LGPD E ISO 27001

Como a norma ajuda na adequação à legislação

ECOTRUST

A falta de privacidade e a preocupação com a segurança de dados são assuntos muito discutidos nos últimos tempos, sobretudo nos ambientes corporativos.

O Brasil é o 3° país no ranking de crimes cibernéticos e, após diversos e sucessivos escândalos de manipulação de dados e vazamentos dos quais tornaram-se rapidamente públicos, atingindo milhares de usuários, algumas medidas foram necessárias.

1890
Direito à Privacidade

1948
Declaração dos Direitos Humanos

2010
Iniciativa Brasileira

2011
Lei de Acesso à Informação

2012
Lei Carolina Dieckmann

2014
Marco Civil da Internet

2018
Lei Geral de Proteção de Dados

Para contornar essa situação caótica, foi criada e aprovada a sanção da **Lei Geral de Proteção de Dados (Lei 13.853/2019)** — uma proposta similar aos modelos que já estavam presentes em mais de 120 países.

Após essas mudanças, resta a cada empresa entender e se adequar da melhor forma possível em relação ao armazenamento e ao tratamento de dados.

Neste e-book, vamos falar detalhadamente sobre todos os aspectos da Lei 13.853/2019 e suas implicações. Boa leitura!

Sumário

06 **Sobre a LGPD**

A quem se aplica a LGPD?

Principais atores no tratamento de dados pessoais

Os princípios da LGPD

11 **Sobre a ISO**

13 **Impacto da LGPD para as organizações**

Sobre o controle de dados pelos titulares

Sobre o princípio da finalidade

O que é considerado tratamento de dados segundo a LGPD?

O que são dados pessoais segundo a LGPD?

Quem fiscaliza o cumprimento das regras da LGPD?

Quais são as consequências para as empresas que não se adequam às regras da LGPD?

20 **Em que condições uma empresa está autorizada a tratar dados?**

Coleta e tratamento de dados segundo a LGPD

Sobre os dados sensíveis

25 **Lei Geral de Proteção de Dados e a Norma ABNT ISO/IEC 27001**

29 **Sobre a EcoTrust**

1

Sobre a LGPD

A Lei Geral de Proteção de Dados (LGPD) é uma legislação que entrou em vigor em **setembro de 2020** no Brasil para estabelecer normas relacionadas ao tratamento de dados de pessoas físicas nas suas mais variadas aplicações e ambientes.

Seguindo as bases do regulamento geral de proteção de dados europeu (GDPR), a LGPD tem mudado a forma de funcionamento e operação das organizações, pois estabelece **regras de coleta, armazenamento, tratamento e compartilhamento de dados pessoais**, tornando a proteção de dados ainda mais relevante.

A quem se aplica a LGPD?

A Lei é válida para qualquer pessoa natural ou jurídica, de direito público ou privado, que realize o tratamento de dados pessoais, online e/ou offline, no Brasil, independentemente de qual seja o país sede em que os dados estejam localizados.

Isso significa que **não importa o porte ou o segmento do seu negócio**. Se você lida com dados pessoais em seus processos organizacionais, você precisa se preocupar com o cumprimento das regras da LGPD.

Principais atores no tratamento de dados pessoais

Do ponto de vista da LGPD, há cinco atores mais importantes no tratamento de dados pessoais:

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 ou DPO

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 de Proteção de Dados

Órgão da administração pública federal cujas responsabilidades são a de zelar pela proteção de dados pessoais e a de fiscalizar o cumprimento da LGPD

Os princípios da LGPD

A Lei Geral de Proteção de Dados elenca, em seu artigo 6º, dez princípios que as organizações devem seguir quanto ao tratamento de dados. É a partir desses princípios que a sua empresa pode planejar ações e traçar metas para garantir a conformidade e a adequação à Lei. Veja quais são eles:

Finalidade: o tratamento dos dados deve ter propósito legítimo, específico, explícito e informado ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades

Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento

Necessidade: limitação do tratamento mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados

Livre Acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais

Qualidade dos dados: garantia da exatidão, clareza, relevância e atualização dos dados ao titular, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento

Transparência: garantia aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial

Segurança: medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão

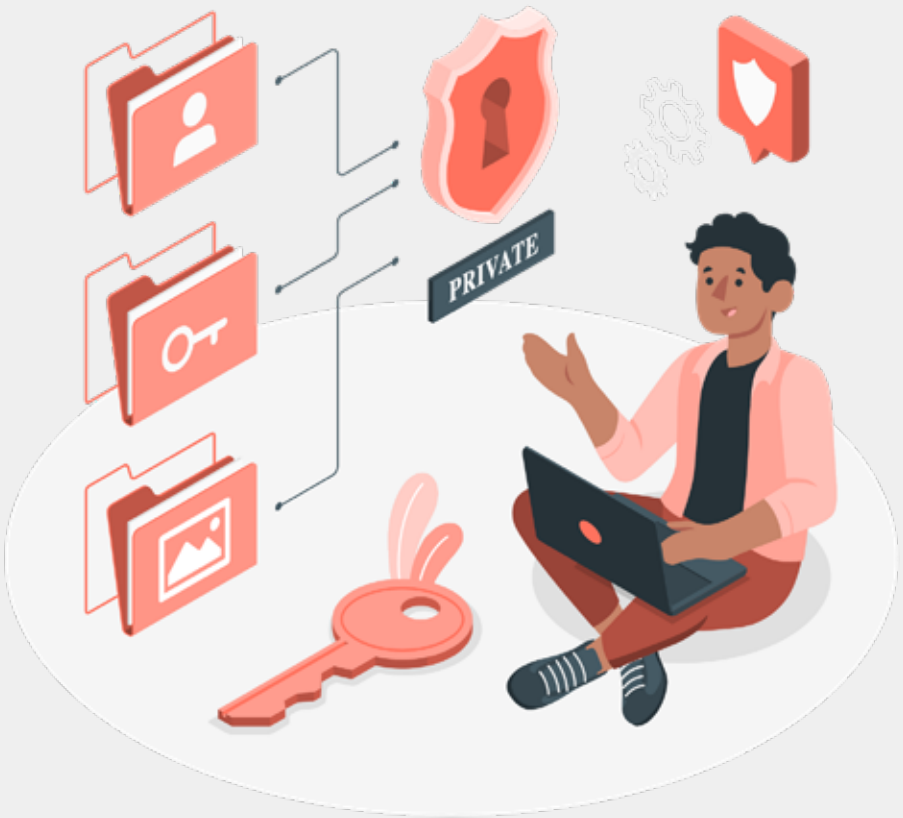
Prevenção: adoção de medidas para prevenção de incidentes de danos para tratamento de dados pessoais

Não discriminação: Impossibilidade do tratamento dos dados para fins discriminatórios, ilícitos ou abusivos

Responsabilização e prestação de contas: adoção de medidas e controles eficazes ao cumprimento das normas de proteção de dados pessoais.

2

Sobre a ISO 27001



A ISO 27001 é uma norma internacional e foi publicada em 2005 pela *International Electrotechnical Commission* (ICE) e pelo *International Organization for Standardization* (ISO).

Sua missão é o **fornecimento de diretrizes para que os gestores consigam implementar políticas de segurança da informação eficientes**.

Ou seja, ela enumera uma série de padrões nos quais as empresas podem basear as suas políticas, estabelecendo regras objetivas e claras.

Quando essa implementação é feita de maneira adequada, a empresa ganha o **certificado ISO 27001**, que confirma a sua responsabilidade e preocupação no que diz respeito à segurança da informação.

3

Impacto da LGPD para as organizações

Você já deve ter se perguntado quais são os modelos de negócios que devem estar de acordo com a LGPD. A resposta é simples: organizações de todos os setores e tamanhos tratam dados pessoais, por isso, **a Lei é válida para todas elas**.

Sobre o **controle de dados** pelos titulares

Em linhas gerais, o principal efeito da LGPD está relacionado ao **maior controle pelos titulares das informações sobre todo o processamento dos seus dados pessoais** — do que decorrem diversas obrigações para controladores (a quem competem as decisões sobre o tratamento dos dados) e operadores (aqueles que tratam os dados de acordo com o estipulado pelos controladores).

Com as mudanças estabelecidas, os titulares de dados pessoais passam a ter os seguintes direitos:

- **Confirmação da existência de tratamento de dados**
- **Acesso aos dados**
- **Correção de informações incompletas ou desatualizadas**
- **Direito à anonimização, bloqueio e eliminação dos dados desnecessários**
- **Portabilidade dos dados a outro fornecedor de serviço ou produto**
- **Conhecimento sobre possíveis compartilhamentos**
- **Direito a esclarecimentos sobre as consequências de não fornecer dados**
- **Direito a revogar o consentimento das informações**

Sobre o **princípio da finalidade**

Está lembrado dos princípios que falamos no tópico anterior? Um dos mais relevantes é o da **finalidade**, por meio do qual os dados deverão ser utilizados apenas para as finalidades específicas para as quais foram coletados e essas finalidades precisam ser devidamente informadas aos titulares.

Somado a isso, também ressaltamos o princípio da **necessidade de coleta**, que significa que somente devem ser coletados os dados mínimos necessários para que se possa atingir a finalidade. Há também a **retenção mínima** que determina a imediata exclusão dos dados após atingida a finalidade pela qual as informações foram coletadas.

Como pode-se observar, na LGPD, um princípio é ligado ao outro de modo que o objetivo principal de **garantir a proteção dos dados dos cidadãos** seja cumprido em sua totalidade.

Assim, a melhor maneira de ter a certeza de que sua empresa está cumprindo as regras da Lei é verificar se cada um dos dez princípios está sendo observado e promover ações que aprimorem essa observação.

O que é considerado **tratamento de dados** segundo a LGPD?

Conforme a Lei Geral de Proteção de Dados, o tratamento é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

O que são **dados pessoais** segundo a LGPD?

Segundo a Lei, o dado pessoal é uma **informação relacionada a pessoa natural identificada ou identificável**. Podem ser citados como exemplos a data de nascimento, os dados de GPS, a profissão, os dados de cadastros em geral, a nacionalidade, os gostos, interesses, entre tantos outros. Na prática, são dados que podem ser usados em diferentes áreas e atividades de uma empresa tais como o marketing, o atendimento ao cliente, os recursos humanos e as áreas de desenvolvimento.

Quem fiscaliza o **cumprimento das regras** da LGPD?

Para garantir que os princípios da Lei Geral de Proteção de Dados sejam seguidos, de maneira geral, as empresas devem contar em seu quadro de funcionários com a figura do **encarregado**, que será o **responsável pelo relacionamento com os titulares dos dados**, a comunicação com a ANPD, a adoção de providências em incidentes de privacidade e a disseminação das práticas relacionadas à proteção de dados pessoais.

Existem exceções a esta regra para o caso dos agentes de tratamento de pequeno porte, que não são obrigados a nomear o encarregado, mas precisam disponibilizar um canal de comunicação com os titulares dos dados.

Além disso, também foi criada a **Autoridade Nacional de Proteção de Dados (ANPD)**. Entre as competências desse órgão estão zelar pela proteção dos dados pessoais, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade e aplicar sanções em caso de tratamento de dados realizado de forma irregular.

Quais são as **consequências** para as empresas que não se adequam às regras da LGPD?

Para as empresas que não promoverem as mudanças necessárias para cumprir as regras da LGPD, a Lei prevê diversas formas de punições. Dentre as possibilidades previstas estão:

- **Advertências com indicação de prazos para adoção de medidas corretivas**
- **Multa simples de até 2% do faturamento da empresa no seu último exercício (excluindo os tributos) e limitada até o valor de R$ 50.000.000,00 por infração**
- **Multa diária (observando o limite anterior)**
- **Publicização da infração após devidamente apurada e confirmada a sua ocorrência**
- **Bloqueio dos dados pessoais a que se refere a infração até sua regularização**
- **Eliminação dos dados pessoais a que se refere a infração**

Vale lembrar que as sanções são aplicadas somente após procedimento administrativo que possibilite a oportunidade de defesa e considerando os seguintes parâmetros:

- **Gravidade e a natureza das infrações e dos direitos pessoais afetados**
- **Boa fé do infrator**
- **Vantagem auferida ou pretendida pelo infrator**
- **Condição econômica do infrator**
- **Reincidência**
- **Grau do dano**
- **Cooperação do infrator**
- **A adoção demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados**
- **Adoção de política de boas práticas e governança**
- **A pronta adoção de medidas corretivas e a proporcionalidade entre a gravidade da falta e a intensidade da sanção**

4

Em que condições uma empresa está autorizada a tratar dados?

Organizações, públicas e privadas, assim como a sua empresa, muitas vezes só podem coletar dados pessoais se tiverem consentimento do titular, segundo a LGPD.

Ainda assim, vincular o consentimento como autorização para tratamento de dados pessoais em alguns negócios pode ser prejudicial, visto que o titular de dados a qualquer momento pode solicitar a **revogação do consentimento**, fazendo com que a empresa tenha uma perda significativa de sua base. Além disso, é preciso um consentimento específico para o tratamento de dados sensíveis.

Os dados pessoais podem ser tratados nas seguintes hipóteses:

I. Mediante o fornecimento de consentimento pelo titular

II. Para o cumprimento de obrigação legal ou regulatória pelo controlador

III. Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da Lei

IV. Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais

V. Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados

VI. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, seguindo os termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)

VII. Para a proteção da vida ou da incolumidade física do titular ou de terceiro

VIII. Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)

IX. Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais

X. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

A solicitação deverá ser feita de maneira clara, informando aos seus consumidores exatamente **aquilo que será coletado, para quais fins e se haverá compartilhamento** dessas informações.

Caso os dados coletados possuam o envolvimento de menores de idade, as informações relacionadas a essa coleta só poderão ser liberadas por meio do consentimento dos pais ou responsáveis legais. Se houver mudança na finalidade ou, até mesmo, no repasse dos dados a terceiros, você e a sua equipe, em nome da sua empresa, deverão solicitar um novo consentimento aos seus clientes.

O usuário também poderá, sempre que desejar, **revogar a autorização existente**, assim como pedir também **acesso, exclusão, portabilidade, complementação ou correção dos dados**. E, se o uso das informações do seu consumidor levar a uma decisão automatizada indesejada, é direito dele pedir uma revisão humana do procedimento.

Coleta e tratamento de **dados** segundo a LGPD

Para realizar a coleta e tratamento de dados, as empresas são obrigadas a comprovar, ao menos, um dos seguintes motivos para o seu tratamento:

- **Consentimento pelo titular**
- **Cumprimento de obrigação legal ou regulatória**
- **Execução de políticas públicas pela administração pública**
- **Estudos por órgão de pesquisa**
- **Execução de documentos contratuais/Diligências Pré-contratuais**
- **Exercício Regulares de Direitos**
- **Proteção da vida ou bem-estar físico do titular**
- **Tutela da saúde**
- **Legítimo interesse do controlador, desde que este interesse não fira direitos fundamentais do titular**
- **Proteção do crédito**

Sobre os **dados sensíveis**

A LGPD trouxe consigo a categoria de dados chamada de "**dados sensíveis**" vinculados a uma pessoa natural.

Essa categoria diz respeito a informações como convicção religiosa, opinião política, origem racial ou étnica, dados referentes à saúde ou à vida sexual, filiação a sindicatos, dados genéticos ou biométricos.

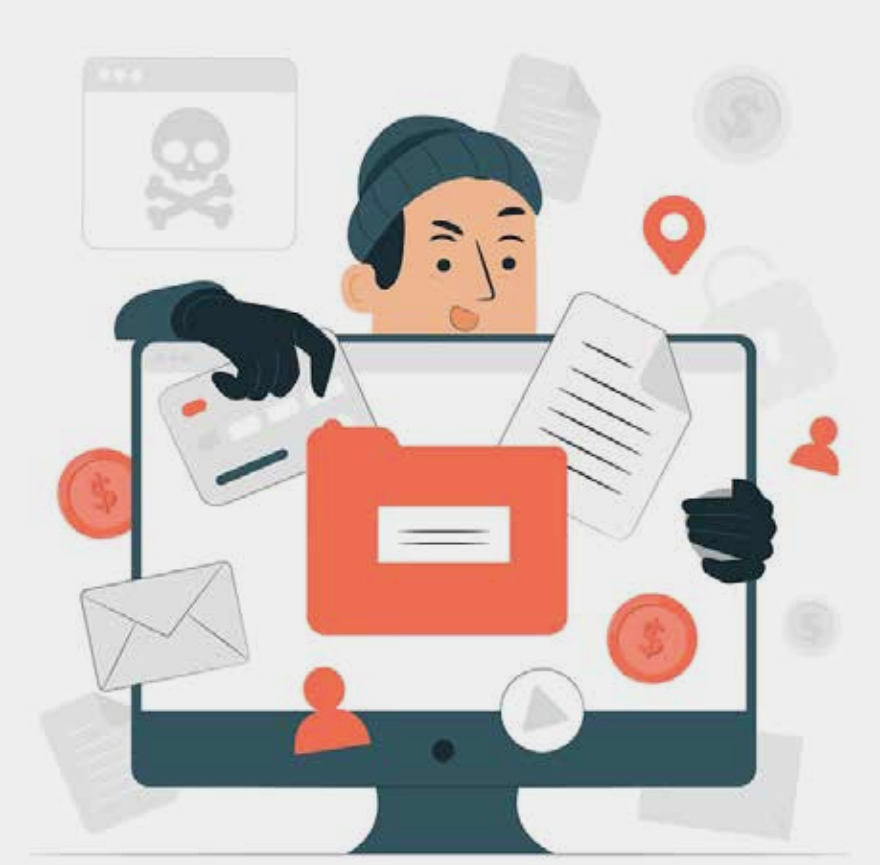
Por poderem ser **objetos de discriminação**, os dados sensíveis necessitam de uma proteção ainda maior. Por isso, eles só podem ser coletados e tratados nas seguintes condições:

- **Quando houver o consentimento, de forma específica e destacada, para finalidades específicas**
- **Para o cumprimento de obrigações legais**
- **Para a realização de estudos por órgãos de pesquisa**
- **Para a proteção da vida do titular ou terceiros**
- **Para o tratamento compartilhado pela administração pública que esteja previsto em Lei ou Regulamentos**
- **Para o exercício regular de direitos em contratos ou processos judiciais e administrativos**
- **Para proteção da vida do titular ou terceiros**
- **Para procedimentos realizados por profissionais ou entidades da área da saúde**
- **Para a garantia de prevenção à fraude e a segurança do titular em sistemas de cadastros eletrônicos**

5

Lei Geral de Proteção de Dados e a Norma ABNT ISO/IEC 27001

Com o aumento dos cibercrimes, os ataques maliciosos estão trazendo diversos prejuízos para todos os tipos de negócios com os vazamentos de dados. Em busca de controles mais eficazes, a preocupação com a utilização de boas práticas de segurança da informação tornou-se essencial para resolver esta questão. Para apoiar e cumprir os princípios da Lei Geral de Proteção de Dados Pessoais (Lei 13.853/2019), listamos aqui os **requisitos da Norma ABNT ISO/IEC 27001** — a qual traz controles atestados e utilizados em muitos países.

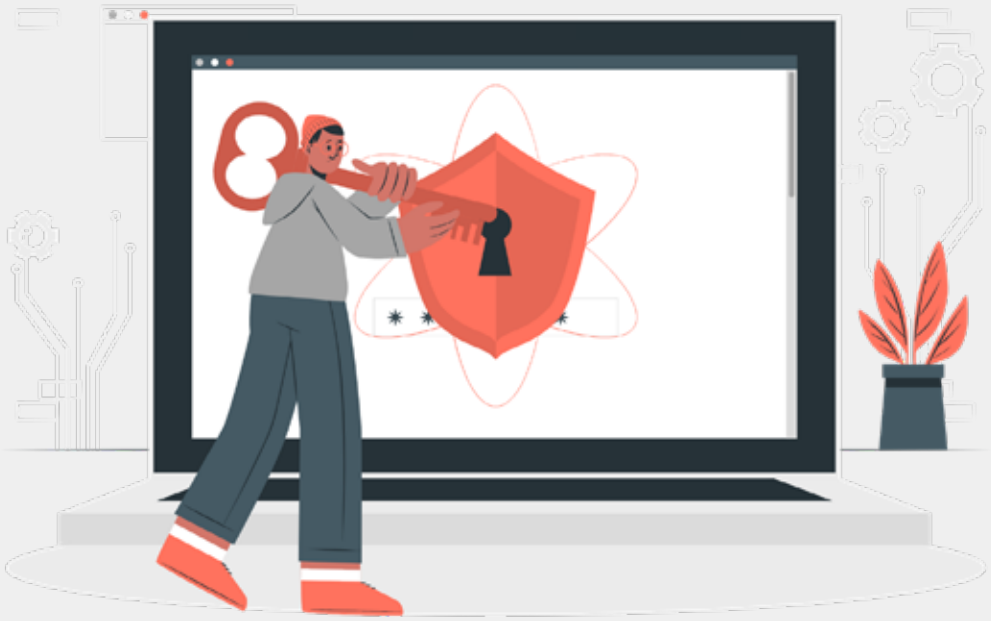


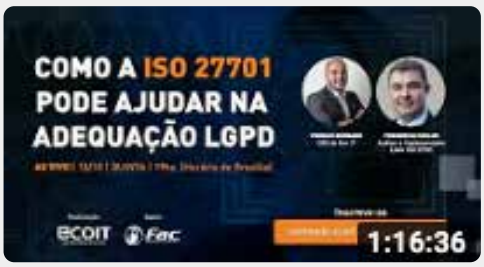
O artigo 46 da LGPD prevê que as empresas que trabalham com tratamento de dados devem adotar medidas de segurança, técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas. Veja o quadro a seguir:

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (13.853/2019)	ABNT NBR ISO/IEC 27001
Medidas de segurança, técnicas e administrativas	A.12.1. Responsabilidade e procedimentos operacionais.
Acessos não autorizados	A.9. Controle de Acesso; A.7.2.2. Conscientização, educação e treinamento de segurança da informação; A.8.2.1. Classificação da informação; A.11. Segurança física e do ambiente; A.12.3.1. Cópias de segurança das informações; A.14.2. Segurança em processos de desenvolvimento seguro.
Situações acidentais ou ilícitas de destruição	A.5.1.1. Políticas para segurança da informação; A.12. Gestão de vulnerabilidades técnicas; A.16. Gestão de incidentes de segurança da informação; A.17.1. Continuidade da segurança da informação.
Informação	6.1. Gestão de Riscos Segurança Informação.
Destruição, perda, alteração, comunicação	A.9. Controle de Acesso; A.12.3. Cópias de Segurança; A.17.1. Continuidade da segurança da informação.
O controlador deverá comunicar à autoridade nacional	16.1.2. Notificação de eventos de segurança da informação; 16.1.3. Notificando fragilidades de segurança da informação.

É possível notar que a norma, apesar de ser uma padronização de segurança internacional, auxilia os gestores a garantirem a adequação à Lei Geral de Proteção de Dados do Brasil.

Seguindo essas diretrizes, as organizações são capazes de adotar um Sistema de Gestão de Segurança da Informação adequado. Além disso, empresas que possuem a certificação como a ISO 27001 comprovam que seguem diretrizes eficazes quanto à segurança cibernética, o que auxilia, inclusive, na respeitabilidade da organização.

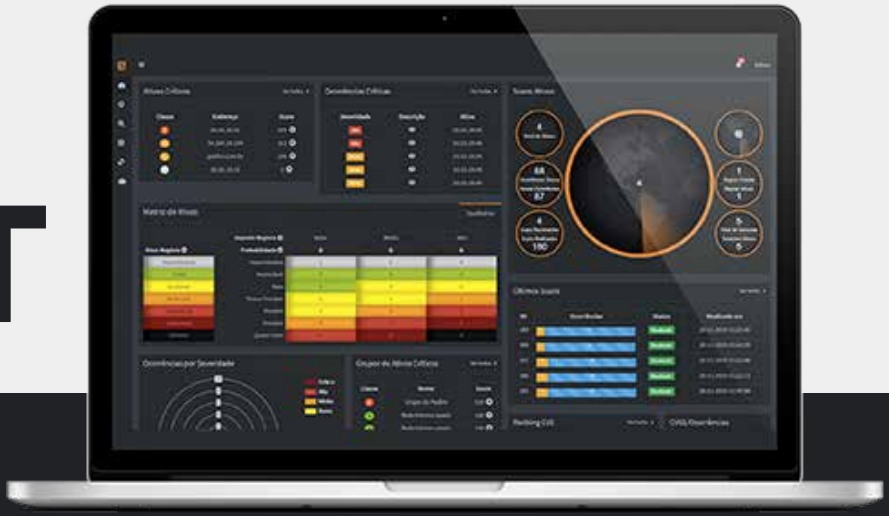




Como a ISO 27701 pode ajudar na Adequação LGPD

ASSISTA AQUI

ECO TRUST



Adotar métodos corretos e eficientes e aplicá-los com regularidade pode resultar na **economia de custos e aumento da competitividade** de negócios que dependem de tecnologia. As vantagens da segurança da informação e da proteção de dados para o presente e o futuro são diversas e podem evitar prejuízos muito severos.

É importante entender que processos relacionados a gestão de vulnerabilidades são os verdadeiros **investimentos em prevenção** e cuidados mais do que necessários. É hora de começar a agir de forma eficiente o mais rápido possível em favor da continuidade do negócio. Veja como a Eco IT pode te ajudar.

A **EcoTrust**, nossa **plataforma de *Inteligência em Riscos Cibernéticos***, possibilita que os líderes de Segurança e TI possam tomar decisões importantes de forma mais assertiva quando o assunto for segurança cibernética. Através da descoberta e gerenciamento de vulnerabilidades e riscos cibernéticos, de forma orquestrada, simplificada e com abordagem orientada aos riscos de negócio, a plataforma traz uma visão estratégica (negócio) com embasamento em indicadores técnicos (táticos e operacionais).

E para comprovar todas essas vantagens, você pode experimentar a plataforma gratuitamente. Basta clicar no botão abaixo.

Conhecer a solução

Entre em contato

Site:

www.ecotrust.io

ECOTRUST