

Conformidade



Agenda

❖ O que veremos hoje:

1. Visão geral sobre conformidade
2. Verificação da conformidade com requisitos legais
3. Auditoria de sistemas de informação
4. Padrões relevantes para a segurança da informação
5. Lei Geral de Proteção de Dados (LGPD)

clideo.com

VISÃO GERAL



clideo.com

3



Contexto



- ❖ Os aspectos legais devem ser considerados no âmbito da segurança da informação
- ❖ As organizações estão sujeitas a leis, padrões e normas, conforme o país em que atua e seu ramo de atividade

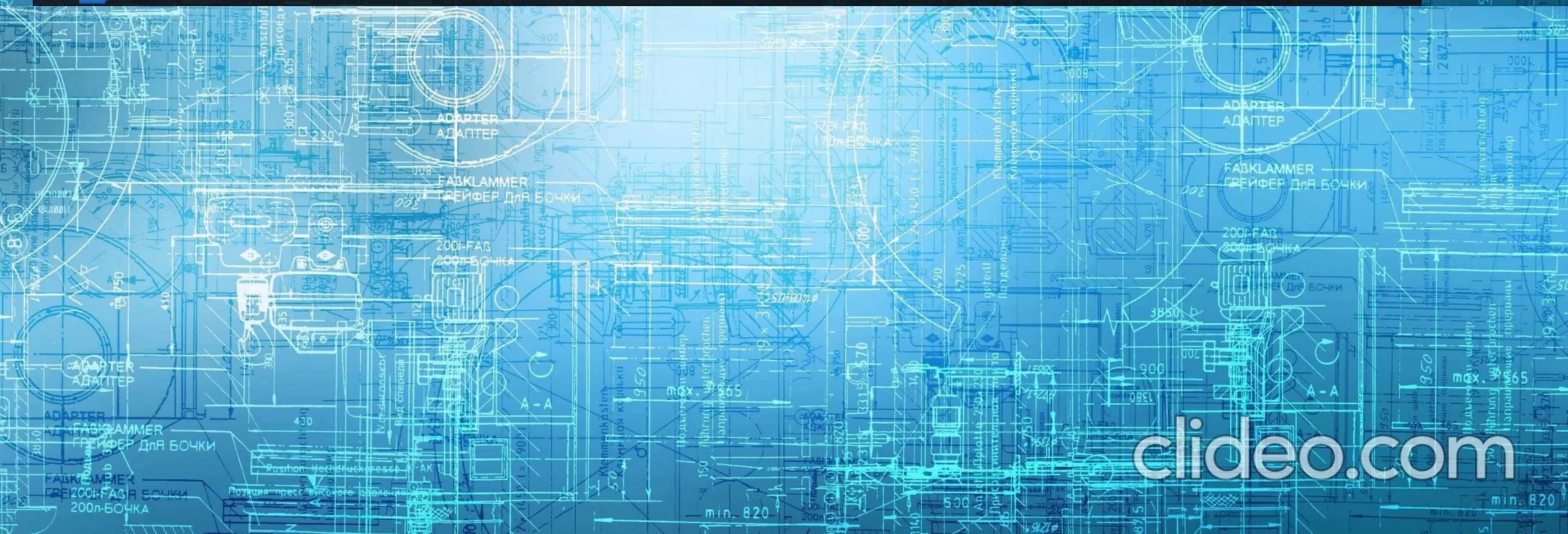
clideo.com

clideo.com



- constitucional
- do consumidor
- penal
- autoral
- contratual

10 - Conformidade





Questões de direito digital



- ❖ **Questão civil:** a montagem de um *website* falsificado na internet, prejudicando determinada organização, pode ocasionar indenização por danos morais e materiais?
- ❖ **Questão trabalhista:** a demissão de um funcionário por mau uso de correio eletrônico é caracterizada como justa causa?
- ❖ **Questão constitucional:** o monitoramento do *e-mail* dos funcionários viola o direito à privacidade?
- ❖ **Questão do consumidor:** o compartilhamento de dados coletados na internet fere o Código de Defesa do Consumidor (CDC)?
- ❖ **Questão penal:** se um funcionário instalar programas piratas na máquina de trabalho, a empresa responde judicialmente?
- ❖ **Questão autoral:** a empresa tem direito aos códigos-fonte dos softwares que encomenda a terceiros?
- ❖ **Questão contratual:** os *e-mails* trocados entre as partes podem ser usados como prova de uma relação contratual?



Exemplo de recomendação para uso de recursos de TI

“Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas pelo usuário no âmbito da infraestrutura de TI, ficando os transgressores sujeitos à lei penal, civil e administrativa, na medida da conduta, **dolosa** ou **culposa**, que praticarem.”

- ❖ **Doloso** → o agente tem intenção de praticar o ato ilícito e obter seu resultado. Ex.: vazamento intencional de dados
- ❖ **Culposo** → o resultado danoso foi obtido sem que o agente quisesse obtê-lo. Ex.: vazamento de dados por negligência de quem deveria cuidar da respectiva segurança



Exemplos de infrações digitais (1)



Conduta	Crime	Legislação	Pena
Enviar vírus, comando, instrução ou programa de computador que destrua equipamento ou dados eletrônicos	Dano	Art. 163, Código Penal	Detenção de 1 a 6 meses ou multa
Publicar foto em rede de relacionamento contendo gestos ou imagens obscenas	Ato obsceno	Art. 233, Código Penal	Detenção de 3 meses a 1 ano ou multa
Copiar um conteúdo sem mencionar a fonte; baixar MP3 ou filme, ilegalmente	Violação de direito autoral	Art. 184, Código Penal	Detenção de 3 meses a 1 ano ou multa (se a violação for com o intuito de lucro: reclusão de 1 a 4 anos e multa)
Criar uma comunidade virtual que ridicularize pessoas por conta de suas religiões	Escárnio por motivo religioso	Art. 208, Código Penal	Detenção de 1 mês a 1 ano e multa
Participar de comunidade virtual que discrimine pessoas por conta de sua etnia (por exemplo: “eu odeio nordestino”, “eu odeio negros”)	Discriminação por preconceito de raça, cor, etnia, religião ou procedência nacional	Art. 20, Lei nº 7.716/89	Reclusão de 1 a 3 anos e multa

clideo.com



Exemplos de infrações digitais (2)



Conduta	Crime	Legislação	Pena
Enviar <i>e-mail</i> dizendo características negativas de uma pessoa (por exemplo: feia, gorda, ignorante, incompetente etc.)	Injúria (a exposição na Internet pode converter em difamação)	Art. 140, Código Penal Art. 139, Código Penal	Detenção de 1 a 6 meses e multa Detenção de 3 meses a 1 ano e multa
Enviar <i>e-mail</i> a terceiros contendo informação considerada confidencial	Divulgação de segredo	Art. 153, Código Penal	Detenção de 1 a 6 meses ou multa
Enviar <i>e-mail</i> dizendo que vai matar a pessoa ou causar-lhe algum mal	Ameaça	Art. 147, Código Penal	Detenção de 1 a 6 meses ou multa
Enviar <i>e-mail</i> com remetente falso ou fazer cadastro em loja virtual com nome de terceiros	Falsa identidade	Art. 307, Código Penal	Detenção de 3 meses a 1 ano ou multa, se o fato não constituir elemento de crime mais grave
Falar em chat ou comunidade que alguém cometeu algum crime (por exemplo: “fulano é um ladrão”)	Calúnia	Art. 138, Código Penal	Detenção de 6 meses a 2 anos e multa
Efetuar transferência financeira através de <i>internet banking</i> com dados bancários de terceiros	Furto	Art. 155, Código Penal	Reclusão de 1 a 4 anos e multa
Funcionário público acessar a rede corporativa e alterar informações sem autorização	Modificação ou alteração não autorizada de sistema de informação	Art. 313-B, Código Penal	Detenção de 3 meses a 2 anos e multa

clideo.com



Direito digital e necessidades atuais



- ❖ Enquanto a legislação referente ao direito digital não for estabelecida por completo, regras claras para a conduta dos funcionários, dirigentes, terceirizados e demais envolvidos devem ser elaboradas pelas organizações
 - **Privacidade x monitoramento**, por exemplo, quanto ao uso, por parte de funcionários, de endereço de e-mail corporativo para receber conteúdo privado
 - **Segurança da informação x usuário**, em particular, no sentido de estabelecer claramente os direitos e sanções legais aplicáveis em caso de problemas
 - **Responsabilidades por atividades realizadas em equipamentos da empresa são relevantes**, pois equipamentos são ativos e devem ser utilizados de modo a não ocasionar processos judiciais
 - **Limites de responsabilidades em ambientes externos** devem ser considerados ao lidarmos com soluções como acesso remoto à rede da organização ou soluções de *home office*
 - Quanto à **necessidade da guarda da prova**, documentos digitais, tais como e-mail, não possuem legislação específica que determine seu uso como prova

VERIFICAÇÃO DA CONFORMIDADE COM REQUISITOS LEGAIS



Legislação vigente



- ❖ Recomenda-se definir, documentar e manter:
 - Requisitos estatutários
 - Requisitos regulamentares
 - Requisitos contratuais

clideo.com





Propriedade intelectual

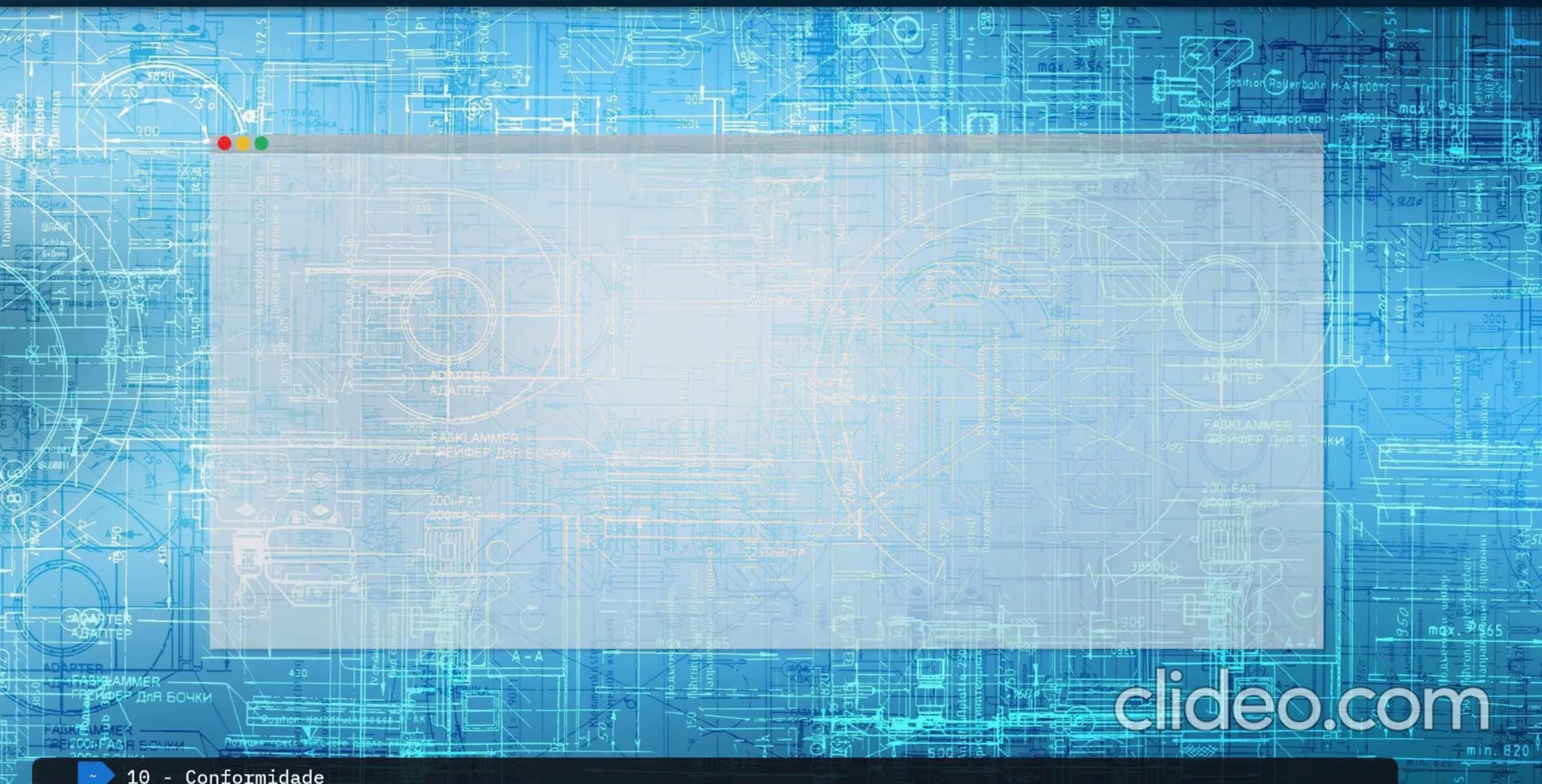


- ❖ Aplica-se ao uso de material com direitos autorais e *software* proprietário
- ❖ Cuidados:

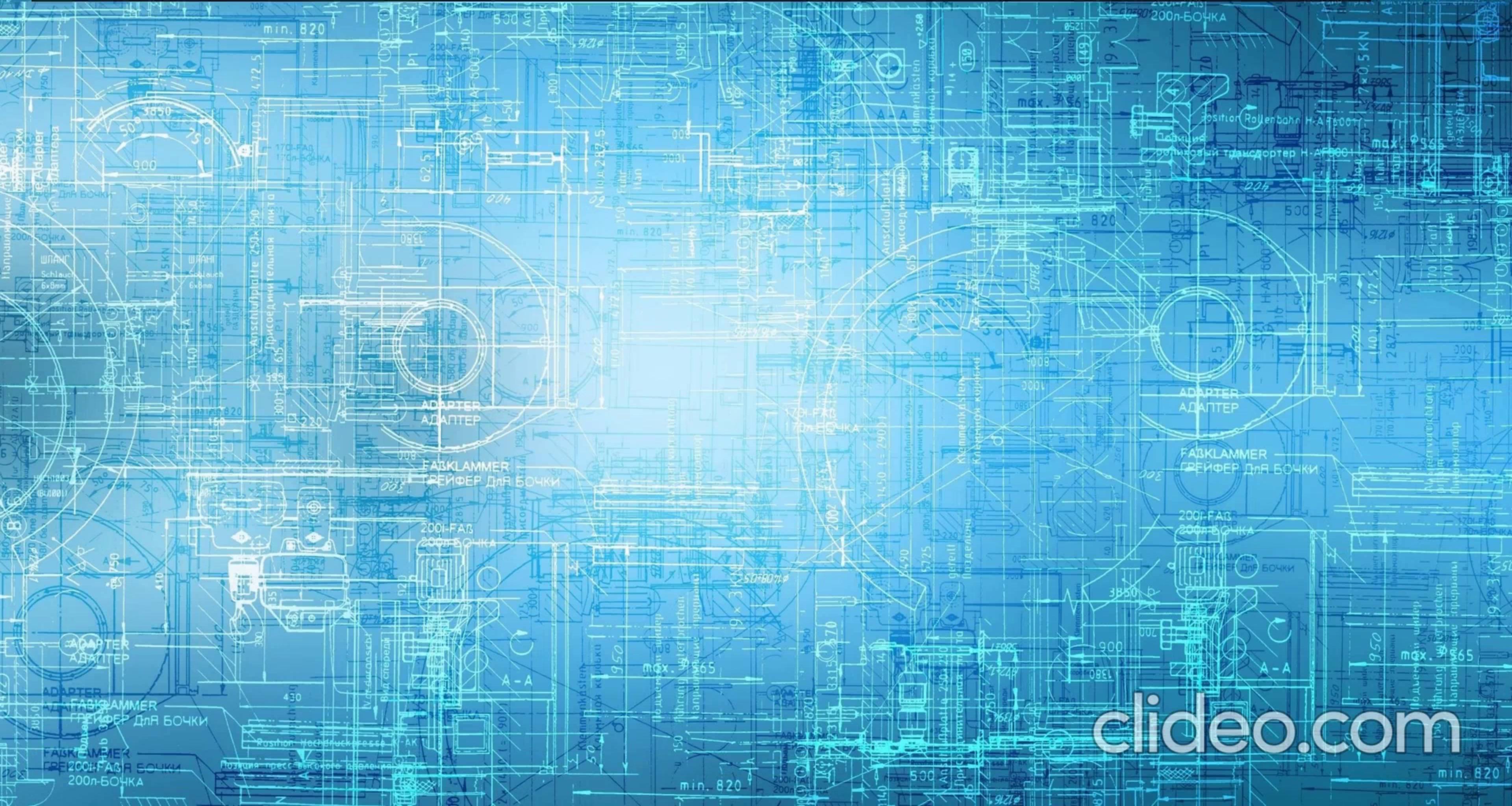
clideo.com



Proteção de registros organizacionais



clideo.com





Prevenção contra mau uso



- ❖ Recursos de processamento de informações devem ser protegidos contra uso não relacionado aos negócios da organização e uso não autorizado
- ❖ Cuidados (norma ABNT ISO/IEC 27002:2013):
 - Monitoramento adequado
 - Uso de ferramentas de apoio (sistemas de detecção de intrusos)
 - Ações disciplinares ou legais
 - Conscientização dos usuários e tomada da respectiva declaração de ciência por escrito



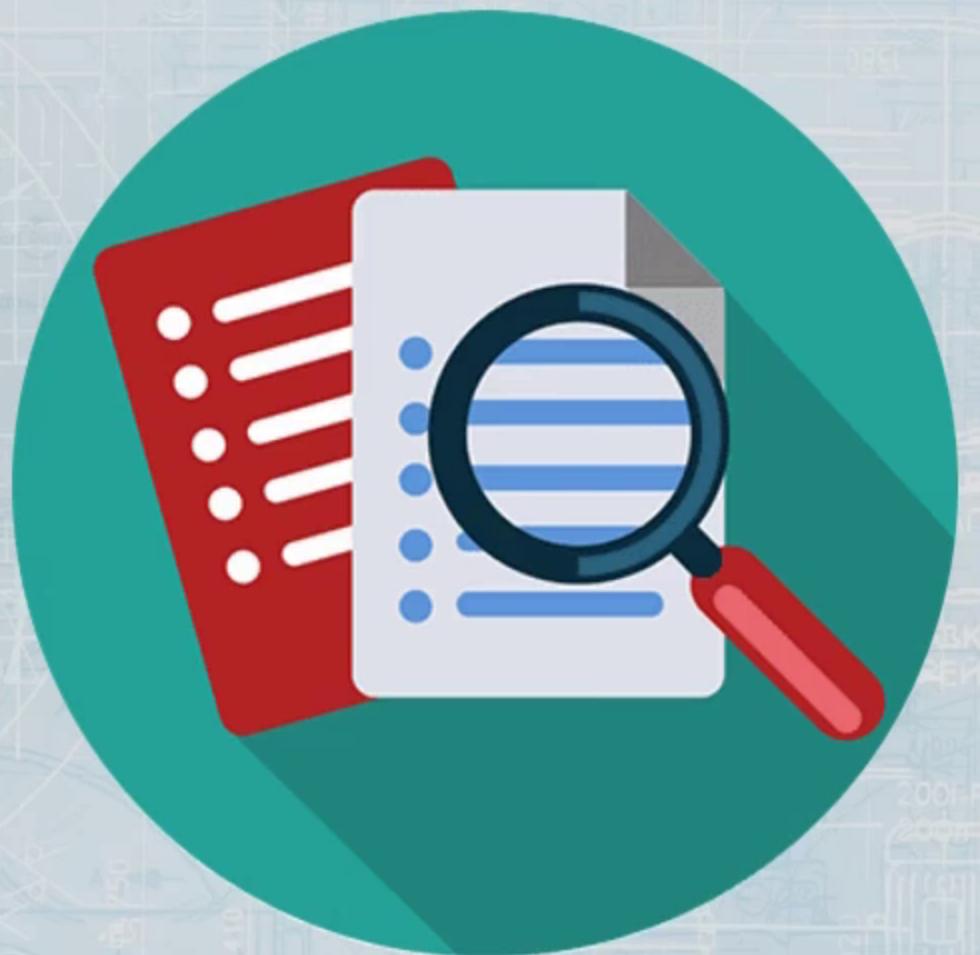
AUDITORIA DE SISTEMAS DE INFORMAÇÃO





Procedimentos de auditoria

- ❖ Durante a auditoria de sistemas de informação, recomenda-se proteger os sistemas e ferramentas empregados, garantindo sua integridade e controle contra acessos não autorizados
- ❖ As atividades de auditoria devem ser realizadas segundo um planejamento adequado, de comum acordo com os dirigentes da organização, de modo a não influenciar seu negócio
- ❖ O acesso às ferramentas de auditoria deve ser controlado, e elas devem ser armazenadas em locais separados ou isolados





Cuidados na auditoria

- 
- ❖ Auditoria acordada com a organização
 - ❖ Escopo da verificação acordado e controlado
 - ❖ Verificação limitada ao acesso apenas para leitura
 - ❖ Acessos além da leitura feitos em cópias isoladas, com sua remoção (ou armazenamento com segurança) ao final
 - ❖ Recursos usados identificados e disponíveis
 - ❖ Acessos monitorados e registrados
 - ❖ Tudo deve ser documentado

PADRÕES RELEVANTES PARA A SEGURANÇA DA INFORMAÇÃO

clideo.com



Padrões relevantes



- ❖ *Control Objectives for Information Technologies (CobiT 4.1)*
 - Framework de governança em TI, apresentando boas práticas para o controle de requisitos, mapas de auditoria, questões técnicas e riscos de negócio
- ❖ *Information Technology Infrastructure Library (ITIL)*
 - Compreende uma biblioteca de boas práticas para a gestão de TI de domínio público focando o cliente e a qualidade dos serviços de TI, estabelecendo um conjunto de processos e procedimentos gerenciais
- ❖ Esses padrões serão estudados em detalhes na disciplina de Gestão e Governança de Tecnologia da Informação, no 6º ciclo do curso de ADS da Fatec Franca

LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

clideo.com



A LGPD



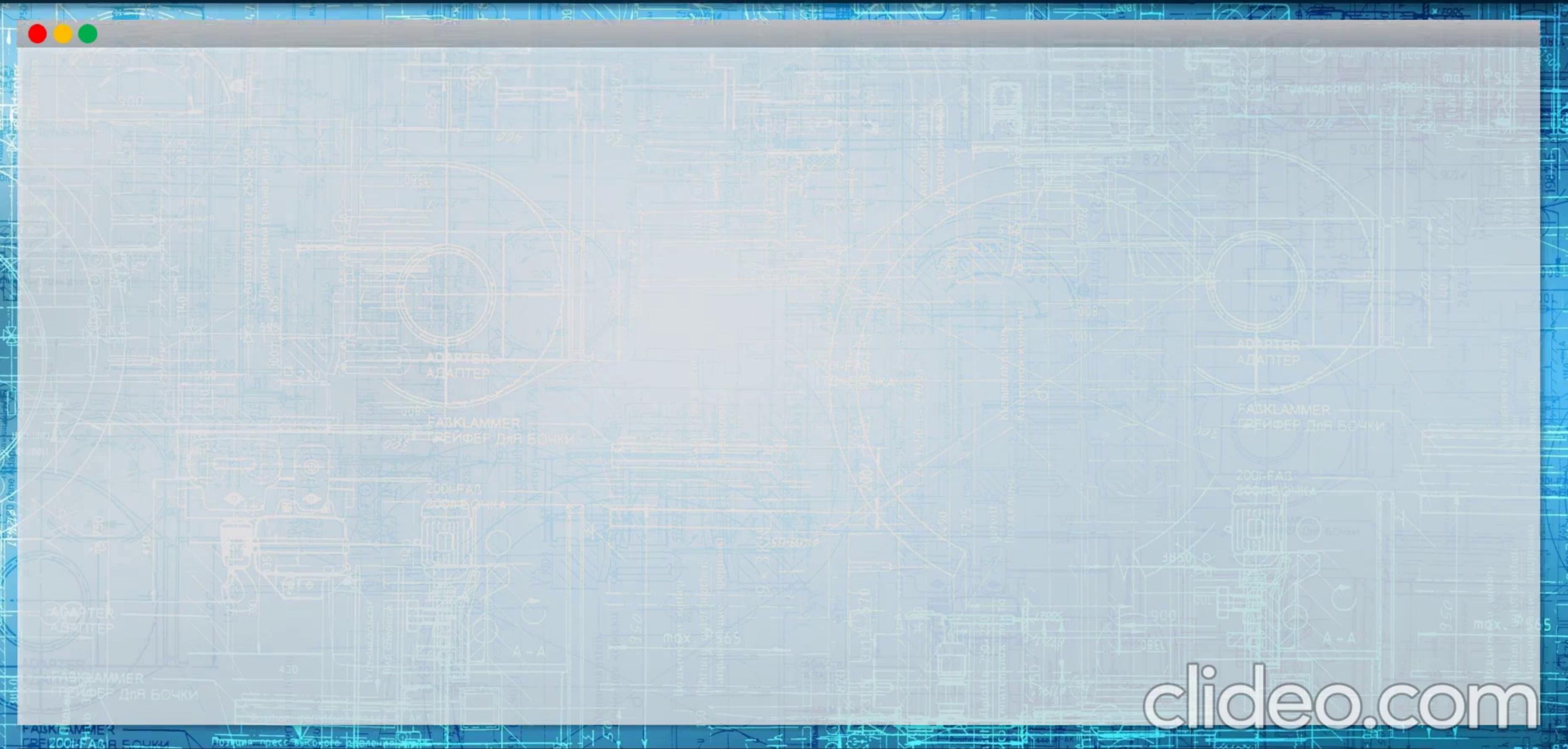
- ❖ Lei nº 13.709, de 14 de agosto de 2018 → Lei Geral de Proteção de Dados Pessoais
- ❖ Inspirada pela GDPR – lei europeia de proteção de dados pessoais, em vigor desde 2018
- ❖ Tem por finalidade normatizar e uniformizar as regras sobre coleta, armazenamento e **tratamento de dados** pessoais do Brasil

clideo.com



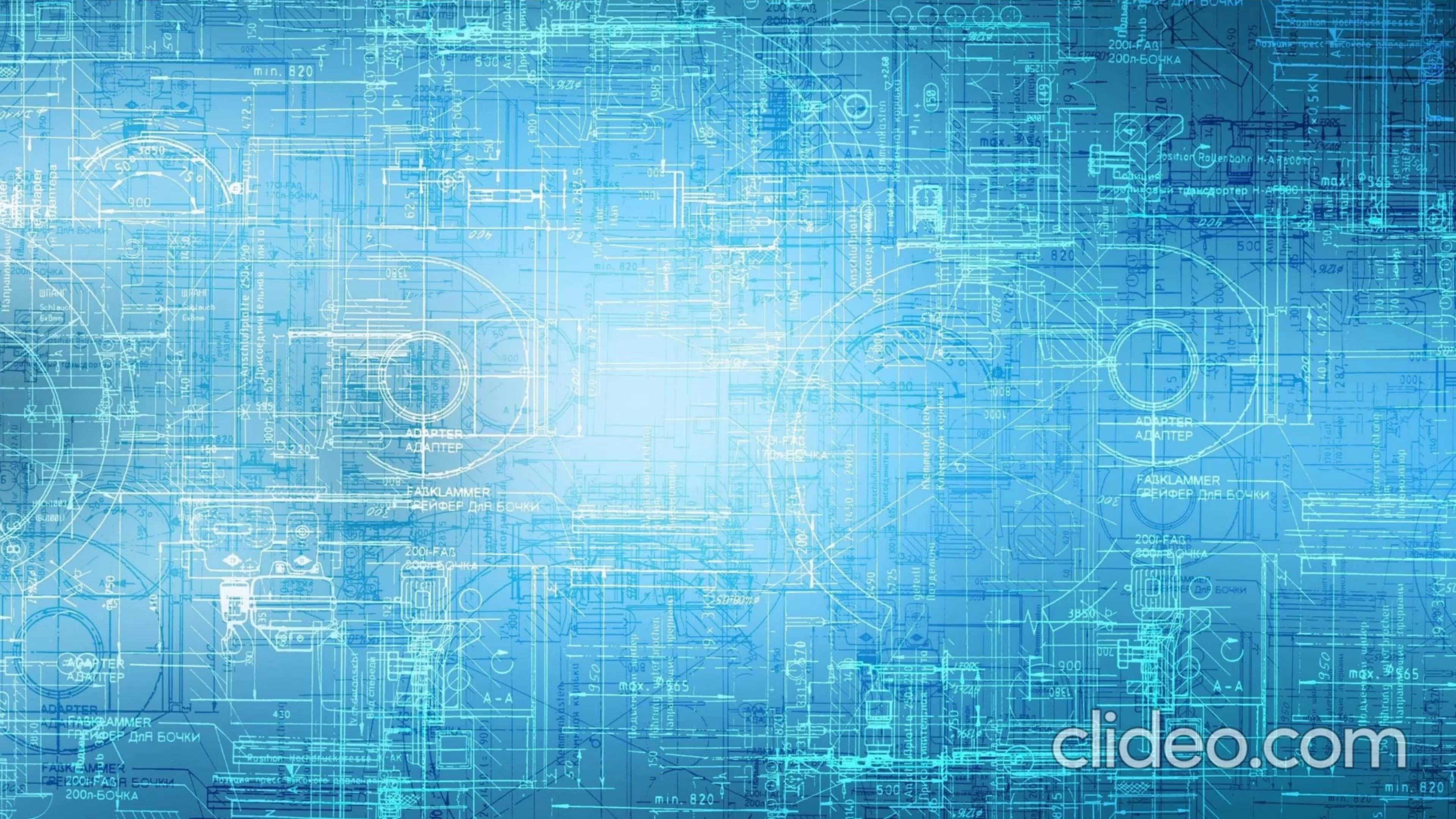


Escopo da LGPD



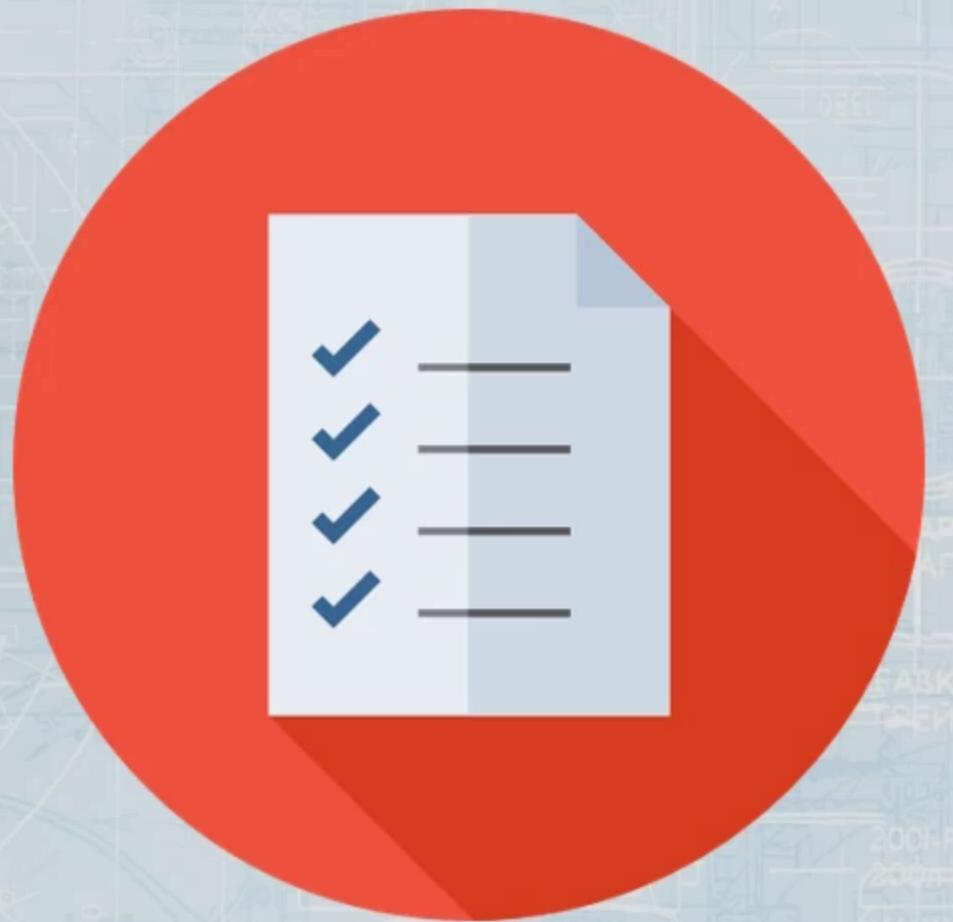
clideo.com

clideo.com





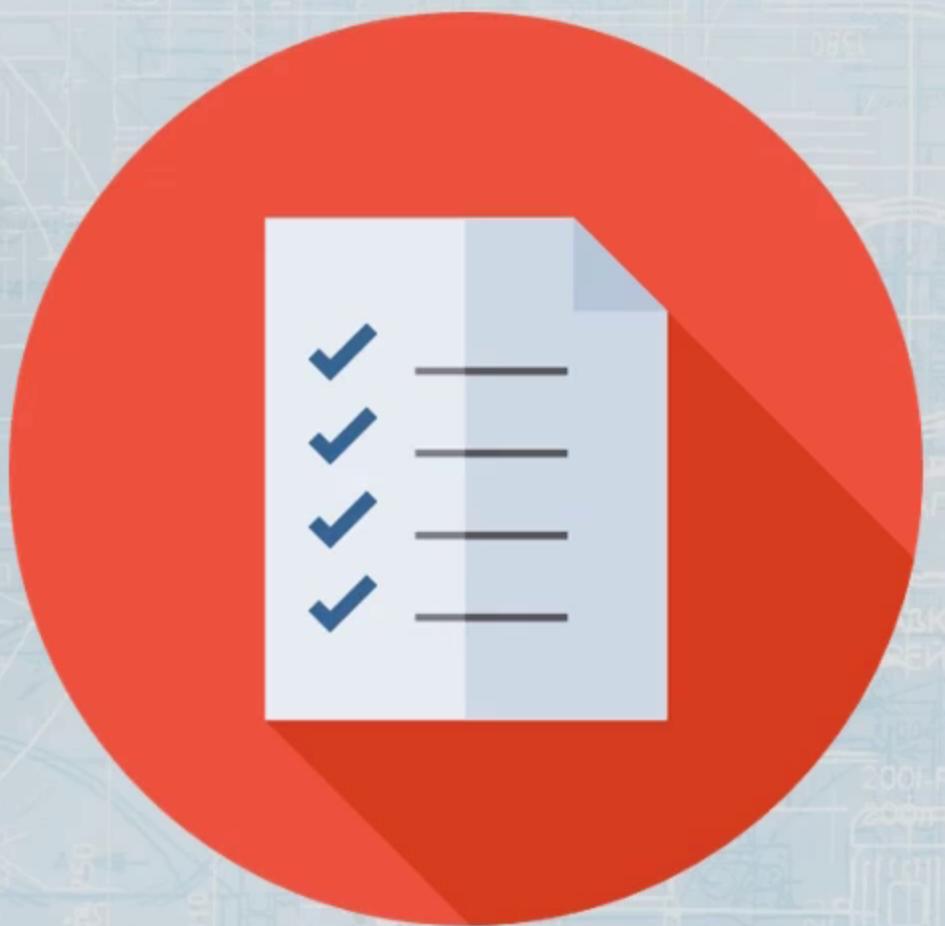
Principais pontos (1)



- ❖ O usuário, que é o titular de seus dados pessoais, precisam dar seu consentimento explícito, isto é, autorizar de forma clara o uso dos dados pela organização
- ❖ Para isso, a organização deve apresentar um Termo de Uso específico, detalhando onde e como os dados serão armazenados, qual é o objetivo da coleta e como será feito o respectivo processamento
- ❖ Caso alguma das áreas da segurança seja alterada no Termo, será preciso que a empresa o reescreva para apresentar novamente ao usuário
- ❖ Esse “contrato” pode ser revogado a qualquer momento, fazendo com que a organização seja obrigada a deletar os dados e entregá-los ao usuário de novo



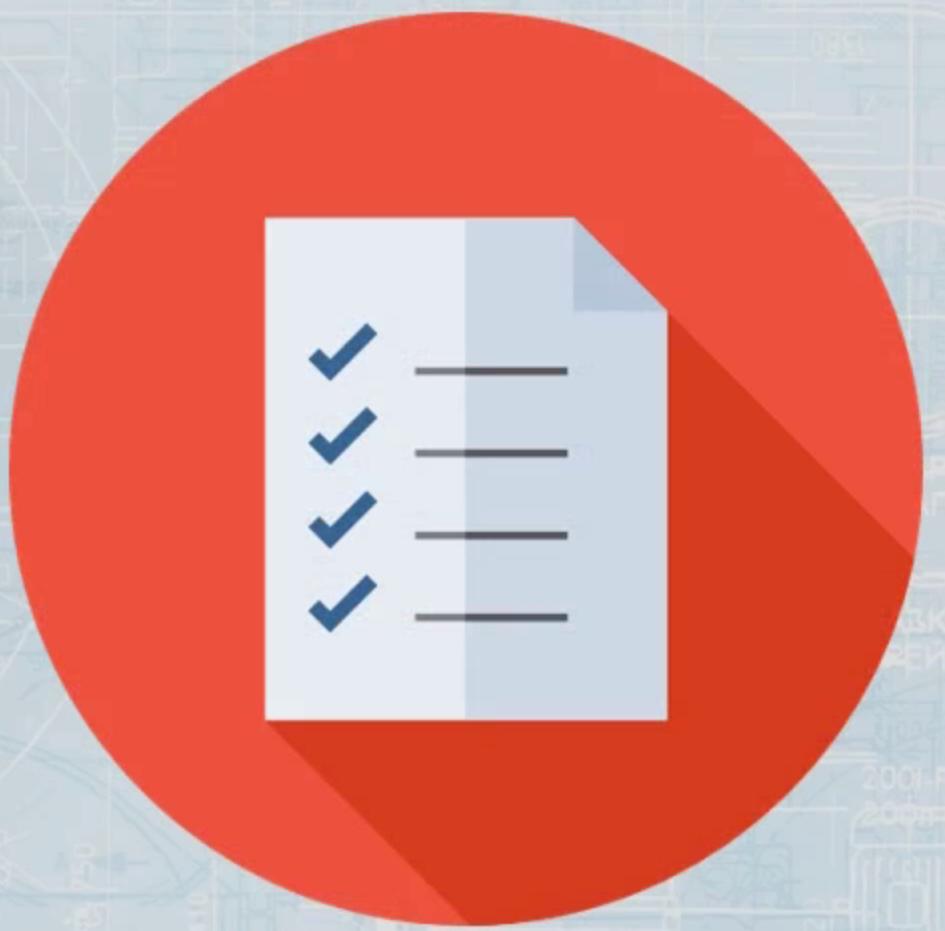
Principais pontos (2)



- ❖ As organizações precisam garantir a segurança da informação, já que serão 100% responsáveis caso algum vazamento de informações sigilosas ocorra, sendo preciso notificar o usuário de forma imediata
- ❖ O proprietário dos dados tem o direito de saber quais informações suas estão sob a responsabilidade da organização. Ele também pode ter conhecimento da finalidade, tratamento e outros detalhes que desejar
- ❖ O proprietário pode ainda requisitar a portabilidade de dados para outros provedores de serviços. Assim, se a pessoa desejar ter uma conta em mais de um banco, ela pode exigir que suas informações sejam transferidas de uma instituição para outra



Principais pontos (3)



- ❖ A Lei estabelece a criação de uma agência reguladora, a Agência Nacional de Proteção de Dados (ANPD), que ficará responsável por regulamentar e coordenar as ações de proteção de dados no território nacional
- ❖ Toda organização, independentemente do seu porte, deverá nomear um **Encarregado de Dados**, cuja responsabilidade é atuar como canal de comunicação entre a organização os titulares dos dados e a ANPD
 - O Encarregado de Dados, para bem desempenhar seu papel, deverá ter **sólidos conhecimentos de segurança da informação** → nova oportunidade de carreira



Sanções previstas pela LGPD



- ❖ A **não conformidade** das organizações à LGPD pode acarretar uma gama de sanções, dentre as quais:
 - **Advertência** → não há cobrança ainda, mas se determina um período para que a empresa se adeque às novas medidas
 - **Multa simples ou diária** → o valor cobrado é de cerca de 2% do faturamento anual da empresa com um limite de R\$ 50 milhões de reais para cada infração
 - **Publicação da ocorrência** → é realizada a divulgação de que a organização infringiu a lei estabelecida (causa danos à reputação e à imagem da empresa)
 - **Bloqueio de dados** → a empresa perde a autorização dos dados relacionados à violação ocorrida
 - **Eliminação de dados** → a organização é obrigada a deletar todos os dados e informações que dizem respeito à transgressão

O QUE VEM POR AÍ

clideo.com
28



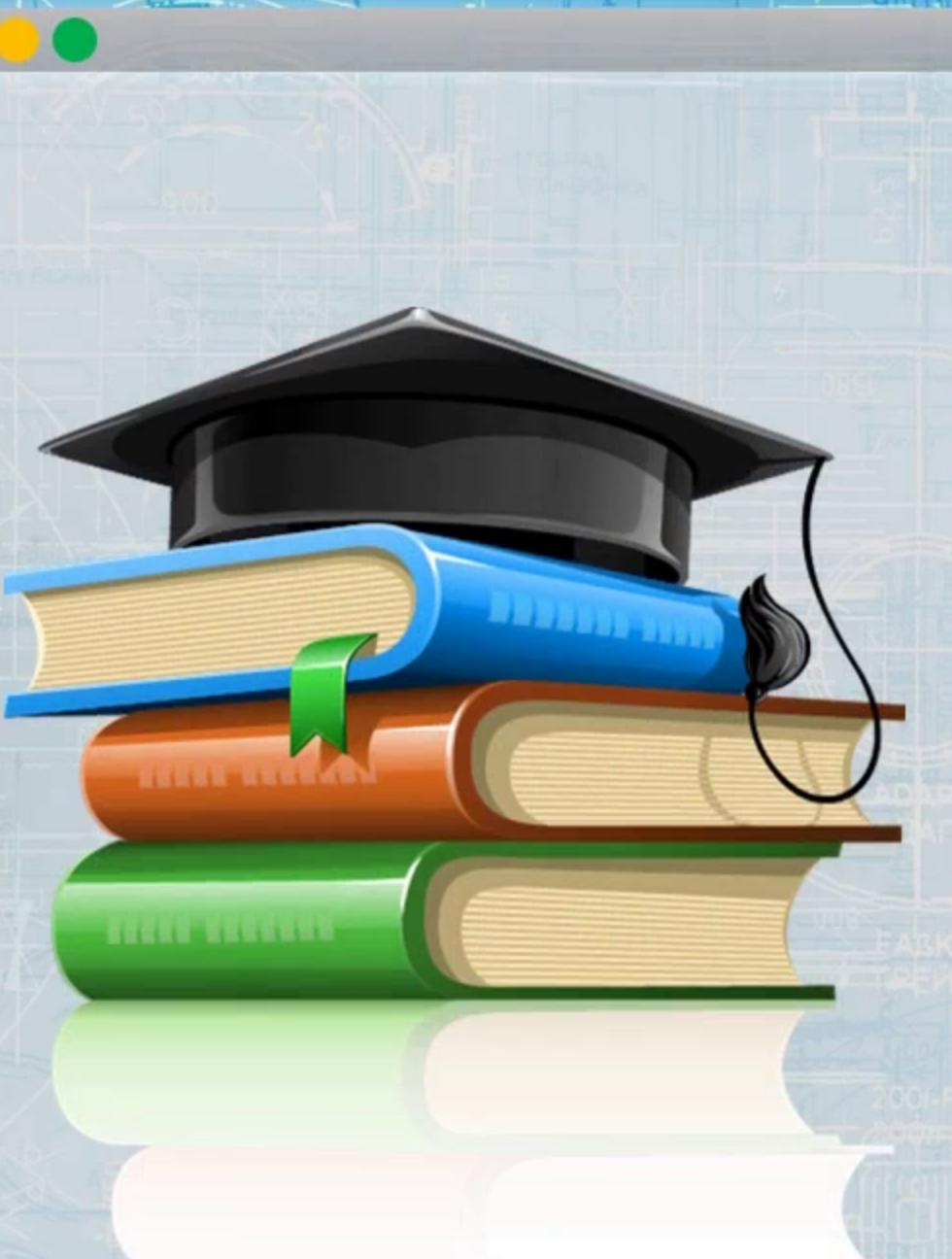
Nas próximas aulas



❖ Entraremos na parte mais técnica da disciplina, para aprender sobre criptografia e suas técnicas



Para saber mais

- 
- ❖ COELHO, Flávia Estélia Silva; ARAÚJO, Luiz Geraldo Segadas de; BEZERRA, Edson Kowask. **Gestão da Segurança da Informação**: NBR 27001 e NBR 27002. Rio de Janeiro: RNP/ESR, 2015, p. 173-196
 - ❖ SYNTEX WESTCOM. **Quais os principais impactos da nova Lei Geral de Proteção de Dados?** Disponível em: <https://blogbrasil.westcon.com/quais-os-principais-impactos-da-nova-lei-geral-de-protecao-de-dados>
 - ❖ SIVIOTTI, Douglas. **LGPD**: Lei Geral de Proteção de Dados Pessoais. Disponível em: <https://pt2.slideshare.net/DouglasSiviotti/lgpd-lei-geral-de-proteo-de-dados-pessoais-174574254>