

A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)



A LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA (LGPD)

A Lei Geral de Proteção de Dados brasileira (LGPD), assegurará aos titulares de dados um maior controle sobre o armazenamento, recuperação e transferência de seus Dados Pessoais, que consistem em quaisquer informações relacionadas à pessoa natural que a identifique (nome, endereço, e-mail, número dos documentos, etc.) ou a torne identificável (dados de GPS, hábitos de consumo, numeração das vestimentas, preferências ou restrições alimentares, dentre outras).

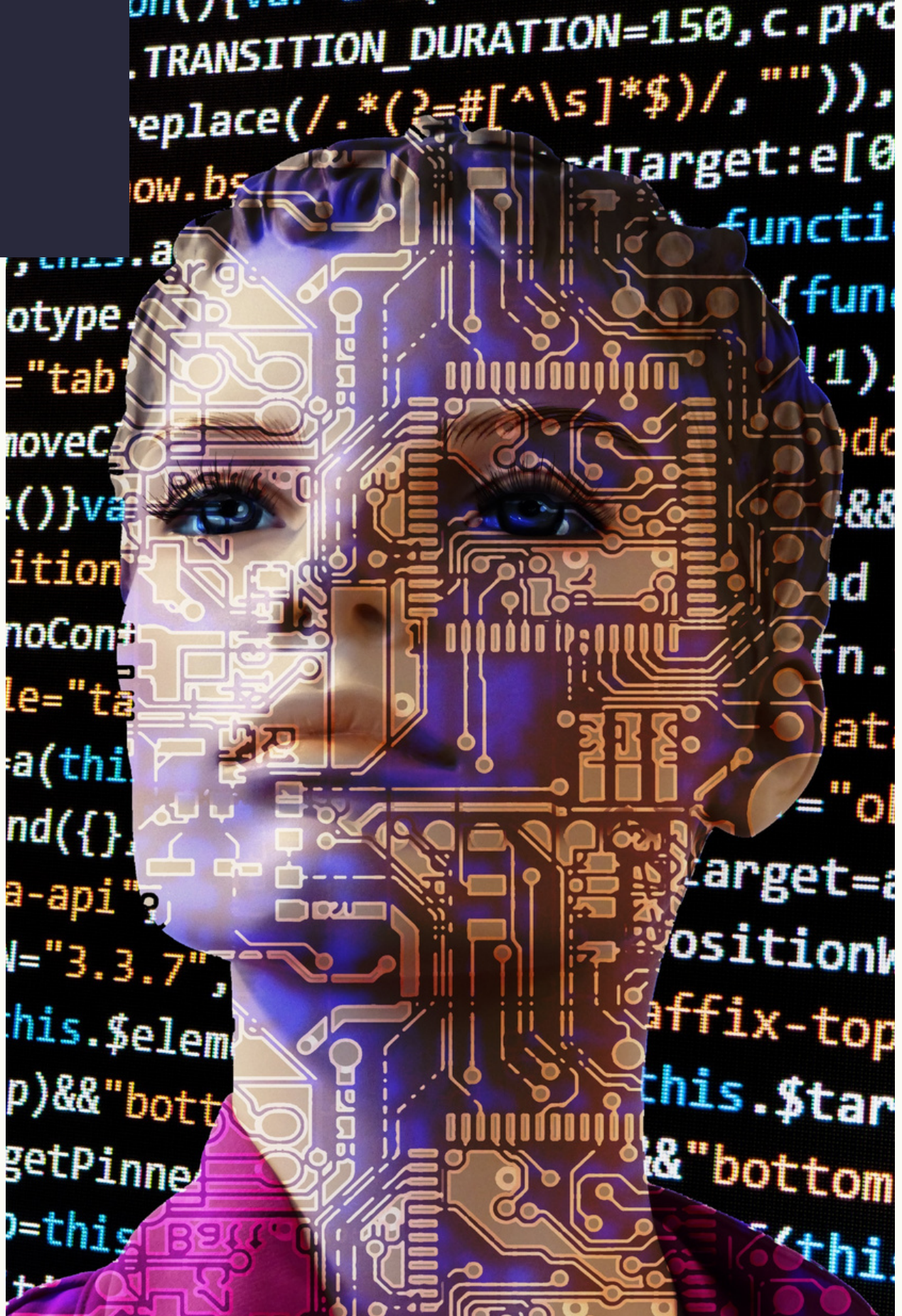
```
timestamp": "2017-06-03T18:42:18.018", "deltaStart",  
class": "com.orgmanager.handlers.RequestHandler", "m  
sizeChars": "5022", "message": "Duration Log", "dura  
webURL": "/app/page/analyze", "webParams": "null", "c  
requestID": "8249868e-afd8-46ac-9745-839146a20f09", "  
rationMillis": "36"} {"timestamp": "2017-06-03T18:43  
webParams": "file=chartdata_new.json", "class": "com.  
essionID": "144o2n620jm9trnd3s3n7wg0k", "sizeChars"  
deltaStartMillis": "0", "level": "INFO", "webURL": "/a  
requestID": "789d89cb-bfa8-4e7d-8047-498454af885d", "  
rationMillis": "7"} {"timestamp": "2017-06-03T18:46:  
class": "com.orgmanager.handlers.RequestHandler", "r  
sizeChars": "10190", "message": "Duration Log", "dura  
webURL": "/app/rest/json/file", "webParams": "file=ch  
requestID": "7ac6ce95-19e2-4a60-88d7-6ead86e273d1", "  
rationMillis": "23"} {"timestamp": "2017-06-03T18:42  
class": "com.orgmanager.handlers.RequestHandler", "m  
sizeChars": "5022", "message": "Duration Log", "durat  
webURL": "/app/page/analyze", "webParams": "null", "c  
requestID": "8249868e-afd8-46ac-9745-839146a20f09", "  
rationMillis": "36"} {"timestamp": "2017-06-03T18:43  
webParams": "file=chartdata_new.json", "class": "com.  
essionID": "144o2n620jm9trnd3s3n7wg0k", "sizeChars"  
deltaStartMillis": "0", "level": "INFO", "webURL": "/a  
requestID": "789d89cb-bfa8-4e7d-8047-498454af885d", "  
rationMillis": "7"} {"timestamp": "2017-06-03T18:46:  
class": "com.orgmanager.handlers.RequestHandler", "m
```

CERTO, ENTENDI! MAS A QUEM A LGPD SE APLICA?

A LGPD será aplicável a todas as empresas que realizem operações de tratamento de Dados Pessoais. Essas empresas deverão solicitar o consentimento explícito do titular, tanto para a coleta quanto para o uso de seus dados, além de ter de conceder a possibilidade de acesso, correção, anonimização, eliminação e de portabilidade dos dados.



Com a NÉRUS não é diferente! Por lidarmos diretamente com os dados pessoais de nossos Clientes, Colaboradores e Parceiros, precisamos gerirlos com a necessária segurança. Fazemos isso por meio do contínuo mapeamento do tratamento de dados, além da realização de investimentos em segurança da informação e manutenção das evidências jurídicas e técnicas do efetivo cumprimento da LGPD e de toda a legislação brasileira.



QUEM É QUEM NA LGPD?

FAZ TODO O SENTIDO!

A NÉRUS, assim como todos os seus Colaboradores, Fornecedores e Parceiros, têm a obrigação de seguir a LGPD por tratar diretamente com Dados Pessoais!

Mas existem vários termos e sujeitos complexos trazidos pela Lei, o que eles significam, afinal?

VAMOS ENTENDER?

DADO PESSOAL

Informação relacionada à pessoa natural identificada ou identificável.

TITULAR DE DADOS PESSOAIS

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

DADO PESSOAL SENSÍVEL

Dado relativo à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

VAMOS ENTENDER?

DADO ANONIMIZADO

Dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (APND)

Órgão da administração pública direta que será responsável por realizar a fiscalização para o cumprimento da LGPD, emitindo normativas e entendimentos sobre a legislação de proteção de dados pessoais.

CONTROLADOR

Pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de Dados Pessoais.

VAMOS ENTENDER?

CONTROLADOR CONJUNTO

Controlador de Dados Pessoais que determina os propósitos e formas do tratamento de DP, junto com um ou mais controladores de Dados Pessoais.

OPERADOR

Pessoa natural ou jurídica que realiza o tratamento de Dados Pessoais em nome do controlador.

ENCARREGADO OU DATA PROTECTION OFFICER (DPO)

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

PRINCÍPIOS DA LGPD

Já deu para ver que a proteção dos Dados Pessoais é um assunto sério!

E é justamente por isso que os sujeitos da LGPD devem agir em observância a vários princípios ao realizar o tratamento dos dados pessoais dos titulares.



E QUE PRINCÍPIOS SÃO ESSES?

FINALIDADE

Não há possibilidade de tratamento de dados pessoais sem que haja uma finalidade, ou seja, um propósito específico e legítimo que legitime esse tratamento.

NECESSIDADE

Visa coibir o tratamento excessivo e desnecessário dos dados pessoais, devendo ser tratados somente os dados mínimos e necessários para a finalidade pretendida, sempre considerando a proporcionalidade do tratamento com os riscos aos titulares.

ADEQUAÇÃO

O tratamento de dados somente poderá ser realizado quando estiver adequado às finalidades informadas aos titulares dos dados, evitando-se, assim, a desvirtuação.

QUALIDADE DOS DADOS

Garantia aos titulares da exatidão, da clareza, da relevância e da atualização dos dados, de acordo com a necessidade e para cumprimento da finalidade específica de seu tratamento.

E QUE PRINCÍPIOS SÃO ESSES?

LIVRE ACESSO

Princípio que permite que os titulares tenham controle dos seus dados, garantindo que eles tenham acesso gratuito e consulta facilitada para saber a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais e os riscos aos titulares.

SEGURANÇA

Princípio que exprime a necessidade de utilização do máximo de medidas técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizado e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

TRANSPARÊNCIA

Impõe a transparência sobre o tratamento de dados, sendo desse modo necessária a garantia aos titulares de informações claras, precisas e facilmente acessíveis.

PREVENÇÃO

Visa prevenir a possibilidade de ocorrência de danos bem antes do tratamento, durante todo o período de vida dos dados até o seu efetivo descarte. A Prevenção perpassa pela adoção de boas práticas de governança para segurança informacional e ações educacionais dirigidas aos Colaboradores, Fornecedores e Parceiros.

E QUE PRINCÍPIOS SÃO ESSES?

NÃO DISCRIMINAÇÃO

Princípio essencial aos fundamentos da lei, destinado à proteção da personalidade e da pessoa humana. Este princípio prevê a impossibilidade de realização do tratamento para fins discriminatórios ilegais ou abusivos.

RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS

Impõe a efetiva demonstração, durante todo o ciclo de vida de tratamento dos dados, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, viabilizando, inclusive, a comprovação de eficácia dessas medidas.

AS BASES LEGAIS DO TRATAMENTO DE DADOS



Compreendidos os Sujeitos e os Princípios da Proteção de Dados, importante ressaltarmos que o Tratamento de Dados Pessoais apenas será legítimo ao observar uma ou mais das bases legais previstas pela LGPD.

AO TODO SÃO 10 (DEZ) BASES LEGAIS

1. **Consentimento:** manifestado de forma livre pelo titular, sem pressão alguma, seja por subordinação hierárquica, econômica ou sob alegação de que sem o seu consentimento haverá impossibilidade de utilização da tecnologia, condicionando o acesso à coleta daqueles dados. É a base legal que opera como Regra.
2. **Cumprimento de Obrigação Legal ou Regulatória:** havendo base legal para o tratamento de Dados Pessoais, seja por relação jurídica ou outro motivo, caso o tratamento ocorra por força de disposição legal ou regulatória, o titular não poderá se opor ao tratamento.
3. **Pela administração para execução de Políticas Públicas:** a Administração Pública poderá realizar o tratamento e o compartilhamento de Dados Pessoais, desde que sejam para a execução de políticas públicas, que podemos entender como a atividade de qualquer órgão da administração que tenha como objetivo atender e solucionar demandas da sociedade.
4. **Para realização de Estudos por Órgãos de Pesquisa:** Órgãos de Pesquisa poderão realizar o tratamento e o compartilhamento de Dados Pessoais, desde que se atenham à anonimização dos Dados Pessoais e devem, ainda, respeitar os princípios da finalidade, adequação e necessidade previstos na LGPD.

AO TODO SÃO 10 (DEZ) BASES LEGAIS

5. Para execução de Contratos ou Procedimentos Preliminares ao Contrato: havendo a necessidade de uma relação contratual a pedido do titular dos dados, será necessário o tratamento de seus dados, existindo, assim, base legal para execução de contrato ou de procedimentos preliminares à sua formalização.

6. Para exercício regular de direitos: é legítimo o tratamento de dados para o exercício de direitos em processos em geral, administrativos, judiciais ou arbitrais, sendo desnecessário solicitar o consentimento para coleta de dados da outra parte para que ocorra o tratamento.

7. Para a proteção da Vida ou Incolumidade Física do Titular ou de Terceiros: embora a privacidade e a intimidade sejam bens jurídicos protegidos, vida é um bem jurídico que se sobrepõe a qualquer outro, podendo o tratamento de dados ser realizado para a proteção dela, em caráter restrito de risco, urgência ou ameaça, não se prestando, contudo, à atividade de prevenção.

AO TODO SÃO 10 (DEZ) BASES LEGAIS

8. **Para tutela da Saúde:** se justifica também em razão da proteção da vida humana, sendo seu tratamento restritivo aos “profissionais da área da saúde” ou “entidades sanitárias”, dentro, é claro, da atuação profissional delas, sendo vedado o tratamento para qualquer outro fim que não esse.

9. **Legítimo Interesse:** base legal de definição aberta. A LGPD apresenta dois exemplos para a aplicação do legítimo interesse, quais sejam, o apoio e promoção de atividade do controlador e proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos da LGPD.

10. **Para a proteção do Crédito:** em consonância com o Código de Defesa do Consumidor (CDC) e com a Lei do Cadastro Positivo (Lei 12.414/11), é legítima a formação de bancos de dados por parte dos serviços de proteção ao crédito, viabilizando o tratamento de Dados Pessoais e o conseqüente fortalecimento do mercado financeiro e do comércio.

Agora que você já tem conhecimentos sobre a importância da Proteção de Dados Pessoais no Brasil, que tal ficar por dentro de como a NÉRUS realiza o Tratamento de Dados Pessoais de seus Clientes, Colaboradores e Parceiros?

A NÉRUS é uma empresa de tecnologia com DNA de vendas, especializada em soluções para varejo e distribuição. Oferece soluções de software para transformação das vendas físicas em digitais, integrando as lojas e transformando as mesmas em Lojas Omnichannel: vendas físicas e digitais reunidas em um só sistema.

Mas vamos a uma explicação prática!

POR DENTRO DO TRATAMENTO DE DADOS PESSOAIS REALIZADO PELA





Em relação ao tratamento dos dados pessoais de seus próprios colaboradores, a **NÉRUS** está na qualidade de agente de tratamento como **CONTROLADOR**. Quanto ao tratamento de dados pessoais dos Clientes das Empresas que utilizam suas soluções, atua na qualidade de **OPERADOR**.

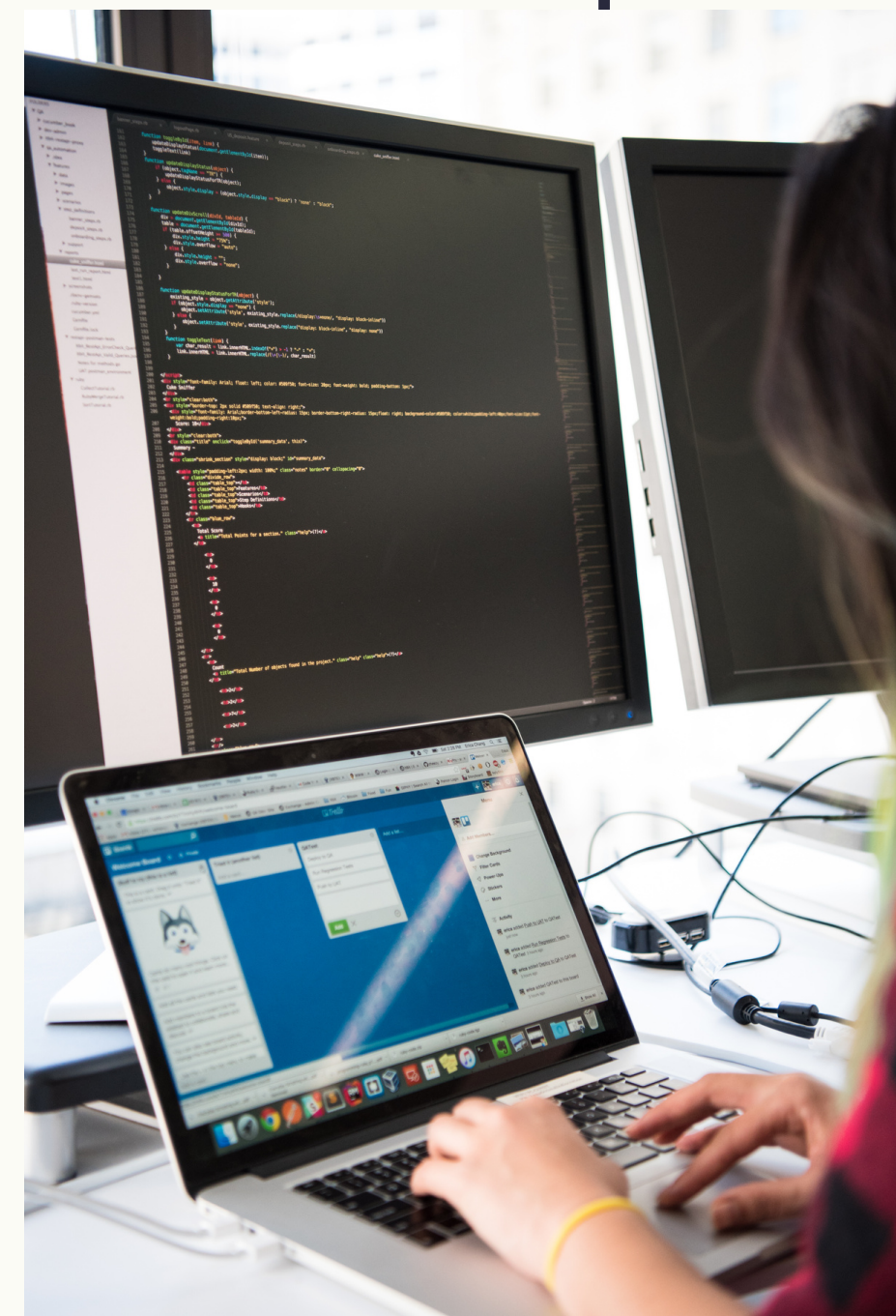
Quando alguém se inscreve para receber nossas Newsletters, está fornecendo consentimento para tratamento de seus dados pessoais.

Com os referidos Dados, a **NÉRUS** consegue endereçar a oferta de novos Produtos, Serviços a potenciais interessados em suas Soluções. De forma mais clara, com as informações recebidas conseguimos viabilizar o envio de novas Newsletters, direcionar a produção de nosso *Marketing* de Conteúdo, bem como enviar convites para outros Eventos.

PELO PRINCÍPIO DA TRANSPARÊNCIA, O TITULAR DOS DADOS PESSOAIS PRECISA ESTAR INFORMADO SOBRE O TRATAMENTO DE SEUS DADOS PESSOAIS E SOBRE OS SEUS DIREITOS.

É EXATAMENTE POR ISSO QUE A NÉRUS SE PREPAROU PARA ATENDER AS SOLICITAÇÕES DOS TITULARES DOS DADOS PESSOAIS DE FORMA ACESSÍVEL E EM TEMPO HÁBIL.

Foi pensando em garantir informações sobre o atendimento e os direitos dos titulares de dados pessoais que a NÉRUS disponibilizou uma extensa e completa Política de Privacidade.



EM NOSSA POLÍTICA DE PRIVACIDADE É POSSÍVEL TER ACESSO A DIVERSAS INFORMAÇÕES PERTINENTES À PROTEÇÃO DE DADOS PESSOAIS, DENTRE AS QUAIS ESTÃO INCLUÍDAS:

- A finalidade do tratamento;
- Os detalhes do tratamento de dados por operadores;
- As bases legais do tratamento;
- O modo pelo qual o dado pessoal foi obtido, caso não seja fornecido diretamente pelo titular dos Dados Pessoais;
- Os direitos dos titulares de Dados Pessoais, especialmente sobre o acesso, acréscimo, correção, solicitação para apagar (desde que a base legal permita), informações de quais Dados Pessoais são tratados, sobre a possibilidade da retirada do consentimento e como exercer esses direitos;
- O tempo em que uma solicitação é respondida;
- O tempo pelo qual aquele dado será tratado, dentro das possibilidades;
- O formato de entrega de cópia ou de portabilidade do dado pessoal, desde que tecnicamente viável.





CANAL DE COMUNICAÇÃO COM OS TITULARES DOS DADOS

Importante!

A NÉRUS se compromete a fornecer cada uma dessas informações no momento da coleta.

Além da Política de Privacidade, a NÉRUS criou um Canal de Comunicação para ser usado pelos Titulares para atendimento das questões relacionadas ao tratamento de seus Dados Pessoais.

Nesse sentido, caso você tenha qualquer assunto relacionado ao Tratamento de Dados Pessoais realizado pela NÉRUS, você pode entrar em contato pelo nosso e-mail:

privacidade@nerus.com.br

CONSCIENTIZAÇÃO E TREINAMENTOS

Por fim, mas não menos importante, a NÉRUS estruturou um Programa de Treinamento Ativo de seus colaboradores, inclusive dos recém-chegados, quanto a importância da Proteção de Dados Pessoais.

O intuito do Programa é qualificar toda a nossa equipe com cursos, treinamentos, palestras e fornecimento de conteúdo, para que estejam cientes das consequências para a NÉRUS em relação aos aspectos legais, às fiscalizações, multas e indenizações, aos danos de reputação e à possibilidade de perda de negócios e oportunidades na hipótese de serem verificados descumprimentos no que tange às determinações da LGPD.

Nesses treinamentos, nossos colaboradores também são conscientizados das consequências disciplinares e de responsabilização na hipótese de não adoção das políticas estabelecidas pela NÉRUS.





MAS AFINAL, QUAL É O PAPEL DO COLABORADOR?

Até aqui já deu para entender que todo colaborador, parceiro, fornecedor e terceiro relacionado a NÉRUS tem uma participação essencial na proteção de dados pessoais. O respeito à privacidade é uma responsabilidade coletiva!

Os colaboradores da NÉRUS, por utilizarem diversos dados pessoais no desempenho de suas funções, devem antes de tudo LER e SE CONSCIENTIZAR de todas as nossas diretrizes acerca da Proteção de Dados Pessoais.

A melhor maneira de ficar por dentro é por meio de nossa Política de Privacidade.

Ah! importante lembrar que é normal ter dúvidas! Mas calma...

Sempre haverá um colega que poderá esclarecer aqueles pontos que não ficarem muito claros para você. Nunca deixe de perguntar.

É claro que só ler e estar informado não é suficiente para garantirmos a proteção dos dados pessoais. É necessário que os nossos colaboradores sejam proativos, de modo a atuar sempre em favor da Privacidade e da Segurança da Informação.



Assim, o papel do Colaborador da NÉRUS na Proteção de Dados Pessoais é amplo, sendo relevante destacar:

A busca de orientações e esclarecimentos com outros colaboradores, quando houver dúvidas relacionadas à Proteção de Dados Pessoais.

O fiel cumprimento de **Política de Privacidade** e demais diretrizes relativas à Proteção de Dados Pessoais.

A proteção dos dados pessoais contra o acesso, modificação, divulgação ou destruição não autorizada pela **NÉRUS**.

A garantia de que os dados pessoais sejam utilizados somente para fins profissionais, notadamente dentro das finalidades para as quais o seu uso fora autorizado pelos Titulares.

A comunicação imediata a outros colaboradores – principalmente àqueles hierarquicamente superiores na estrutura organizacional da **NÉRUS** – acerca de qualquer descumprimento ou violação das diretrizes de Proteção de Dados Pessoais.

Com intuito de orientar os usuários de nossos sistemas, a Nérus criou esta mini cartilha que ressalta os principais pontos de atenção que o cliente deve ter em relação a segurança da informação para melhorar a rastreabilidade, integridade e confidencialidade dos dados que trafegam em nossos sistemas.

MELHORES PRÁTICAS DE INFRAESTRUTURA

- Fazer acesso exclusivamente via VPN

A utilização da VPN garante que todo acesso seja realizado apenas por aqueles que possuem uma chave de acesso disponibilizada para esse fim, ou seja, não basta ter os dados de acesso como IP, usuário e senha, adicionando assim mais uma camada de segurança nesses acessos. Além disso, inibe que dados sejam capturados por terceiros durante o tráfego das informações (criptografia in transit).



- Fechar portas de acesso externo aos servidores.

Não permitir acessos externos liberados para a internet, pois essa prática evita ataques de DDOS (Sobrecarga) ou Força Bruta (Quebra de senhas) aos servidores.

- Disponibilizar chave de acesso individualizada.

Para fins de rastreabilidade, é importante que a chave de acesso dos colaboradores internos e ou externos sejam individualizadas. Dessa forma pode-se ter um controle maior de quando um colaborador ou prestador acessou uma base e o que foi realizado por ele.

- Definir senhas fortes

Utilizar senhas longas, com números, letras, maiúsculas e minúsculas e caracteres especiais.

PROMOVER TROCAS DE SENHAS PERIÓDICAS (MÁXIMO DE 6 EM 6 MESES)

- Ativar os logs do banco de dados e guardá-los de acordo com a política de segurança da empresa.

Com isso garante-se a rastreabilidade completa de tudo o que foi incluído, modificado ou retirado no repositório de informações do sistema

- Manter bases de produção e teste em ambientes totalmente separados.

Ao manter as bases de teste em um ambiente separado do de produção, pode-se garantir que os acessos realizados por terceiros (como a Nérus) sejam realizados apenas nesse ambiente controlado (de teste) e nunca nos dados sensíveis da produção.



MELHORES PRÁTICAS DO NÉRUS:

- Disponibilizar senhas individuais tanto para colaboradores internos e ou externos (prestadores de serviços)

Para fins de rastreabilidade, é importante que os acessos dos colaboradores internos e externos sejam feitos por logins distintos. Dessa forma pode-se ter um controle maior do que cada usuário fez no sistema.

- Definir senhas fortes

Utilizar senhas longas, com números, letras, maiúsculas e minúsculas e caracteres especiais.



MELHORES NÉRUS:

PRÁTICAS DO

- Promover trocas de senhas periódicas.
- Ativar parâmetros para inclusão de novos usuários entrarem bloqueados.
- Ativar parâmetros para gerar logs do sistema.
- Monitoramento constante dos usuários masters
- O privilégio de usuário master (ADM) deve ser mais controlado e restrito que o de um usuário normal, visto que ele tem o domínio total do sistema e inclusive o controle aos outros usuários. Portanto, o monitoramento e controle deve ser mais cauteloso.

E PARA O FORNECEDOR, A SITUAÇÃO É DIFERENTE?



Nesse sentido, Fornecedores e Terceiros que se relacionam com a NÉRUS também possuem um papel fundamental na Proteção de Dados Pessoais, cumprindo a eles:

O esforço no estabelecimento e manutenção da comunicação ativa sobre a gestão dos dados e informações transmitidas pela NÉRUS.

A observância da **Política de Privacidade** e demais diretrizes relativas à Proteção de Dados Pessoais.

A garantia de que seus colaboradores, consultores e parceiros ajam em harmonia com a Proteção de Dados Pessoais, notadamente com as diretrizes estabelecidas pela NÉRUS.

A devolução ou destruição dos dados pessoais tratados – a depender do caso concreto, quando do fim da relação comercial estabelecida com a NÉRUS.

A comunicação imediata à NÉRUS acerca de qualquer descumprimento ou violação das diretrizes de Proteção de Dados Pessoais.

**MUITO
OBRIGADO
PELA
LEITURA!**

CONTAMOS COM O SEU MÁXIMO EMPENHO PARA QUE A NÉRUS SEJA SEMPRE RECONHECIDO COMO UMA EMPRESA QUE RESPEITA, PROFUNDAMENTE, A PRIVACIDADE DOS DADOS PESSOAIS!

EM CASO DE DÚVIDAS, CONSIDERE ENTRAR EM CONTATO POR MEIO DE NOSSOS SERVIÇOS DE ATENDIMENTO

<https://nerus.com.br/fale-conosco/>

MELO CAMPOS
ADVOGADOS
— 97ANOS —

 **NÉRUS**