

Treinamento de reciclagem

sobre a lei geral de proteção de dados - LGPD e
segurança da informação - SI



LGPD: Lei Geral de Proteção de Dados

Iniciamos o nosso treinamento de reciclagem sobre a LGPD e Segurança da Informação, lembrando os conceitos principais, sendo eles:

A Lei Geral de Proteção de Dados (LGPD), Lei 13.709/2018, entrou em vigor no ano de 2020 e trouxe regras para o uso de dados pessoais no Brasil, tanto no âmbito online quanto offline, nos setores privados e públicos.

A LGPD passou a valer em 2020, mas as penalidades começaram a valer somente em 2021. Desse modo, a lei se encontra 100% em vigor.

Um dos principais fundamentos da LGPD é assegurar o direito à privacidade e à proteção de dados pessoais dos cidadãos, por meio de práticas transparentes e seguras, garantindo direitos e liberdades fundamentais. As regras possuem o objetivo de organizar o tratamento dos dados pessoais pelas empresas para fortalecer a segurança jurídica destes.

SI: Segurança da Informação

A Segurança da Informação é um campo dentro da tecnologia da informação que busca defender ambientes virtuais e bancos de dados de ameaças. Ou seja, são mecanismos e ferramentas de proteção contra invasões que possam colocar em risco informações que estão no meio digital.

Trata-se de um esforço pautado por ações que objetivam mitigar riscos e garantir a continuidade das operações.

Falar sobre Segurança da Informação, é um conceito bastante abrangente, mas que podemos entender de forma mais clara **dividindo em duas partes:**

- **Informação:** conteúdo de valor para uma empresa ou profissional
- **Segurança:** a percepção de proteção contra perigos, ameaças e incertezas.

O objetivo da segurança da informação, portanto, é **garantir à empresa segurança** nos processos.

O grupo **Credfranco** deve se submeter a **LGPD**?

A RESPOSTA É **SIM**

Todas as pessoas físicas ou jurídicas, de direito público ou privado, que tratem dados pessoais no Brasil ou que colem dados no Brasil ou, ainda, quando o tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços a titulares localizados no Brasil, independentemente do meio, do país de sua sede ou país onde estejam localizados os dados, **DEVEM SE ADEQUAR À LGPD**.

Portanto, o grupo **Credfranco** se encontra em conformidade com o processo de adequação à **LGPD** e desenvolve mecanismos de segurança para proteção de dados pessoais.



Atualmente, as instituições financeiras e suas subsidiárias estão no radar da **Autoridade Nacional de Proteção de Dados – LGPD** em virtude do grande número de dados pessoais tratados.

Dado sensível e dado pessoal

Você já sabe, mas não custa lembrar.... qual a diferença de dado pessoal para dado sensível?

Dado pessoal:

Qualquer informação relacionada a uma pessoa natural (física) que possa ser identificada a partir dos dados coletados. É um conceito central da LGPD, que busca proteger a privacidade dos titulares de dados pessoais que sejam objeto de tratamento.

Dado sensível:

Os dados pessoais sensíveis são relativos à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, saúde, vida sexual, dado genético ou biométrico.

Só poderão ser submetidos a tratamento mediante consentimento específico e destacado do titular para finalidades específicas ou para cumprimento de obrigação legal ou regulatória pelo controlador ou garantia de proteção à fraude e à segurança do titular



você sabia?

A voz, vídeos e imagens que identificam a pessoa **são considerados dados sensíveis** e necessitam de **um cuidado maior** de acordo com a Lei Geral de Proteção de Dados - LGPD?

Como você pode realizar o **tratamento de dados de forma segura?**

Colete sempre o consentimento do titular antes de utilizar o dado sensível e informe de forma objetiva e simples sobre a LGPD, seja por meio de termo de consentimento, como também nas ligações.

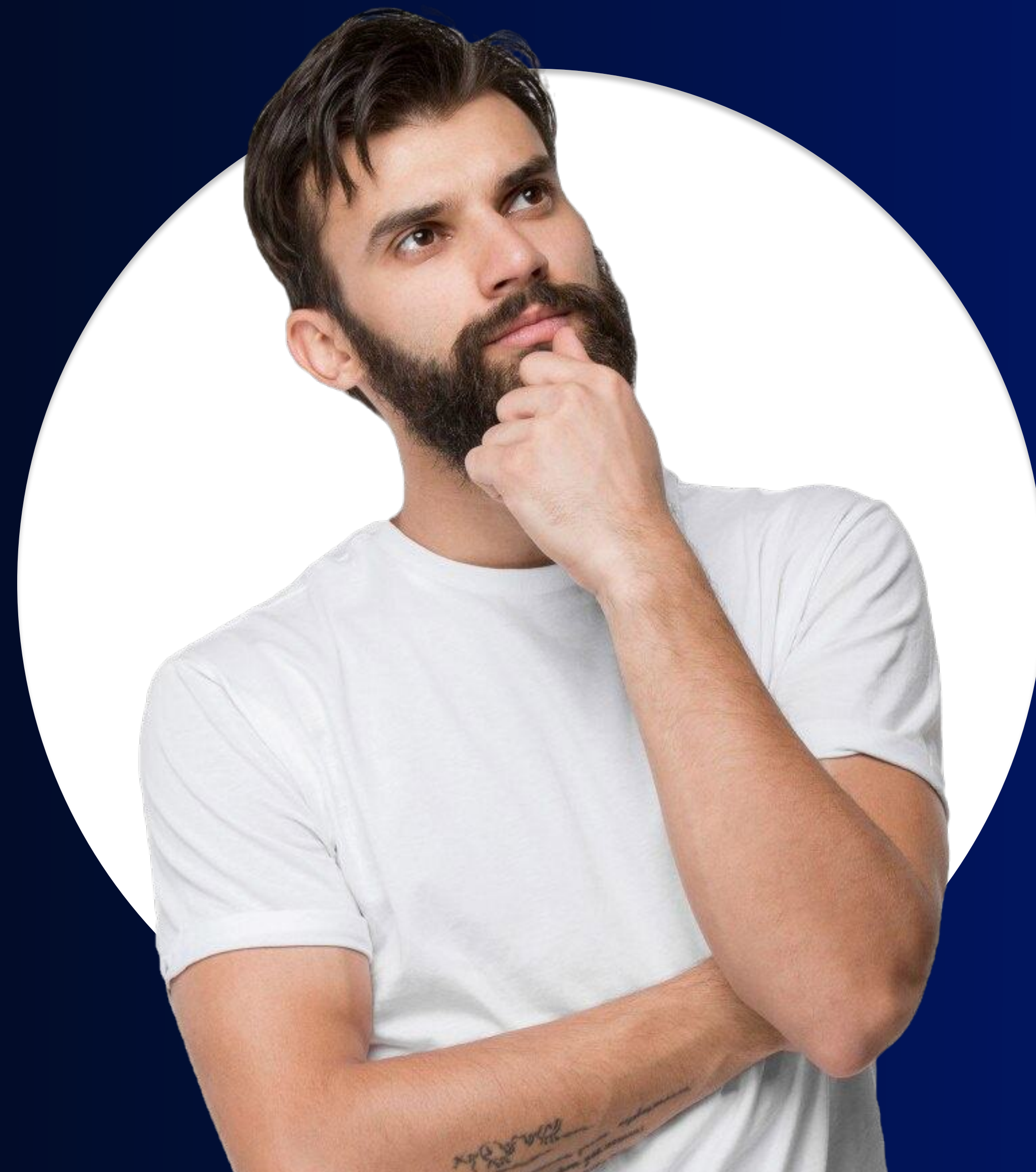
Somos controladores ou operadores em relação as instituições financeiras?

Controlador: Pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais.

Operador: Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.



O Grupo **Credfranco** é considerado **OPERADOR** de dados pessoais em relação às Instituições Financeiras, sendo eles, controladores.



Por sermos **operadores** não temos **responsabilidades junto à lei?**

A RESPOSTA É NÃO

A responsabilidade na LGPD é solidária, isso significa que todos os agentes (operadores e controladores) respondem de acordo com sua culpa.

Portanto, todos devem seguir os parâmetros legais cientes das suas responsabilidades.



E quem de fato **fiscaliza a LGPD no Brasil?**

para regular e fiscalizar a aplicação da lei, foi criada a autoridade nacional de proteção de dados (ANPD)

As responsabilidades da ANPD são:

- Zelar pela proteção dos dados pessoais;
- Elaborar as diretrizes para a política nacional de proteção de dados pessoais e da privacidade;
- Fiscalizar e aplicar as sanções previstas na LGPD;
- Editar regulamentos e procedimentos sobre a proteção de dados pessoais.
- Estimular o conhecimento sobre proteção de dados pessoais na população;

- Cooperar com outras autoridades de proteção de dados (internacionais);
- Implementar mecanismos para o registro de reclamações sobre tratamento em desconformidade com a lei;
- Apreciar petições do titular contra controlador após comprovação de não solução no prazo determinado;
- Realizar auditorias ou determinar sua realização para as atividades fiscalizatórias;
- Estimular a adoção de padrões para serviços e produtos que facilitem o controle dos titulares.

Já aconteceu alguma multa de LGPD no Brasil?

A RESPOSTA É SIM



A ANPD aplicou em **07/07/2024** a **primeira multa administrativa** por descumprimento à LGPD.

Quais são as penalidades previstas na LGPD?

- Advertência
- Multa simples
- Multa diária - multa de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos e limitada, no total, a **R\$50 milhões por infração**.
- Publicização
- Bloqueio dos dados
- Suspensão parcial do banco de dados
- Eliminação dos dados
- Suspensão do exercício da atividade de tratamento
- Proibição total ou parcial do exercício da atividade de tratamento



Qual o papel do **Grupo Credfranco** em relação à **LGPD**?



- Agir em conformidade com a LGPD respeitando o tratamento dos dados pessoais
- Promover os treinamentos de conscientização sobre a LGPD
- Cumprir todas as fases do processo de adequação
- Elaborar todas as documentações obrigatórias

Qual o papel dos **colaboradores e parceiros** do **Grupo Credfranco**?



- Realizar todos os treinamentos obrigatórios sobre a LGPD
- Agir em conformidade com as diretrizes e políticas estabelecidas pelo Grupo Credfranco
- Propagar a cultura da proteção de dados para todos

Pilares da segurança da informação

Os Pilares da segurança da informação dão o norte de como proteger a empresa, sendo eles:

01

Integridade

O pilar Integridade é responsável por manter as características originais dos dados, tal como foram configuradas na sua criação. Desta forma, as informações não podem ser alteradas sem autorização.

Se houver alteração indevida nos dados, significa que houve perda de integridade, sendo necessário implementar mecanismos de controle para evitar alteração não autorizada de informações.

02

Confidencialidade

Este pilar protege as informações de acessos não autorizados, estabelecendo privacidade para os dados da sua empresa, evitando situações de ciberataques ou espionagem.

A base desse pilar é o controle do acesso por meio de autenticação de senha, que também pode ocorrer por meio de varredura biométrica e criptografia, o que vem gerando resultados favoráveis nesse sentido.

03

Disponibilidade

O ideal em um sistema de informação é que os dados estejam disponíveis para o que for necessário, garantindo o acesso do usuário em tempo integral. Isso requer estabilidade e acesso permanente aos dados do sistema por meio de manutenção rápida, atualizações constantes e depuração.

É importante lembrar a vulnerabilidade dos sistemas que são suscetíveis a apagões, incêndios, ataques de negação e muitas outras possibilidades de ameaças que existem neste contexto.

04

Autenticidade

Confirmação de que os dados possuem legitimidade, ou seja, não haja manipulação ou intervenções externas de terceiros passando-se por colaboradores. Para tal objetivo, é necessário documentar as ações feitas pelos usuários na rede e nos sistemas.

Os dados corporativos devem ter processos para identificar a sua autenticidade e isso é uma das tarefas da equipe de Segurança da Informação. A configuração de um log de acesso ajuda a confirmar a veracidade de um determinado registro.

05

Legalidade

Por fim, é necessário ter uma Política de Segurança para assegurar que todos os procedimentos relacionados à informação dentro da empresa sejam feitos de acordo com a lei. Isso evita que ocorram impedimentos operacionais, averiguações e auditorias de órgãos fiscalizadores.

Adequar o conteúdo protegido à legislação é primordial, principalmente porque irá vigorar em agosto de 2020 a nova Lei Geral de Proteção de Dados Pessoais, que exigirá maior rigor de todas as empresas.

Quais são as principais ameaças à segurança da informação?

Hackes

Vírus

Arquivos
corrompidos

Clonagem de
dados

Invasões

Vazamento de
dados

e muito mais!

Portanto, percebam que tanto a LGPD quanto a Segurança da Informação **se complementam e buscam trazer mecanismos de segurança** para proteger às empresas. O grupo Credfranco se esforça constantemente para estar em compliance com as normas acima expostas.



**LGPD e Segurança da
Informação é um
trabalho conjunto,
contamos com vocês!!**