LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Do Planejamento à Prática

THE FORENSE | SUA SEGURANÇA DIGITAL

SUMÁRIO

TUDO TEM SEU PREÇO!

TWITTER FACEBOOK E-MAIL INSTAGRAM WHATSAPP

SUA PRIVACIDADE EM TROCA DE SERVIÇOS !

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A Lei no. 13.709/2018, conhecida como a Lei Geral de Proteção de Dados - LGPD, regulamenta o tratamento de dados pessoais.

Onde estão esses dados?

Meio Físico

Meio Digital

Por quem?

Pessoa Natural

Pessoa Jurídica

Quais áreas?

Direito Público

Direito Privado

OBJETIVO

Garantia de transparência, proteção e privacidade quanto ao uso dos Dados Pessoais coletados por empresas, ou outras pessoas físicas, no território brasileiro.

ENTROU EM VIGOR EM 18 DE SETEMBRO DE 2020.

CONCEITOS BÁSICOS DA LGPD

CONCEITOS BÁSICOS DA LGPD

DADO PESSOAL

Informação relacionada a pessoa natural identificada ou identificável. Exemplo: nome, cpf, título de eleitor.

DADO PESSOAL SENSÍVEL

- Origem Racial ou Étnica
- Convicção Religiosa
- Opinião Política
- Filiação Sindical
- Dado referente à Saúde ou à Vida Sexual
- Dado Genético ou Biométrico

DADO ANONIMIZADO

Dado relativo ao titular que não possa ser identificado.

CONSENTIMENTO

Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada

ANONIMIZAÇÃO

Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo

CONCEITOS BÁSICOS DA LGPD

TITULAR

Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

CONTROLADOR

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

OPERADOR

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

ENCARREGADO

Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)

AUTORIDADE NACIONAL (ANPD)

Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional

PRINCÍPIOS DA LGPD

10 PRINCÍPIOS DA LGPD

1

Finalidade

Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular.

2

Adequação

Compatibilidade do tratamento com as finalidades informadas ao titular.

3

Necessidade

Limitação do tratamento ao mínimo necessário para a realização de suas finalidades.

4

Livre Acesso

Consulta facilitada e gratuita sobre a forma e a duração do tratamento.

5

Qualidade dos Dados

Exatidão, clareza, relevância e atualização dos dados.

6

Transparência

Informações claras.

7

Segurança

Utilização de medidas técnicas e administrativas adequadas a proteger os dados pessoais.

8

Prevenção

Adoção de medidas para prevenir a ocorrência de danos.

9

Não Discriminação

Proíbe a realização do tratamento para fins discriminatórios ilícitos ou abusivos.

10

Responsabilização e Prestação de Conta

Adoção de medidas eficazes e capazes de comprovação.

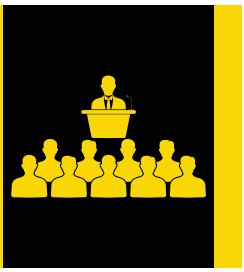
TRATAMENTO DE DADOS PESSOAIS

TRATAMENTO DE DADOS PESSOAIS

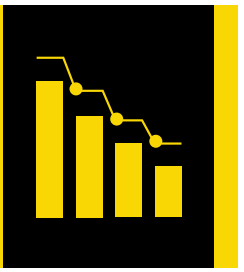
Mediante consentimento pelo titular.

Cumprimento de obrigação legal pelo controlador.

Tratamento de dados em políticas públicas.



Estudos por órgãos de pesquisa.



Execução de contrato.

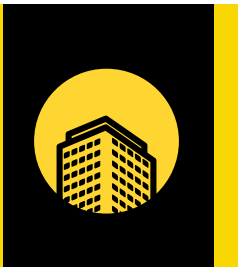
TRATAMENTO DE DADOS PESSOAIS

Exercício regular de direitos.

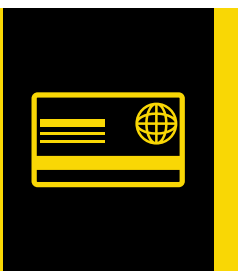
Proteção da vida.

Tutela da saúde.

Atender aos interesses legítimos do controlador.



Proteção do crédito.

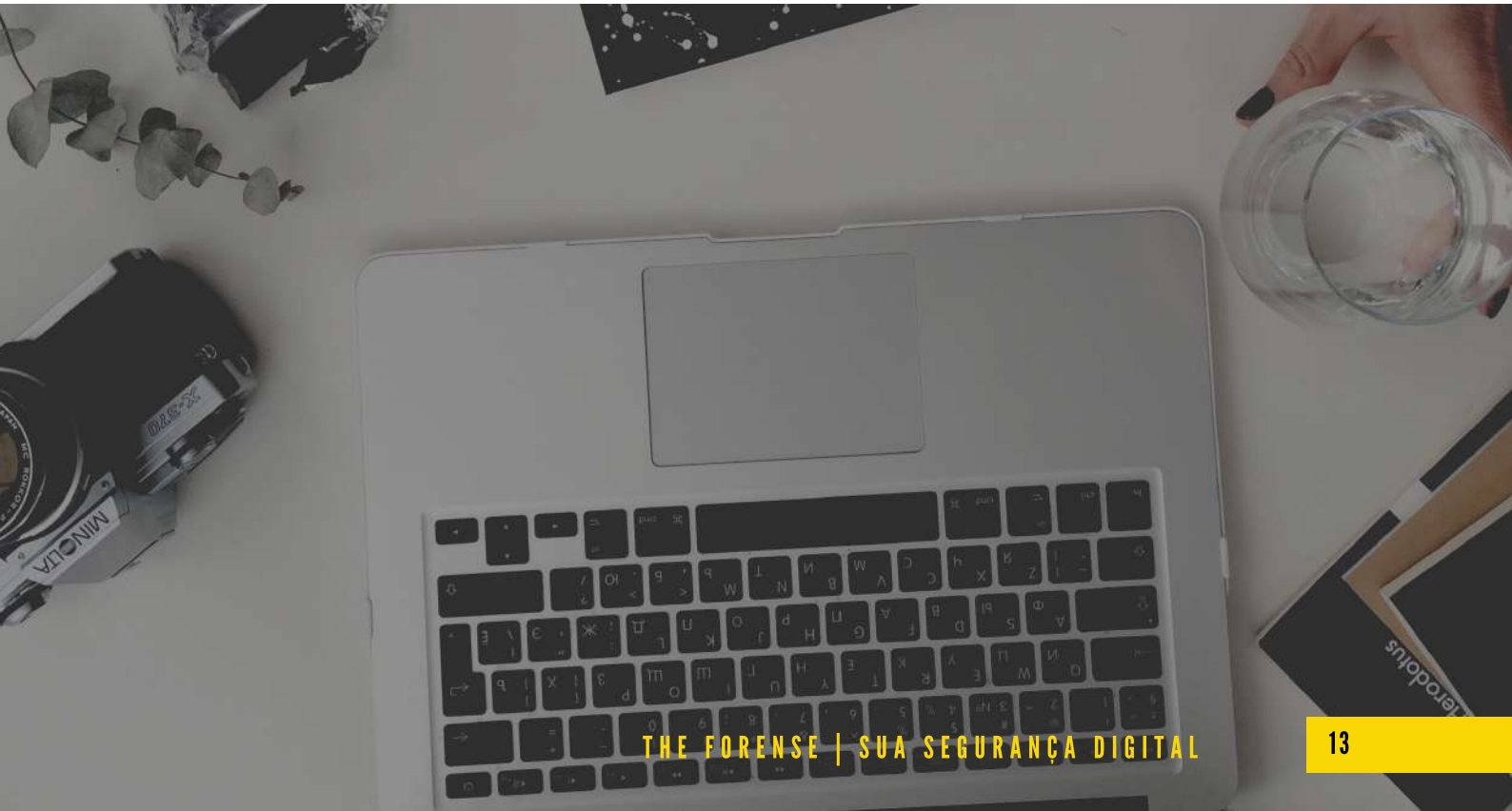


NÃO APLICAÇÃO DA LGPD NO TRATAMENTO DOS SEGUINTES DADOS

- Realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

- Realizado para fins exclusivamente:
  - Jornalístico e Artísticos; ou
  - Acadêmicos.

- Realizado para fins exclusivos de:
  - Segurança pública;
  - Defesa nacional;
  - Segurança do Estado;
  - Atividades de investigação e repressão de infrações penais.



DIREITOS DOS TITULARES

DIREITOS DOS TITULARES

1. Confirmação da existência de tratamento e oposição ao tratamento, se irregular;
2. Acesso aos dados;
3. Correção de dados incompletos, inexatos ou desatualizados;
4. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados ilicitamente;
5. Portabilidade dos dados a outro fornecedor de serviço ou produto;

DIREITOS DOS TITULARES

6 Eliminação dos dados pessoais;

7 Ser informado pelas entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

8 Ser informado sobre a possibilidade de não consentir com o tratamento de dados;

9 Revogação do consentimento;

10 Reclamação à Autoridade Nacional.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS

AUTORIDADE NACIONAL DE PROTEÇÃO DOS DADOS

É o órgão responsável pela fiscalização e regulamentação que ensejam a LGPD.

Principais funcionalidades:

- Zelar pela proteção dos dados pessoais;
- Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação;
- Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
- Editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco;
- Realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização ;

AUTORIDADE NACIONAL DE PROTEÇÃO DOS DADOS

- Editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;

- Garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento;

- Comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

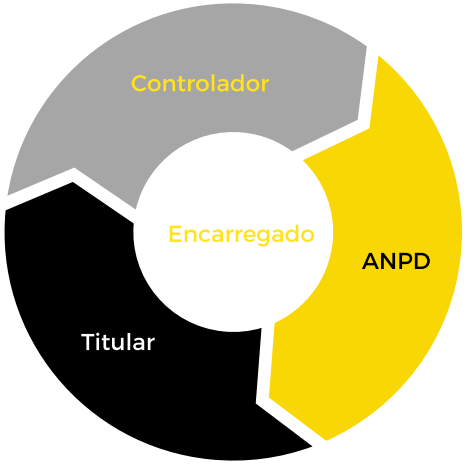
- Implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.

ENCARREGADO

ENCARREGADO

Conhecido na Europa como DPO (data protection officer)

Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).



A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

ATIVIDADES DO ENCARREGADO

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

RELATÓRIO DE IMPACTO

RELATÓRIO DE IMPACTO

É a documentação do controlador que contém a **descrição dos processos de tratamento de dados pessoais** que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

A autoridade nacional poderá **solicitar ao controlador relatório de impacto à proteção de dados pessoais**, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

O QUE DEVERÁ CONTER NO RELATÓRIO?

1. **A descrição dos tipos de dados coletados;**
2. **A metodologia utilizada para a coleta e para a garantia da segurança das informações;**
3. **A análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.**

SANÇÕES

SANÇÕES

- Advertência;
- Multa de até 2% do faturamento do grupo, limitada, no total, a R$50.000.000,00 (cinquenta milhões de reais) por infração;
- Multa diária;
- Publicização da infração após apuração e confirmação da sua ocorrência;
- Bloqueio dos dados pessoais;
- Eliminação dos dados pessoais;
- Suspensão parcial do funcionamento do banco de dados;
- Proibição parcial ou total do exercício de atividades relacionado ao tratamento de dados.

CHECKLIST DA LGPD

CHECKLIST DA LGPD

A empresa tem mapeado os dados pessoais utilizados?	☐ Sim ☐ Não
Possui documentação de onde e como os dados pessoais estão armazenados e utilizados?	☐ Sim ☐ Não
Existe compartilhamento de dados pessoais com terceiros?	☐ Sim ☐ Não
Foi realizado avaliação dos dados pessoais estritamente necessários ao processo de tratamento?	☐ Sim ☐ Não
Se existir transferência internacional de dados, é realizada para países com regulamentação compatível?	☐ Sim ☐ Não
Os contratos já foram revisados para estarem de acordo com a LGPD?	☐ Sim ☐ Não
Na coleta de dados pessoais, é realizado o consentimento?	☐ Sim ☐ Não
Existe procedimento para revogar o consentimento?	☐ Sim ☐ Não
Os usuários têm conhecimento dos dados compartilhados com outras instituições?	☐ Sim ☐ Não

CHECKLIST DA LGPD

Existe procedimento que determine por quanto tempo os dados serão armazenados?	☐ Sim ☐ Não
Existe canal facilitado para consulta dos dados pelo titular?	☐ Sim ☐ Não
Existem procedimentos para garantir o sigilo dos dados?	☐ Sim ☐ Não
Existem controle de acesso quanto ao possível uso dos dados pessoais por terceiros não autorizados?	☐ Sim ☐ Não
Possui verificação de log de quem acessou e/ou alterou dados pessoais?	☐ Sim ☐ Não
A política de privacidade está de acordo com a LGPD?	☐ Sim ☐ Não
Foi indicado um Encarregado de proteção de dados?	☐ Sim ☐ Não
Existe relatório de impacto à proteção de dados pessoais?	☐ Sim ☐ Não
Existe procedimento de informação aos titulares caso haja vazamento dos dados?	☐ Sim ☐ Não

Avaliação de Conformidade com a LGPD

Resultado da sua empresa	Análise de Conformidade
Você marcou positivamente(SIM) de 0 a 6 vezes? 	Sua empresa precisa se preparar para a LGPD, há muito para se fazer, é necessário a conscientização de direção e colaboradores. Aspectos como gestão de dados, documentação legal e segurança da informação devem ser iniciados urgentemente.
Você marcou positivamente(SIM) de 7 a 12 vezes? 	Há um ponto positivo, um passo foi dado pela sua empresa. Deve ser avaliado quais os pontos fracos e reunir a equipe para priorizar as medidas que serão tomadas. O planejamento estratégico facilitará a continuação do processo de implantação.
Marcou positivamente(SIM) de 13 a 18 vezes. 	Parabéns! Caminhos foram construídos para que possam estar em conformidade com a LGPD. É importante realizar validações do processo, portanto, aproveite o período que ainda falta para conduzir os processos de validação.

O QUE MINHA EMPRESA DEVE FAZER?

COMO IMPLANTAR A LGPD?

1

Reunir a Equipe

Apresentar a importância da LGPD e eleger um responsável para o processo de implantação.

2

Coletar Informações

Realizar mapeamento de dados, documentação legal (contratos, política de segurança) e segurança da informação.

3

Gap Analysis

Identificar, Analisar e Avaliar riscos.

4

Plano de Ação

Elaborar o Plano de Implantação, definindo etapas e processos para a execução.

5

Governança de Tratamento de Dados

Adequar o tratamento de dados conforme a LGPD.

6

Gestão de Documentação Legal

Adaptar contratos e termos.

7

Governança de Segurança de Dados

Realizar medidas de segurança, alinhando as boas práticas de segurança, alinhando a implantação de ferramentas de prevenção de perda de dados.

8

Treinamento

Capacitar todos os colaboradores quanto as boas práticas de proteção e privacidade de dados.

9

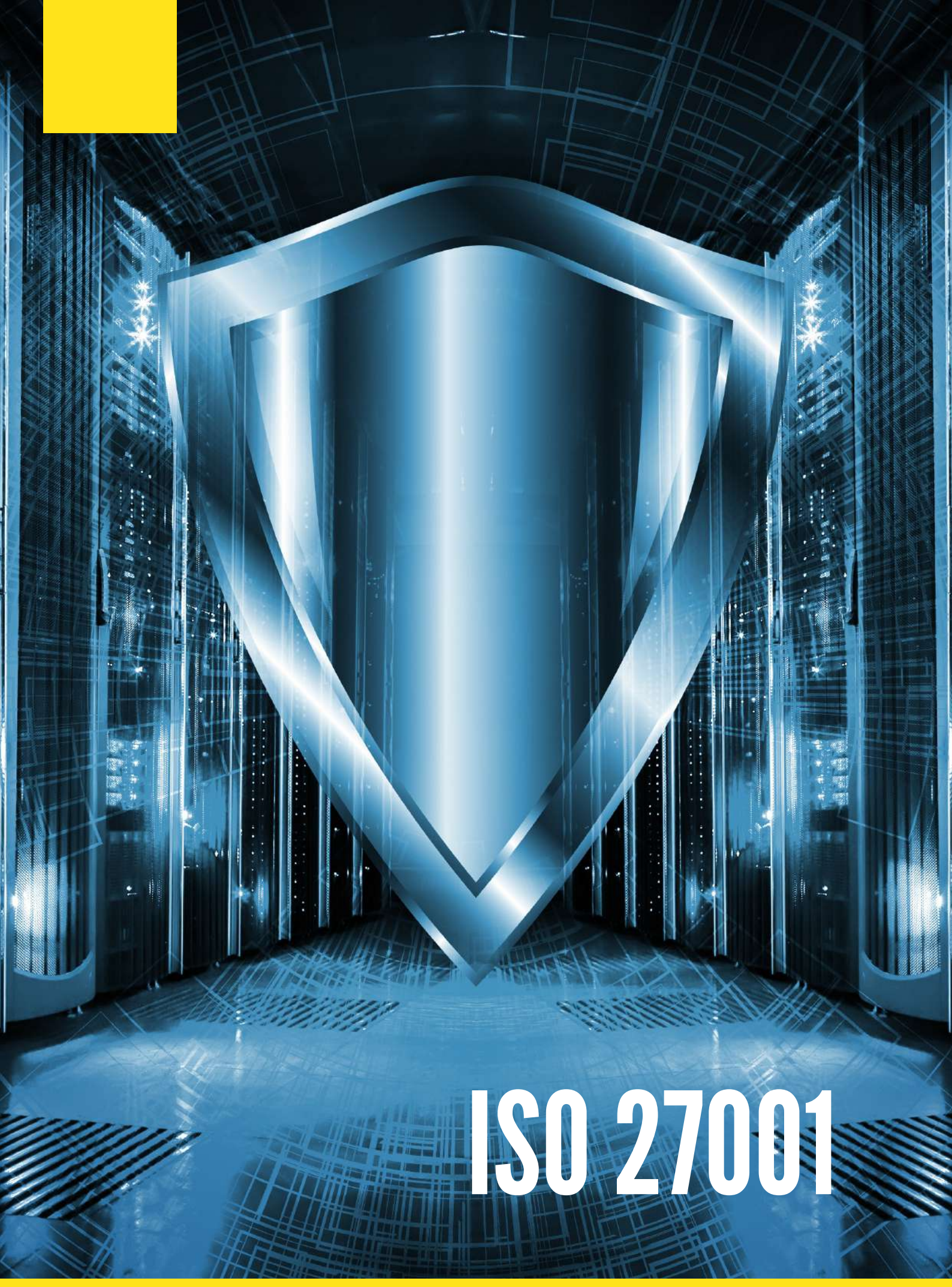
Definição do DPO

Definir o responsável para acompanhamento e monitoramento das atividades de privacidade de dados.

10

Relatório de Impacto

Elaborar relatório das análises e ações realizadas na implantação da LGPD.



ISO 27001

CYBER SEGURANÇA

É o conjunto de procedimentos, ações e técnicas, que visam garantir a confidencialidade, disponilidade e integridade dos ativos de uma organização.

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados

Disponibilidade: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada;

Integridade: propriedade de salvaguarda da exatidão e completeza de ativos.

Ativo: qualquer coisa que tenha valor para a organização

SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO (SGSI)

É a parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar de forma crítica, manter e melhorar a segurança da informação.

A ISO 27001 é a norma que provém um SGSI, inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos.

MODELO PDCA APLICADO AOS PROCESSOS DO SGSI

Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.

Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Implementar e operar a política, controles, processos e procedimentos do SGSI.

Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.

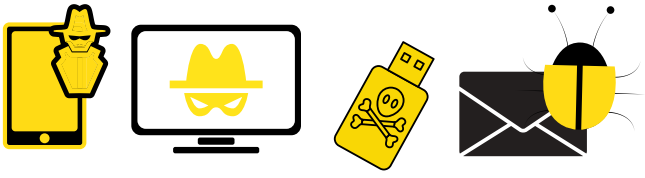
A organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto das atividades de negócio globais da organização e os riscos que ela enfrenta.

Esse processo deve ser continuo, visto que os riscos podem acontecer a qualquer momento, no entanto, vale ressaltar que as vulnerabilidades estão em constante evolução, novos tipos de ameaças são lançadas diariamente e os procedimentos de segurança, necessitam estarem prontos para ter respostas a incidentes.

Gestão de Riscos

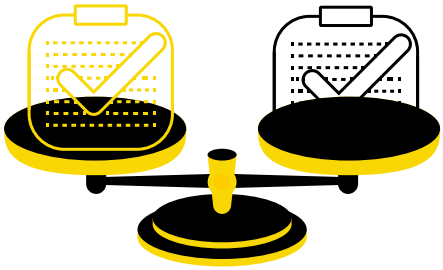
São atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos.

Identificar os riscos
Identificar os impactos que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos.



Análise de Riscos
Uso sistemático de informações para identificar fontes e estimar o risco.

Avaliação de Riscos
Processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.



Tratamento do Risco
Processo de seleção e implementação de medidas para modificar um risco.

PROCEDIMENTOS DE SEGURANÇA - ISO 27001

Ao se falar em segurança da informação, a primeira preocupação que se tem, por parte das organizações, diz respeito aos custeio das aplicações que serão adotadas, no entanto, ao longo dos anos, foram deixados de lado por questão de prioridades.
Investir em serviços ou produtos que gere um aumento no lucro das empresas tornou-se elo primordial, e, além disso, as medidas de segurança podem minimizar fraudes e riscos. Em muitos casos as empresas só descobrem as fraudes após um longo período de ocorrência ou por uma denúncia. Colaboradores realizam desvios através dos Sistema de Informações, excluindo vendas realizadas e embolsando o dinheiro, dando baixa em produtos danificados ou defeituosos.

Os procedimentos de segurança poderiam minimizar alguns riscos e fraudes, sem que a necessidade de se fazer investimentos caros.
DENTRE as rotinas a serem estabelecidas nas organizações, a capacitação de colaboradores deve ser seu maior investimento, pois a execução ocorre por intermédio desses colaboradores.
O investimento deve ser levado em consideração ao tamanho da organização, muitas medidas podem ser feitas a baixo custo, sendo fundamental uma análise dos riscos, planejamento e monitoramento das ações de medidas de segurança.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

São diretrizes ou regras para a segurança da informação, observando os requisitos de negócios, as regulamentações vigentes e em conformidade com a lei.
Deve conter as normas que visam a Proteção de Dados e Privacidade da Informação Pessoal.
Na implantação da Política de Segurança da informação é importante garantir que todos os colaboradores estejam cientes do processo, assim, se faz necessário documentar esta etapa, através da assinatura de termo de aceite.

Proteção de Dados e Privacidade da Informação Pessoal

Deve assegurar que a proteção de dados esteja de acordo com a LGPD, para tanto, devemos observar o cumprimento de medidas regulatórias, contratos, termos de consentimento e política de privacidade.

POLÍTICA DE CONTROLE DE ACESSO

É um dos pontos principais da segurança, pois contém o que cada colaborador deve ter acesso aos sistemas de informação. Deve ser documentada e avaliada de acordo os requisitos de negócio, levado em consideração a segurança da informação.

Identificação e autenticação de usuário

Cada usuário deve possuir um identificador único (ID de usuário), para uso pessoal e intransferível, e um meio de autenticação, geralmente é utilizado a senha, que validade o usuário ao acessar um Sistema.

Gerenciamento de Senha do Usuário

O procedimento de concessão de senhas deve ser gerenciado e formalizado, contendo o período de liberação e a finalização desse acesso, que deve ocorrer imediatamente ao término de contrato do colaborador.

Restrição de acesso à informação

As permissões de acesso à informação deve ser de acordo com a função dentro da organização, sendo descrito na política de acesso.

Uso de senhas

As boas práticas de segurança devem ser aplicadas ao uso de senhas. Os usuários devem utilizar senhas mais longas, utilizando caracteres, letras e números, evitando colocar datas comemorativas.

Todos os colaboradores devem ter um ID de usuário e uma senhas, para realizar a acesso a computadores, e aos Sistemas de Informação, não sendo permitido o uso por outro colaborador.

Esse processo facilita a análise de fraudes, mas é necessário estabelecer um cultura de que o uso de senhas é exclusiva.

Em muitas empresas diversas fraudes são realizadas por colaboradores que fazem o uso de senhas de outros colaboradores, que conseguem de maneira fácil e inocentemente.

CONTROLES DE AUDITORIA DE SISTEMAS DE INFORMAÇÃO

Na realização de atividades de auditoria é importante que a organização esteja com os processos definidos: uso de ID de usuário e senha. Tanto para os Sistemas Operacionais, quanto para os Sistemas de Informação, Política de Segurança e Privacidade. No entanto, há necessidade de planejamento para evitar a interrupção das atividades do negócio.

Coleta de Evidências

Na ocorrência de incidentes de segurança, em que envolva ação civil ou criminal, as evidências devem estar em conformidade com a legislação vigente, sendo observadas os formas de coleta, armazenamento e análise.
Muitas empresas não seguem essas normas nas ocorrências de incidentes e provas coletadas, o que gera a nulidade de provas nos processos judiciais.

Registros (log) de Auditoria

Os arquivos Logs registram informações sobre as operações realizadas dentro de sistemas de informações, atividades de usuários, horário de login/logoff, transações, entre outras informações.
Esses registros podem ser utilizados para futuras investigações, pois determinam muito sobre atividades realizadas nos Sistemas de Informação(SI).
As empresas devem exigir que os seus SI possuam registros logs, pois esta funcionalidade poderá identificar possíveis fraudes, bem como, a identificação dos responsáveis, evitando , assim, perdas financeiras.

BACKUP

O Backup é a cópia de segurança dos dados, geralmente armazenado em discos externos ou em nuvem. Muitas organizações fazem mais de uma cópia, onde a primeira fica na empresa e a segunda unidade, é guardada em um ambiente externo.

A política de backup deve ser planejada, com horário, responsável e rotinas de verificação. Os testes de backup devem ser realizados, pois na na ocorrência de falhas, os dados não se encontram intactos. Vale a pena ressaltar que os backups tem sido a única saída para casos de Ransomwares, sequestro de dados, ocorrentes em empresas de todo o mundo.

Na conformidade com a LGPD e para maior proteção dos dados pessoais se faz necessário a criptografia dessa cópia de segurança, evitando excesso de backups.

AUTOR

Raimundo Pereira da Cunha Neto, atua na área de Tecnologia da Informação há 20 anos, onde iniciou a carreira como Consultor de Informática pelo Ministério da Saúde (1999 – 2008), onde era responsável pela base de dados, no Piauí, de pacientes com HIV/DST/AIDS.

- Formado em Ciência da Computação (UESPI - 2003);
- Especialista em Redes de Computadores (FSA - 2011);
- Mestre em Segurança de Redes de Computadores (UFMA - 2011);
- Doutorando em Engenharia Biomédica (UNIVAP)

- Coautor do Livro de Informática Forense (2018);
- Diretor do Núcleo de Tecnologia da Informação da FAETE (2002 – 2009);
- Membro da Comissão de Direito Digital da OAB-PI (2017 -2018);
- Diretor de Pesquisa e Tecnologia da APECOF(2017 - 2019);
- Perito AdHoc em Computação Forense(Desde 2017);
- Professor Universitário de Graduação e Pós Graduação (Desde 2005);
- Coordenador de Curso de Graduação em Análise e Desenvolvimento de Sistemas (2012 a 2016);
- Coordenador de Pós Graduação em Engenharia de Software(2014 – 2018) e Segurança de Redes de Computadores (2015 - 2018);
- Campeão do Sebrae Like a Doctor 2019.
- Palestrante sobre as áreas de Segurança da Informação e Lei de Proteção de Dados.
- CEO da The Forense (Desde 2017).

THE FORENSE

A The Forense é uma empresa especializada em segurança digital, com profissionais qualificados com mais de 20 anos de experiência no mercado de Tecnologia da Informação, com ênfase em Segurança da Informação.
Nossa empresa atua nas área de Perícia Digital, Lei Geral de Proteção de Dados Pessoais, Compliance Digital, Treinamento, Assistência Técnica Judicial, Monitoramento de Dispositivos, Auditoria de Sistemas de Informação, Exames de Crimes Eleitorais na Internet e Reconhecimento Facial.

Os inúmeros desafios da LGPD podem gerar um transtorno para sua empresa, portanto, conte com quem tem experiência nas áreas Jurídica, Segurança da Informação e Administrativa. Utilizamos metodologias que visam realizar estratégias em todos os segmentos da sua empresa para a proteger os dados pessoais, bem como minimizar riscos de fraudes e alinhar mecanismos de auditoria.
Faça já nosso curso de LGPD do Planejamento à Prática: https://hotm.art/F7bbLCav
Consulte nosso site serviços e cursos.

INFORMAÇÕES

contato@theforense.com.br
www.theforense.com.br

TELEFONE

(86) 3305-4008 / 9.9953-5754