ESPECIALIZAÇÃO EM SEGURANÇA CIBERNÉTICA

LEIS E REGULAMENTAÇÕES

Filipe Sousa
Gelson Filho
Rodrigo Camargo
Otávio Marelli

Prof MSc Nilton Stringasci Moreira

Atividade Avaliativa

1) Escolha uma empresa no mercado de um segmento que possua uma grande quantidade de dados pessoais e dados pessoais sensíveis. A empresa infere que existem diversas áreas que possuem dados pessoais e/ou dados pessoais sensíveis armazenadas em suas máquinas, em arquivos Word, Excel, PDF, PPT, além de também terem tais informações armazenadas em banco de dados. Como detectar se existem informações nas estações de trabalho em base de dados não estruturadas e quais são elas? Disserte sobre como poderia ser realizado na prática, para uma grande empresa e para uma empresa de pequeno porte.

Para a operação de uma empresa locadora de automóveis, as atendentes presenciais realizam a coleta de dados de seus clientes durante o processo de locação. Entre essas informações estão dados que identificam claramente o cliente, como o próprio nome, os dos pais, data de nascimento, número da carteira de motorista, número do registro geral, endereço residencial, foto da carteira nacional de habilitação, entre outras informações.

Dessa forma os dados armazenados a princípio na máquina da atendente, onde foi tirada cópia da CNH e a coletada foto do cliente no local, em seguida esses mesmos dados são utilizados para elaboração do contrato que também é scaneado e armazenado localmente e posteriormente tais dados são carregados para o banco de dados remoto da empresa.

É espero que as informações como a cópia da CNH e do contrato com dados do cliente são removidas da máquina uma vez que a Lei Geral de Proteção de dados (Lei 13.709 de 2018) impõe que empresas e órgãos públicos devem tratar os dados pessoais de seus clientes, parceiros e funcionários de maneira transparente e ética em relação ao uso dessas informações. Sob o tratamento de dados entendesse que inclua todas as operações realizadas com dados pessoais, tais como:

- Coleta;
- Classificação;
- Armazenamento;
- Eliminação;
- Difusão;
- Aplicação.

Dessa forma como citado anteriormente, a primeira etapa de tratamento e limpeza de dados sensíveis fora de bases de dados estruturadas que devem ser tratadas é logo nas estações de trabalho dos atendentes e nas impressoras/scanners das bases físicas de retirada de veículos.

Onde é observado que durante o aluguel dos veículos é feito a impressão do contrato para assinatura física, o que gera um documento físico com informações sensíveis do cliente que poderia ser facilmente substituído por um sistema de assinatura digital, altamente difundido nos dias atuais, o que mitigaria problemas como perda de documento, vazamento do arquivo scaneado e armazenado na máquina local, etc.

Outra medida plausível é a adoção de ferramentas que impeçam a persistência de arquivos do tipo, onde por exemplo, é feita e remoção deles após a submissão ao banco de dados gerais da empresa, onde haverá maior controle

deles, como a adoção de catalogação das informações contidas neles, controle de acesso, etc.

Também é possível realizar a adoção de softwares do tipo “Data Loss Prevention” (DLP) que são responsáveis por ajudar a evitar o compartilhamento, transferência ou uso inseguro ou inapropriado de dados sensíveis, principalmente nos setores que possam ter acesso a esse tipo de informação como por exemplo, a área jurídica que possa estar avaliando algum contrato.

Por fim atuar sobre o elo mais fraco dessa cadeia se dá no treinamento dos colaboradores conscientizando-os sobre os riscos envolvidos no mal manuseio desse tipo de informações, a conscientização das políticas de segurança da empresa, e o papel de cada um na manutenção e aplicação das normativas descritas na LGPD.

2) Realize uma pesquisa e relate todas as formas e tecnologias a nosso dispor, para atender ao requisito da Lei intitulado “Anonimização”

De acordo com a Lei Nº 13.709, de 14 de agosto de 2018, dado anonimizado pode ser considerado todo dado pertencente a um titular que não possa ser identificado. “Anonimização”, por outro lado, caracteriza-se pela utilização de técnicas de tratamento de dados a fim de torná-lo anonimizado, impedindo que esse dado possa ser utilizado para associar direta ou indiretamente um indivíduo.

Dentre as técnicas que atualmente podem ser utilizadas para realizar a anonimização se encontram:

- Máscara de dados, ou encobrimento de caracteres: Consiste em ocultar parte ou todo o dado que está sendo tratado. Um exemplo comum é a utilização de asteriscos, ou outros símbolos. Ao adentrar uma universidade com reconhecimento facial, a câmera ao reconhecer o estudante exibe o CPF dele no visor, porém a fim de tornar esse dado anonimizado é necessário ocultar parte do CPF, exibindo portanto somente os três primeiros e o último dígito: “111*******1”;
- Supressão de dados: Esta técnica consiste em eliminar parcialmente dados sensíveis, como a remoção de datas de nascimento, mantendo apenas a idade, mas não é uma técnica tão confiável, uma vez que dados poderiam ser “inferidos” ou resgatados;
- Generalização: Esta técnica, quando aplicada, transforma os dados específicos em um outro conjunto de dados. Uma idade com o valor de “30” poderia ser transformada em um conjunto de números como “40-80”. Embora ainda não seja uma técnica tão amplamente aplicada, uma vez que valores numéricos são mais facilmente generalizados, enquanto textos e outros campos mais complexos como documentos pessoais apresentam ainda maiores desafios para a generalização. Apesar disso, em alguns casos pode ser útil aplicar a generalização aliada à outras formas de anonimização, como a supressão de dados, por exemplo.
- Adição de ruídos: É uma técnica que consiste em adicionar perturbações aos dados de um dataset específico, alterando de forma

aleatória os valores ali presentes, dificultando a identificação dos dados originais;

- Agregação de dados: Essa técnica de anonimização consiste em “resumir” os dados presentes no dataset, simplificando grandes conjuntos de dados e permitindo que estes apresentem menos entradas, diferenciando-se da generalização por modificar os dados de forma ativa;
- Hashing: Esta técnica aplica uma função matemática aos dados a fim de transformá-los em uma sequência de caracteres irreversível. Mesmo que sejam feitas pequenas alterações como de “Teste1” para “Teste2”, as técnicas de hashing devem ser capazes de gerar hashes completamente diferentes para estes dois valores, sendo uma técnica muito empregada ao salvar senhas em um banco de dados, dessa forma, mesmo que um atacante obtenha o banco de dados com as senhas dos usuários, não será capaz de obtê-las através de uma “função reversa”, pois esta é uma das características de hashing.

Um exemplo prático que pode ser dado quanto à anonimização de dados é um cenário no qual uma empresa realiza uma pesquisa de mercado, e durante essa pesquisa obtém dados dos entrevistados como nome, rg, ou outros dados sensíveis, que possam caracterizá-lo. Estes dados passam por um processo de hashing, uma das técnicas citadas acima, e a partir deste momento deve ser quase impossível retornar os dados aos valores iniciais correspondentes, portanto mesmo que a empresa sofra um ataque de agentes maliciosos e esse banco de dados seja vazado, os dados pessoais permanecem seguros, pois o atacante não poderá revertê-los aos valores originais, atendendo portanto ao critério de “Anonimização” da LGPD.

3) Realize uma pesquisa e relate todas as formas e tecnologias a nosso dispor, para atender ao requisito da Lei intitulado “Pseudonimização”

De acordo com a Lei Nº 13.709, de 14 de agosto de 2018, a pseudonimização de dados também é caracterizada por tratamentos tecnológicos por meio dos quais os dados passam a não mais poder serem utilizados para realizar associação direta ou indireta a um indivíduo, senão por uso de informações adicionais que estejam guardadas pelo controlador/administrador dos dados em um ambiente separado, seguro e devidamente controlado.

Dentre as técnicas que atualmente podem ser utilizadas para realizar a pseudonimização se encontram:

- Tokenização: Essa técnica consiste na substituição dos dados sensíveis por “Tokens”, uma sequência única de caracteres que passa a ser utilizada para representar o dado, e está restrito a um sistema de mapeamento seguro. Este sistema é mantido em um ambiente controlado externo ao dataset, pois ter acesso aos dados de mapeamento tornaria possível realizar a associação direta dos tokens com os dados originais. Este sistema é comumente utilizado por instituições financeiras a fim de proteger os dados de seus clientes, como números de cartões de crédito;
- Criptografia: A criptografia, assim como o uso de hashes, trata-se de uma função matemática que é aplicada aos dados a fim de transformá-

los em um valor ininteligível, porém a diferença consiste no fato de que na criptografia são geradas chaves, tendo muitas vezes um sistema de chave pública e chave privada, e somente aqueles que tenham acesso a essas chaves é que podem realizar a leitura dos dados através de uma função de criptografia reversa que é realizada quando a chave correta é utilizada;

- Pseudônimos: Essa técnica é pouco utilizada, mas consiste na utilização de pseudônimos como nomes fictícios ou códigos que são utilizados para substituir informações sensíveis. Essa técnica pode ser facilmente rastreada diretamente aos dados originais, portanto é pouco recomendada, e se utilizada, deve ser utilizada em conjunto com outras técnicas a fim de garantir a segurança dos dados.

Em um cenário prático, uma empresa que armazena os dados de seus clientes, mas precisa utilizar esses dados para um fim específico e deseja armazená-lo de forma segura poderia utilizar técnicas de criptografia para realizar a pseudonimização dos dados, dessa forma seria possível utilizar a chave para descriptografar estes dados e retorná-los aos valores originais para executar o fim específico desejado, em seguida os dados poderiam ser criptografados novamente para serem salvos no banco, tornando o armazenamento seguro, ainda que seja possível recuperar os dados caso se tenha a chave.

4) Escolha 5 formas de tratamento descritas a seguir, assim como preconiza a Lei 13.709 (LGPD) e, relate como elas podem ser realizadas na empresa de forma segura. São elas: tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Inicialmente deve-se identificar o valor de cada documentação. Depois de realizar uma pesquisa consolidação de um modelo sucinto com diretrizes definidas para classificação, rotulagem e manuseio das informações que podem ser adotados dentro de nosso processo.

Diretrizes:

- As pessoas somente devem possuir acesso às informações que sejam necessárias, direta ou indiretamente, ao desenvolvimento de suas atividades de trabalho e demais responsabilidades associadas.
- A classificação da informação deverá ser realizada pelos gestores de cada área ou colaboradores designados por eles.
- O gestor deve garantir que todas as informações que compete a ele e sua área, esteja devidamente classificado e rotulado.
- Todos os colaboradores são responsáveis por tratar as informações de acordo com o seu nível de classificação, seguindo as diretrizes de tratamento aqui estipuladas.

- Periodicamente poderá ser realizado um processo de auditoria, monitoramento e medição para verificar a aderência no processo de classificação e tratamento da informação, a modo de obter métricas, sugestão de melhoria e para criar plano de ação.

Nível de classificação:

Níveis de Classificação	Características
Pública	Informações que podem ou devem ser divulgadas publicamente. A divulgação deste tipo de informação não causa problemas a Instituição ou a seus clientes, funcionários e parceiros, podendo ser compartilhada livremente com o público em geral, desde que seja mantida sua integridade.
Interna	Informações internas são aquelas divulgadas a todos os colaboradores e prestadores de serviços, desde que estes estejam comprometidos com a confidencialidade das informações.
Reservada	Informações confidencial são aquelas restritas a um determinado grupo, área ou cargo, que necessitem conhecê-las para o desempenho de suas tarefas profissionais na instituição.
Secreta/Confidencial	Informações Secretas/Confidenciais são aquelas que requerem um tratamento especial, pois cuja divulgação não autorizada ou acesso indevido, pode gerar prejuízos financeiros, legais, normativos, contratuais ou na reputação, imagem ou estratégia da Instituição.

Rotulação da informação

- Todas as informações da Instituição devem ser rotuladas com no mínimo o nível de classificação atribuída, grupo de acesso e data de criação;
- A rotulação da informação deve estar clara o nível de classificação e o grupo de acesso.
- A extração de sistemas de informações, deve conter rótulos apropriados da classificação da informação.
- O responsável pela rotulação da informação é o mesmo que fez o processo de classificação.
- Informações armazenadas em servidores de arquivos e outros dispositivos de armazenamento, devem possuir rótulo claro de grupo de acesso, sendo pasta compartilhada deve possuir bloqueio para acesso não autorizado.
- Os documentos em meios digitais devem possuir cabeçalho/rodapés, informando a categoria da informação.

Tratamento da Informação

- O tratamento adequado da informação deve prover maior controle e proteção, visando garantir sua confidencialidade, integridade e disponibilidade;
- O tratamento, cuidado e zelo com a informação, deve ser igual a todos, independentemente da pessoa, cargo ou área, para as mais diversas situações.

Segue uma figura referencial das diretrizes para o tratamento das informações em função do tipo de cenário e do nível de classificação.

Cenário	Público	Interno	Reservado	Secreto/confidencial
Acesso Lógico ou Físico	Sem Restrições	Somente para colaboradores da Instituição	Somente pessoas do grupo de acesso	Somente pessoas do grupo de acesso. Adicionalmente devem ser consideradas técnicas de proteção e integridade.
Armazenamento em arquivos digitais (rede)	Sem Restrições	Somente nos servidores de arquivos na rede da Instituição	Somente nos servidores de arquivos na rede da Instituição e com controle de acesso.	Somente nos servidores de arquivos na rede da Instituição e com controle de acesso. Preferencialmente com mais um nível de acesso (ex. criptografia).
Reprodução (impressa ou digital)	Sem Restrições	Somente para os colaboradores da Instituição	Somente para o grupo de acesso ou para outras pessoas somente com autorização do gestor responsável.	Somente com a autorização do gestor responsável.
Transmissão Digital	Sem Restrições	Interno, sem restrições. Para fora da Instituição, é necessário a autorização do gestor responsável.	Somente para o grupo de acesso. Para fora do grupo de acesso, é necessária a autorização do proprietário da informação.	Somente para o grupo de acesso. Para fora do grupo de acesso, é necessária a autorização do proprietário da informação. Adicionalmente devem ser consideradas técnicas de proteção e garantias de integridade.
Eliminação de mídia digital e/ou analógica	Sem Restrições	Somente dentro das áreas da Instituição	O dispositivo deverá ser destruído fisicamente ou as informações devem ser destruídas, apagadas ou sobre gravadas por meio de técnicas que tornem as informações originais irrecuperáveis.	O dispositivo deverá ser destruído fisicamente ou as informações devem ser destruídas, apagadas ou sobre gravadas por meio de técnicas que tornem as informações originais irrecuperáveis.

A classificação da informação deverá ser realizada pelos gestores de cada área, cabe aos profissionais da Segurança da Informação garantir que os requisitos de cada nível sejam devidamente atendidos. A efeito de exemplo, classifica-se os dados adquiridos pela relação clientes/empresa como secreto ou confidencial, visto que podem conter informações privadas dos clientes ou colaboradores. Uma vez classificado com este nível devem-se considerar técnicas para garantir confidencialidade e integridade dos dados, tais como, medidas de segurança, na transferência e recebimento destes dados. Assim como um diferente tipo de tratamento para cada cenário.

Uma vez que informação são recursos estratégicos para as organizações, em sua maioria é comum o não compartilhamento da forma ou metodologia que utilizam para classificação, rotulagem e tratamento de seus dados, os quais poderiam contribuir para o enriquecimento do modelo proposto.

Referencias Bibliográficas

Tecnologia da Informação-Técnicas de Segurança – Código de Prática para controles de segurança da informação, NBR ISO/IEC 27002:2013, ABNT - Associação Brasileira de Letras, Rio de Janeiro, 2013.

L. S. Mendes, "Transparência e privacidade : Violação e proteção da informação pessoal na sociedade de consumo", publishedVersion, reponame:Repositório Institucional da UnB, 2008. Consult. 2022-11-05. [Em linha]. Disponível: http://repositorio.unb.br/handle/10482/4782

D. Santos e N. Rodrigues, "Política de armazenamento, anonimização e descarte", ÁLAMO ENGENHARIA S/A, São Paulo/SP, P(LGPD)07, junho de 2021. Consult. 2022-11-01. [Em linha]. Disponível: https://alamoengenharia.com.br/wp-content/uploads/2021/05/PLGPD07-Politica-de-Armazenamento-Anonimizacao-e-Descarte-Rev-01.pdf

B. Reis, J. Mota e P. Oliveira. "Classificação da informação". Universidade Católica de Brasília (UCB), Campos Universitário II, SGAN 916 – Módulo B – Brasília – DF – Brasil. http://www.lyfreitas.com.br/ant/artigos_mba/artclassinfo.pdf (consult. 2022-11-01).