REVISTA DO CCEI
ISSN Impresso: 1415-2061
ISSN Online: 2356-6635
Centro de Ciências
Economia e Informática
Revista Técnico-Científica
URCAMP
EDIURCAMP

PROPOSTAE VALIDAÇÃO DE UM MODELOPARA ANÁLISE DE RISCO DE INFORMAÇÕES PESSOAIS NA INTERNET

PROPOSAL AND VALIDATION OF A MODEL FOR ANALYZING THE RISK OF PERSONAL INFORMATION ON THE INTERNET

Lucidia Assunção Silveira[1]; Érico Marcelo Hoff do Amaral1[2]; Alex Camargo[2]

Resumo: Com o aumento de serviços disponíveis na WEB, aumenta também o número de informações pessoais que são compartilhadas neste ambiente. Este estudo teve por objetivo propor e avaliar um modelo de análise de risco (MAR) para informações pessoais publicadas na Internet, o qual relacione as informações de um indivíduo ao nível de risco que a divulgação dos seus dados pode ocasionar. No intuito de avaliar o modelo proposto foi realizado um experimento com 10 indivíduos, com diferentes características pessoais, profissionais e de comportamento na rede, para os quais calculou-se o índice geral de risco através da equação desenvolvida. Observando que mesmo indivíduos que não têm acesso à redes sociais ainda têm informações vazadas.

Palavras-chave: Análise de Riscos;Segurança da informação; Vazamento de dados.

Abstract: *With the increase in services available on the WEB, it also increases the number of personal information that is shared in this environment. This study aimed to propose and evaluate a model of risk analysis (MAR) for personal information published on the Internet, which relates the information of an individual to the level of risk that the disclosure of their data may cause. In order to evaluate the proposed model, an experiment was carried out with 10 individuals, with different personal, professional and behavioral characteristics in the network, for which the general risk index was calculated through the developed equation. Noting that even individuals who do not have access to social networks still have leaked information.*

Keywords: *Data leakage;.Informationsecurity; Riskanalysis.*

1 INTRODUÇÃO

Embora pareça um termo deste milênio, já nos anos 1970, Katz (1976) estudou os efeitos legais de vazamento de informações governamentais vazadas por funcionários do governo. Ou seja, basta que organizações ou pessoas queiram manter sigilo sobre uma informação para que se tenha interesse nestas informações.

Atualmente, com a expansão na utilização de dispositivos móveis, tais como smartphones, têm facilitado a vida dos usuários, fazendo com que seja possível acessar as mais diversas aplicações por meio destes aparelhos.Porém, quando o usuário tem uma gama tão diversificada de serviços à sua disposição na

[1] Graduanda Engenharia de Computação.
{lucidiasilvera@gmail.com}

[2] Dr. Informática na Educação, Universidade Federal do Pampa (UNIPAMPA).
{ericohoffamaral@gmail.com}

[3] Msc. Engenharia de computação. Prefeitura Municipal de Bagé
{alexcamargoweb@gmail.com}

web, aliada à sensação de proteção por não estar no "mundo real", ele acaba deixando de lado a precaução e facilitando para que criminosos acabem se aproveitando dessa situação para adquirir conhecimento sobre este usuário e pessoas de seu circulo de amizades (LAM et al., 2008).

Em posse dessas informações, existem inúmeras possibilidades de crimes que podem ser cometidos, sejam eles golpes ou não. Abertura de contas em bancos, compra de bens e serviços e financiamentos de veículos, são exemplos de golpes que podem gerar muitos problemas em curto prazo para a vítima. Além disso, crimes como sequestros e invasão de domicílios vêm sendo muito facilitados graças a postagens em redes sociais, como check-ins, por exemplo (SILEO, 2013).

Com base nos fatos apresentados, percebe-se a necessidade de uma solução que conscientize o usuário sobre os perigos do compartilhamento de informações em locais de acesso livre, fornecendo a este um índice que reflita o grau de risco ao qual está vulnerável pela exposição destas informações.

Esta pesquisa apresenta, além desta seção de introdução, uma seção de referencial teórico, onde são abordados tópicos necessários para o entendimento do problema. Na seção 3 é apresentada a metodologia desenvolvida para o trabalho, seguida da seção de implementação. Na seção 5 é feita a análise dos testes realizados e, por fim, são expostas as conclusões.

2. REFERENCIAL TEÓRICO

Nesta seção são abordados temas de importância para a realização e entendimento deste trabalho, bem como trabalhos que tenham correlação com a pesquisa realizada.

2.1. VAZAMENTO DE INFORMAÇÕES

O padrão internacional de gerenciamento de segurança da informação menciona que o termo "divulgação não autorizada de informações" também pode ser usado para especificar o ato de possibilitar à pessoas o acesso a informações as quais não deveriam ter (ISO/IEC, 2005).

Molok *et al.* (2010) diz que este vazamento pode acontecer por diversos meios, como: conversas, armazenamento em nuvem, conferências e redes sociais online (OSN). De acordo com Ahmad (2013), vazamentos em OSN são os mais preocupantes, visto que no momento em que estas informações são publicadas podem ser acessadas por qualquer pessoa, indexadas pelo Google e arquivadas, tornando-as virtualmente permanentes.

Considerando, por exemplo, um perfil do Facebook[1], Cortela (2013) menciona que a gama de informações pessoais que podem ser adicionadas a um perfil é muito grande. Acrescenta ainda que aliando isto ao fato de muitos usuários preencherem o perfil completo, não atentando para as

configurações de privacidade, cria-se um grande problema. Malandrino et al. (2013) acrescentam que a tarefa de proteger a privacidade dos usuários fica ainda mais difícil porque estes não são conscientizados quanto à divulgação de informações pessoais.

Mesmo com inúmeros casos relatados e divulgação da mídia, os usuários acabam ainda postando informações, pois o "anonimato" e o fato de estar se comunicando com uma máquina, em vez de outras pessoas, torna o ato de compartilhar mais fácil (COLLINS, 2005).

Enquanto um hacker precisa de um significativo nível de exposição para obter uma informação, através das OSN é possível obtê-la sem contato físico e rastros, e quem se encarrega dessa tarefa são os engenheiros sociais (CORTELA, 2013).

2.2. ENGENHARIA SOCIAL

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT, 2000), engenharia social é o termo usado para métodos de obtenção de informações importantes de um usuário, usando a ingenuidade ou confiança da vítima. Essas informações podem ser obtidas através de ligações telefônicas, e-mails ou utilizando pesquisa em redes sociais e mecanismos de busca e recuperação de dados.Com os dados obtidos na web, seja via OSN ou não, é possível cometer inúmeros crimes, desde golpes como roubo de identidade (COELHO, 2016) a sequestros (G1, 2010), por exemplo.

Enquanto um hacker precisa de um significativo nível de exposição para obter uma informação, através das OSN é possível obtê-la sem contato físico e rastros, e quem se encarrega dessa tarefa são os engenheiros sociais (CORTELA, 2013). Com os dados obtidos na web, seja via OSN ou não, é possível cometer inúmeros crimes, desde golpes como roubo de identidade (COELHO, 2016) a sequestros (G1, 2010), por exemplo.

Segundo Mitnick e Simon (2011) fator humano é o elo mais fraco quando se trata de segurança. Dizem ainda que ataques de engenharia social são bem-sucedidos mais comumente quando as pessoas são ignorantes nas questões de boas práticas de segurança. É por isso que engenheiros sociais utilizam, muitas vezes, tecnologia de baixo custo e baixo desempenho para cometer crimes, indo contra o senso comum de que são necessárias máquinas poderosas e caras para vencer medidas de segurança de sistemas (WINKLER e DEALY, 1995).

2.3. ANÁLISE DE RISCO

Na área da computação, a tarefa de analisar riscos de ocorrência de incidentes é essencial para a gestão de segurança da informação, já que permite identificar o grau de proteção necessária, conforme apontado por Campos (2007) e Oliveira (2009).

Segundo a norma ISO/IEC 27005 (2008), que descreve procedimentos do processo de gestão de risco de segurança da informação e suas atividades, a análise de riscos identifica, quantifica ou descreve qualitativamente os riscos, tornando possível para os gestores priorizar certos aspectos de acordo com sua gravidade e critérios pré-estabelecidos.

A análise se divide em identificação e em estimativa de riscos. Na estimativa, mensura-se a consequência ou o impacto dos cenários e sua probabilidade. Esta estimativa pode ser qualitativa ou quantitativa, ambas opções oferecem vantagens e desvantagens, sendo a subjetividade e a falta de dados históricos, respectivamente, algumas das desvantagens das abordagens, conforme adiciona Silva (2009). Também é realizada uma avaliação das consequências e da probabilidade dos incidentes.

A norma 27005 esclarece, ainda, que o risco é estimado por meio da combinação entre a probabilidade de um cenário de incidente e suas consequências, fazendo com que seja possível gerenciar um risco alterando as consequências deste ou a probabilidade de que o evento ocorra (SILVA, 2009).

2.4. TRABALHOS CORRELATOS

Muita pesquisa tem sido feita quando o assunto é segurança da informação. Antes de 2013 não era possível encontrar um trabalho que relacionasse o nível de exposição de um indivíduo à quantidade e tipo de informações que este publica ou são publicadas sobre ele (SILVA *et al.*, 2014). Porém, atualmente podem ser encontradas pesquisas que realizam este tipo de cálculo, utilizando diferentes abordagens e com diferentes enfoques.

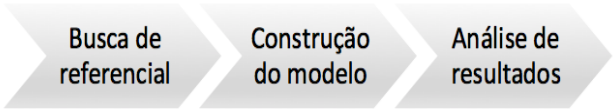
A pesquisa de Kim *et al.* (2015), por exemplo, desenvolve equações de risco para cenários diferentes, isto é, onde o atacante tem um objetivo diferente, como, spam ou perseguir, por exemplo. Cada um dos cenários resulta em informações com índices de risco diferentes e o dano potencial é calculado de forma diferente também para cada cenário, utilizando apenas o Facebook como instrumento de pesquisa das informações. Já no trabalho de Silva *et al*. (2014), foram selecionados 10 indivíduos para a realização de um estudo de caso. O objetivo desta pesquisa era analisar o grau de exposição dos dados de pessoas físicas disponíveis na web. As informações são classificadas de 1 até 4 pontos e o índice de exposição é calculado somando todos os pontos de informações encontradas sobre a pessoa.

Porém, estes trabalhos não apresentam uma abordagem mais generalizada e adequada ao cenário atual local, visto que o trabalho de Kim *et al*. foi realizado na Coréia e o trabalho de Silva *et al*. oferece um modelo com poucas informações analisadas.

3. METODOLOGIA

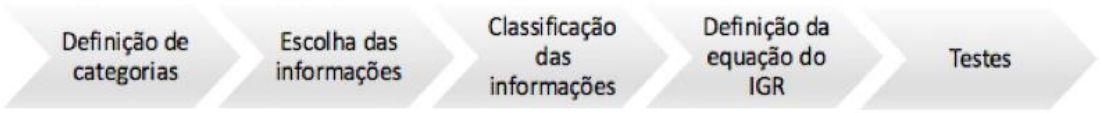
A fim de alcançar os objetivos deste estudo foi necessário um planejamento sobre os métodos a serem adotados para sua realização, esta é uma pesquisa de natureza aplicada, tendo como objetivo gerar conhecimentos que podem ser postos em prática e usados na solução de problemas específicos (SILVA e MENEZES, 2005). Na Figura 01 é possível observar a sequência de passos adotada.

Figura 01. Etapas da Metodologia



Na primeira etapa foi realizada a busca de referencial teórico que pudesse embasar o estudo. Logo após, foi realizada a segunda etapa, de construção do modelo de análise de risco. Esta etapa é dividida em sub-etapas, que são apresentadas na Figura 02.

Figura 02. Etapas da Metodologia.



O primeiro passo é a definição das categorias de informações que o modelo irá contemplar. Logo após, são escolhidas as informações que se enquadram nestas categorias e são consideradas relevantes para o estudo.

O terceiro passo envolve a classificação destas informações de acordo com o nível de risco que estas oferecem ao serem divulgadas. Esta atribuição se dá com base em informações adquiridas na pesquisa de referencial para este estudo, bem como reporte de crimes e golpes na imprensa.

Após se ter em mãos a estrutura do modelo, é definida a equação do índice geral de risco (IGR), que atribui um peso a cada uma das categorias para o cálculo do nível de risco de um indivíduo, seguido pela realização de testes deste modelo.

4. IMPLEMENTAÇÃO

Esta seção contempla a realização das etapas descritas na seção de metodologia.

4.1. DEFINIÇÃO DE CATEGORIAS E ESCOLHA DAS INFORMAÇÕES

Para a definição das categorias abordadas no estudo, tomou-se como base o método desenvolvido por Kim et al. (2015), adaptando para a realidade brasileira, visto que o estudo citado foi realizado na Coréia. Na Figura 03 é possível observar as categorias definidas por Kim et al. cinza e as desenvolvidas para este trabalho em azul.

Figura 03. Categorias do modelo.

A categoria Públicas foi dividida em 3 categorias: Básicos, que aborda informações de contato e endereço; Documentos, que contém informações referentes à documentos pessoais e; Relacionamentos, para informações de familiares.

A categoria Educação é correlata à categoria Escolaridade, assim como Informações Financeiras com Informações Bancárias. A categoria Trabalho segue com o mesmo nome. Além destas categorias, foi adicionada a categoria Automóveis, para informações de veículos, que não existia no estudo Coreano.

Com as categorias já definidas, as informações pertencentes à cada categoria foram definidas. Esta escolha se deu com base no estudo de Kim et al., adaptando para a realidade brasileira; estrutura de perfis de redes sociais e; relatos de crimes pela imprensa.

4.2. CLASSIFICAÇÃO DAS INFORMAÇÕES

Para que a resposta do modelo seja um índice numérico, fez-se necessário quantificar o risco de cada informação. Para isto foi criada uma escala de classificação de risco, que pode ser observada na Figura 04.

Figura 04. Escala de classificação de risco.

REVISTA DO CCEI
ISSN Impresso: 1415-2061
ISSN Online: 2356-6635
Centro de Ciências
Economia e Informática
Revista Técnico-Científica
URCAMP
EDIURCAMP

0	1	2	3	4	5
Irrelevante	Baixíssimo	Baixo	Considerável	Alto	Altíssimo

Para classificar foram usados os seguintes critérios: nível de individualidade que a informação oferece e comparações encontradas em estudos que envolvem tambémoutras áreas, como a sociologia (LINDAMOOD, 2009) e educação (VASCONCELOS, 2006). No caso do nível de individualidade, um exemplo seria: conhecer o endereço completo de um indivíduo é mais perigoso que saber apenas a cidade que este mora.

Para a categoria Básicos, a classificação das informações pode ser observada na Tabela 01. Pode-se observar que quanto maior detalhamento no endereço, por exemplo, maior é o índice de risco obtido.

Já para a categoria Documentos a classificação pode ser vista na Tabela 02. Os dados desta categoria são muitas vezes usados em crimes de fraude de identidade e também para obter mais confiança da vítima no momento da abordagem para algum outro golpe.

Tabela 01. Pesos para categoria básicos.

Informação		Peso
Telefone	Celular	3
	Residencial	3
E-mail		1
Nascimento	Dia+ Mês / Mês + Ano	0
	Ano + Dia + Mês	1
	Local + Ano	1
	Ano + Dia + Mês + Local	2
Endereço	Estado / Cidade	0
	Bairro	2
	CEP / Rua	3
	Número da Residência /Prédio	5

Tabela 02. Pesos para categoria documentos.

Informação	Peso
Título de Eleitor	3
Passaporte	3
RENACH	4
RG / CPF	5

Na categoria Automóveis, as informações são classificadas de acordo com a Tabela 03, sendo o maior perigo haver a combinação de placa e o Registro Nacional de Veículos Automotores (RENAVAM), pois através destas informações pode-se visualizar informações sobre o dono do veículo no site do Departamento de Trânsito.

Em Escolaridade, algumas informações dependem da idade do indivíduo ao qual pertencem visto que, sendo menor de idade o indivíduo pode ser vítima de pedófilos ou criminosos que querem extorquir dos responsáveis pela criança (VASCONCELOS, 2006). A categoria pode ser observada na Tabela 4.

Tabela 03. Pesos para categoriaautomóveis.

Tabela 04. Pesos para categoriaescolaridade.

Informação	Peso	Condicional
E.scola de E. Fundamental	1	3
Escola de E. Médio	1	3
Faculdade	1	-
Curso	1	-

Informação	Peso
Modelo	1
Placa	3
RENAVAM	3
Placa + RENAVAM	4

Embora para as informações cargo e empresa tenham sido feitas pesquisas em áreas criminais e de sociologia, não se encontrou nenhum estudo que estabelecesse níveis de perigo para estas informações, logo foi criada a convenção apresentada na Tabela 05, da categoria Trabalho.

Na categoria Informações Bancárias, as informações são comumente utilizadas em golpes de compras utilizando os dados da vítima. Os pesos de cada informação podem ser observados na Tabela 06.

Tabela 05. Pesos para categoriatrabalho.

Informação		Peso
Empresa	Instituição financeira	5
	Órgão de segurança	5
	Outros	2
Cargo	Político	4
	Proprietário / Membro de diretoria	4
	Outros	2
Registro		3
Salário		3

Tabela 06. Pesos para categoriainformaçõesbancárias.

Informação	Peso
Banco / Agência	1
Banco + Conta + Agência	3
Número do cartão	4
Cartão + C. de segurança	5
Conta + Senha da conta	5
Cartão+ Senha do cartão	5

Pode-se observar que, por exemplo, se o indivíduo ocupa um cargo em uma instituição financeira (como banco ou transportadora de valores, por exemplo), este tem um maior risco do que muitos outros indivíduos que trabalham em outros tipos de empresas que não têm contato com altas quantias em dinheiro. Recentemente, até casos de sequestro de familiares de funcionários chegaram à mídia (G1, 2017).

Por fim, na categoria Relacionamentos, as informações são classificadas da maneira exibida na Tabela 07. O condicional tem relação com o que foi estabelecido na categoria Escolaridade.

Tabela07. Pesos para categoriarelacionamentos.

REVISTA DO CCEI
ISSN Impresso: 1415-2061
ISSN Online: 2356-6635
Centro de Ciências
Economia e Informática
Revista Técnico-Científica
URCAMP
EDIURCAMP

Informação	Peso	Condicional
Filhos	1	3
Irmãos	1	3
Pais	1	3
Cônjuge	1	-
Estado civil	2	-

4.3. DEFINIÇÃO DA EQUAÇÃO DO ÍNDICE GERAL DE RISCO (IGR)

Em primeiro lugar foram definidas as faixas de risco, que podem ser observadas na Figura 05. Foram criados 10 perfis, com índices aleatórios para cada categoria, respeitando os valores máximos de cada uma (exibidos na coluna C), a fim de testar as equações que seriam desenvolvidas. Os perfis podem ser observados na Tabela 8.

Figura 05. Faixas de risco para o IGR.

0 ≤ IGR < 2	2 ≤ IGR < 4	4 ≤ IGR < 6	6 ≤ IGR < 8	8 ≤ IGR < 10
Baixíssimo	Baixo	Considerável	Alto	Altíssimo

Tabela 08. Perfis aleatórios de teste.

Categoria	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	C
Básicos	1	0	1	2	5	2	3	1	0	0	5
Documentos	0	3	3	4	5	4	5	0	3	5	5
Inf. Bancárias	0	3	5	5	1	3	0	0	1	5	5
Automóvel	4	0	1	4	1	1	0	4	4	1	4
Relacionamentos	2	3	1	3	2	2	3	1	0	1	3
Escolaridade	1	1	3	1	0	0	0	1	3	3	3
Trabalho	5	4	0	0	3	2	2	3	5	0	5

A partir destes perfis, passou-se ao processo de determinação da equação do IGR. Em todos os testes os índices das categorias Documentos e Inf. Bancárias apresentam maior peso dentro da equação, visto que estas informações são consideradas mais sensíveis (MADDEN, 2014), (UTICA, 2017), ou seja, há uma maior probabilidade de estas serem usadas caso encontradas por criminosos.

1. Proposta de Equação 1

No primeiro teste, assumiu-se uma equação de média ponderada tradicional. Em um cálculo de média ponderada os pesos atribuídos a cada valor diferem e são conhecidos a priori (LOPES e MORAN, 1999). Assim, chegou a Equação 01. Sendo B para a categoria Básicos, D para Documentos, $ para Informações Bancárias, C para Automóveis, T para Trabalho, E para Escolaridade e R para Relacionamentos. Os resultados para os 10 perfis determinados é apresentado na Tabela 09.

Equação 01

$$IGR = \frac{4*B + D*5 + \$*5 + C*3 + T*2 + E*1 + R*2}{22}$$

Tabela 09. IGR para perfis aleatórios.

A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	C
1,5	2,1	2,4	3,3	2,9	2,5	2,2	2,3	2,1	2,7	5,27

REVISTA DO CCEI
ISSN Impresso: 1415-2061
ISSN Online: 2356-6635
Centro de Ciências
Economia e Informática
Revista Técnico-Científica
URCAMP
EDIURCAMP

Como pode ser observado, os índices não se adequaram às faixas definidas e, em perfis onde a categoria Documentos e a categoria Inf. Bancárias têm índice alto (como o perfil A10), onde o IGR deveria ser o mais próximo possível do máximo, ele não chega nem à metade do máximo observado (5,27). Logo, a equação foi descartada.

2. Proposta de Equação 2

Para esta equação, optou-se por dar maior peso para as categorias mais sensíveis e adequar o resultado às faixas de risco estabelecidas. Assim, alcançou-se a Equação 02.Seus resultados podem ser observados na Tabela 10.

Equação 02

$$IGR = \frac{\frac{4*B + C*3 + T*2 + E*1 + R*2}{12} + \frac{D*5 + \$*5}{2}}{3}$$

Tabela 10. IGR para perfis aleatórios.

A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	C
0,9	3,2	7	8,25	6,6	6,25	4,8	0,7	4	8,5	9,75

Esta equação acabou sendo considerada inadequada, pois observou-se que, em contrapartida à anterior, as categorias mais sensíveis ocuparam uma porcentagem muito grande do IGR, e as outras 5 categorias não eram levadas tão em conta. Além disso, o IGR tinha um máximo de 9,75, sobrando alguns décimos na escala de classificação que poderiam ser melhor aproveitados pelas outras categorias.

3. Proposta de Equação 3

Para esta equação optou-se por atribuir um valor máximo de 80% do IGR para as categorias mais sensíveis e distribuir o restante para as outras categorias. Também visou-se explorar mais as faixas de risco, chegando o mais perto possível do máximo da escala (10), conforme apresentado na Equação 03. O resultado do IGR para os 10 perfis aleatórios pode ser observado na Tabela 11.

Equação 03.

$$IGR = (\$ + D)*0{,}8 + B*0{,}2 + C*0{,}05 + T*0{,}06 + E*0{,}033 + R*0{,}133$$

Tabela 11. IGR para perfis aleatórios.

A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	C
0,999	7,632	6,882	8,232	6,296	6,436	5,119	0,746	2,999	8,282	9,998

Pode-se observar que se chegou muito perto dos 10 pontos de IGR, assim como os perfis com índices altos nas categorias sensíveis (como o perfil A10) têm um IGR que se encaixa na faixa mais alta. Assim, esta equação foi considerada adequada e é a equação adotada no modelo.

4.4. EXPERIMENTOS

Após a identificação da equação mais adequada para o IGR, foram definidos 10 perfis reais, com características diferentes a serem exploradas, estes perfis são exibidos na Tabela 12.

As informações pessoais destas pessoas foram pesquisadas manualmente na web e, através dos dados encontrados foram atribuídos os pesos de cada categoria, que corresponde ao maior peso encontrado dentro das informações da categoria. O número de informações encontradas para cada perfil pode ser observado na Tabela 13.

Tabela 12. Perfis reais de teste.

Identificador	Descrição
P1	Alguém da família próxima
P2	Alguém muito conhecido
P3	Alguém da família mas que não tem acesso à Internet
P4	Alguém que tenha perfil no Facebook
P5	Alguém que passou em um concurso público e seja conhecido
P6	Alguém que trabalhe em instituição financeira e seja conhecido
P7	Alguém que seja professor de universidade Federal
P8	Alguém que seja menor de idade
P9	Alguém que passou em concurso público e seja desconhecido
P10	Alguém que foi candidato à cargo político

Tabela 13. Número de informações encontradas para cada perfil.

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
4	10	6	12	11	12	15	6	12	17

O IGR foi calculado, então, para cada um destes indivíduos.

5. RESULTADOS E CONCLUSÃO

Para a criação do modelo, desde definição de quais informações seriam analisada até a determinação do peso dessas informações e das categorias nas quais são divididas, bem como a criação da equação do IGR, foi necessário um processo longo de pesquisa bibliográfica.

Assim, os testes com perfis reais foram necessários para verificar se o modelo criado era válido, bem como analisar características de informações encontradas para cada perfil diferente, desde pessoas que não têm acesso à Internet até pessoas com vida pública. Desta maneira, o resultado dos testes dos perfis reais pode ser observado na Tabela 14.

Tabela 14. Resultados do teste de perfis reais.

CATEGORIA	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
Básicos	0	1	5	0	3	5	3	1	5	3
Documentos	0	0	0	0	0	0	5	0	5	5
Banco	0	0	0	0	0	0	0	0	0	0
Automóvel	0	0	0	0	0	0	0	0	0	0
Relacionamentos	2	2	0	2	2	0	2	0	1	2
Escolaridade	1	1	0	1	0	1	1	3	0	1
Trabalho	0	0	0	0	3	5	2	0	0	4
IGR	0,299	0,499	1	0,299	1,046	1,333	5,019	0,299	5,133	5,139

Pode se observar que informações bancárias e de automóveis não foram encontradas para nenhuma destas pessoas, sendo o primeiro caso um fator que impacta mais no resultado do IGR, visto que a categoria de Inf. Bancárias é uma das mais pesadas.

Das 105 informações encontradas para os 10 perfis, 45 foram encontradas em perfis do Facebook, o que reflete o que foi levantado nas pesquisas para referencial, de que as OSN são grandes fontes de vazamento de informações. Porém, através do perfil 2 pode se verificar que, mesmo que a pessoa não tenha acesso à Internet, isso não quer dizer necessariamente que ela está livre dos riscos de vazamento de informações.

Também pode se observar que pessoas que têm uma vida pública (perfis 7, 9 e 10, por exemplo) apresentam maior IGR, visto que mais dados pessoais destas pessoas são divulgados.

O controle das informações que são publicadas na web, embora difícil, é muito necessário, visto que pode se descobrir informações relacionadas à todos os aspectos da vida de uma pessoa analisando os rastros dela online, porém, nem sempre se tem este controle, visto que a empresa onde se trabalha ou amigos podem revelar informações que podem ser úteis para criminosos.

Visualizando a conscientização, é importante que o modelo que este usuário usará seja adequado e coerente e não algo imparcial e sem justificativa de escolha, por isto este trabalho consistiu em várias etapas de construção bem definidas, com propostas de equação distintas testadas, a fim de se definir a que melhor se adequa à proposta do modelo e ao contexto em que se vive.

REFERÊNCIAS

AHMAD, Atif. Disclosureoforganizationalinformationon social media: Perspectives fromsecurity managers. 2013.

Associação Brasileira de Normas Técnicas. NBR ISSO/IEC 27005: Gestão de risco de segurança da informação. Rio de Janeiro, 2008.

Campos, A. Sistema de Segurança da Informação: Controlando os Riscos. 2007. Florianópolis: Visual Books, 2. Ed.
CERT. Cartilha de Segurança da Internet. 2000. http://cartilha.cert.br/sobre/old/cartilha_seguranca_1.0.pdf. Acesso em: 4 de maio de 2017.

COELHO, Rute. Roubo de identidade aumenta de expressão nas redes sociais. 2016. http://www.dn.pt/sociedade/interior/roubo-de-identidade-aumenta-de-expressao-nas-redes-sociais-5007344.html. Acesso em 17 de maio de 2017.

COLLINS, Brendan. Privacyandsecurityissues in Social Networking. 2005. https://www.fastcompany.com/1030397/privacy-and-security-issues-social-networking. Acesso em 2 de fevereiro de 2017.

CORTELA, João José Corrêa. Engenharia social no Facebook. 2013. Tese de Doutorado. Dissertação de Mestrado-Universidade Estadual de Londrina, Londrina, PR.

G1. Quadrilha escolhia vítimas para sequestro pela internet, diz polícia. 2010. http://g1.globo.com/sao-paulo/noticia/2010/08/quadrilha-escolhe-vitimas-para-sequestro-pela-internet-diz-policia.html. Acesso em: 3 de janeiro de 2017.

G1. Criminosos sequestram família de tesoureiro do Banco do Brasil em Resende. 2017. http://g1.globo.com/rj/sul-do-rio-costa-verde/noticia/criminosos-sequestram-familia-de-tesoureiro-do-banco-do-brasil-em-resende.ghtml. Acesso em 10 de julho de 2017.

KATZ, Alan M. GovernmentinformationleaksandtheFirstAmendment. California Law Review, p. 108-145, 1976.

KIM, Pyong, LEE, Younho e KHUDAYBERGENOV, Timur. A method for quantitativemeasuringthedegreeofdamagebypersonalinformationleakage. JournaloftheKoreaInstituteofInformation Security andCryptology, v. 25, n. 2, p. 395-410, 2015.

LAM, Ieng-Fat; CHEN, Kuan-Ta; CHEN, Ling-Jyh. Involuntaryinformationleakage in social network services. International Workshop on Security. Springer Berlin Heidelberg, 2008. p. 167-183.

LINDAMOOD, Jack et al. Inferringprivateinformationusing social network data. Proceedingsofthe 18th internationalconferenceon World wide web. ACM, 2009. p. 1145-1146.

LOPES, Celi Aparecida Espasandin; MORAN, R. C. C. P. A estatística e a probabilidade através das atividades propostas em alguns livros didáticos brasileiros recomendados para o ensino fundamental. In: CONFERÊNCIA INTERNACIONAL "EXPERIÊNCIAS E EXPECTATIVAS DO ENSINO DA ESTATÍSTICA PARA O SÉCULO. 1999. p. 20-22.

MADDEN, Mary. AmericansConsiderCertainKindsof Data tobe More Sensitivethan Others.http://www.pewinternet.org/2014/11/12/americans-consider-certain-kinds-of-data-to-be-more-sensitive-than-others/. Acesso em 5 de abril de 2017.

MALANDRINO, Delfina et al. Privacyawarenessaboutinformationleakage: Who knowswhataboutme?.Proceedingsofthe 12th ACM workshop on Workshop onprivacy in theelectronicsociety. ACM, 2013. p. 279-284.

MITNICK, Kevin D. e SIMON, William L. The artofdeception: Controllingthehumanelementofsecurity. John Wiley& Sons, 2011.

MOLOK, NurulNuha Abdul, AHMAD, Atif e CHANG, Shanton. Understandingthefactorsofinformationleakagethrough online social networking tosafeguardorganizationalinformation. 2010.

OLIVEIRA, Maria Angélica Figueiredo; NUNES, Raul Ceretta; ELLWANGER, Cristiane. Uma metodologia seis sigma para implantação de uma gestão de segurança da informação centrada na percepção dos usuários. Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, p. 173-186, 2009.

SILEO. Facebook Status Update Leads toRobbery. 2013. http://www.sileo.com/facebook-status-update-leads-to-robbery/. Acesso em 3 de julho de 2017.

SILVA, Edna Lúcia da; MENEZES, EsteraMuszkat. Metodologia da pesquisa e elaboração de dissertação. 2001.

SILVA, Narjara Bárbara Xavier, DE ARAÚJO, Wagner Junqueira e DE AZEVEDO, Patrícia Morais. 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, v. 6, n. 2, 2014.

SILVA, Pedro JS. Análise/Avaliação de Riscos de Segurança da Informação para a Administração Pública Federal: um enfoque de alto nível baseado na ISO/IEC 27005.[Sl], 6 2009. Monografia de Conclusão de Curso (Especialização) - Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília, 2009.

UTICA COLLEGE. Center for Identity Management andInformationProtection. Most common schemes. http://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm. Acesso em 2 de maio de 2017.

VASCONCELOS, Ana Maria Pinheiro et al. Navegar com segurança: protegendo seus filhos da pedofilia e da pornografia infanto-juvenil na internet. 2006.

WINKLER, Ira S.; DEALY, Brian. Information Security Technology? Don'tRelyon It. A Case Study in Social Engineering. USENIX Security. 1995.