

**UNIVERSIDADE FEDERAL DE MINAS GERAIS
ESCOLA DE CIÊNCIA DA INFORMAÇÃO**

Ana Paula Dias

**A SEGURANÇA DA INFORMAÇÃO EM ASSESSORIAS DE
COMUNICAÇÃO:
UM ESTUDO DE CASO SOBRE A POLÍCIA CIVIL DE MINAS GERAIS**

Belo Horizonte
2015

Ana Paula Dias

**A SEGURANÇA DA INFORMAÇÃO EM ASSESSORIAS DE
COMUNICAÇÃO:
UM ESTUDO DE CASO SOBRE A POLÍCIA CIVIL DE MINAS GERAIS**

Monografia apresentada ao Programa de Pós-Graduação em Ciência da Informação da Escola de Ciência da Informação da Universidade Federal de Minas Gerais, como requisito para a obtenção do Grau de Especialista em Gestão de Informação e Pessoas.

Linha de pesquisa: segurança da informação em assessorias de comunicação

Orientador: Prof. Maurício Barcellos Almeida. Universidade Federal de Minas Gerais

Belo Horizonte

2015

Agradecimentos

A Deus, por me dar forças todos os instantes e não me deixar desistir. Aos meus pais e meu irmão, por serem minha base em tudo o que faço. Aos amigos queridos, por entenderem minhas ausências ao longo do último semestre. Obrigada por compreenderem que a minha prioridade era a conclusão deste projeto. À UFMG, por abrir minha mente através do curso. Aos mestres que tive durante a trajetória. Todos contribuíram de alguma forma para a profissional que foi aprimorada em mim. Ao Maurício, por acreditar em minhas ideias e me dar espaço para criar, colaborando, sempre, com sugestões que enriqueceram. A todos os chefes e demais colegas de trabalho pelo tempo que me foi dispensado, seja pessoalmente, por telefone ou *e-mail*. Tive ajuda de muitas pessoas para minha pesquisa, e cada um de vocês tem uma parcela neste resultado. Não conseguiria sozinha. A mim, porque sei que nada veio de graça. Tudo foi resultado de esforço, perseverança e dedicação. Este trabalho é a conclusão de um ciclo, que sai de cena para dar lugar a outros que virão.

RESUMO

Assessorias de comunicação são setores estratégicos dentro das organizações que desejam serem vistas e lembradas por seu público. Por isso, torna-se necessária a utilização de procedimentos que protejam os dados e permitam mais estabilidade nos processos diários. Tais técnicas de segurança da informação podem evitar o roubo de dados, senhas, criptografias e vazamento de informações essenciais para o andamento dos negócios da empresa. Pensando nesse contexto, o trabalho a seguir discute os temas segurança da informação e assessoria de comunicação. Através de um questionário para avaliação do nível de segurança presente na Assessoria de Comunicação da Polícia Civil de Minas Gerais, observou-se que há falhas em diversos processos utilizados diariamente no setor, mas que alguns deles, no entanto, podem ser resolvidos de forma simples, apenas trabalhando a conscientização dos funcionários para mudanças em suas práticas.

Palavras-chave: segurança da informação; assessoria de comunicação; Polícia Civil de Minas Gerais.

ABSTRACT

Press offices are strategic sectors inside organizations who wish to be seen and remembered by your audience. Therefore, it becomes necessary to use proceedings to protect the data and allow more stability in the daily processes. Such information security techniques can help prevent theft of data, passwords, encryptions and leakage of information essential to the progress of the company's business. Thinking about this context, the following paper discusses the information security issues and press office. Through a questionnaire to assess the level of security in the Civil Police of Minas Gerais Press Office, it was observed that there are flaws in various processes used daily in the department, but some of them, however, can be solved simply, just working the awareness of employees to changes in their practices.

Keywords: information security; press office; Civil Police of Minas Gerais.

LISTA DE ILUSTRAÇÕES

Quadro 1 – Principais definições da ontologia de segurança	13
Quadro 2 – Principais atividades de uma assessoria de imprensa.....	41
Figura 1 – Página de <i>login</i> da rede <i>wireless</i> da Cidade Administrativa de Minas Gerais....	57

SUMÁRIO

1 INTRODUÇÃO	7
2.1 SEGURANÇA DA INFORMAÇÃO	9
2.1.1 O valor da informação e a segurança da informação nas organizações	10
2.1.2 Política de segurança da informação	16
2.1.3 <i>Hackers, crackers</i> e o elo mais fraco	18
2.2 ASSESSORIA DE COMUNICAÇÃO	24
2.2.1 Um pouco de história	24
2.2.2 A comunicação empresarial e a formação da opinião pública	28
2.2.3 O papel do assessor de imprensa e o jornalismo empresarial	31
2.2.4 <i>Marketing</i> empresarial, o fomento à prática de consumo e a gestão de crises.....	36
2.2.5 O que faz uma assessoria de comunicação?	40
3 METODOLOGIA E RESULTADOS	48
3.1 Contexto	48
3.2 Metodologia	49
3.3 Perfil dos entrevistados.....	49
3.3.1 Sexo	49
3.3.2 Idade.....	49
3.3.3 Formação acadêmica.....	50
3.3.4 Tempo em que está na organização (considerado apenas o tempo na Ascom, caso a pessoa tenha passado por mais de um setor)	51
3.3.5 Setor da Ascom onde trabalha.....	51
3.4 Análise dos questionários	51
4 CONCLUSÃO.....	60
REFERÊNCIAS BIBLIOGRÁFICAS	63

ANEXOS.....	65
Anexo A: Questionário aplicado aos funcionários da Assessoria de Comunicação da Polícia Civil de Minas Gerais.....	65
Anexo B: Resolução SEPLAG nº 69/2009	69

1 INTRODUÇÃO

Segurança da informação é um tema em voga nos dias atuais, em todo o mundo. Com o avanço tecnológico, estamos, cada vez mais, à mercê da *internet* e das novas tecnologias, e, conseqüentemente, cada vez mais expostos na rede. Com as organizações empresariais não é diferente. Além das ameaças físicas, a *internet* faz com que as empresas estejam sujeitas a ameaças e vulnerabilidades também no meio *web*, e, por isso, muito tem se pensado em segurança da informação, para proteger os dados internos e resguardar produtos, bens e serviços.

A assessoria de comunicação é um setor estratégico, de inteligência, e que trabalha para promover seus assessorados na imprensa. Normalmente, o setor é ocupado por jornalistas, publicitários, relações públicas, profissionais de *marketing* e de *design* gráfico, que podem atender demandas internas, da própria instituição, ou externas, advindas de veículos de imprensa.

Mas como a segurança da informação é trabalhada nas assessorias de comunicação, um setor tão delicado e sujeito a exposições? Ela está presente no dia a dia dos profissionais desse setor, que lidam diretamente com a informação? Pensando nesse cenário, propôs-se o presente trabalho, com o intuito de avaliar a segurança da informação em assessorias de imprensa. Como objeto para estudo, escolheu-se a Assessoria de Comunicação da Polícia Civil de Minas Gerais (Ascom PCMG), responsável pela comunicação da instituição em todo o estado.

No primeiro capítulo do deste trabalho, sobre segurança da informação, buscou-se apresentar o valor da informação e de sua segurança nas organizações; descrever a importância da presença de uma política de segurança da informação nas empresas, para normatização dos processos; e descrever a engenharia social e outros conceitos relacionados a ela, como *hackers* e *crackers*, além do elo mais fraco no sistema, que é o usuário.

O segundo capítulo, sobre assessoria de comunicação, apresenta um resumo da história do jornalismo empresarial; descreve a importância da comunicação empresarial para a construção da opinião pública acerca de uma organização; discorre sobre a função do assessor de imprensa no cenário do jornalismo empresarial; aborda o *marketing* empresarial

e como ele fomenta a prática do consumo de produtos e ideias de uma empresa; e, por fim, apresenta um resumo sobre as funções de uma assessoria de comunicação.

No terceiro e último capítulo apresenta-se a análise e os resultados obtidos. Para tanto, elaborou-se um questionário para distribuição por todos os funcionários da Ascom a fim de medir, de forma qualitativa, como o setor lida com a segurança da informação, e como os funcionários enxergam o tema em seus ambientes de trabalho. O objetivo inicial do questionário é a identificação de possíveis problemas ou dificuldades que os profissionais enfrentem no seu cotidiano. Mas nada impede que, futuramente, este trabalho seja usado como base inicial para a construção de um projeto de melhoria do setor.

2.1 SEGURANÇA DA INFORMAÇÃO

A preocupação com a segurança da informação existe desde o início da civilização humana, como cita Laureano (2005). No antigo Egito, por exemplo, apenas as castas tidas como superiores podiam acessar os manuscritos da época, e menos pessoas ainda podiam escrevê-los.

Araújo, Azevedo e Silva (2013) citam Simon Singh (2001), em sua obra “O livro dos códigos”, que aponta que, desde o antigo Egito, a informação é tida como algo valioso de acordo com interesses da sociedade, como culturais, econômicos e políticos. A partir daí, pode-se observar uma espécie de batalha entre aqueles que criam os códigos e os que os decifram.

Na sociedade da informação, a partir da industrialização e do aumento da competitividade empresarial, a informação passou a ser considerada como elemento essencial à formação da inteligência competitiva, sendo utilizada cada vez mais de forma estratégica para a tomada de decisão e otimização dos resultados. (ARAÚJO; AZEVEDO; SILVA, 2013, p. 38).

No mundo moderno, a evolução da tecnologia vem tornando cada vez mais fácil a disseminação da informação dentro das organizações e entre organizações. A disponibilidade de informações, somada à competitividade do ambiente de negócios, fez com que a segurança da informação tenha angariado um alto nível de importância. No entanto, ainda que as empresas percebam a necessidade de inserí-la no âmbito organizacional, em geral ainda não há muita clareza sobre como fazê-lo, como apontam Almeida, Coelho e Souza (2010).

A expressão *segurança da informação*, em geral, tem sido associada a sistemas informatizados e aos dados que estes manipulam. Diz respeito a uma série de aspectos associados à Tecnologia da Informação (TI), como por exemplo, controle de acesso a recursos, segurança em comunicação, gestão de riscos, políticas de informação, sistemas de segurança, diretrizes legais, segurança física, criptografia, dentre outros. (KRAUSE; TIPTON, 1997, *apud* ALMEIDA; COELHO; SOUZA, 2010, p. 155).

No entanto, Almeida, Coelho e Souza (2010) ressaltam que a segurança da informação não está ligada somente à proteção em computadores e redes, uma vez que as informações de uma organização não se concentram somente em meios digitais, e a totalidade de

informações de uma empresa não se concentra somente dentro da empresa, podendo se expandir para além de suas paredes.

O restante do presente capítulo está organizado como segue: a seção 1.1 apresenta o valor da informação e de sua segurança nas organizações. A seção 1.2 descreve a importância da presença de uma política de segurança da informação nas empresas, para normatização dos processos. Já a seção 1.3 descreve a engenharia social e outros conceitos relacionados a ela, como *hackers* e *crackers*, além do elo mais fraco no sistema, que é o usuário.

2.1.1 O valor da informação e a segurança da informação nas organizações

A informação é a principal matéria-prima de qualquer organização, algo vital para a construção de estratégias de uma empresa. Por isso é tão importante ter controle sobre ela e tratá-la com cuidado, aponta Laureano (2005).

No entanto, como explanam Araújo, Azevedo e Silva (2013), paralelamente ao fato de serem consideradas o maior bem de uma organização, as informações são, também, alvo de risco constante. Isso porque, com o desenvolvimento das Tecnologias da Informação e Comunicação (TIC) e o crescimento da *internet*, as empresas utilizam cada vez mais a *web* para gerir seus negócios, ampliando, assim, o leque de incidentes possíveis devido a essa exposição.

Laureano (2005) cita o conceito de engenharia da informação, “um conjunto empresarial de disciplinas automatizadas, dirigido ao fornecimento da informação correta para a pessoa certa, no tempo exato” (LAUREANO, 2005, p. 8), para demonstrar o valor da segurança da informação para as organizações.

Como afirma Silva (2010), as organizações possuem informações que permitem a geração de conhecimentos e, através disso, constroem seu diferencial competitivo. Por isso, tanto as informações, como o conhecimento proveniente delas, são considerados patrimônios, ativos importantes das empresas, que devem ser protegidos. Esses estão sujeitos a uma série de ameaças, divididas por Sêmola (2003), citado por Silva (2010):

Naturais – aquelas decorrentes de fenômenos da natureza, como enchentes, terremotos, tempestades etc. **Involuntárias** – as inconscientes, que podem ser causadas por desconhecimento, acidentes, erros etc. **Voluntárias** – as decorrentes de ação de agentes humanos, como invasores, espões, ladrões, incendiários etc. (SILVA, 2010, p. 11).

Araújo, Azevedo e Silva (2013) citam Sêmola (2006) e as propriedades que ele considera indispensáveis para garantir o tratamento de segurança da informação de forma eficaz. São elas:

(1) **confidencialidade** – acessibilidade da informação aos agentes autorizados e inacessibilidade aos agentes não autorizados; (2) **integridade** – possibilidade de alteração da informação para os agentes autorizados e impedimento de alteração para os agentes não autorizados; e (3) **disponibilidade** – acessibilidade da informação apenas aos agentes autorizados a qualquer momento. (SÊMOLA, 2006, *apud* ARAÚJO; AZEVEDO; SILVA, 2013, p. 39).

Essas propriedades estão ligadas às variáveis organizacionais que são identificadas como integrantes de risco em segurança da informação. São eles:

a) **ameaças** – podendo ser internas (ex.: desastres naturais, como inundação; ação voluntária por funcionários insatisfeitos, ou ação involuntária por ingenuidade) e externas (*cracker*, engenharia social, vírus); b) **vulnerabilidades** – considerando as principais como físicas (ex.: ausência de mecanismo de controle de acesso); tecnológicas (ex.: configuração inadequada de *firewall* ou de projetos de *software*) ou humanas (ex.: ausência de conscientização por meio de treinamentos para disseminação de políticas de segurança da informação; e c) **impactos** – resultado de um incidente indesejável (ex.: prejuízo financeiro; danos à imagem). (ARAÚJO; AZEVEDO; SILVA, 2013, p. 39).

Silva (2010) acrescenta que a segurança absoluta é uma utopia, e que as ameaças só se tornam reais, concretas, quando encontram vulnerabilidades que podem afetar a empresa. “Essas vulnerabilidades podem ser físicas (instalações), técnicas (equipamentos e aplicativos), processuais (normas, definições e configurações) ou humanas (comportamentais).” (SILVA, 2010, p. 11). Para que haja a manutenção da segurança da informação em uma organização, é necessário que as vulnerabilidades sejam identificadas de forma correta, para que possam ser definidos meios de anular ou minimizar seus efeitos. Esses meios podem ser preventivos ou corretivos.

Laureano (2005) enumera quatro situações em que a informação é posta em risco dentro das empresas, e que devem ser tratadas com atenção, para evitar e minimizar tais ameaças. São elas o manuseio, o armazenamento, o transporte e o descarte.

A partir dessas propriedades listadas e suas fraquezas, percebe-se que o fator humano é o elemento mais importante quando se pensa em gerir a segurança da informação. Entretanto, também é o elo mais fraco da segurança, devido ao fato de que a execução e suporte dos processos das empresas são responsabilidade das pessoas, exploram Araújo, Azevedo e Silva (2013).

Não adianta a organização investir em sistematização de processos e implementação de tecnologias sofisticadas se os seus funcionários estão insatisfeitos, podendo utilizar informações corporativas de forma intencional e indevida, ou se não estão conscientes das ameaças existentes através do relacionamento interpessoal e da comunicação humana dentro e fora da organização, possibilitando o repasse de informações sigilosas de forma involuntária a pessoas mal intencionadas por meio de engenharia social – técnica considerada como a maior ameaça à segurança da informação nas organizações (...). (MITNICK; SIMON, 1963, *apud* ARAÚJO; AZEVEDO; SILVA, 2013, p. 39).

Almeida, Coelho e Souza (2010) discursam sobre a importância do envolvimento dos funcionários diretamente envolvidos nas atividades cotidianas quando uma empresa pretende implantar a segurança da informação. “Os funcionários envolvidos nas atividades diárias das organizações são a melhor fonte para determinar a importância das informações no contexto corporativo, e, sempre que possível, devem ser convocados a participar ativamente do planejamento da segurança.” (ALMEIDA; COELHO; SOUZA, 2010, p. 158-159).

A adoção de rígidas medidas de segurança tecnológica não surte o efeito desejado se os funcionários deixam portas abertas, computadores com acesso liberado, pastas largadas sobre as mesas ou trocam “confidências” sobre decisões estratégicas de forma promíscua. (SILVA, 2010, p. 12).

Uma opção que ajuda a operacionalizar o trabalho em organizações e tornar mais fácil a proteção da informação é o uso de uma linguagem universal dentro da empresa, que possua significados em conformidade com todos os setores. Tal linguagem pode melhorar o modo como os funcionários aprendem novas práticas e dividem seus conhecimentos com um nível reduzido de imprecisão. Essa linguagem poderia ser operacionalizada por uma ontologia.

O termo ontologia “é originário da filosofia e tem sido utilizado desde os anos 1980 na Ciência da Computação e na Ciência da Informação para designar uma estrutura de organização da informação baseada em um vocabulário representacional.” (ALMEIDA; COELHO; SOUZA, 2010, p. 159).

O Quadro 1 traz as principais definições da ontologia de segurança da informação, elaborado por Almeida, Coelho e Souza (2010), a partir de revisão de literatura.

Organização	(...) é uma entidade social composta por recursos materiais e humanos, a qual possui objetivos comuns, procedimentos sistemáticos para controle de seu desempenho e limites definidos que a separam do ambiente. Pode ser uma instituição pública ou privada.
Atributo de segurança	(...) é uma propriedade atribuída a um ativo, a qual diz respeito a requisitos de segurança. Pode ser um atributo de confidencialidade, de integridade e de disponibilidade.
Ativo	(...) é um bem de propriedade da organização, utilizado para alcançar seus objetivos sociais. Pode ser um equipamento, estoque, imóvel, dentre outros.
Controle	(...) é um procedimento padrão sistemático implementado para atenuar vulnerabilidades, bem como para proteger ativos através de medidas preventivas e corretivas.
Ameaça	(...) é uma possibilidade de dano aos ativos da organização, que afeta os atributos de segurança específicos e explora vulnerabilidades da organização. Pode ser de origem humana ou natural e ter como fonte um evento acidental ou uma ação deliberada.
Vulnerabilidade	(...) é uma situação caracterizada pela falta de medidas de proteção adequadas. (...) possui um grau de severidade associado (por exemplo, crítico, moderado ou baixo). Pode ser (...) de origem administrativa, técnica ou física.

Quadro 1: Principais definições da ontologia de segurança.
Fonte: ALMEIDA; COELHO; SOUZA, 2010, p. 161.

Almeida, Coelho e Souza (2010) destacam que a proposta de uma ontologia em uma organização permite que a segurança da informação seja abordada além dos fatores relacionados à TI, como por exemplo:

i) **questões relativas à cultura organizacional**, como o ambiente de trabalho inadequado, exposição de dados, dentre outros; ii) **questões que envolvem ativos tangíveis da organização**, como segurança e acesso a locais de trabalho (prédios, instalações), segurança física do patrimônio, proteção contra desastres naturais e vandalismo, dentre outras; iii) **questões sobre documentos**, em geral abordadas na Arquivística, como por exemplo: confidencialidade, integridade, confiabilidade; iv) **questões relacionadas ao fator humano**, como: treinamento, conscientização, regulamentação do término de contratos de trabalho, regulamentação de contratos com terceiros, dentre outras. (ALMEIDA; COELHO; SOUZA, 2010, p. 164).

Laureano (2005) assevera que a segurança se constitui de um processo, e que, para alcançá-la, um profissional de segurança deve se basear em analisar o problema, sintetizar uma solução e avaliar a solução. O autor cita o método *PDCA (Plan, Do, Check and Action)*, que pode ser traduzido como Planejar, Executar, Verificar e Agir. Criado na década de 1920 por Shewhart, é o principal processo da administração pela qualidade total. “Ele se baseia no controle de processos, mas pode ser adaptado para ser utilizado em um ciclo de verificação da informação em um processo de segurança (...)”. (LAUREANO, 2005, p. 50). As etapas do método podem ser descritas da seguinte forma:

“**Plan** – definir o que se quer, planejar o que será feito, estabelecer metas e definir os métodos que permitirão atingir as metas propostas. (...). **Do** – tomar iniciativa, educar, treinar, implementar, executar o planejamento conforme as metas e métodos definidos. (...). **Check** – verificar os resultados que se está obtendo, verificar continuamente os trabalhos para ver se estão sendo executados conforme planejados. (...). **Action** – fazer correções de rotas se for necessário, tomar ações corretivas ou de melhoria, caso tenha sido constatada na fase anterior à necessidade de corrigir ou melhorar processos. (...)”. (LAUREANO, 2005, p. 51).

Silva (2010) fala que o grande problema com relação à inserção de procedimentos de segurança em uma empresa é a mudança cultural causada por ela, porque coloca restrições a eventuais “comodidades” às quais os funcionários podem estar acostumados. O autor salienta que essa implementação deve ser feita de forma gradativa, porém contínua e permanente, e que os resultados só aparecem, de fato, a médio e longo prazo.

Como escrevem Almeida, Coelho e Souza (2010), apesar de fundamentais, as práticas de segurança da informação nem sempre são adotadas nas empresas, haja vista o valor do investimento necessário e a não garantia de efetividade das medidas. Um fator importante para que sejam adotadas tais práticas de segurança é a classificação das informações contidas na organização, para saber o que deve ser protegido ou não.

Para que possam lidar com tal complexidade, as empresas utilizam alguns mecanismos de proteção, que se fundamentam em políticas de segurança da informação, análise de riscos e classificação da informação.

Uma **política de segurança** é um plano de alto nível que estabelece como a segurança deve ser praticada e em que nível de segurança – com custos e benefícios inerentes – a organização está disposta a aceitar. A **análise de riscos** consiste na prática de confrontar o valor da informação com os riscos inerentes às perdas, bem como identificar meios de proteção para reduzir riscos. Os procedimentos de **classificação da informação** agrupam entidades similares em categorias, possibilitando implementar medidas de proteção com vistas à garantia de confidencialidade da informação. (ALMEIDA; COELHO; SOUZA, 2010, p. 156).

Com relação à classificação da informação, como aponta Laureano (2005), ela pode ser classificada de acordo com níveis de prioridade, respeitando a necessidade de cada organização e a importância dessa classificação para a conservação das atividades na empresa. O autor cita quatro níveis de classificação:

Pública – informação que pode vir a público sem maiores consequências danosas ao funcionamento normal da empresa, e cuja integridade não é vital; **Interna** – o acesso a esse tipo de informação deve ser evitado, embora as consequências do uso não autorizado não sejam por demais sérias. (...); **Confidencial** – informação restrita aos limites da empresa, cuja divulgação ou perda pode levar ao desequilíbrio operacional, e, eventualmente, perdas financeiras ou de confiabilidade perante o cliente externo, além de permitir vantagem expressiva ao concorrente; **Secreta** – informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital para a companhia. (LAUREANO, 2005, p. 8).

Almeida, Coelho e Souza (2010) apontam que, dentre as iniciativas existentes para lidar com problemas relativos à segurança da informação, ganham destaque as governamentais, as normativas e as tecnológicas. Com relação às duas primeiras, pode-se citar, por exemplo, as estabelecidas pelo ISOO (2003) para a segurança da informação no governo norte-americano:

Algumas regras sobre classificação de documentos são especificadas, como por exemplo: i) apenas pessoas autorizadas podem classificar documentos originais; ii) apenas três níveis de classificação devem ser utilizados: *supersecreto*, *secreto* e *confidencial*; iii) informações que não sejam de interesse da segurança nacional não devem ser inseridas no sistema de classificação. O ISOO (2003) descreve ainda marcas obrigatórias que, aplicadas aos documentos originais, identificam os níveis de segurança a adotar: i) marcas em partes do documento, caso essas

partes possuam diferentes classificações; ii) classificação do documento como um todo, considerando-se o nível de classificação mais restrito atribuído a uma parte do documento; iii) inserção de campos específicos no documento, como por exemplo: *classificado por, razão da classificação e data final da classificação*. (ALMEIDA; COELHO; SOUZA, 2010, p. 156-157).

Com relação às iniciativas de caráter tecnológico, citam-se a norma ISO/IEC-15408-1, de 2005, que “é a principal referência para a avaliação de atributos de segurança em produtos e sistemas de TI, os quais são denominados *objetos de avaliação*.” (ALMEIDA; COELHO; SOUZA, 2010, p. 157). A norma foi criada para auxiliar usuários de TI, que nem sempre possuem meios de avaliar questões relacionadas à segurança. Ela determina um critério comum para avaliação, de forma que o resultado seja significativo para diversas audiências.

O resultado das avaliações (...) auxilia consumidores de TI a decidir se um produto ou sistema atende aos requisitos de segurança. Do ponto de vista do desenvolvedor, a norma descreve funções de segurança que devem ser incluídas no projeto do objeto de avaliação. Finalmente, do ponto de vista dos avaliadores e de outros membros da organização, a norma determina as responsabilidades e ações necessárias para a avaliação desse objeto. (ALMEIDA; COELHO; SOUZA, 2010, p. 158).

Além disso, várias outras iniciativas vêm sendo criadas com o mesmo objetivo, ou seja, propor segurança da informação na área de Tecnologia da Informação: “(...) uma grande diversidade de iniciativas para segurança da informação na área de TI tem sido proposta desde os anos 1980, a saber: roteiros para avaliações e para auditorias (...), listas de verificação (...), diretrizes e critérios (...), listas de termos e taxonomias.” (ALMEIDA; COELHO; SOUZA, 2010, p. 158).

2.1.2 Política de segurança da informação

A política de segurança é um meio que as organizações possuem de padronizar processos, conforme aponta Laureano (2005). Ela deve ser seguida por todo o escopo da empresa, e define de que forma ela irá proteger, controlar e monitorar seus ativos computacionais e as informações manipuladas por eles. A política também estabelece responsabilidades de funções, e deve ser criada de forma integral com as políticas da empresa como um todo, além de suas metas e planejamento estratégico. Para o autor, uma política de segurança pode atender a vários propósitos, como:

1. Descreve o que está sendo protegido e por quê; 2. Define prioridades sobre o que precisa ser protegido em primeiro lugar e com qual custo; 3. Permite estabelecer um acordo explícito com várias partes da empresa em relação ao valor da segurança; 4. Fornece ao departamento de segurança um motivo válido para dizer “não” quando necessário; 5. Proporciona ao departamento de segurança a autoridade necessária para sustentar o “não”; 6. Impede que o departamento de segurança tenha um desempenho fútil. (LAUREANO, 2005, p. 56).

O documento “Política de Segurança da Informação do IPHAN” (Instituto do Patrimônio Histórico e Artístico Nacional), de 2013, apresenta as seguintes definições para segurança da informação e política de segurança da informação:

Segurança da Informação (SI) é a disciplina dedicada à proteção da informação de forma a garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de atuação de uma instituição. A **Política de Segurança da Informação (PSI)**, por sua vez, é o documento formal que orienta e estabelece as diretrizes corporativas para a proteção dos ativos de informação e a gestão da segurança da informação. (BRASIL, 2013, p. 1).

Ainda com relação à política de segurança da informação, Laureano (2005) aponta que as decisões em uma empresa podem ser divididas em três níveis: estratégico, tático e operacional. No nível estratégico, a palavra-chave é valores, um rumo a ser tomado. O bom senso é a ferramenta usada pelos profissionais para a tomada de decisão, em muitos casos.

Já no nível tático, a palavra-chave é padronização de ambiente. “Equipamentos, software, senhas, utilização de correio eletrônico, cópias de segurança, segurança física etc. Tudo isso precisa e deve ser padronizado”, para que não haja “um elo mais fraco na corrente” (LAUREANO, 2005, p. 60).

No nível operacional, a palavra-chave é detalhamento. “A parte operacional da política de segurança vem exatamente para padronizar esses detalhes de configurações dos ambientes (...). Se a configuração está no papel, não há como ser realizada de forma diferente”. (LAUREANO, 2005, p. 61).

A Política de Segurança da Informação do IPHAN, por exemplo, dispõe que os documentos que integrarão a estrutura normativa de gestão de segurança da informação do instituto sejam divididos em três categorias:

A. **Política – nível estratégico:** (...) define as regras de alto nível que representam os princípios básicos que o IPHAN decidiu incorporar à sua gestão de acordo com a visão estratégica da alta direção. Serve como base para que as normas e os procedimentos sejam criados e detalhados. B. **Normas – nível tático:** especificam, no plano tático, as escolhas tecnológicas e os controles que deverão ser implementados para alcançar o cenário definido estrategicamente nas diretrizes da política. C. **Procedimentos – nível operacional:** instrumentalizam o disposto nas normas e na política, permitindo sua direta aplicação nas atividades do IPHAN. (BRASIL, 2013, p. 12).

De acordo com a Política de Segurança da Informação do IPHAN, caso essa divisão de estrutura normativa fosse feita em esquema de pirâmide, os procedimentos estariam na base, as normas no meio e a política no topo.

2.1.3 *Hackers, crackers* e o elo mais fraco

O desenvolvimento de *sites* de redes sociais fez com que surgisse um fenômeno chamado de “hipermobilidade estética dos internautas”, que consiste no aumento da exposição excessiva de informações pessoais no meio *web*, aumentando, assim, os riscos associados à essa exposição, inclusive aqueles relacionados à aplicação do que é conhecido como engenharia social. Ela “(...) é um termo que define algumas práticas utilizadas para obter acesso a informações, por meio de quebra de sigilo de sistemas, organizações ou de indivíduos, utilizando-se de pesquisas, trapaças, ou exploração da confiança das pessoas.” (ARAÚJO; AZEVEDO; SILVA, 2013, p. 37).

A engenharia social pode ser definida como uma técnica utilizada por indivíduos que, através de persuasão, manipulação e influência, conseguem obter informações sigilosas a respeito de uma empresa ou pessoa, utilizando-se ou não de tecnologia para essa obtenção. A informação adquirida pode ser utilizada de forma benéfica, por exemplo, para proteger um sistema, ou maléfica, como forma de ataque.

Araújo, Azevedo e Silva (2013) ainda escrevem que o engenheiro social não tem uma identidade pré-definida. Ele pode atuar em qualquer área, então, qualquer pessoa poderia ser um engenheiro social. A ação desses indivíduos começa a partir da identificação de pontos fracos e vulnerabilidades no ambiente em que pretende agir. A principal forma de

ataque é através das vulnerabilidades dos seres humanos, dentre as quais se destacam a vontade de ser útil, a busca por novas amizades, a propagação de responsabilidades e a persuasão.

Peixoto (2006), citado por Silva (2010), define o engenheiro social como sendo alguém educado, gentil, agradável, simpático, carismático, criativo, flexível, dinâmico, persuasivo e envolvente. Normalmente, são pessoas inteligentes, que vão descobrindo e somando, pouco a pouco, as informações desejadas dos indivíduos ou empresas, para que, assim, possa realizar fraudes. O engenheiro social é capaz de enganar pessoas reunindo talentos de influência e persuasão.

O engenheiro social se baseia em três aspectos para atuar. São eles: motivação pessoal, falta de controle da organização e oportunidade. Desses três, apenas o primeiro não pode ser controlado. Nos outros, é possível estabelecer intervenções para atuar contra a ação dos invasores.

(...) julgamos que o mais importante aspecto relativo à segurança das informações corporativas que merece ser destacado é, inquestionavelmente, a necessidade de capacitação (cognitiva e comportamental) dos usuários dos diversos sistemas da organização, dos gestores e dos manipuladores do capital intelectual da instituição. (SILVA, 2010, p. 21).

É de suma importância que as empresas invistam na área de segurança da informação e adotem tais medidas como forma de proteger informações sigilosas, evitar prejuízos e promover a manutenção do bem-estar da sociedade.

Por algum tempo, os problemas associados a esse campo [a segurança da informação] foram tratados como problemas técnicos que seriam resolvidos apenas por engenheiros e cientistas computacionais, utilizando a linguagem computacional. No entanto, a teoria econômica revelou que muitos dos problemas abordados nesse campo também estão ligados a incentivos econômicos. (CORTEZ; KUBOTA, 2013, p. 758).

O grau de vulnerabilidade cibernética de uma organização está diretamente associado ao número de funcionários com acesso à internet. (CORTEZ; KUBOTA, 2013). Na verdade, quanto mais funcionários possuir, maior será o grau de vulnerabilidade da organização, pela presença de maior número de canais de intrusão, como contas de *e-mail* e número de acesso a *sites* indevidos na *internet*.

De acordo com dados de pesquisas feitas pelo Comitê Gestor de Informática (CGI) em 2009¹, citadas por Cortez e Kubota (2013):

as firmas de maior porte são aquelas mais propensas a adotar mecanismos de segurança de informação e, igualmente, a identificar problemas de segurança. Uma análise simplista poderia inferir que quanto mais se investe em segurança, mais problemas ocorrem. A interpretação dos autores, discutida com os especialistas do CGI, é de que quanto maior a sofisticação tecnológica e o investimento em ferramentas de segurança, maior a probabilidade de identificar e informar os problemas. (...). As ameaças e intrusões cibernéticas são uma realidade da *internet*. Se, por exemplo, um computador sofre ameaça de infecção por vírus, o usuário terá chance de detectar e resolver o problema caso tenha uma ferramenta de antivírus instalada. Caso contrário, o computador será contaminado, independente do conhecimento ou não do usuário. (CORTEZ; KUBOTA, 2013, p. 767).

Cortez e Kubota (2013) citam Cremonini e Nizovtsev (2006) e os dois efeitos sobre a frequência de incidentes que eles descrevem como consequência de qualquer aumento no nível de segurança:

O efeito direto é atribuído às características técnicas de um sistema e diminui a probabilidade de sucesso de um determinado ataque devido ao esforço. Já o efeito indireto, ou de comportamento, diminui a quantidade de esforço que um atacante coloca em tentativas de intrusão, assim diminuindo ainda mais a frequência dos ataques e a perda esperada. Isso sugere que se esse efeito fosse ignorado, o resultado seria a má alocação de recursos de segurança. (...). Sistemas com melhores níveis de segurança têm incentivos mais fortes para revelar suas características de segurança para os atacantes do que sistemas com baixa proteção. (CORTEZ; KUBOTA, 2013, p. 759).

Ataques que envolvem a perda de informação confidencial têm um impacto mais acentuado do que os demais tipos de ataques, explanam Cortez e Kubota (2013).

ARAÚJO; AZEVEDO; SILVA (2013, p. 40) definem *hackers* como “pessoas que invadem os sistemas de computadores sem interesses financeiros, somente pelo desafio”, e *crackers* como “indivíduos que invadem com o intuito de destruir, roubar dinheiro, senhas ou informações”. A palavra *cracker* vem do inglês “*crack*”, que significa “quebrar”. Diante das características amplas de um engenheiro social, ambos poderiam se encaixar nessa definição.

¹ Referência: Comitê Gestor de Informática (CGI) (2010). Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil: TIC Domicílios e TIC Empresas 2009. São Paulo: Comitê Gestor de Informática no Brasil.

De forma sucinta, o engenheiro social percorre as seguintes etapas: 1) reúne todo tipo possível de informações sobre as pessoas, seus perfis, vulnerabilidades relacionadas e as do ambiente; 2) desenvolve relacionamento com a vítima por meio da aproximação e estreitamento de laços, a fim de ganhar confiança e obter acesso aos dados e ambientes; 3) explora todo tipo possível de informação e relacionamento na área de ataque; e 4) executa o ataque à empresa ou ao indivíduo. (LENNERT; OLIVEIRA, 2011, *apud* ARAÚJO; AZEVEDO; SILVA, 2013, p. 41).

Silva (2010) categoriza os engenheiros sociais de acordo com a crueldade e competências técnicas de seus atos:

Os *hackers* ou “*white hat*” – aqueles que após detectarem uma falha na segurança e invadirem uma organização, deixam um alerta para que a incorreção seja eliminada. Praticamente fazem a invasão pela satisfação de vencer o desafio de superar as barreiras existentes. Os *crackers* ou “*black hat*” – aqueles que possuem praticamente o mesmo nível de conhecimento do tipo anterior, mas diferem dele pelos objetivos realmente criminosos, causando qualquer espécie de prejuízo ao invadido e, se possível, obtendo lucro pessoal. Os *phreakers* – aqueles que, essencialmente, manipulam equipamentos e sistemas de telecomunicações para conseguirem as informações desejadas. (SILVA, 2010, p. 20).

De acordo com Lennert e Oliveira (2011), citados por Araújo, Azevedo e Silva (2013), para essa última etapa, o engenheiro social faz uso das seguintes técnicas:

a) *phishing* – invade computadores por meio de vírus e busca as informações de interesse; b) abordagem física – faz chamadas por telefone buscando informações precisas para uso indevido, recolhe documentos e papéis de conteúdo relevante que não foram devidamente descartados, por exemplo, no lixo; c) abordagem psicológica – usa do apelo sentimental e da amizade; d) entretenimento – faz uso das conversas em locais de lazer, quando o indivíduo está distraído, para obter informações de seu interesse e, por fim, e) solidariedade – faz uso da generosidade das pessoas desenvolvendo, por exemplo, campanhas de doação e eventos restritos. (LENNERT; OLIVEIRA, 2011, *apud* ARAÚJO; AZEVEDO; SILVA, 2013, p. 41).

No âmbito organizacional, os *sites* de redes sociais podem ser utilizados pelos engenheiros sociais como forma de obter informações sigilosas sobre a empresa. Araújo, Azevedo e Silva (2013) apontam que o elo mais frágil nos sistemas de segurança da informação são as pessoas que fazem uso deles, sejam os mesmos físicos ou virtuais. Por isso, faz-se necessário que as políticas de segurança da informação sejam valorizadas, e que sejam realizados treinamentos diversos, nos ambientes de dentro da empresa e doméstico, para que os funcionários adquiram consciência das vulnerabilidades e ameaças às quais estão

sujeitos através das técnicas de engenharia social e sua maximização através do uso de redes sociais. Também tornam-se necessários treinamentos para o uso adequado desses *sites* e suas configurações de privacidade e segurança.

Nos ambientes corporativos, para solucionar ou minimizar problemas relacionados à falha humana, é necessário que se estabeleçam normas de conduta, políticas de informação. Uma política pode ser definida como um documento que determina diretrizes a serem seguidas pelos funcionários da organização e aplicadas nos processos da empresa. Uma boa política de informação pode ser executada através do seguinte planejamento: “avaliação de riscos (...); análise do custo/benefício da informação (...); criação de diretrizes e sua formalização em políticas (normas e procedimentos) e sua divulgação; pesquisa contínua para atualização da política (...); programa de treinamento e conscientização dos usuários (...); plano de gestão de crise (incidentes) (...)” (ARAÚJO; AZEVEDO; SILVA, 2013, p. 46).

Sob o ponto de vista de qualquer organização, seja uma agência financiadora com 400 funcionários, seja uma organização de base, quanto mais os emaranhados institucionais estiverem adensados em torno de si, mais as suas ações serão guiadas pelos princípios da engenharia social, o que implica a tentativa de excluir ao máximo outras temporalidades que eventualmente perpassam a organização, e a aproximação a uma forma de pensar que precisa supor o vácuo social para ser bem-sucedida. (VIANNA, 2014, p. 112-113).

Conscientizar os usuários e executar uma política de gestão da segurança da informação tornam-se essenciais para a organização, com o intuito de evitar possíveis ataques de engenheiros sociais e suas consequências.

Nos ambientes organizacionais, faz-se necessária a implantação de políticas de segurança da informação, que atendem tanto para a capacitação dos usuários, configuração e uso correto de ferramentas e para a preservação da privacidade, quanto para a conscientização acerca das vulnerabilidades e ameaças existentes no relacionamento interpessoal e na comunicação humana, principalmente no ambiente virtual, bem como acerca dos comportamentos de prevenção e tais ataques de engenharia social. (ARAÚJO; AZEVEDO; SILVA, 2013, p. 53).

É possível estabelecer alguns níveis de barreiras para dificultar ao máximo a atuação de um engenheiro social. Silva (2010) lista as seguintes:

Barreiras físicas (portas, cadeados, trancas); controle de acesso (estabelecimento de senhas, perfis de usuário e registro de acesso realizado); classificação das informações (grau de sigilo); uso de processo

de codificação e autenticação (criptografia, certificação digital) das informações que circulam na rede da organização; armazenamento distribuído das informações organizacionais; e realização periódica de cópias de segurança (*backup*). (SILVA, 2010, p. 21).

A engenharia social envolve em grande medida um procedimento lógico em torno de formulações linguísticas.

De acordo com a lógica da engenharia social, um bom planejamento permite não apenas um projeto estruturado, como também um maior *accountability* [responsabilização]. A matriz torna-se a referência contra a qual se avalia o projeto, e dentro do mundo do desenvolvimento há vários modelos utilizados. (VIANNA, 2014, p. 102-103).

Cortez e Kubota (2013) defendem a hipótese de que as empresas que adotam mecanismos de defesa e aderem à segurança da informação são mais propensas a identificarem mais tipos de problemas de segurança. Porém, isso ocorre não por falta de eficiência dos investimentos obtidos, e sim pelo fato de que, por possuírem um sistema sofisticado de defesa, as empresas estão mais capazes de identificar problemas relacionados à segurança. Os autores acrescentam dizendo que investimentos em defesa cibernética ampliam as chances de identificação de um problema de segurança, permitindo maiores chances de resistência das empresas, de forma a evitar prejuízos maiores.

2.2 ASSESSORIA DE COMUNICAÇÃO

A comunicação empresarial se baseia em um tripé onde o jornalismo, a propaganda e *marketing* e as relações públicas têm o mesmo peso estratégico, como citam Lorenzon e Mawakdiye (2011). Quando as primeiras formas de jornalismo empresarial surgiram, não tinham as mesmas funções que exercem hoje nas empresas. Mas, com o passar dos anos, as organizações foram percebendo que a assessoria de comunicação é um setor essencial em seu escopo, porque, além de englobar várias áreas, prepara as empresas para lidarem com a imprensa, ajuda na gestão de crises e no planejamento de diversas ações.

O restante deste capítulo está organizado da seguinte forma: a seção 2.1 apresenta um resumo da história do jornalismo empresarial; a seção 2.2 descreve a importância da comunicação empresarial para a construção da opinião pública acerca de uma organização; a seção 2.3 discorre sobre a função do assessor de imprensa no cenário do jornalismo empresarial; a seção 2.4 aborda o *marketing* empresarial e como ele fomenta a prática do consumo de produtos e ideias de uma empresa; e, por fim, a seção 2.5 apresenta um resumo sobre as funções de uma assessoria de comunicação

2.2.1 Um pouco de história

Os primeiros indícios de jornalismo empresarial surgem nas cartas circulares das cortes da dinastia Han, fundada na China em 202 a.C. por Liu Pang, como aponta Rego (1986b). Assim, essa modalidade de comunicação teve suas origens nos primórdios do uso do papel, já que foi no período de domínio dessa dinastia na China que foram fabricadas as primeiras folhas de papel, através da filtragem de fibras vegetais da amoreira e do bambu.

Ainda considerando-se tais documentos como os pioneiros do jornalismo empresarial, pode-se dizer que a modalidade surgiu em uma época de grande progresso econômico e cultural, pois foi durante os 418 anos da dinastia Han que a China teve aumentado o seu comércio com o Oriente Médio, o que ocasionou em grande desenvolvimento econômico. Nessa mesma época, a escultura, a pintura e a poesia alcançaram posições de grande

importância; o budismo foi introduzido no país, advindo da Índia; e o taoísmo foi estabelecido oficialmente.

Lemos e Del Gaudio (2003) apontam que o termo mais conhecido para designar veículos de empresa é *house organ*. Essa expressão americana pode ser usada para jornais impressos e demais publicações produzidas pelas empresas, para se comunicarem com seus públicos interno e externo. Partindo-se desse pressuposto, “as cartas comerciais que circulavam na Europa do século XVI, consideradas precursoras do jornalismo, também poderiam ser tomadas como os primeiros *house organs*.” (LEMOS; DEL GAUDIO, 2003, p. 256).

De acordo com Rego (1986b), o verdadeiro e definitivo aparecimento do jornalismo empresarial se deu no período da revolução industrial, ocorrida entre meados do século XVIII e o início do século XX. Foi um período com grandes mudanças sociais em decorrência do desenvolvimento tecnológico registrado na Europa nessa época.

Com o avanço tecnológico e industrial, pequenas indústrias rurais e domésticas da Inglaterra, e, depois, também de outros países, começaram a desaparecer. O crescimento das indústrias trouxe uma ruptura nas relações que existiam entre empregados e empregadores. Os contatos pessoais e de família passaram a dar lugar a relações contratuais e impessoais, e ficou difícil para o operário enxergar e compreender seu lugar em relação à totalidade das empresas.

A partir daí, começaram a surgir ideias de pessoas que acreditavam que uma das maneiras de resolver essas contradições internas seria a criação de jornais e revistas para os funcionários, com o objetivo de familiarizá-los com seus interesses e diminuir as distâncias entre a administração das empresas e a base operária.

Rego (1986b) aponta que, além dos motivos internos, outro fator que ocasionou o surgimento de jornais de empresas foi o fato de que, com as facilidades de produção estabelecidas na revolução industrial, houve um aumento de concorrência. As empresas tiveram, então, que ampliar seus mecanismos de comunicação, para se tornarem mais conhecidas e ganharem o público. “Assim, surgiram as raízes dos dois tipos fundamentais de publicações de empresa: as externas (destinadas aos consumidores, acionistas, representantes, distribuidores) e as internas (destinadas aos funcionários).” (REGO, 1986b, p. 18-19).

Em meados do século XIX ocorreu um grande avanço tecnológico da indústria de comunicações, facilitando e barateando a produção de jornais, o que abriu novos horizontes para os campos de impressão e editoração. Com isso, foram ocorrendo mudanças gradativas e que melhoraram significativamente os processos, com novas formas de impressão, maquinário e novas fontes de matéria-prima de papel. Mais tarde, o fortalecimento de movimentos sindicais nos Estados Unidos e na Europa também contribuiu para o crescimento do jornalismo empresarial.

No âmbito da tendência da empresa à organização e à estruturação dos serviços, as publicações passaram a ser instrumentos de comunicação, servindo tanto para a comunicação da comunidade operária com os centros de decisão como para a da administração com a base, aprimorando o sistema operacional da empresa. As publicações empresariais tornaram-se, aos poucos, independentes dos motivos que levaram à sua criação, transformando-se em instrumentos do sistema empresarial destinados a favorecer o aumento de produção e a obtenção de maiores lucros, como os demais. (REGO, 1986b, p. 20).

Lemos e Del Gaudio (2003) explanam que no fim do século XIX, as publicações de empresas começaram a se difundir com mais frequência, sobretudo nos Estados Unidos e na Europa. A intenção era de contraposição à imprensa sindical, e de facilitação à transição de operários que saíam do campo para as grandes indústrias onde ainda não conseguiam se identificar.

Rego (1986b) aponta que, a partir de 1888, começaram a surgir, de forma regular e em vários países, os jornais de empresa, em número e prestígio crescentes. No entanto, a I Guerra Mundial fez com que esse progresso fosse interrompido. Após o seu término, porém, houve uma explosão de jornais e revistas empresariais. Em 1929, a crise econômica decorrida da quebra da bolsa de Nova York fez com que, novamente, o progresso do jornalismo empresarial desse uma diminuída.

Rego (1986b) argumenta que, na II Guerra Mundial, ocorreu um processo semelhante ao que ocorrera com a I: uma parada no crescimento durante os conflitos, e um renascimento dos jornais de empresa após esse período. Atualmente, o jornalismo empresarial é uma realidade em quase todos os países do Ocidente.

A maioria dos dirigentes de empresa acredita que, em momentos de crise, o jornal interno ou qualquer outra publicação mantida pela firma devem estar entre os primeiros cortes de despesa a serem efetuados. (...) o jornalismo empresarial continua a ser encarado como “artigo supérfluo” por grande parte dos empresários, que ignoram que é exatamente nos momentos de

crise que essa atividade se revela mais útil para as empresas. Nesses períodos, as relações internas com os empregados ficam mais difíceis, conflitos surgem e precisam ser superados, e as publicações internas são arma de grande valor para resolver os problemas. Da mesma forma, nos momentos de dificuldade, os públicos externos precisam ser tranquilizados e alertados para as possibilidades de se vencer a crise. Novamente, as publicações empresariais tornam-se da maior utilidade, muito mais do que quando as coisas caminham normalmente e não existe a necessidade de estímulos excepcionais para manter a estabilidade dos negócios e do sistema. (REGO, 1986b, p. 22).

Lemos e Del Gaudio (2003) apontam que o primeiro jornal de empresa no Brasil surgiu em 1926, publicado pela multinacional General Motors. Porém, somente a partir da década de 1960 as empresas nacionais começaram a criar jornais em número significativo.

Como cita Rego (1986b), no Brasil, o jornalismo empresarial teve início muitos anos após seu aparecimento e expansão nos Estados Unidos e na Europa. Essa especialidade jornalística só foi inaugurada no país 100 anos após o seu início nos Estados Unidos. Isso pode ser explicado devido ao fato de que o processo de industrialização no Brasil foi atrasado em relação aos Estados Unidos e a maior parte dos países da Europa. “Nossa “revolução industrial” praticamente só teve início em 1930, quando a revolução política ocorrida naquele ano começou a dar prioridade ao setor industrial, ao contrário do que havia ocorrido até então.” (REGO, 1986b, p. 26).

De acordo com Lorenzon e Mawakdiye (2011), o modelo de jornalismo empresarial utilizado pelas organizações brasileiras foi definido entre as décadas de 1940 e 1960, quando o país se encontrava em um surto de industrialização pós Segunda Guerra Mundial (1939-1945). Os jornais empresariais brasileiros foram trazidos pelas corporações norte-americanas, e se tornaram produtos híbridos, que juntam jornalismo, *marketing* e relações públicas, assim como os vindos dos EUA.

O modelo de jornal empresarial americano faz o que se pode chamar, como dizem Lorenzon e Mawakdiye (2011), de matar “vários coelhos com uma única cajadada” (LORENZON; MAWAKDIYE, 2011, p. 55), porque trabalham a venda do produto e a comunicação na empresa. Por isso, o modelo foi adotado, também, pelas empresas de origem europeia e pelas brasileiras.

De acordo com Rego (1986b), também podemos citar o crescimento das Relações Públicas como um fator associado ao crescimento do jornalismo empresarial no Brasil. De acordo

com o autor, apenas em 1951 apareceu o primeiro departamento de Relações Públicas em âmbito nacional no Brasil. Outro fator que pode ser citado como motivo para o atraso dos jornais de empresa em nosso país é a demora com que recebemos avanços tecnológicos nas artes gráficas e editoriais. “Dessa maneira, foi apenas durante os anos 1940 e 1950, quando também se desenvolveram as indústrias, as Relações públicas e a tecnologia no setor editorial, que o jornalismo empresarial começou a firmar-se no país.” (REGO, 1986b, p. 27).

A partir dos anos 1970, as assessorias de imprensa desenvolvem-se tanto nas empresas privadas como em órgãos de governo, com os esforços voltados para favorecer a publicação de notícias sobre a expansão da economia e diminuir o peso de eventuais informações negativas. (LEMOS; DEL GAUDIO, 2003, p. 257).

Como aponta Rego (1986b), as Relações Públicas dividiram os públicos da empresa em três grandes grupos, e deram a cada um deles um canal próprio de comunicação, descritos a seguir.

O público interno, constituído por empregados, agentes, vendedores e todo o pessoal ligado diretamente à empresa, ficou com as suas publicações internas; as publicações externas foram destinadas aos acionistas, consumidores reais e consumidores em potencial, distribuidores e representantes; e, com base na suposição de que muitas informações relativas à empresa, como sua organização, história, produtos, vendas, expansão e programas interessam tanto a consumidores, acionistas, distribuidores como a vendedores e empregados, surgiu um público misto, que ganhou, conseqüentemente, uma publicação mista (interna/externa). (REGO, 1986b, p. 31).

Lemos e Del Gaudio (2003) escrevem que, a partir dos anos de 1980, o jornalismo empresarial no Brasil deu uma guinada. Isso pode ser atribuído à industrialização e à organização dos trabalhadores, que se fortaleceu através do movimento sindical no país.

2.2.2 A comunicação empresarial e a formação da opinião pública

Uma empresa pode ser descrita como uma unidade socioeconômica voltada para gerar bens econômicos, através da relação entre produtor e consumidor, e que também objetiva desempenhar um significativo papel no contexto social, como aponta Rego (1986a).

É de alta relevância o papel formador da empresa, dentro dos sistemas políticos, sua contribuição social, por meio da geração de empregos, descoberta de processos, avanços tecnológicos, enfim, seu papel de vanguarda na elaboração de estratégias, produtos e serviços que resultam em progresso. Quanto à sua natureza econômica, é bom enfatizar que, graças à produção de bens e serviços para uma relação de troca, a empresa cria as condições para se viabilizar. Conciliando aspectos sociais e econômicos, a organização ajusta-se ao escopo para o qual foi idealizada. (REGO, 1986a, p. 13).

Lidar com a opinião pública não é algo trivial. Ela “é a formação de um senso crítico e uma opinião de públicos distintos, seus líderes de opinião e os seus seguidores.” (TUZZO, 2013, p. 19). A autora defende que é importante desenvolver um trabalho de propagação do que se quer repassar para o público que se pretende atingir. Cada grupo que se deseja alcançar deve ser estudado.

Semelhante à empresa, a comunicação é um sistema aberto. “Como sistema, a comunicação é organizada pelos elementos – fonte, codificador, canal, mensagem, decodificador, receptor, ingredientes que vitalizam o processo.” (REGO, 1986a, p. 15). Esse processo, segundo o autor, é dividido em duas partes: a primeira é a transmissão da mensagem, e, a segunda, a recuperação que a fonte necessita para o controle da comunicação.

A aplicação de um modelo de comunicação calcado na cultura organizacional influi decisivamente sobre a eficácia geral da empresa. Como técnica, a comunicação direciona naturalmente seus estudos para a procura de mensagens adequadas, corretas, oportunas, claras, concisas, precisas, que possam ser assimiladas sem ruídos pelos participantes organizacionais. Para atingir tal meta, a comunicação procurará ajustar seu discurso, estudando as habilidades e a complexidade e/ou simplicidade dos conteúdos, a oportunidade e regularidade dos fluxos, o tamanho dos grupos. (REGO, 1986a, p. 16-17).

Tuzzo (2013) ressalta que, apesar de a grande maioria das pessoas acreditar que a opinião pública só se constrói a partir das veiculações midiáticas, ela se dá, também, a partir da construção de um senso crítico.

Pensar em Assessoria de Comunicação significa pensar na construção da opinião pública pelos sistemas de comunicação, destacando o papel dos Jornalistas, dos Relações Públicas e dos Publicitários no processo, e o caráter multidisciplinar da comunicação. Além disso, destaca-se a relação entre as Assessorias de Comunicação e os meios de comunicação de massa para a formação da opinião pública, pois a mesma só pode se formar se o determinado público tiver conhecimento dos assuntos sobre os quais

deva pensar. Ninguém pode formar opinião sobre o que não conhece. (TUZZO, 2013, p. 20).

Para ajustar seu discurso, Rego (1986a) aponta que a comunicação empresarial reúne diversas áreas, dependentes entre si, para promover o efeito desejado.

(...) em processo de compreensão, multidisciplinar, aparecerão permeados nas mensagens de comunicação fundamentos da Linguística, de Sociologia, Antropologia, Ética, Direito etc. A comunicação é, portanto, uma área multidisciplinar, mediando os interesses dos participantes, os interesses da empresa, enquanto unidade econômica, e os interesses da administração. Essa grande característica do fenômeno comunicacional – de mediação de objetivos – mostra sua magnitude e importância para o equilíbrio do microclima interno. Na outra ponta do sistema, estão as vertentes comunicativas, ajustando a identidade empresarial ao meio social, processo que engloba as tarefas clássicas e bem definidas de Relações Públicas, Publicidade, Jornalismo, Editoração, Identidade Visual e os modelos de sistemas de informação. (REGO, 1986a, p. 17).

Como cita Rego (1986a), alguns poderes legitimam a empresa, e a comunicação é um poder que, apenas por existir, gera influências. Ela transfere, de forma simbólica, ideias entre interlocutores.

A comunicação, como processo e técnica, fundamenta-se nos conteúdos de diversas disciplinas do conhecimento humano, intermedia o discurso organizacional, ajusta interesses, controla os participantes internos e externos, promove, enfim, maior aceitabilidade da ideologia empresarial. Como poder expressivo, exerce uma *função-meio* perante outras *funções-fim* da organização. Nesse sentido, chega a contribuir para a maior produtividade, corroborando e reforçando a economia organizacional. (REGO, 1986a, p. 17).

Tuzzo (2013) destaca que, no planejamento integrado da comunicação, a publicidade e a propaganda recebem destaque. “(...) a propaganda é a manipulação planejada da comunicação, que por meio da persuasão visa promover comportamentos em benefício do anunciante. É como se ela tentasse vender para quem não quer comprar.” (TUZZO, 2013, p. 36). A autora ressalta que a opinião pública vende muito mais do que produtos, mas também ideologias, que geram identificação do público-alvo com determinado objeto, produto ou serviço, além de lucros.

2.2.3 O papel do assessor de imprensa e o jornalismo empresarial

Um episódio ocorrido em 1882 tornou-se um caso emblemático. Foi quando um empresário norte-americano, William Henry Vanderbilt (1821-1885), foi entrevistado por um repórter no jornal *The New York Times*, que pedia esclarecimentos acerca da paralisação dos serviços ferroviários prestados por sua companhia. William respondeu ao repórter: “O público que se dane”. Com isso, tornou-se uma figura representativa de uma época em que os dirigentes de instituições queriam distância de jornalistas, e preferiam que eles não existissem. Atualmente, essa realidade parece incompatível com a que vivemos, como cita Monteiro (2003).

Hoje, o que observamos é uma verdadeira disputa pela visibilidade midiática. O que existe é o que está na mídia. Publicizar, tornar públicos acontecimentos considerados relevantes, passou a ser uma das mais importantes estratégias adotadas pelos diversos campos sociais para obter aprovação da sociedade e garantir sua legitimidade. No mundo contemporâneo, o saber fundamentado na autoridade “daquele que fala” passou a ser legitimado por “aquele que ouve”, a opinião pública. (MONTEIRO, 2003, p. 140).

Monteiro (2003) fala sobre o campo dos *media*, expressão que pode ser utilizada para definir o “espaço de mediação mobilizado pelos diversos campos sociais para comporem seus objetivos e interesses” (MONTEIRO, 2003, p. 141). O autor argumenta que esse campo tem sido mobilizado por diversas instituições para promover acontecimentos e produzir notícias para divulgação na mídia. Com isso, “as instituições inserem-se no espaço público, construindo não apenas uma representação de si mesma (mais conhecida por “imagem institucional”), como também a realidade do campo em que atuam.” (MONTEIRO, 2003, p. 141).

Lorenzon e Mawakdiye (2011) afirmam que a assessoria de imprensa é algo que se tornou imprescindível nos dias de hoje, devido à demanda do mercado e a complexidade das organizações atuais.

Já não basta para as empresas investirem em publicidade para elevar o volume de vendas, nem em *marketing* e em relações públicas para consolidarem uma imagem positiva junto da opinião pública. São ambos universos marcados pela retórica e pela indução e operam fora do campo da verificabilidade, que se tornou uma exigência das sociedades modernas. (LORENZON; MAWAKDIYE, 2011, p. 12).

Quanto ao cargo de assessor de imprensa, Brandão e Carvalho (2003) citam que, de forma tradicional, as funções de assessoria são executadas por profissionais que desempenham funções de relações públicas nas empresas. Assim o é na Europa e nos Estados Unidos, onde, para exercer tal função, o funcionário não precisa ser, necessariamente, jornalista, publicitário, relações públicas, ou ter qualquer outra formação.

Já no Brasil, como afirmam Brandão e Carvalho (2003), a função de assessor de imprensa passou a ser defendida a partir de meados da década de 1980, sobretudo por um grupo de profissionais atuantes na Federação Nacional dos Jornalistas (Fenaj) e nos sindicatos. Esse grupo defendia a função e tentou, por várias vezes, aprovar, junto ao Congresso Nacional, um projeto de lei que determinava que somente jornalistas poderiam ocupar tal cargo.

A mudança não foi por acaso, nem desinteressada. Com o fim da ditadura militar no Brasil, a função de assessor, até então ocupada por outros profissionais, podia e precisava legitimar-se para ser condignamente ocupada pelos jornalistas. Afinal, era mais bem remunerada do que o cargo de repórter nos jornais, menos estressante e a demanda no mercado aumentava a cada dia com o retorno à democracia. (BRANDÃO; CARVALHO, 2003, p. 200).

Em 1986, como explicam Brandão e Carvalho (2003), a Fenaj lançou, no Congresso Nacional, o *Manual de assessoria de imprensa*, que determinava as funções de jornalistas, publicitários e relações públicas. Portanto, pode-se dizer que os motivos que defendiam os direitos dos jornalistas em assessorias de imprensa foram econômicos, em função do curso do mercado.

Monteiro (2003) fala que a divulgação de assuntos de instituições na mídia tem um caráter intencional e negociado, o que deixa claro que só é divulgado aquilo que a instituição acredita ser importante e interessante ser noticiado. Além disso, as empresas também se utilizam de estratégias para que esse acontecimento passe a ser de domínio público. A autora cita alguns motivos que comprovam essa constatação: o primeiro é o fato de que a maioria das instituições tem a intenção de se mostrar, junto à imprensa, como uma referência em seu campo de atuação, naquilo em que ela faz. Em segundo lugar, aparece o fato de que nem tudo o que acontece nas instituições vira notícia na imprensa. Em terceiro lugar, vem o fato de que a produção da notícia institucional envolve interesses e campos distintos, que podem ser divergentes ou convergentes. Há casos em que, diante de um assunto polêmico, a empresa prefira se omitir. E há casos em que, quando há o interesse em divulgar algo, o assunto é transformado em notícia.

Monteiro (2003) cita a célebre frase de Amos Cummings (1838-1902), ex-editor do jornal *The New York Sun*, que diz: “se um cachorro morde um home, não é notícia, mas, se um homem morde um cachorro, é notícia”, para reforçar que, em geral, o que se torna notícia é aquilo que foge do senso comum, da realidade cotidiana de todos, o que rompe a rotina. A autora cita os atributos gerais que conceituam a notícia: “atualidade, interesse, importância e facilidade de assimilação” (MONTEIRO, 2003, p. 143), e explica que a notícia pode ser conceituada sob diversas angulações.

Entre elas, as que a veem não como um “espelho da realidade”, mas como uma “construção da realidade”, na qual o jornalista (produtor da notícia), teoricamente regido pela lógica da objetividade e da imparcialidade predominante no fazer jornalístico, na prática é afetado por inúmeros fatores que o levam a interagir socialmente e a realizar uma série de negociações durante o processo de produção da notícia. (MONTEIRO, 2003, p. 144).

Mafei (2007) fala que um bom assessor de imprensa sabe reconhecer seus limites éticos, e não os ultrapassa. “Não mente, não engana, não ameaça, não oferece vantagens a jornalistas em troca da inserção de reportagem positiva sobre seu cliente.” (MAFEI, 2007, p. 25). A autora aponta que o foco do assessor é sempre auxiliar seu assessorado com a imprensa, em busca da notícia exata.

O bom assessor tem muito de um bom repórter. Apura criteriosamente informações sobre o assessorado, busca dados que compõem uma notícia, procura fontes confiáveis (dentro e fora da organização, se for necessário) para averiguar a abordagem que tem em mente. Na hora de divulgar, tem a função de ajudar seu assessorado a identificar se o fato que ele quer ver divulgado é de interesse público e, assim, passível de se tornar objeto de matéria. Caso não seja, o tema não deve ser levado à mídia. (MAFEI, 2007, p. 25).

Monteiro (2003) fala que, para se transformar em notícia, um acontecimento passa por três conjuntos de agências: o primeiro é o dos promotores de notícias, aqueles que identificam fatos para outros e os promovem. O segundo grupo é o dos profissionais que se “alimentam” desses fatos, os jornalistas dos veículos de comunicação. O terceiro é o do público, consumidores da notícia. Por esse motivo, as fontes institucionais são consideradas “definidores primários”.

Em alguns casos, como nas instituições voltadas para as áreas de medicina, saúde, segurança pública, ou naquelas cuja atividade envolve conhecimento jurídico ou científico, por exemplo, aos requisitos exigidos de uma fonte institucional – afirmações “objetivas”, “autorizadas”, “dignas de crédito” – está agregada sua condição de “perito” ou “autoridade” no

assunto. Nesses casos, pesa mais a atividade desenvolvida do que a posição da fonte ou seu poder de representação. (MONTEIRO, 2003, p. 145-146).

Com relação às instituições públicas, Monteiro (2003) aponta que o fato de tornar público o trabalho feito, através da imprensa, tem como razão a prestação de contas à sociedade, para que ela possa averiguar o que está sendo feito e analisar se está de acordo com o que é de seu interesse e necessidade, fazendo com que a população crie identidade com a instituição, tornando-se sua aliada.

Mafei (2007) aponta que, apesar de haverem divergências entre os papéis do assessor de imprensa e do jornalista de redação, ambos possuem objetivos em comum. O mais importante deles é que os assessores trabalham, diariamente, para aumentar o fluxo de informações entre a sociedade e os meios de comunicação de massa. Com isso, eles facilitam o acesso entre jornalistas de redação e fontes, e criam um vínculo, um canal direto com a imprensa. A base desse relacionamento é a informação com exatidão e correta.

O mercado quer um profissional de assessoria de comunicação capaz de entender profundamente a atuação do assessorado, em áreas distintas, ou seja, um verdadeiro perito. (...). Com esse conhecimento, saberá distinguir, com a devida segurança, como reagirão os diferentes públicos daquela organização frente a informações divulgadas. O assessor não deve ser passivo, mas antecipar cenários que possibilitem a elaboração de um planejamento estratégico de comunicação capaz de criar uma imagem positiva do assessorado. Deve pensar como um profissional de *marketing*, identificando as medidas adequadas, por exemplo, para divulgar produtos e serviços, satisfazendo o consumidor. (...). (MAFEI, 2007, p. 46).

Monteiro (2003) cita que o processo de tornar notícia algo que acontece na organização pode ter duas origens: pode partir de uma demanda da imprensa ou de uma iniciativa interna da organização. Com relação ao segundo caso, a ideia de publicizar algum fato pode partir de algum funcionário ou do assessor de imprensa, por exemplo. No caso, os dois terão visões e opiniões diferentes sobre o fato e sobre a sua divulgação ou não.

É comum, em uma instituição, o assessor de imprensa achar que um assunto dá uma grande matéria e, ao procurar o técnico responsável, encontrar resistência, porque os resultados até o momento obtidos ainda não são definitivos e, portanto, sua divulgação colocaria em risco a instituição, o trabalho que é desenvolvido ou o próprio técnico. No entanto, aquele assunto pode ser de interesse da chefia, porque mostra que a empresa está "sintonizada" com as preocupações do governo ou da sociedade. Também é comum o contrário, o empregado procurar o assessor de imprensa para divulgar o resultado de seu trabalho e receber como resposta um "isso não dá matéria". (MONTEIRO, 2003, p. 152).

Monteiro (2003) assevera que há, nas empresas, uma anuência geral sobre o tipo de notícia que deve ser evitada a divulgação: “as que tratam de informação sigilosa e as que causam danos à credibilidade, confiabilidade, competência da instituição” (MONTEIRO, 2003, p. 152). A autora também argumenta que o sigilo é necessário para não prejudicar o andamento de algo que esteja sendo feito, como um trabalho, negociação ou projeto.

A informação é o que é possível e (...) legítimo mostrar, mas também o que devemos saber, o que está marcado para ser percebido, como se houvesse uma seta ou uma legenda indicando que aquilo é verdade e deve ser visto ou sabido. Por conseguinte, não é qualquer informação institucional que é transformada em notícia para a mídia. (MONTEIRO, 2003, p. 146).

Mafei (2007) aponta que, apesar de ser inserida entre as práticas de relações públicas, a assessoria de imprensa se difere dessa primeira, “já que sua atividade implica estabelecer canais indiretos (por intermédio da imprensa) de comunicação com todos os interlocutores com os quais se relacionam os assessorados.” (MAFEI, 2007, p. 47).

A autora escreve que a divulgação de assuntos de instituições, com o objetivo de pautar a imprensa demanda que os assessores sejam, cada vez mais, especialistas nas rotinas e processos de produção da notícia. Por isso, não restam dúvidas quanto à necessidade de que assessores de imprensa sejam, de fato, jornalistas.

Segundo Monteiro (2003), uma das estratégias utilizadas pelas assessorias de imprensa para promover a empresa é o agendamento prévio de acontecimentos, que pode ser feito através de *releases* e sugestões de pauta enviadas antecipadamente aos veículos de comunicação, afim de que saibam, com tempo hábil, que algum fato importante ocorrerá. Isso favorece a rotina daqueles profissionais que trabalham com a notícia, e permite que organizem seu trabalho.

Conscientes da importância do acesso à mídia e do poder que têm junto a elas, as instituições trabalham para serem “lembradas pela imprensa”, para ampliarem sua presença nos veículos e, mais do que isso, para serem reconhecidas como referências. Para atingir esses objetivos, produzem textos informativos para divulgação jornalística, compreendendo pautas, *releases*, *position papers*, informes oficiais, comunicados, artigos, notas técnicas. Enfim, produzem notícias. (MONTEIRO, 2003, p. 146).

Outra estratégia citada por Monteiro (2003) para a divulgação de uma notícia é valorizar o que é novo. Também é possível atualizar uma informação, através de uma técnica chamada

newspeg, na qual um acontecimento da realidade pode legitimar a noticiabilidade de outro. Como exemplos, a autora cita: 1) A existência de um fato, que pode acarretar na divulgação de outro. Por exemplo, no caso de um acidente de trânsito que tenha grande divulgação pela mídia, pode-se divulgar, por exemplo, em outras matérias, a importância do uso do cinto de segurança ou de cadeiras para crianças. 2) O tempo pode ser utilizado como “gancho” para a divulgação de algo: cinco anos, dez anos, 20 anos de um determinado fato. 3) Datas comemorativas: dia das crianças, dia das mães, dia dos pais, Natal. 4) Sazonalidade. Por exemplo, no verão, matérias sobre cuidados com a pele, refeições leves, viagens e passeios aquáticos.

2.2.4 Marketing empresarial, o fomento à prática de consumo e a gestão de crises

Uma das primeiras definições de *marketing*, feita pela Associação Americana de *Marketing* (1948), o caracteriza como “desenvolvimento das atividades de negócios que visam dirigir o fluxo de bens e serviços do produtor ao consumidor” (TONDATO, 2013, p. 135-136). De acordo com a autora, para que o *marketing* se desenvolva é necessária a atuação da comunicação, através da publicidade ou do relacionamento com o público-alvo.

Brandão e Carvalho (2003) citam que, em geral, a imagem é o patrimônio da empresa, e possui importância maior até que os próprios produtos ou serviços oferecidos por ela. Essa extrema valorização da imagem corporativa está relacionada com o surgimento e crescimento das empresas prestadoras de serviços. Esse fenômeno pode ser observado a partir da década de 1970.

A partir dos anos 1990, com o crescimento das indústrias de bens imateriais, a identidade institucional passou a ser o grande diferencial das empresas no quesito competitividade. O conceito de identidade é usado na administração com um sentido muito parecido com o de imagem.

Recentemente, a identidade corporativa ajustou-se ao conceito de imagem como uma visão capaz de ser construída apenas com base em elementos visuais e estéticos. Imagem como jogo com sentimento, desejos e pulsões; enfim, a psique do público consumidor. Nesse sentido, a identidade de uma empresa não está em si mesma, mas na visão que o consumidor e a

opinião pública têm dela, e isso depende não tanto de atitudes concretas, da excelência de produtos ou serviços, mas sobretudo da aura erigida pelo *marketing*. (BRANDÃO; CARVALHO, 2003, p. 191).

Jordão (2013) explica que existem várias teorias criadas para entender o consumo e suas motivações, as quais variam de acordo com as necessidades biológicas, psicológicas e sociais dos indivíduos. “Consumo é ação. Há, portanto, um sentido subjetivo dado pelo agente que vai orientar o consumo dos mais diferentes tipos” (JORDÃO, 2013, p. 259). O consumo é, assim, “uma forma de os atores sociais comunicarem seus estilos de vida, seus *status*” (JORDÃO, 2013, p. 259). Para a autora, o consumo serve para diferenciar as pessoas entre classes e gerar significados:

(...) os significados são entendidos por todos sobre o que é de bom gosto ou é vulgar, o que é distinto ou o que é popular, também são os significados dos bens consumidos e a maneira de usá-los que vão dizer sobre os mecanismos de inclusão e exclusão que a sociedade de consumo impõe às classes. (JORDÃO, 2013, p. 260).

Para Brandão e Carvalho (2003), autores da comunicação defendem quase sempre os pontos de vista semelhantes, que são:

a) (...) a imagem/identidade da empresa é seu maior patrimônio, seu maior valor; b) (...) ela é que representa a empresa junto a seus públicos e à opinião pública em geral; c) (...) justamente por isso, é ela que realmente vende a empresa no mercado; d) e, finalmente, que cabe à comunicação construir e/ou manter esse que é o mais precioso bem da empresa: sua imagem. (BRANDÃO; CARVALHO, 2003, p. 192).

Brandão e Carvalho (2003) argumentam que, pensando em manter a boa imagem institucional, as empresas se preocupam com a opinião pública. Os direitos do consumidor trouxeram uma nova ferramenta e competitividade no mercado. Por isso, as novas técnicas de atendimento ao cliente pretendem criar uma relação mais íntima e personalizada entre consumidor e empresa.

Com base nesse contexto corporativo em que criar uma relação de intimidade com o cliente é necessário para agregar valor aos serviços, surgiram novos postos nas empresas, como os de *ombudsman* e as seções de atendimento ao cliente, até ferramentas virtuais como o 0800. (BRANDÃO; CARVALHO, 2003, p. 197).

Jordão (2013) discursa que a sociedade de consumo se estabelece sobre padrões, e cada grupo compra aquilo que o representa e faz com que se identifique mais.

As pessoas não compram somente produtos. Elas compram um ou vários estilos de vida. As indústrias lançam continuamente novos produtos ou os mesmos com um detalhe a mais (diversificação), que vai tornar os antigos obsoletos, tornando, na lógica da sociedade de consumo, o novo superior ao antigo. A sedução fica a cargo dos meios de comunicação de massa, que distraem, mas ao mesmo tempo prendem os consumidores às novidades a serem consumidas. (JORDÃO, 2013, p. 261).

A autora lembra que, o que move a sociedade de consumo é, além da necessidade, o fato de existir um objeto novo a ser adquirido. Por isso as coisas se tornam facilmente obsoletas, e os objetos novos são o centro das atenções.

Os autores Brandão e Carvalho (2003) asseveram que atender bem aos direitos do consumidor seria impensável nos dias de hoje sem a utilização da tecnologia. Atender ao seu público não é uma questão de transparência empresarial, e sim de visibilidade, pois, é uma questão de mercado, de imagem. Por isso, o atendimento virou um fato político da empresa.

Brandão e Carvalho (2003) argumentam que uma das maiores ferramentas de *marketing* que existem atualmente é a *internet*. Praticamente todas as empresas, grandes ou pequenas, possuem *sites* que “vendem” a sua imagem ao público.

As corporações tendem a ver a *internet* como uma extensão de suas sedes físicas – o sítio transforma-se em uma espécie de *loja virtual*, oferecendo a familiaridade das instalações reais e virtualizando o acesso aos produtos. Trata-se de passar a sensação de que, mesmo distante, o cliente pode “tocar” a empresa. Nesse sentido, busca-se dar continuidade na construção da imagem corporativa: usam-se as mesmas cores, a mesma linguagem para identificação e comunicação com o público, os mesmos produtos... E, é claro, esses são atributos indispensáveis para que o cliente sinta-se “em casa”. (BRANDÃO; CARVALHO, 2003, p. 201).

Para Brandão e Carvalho (2003), as empresas que compreendem a grandeza da *internet* podem e devem explorá-la para construir comunidades com seus usuários, para que sejam trocadas ideias livremente. Essas comunidades podem agregar valor à marca da empresa e permitem uma observação das opiniões espontâneas de seus clientes.

Mas, nem só de bons frutos vivem as empresas. Forni (2003) fala que nenhuma organização está imune à crise, não importando o seu tamanho, tempo de existência ou o quanto é admirada no mercado.

Não importa a intensidade. Existem algumas devastadoras, que chegam de surpresa e só não acabam com a empresa à custa de milhões de dólares de investimento publicitário e compensação de prejuízos. Outras, menores, podem surgir de notícias ou fatos insignificantes em sua dimensão, mas complicados em seus desdobramentos. (FORNI, 2003, p. 363).

Forni (2003) argumenta que decidir o que comunicar durante uma crise é uma decisão estratégica. O que falar, para quem e como falar, e como se posicionar diante dos públicos interno e externo são decisões importantes, que podem, inclusive, definir os rumos de uma crise. No entanto, o autor ressalta que algumas crises são previsíveis e dificilmente podem ser evitadas.

É bom lembrar que existem ameaças à imagem que são previsíveis. Um repórter, por exemplo, passa longo tempo pesquisando matéria polêmica, geralmente fruto de denúncia ou de investigação iniciada pela própria empresa atingida. A organização acompanha essa apuração, presta todas as informações, mesmo sabendo que sua divulgação poderá gerar vários contratemplos. Ainda que não saiba a versão final da publicação, o interessado tem como prever as consequências com certa dose de acerto. E até pode planejar o *day after*. (FORNI, 2003, p. 365).

Forni (2003) ressalta que o principal elemento de uma crise é a surpresa, e que ela pode ter infinitas origens inusitadas, como vazamentos, sejam eles intencionais ou não; descuidos, frutos de inexperiência; ou até mesmo testemunhos de indivíduos suspeitos ou que tenham sido prejudicados de alguma forma.

Um fato importante apontado por Forni (2003) é o de que, nos dias atuais, existem muitas formas e meios de se propagar uma informação. Portanto, quando uma crise é instalada, a velocidade da comunicação pode fazer com que ela se alastre rapidamente. Por isso, hoje, muitas vezes a imprensa fica sabendo dos acontecimentos negativos antes mesmo da própria empresa. Para tentar remediar esses momentos conturbados, é importante que a organização seja ágil nas respostas. A imprensa se alimenta da crise. O importante é que a área de comunicação saiba ser rápida, para que a informação não dê lugar ao espetáculo.

Nessa hora, por inexperiência ou precipitação, cometem-se vários erros: tentar desqualificar o jornalista, irritar-se ou deixar para responder no dia seguinte, como se o tempo reduzisse a capacidade de o repórter apurar e escrever. A maioria dos autores enfatiza que não existe nada de pessoal

quando os jornalistas mergulham na apuração de denúncias ou fatos negativos. Reagir pode ser muito pior. (FORNI, 2003, p. 368).

Forni (2003) cita alguns exemplos de procedimentos que considera, deveriam ser evitados diante de uma crise. O primeiro deles é deixar o jornalista sem retorno; o segundo é omitir-se quando já há uma crise instalada; o terceiro refere-se ao fato de que, quando alguma matéria aparentemente sem sentido for publicada, é preciso analisá-la bem, bem como a sua dimensão, para que não haja réplica. Outro equívoco citado pelo autor é retaliar o jornalista. Isso pode ser feito por meio jurídico, presencial, ou através de uma carta esclarecedora. O autor acredita que uma boa conversa seja a melhor opção nesses casos. Em alguns casos, como aponta Forni (2003), dependendo do tamanho da crise, pode ser necessária a parceria com uma agência de publicidade ou até mesmo a contratação de uma assessoria externa.

Os embates entre empresas, governos, políticos e empresários com a imprensa fazem parte da própria história da comunicação no Brasil. Exercendo mal ou bem seu direito de informar, a imprensa em qualquer lugar do mundo sempre procurou assumir o papel de “fiscal dos que não têm voz”. E por isso esteve sempre em conflito com os poderosos. (FORNI, 2003, p. 387).

Contudo, observa-se que uma boa estratégia para as empresas é não brigar com a imprensa, mas sim tentar manter uma boa relação, sempre que possível. Isso ajuda a manter a boa imagem da empresa junto ao público.

2.2.5 O que faz uma assessoria de comunicação?

Pode-se definir a prática de assessoria de imprensa como a “gestão dos fluxos de informação e relacionamento entre fontes e jornalistas” (DUARTE, 2003, p. 236). Em uma assessoria, pode-se encontrar, trabalhando em conjunto, jornalistas, relações públicas, publicitários, equipe de *marketing*, recursos humanos e planejamento. Para englobar esse sistema integrado, existem as assessorias de comunicação, onde encontram-se profissionais de diversas áreas. Com essa expansão, os produtos e serviços oferecidos pelas assessorias podem ser ampliados, assim como as tarefas e desafios, e torna-se mais

difícil administrar esses diversos canais de comunicação. Por isso, o nome assessoria de imprensa é restritivo, se considerarmos todo o escopo de profissionais envolvidos nos trabalhos de comunicação de uma organização.

Duarte (2003) propõe um glossário com os produtos e serviços oferecidos por uma assessoria de imprensa ou assessoria de comunicação. Os conceitos estão descritos no quadro abaixo. Vale destacar que nem todos os tópicos descritos estão presentes em todas as assessorias existentes. Muitas vezes, o trabalho é adaptado para o tamanho da empresa e até mesmo para a quantidade de pessoal e recursos disponíveis para execução do trabalho. Os nomes das atividades desenvolvidas e suas descrições também podem variar de organização para organização. O que se apresenta a seguir, no Quadro 2, são conceitos gerais que auxiliam as organizações na busca por seus objetivos.

<p>1. Acompanhamento de entrevistas</p>	<p>Ao Assessor de Imprensa (AI) cabe o acompanhamento das entrevistas do assessorado ou membros da organização. (...). Essa postura permite ao assessor verificar o desempenho da fonte, os interesses do jornalista, ajuda a resolver algum problema ou dúvida e até evita armadilhas (...) ou erros do entrevistado. (...). Recomenda-se, também, uma rotina de avaliação posterior da entrevista com o entrevistado. Ajuda a identificar vícios (de fala, de postura física, de abordagem dos assuntos) e, ao longo do tempo, garante à fonte maior segurança e habilidade em lidar com jornalistas, criando uma espécie de “autonomia competente”. (...).</p>
<p>2. Administração da Assessoria de Imprensa (AI)</p>	<p>(...) atuar como assessor, mesmo que em uma estrutura mínima, exige habilidades, conhecimentos e postura típicos de gerente: bom trânsito em todos os níveis hierárquicos, noções de administração, estratégia empresarial, planejamento, conhecimento da cultura e da história da organização e dos papéis e poder dos integrantes. (...). Elaborar orçamentos, projetos, escalas de trabalho, avaliação, são demandas internas que passam a fazer parte da rotina, e que, mais do que “burocracia”, ajudam a organizar as atividades e facilitam a obtenção de bons resultados. (...).</p>
<p>3. Apoio a eventos</p>	<p>Eventos são uma atividade típica de relações públicas, mas, se podem chamar a atenção de jornalistas, passam a exigir atenção especial. (...). Organizá-los frequentemente reúne profissionais de comunicação de diferentes áreas. O assessor deve ajudar já no planejamento, orientando de acordo com as possibilidades e interesses dos veículos de comunicação. (...).</p>
<p>4. Apoio a outras áreas</p>	<p>É fundamental para o sucesso da organização que todas as atividades relacionadas à comunicação (<i>marketing</i>, publicidade, assessoria de imprensa, relações públicas, atendimento ao cliente) atuem de maneira integrada, assumindo a noção de que fazem parte de um sistema de comunicação com funções independentes, convergentes e vinculadas aos mesmos objetivos organizacionais.</p>

	Assim, passa a ser essencial que cada área de comunicação mantenha o foco na visão de negócio e na missão da organização e busque atuar em conjunto com as demais. (...).
5. Arquivo de material jornalístico	Um arquivo é fundamental para atender a demandas rotineiras e emergenciais de uma assessoria. (...). Se considerarmos que são poucas as organizações que dispõem de bibliotecas, arquivos e museus corporativos e, que na maioria dos casos as informações ficam espalhadas em diversos departamentos ou mesmo podem ser desprezadas a cada nova gestão, a eficiência da assessoria em disponibilizar material e informações merecerá reconhecimento imediato. (...).
6. Artigos	Têm boa aceitação nos veículos de comunicação. Seu conteúdo é basicamente opinativo e interpretativo e, em geral, oferece uma análise sobre assunto de interesse do público. (...). Os veículos de comunicação têm espaço reservado para esse tipo de texto (...). (...). Como nem sempre o assessorado tem tempo e disposição para escrever, é o tipo de tarefa que exige um bom redator, um <i>ghost-writer</i> , em geral o AI. (...).
7. Atendimento à imprensa	(...). Para estabelecer boa convivência, é fundamental compreender que normalmente o jornalista precisa ter atendimento rápido, personalizado e acesso a fontes de informação qualificadas. O assessor passa a ser referência principal dos jornalistas, como uma ponte entre redação e organização, agindo como um mediador qualificado. Para exercer esse papel, deve ter trânsito facilitado com as fontes de informação, conhecer a organização, suas políticas e atuação, assim como os interesses, forma de atuação dos jornalistas e saber orientar sobre seu atendimento. Ao mesmo tempo, o próprio assessor precisa ter sua atuação compreendida pelos dirigentes e empregados, o que facilitará o trabalho. Horário de expediente compatível com o das redações e estrutura mínima que permita criar e atender a demandas também são indispensáveis.
8. Avaliação dos resultados	(...). A eficácia da assessoria deve ser avaliada com base nos objetivos previamente definidos com os dirigentes ou fontes, numa perspectiva estratégica, vinculada aos interesses da instituição. Assim, o primeiro passo é ter clareza sobre o que o dirigente espera, suas expectativas com relação ao desempenho da assessoria. (...). A consciência sobre a necessidade de relação entre interesses e objetivo da organização e o trabalho da assessoria torna importante estabelecer uma rotina de discussão sobre temas como foco das ações, análise dos resultados, potencial de interesse da imprensa por determinados assuntos, comportamento da fonte com o jornalista etc. O assessor também deve criar mecanismos de autoavaliação sobre o relacionamento com jornalistas e veículos de comunicação, sobre a capacidade de criar e atender a demandas, de aproveitar oportunidades. (...).
9. Banco de dados	Organizar, saber utilizar ou, pelo menos, ter conhecimento e acesso a bancos de dados consolidados torna-se uma vantagem substancial para um assessor. E as organizações em geral têm algum tipo de sistema de informação para suporte à gestão. (...).

<p>10. Brindes</p>	<p>Podem sem foco de embaraços entre assessorias e redações. Por isso, a avaliação deve ser cuidadosa. (...). O tipo mais adequado é o material promocional da própria empresa. Uma opção elegante é a seleção de brindes específicos para jornalistas. Blocos, canetas, publicações e agendas, por exemplo, são sempre recebidos com simpatia. (...).</p>
<p>11. Capacitação de jornalistas</p>	<p>Assim como as fontes precisam entender como atua a imprensa, muitas vezes os jornalistas que cobrem determinada área teriam vantagens com um treinamento para compreender melhor determinado tema. Cursos, painéis, seminários para a imprensa sobre economia, ciência e direito são, tradicionalmente, bem-sucedidos (...). Além de aumentar a intimidade com o assunto, tendem a estimular o interesse pela área, com conseqüente reflexo na agenda das redações. (...).</p>
<p>12. Clipping e análise do noticiário</p>	<p>O <i>clipping</i> é uma das atividades mais típicas de uma assessoria de imprensa. Consiste em identificar rotineiramente na imprensa as citações sobre a organização ou temas previamente determinados, organizá-las e encaminhá-las para conhecimento dos interessados. Geralmente, os recortes são colados em folhas padronizadas acrescidos de informações sobre veículo, data, página de publicação, algum tipo de classificação e outros dados que sejam considerados importantes. (...). Uma mesma organização pode ter diferentes <i>clippings</i>, distribuídos a grupos segmentados. (...). O trabalho é realizado pelo próprio assessor, por alguém da equipe, estagiários ou por meio da contratação de empresas especializadas. (...). (...) permite maior clareza na identificação de como a organização ou o assessorado estão sendo percebidos pela imprensa, de modo que sirva de subsídio para análise dos ambientes geral ou competitivo. (...).</p>
<p>13. Concursos de reportagem</p>	<p>São uma alternativa para despertar o interesse para um tema, promovendo, indiretamente, a aproximação imprensa e organização. Ser reconhecido como competente e, ainda, premiado por produzir uma matéria com um tema nobre geralmente desperta o interesse do jornalista. (...).</p>
<p>14. Contatos estratégicos</p>	<p>O assessor deve procurar manter uma rotina de contatos regulares com as redações, evitando basear a ligação em <i>releases</i>, produto cada vez mais desgastado. Visitas, encontros informais, telefonemas regulares (...) e contatos, inclusive com o pessoal de apoio, têm diversas finalidades:</p> <ol style="list-style-type: none"> 1 – Administrativa: manter-se atualizado sobre nomes e funções dos jornalistas, dados como endereços, telefonemas, fax, <i>e-mail</i>, identificação de veículos e editorias de interesse. 2 – Operacional: atualizar-se sobre estrutura interna, horários de fechamento, interesses editoriais, identificação das pessoas responsáveis pela seleção das pautas, avaliar o relacionamento com os veículos e profissionais. 3 – Pauta: o fornecimento de pautas e informações interessantes e personalizadas é o melhor serviço que um assessor de imprensa pode prestar ao jornalista. (...). 4 – Prospecção: jornalistas têm grande circulação no ambiente em que as organizações atuam e por isso podem fornecer informações e comentários sobre parceiros, como a empresa está sendo vista,

	boatos em circulação, conjuntura política etc. (...). 5 – Manutenção do bom relacionamento: é indispensável a manutenção de um bom relacionamento nas redações, não apenas com editores, pauteiros, mas também repórteres e, inclusive, estagiários (...). (...).
15. Dossiê	Reunião de material sobre determinado tema, com o objetivo de informar o assessorado ou jornalista. Inclui farta e variadas informações: <i>clipping</i> , <i>releases</i> , documentos, análises, relatórios, dados estruturados ou brutos. (...).
16. Encontros fonte e jornalista	Podem ser articulados como rotina e seu objetivo principal é a conversa, o conhecimento mútuo, muitas vezes sem tema claramente definido. Geralmente, acontece em uma refeição combinada com antecedência, na organização, em um restaurante ou por meio de visita. (...).
17. Entrevistas coletivas	(...). A função das entrevistas coletivas limita-se a casos extraordinários, em que há necessidade de reunir jornalistas de vários veículos, ao mesmo tempo, para passar informações relevantes e de interesse público imediato ou, ainda, em casos especiais de lançamentos, assinatura de contratos ou eventos similar. A coletiva também é particularmente útil em situações emergenciais, quando muitos jornalistas procuram a organização ao mesmo tempo. (...). A sequência de uma coletiva consiste em apresentar as regras (como serão feitas as perguntas, critérios na sequência, duração e outros aspectos que possam gerar conflitos ou dúvidas), apresentação da fonte, exposição do tema, questionamentos, encerramento e, dependendo das circunstâncias, entrevistas individuais. (...).
18. Fotos	As fotos são utilizadas para acompanhamento de <i>releases</i> , disponibilização na <i>internet</i> , produção de publicações institucionais, em relatórios dirigidos ao público externo e para emergências de todo tipo. Uma das alternativas mais razoáveis é a contratação de fotógrafo <i>freelance</i> para atualização regular do arquivo (...). (...).
19. Jornal mural	(...). O assessor tem a opção de criar espaços informativos em murais do tipo “falamos de nós” com recortes de notícias veiculadas na imprensa ou produzir material específico para comunicação interna. (...). Outra alternativa é a criação de um boletim específico para afixação em murais. (...).
20. Levantamento de pautas	Tarefa sistemática e fundamental para o bom trabalho de um assessor de imprensa. (...). O assessor deve procurar criar uma rede de informantes na organização que lhe permita manter-se atualizado sobre tudo o que ocorre e, particularmente, sobre o que pode interessar à imprensa. (...). Banco de pautas: sistema físico que permite a identificação e acesso rápido a informações estruturadas para uso interno.
21. Mailing ou cadastro de jornalistas	É a lista de jornalistas e veículos de interesse de determinada assessoria e pode ser subdividida de acordo com critérios particulares: jornalistas locais, de interesse nacional, especializados,

	colunistas, pauteiros. (...). O <i>mailing</i> deve ter avaliação e atualização permanentes para manter sua eficiência. (...).
22. Manuais	<p>A elaboração de manuais padroniza procedimentos, dá identidade à organização, orienta a equipe e as fontes e ainda ajuda a organizar a circulação da informação. (...). Os manuais mais comuns são:</p> <p>Redação: orienta sobre padronização de títulos, texto, siglas, grafia, para uso nos <i>releases</i> e publicações. (...).</p> <p>Editoração: define características que deem uniformidade à variedade de publicações jornalísticas de uma organização. (...) como diagramação, linha editorial, público, tipologia, papel etc.</p> <p>Relações com a imprensa: (...). Pode-se incluir glossário, noções sobre o funcionamento dos veículos de comunicação e papel de atuação do jornalista, dicas específicas para atendimento a veículos como TV e rádio, definir pessoas e cargos autorizados a falar sobre determinados assuntos, uniformizar linguagem, descrever o sistema de trabalho na assessoria.</p> <p>Apoio ao jornalista: (...). O objetivo é estimular e facilitar o acesso à organização e a compreensão dos temas de interesse. (...).</p>
23. Nota oficial	<p>Documento distribuído à imprensa, muitas vezes também veiculado de forma paga, como declaração, posicionamento oficial ou esclarecimento sobre assunto relevante, urgente e de grande interesse público. Sua elaboração e divulgação reduz a chance de boatos, dúvidas e pressões por informação. (...). A nota oficial pode ser chamada de Comunicado, termo também adotado como sinônimo de <i>release</i>. <i>Position paper</i>: texto oficial de natureza política, que informa e detalha sobre a posição da organização a respeito de um tema relevante, geralmente polêmico e complexo. (...).</p>
24. Pauta	<p>Do ponto de vista de uma assessoria de imprensa, é um assunto que pode ser sugerido a um ou mais jornalistas com a intenção de que se transforme em notícia. (...). O <i>release</i> é um tipo de sugestão de pauta, mas geralmente contém informação de interesse abrangente, que o torna impessoal e genérico, mesmo quando o envio é segmentado. (...).</p> <p>Boletim de sugestões de pauta: conjunto de assuntos que podem transformar-se em notícia, como um “alerta”; mas, pela limitação de informações, exige a busca de detalhes. (...). Na pauta exclusiva entra-se em contato com determinado jornalista que possa ter interesse em assunto particularmente interessante e apresenta-se a proposta de pauta e encaminhamento do assunto, garantindo-se exclusividade. (...).</p>
25. Planejamento	<p>Ao iniciar qualquer trabalho, O AI deve identificar as posições e interesses (públicos e reservados) dos dirigentes aos quais está vinculado por meio de reuniões francas e objetivas. Isso, apoiado no conhecimento da imprensa e da organização, ajuda a estabelecer metas e planejar formas de atingi-las (...). (...).</p> <p>Plano de comunicação: (...). Ele define ações para a rotina e crises, prioridades, recursos humanos e materiais, sistemas de avaliação, orçamento, explicita estratégias e instrumentos, estabelecendo os procedimentos de cada área. (...).</p> <p>Plano de divulgação jornalística: documento setorial limitado às ações para relacionamento e divulgação de uma organização, pessoa, produto, serviço, ideia da imprensa. (...).</p>

	Plano para crises: (...). Ele ajuda a reduzir a margem de erros, a controlar a situação e o impacto negativo que uma crise inesperada pode causar. Pode incluir ações de administração de vários tipos: acidente, denúncia, manifestações, crime, orientando a área de comunicação e demais empregados sobre como proceder. (...).
26. Press-kit	Conjunto de material, geralmente reunido em uma pasta ou envelope, enviado à redação ou distribuído aos jornalistas durante uma cobertura, lançamento, coletiva, visita, que busca informar a respeito de determinado assunto. (...). Pode conter um conjunto de <i>releases</i> , CD, cartaz, disquete, catálogo, estatísticas, análises, cópias de documentos, discursos, bloco para anotações, caneta, artigos, folhetos, fotos, brinde, produtos. (...).
27. Publieditorial	Material pago veiculado sob a forma de matéria jornalística e muitas vezes produzido por assessores de imprensa sob encomenda de agências de publicidade. (...).
28. Relatórios	Um bom ponto de partida para a avaliação permanente da atuação e demonstração dos resultados obtidos na AI é a produção de relatórios após a conclusão de determinados projetos e ações e mesmo periodicamente. (...).
29. Release	Material distribuído à imprensa para sugestão de pauta ou veiculação gratuita. Também é conhecido por <i>press release</i> ou comunicado. É o instrumento mais usual e tradicional em uma assessoria de imprensa e objetiva informar ou chamar atenção do jornalista para um assunto que possa tornar-se notícia. (...). (...) é entendido como sugestão de pauta e não como notícia acabada, embora até possa ser veiculado na íntegra. (...).
30. Site	(...). Um dos serviços mais comuns é a criação de locais específicos do tipo “sala de imprensa” com a oferta de <i>releases</i> e informações específicas para jornalistas (...). O <i>site</i> pode tornar-se uma fonte regular de consulta e ser utilizado pelo jornalista sem sequer entrar em contato com a assessoria. (...).
31. Textos em geral	Mesmo que não seja sua atribuição original, é razoável que o AI contribua na redação, edição ou avaliação de um discurso de dirigente, texto para uma palestra, relatório, folheto, documentos do tipo Balanço Social, Relatório Anual ou mesmo a organização de uma apresentação. Por suas características de linguagem e público, essas demandas muitas vezes são atribuídas a um profissional com formação em Comunicação (...). (...).
32. Treinamento para fontes (<i>Media training</i>)	(...). O investimento em capacitação é uma das melhores maneiras de qualificar o relacionamento com a imprensa, porque ajuda a fonte a compreender e atender às necessidades do jornalista e a melhor aproveitar as oportunidades de exposição. (...). Entrevistas simuladas, exercícios em laboratórios, orientações sobre peculiaridades da imprensa local, análise conjunta dos resultados obtidos em entrevistas ajudam a capacitar as fontes e, conseqüentemente, melhoram o atendimento à imprensa. (...).

<p>33. Veículos jornalísticos institucionais</p>	<p>(...). O trabalho do AI pode incluir, por exemplo, a elaboração ou participação no projeto editorial e gráfico e acompanhamento de sua produção, até para manutenção de uma coerência nas mensagens e objetivos. Os veículos informativos institucionais são instrumentos muito importantes na manutenção de fluxos eficientes de informação e assumem características e nomenclatura próprias (informativo, <i>house organ</i>, vídeo-jornal, fax-boletim, <i>newsletter</i>, rádio interna, boletim digital, noticiário digital ou eletrônico). (...)</p>
<p>34. Visitas dirigidas</p>	<p>Visitas constituem um eficiente meio de aproximar jornalistas da organização. Um programa desse tipo talvez não busque a veiculação imediata de uma notícia, mas a melhoria do relacionamento (...). (...) é importante considerar que o roteiro tenha interesse para o jornalista e haja informação à disposição. (...).</p>

Quadro 2: Principais atividades de uma assessoria de imprensa.

Fonte: DUARTE, 2003, p. 236-255.

3 METODOLOGIA E RESULTADOS

3.1 Contexto

A Polícia Civil foi criada em 10 de maio de 1808, por Dom João VI, então Príncipe Regente do Brasil. Na ocasião, ele instituiu, através do Alvará Régio, a Intendência Geral de Polícia da Corte e do Estado do Brasil, no Rio de Janeiro, fazendo surgir, assim, a primeira instituição de Polícia Judiciária do país, nos moldes do que havia em Portugal.

Hoje, os funcionários da instituição são, em sua maioria, servidores concursados do estado. Na Assessoria de Comunicação da Polícia Civil de Minas Gerais (Ascom PCMG) trabalham, atualmente, 21 pessoas. Dessas, 13 são servidores concursados e oito são funcionários contratados, que ocupam cargos de livre nomeação e exoneração.

Há de se considerar que o governo estadual vigente tem poder de interferência direta na contratação de servidores que ocupam cargos comissionados, o que causa, eventualmente, trocas de pessoas, devido a mudanças eleitorais. Tal interferência ocorre porque os cargos em comissão são escolhidos, em sua maioria, por indicação, o que, logicamente, está relacionado à confiança com a chefia imediata e proximidade com o partido eleito.

Quanto ao trabalho desempenhado, a Assessoria de Comunicação da Polícia Civil é responsável por todo o trabalho de comunicação da instituição no estado, realizando atendimentos a órgãos de imprensa, que demandam informações diárias, e a delegacias, que demandam divulgação de trabalhos policiais realizados.

Os funcionários da Ascom trabalham, em sua maioria, na Cidade Administrativa de Minas Gerais (CAMG). Porém, em alguns casos, há núcleos avançados de assessoria, onde os assessores trabalham diretamente nos locais pelos quais respondem. É o caso do Departamento de Trânsito de Minas Gerais (Detran/MG), onde trabalham duas assessoras; do Departamento de Investigação de Homicídios e Proteção à Pessoa (DHPP), onde trabalha uma assessora; e da Divisão Especializada de Referência da Pessoa Desaparecida (DRPD), onde trabalha uma assessora.

Para o presente trabalho, considerado um estudo de caso, elaborou-se um questionário de avaliação da segurança da informação no âmbito da Assessoria de Comunicação da Polícia Civil de Minas Gerais (Ascom PCMG). O mesmo foi enviado para 19 dos 21 funcionários do setor. O questionário não foi enviado apenas para um servidor, que não possui formação superior na área de comunicação social e exerce função administrativa na Ascom. A redatora deste trabalho também não respondeu ao questionário e não foi considerada para as estatísticas a seguir. Dezoito pessoas se dispuseram a responder as perguntas, apenas uma não quis. As respostas foram obtidas em outubro de 2015.

3.2 Metodologia

Para a elaboração desta pesquisa, classificou-se a mesma de acordo com alguns pontos de vista. Do ponto de vista de sua natureza, é uma pesquisa aplicada. Apesar de não propor soluções para um determinado problema da instituição, aponta-se o que poderia ser melhorado para que o trabalho, conseqüentemente, seja melhorado também. Do ponto de vista da forma de abordagem ao problema, apresenta-se uma pesquisa qualitativa, porque o objetivo principal é discutir o problema em si, e não dar enfoque principal aos números obtidos na pesquisa. Do ponto de vista dos objetivos, é uma pesquisa exploratória, porque reúne pesquisa bibliográfica e estudo de caso sobre um determinado assunto, com o objetivo de proporcionar proximidade com o problema. Do ponto de vista dos procedimentos técnicos, é um levantamento, pois o objetivo foi a listagem dos problemas, e não um estudo aprofundado dos mesmos.

3.3 Perfil dos entrevistados

3.3.1 Sexo:

Mulheres: dez

Homens: oito

3.3.2 Idade:

Média de idade (idade total: 621, dividida pelo número total de respondentes: 18): 34,5.

A pessoa mais nova do setor tem 25 anos.

A pessoa mais velha do setor tem 51 anos.

3.3.3 Formação acadêmica:

Graduação: todas as 18 pessoas possuem curso superior.

Jornalistas: dez pessoas;

Publicitários: duas pessoas;

Relações Públicas: três pessoas;

Produção Editorial: uma pessoa;

Direito: uma pessoa;

Ciência da Informação e Sistemas de Informação: uma pessoa.

Dessas 18 pessoas, quatro são policiais civis: um jornalista, um relações públicas, um formado em Direito e um formado em Ciência da Informação e Sistemas de Informação.

Pós-graduação: 11 pessoas.

Concluídas:

Uma pessoa possui MBA em Marketing;

Uma pessoa pós-graduada em Gestão Estratégica da Comunicação;

Uma pessoa pós-graduada em Gestão Estratégica da Informação;

Uma pessoa pós-graduada em Comunicação Empresarial;

Uma pessoa pós-graduada em Jornalismo e Práticas Contemporâneas;

Uma pessoa pós-graduada em Produção e Criação em Mídia Eletrônica;

Uma pessoa pós-graduada em Gestão Estratégica de Negócios;

Uma pessoa pós-graduada em Gestão de Marketing;

Uma pessoa pós-graduada em B2B (Business to Business).

Em curso:

Uma pessoa pós-graduanda em Planejamento e Gestão Estratégica;

Uma pessoa pós-graduanda em Comunicação Digital.

Mestrado: duas pessoas.

Concluído:

Uma pessoa mestra em Gestão de Conteúdo em Website.

Em curso:

Uma pessoa mestranda em Ciência da Informação.

3.3.4 Tempo em que está na organização (considerado apenas o tempo na Ascom, caso a pessoa tenha passado por mais de um setor):

Pessoa com menos tempo na Ascom está lá há quatro meses (em outubro de 2015).

Pessoa com mais tempo na Ascom está lá há 13 anos (em outubro de 2015).

3.3.5 Setor da Ascom onde trabalha:

Em um único setor:

Atendimento à imprensa: cinco pessoas;

Núcleo de mídias sociais: uma pessoa;

Cerimonial: três pessoas;

Clipagem, fale conosco, Portal da Transparência, expediente e afins: uma pessoa;

Publicidade e marketing do Detran/MG: uma pessoa;

Assessora do Delegado Assistente do Chefe da Polícia Civil: uma pessoa;

Delegado Assistente do Chefe da Polícia Civil: uma pessoa;

Coordenação de atendimento à imprensa: uma pessoa;

Assessor-chefe da Ascom: uma pessoa.

Em mais de um setor ou função:

Uma pessoa transita entre o atendimento à imprensa e o núcleo de mídias sociais;

Uma pessoa transita entre o núcleo de mídias sociais, o atendimento à imprensa e a produção de clipping, ficando prioritariamente nessa primeira função;

Uma pessoa transita entre o setor de Comunicação Visual e o Cerimonial.

3.4 Análise dos questionários

Nos capítulo 2 do presente trabalho já se falou o que é uma assessoria de comunicação, para que serve nas empresas e quais profissionais costumam trabalhar nesse setor. No capítulo 1 foi falado sobre o que é segurança da informação e qual o seu papel para que as organizações realizem suas transações comerciais de forma segura, e protejam seu produto de consumo ou serviço que oferece.

Pensando nesse cenário pré-descrito anteriormente, propôs-se o presente questionário, com o intuito de avaliar, de forma qualitativa, como a Assessoria de Comunicação da Polícia Civil de Minas Gerais lida com a segurança da informação, e o que os funcionários do setor pensam a respeito sobre o assunto. O objetivo inicial do questionário é a identificação de possíveis problemas ou dificuldades que os profissionais enfrentem no seu cotidiano. Mas nada impede que, futuramente, este trabalho seja usado como base inicial para a construção de um projeto de melhoria do setor.

Com relação ao questionário, o mesmo foi distribuído a 19 dos 21 funcionários do setor. Dezoito pessoas se dispuseram a respondê-lo, e a análise a seguir foi feita com base nas respostas dos mesmos, recebidas em outubro deste ano.

O que se pode concluir, inicialmente, já na pergunta 1.a), é que a maioria dos respondentes acredita que sabe definir o que é segurança da informação: 15 pessoas. Três pessoas responderam que já leram algo por alto a respeito desse assunto.

Na pergunta 1.b), dez pessoas responderam que sim, são capazes de manter a segurança da informação. Duas pessoas responderam que não, três pessoas disseram que precisariam de treinamento e três disseram que não haviam respondido sim à pergunta anterior, pré-condição para responder à questão.

Na pergunta 2, oito pessoas acreditam que o nível de segurança das informações com as quais lidam em seus processos diários é médio. Seis pessoas responderam que o nível é baixo. Isso seria um ponto a ser considerado, levando em conta que o número de pessoas para as duas respostas foi parecido. Três pessoas consideram que o nível é alto, e uma pessoa considera que é inexistente.

Na pergunta 3, a maioria das pessoas (nove) responderam que consideram médio o nível de segurança contido nos sistemas com os quais lidam diariamente. Aqui foram considerados todos os sistemas utilizados pela organização, os tipos de *e-mails*, telefones e demais formas de comunicação das quais os funcionários se utilizam para trabalhar. Seis pessoas responderam que o nível é baixo. Outras duas pessoas responderam que é alto, e uma pessoa respondeu que é inexistente.

Na pergunta 4, 14 pessoas responderam que sim, consideram necessário algum tipo de mudança na empresa, seja nos processos, com relação aos sistemas utilizados e até

mesmo às atitudes dos funcionários, para melhora do nível de segurança com as quais a Ascom lida diariamente. Outras quatro pessoas responderam que não.

Na pergunta 5, 14 pessoas responderam que sim, consideram que existem falhas nos processos seguidos pelos profissionais da Assessoria de Comunicação que poderiam ser melhoradas ou até mesmo resolvidas. Duas pessoas responderam que não, e outras duas pessoas responderam que não entenderam a pergunta. Nessa pergunta foi pedido aos respondentes que descrevessem brevemente, no caso de terem respondido sim. Seguem abaixo as respostas dos funcionários. Uma pessoa respondeu sim, mas não descreveu.

- 1) “Penso que a assessoria de imprensa poderia ter mais controle de dados sigilosos em segurança pública, como informações em *off*.” (está na Ascom há um ano e nove meses).
- 2) “Não existe a cadeia de segurança da informação no âmbito da Ascom. O processo é praticamente realizado automaticamente, sendo o controle das informações muito fragilizado. O filtro da informação e a cadeia de conhecimento são praticamente horizontais.” (está na Ascom há oito meses).
- 3) “De uma forma geral, acredito não ser totalmente seguro contas da instituição no provedor do Gmail, por exemplo.” (está na Ascom há um ano e cinco meses).
- 4) “Entendo que é preciso, antes de tudo, treinamento e capacitação para gerar motivação entre os profissionais.” (está na Ascom há um ano e nove meses).
- 5) “Os funcionários devem se preocupar diariamente em não divulgar informações estratégicas para o público/imprensa.” (está na Ascom há um ano e nove meses).
- 6) “Melhorias em relação a quem tem acesso às informações, registros de quem tem ciência de determinadas informações e que as pessoas tenham consciência e pratiquem o sigilo.” (está na Ascom há dez meses).
- 7) “Acho que o trabalho sempre pode ser aprimorado. Por isso acho que, às vezes, as informações não circulam bem entre todos da assessoria, e acho que essa falha pode ser corrigida. Tem ruído na comunicação e precisamos otimizar isso.” (está na Ascom há um ano e cinco meses).

- 8) “Deveria haver uma troca maior de informações entre todos os funcionários da Ascom, em relação às informações externas que chegam, pois pode ser de interesse dos demais funcionários, estatísticas que chegam e não tomamos ciência que chegaram, ou que temos disponíveis etc.” (está na Ascom há 13 anos).
- 9) “O setor apresenta falhas em procedimentos e mecanismos referentes à comunicação (tanto interna quanto externa) comprometendo a integridade e disponibilidade da informação. Muitas informações deixam de ser compartilhadas ou são divulgadas de maneira equivocada ou imprecisa devido a essa deficiência do setor.” (está na Ascom há um ano e nove meses).
- 10) “Gestão com ética, para que a informação, quando se refere a operações policiais, coletivas de imprensa e afins, não seja para apenas um veículo, excluindo propositalmente os outros, mas sim para todos.” (está na Ascom há três anos e cinco meses).
- 11) “Considero que seria interessante que os integrantes da Ascom, por exemplo, tivessem senhas individuais de acesso ao REDS e não compartilhassem, como atualmente, a senha pessoal de apenas uma colega.” (está na Ascom há dois anos e quatro meses).

O Registro e Eventos de Defesa Social (REDS) é um sistema unificado criado em 2004 para registro de Boletins de Ocorrências. Ele permite acesso a todos os órgãos de Defesa Social do estado de Minas Gerais (Polícia Militar, Polícia Civil e Corpo de Bombeiros Militar), que utilizam o mesmo local para registros, possibilitando integração entre as instituições.

- 12) “Existem diversos sistemas de autenticação do usuário, como biometria. Hoje, o sistema de uso coletivo é compartilhado por sistema gratuito. Uma vez que a senha seja divulgada por qualquer um dos operadores, daria acesso total a todas as informações recebidas, geradas e disseminadas pela Ascom.” (está na Ascom há três anos).
- 13) “Há demora na identificação da unidade onde determinados casos estão sendo investigados. Isso, geralmente, é porque as ocorrências demoram a tramitar, não havendo interesse do suposto receptor de um caso de maior repercussão em procurar as informações. A partir daí, é necessário um aprimoramento dessa

tramitação e o envolvimento dos profissionais da Ascom, tendo como base as demandas de imprensa, que de certa forma é intermediária da sociedade.” (está na Ascom há três anos).

A pergunta 6 foi com relação ao nível de preparo dos funcionários que trabalham na Ascom, considerando o setor como um todo. A pergunta foi se a pessoa considera que ela e os colegas de trabalho estão preparados para lidar com as dificuldades diárias relacionadas à segurança da informação. Onze pessoas responderam: a maioria sim / a minoria não. Outras sete pessoas responderam: a maioria não / a minoria sim.

A pergunta 7 foi semelhante à 6, porém considerando-se as fontes oficiais (pessoas físicas) com as quais os profissionais da Ascom lidam diariamente para obter as informações necessárias para desempenhar o trabalho. A pergunta foi se elas consideram que as fontes têm consciência da necessidade de segurança da informação para sigilo e cuidado com o conhecimento pertencente à empresa. Dez pessoas responderam: a maioria sim / a minoria não. Outras oito pessoas responderam: a maioria não / a minoria sim.

A pergunta 8 parte das respostas das perguntas 6 e 7. Perguntou-se aos funcionários se eles consideram necessário algum tipo de treinamento periódico para atualização e reciclagem dos funcionários, no sentido de alertá-los para a necessidade de segurança da informação diariamente na organização. Quatorze pessoas responderam sim e quatro responderam não.

A pergunta 9 pedia que os profissionais citassem algum exemplo de um momento deles ou que tenham presenciado na organização em que perceberam que a segurança da informação foi falha, ou um momento em que acreditam que o nível de segurança da informação tenha sido total, para o caso de considerarem não haver falhas. Foi pedido que assinalassem aqueles que não haviam entendido a questão proposta, e três pessoas marcaram essa opção. As outras 15 respostas seguem abaixo.

- 1) “Lembro-me de uma situação em que, por descuido de um colega, que se esqueceu de determinar a declaração de uma fonte como *off*, acabei por passar uma informação de conteúdo sigiloso. Penso que se estamos trabalhando com dados de alta repercussão, deveria haver um controle maior sobre esses mecanismos.” (está na Ascom há um ano e nove meses).

- 2) “Por ter trabalhado tanto na área operacional, onde as informações eram repassadas à Ascom sem qualquer controle, e por estar trabalhando no setor de comunicação da Polícia Civil atualmente, percebo um grande amadorismo em relação ao controle da informação. Não há qualquer filtro, senha, cadeia de processo, ordem de serviço, criptografia, elementos imprescindíveis para se ter o conhecimento de em que nível está a informação e que é responsável por um eventual vazamento ou deturpação. Desta forma, prefiro mencionar de forma ampla que exemplificar, pois com exemplos alcançamos os profissionais envolvidos.” (está na Ascom há oito meses).
- 3) “Usamos a planilha do Gmail para fazer as anotações do atendimento, e ela não é totalmente segura. Muitos usuários que já saíram podem ter acesso. E ela também não é plenamente confiável. Por exemplo, quando apagamos uma linha com outras pessoas conectadas, corremos o risco de perder muitas informações ali anotadas.” (está na Ascom há um ano e nove meses).
- 4) “Na instituição como um todo (...) acredito que já teve a segurança da informação falha em entrevistas coletivas por falta de assessoramento do entrevistado. Sugiro *media training* para as fontes da instituição.” (está na Ascom há um ano e cinco meses).
- 5) “Na área de Relações Públicas, é comum eventos conflitantes com a agenda do Chefe da Polícia, ou até mesmo do Governador. Os organizadores querem/desejam a presença da chefia, mas não consultam disponibilidade. São, portanto, estimulados a consultar e a informação é disponível. De certa forma, a pré-disponibilidade do chefe pode gerar algum constrangimento caso ele não compareça no evento.” (está na Ascom há um ano e nove meses).
- 6) “Sinto insegurança com relação à *internet* e celular usados na instituição, já que há evidências de que são grampeados/monitorados.” (está na Ascom há um ano e nove meses).

Um exemplo que comprova, de forma direta, que há o monitoramento das redes internas da CAMG aparece quando um servidor ou visitante faz *login* na rede interna de *internet* sem fio, *wi-fi*. A rede pode ser acessada por todos, sem a utilização de senhas. Porém, para que o *login* se complete, é necessário que a pessoa aceite os termos de condição que aparecem no navegador de *internet*, assim que a rede se conecta. A mensagem é a seguinte:

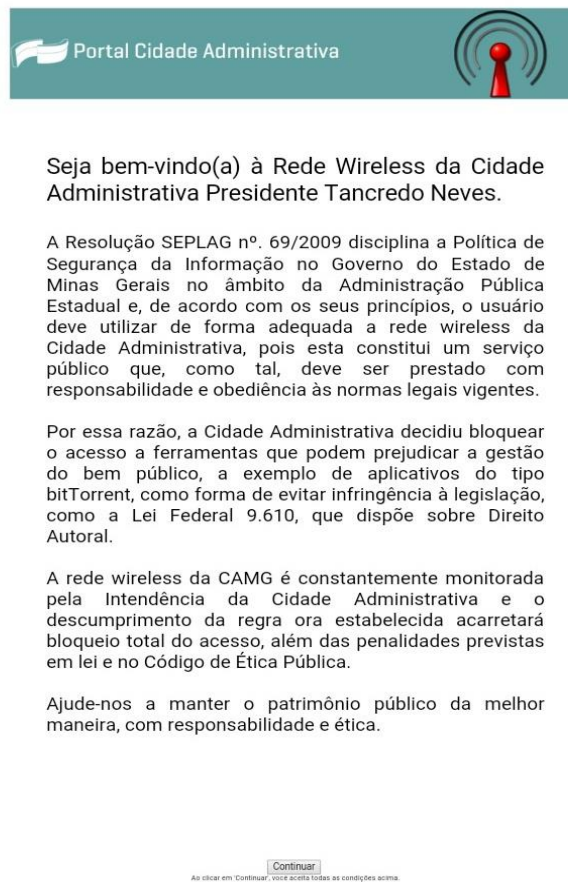


Figura 1: Página de *login* da rede *wireless* da Cidade Administrativa de Minas Gerais.
Fonte: imagem de tela de celular / arquivo pessoal.

A Resolução SEPLAG n° 69/2009, citada na mensagem de *login* do *wi-fi*, pode ser consultada nos anexos deste trabalho. Ela dispõe sobre a Política de Segurança da Informação no Governo do Estado de Minas Gerais.

- 7) “Muitas das vezes, as fontes repassam informações diretamente para a imprensa, sem passar pela assessoria de imprensa. Às vezes, somos questionados sobre assuntos que não temos conhecimentos (não fomos avisados), e a imprensa já fez até matéria. Às vezes, a informação poderia ser melhor trabalhada pela assessoria e divulgada de outra forma para otimizar o trabalho ou destacar o trabalho da Polícia, ou ainda, tentar transformar a pauta em uma grande matéria para a imprensa.” (está na Ascom há um ano e cinco meses).
- 8) “Diariamente, utilizamos um email do Gmail, isto é, sem qualquer tipo de segurança específica para as informações que compartilhamos. Diariamente, utilizamos uma

planilha armazenada em nuvem, e nela postamos inclusive informações sigilosas (*off*) sem qualquer filtro. Um texto enviado para a revisão é geralmente alterado e enviado à imprensa, sem que o autor primário seja consultado sobre as mudanças. Em um destes episódios, presenciei um “justiceiro” – que matou um estuprador para defender uma menor – que tornou-se o próprio estuprador da menor. Os problemas com a segurança da informação vão além da utilização de sistemas inadequados, atingem rotinas básicas na produção textual. Lembrando que, ao transformar o “justiceiro” em estuprador, condenamos um ser humano pela opinião pública, além de comprometermos a integridade física dele nos presídios.” (está na Ascom há um ano e nove meses).

- 9) “Um solicitante do Portal da Transparência questionou o porquê de um determinado Governador do Estado de MG, no passado, ter recebido uma condecoração da instituição/PCMG. Ele solicitou a lista de todos os agraciados. Tivemos que repassar a solicitação para o crivo último da instituição, para a aprovação do repasse de tais informações, mesmo porque se tratava de um ex chefe de estado e não sabíamos se a solicitação era de cunho político, já que estávamos em época de eleições presidenciais e estaduais. A informação foi tratada com o máximo sigilo. Seu trâmite, dentro disso, teve absoluto sucesso, sendo repassado ao solicitante, após discussão entre todos os envolvidos na elaboração da resposta, conforme determinação final do Chefe da Polícia Civil na época. Em todo processo, envolvemos na demanda as pessoas qualificadas para a complexidade da resposta, facilitando o sigilo da informação, facilitando o entendimento sobre o assunto e a elaboração da resposta que foi aceita pelo solicitante.” (está na Ascom há 13 anos).
- 10) “O crescente uso das redes sociais faz com que as pessoas passem a compartilhar informações sem muita cautela, divulgando, por vezes, conteúdo de cunho confidencial. Um servidor da instituição já chegou a divulgar, em rede social aberta, a realização de uma operação policial antes que essa tivesse sido concretizada, o que poderia ter comprometido a efetividade do trabalho. Acredito que isso tenha acontecido em virtude do despreparo do servidor em relação aos procedimentos relativos à segurança da informação.” (está na Ascom há um ano e nove meses).
- 11) “Várias vezes, operações policiais sigilosas tiveram o trabalho prejudicado pela presença de determinado veículo de imprensa (Record), que foi informado de horário, local e teor da operação, para que pudesse acompanhar e dar o furo de

notícia, não importando que prejudicaria o andamento da operação. Consternado, o delegado que chefiou cada operação sempre ligava para a Ascom, atribuindo aos assessores de comunicação a culpa. Porém, às vezes, a informação sai da própria delegacia, inclusive antes de a Ascom ficar sabendo. Outro caso ocorreu quando o gestor da Ascom passou informações sigilosas (nome, telefone, endereço, histórico da ocorrência...) de pessoas que fizeram boletins de ocorrência, para determinado veículo de imprensa (TV Globo), em *off*.” (está na Ascom há três anos e cinco meses).

- 12) “O registro por escrito, na planilha de atendimento, de informações que devem ser mantidas em *off*, é um sinal claro de fragilidade de segurança da informação. Dados estatísticos, muitas vezes, ficam disponíveis na caixa de *e-mails*, podendo ser facilmente acessados por pessoas estranhas ao setor ou mesmo serem enviados, equivocadamente, para veículos de imprensa.” (está na Ascom há dois anos e quatro meses).
- 13) “A assessoria de imprensa não informar para a imprensa dados de investigação ainda em andamento.” (está na Ascom há quatro meses).
- 14) “Cotidianamente, observo operadores levantarem de suas estações de trabalho, para almoçarem, usar sanitários, buscar água ou café, deixando seus respectivos computadores, com planilhas e informações em aberto, sem mesmo desligarem o monitor ou bloquearem o uso. Outro fato é o corredor onde estão localizados as estações. Qualquer pessoa que transitar no local podem observar as telas. Uma simples película de privacidade nos monitores já resultaria em melhora da segurança.” (está na Ascom há três anos).
- 15) “No caso do desligamento de um *freezer* no Instituto de Criminalística, a forma com que as informações circularam interna e externamente foi falha, confusa e com direcionamentos que interessavam mais a determinados grupos e não à instituição como um todo, o que resultou em desgaste na imagem da PCMG.” (está na Ascom há três anos).

4 CONCLUSÃO

Este trabalho é apenas uma pequena semente em um oceano profundo que compõem os temas em questão, aqui abordados. No entanto, após a conclusão do mesmo, o que fica é a mensagem principal de que não se pode pensar em assessoria de comunicação, nos dias de hoje, sem relacioná-la à segurança da informação.

As assessorias são setores estratégicos nas empresas, e, portanto, sujeitos a diversas ameaças e vulnerabilidades, não só no espaço físico de onde as organizações se encontram, como também no meio *web*, muito utilizado por *crackers*, especialistas em quebra de sistemas que têm o intuito de roubar senhas, dados e sequestrar bens imateriais das empresas, agindo de má fé.

Para o desenvolvimento do presente trabalho, elaborou-se um questionário de avaliação da segurança da informação no âmbito da Assessoria de Comunicação da Polícia Civil de Minas Gerais (Ascom PCMG). O mesmo foi enviado para 19 dos 21 funcionários do setor. Dezoito pessoas se dispuseram a responder as perguntas, e as respostas foram obtidas em outubro de 2015.

A análise de resultados foi feita com base no retorno dos 18 respondentes. Através das respostas obtidas, percebe-se que a maioria dos funcionários do setor (15 pessoas), acredita que sabe definir o que é segurança da informação, mas apenas dez acreditam que são capazes de mantê-la.

Com relação às informações com as quais lida diariamente, a maioria dos servidores (oito pessoas) acredita que o nível de segurança contido nelas é médio. Já com relação aos sistemas dos quais se utilizam para trabalhar, nove pessoas acreditam que possuem nível médio de segurança.

Quatorze pessoas acreditam ser necessária algum tipo de mudança na empresa, para que se obtenha um maior nível de segurança da informação. O mesmo número de pessoas acredita haver falhas nos processos seguidos pelos profissionais da assessoria. Como exemplo citado mais de uma vez pelos respondentes, aparece o fato de o setor não utilizar endereços de *e-mail* institucionais em demandas diárias.

Com relação ao nível de preparo dos próprios profissionais da Ascom em relação à segurança da informação, onze pessoas acreditam que a maioria possui preparo e a minoria não. Já com relação ao nível de preparo das fontes oficiais (pessoas físicas) da assessoria para lidar com a segurança da informação, dez pessoas consideram que a maioria das fontes é preparada e a minoria não.

Quatorze pessoas consideram necessário algum tipo de treinamento periódico para otimizar os processos realizados no setor. Com relação à falhas de segurança da informação, a maioria dos funcionários citou o fato de que, muitas vezes, a informação não perpassa por todos os funcionários do setor, e isso acarreta problemas como respostas equivocadas dadas pela assessoria; retrabalho de algum levantamento que já tenha sido feito; e falta de unicidade no setor.

Apesar de os números dos questionários apresentarem resultados quantitativos, o que se observa, através desta pesquisa, é um resultado qualitativo, pois o mesmo permitiu enxergar, através de respostas claras dos funcionários, falhas que existem no cotidiano do setor e podem ser resolvidas. Algumas delas demandam, sim, verba para que sejam executadas, mas, em contrapartida, outros procedimentos são simples e que não geram custos à instituição, estando muito mais relacionados à cultura organizacional e práticas diárias do que à verba direta para realização.

Algumas sugestões de mudanças necessárias puderam ser identificadas a partir da realização deste trabalho. Uma delas seria a criação de e-mails institucionais individuais para os funcionários, em um servidor que suporte o volume de trabalho diário da assessoria. Outra sugestão, também de suma importância, seria a realização periódica, a cada seis meses, de treinamentos com as fontes oficiais da PCMG, aquelas que concedem entrevistas constantes à imprensa. Nesse caso, devido à grandiosidade do Estado e divisão da Polícia em departamentos, os treinamentos poderiam ser planejados em escalas, por departamentos, para que todos os porta-vozes fossem contemplados. Outra sugestão de mudança mais simples, porém, não menos importante, seria um treinamento anual com os servidores que compõem a assessoria, relacionado à segurança da informação, onde seriam repassados assuntos como o bloqueio de computadores quando o servidor se levanta da mesa e a movimentação de informações sigilosas em celulares pessoais, por exemplo.

O assunto é amplo e não era tida como pretensão a abordagem total de todas as vertentes da segurança da informação e de assessorias de comunicação. O que se expôs foi uma pequena ponta do problema, que, espera-se, ainda possa ser discutido e estudado amplamente, para melhora dos processos e fortalecimento do setor na Polícia Civil de Minas Gerais.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Maurício Barcellos. Noções básicas sobre metodologia de pesquisa científica. Disponível em <<http://mba.eci.ufmg.br/downloads/metodologia.pdf>>. Acesso em 17 jul. 2015.

ALMEIDA, Maurício Barcellos; COELHO, Kátia Cardoso; SOUZA, Renato Rocha. Uma proposta de ontologia de domínio para segurança da informação em organizações: descrição do estágio terminológico. **Informação & Sociedade: Estudos**, João Pessoa, v. 20, n. 1, p. 155-168, jan./abr. 2010. Disponível em <<http://www.ies.ufpb.br/ojs/index.php/ies/article/view/3753>>. Acesso em 17 set. 2015.

ARAÚJO, Wagner Junqueira de; AZEVEDO, Patrícia Morais de; SILVA, Narjara Bárbara Xavier. Engenharia social nas redes sociais *online*: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. **Revista Ibero-Americana de Ciência da Informação (RICI)**, Brasília, v. 6, n. 2, p. 37-55, ago./dez. 2013. Disponível em <<http://periodicos.unb.br/index.php/RICI/article/view/9222>>. Acesso em 17 set. 2015.

BRANDÃO, Elizabeth; CARVALHO, Bruno. Imagem corporativa: *marketing* da ilusão. In: DUARTE, Jorge (org). **Assessoria de imprensa e relacionamento com a mídia: teoria e prática**. São Paulo: Atlas, 2003. p. 189-205.

BRASIL. Ministério da Cultura, Instituto do Patrimônio Histórico e Artístico Nacional, Comitê Gestor de Tecnologia da Informação. Política de Segurança da Informação do IPHAN. Dispõe acerca da Política de Segurança da Informação no âmbito do Instituto do Patrimônio Histórico e Artístico Nacional. Brasília, out. 2013, p. 1-18. Disponível em <<http://portal.iphan.gov.br/uploads/ckfinder/arquivos/Pol%C3%ADtica%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o.pdf>>. Acesso em 17 set. 2015.

CORTEZ, Igor Siqueira; KUBOTA, Luís Cláudio. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. **Revista de Administração da Universidade de São Paulo (Rausp)**, São Paulo, v. 48, n. 4, p. 757-769, out./nov./dez. 2013. Disponível em <http://www.rausp.usp.br/busca/artigo.asp?num_artigo=1560>. Acesso em 17 set. 2015.

DUARTE, Jorge. Produtos e serviços de uma assessoria de imprensa. In: DUARTE, Jorge (org). **Assessoria de imprensa e relacionamento com a mídia: teoria e técnica**. São Paulo: Atlas, 2003. p. 236-255.

FORNI, João José. Comunicação em tempo de crise. In: DUARTE, Jorge (org.). **Assessoria de imprensa e relacionamento com a mídia: teoria e técnica**. São Paulo: Atlas, 2003. p. 363-388.

FRANCELIN, Antonio Edison. Transformações profundas: Com duzentos anos, Polícia Civil já foi Judiciária. **Revista eletrônica ConJur – Consultor Jurídico**, ago. 2010. Disponível em <<http://www.conjur.com.br/2010-ago-09/duzentos-anos-historia-policia-civil-foi-policia-judiciaria>>. Acesso em 15 nov. 2015.

JORDÃO, Janaína Vieira de Paula. Práticas de consumo: um estudo das motivações do consumidor a partir da Sociologia da Experiência. In: TUZZO, Simone Antoniacci; TEMER,

Ana Carolina Rocha Pessôa (org.). **Assessoria de comunicação e marketing**. Goiânia: FACOMB/UFG, 2013. p. 257-277.

LAUREANO, Marcos Aurélio Pchek. Gestão de Segurança da Informação. 2005, p. 1-127. Apostila. Disponível em <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em 17 set. 2015.

LE MOS, Cláudia; DEL GAUDIO, Rozalia. Publicações jornalísticas empresariais. In: DUARTE, Jorge (org). **Assessoria de imprensa e relacionamento com a mídia: teoria e técnica**. São Paulo: Atlas, 2003. p. 256-285.

LORENZON, Gilberto; MAWAKDIYE, Alberto. Manual de assessoria de imprensa. 3 ed. Campos do Jordão: Mantiqueira, 2011. 80 p.

MAFEI, Maristela. Assessoria de imprensa: como se relacionar com a mídia. 3 ed. São Paulo: Contexto, 2007, 127 p.

MINAS GERAIS. Secretaria de Estado de Planejamento e Gestão. **Resolução nº 69**. Institui a Política de Segurança da Informação no Governo do Estado de Minas Gerais no âmbito da Administração Pública Estadual. Belo Horizonte, 17 de setembro de 2009. Disponível em: <http://www.planejamento.mg.gov.br/images/phocadownload/resolucoes/2009/resolucao_se_plag_69_2009.doc>. Acesso em 18 set. 2015.

MONTEIRO, Graça França. A notícia institucional. In: DUARTE, Jorge (org). **Assessoria de imprensa e relacionamento com a mídia: teoria e técnica**. São Paulo: Atlas, 2003. p. 140-160.

REGO, Francisco Gaudêncio Torquato do. A comunicação como poder nas organizações. In: **Comunicação empresarial/Comunicação institucional: conceitos, estratégias, sistemas, estrutura, planejamento e técnicas**. São Paulo: Summus Editorial, 1986a. p. 13-18.

REGO, Francisco Gaudêncio Torquato do. Uma visão histórica. In: **Jornalismo empresarial: teoria e prática**. São Paulo: Summus Editorial, 1986b. p. 17-34.

SILVA, Abner de Oliveira e. Engenharia social: o fator humano na segurança da informação. **Coleção Meira Mattos – Revista das Ciências Militares**, Rio de Janeiro, n. 23, set./out./nov./dez. 2010. Disponível em: <<http://www.eceme.ensino.eb.br/meiramattos/index.php/RMM/article/view/16>>. Acesso em 08 set. 2015.

TONDATO, Márcia Perencin. *Marketing* e comunicação: entre a parceria e a disputa, a integração. In: TUZZO, Simone Antoniacci; TEMER, Ana Carolina Rocha Pessôa (org.). **Assessoria de comunicação e marketing**. Goiânia: FACOMB/UFG, 2013. p. 131-172.

TUZZO, Simone Antoniacci. Assessoria de Comunicação e formação da Opinião Pública. In: TUZZO, Simone Antoniacci; TEMER, Ana Carolina Rocha Pessôa (org.). **Assessoria de comunicação e marketing**. Goiânia: FACOMB/UFG, 2013. p. 17-51.

VIANNA, Catarina Morawska. Lições em engenharia social: a lógica da matriz de projeto na cooperação internacional. **Horizontes Antropológicos**, Porto Alegre, ano 20, n. 41, p. 87-115, jan./jun. 2014. Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-71832014000100004&lng=pt&nrm=iso&tlng=pt>. Acesso em 17 set. 2015.

ANEXOS

Anexo A: Questionário aplicado aos funcionários da Assessoria de Comunicação da Polícia Civil de Minas Gerais

A expressão *segurança da informação* está associada a diversos fatores. Entre eles, podemos citar dados presentes em sistemas informatizados, “controle de acesso a recursos, segurança em comunicação, gestão de riscos, políticas de informação, sistemas de segurança, diretrizes legais, segurança física, criptografia, dentre outros”. (KRAUSE; TIPTON, 1997, *apud* ALMEIDA; COELHO; SOUZA, 2010, p. 155).

Partindo desses conceitos de segurança da informação, por favor, responda ao questionário abaixo, considerando as perguntas a partir do seu ponto de vista como contratado/servidor da Polícia Civil de Minas Gerais. Ressalta-se que os nomes e funções específicas dos entrevistados **NÃO SERÃO DIVULGADOS EM HIPÓTESE ALGUMA** ao longo dessa pesquisa, nem mesmo após a conclusão da mesma. Os dados serão analisados e utilizados unicamente para fins acadêmicos.

Questionário de avaliação da segurança da informação no âmbito da Assessoria de Comunicação (Ascom) da Polícia Civil de Minas Gerais

- Nome completo:
- Idade:
- Formação acadêmica (considere graduação e pós-graduação):
- Tempo em que está na organização (se já passou por mais de um setor, considere apenas o seu tempo na Ascom):
- Setor da Ascom onde você trabalha:

1. a) Você saberia definir o que é segurança da informação?

A () Sim

B () Não

C () Já li algo por alto

D () Precisaria de treinamento

E () Não entendi a pergunta

1. b) Caso tenha respondido sim à pergunta acima, você acredita que é capaz de mantê-la?

A () Sim

B () Não

C () Precitaria de treinamento

D () Não respondi sim à pergunta anterior

E () Não entendi a pergunta

2. Com relação aos parâmetros gerais de seu trabalho cotidiano, analisando apenas os processos aos quais você segue diariamente, você considera que o nível de segurança das informações com as quais você lida é:

A () Alto

B () Médio

C () Baixo

D () Inexistente

E () Não entendi a pergunta

3. Agora pense no nível de segurança dos sistemas com os quais você lida diariamente. Aqui entram todos os sistemas utilizados pela organização, os tipos de *e-mails*, telefones e demais formas de comunicação das quais você se utiliza para trabalhar. Agora pense se você considera que eles são seguros ou não. Caso pudesse classificá-los, você acredita que o nível de segurança contido neles é:

A () Alto

B () Médio

C () Baixo

D () Inexistente

E () Não entendi a pergunta

4. Você considera necessário algum tipo de mudança, seja nos processos da empresa, com relação aos sistemas utilizados e até mesmo às atitudes dos funcionários, para melhora do nível de segurança com as quais a Assessoria de Comunicação lida diariamente?

A () Sim

B () Não

C () Não entendi a pergunta

5. Pensando em todos os processos seguidos pelos profissionais da Assessoria de Comunicação, você considera que existem falhas nos mesmos que poderiam ser melhoradas ou até mesmo resolvidas?

A () Sim

B () Não

C () Não entendi a pergunta

Caso tenha respondido sim, poderia descrever brevemente?

6. Agora considere o nível de preparo dos funcionários que trabalham no mesmo setor que você (pense na Assessoria de Comunicação como um todo). Você considera que você e seus colegas de trabalho estão preparados para lidar com as dificuldades diárias relacionadas à segurança da informação?

A () A maioria sim / a minoria não

B () A maioria não / a minoria sim

C () Não entendi a pergunta

7. Considere as fontes oficiais (pessoas físicas) com as quais você lida diariamente para obter as informações necessárias para desempenhar o seu trabalho. Você considera que elas têm consciência da necessidade de segurança da informação para sigilo e cuidado com o conhecimento pertencente à empresa?

A () A maioria sim / a minoria não

B () A maioria não / a minoria sim

C () Não entendi a pergunta

8. A partir das suas respostas nas perguntas 6 e 7, você considera necessário algum tipo de treinamento periódico para atualização e reciclagem dos funcionários no sentido de alertá-los para a necessidade de segurança da informação diariamente na organização?

A () Sim

B () Não

C () Não entendi a pergunta

9. Por favor, cite abaixo algum exemplo de um momento seu ou que você tenha presenciado na organização em que você percebeu que a segurança da informação

foi falha. Caso você considere que não há falhas no nível de segurança da empresa, por favor, cite um exemplo de um momento em que você acredita que o nível de segurança da informação tenha sido total. Não é necessário citar nomes, nem locais. Apenas fale resumidamente sobre um caso que você se lembre.

() Marque ao lado caso você não tenha entendido a questão proposta.

Anexo B: Resolução SEPLAG nº 69/2009

RESOLUÇÃO Nº. 69, DE 17 DE SETEMBRO DE 2009.

Institui a Política de Segurança da Informação no Governo do Estado de Minas Gerais no âmbito da Administração Pública Estadual.

A SECRETÁRIA DE ESTADO DE PLANEJAMENTO E GESTÃO, no uso da atribuição que lhe confere o 93, §1º, inciso III, da Constituição do Estado e o art. 16 do Decreto nº. 44.998, de 30 de dezembro de 2008, e considerando a necessidade de estabelecer diretrizes para uma Política de Segurança da Informação,

RESOLVE:

Art.1º Fica instituída a Política de Segurança da Informação do Estado de Minas Gerais, constituída por um conjunto de diretrizes e normas que estabelecem os princípios de proteção, controle e monitoramento das informações processadas, armazenadas ou custodiadas pelos Órgãos e Entidades do Poder Executivo da Administração Pública Estadual Direta, Autárquica e Fundacional.

Art.2º A Política de Segurança da Informação se aplica a todos aqueles que exerçam, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública no âmbito dos órgãos e entidades da Administração Pública Estadual.

Art.3º Para efeitos desta Resolução se aplicam os seguintes conceitos:

I - segurança da Informação: conjunto de medidas para o estabelecimento de controles necessários à proteção das informações do Estado durante sua criação, aquisição, uso, transporte, guarda e descarte, contra destruição, modificação, comercialização ou divulgação indevidas e acessos não autorizados, acidentais ou intencionais visando à garantia da continuidade dos processos e serviços do Estado e a preservação de seus aspectos básicos, a saber: confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

II- confidencialidade: garantia de que a informação é acessível somente a pessoas autorizadas;

III- integridade: salvaguarda da exatidão e completeza da informação;

IV- disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes;

V- autenticidade: garantia de que uma informação, produto ou documento é do autor a quem se atribui;

VI- legalidade: garantia de que ações sejam realizadas em conformidade com os preceitos legais vigentes e que seus produtos tenham validade jurídica;

VII- usuário: toda pessoa a qual se aplica a Política de Segurança da Informação do Estado de Minas Gerais.

Art.4º A Política de Segurança da Informação tem como diretrizes:

I - gestão de riscos: os órgãos e entidades do Governo do Estado de Minas Gerais devem adotar o modelo de gestão de riscos para o Sistema de Gestão de Segurança da Informação;

II - proteção da informação: as informações geradas, adquiridas, armazenadas, processadas, transmitidas e descartadas pelas unidades administrativas devem ter mecanismos de proteção adequados, de forma a resguardar sua confidencialidade, integridade, disponibilidade, autenticidade e legalidade;

III - classificação da informação: as informações devem ser classificadas de forma a serem protegidas adequadamente;

IV - controle de acesso às informações: toda informação utilizada pelas unidades administrativas deve ter seu acesso controlado de acordo com a sua classificação;

V - educação em segurança da informação: os usuários devem ser instruídos a respeito da correta utilização das informações e dos recursos computacionais disponibilizados pelo Estado;

VI - responsabilidade pela segurança da informação: o usuário é responsável pela segurança das informações as quais tenha acesso;

VII - gestão de continuidade do negócio: os órgãos e entidades são responsáveis por elaborar e manter um plano de continuidade de negócios, de acordo com as suas necessidades, de forma a reduzir os impactos decorrentes da interrupção de serviços causada por desastres ou falhas da segurança.

§1º Os mecanismos de proteção devem estar em conformidade com a legislação vigente, com o Código de Conduta Ética do Servidor Público e da Alta Administração Estadual, e com a versão vigente da série 27000 da ISO.

§ 2º Até que seja estabelecida uma norma geral, as informações devem ser classificadas, em sigilosa, restrita e pública, por cada órgão ou entidade responsável por sua salvaguarda, no âmbito de sua competência, de acordo com os termos previstos em Lei.

§ 3º As informações referentes aos cidadãos, que estejam sob a custódia do Estado, devem ter seus acessos controlados e restringidos, visando a garantir, assim, o direito individual e coletivo das pessoas, a inviolabilidade de sua intimidade e o sigilo de suas informações, nos termos previstos em Lei.

SS4º O usuário deve notificar à área responsável pela segurança da informação em casos de suspeita ou violação das regras ou em caso de falhas de Segurança da Informação.

Art.5º Para os fins deste Decreto compete:

I - ao Comitê de Tecnologia da Informação e Comunicação:

a) coordenar as ações necessárias para a implantação do Modelo de Gestão de Segurança da Informação;

b) avaliar periodicamente a Segurança da Informação, por meio da análise de indicadores;

II - à área responsável pela Segurança da Informação:

a) identificar necessidades específicas de Segurança da Informação e propor as implementações necessárias;

b) elaborar documentos necessários à Segurança da Informação;

c) elaborar e manter indicadores de Segurança da Informação;

d) elaborar, manter e implementar o plano de continuidade dos negócios;

- e) elaborar programas de treinamento e de conscientização em Segurança da Informação;
- f) analisar os incidentes de segurança da informação e recomendar as correções necessárias.

III - à Auditoria-Geral do Estado e às unidades setoriais e seccionais de auditoria compete zelar pelo cumprimento do disposto nesta Resolução.

Art.6º O usuário que não cumprir as normas estabelecidas nesta Resolução estará sujeito às penalidades previstas em Lei.

Art.7º Normas complementares a essa Resolução serão expedidas por meio de Resoluções da Secretaria de Estado de Planejamento e Gestão - Seplag.

Art.8º Esta Resolução entra em vigor na data de sua publicação.

Belo Horizonte, 17 de setembro de 2009

Renata Vilhena

Secretária de Estado de Planejamento e Gestão