livro **A terceira onda**, escrito em 1980.

Resumidamente, as ondas foram separadas de acordo com o desenvolvimento humano e suas formas de produção e de convivência.

Em princípio o homem vivia como nômade e quando começou a trabalhar a terra e usar animais no trabalho e na domesticação, passou a trabalhar na terra, cultivando alimento para sua subsistência.

Nessa época (onda) as pessoas dependiam, basicamente, do seu esforço físico e da terra (clima) para sobreviverem.

Mais tarde, bem mais tarde, com o desenvolvimento da indústria as pessoas começam a trabalhar e produzir em grande escala. Nesse período, o que tinha valor eram as máquinas e ainda o serviço braçal, onde se valorizava os que cumpriam as ordens sem questionar (você não é pago para pensar!).

Já na terceira onda, a chamada onda da informação ou do conhecimento, o valor intangível é que tem maior destaque. O trabalhador passa a ter mais valor justamente porque pensa.

São as ideias, a criatividade, a marca, a reputação.... O conhecimento passa a ter mais valor do que o material (os bens).

É nesse contexto, na era (onda) da informação em que estamos vivendo, é que podemos questionar se realmente seria a era da informação ou da desinformação.

Vamos conceituar desinformação a fim de podermos falar a mesma linguagem neste texto.

Desinformação é uma ação ativa, com a finalidade de confundir, de enganar. Foi criada para este fim. Pode ser utilizada para aproveitar o estereótipo já existente, especificamente na cultura de um povo com a finalidade de influenciar a opinião das pessoas.

A propaganda midiática provou sua força em várias ocasiões aqui no Brasil e no mundo, seja elegendo políticos ou acusando empresários, nem sempre de forma honesta, como nós já sabemos.

A força da propaganda já havia sido demonstrada com eficácia por Napoleão.

Podemos recordar, ainda, o ministro da propaganda Joseph Goebbels, que idolatrava Hitler, transformando-o numa marca e as consequências desta ação.

Romeu Tuma Junior, ex-secretário nacional de Justiça, publicou em seu livro – **Assassinato de Reputações**, alguns métodos utilizados no Brasil para manchar o nome de empresários ou adversários políticos que se opõem ao governo.

O livro, entre outras denúncias, conta a história de uma maleta francesa, capaz de interceptar ligações telefônicas e os casos de “vazamentos” de informações de maneira proposital de escutas arranjadas.

Recentemente, a revista Veja (edição 2.436 de 29/07/2015) denunciou o senador Romário (ex-jogador), o qual, segundo a revista, possuía 7,5 milhões num banco na Suíça e que não haveria declarado ao fisco.

Nesse caso, o baixinho decidiu ir buscar o dinheiro que nunca existiu e agora processa a revista, exigindo dez vezes o valor que ele teria na Suíça. A revista já se desculpou por ter publicado recibos falsos.

Os interesses são tão escusos como podemos ver em vários episódios da história que nos faz lembrar a necessidade da vigilância epistêmica.

Vigilância epistêmica significa não acreditar em tudo o que é escrito e dito por aí e, principalmente, achar que não uma segunda intenção no que nos dizem.

É viver ingenuamente.

A vigilância epistêmica é um nome bonito para ligar o desconfiômetro.

Infelizmente não se pode confiar na mídia e em tudo o que é publicado. Na internet não existe critério de classificação da veracidade das informações, o Google indexa todos os artigos, notícias, blogs sem nenhum critério de avaliação.

Por vezes a informação mais técnica, escrita por especialistas será encontrada na sétima ou oitava página classificada na sua busca.

Qual o resultado disso para a nossa cultura? Quais os malefícios que isso pode trazer?

Aumentar a nossa vigilância epistêmica é uma necessidade cada vez mais real num tempo em que grande parte da mídia produz matéria com a intenção clara de desinformar – passar informação falsa de maneira proposital.

Uma Mentira contada mil vezes, torna-se uma verdade.

Joseph Goebbels

A ameaça dos engenheiros sociais

Como atuam os engenheiros sociais, pessoas que sem o uso da força, conseguem obter informações sigilosas para utilizá-las em extorsões.

Existe um jargão que diz que “a corrente da segurança é tão forte quanto seu elo mais fraco”. Um desses elos sempre foi o homem, que poderia ser o mais forte, mas que, normalmente, é o mais fraco.

Apesar de todo treinamento, o ser humano muitas vezes responde aos seus instintos sociais de camaradagem, confiança ou mesmo por pura distração, revela informações sigilosas, respondendo perguntas simples e diretas, que o faz fornecer dados confidenciais. Isso é o que acontece quando as pessoas são vítimas da engenharia social, um conceito cada vez mais comum em conversas empresariais. Trata-se de uma maneira de se obter informações confidenciais sobre determinada pessoa, equipamento, campanha ou empresa, sem o uso da força, apenas com inteligência, técnica, perspicácia e persuasão.

Muitas pessoas associam este termo à informática, acreditando que apenas os que têm acesso a determinados programas e documentos em formato digital está sujeito a este tipo de ataque. Ledo engano.

Frank W. Abagnale, um ex-fraudador americano, conceituou engenharia social como “a arte e a ciência de induzir pessoas a agirem de acordo com seus desejos”. Seus feitos foram tão impressionantes que geraram o filme “**Prenda-me se for capaz**” (2002), dirigido por Steven Spilberg, protagonizado por Leonardo DiCaprio e Tom Hanks.

O fato é que este método de subversão psicológica é cada vez mais usado por todo tipo de pessoa. Veja o que os presos da penitenciária de Bangu I, no Rio de Janeiro, têm feito, através de celulares. Eles ligam para um telefone fixo de qualquer cidade, conversam com a pessoa que atende a chamada (que pode ser uma empregada doméstica) e conseguem extrair informações importantes sobre os donos da casa. A partir destas informações, os bandidos passam a extorquir a família, ameaçando de sequestro e outros crimes caso suas exigências não sejam atendidas. Muitos já foram vítimas deste tipo de extorsão e, infelizmente, muitos ainda o serão.

Outro tipo de engenharia social é praticado via e-mail. O engenheiro social envia uma mensagem informando que detectou um vírus no computador e que para eliminá-lo é necessário instalar um aplicativo anexo. Na verdade, este aplicativo irá espionar todo o conteúdo do PC e deixará uma porta aberta para acessar seus dados.

Estes são apenas alguns exemplos dos métodos utilizados pelo engenheiro social. Para evitar problemas, é preciso alertar as empresas da necessidade de treinamento dos seus funcionários, conscientizando-os do perigo a que estão expostos diariamente.

De nada adiantam grandes investimentos em tecnologia e equipamentos se as pessoas não estiverem preparadas para enfrentar os engenheiros sociais. Como escreveu Kevin Mitnick, em "**A Arte de Enganar**", a verdade é que não existe uma tecnologia no mundo que evite o ataque de um engenheiro social. Mitinick é o hacker mais conhecido no mundo e usava a maior parte do tempo, cerca de 80%, tirando informações através dos métodos de engenharia social e apenas 20% usando o computador.

Um estudo recente divulgado pelo instituto norte-americano Gartner prevê que a engenharia social será a principal ameaça para os sistemas tecnológicos de defesas das grandes corporações e usuários de internet daqui a dez anos. Todos são vítimas em potencial.

Por que as pessoas contam seus segredos?

Mesmo com toda a sensação de insegurança vivida atualmente pela sociedade, muitas pessoas ainda são ingênuas, confiam em desconhecidos e, pior, não sabem avaliar o valor das informações a eles confiadas, normalmente porque não acham que esses dados são importantes.

O engenheiro social é um oportunista com um grande talento para observar as pessoas, avaliando-as para suas investidas.

Ele também não deixa de possuir um espírito empreendedor, arriscando-se para conseguir o que quer. Além disso, usa os sentimentos mais comuns das pessoas como armas a seu favor, como **medo, vaidade, ambição, cobiça, vingança e ira**.

Assim, muitas vezes as pessoas falam mais do que devem por se sentirem injustiçadas, insatisfeitas com a empresa.

Logicamente existem outros motivos, como por exemplo:

• **Vontade de ser útil** – O ser humano, normalmente, procura agir com cortesia, ajudando outras pessoas quando necessário.

• **Busca por novas amizades** – As pessoas sentem-se bem quando elogiadas e ficam mais vulneráveis e abertas a dar informações.

• **Propagação de responsabilidade** – Trata-se da situação na qual o indivíduo considera que ele não é o único responsável por um conjunto de atividades.

• **Persuasão** – Compreende quase uma arte a capacidade de persuadir pessoas, onde se busca obter respostas específicas. Isto é possível porque as pessoas têm características comportamentais que as tornam vulneráveis à manipulação.

Vale observar que o sucesso da engenharia social depende da compreensão do comportamento do ser humano, além da habilidade de persuadir outros a disponibilizar informações ou realizar ações desejadas pelo engenheiro social. Perceba ainda que o medo de perder o emprego ou vontade de ascender na empresa pode resultar na entrega de informação de natureza proprietária. Dessa forma, observa-se que a engenharia social possui uma sequência de passos na qual um ataque pode ocorrer:

• **Coleta de informações** – O engenheiro social busca as mais diversas informações dos usuários como número de CPF, data de nascimento, nomes dos pais, informações sobre os filhos, rotina e manuais da empresa. Essas informações ajudarão no estabelecimento de uma relação com alguém da empresa visada.

• **Desenvolvimento de relacionamento** – O engenheiro social explora a natureza humana de confiar nas pessoas até que se prove o contrário.

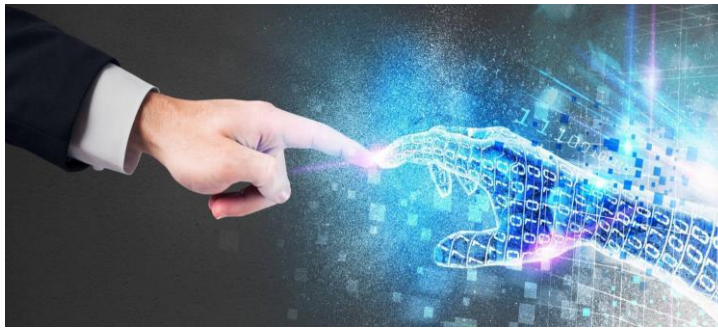
• **Exploração de um relacionamento** – O engenheiro social procura obter informações da vítima ou empresa como, por exemplo, senha, agenda de compromissos, dados de conta bancária ou cartão de crédito a serem usados no ataque.

• **Execução do ataque** – O engenheiro social realiza o ataque, fazendo uso de todas as informações e recursos obtidos.

Quando lemos essas ações praticadas pelo engenheiro social, parece-nos pouco provável que aconteça, mas na prática, isso acontece com mais facilidade do que se imagina. Basta ver o que ocorreu em uma auditoria realizada no início deste ano na Internal Revenue Service (IRS), a Receita Federal americana. As pessoas que trabalham na instituição são treinadas e sabem da importância das informações a que têm acesso.

Mesmo assim, durante uma simulação da auditoria, das cem pessoas envolvidas, incluindo gerentes, 35 delas passaram as informações solicitadas pelos pseudo-engenheiros sociais, informando suas chaves e senhas.

Se com essas pessoas treinadas isso aconteceu, imagine o que não aconteceria em sua empresa. Só a conscientização e o treinamento constante podem evitar o êxito de um engenheiro social.



O avanço tecnológico e a segurança das informações

Estes artigos foram inseridos nesta obra por relacionarem-se diretamente com o assunto em tela, ou seja, a segurança das informações.

Sempre que as facilidades tecnológicas são difundidas, seja através de softwares, aplicativos ou qualquer outro meio de interligação entre aparelhos eletrônicos, e isso é uma tendência, as vulnerabilidades aumentam na mesma proporção.

Cada inovação tecnológica, ainda que esteja legada a outra tecnologia sempre terá como seu “operador raiz” o ser humano e com ele toda a sorte de falhas e negligências próprias do seu DNA, da sua formação, da sua educação para a segurança e conscientização do valor das informações, sejam na esfera pessoal ou profissional.

Edison Fontes, em seu livro **Segurança da Informação – o usuário faz a diferença** (2006) já dizia “A informação, independentemente de seu formato, é um ativo importante da organização. Por isso, os ambientes e os equipamentos utilizados para seu processamento, seu armazenamento e sua transmissão devem ser protegidos. ”

A informação na internet

Nas décadas de 1970 e 1980, além de ser utilizada para fins militares, a Internet também foi um importante meio de comunicação acadêmico.

Para se ter uma ideia de como a internet se difundiu mundo a fora observe o número de dispositivos conectados à rede mundial de computadores.

Em 1984 eram 1.000 computadores conectados à internet, mas teve uma crescente difusão do seu uso a partir de 1990 quando começou a alcançar a população em geral, obtendo o número espantoso de 1 milhão de dispositivos conectados em 1992.

Em 2008 era 1 bilhão e que em 2014 eram 10 bilhões.

A pesquisa realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic), referentes a informações do ano de 2018, mostra que cerca de 46,5 milhões de domicílios têm acesso a internet no Brasil, ou seja, 67% de todas as casas no país têm acesso a rede.
Com a pandemia causada pela COVID-19 esse número aumentou ainda mais.
De acordo com a pesquisa TIC Domicílios de 2019, publicada em maio de 2020, o Brasil possui 134 milhões de usuários de Internet, o que corresponde a 74% da população brasileira, ou seja, em cada quatro brasileiros, três têm acesso à internet.
Hoje, cerca de 51% da população mundial possui conexão à Internet.
Em 1995, era inferior a 1%.
O número de usuários da Internet aumentou dez vezes entre 1999 e 2013.
O primeiro bilhão foi alcançado em 2005.
O segundo bilhão em 2010.
O terceiro bilhão em 2014.
O quarto em 2018.

Com números espantosos de usuários da rede mundial de computadores espalhados no mundo, também chegamos a números astronômicos em relação aos ataques virtuais.

O Brasil sofreu mais de 1,6 bilhão de tentativas de ataques cibernéticos no primeiro trimestre deste ano, de um total de 9,7 bilhões da América Latina.

É o que indicam dados coletados pela Fortinet através de sua plataforma que coleta e analisa incidentes de segurança cibernética em todo o mundo.

(Fonte: **https://olhardigital.com.br/fique_seguro/noticia/brasil-teve-mais-de-1-6-bilhao-de-ataques-ciberneticos-em-tres-meses/100420**)

Dividindo a internet

Para entender esses dados, devemos analisar como a internet é dividida, pelo menos de uma forma didática e simplificada para a nossa compreensão.

Basicamente, podemos dividi-la em três camadas:

A Surface Web, a mais comum, que todos nós navegamos e que utiliza mecanismos de busca (Google, Yahoo!, Bing, etc) consegue indexar.

O Web crawlers, ou bot, é um algoritmo usado para analisar o código de um site que esteja nesta divisão da internet (Surface Web) e ele indexa essas informações para que apareçam nas buscas que fazemos no google, por exemplo.

Lado escuro da web:

A **Deep Web** é a divisão da internet que os motores de busca, como o google, Yahoo, Bing e outros, não conseguem indexar, ou seja, nós não encontramos os sites que estão na Deep Web através destes mecanismos de busca. Eles são invisíveis para nós.

Na Deep Web há uma parte, que aqui nós chamamos de divisão apenas com o intuito de facilitar o entendimento, mas que fica no interior da Depp Web, é a Dark Web.

Na **Dark Web** os usuários conseguem acessos anônimos, e é a parte mais sombria da rede, onde existe de tudo.

Nesses ambientes (Deep e Dark Web) o acesso é através de browser específicos, os mais conhecidos são o TOR e o I2P.

O uso do protocolo The Onion Routing (TOR) é o mais comum e o objetivo é justamente não revelar o seu IP (Internet Protocol) que é o nosso endereço, é um número identificador dado ao seu computador, ou roteador, ao conectar-se à internet.

Na Deep Web estão todos os conteúdos que não podem ser indexados pelos sites de busca e, dessa forma, não está disponível para quem navega na internet (Surface Web).

Mas o que é encontrado na Deep Web?

Encontra-se de tudo, desde informações, pesquisas, debates, opiniões, fóruns, militância política, até crimes de tráfico de drogas, armas, pedofilia, aluguel de hacker, etc.

É nesse ambiente que se desenvolve o jornalismo investigativo, principalmente em países como o Irã, China e Coreia do Norte, os quais costumam controlar as informações disponíveis na internet convencional (Surface Web), de modo que a atividade de jornalistas nestes países é tarefa difícil e até mesmo perigosa.

Também foi nesse ambiente que foi desenvolvida o WikiLeaks com a colaboração de Julian Assange que posteriormente vazou diversos documentos secretos do governo dos Estados Unidos da América.

Lembrando que não há crime em navegar na Deep web ou Dark Web e que a Polícia Federal e ABIN também navegam nessas áreas da internet para identificar criminosos.

Porém o risco para aventureiros neste cenário é muito alto.

Criminosos que agem nesta “divisão” da internet são muito mais hábeis e, portanto, muito mais perigosos.

Já temos problemas suficientes com aqueles que navegam na Surface Web, como por exemplo os crimes de fraudes, golpes de engenharia social, clonagem de aplicativos e sites, sequestro de dados (Ransomware), sextorsão, vírus, etc.

Ou seja, já temos muito trabalho para mantermos a nossa segurança na Surface Web para irmos nos aventurar em áreas muito mais perigosas.

E nesses casos mais comuns, na superfície da internet, uma das proteções mais comuns, além do uso de antivírus e firewall e outros softwares que precisam estar sempre atualizados, inclusive os browsers (Chrome, Explorer, Safari, etc.), as senhas são muito importantes.

Proteja suas senhas

Procure criar senhas com grande quantidade de caracteres e diferentes tipos de caracteres. Não utilize dados pessoais, como nome, sobrenome e datas ou dados que possam ser facilmente obtidos sobre você.

Evite reutilizar suas senhas, sempre que possível.

Troque periodicamente suas senhas.

Não informe senhas via e-mails, telefonemas ou WhatsApp, por exemplo. A sua senha é intransferível e individual.

Na empresa, tudo que alguém fizer usando a sua senha estará sob sua responsabilidade.

Um exemplo simples de senha para dificultar o acesso de terceiros é usar a primeira letra de uma frase simples que você consegue guardar com facilidade.

O meu time ganhou o Brasileirão em 2021, neste caso, a senha seria OmtgoBe2021.

Outro exemplo poderia ser: @ aniversário da minha primeira filha é no mês de julho de 1988. Neste caso a senha seria @admpfénmdjd1988 e é claro que você não vai esquecer.

Conclusão

As tecnologias e a internet vieram para ficar e com elas e a criatividade dos criminosos, nunca estaremos cem por cento seguros, portanto se aventurar em áreas suspeitas é assumir um risco que pode trazer grandes aborrecimentos.

Com o avanço tecnológico, os Smartphones estão cada vez mais potentes, substituindo muitas aplicações do computador e somado a facilidade de acesso, os ataques ficaram mais frequentes e cada vez mais engenhosos.

Portanto, só com atenção aos detalhes é que podemos evitar de cair nas armadilhas dos criminosos.

O avanço tecnológico e do conhecimento humano com foco na segurança

O avanço tecnológico é inevitável, cada vez mais a tecnologia estará apoiando a segurança pública e privada e isto é um fato inexorável.

A produção do conhecimento humano demonstrada através dos avanços tecnológicos, entre outras áreas da ciência, e podem ser observadas em alguns exemplos da nossa história recente.

Basta observarmos que a tecnologia de ouvir músicas via rádio, só ficou totalmente difundida acima de 50 milhões de usuários após 38 anos. A TV levou 13 anos para alcançar o mesmo público, a Internet 4 anos, ipod 3 anos, facebook 2 anos, que hoje tem mais de 1,3 bilhão de usuários.

A rede mundial de computadores, ou Internet, surgiu em plena Guerra Fria. Criada com objetivos militares, seria uma das formas das forças armadas norte-americanas de manter as comunicações em caso de ataques inimigos que destruíssem os meios convencionais de telecomunicações.

Nas décadas de 1970 e 1980, além de ser utilizada para fins militares, a Internet também foi um importante meio de comunicação acadêmico.

O número de dispositivos conectados em 1984 eram 1.000 e com a difusão do uso da internet a partir de 1990 começou a alcançar a população em geral, obtendo o número espantoso de 1 milhão de dispositivos conectados em 1992, já em 2008 era 1 bilhão e que em 2014 eram 10 bilhões. Em 2017 existiam 9 bilhões desses dispositivos ao redor do mundo.

O departamento de inteligência os USA realizou um estudo mostrando que a tendência de que os alunos de hoje terão entre 10 e 14 empregos diferentes até os 38 anos de idade. Há alguns anos atrás a chamada geração “X” jamais imaginaria essa mudança comportamental e que hoje é tão valorizada pelos *Headhunter.*

Em 1900, estima-se que o conhecimento humano dobrava a cada 100 anos, em 1945, o conhecimento dobrava a cada 25 anos. Em 2014 o conhecimento humano dobrava a cada 13 meses. Estima-se que em 2022 o conhecimento humano dobrará a cada 12 horas.

Portanto, fica claro que o desenvolvimento humano e tecnológico ainda está longe de ser imaginado, exceto por cenaristas que prospectam hipóteses plausíveis, de acordo com essas estimativas.

A busca por um sistema de segurança que seja integrado, com a convergência de conhecimentos e tecnologias públicas e privadas com a finalidade de diminuir a criminalidade e a violência que hoje impera no nosso país é uma das preocupações dos estudiosos.

A tecnologia, segundo o professor Carlos Caruso, em seu livro **Guia do Gestor de Segurança Empresarial** (p.15) “é a maior aliada da segurança”, e com base nas estimativas de crescimento deste segmento, fica cada vez mais clara e verdadeira tal afirmação.

Com isso, cada vez mais necessitaremos de profissionais com maior qualificação e preparo para o uso e a distribuição desses equipamentos de forma eficaz, porém uma pratica comum aos projetos que foram implantados em diversas indústrias e até condomínios, têm deixado um “gap”, uma fenda, uma ruptura estrutural em todo o sistema de segurança. É a falta de manutenção.

O conceito de manutenção tem origem militar, visando a necessidade de manter o efetivo humano e de equipamentos nas frentes de batalha.

A falta de manutenção é tão importante quanto a implantação de um sistema eletrônico, que integrado a outros sistemas de automação, aos meios técnicos passivos, ao treinamento do homem de segurança e aos meios organizacionais completam tudo isso e nos lembra o quão verdadeiro é o jargão que diz que a segurança, representada por uma corrente, pode ser medida pelo elo mais fraco. Ou seja, ela sempre se romperá onde for mais fraca, e nesse caso, pode ser a falta de manutenção.

Portanto é necessário pensar o sistema integrado de segurança de modo efetivo, com resultados positivos ao longo do tempo e isso é impossível sem um bom plano de manutenção, já que a finalidade da manutenção é permitir confiabilidade de capacidade de prevenção e resposta da segurança.

Apesar do crescimento exponencial da tecnologia e o crescente conhecimento humano, nada será eficaz por muito tempo sem que ele seja atualizado, treinado, auditado e corrigido.

Além disso, há de se considerar que o criminoso não permanece “estacionado” em relação aos conhecimentos e técnicas, para burlar qualquer tipo de sistema, muito desse conhecimento vem das prisões e também através da mídia.

Para finalizar quero deixar uma frase de Alvin Toffler, um economista e futurista americano, autor do livro **A terceira onda**: “***O futuro é construído pelas nossas decisões diárias, inconstantes e mutáveis, e cada evento influencia todos os outros.”***

inovação e tecnologia na aplicação pratica da segurança privada

Desde a abertura de mercado no Brasil, ocorrida na virada dos anos 80 para os 90, ainda no governo Collor, a competição empresarial se tornou mais difícil, na época, muitas empresas quebraram e muitas ainda patinam na competição globalizada.

A inovação, não só tecnológica, mas de gestão, produção e prestação de serviços ainda vão mudar o mundo, mais rápido do que se imagina hoje.

Apenas para citar alguns exemplos de inovação, podemos observar as mudanças na produção, criadas por Henry Ford, no início do século XX, com sua linha de montagem que revolucionaria a indústria automobilística.

O Cirque du Soleil, com a criação de outro tipo de entretenimento, deixando a competição entre circos e passando para outro patamar, o conhecido Oceano Azul, citado no livro de **A Estratégia do Oceano Azul** (2005).

No livro os autores W. Chan Kim, Renée Mauborgne definem que uma boa estratégia para se chegar ao oceano azul é baseada em três premissas: foco, singularidade e mensagem consistente ao mercado.

Isso é inovação, que nas palavras dos autores, é chamada de "inovação de valor, pois em vez de se esforçarem para superar os concorrentes, concentraram o foco em tornar a concorrência irrelevante, oferecendo saltos no valor para os compradores e para as próprias empresas, que assim desbravaram novos espaços de mercado inexplorados... A inovação de valor é uma nova maneira de raciocinar sobre a execução da estratégia, que resulta na criação de um novo espaço de mercado e no rompimento com a concorrência. Muito importante, a inovação de valor desafia um dos dogmas mais comuns da estratégia baseada na concorrência – o trade-off valor-custo" (A Estratégia do Oceano Azul, pág. 33).

Mas como e porque ocorrem as inovações?

Quem responde a esta pergunta é o físico Clemente Nóbrega, no seu livro **A Intrigante Ciência das Ideias que Dão Certo** (2015) ele cita o Teorema de Ian Morris, que diz que a "mudança é causada pela preguiça, ambição e medo das pessoas que buscam maneiras mais vantajosas e segura de se fazer as coisas. Elas reagem pressionadas por necessidades induzidas por mudanças em suas geografias, e raramente sabem o que estão fazendo" (pág.14).

Ele afirma, e dá vários exemplos, que a geografia no mundo empresarial são comportamentos e atitudes. Empresas que não chance para criar e errar não possuem uma geografia adequada para inovação. Para se ter uma ideia da importância do ambiente de trabalho, Nobrega daria nota sete para a influência do ambiente na inovação e três para o gênio criador da inovação.

A preguiça citada por ele refere-se à comodidade ou busca de facilidades para executar uma determinada tarefa, que é o que todos nós fazemos quando vamos executar alguma coisa, procuramos o modo mais simples e eficaz para realiza-la. Ele também traduz como comodismo.

A ambição é querer ganhar mais e ambição tem custo, o custo do aprendizado por subtração (através dos erros). Muitas empresas por medo ou comodismo deixam a ambição de lado e continuam a fazer o mesmo, o tempo todo.

A produção do conhecimento humano demonstrada através dos avanços tecnológicos, entre outras áreas da ciência, que podem ser observadas em alguns exemplos da nossa história recente.

Basta observarmos que a tecnologia de ouvir músicas via rádio, só ficou totalmente difundida acima de 50 milhões de usuários após 38 anos. A TV levou 13 anos para alcançar o mesmo público, a Internet 4 anos, ipod 3 anos, facebook 2 anos, que hoje tem mais de 1,3 bilhão de usuários.

Mudanças tecnológicas trazem consigo a mudança comportamental e de gestão. O WhatsApp que tem cerca de 1 bilhão de usuários e possui 55 funcionários. Além disso, como diversas empresas utilizam o aplicativo para comunicação e reuniões, alterando seus processos de comunicação, tirando proveito da tecnologia e barateando seus custos com ligações entre outras oportunidades de ações pontuais para cada tipo de negócio.

Com muito mais mudanças e disrupturas com serviços convencionais, o desenvolvimento da revolução 4.0 que trouxe consigo: a inteligência artificial, a robótica, IoT - internet das coisas, os veículos autônomos, a impressão em 3D, a nanotecnologia, a biotecnologia, o armazenamento de energia, mudando as empresas, os negócios e o comportamento das pessoas.

A inovação não é apenas tecnológica, é de gestão, de empoderamento. Ela se refere a forma com que a empresa presta serviço, processa informações, constrói coisas, dá resultado, etc.

De acordo com o professor Fernando Só e Silva e Michel Pipolo de Mesquita, no livro **Competitividade em Gestão de Serviços: Service Level Agreement (SLA) e Service Level Management (SLM)**, 2018 relata que " O conhecimento sobre gestão nos ensina que o conceito de tecnologia está presente na própria definição de serviços: Serviço é o resultado de um processo, composto por entradas, na forma de inteligência humana, informações recursos materiais, intervenção da mão de obra especializada. Tudo isso processado por meio de algum tipo de atividade, resultando, então, numa saída, a entrega do serviço" (pág. 112).

Além disso, os autores complementam "A aplicação de tecnologia no gerenciamento de serviços deve estar relacionada à melhoria da qualidade, aumento da produtividade, redução de custos e interações com o cliente. A percepção de qualidade pelo cliente, muitas vezes baseia-se em alguns indicadores, destacando-se:

Confiabilidade – capacidade de entrega de serviço;

Acuracidade – capacidade de o serviço ser entregue considerando todo o escopo especificado;

Consistência – Estar de acordo com o especificado no contrato, seguindo padronização, tem regularidade e baseado em alguma lógica;

Velocidade – As atividades são realizadas e a equipe demonstra agilidade no cumprimento das tarefas;

Resolutividade – eficiência na capacidade de resolver problemas quando aparecem" (pág. 113).

Muitas empresas têm medo de fazer mudanças em seu modelo de negócios, mas esse cenário de disruptura apresenta também outras oportunidades de geração de novos negócios, inclusive com a abordagem tecnológica, ou seja, tirando proveito das mudanças, usando-as em seu favor.

Algumas empresas de segurança já perceberam essa tendência trazida pela quarta revolução industrial e começam a desenvolver startups para novos serviços e produtos.

A ABSEG – Associação Brasileira de Profissionais de Segurança possui um Comitê de startup que atua diretamente com proposições para novos serviços diretamente ligados à segurança privada.

Outra forma de utilização da tecnologia, nesse caso, para o desenvolvimento das pessoas foi o de aproximação da realidade utilizando um ambiente virtual nos treinamentos possibilita melhorar a curva de aprendizado no que diz respeito às atitudes no cotidiano do trabalho operacional.

Muitas vezes, os profissionais de segurança não têm a oportunidade de treinar além do disparo com a arma de fogo

e este treinamento aprimora e desenvolve o conhecimento profissional.

Ele foi desenvolvido pela **TIS Academy**, sendo que a inovação está em integrar as tecnologias de Realidade Virtual, IoT e algoritmos analíticos com uma metodologia educacional ativa, chamada PBL (Problem Basead Learning) e com a personalização do aprendizado. Esta plataforma permite que o profissional assuma uma postura mais ativa, na qual ele resolve problemas e constrói seu próprio conhecimento.

A plataforma é composta por três partes que se comunicam via tecnologia 3G/Wi-Fi para permitir que os dados dos treinamentos realizados, tanto com o TIS MB (simulador mobile), quanto pelo TIS VR (simulador standard), possam ser enviados e armazenados na plataforma de *cloud computing* (InfoTIS).

Com esse tipo de simulador é possível não só treinar a parte de uso progressivo da força e tiro, mas também as técnicas de segurança como OMD (Observar, Memorizar, Descrever) e IDA (Identificar, Decidir, Agir) de forma escalável.

Sendo este, mais um exemplo de inovação nas nossas atividades operacionais da segurança privada, com baixo custo, melhor treinamento dos profissionais, adequação a contratos que exijam treinamentos constantes e uso de tecnologia.

Para finalizar, quero citar o escritor e futurista Alvin Toffler “O analfabeto do século XXI não será aquele que não consegue ler e escrever, mas aquele que não consegue aprender, desaprender e reaprender”.

Referências

Artigos de Cláudio dos Santos Moretti - CES, ASE.

A ameaça dos engenheiros sociais. Artigo publicado no Jornal da Segurança nº 131 de julho de 2005.

A proteção das informações está nas pessoas Artigo publicado no Jornal da Segurança nº 133 de setembro de 2005.

Vigilância epistêmica. Artigo publicado no Jornal da Segurança nº 255 de novembro de 2015

O avanço tecnológico e do conhecimento humano com foco na segurança. Artigo publicado no Jornal da Segurança nº 262 de junho de 2016.

A importância da segurança da informação. Artigo publicado no site (**https://administradores.com.br/artigos/a-importancia-da-seguranca-da-informacao**) em 08/12/16.

Boatos comprometendo a marca ou a reputação de pessoas ou empresas se espalham na internet. Artigo publicado no Jornal da Segurança nº 276 de fevereiro de 2017.

A era da pós-verdade. Artigo publicado no Jornal da Segurança nº 274 de junho de 2017.

A informação como ativo mais importante do negócio. Artigo publicado na revista Segurança Eletrônica nº 11 de dezembro de 2017.

Cuidados com as informações e as ações do engenheiro social. Artigo publicado no Jornal da Segurança nº 282 de fevereiro de 2018.

Inovação e tecnologia na aplicação pratica da segurança privada. Publicado no site http://revistaseguranca.com.br em 26 de julho de 2018.

A segurança da informação. Artigo publicado na revista Segurança Estratégica nº 314 de outubro de 2020.

A importância da informação. Artigo publicado na revista Gestão de Riscos nº 147 de outubro de 2020.

Outras referências citadas

ABAGNALE, Frank. **Prenda-Me Se For Capaz**. Editora Record. Rio de Janeiro. 2003.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2013 **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.** Rio de Janeiro**,** 2013.

BEAL, Adriana – **Gestão estratégica da Informação.** 1ª ed. São Paulo: Atlas, 2004.

CALTABIANO, Mariana. **Vips - Histórias Reais De Um Mentiroso**. Editora JABOTICABA. 2ª Edição. São Paulo, 2011.

CARUSO, Carlos**. Guia do Gestor de Segurança Empresarial.** Editora do Autor. São Paulo, 2016.

CORTELLA, Mário Sérgio. **Não nascemos prontos! Provocações filosóficas**. **Editora:** Vozes Nobilis 19ª Edição. São Paulo, 2015.

CLEMENTE, Nobrega. **Intrigante Ciência das Ideias que Dão Certo. Editora:** Alta Books; Edição: 1ª, 2015.

FONTES, Edison. **Segurança da Informação: o usuário faz a diferença.** Editora Saraiva. São Paulo, 2006.

KIM, W. Chan; Renée Mauborgne. **A Estratégia do Oceano Azul: Como criar novos mercados e tornar a concorrência irrelevante**. Editora Sextante. Rio de Janeiro. 2018.

MITNICK, Kevin D.; SIMON, William L. **A Arte de Enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação.** Editora Pearson Universidades. 1ª Edição. São Paulo, 2003.

SÊMOLA, Marcos – **Gestão da Segurança da Informação.** 4ª ed. – Rio de Janeiro: Campus, 2003.

SÓ, Fernando e Silva; Mesquita Michel Pipolo. **Competitividade em Gestão de Serviços: Service Level Agreement (SLA) e Service Level Management (SLM).** Editora **www.revistasegurancaeletrônica.com.br**. São Paulo, 2018.

THOLT, Carlos. **Decida com Inteligência**. Editora**:** Thesaurus Rio de Janeiro. 2006.

TOFLER, Alvin. **A terceira onda. Editora:** Editora Record. 1ª edição. Rio de Janeiro, 11981

TUMA, Romeu Júnior. **Assassinato de Reputações. Um Crime de Estado**. Editora Topbooks. 1ª Edição. Rio de Janeiro, 2013.

TZU, Sun. Tradução: André da Silva Bueno. **A Arte da Guerra: Os treze capítulos completos**. Editora**:** Jardim dos Livros. São Paulo, 2008.

Outros livros do autor

Coletânea Gestão de Riscos Empresariais

Este material foi elaborado a partir das diversas publicações pelo autor no Jornal da Segurança, na Revista Gestão de Riscos e do SESVESP com temas relacionados à Gestão de Riscos Empresariais;

Nele você encontrará os métodos de análise de riscos mais utilizados no Brasil, como o método estatístico, Mosler, T. Fine e o método básico Brasiliano.

Os artigos sofreram pequenos ajustes a fim de atualiza-los sobre os temas e, principalmente por conta da publicação da ISO/NBR 31000 e 31010, nos casos dos artigos que foram publicados antes destas normas.

Também foram editados em sequência mais sistêmica com o objetivo de facilitar o entendimento e não na ordem cronológica em que foram publicados.

O objetivo deste material é auxiliar o gestor de segurança iniciante, principalmente, para desenvolvimento e aprofundamento nesta matéria, com conceitos e apresentação de alguns métodos de análise de riscos que possibilitem a elaboração de um plano tático de segurança da sua área de atuação, haja vista que a gestão de riscos é aplicável a qualquer tipo de negócio.

Além do plano de segurança, após a análise e avaliação dos riscos, poderá ser utilizado, de acordo com o negócio e apetite ao risco, para a elaboração dos planos de emergências e/ou de continuidade do negócio.

Coletânea Gerenciamento de Crises Corporativas

Este E-book foi elaborado a partir de diversos artigos publicados no Jornal da Segurança e na Revista Gestão de Riscos e tratam de um tema muito importante para todos os profissionais de segurança, que é o gerenciamento de crises empresariais, o qual está ligado diretamente ao tema do E-book anterior que é a gestão de riscos.

É a partir da avaliação de riscos que a empresa decidirá sobre aqueles riscos mais críticos para o negócio e que necessitam de uma resposta imediata, preparada e treinada para determinados riscos.

Os planos de emergência e de continuidade do negócio buscam diminuir os impactos causados por determinados riscos identificados.

O objetivo desta coletânea é o de contribuir, ainda que modestamente, com o desenvolvimento da área da segurança privada, principalmente aos estudantes de gestão de segurança e aos gestores formados.

A Segurança Privada no Brasil

Este livro tem como objetivo dar diversos esclarecimentos quanto a atividade de segurança privada no Brasil, desde o início, com seu histórico de “nascimento” no contexto regulatório, em 1969 e suas aplicações e mudanças de lá até os tempos atuais, em 2020.

Nesse período a legislação aperfeiçoou a fiscalização e o preparo dos seus profissionais, os vigilantes.

Também, num período mais recente, surge a necessidade de formar o gestor, formalmente, nas universidades.

Observamos que, ainda de maneira formal, os profissionais de segurança, seja na sua atuação de supervisão, gestão ou direção, buscam cada vez mais, o aprimoramento, seja através de cursos de extensão universitária, especializações como pós-graduação e MBA mas também pela busca de certificações que possam comprovar seu aprimoramento neste segmento.

A atividade de segurança privada ainda aguarda a promulgação de uma legislação mais atualizada e que poderá dar início a uma nova era desta atividade tão importante no Brasil.

Com ela, espera-se a diminuição da atividade clandestina, que traz enormes perdas para o mercado de segurança e para os profissionais, realmente habilitados para trabalharem neste segmento.

O Brasil ainda tem muito para desenvolver nesta área e a convergência dos interesses dos empresários, profissionais de segurança e das autoridades que estão trabalhando no sentido de dar as melhores soluções, legislativa, de gestão, de uso de tecnologia e de formação profissional para auxiliar na segurança que a sociedade precisa e merece.

Boa leitura!

Claudio_moretti@uol.com.br