# CARTILHA DE BOAS PRÁTICAS DO SERVIDOR PÚBLICO

## LEI GERAL DE PROTEÇÃO DE DADOS

**Aqui você está protegido!**


Olá, eu sou o Transparício, o gestor mais querido do Brasil, e te convido a correr comigo rumo a uma gestão nota 10!
81
79
16


**28°– LEI GERAL DE PROTEÇÃO DE DADOS**

Em âmbito nacional, já está vigente a LEI GERAL DE PROTEÇÃO DE DADOS nº. 13709/18, que dispõe sobre o tratamento e dados, regulando e limitando o uso de informações pessoais, com intuito de proteger direitos fundamentais de liberdade e privacidade dos cidadãos. Com vigência escalonada desde 2018, essa lei trouxe inúmeras implicações, inclusive sanções administrativas que precisam ser observadas com cuidado.

**27° – PODER PÚBLICO COLETA E ARMAZENA DADOS PESSOAIS E SENSÍVEIS**

A maior coleta de dados é realizada pelo PODER PÚBLICO, são armazenadas informações pessoais diariamente e, por esse motivo, torna-se responsável pela sua utilização, compartilhamento e armazenamento. Deve ser assegurado ao titular de dados a proteção e privacidade deles, bem como é obrigatório manter a transparência sobre a finalidade e o uso das informações.

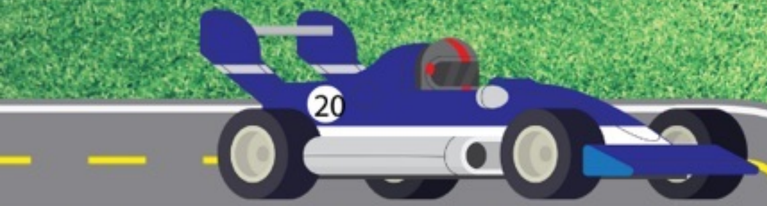

**26° - DESAFIOS LGPD**

A adequação à LGPD exige providências profundas em conformidade e transformação no poder público e, com toda certeza, são nas atitudes do dia a dia que vamos aperfeiçoando a compreensão e replicação das boas práticas que a lei inova. Pode-se dizer que o maior desafio é na MUDANÇA CULTURAL, para que a disseminação destas boas práticas aconteça de forma rápida e permanente.

**25° – ABRANGÊNCIA**

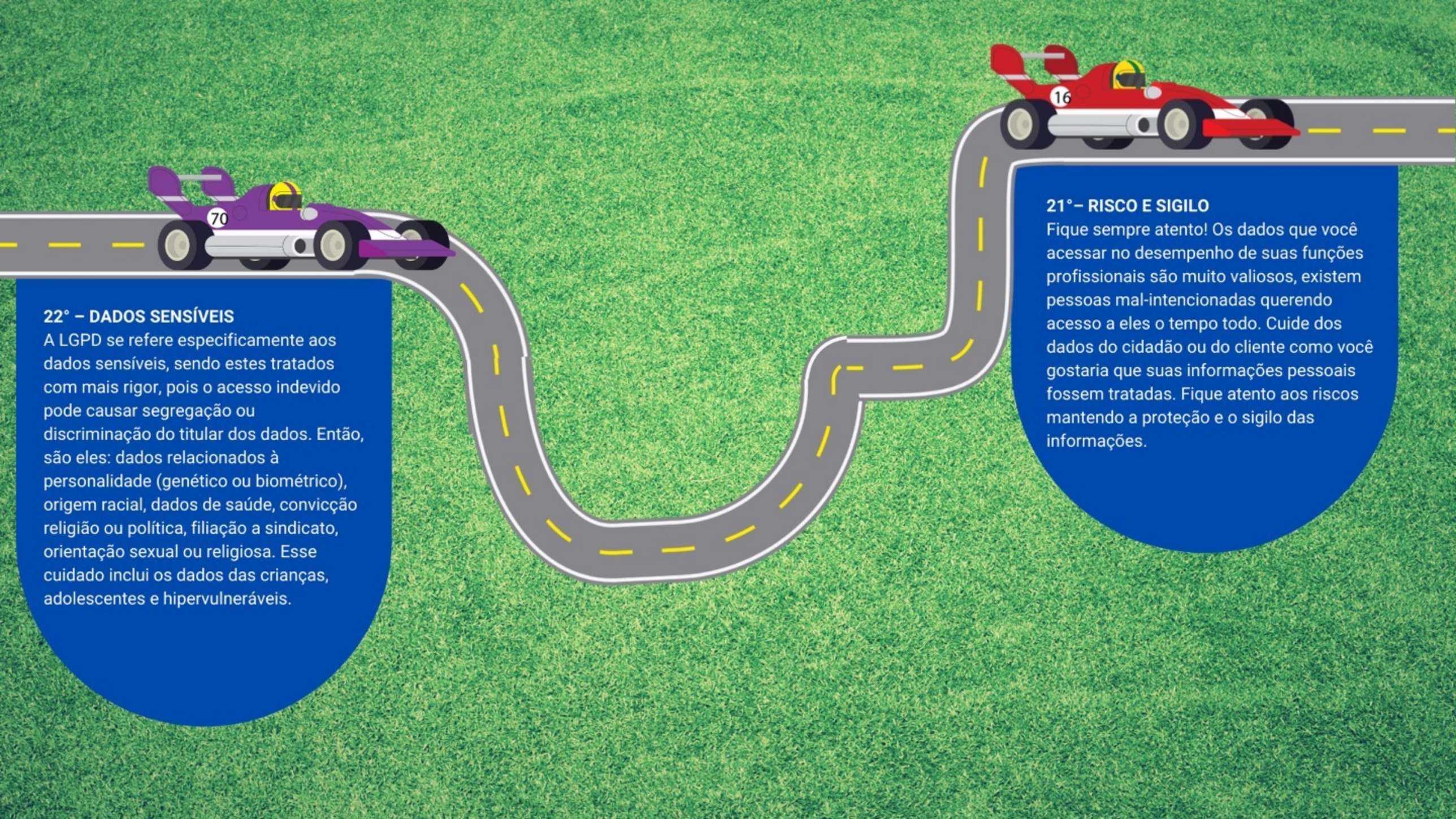
Tanto a pessoa jurídica de direito público, como a pessoa jurídica de direito privado, startups, pequenas, médias e grandes empresas devem se adequar, variando apenas o nível de exigência. Mas, em todas as situações, a lei protege quaisquer tipos de dados pessoais: (nome, endereço, números de documentos, hábitos pessoais, dados de saúde, dados laborais, menores e idosos), documentos físicos, virtuais, imagem, som e/ou biometria.

**24°- ANPD**
Autoridade Nacional de Proteção de Dados – ANPD é o órgão diretamente ligado à presidência da república que possui atribuições relacionadas à proteção e privacidade de dados pessoais e, principalmente, promover a fiscalização, apuração e aplicar sanções e penalidades pecuniárias em caso de crise de dados ocorridas no Brasil.





**23°- TRATAMENTO DE DADOS**
Toda a cadeia de tratamento de dados pessoais é protegida por lei, desde a coleta, processamento, armazenamento, compartilhamento e descarte. Durante esse processo, é importante exigir de seus fornecedores ou parceiros que também se mantenham adequados à lei, para evitar crises de dados. O cuidado abrange produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração e eliminação.

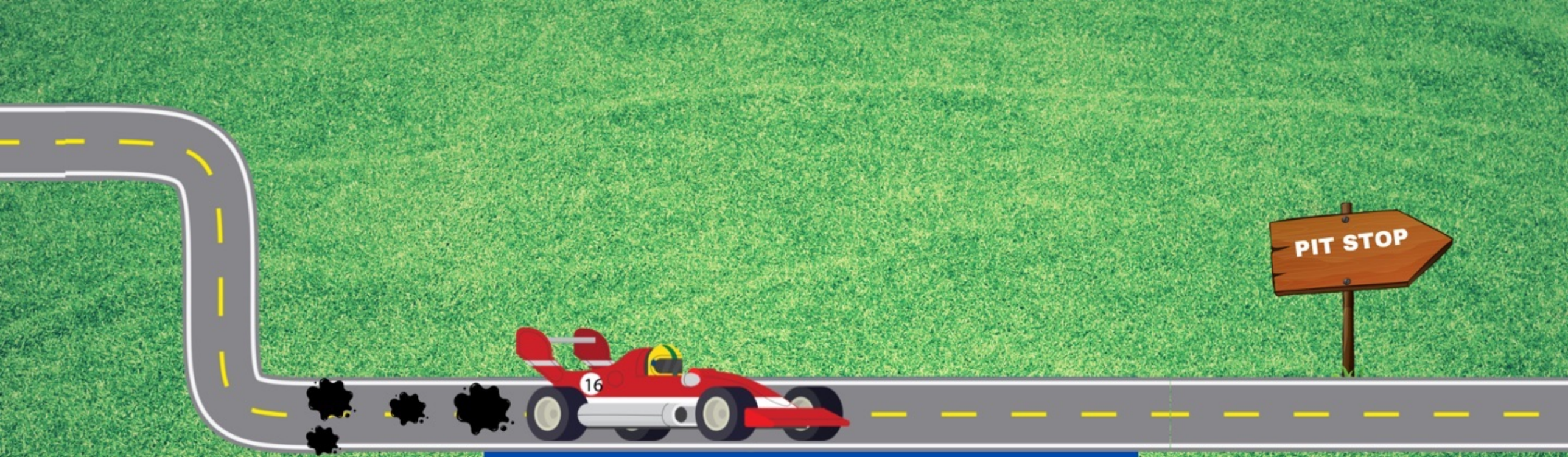



**22° – DADOS SENSÍVEIS**

A LGPD se refere especificamente aos dados sensíveis, sendo estes tratados com mais rigor, pois o acesso indevido pode causar segregação ou discriminação do titular dos dados. Então, são eles: dados relacionados à personalidade (genético ou biométrico), origem racial, dados de saúde, convicção religião ou política, filiação a sindicato, orientação sexual ou religiosa. Esse cuidado inclui os dados das crianças, adolescentes e hipervulneráveis.

**21°– RISCO E SIGILO**

Fique sempre atento! Os dados que você acessar no desempenho de suas funções profissionais são muito valiosos, existem pessoas mal-intencionadas querendo acesso a eles o tempo todo. Cuide dos dados do cidadão ou do cliente como você gostaria que suas informações pessoais fossem tratadas. Fique atento aos riscos mantendo a proteção e o sigilo das informações.

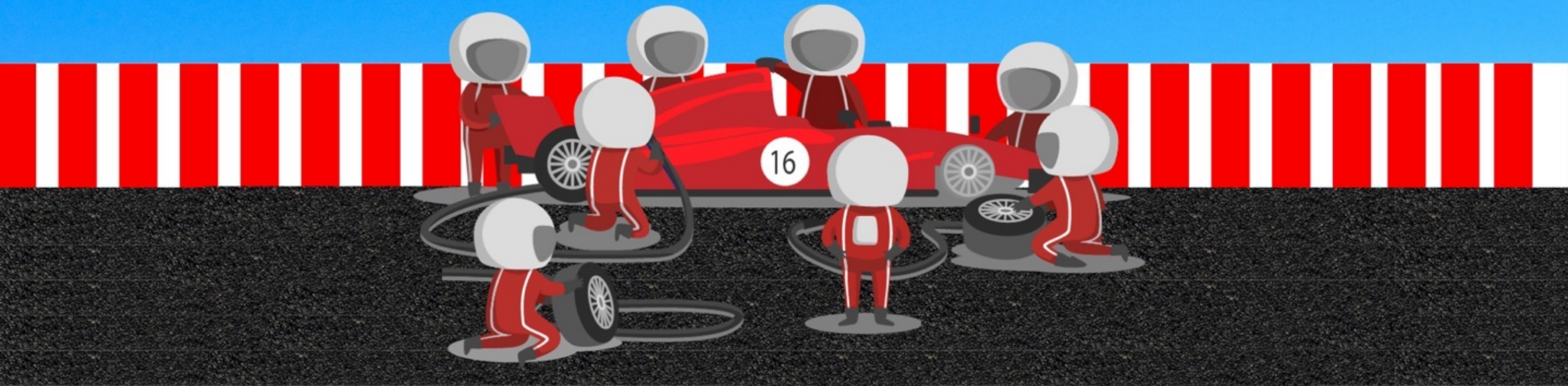



**20°- VAZAMENTO DOS DADOS PESSOAIS**

Já ficou claro que é possível ocorrer vazamento de dados pessoais, não é? Assim, devemos lembrar que o cuidado deve ser constante para evitar acessos não autorizados, coletas excessivas, dados repassados para terceiros ou divulgados na internet de forma indevida. Por esse motivo é tão fundamental aplicar as recomendações das políticas de privacidade e segurança que foram criadas para você e sua equipe, no módulo preteção de dados.

# Volta 2

## COMO EVITAR VAZAMENTOS?



**19° – SENHAS FORTES**

Reforçar as senhas de acesso as contas dos usuários com números, letras e símbolos, ter um gerenciador de senhas no sistema com prazo de validade pré-definido e, em hipótese nenhuma, repassar sua senha para terceiros ou guardar o número em local de fácil acesso. Todas as senhas que criamos são pessoais e intransferíveis.

Outra informação importante é que NÃO devemos repetir senhas, colocar datas comemorativas ou sequencia padrão, ex. 123456. Assim, evita-se o vazamento e acessos não autorizados pela obviedade numérica.


**18° – DESCARTE DE DOCUMENTOS E MÍDIAS**

Ao descartar documentos e mídias (pen drive e discos) que contenham dados pessoais, tome o devido cuidado para torná-los imprestáveis para terceiros. Sempre que possível utilize o triturador, esses equipamentos são acessíveis e de fácil utilização. Já em relação aos dados armazenados, você pode sobrescrever discos, restaurar opções de fábrica ou destruir fisicamente o hardware. Também é interessante utilizar métodos de evidência, por meio de protocolos numéricos e/ou e-mails de aviso automáticos para que o titular de dados saiba que o descarte foi realizado, informe-se dos procedimentos adotados pelo setor de tecnologia ou através do Encarregado/DPO.

**17° - EVITE ACESSAR**

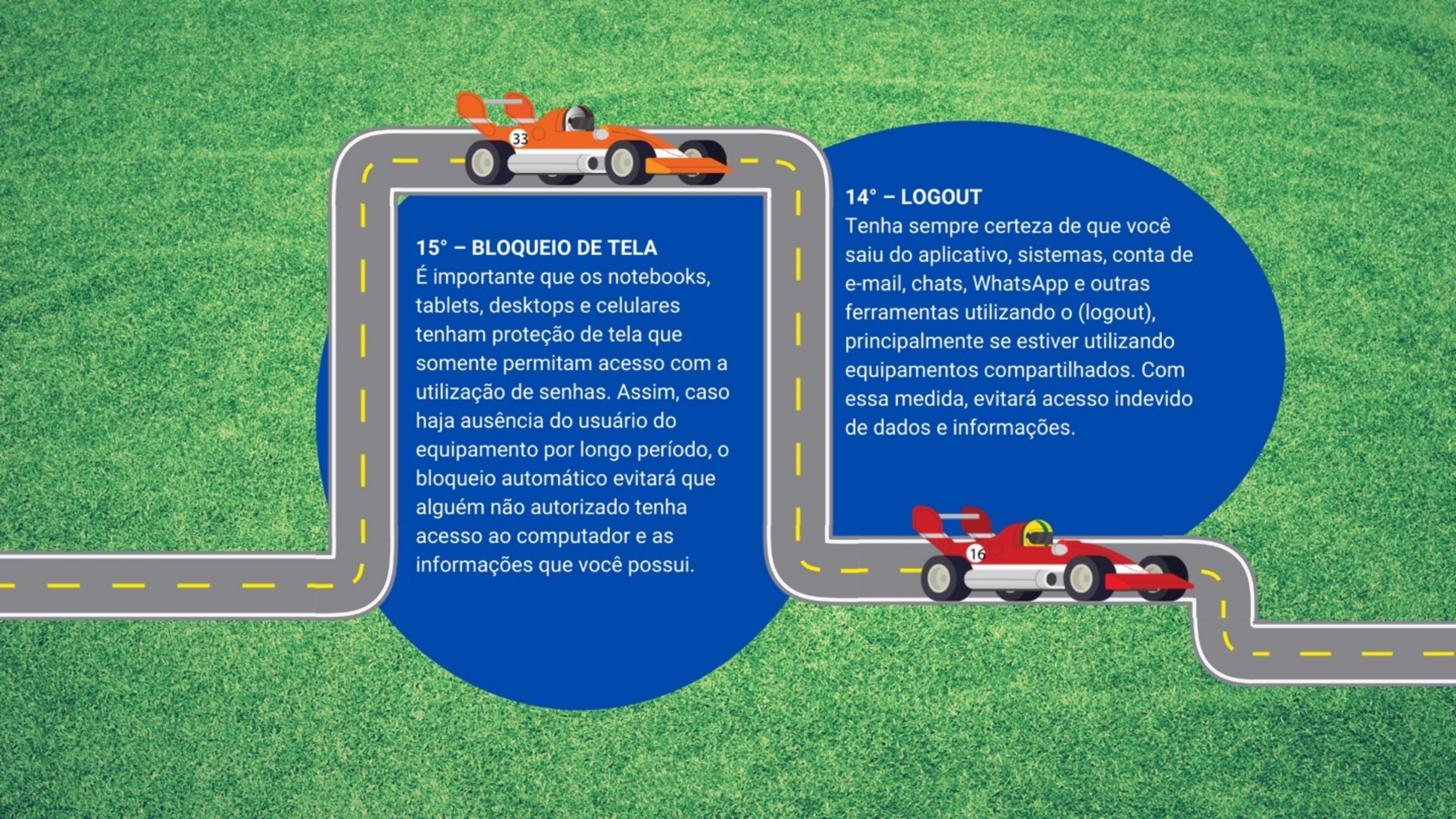
Muito cuidado quando resolver acessar sites, abrir arquivos, clicar em imagens que você não tenha certeza de sua procedência e originalidade. Mesmo que o texto enviado remeta a uma situação de urgência ou comoção. Em caso de dúvidas, contate imediatamente sua chefia direta ou o setor de tecnologia da organização envolvida e busque maiores informações.



**16° - VERIFICAÇAO DE TELAS E LINKS DE ACESSO**

Antes de se logar no e-mail institucional, portal, servidor, imprimir aquele boleto para efetuar um pagamento ou aceitar aquela promoção relâmpago, verifique as telas, os endereços eletrônicos, os links e demais informações do local de acesso.

Existem inúmeros dispositivos e armadilhas que são enviados pela internet para bloquear computadores, invadir sistemas, sequestrar senhas e informações para golpes, desvios de dinheiro ou pedidos de resgate.




**15° – BLOQUEIO DE TELA**

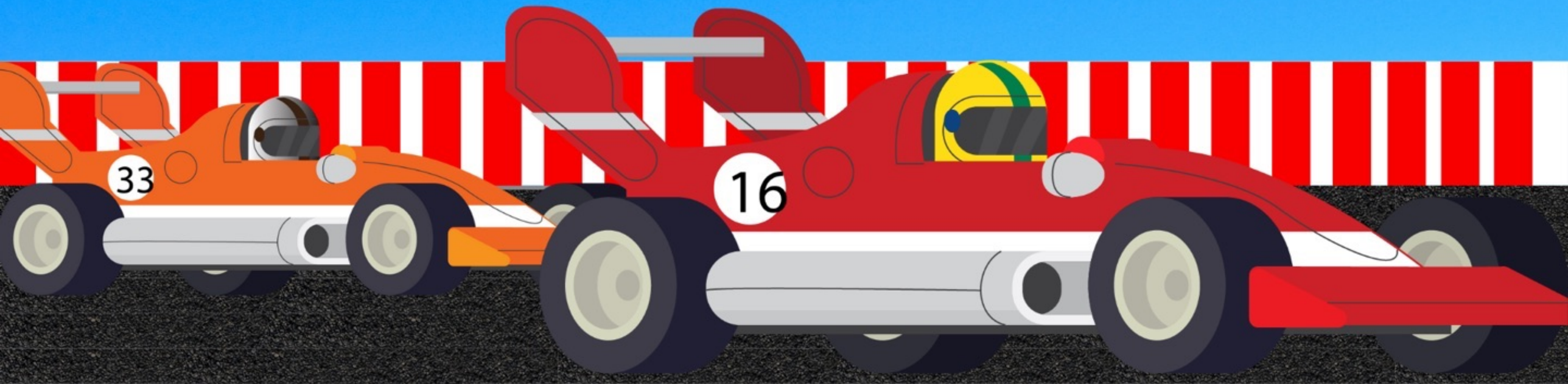
É importante que os notebooks, tablets, desktops e celulares tenham proteção de tela que somente permitam acesso com a utilização de senhas. Assim, caso haja ausência do usuário do equipamento por longo período, o bloqueio automático evitará que alguém não autorizado tenha acesso ao computador e as informações que você possui.

**14° – LOGOUT**

Tenha sempre certeza de que você saiu do aplicativo, sistemas, conta de e-mail, chats, WhatsApp e outras ferramentas utilizando o (logout), principalmente se estiver utilizando equipamentos compartilhados. Com essa medida, evitará acesso indevido de dados e informações.

# Volta 3

# O DIA A DIA NO TRATAMENTO DE DADOS PESSOAIS.



**13° – REAL NECESSIDADE**

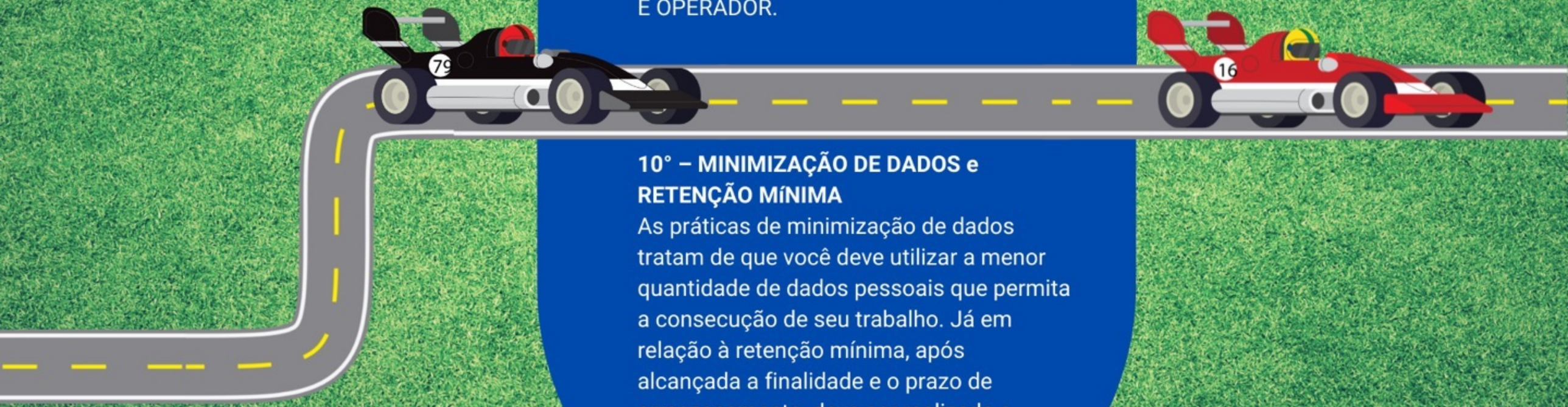
Ao solicitar os dados de alguém, questione-se sobre a real necessidade de coletá-los para aquilo que se pretende, e se legalmente você está amparado para tratar aquela informação. Cso entenda que não pode coletar, pois são indevidos ou não há necessidade, converse com sua chefia direta e esclareça a dúvida. Faça sugestões, elas são importantes para a evolução das boas práticas.

**12° – PRINCÍPIO DA FINALIDADE**

Os dados pessoais coletados deverão ser utilizados apenas paras as finalidades específicas ou estritamente similares para as quais foram coletadas e devidamente informadas aos titulares.

**11° – BASE LEGAL**

Todo fluxo de tratamento de dados pessoais e dados pessoais sensíveis tem uma base legal que justifique, este item está literalmente previsto na lei, e deve ser muito bem observado pelo CONTROLADOR E OPERADOR.




**10° – MINIMIZAÇÃO DE DADOS e RETENÇÃO MíNIMA**

As práticas de minimização de dados tratam de que você deve utilizar a menor quantidade de dados pessoais que permita a consecução de seu trabalho. Já em relação à retenção mínima, após alcançada a finalidade e o prazo de armazenamento, deve ser realizada a menor retenção possível de dados ou a imediata exclusão destas informações.


**9° – COMPARTILHAMENTO DE DADOS**

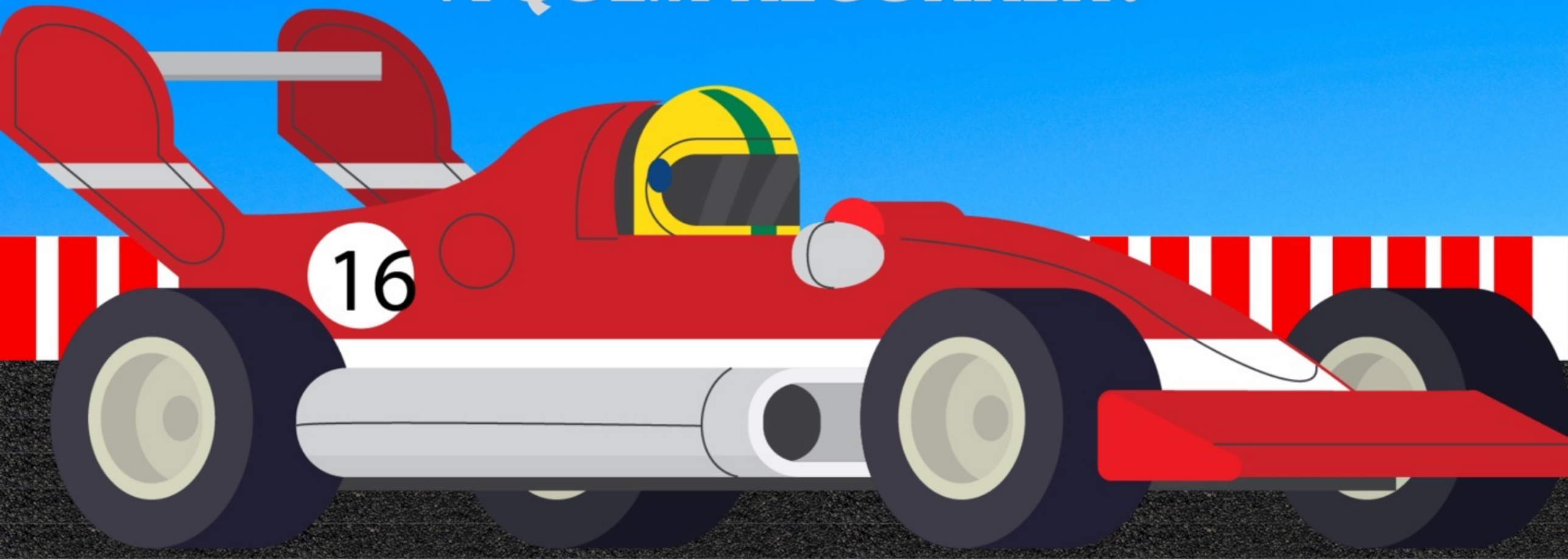
Muitas vezes o PODER PÚBLICO ao utilizar dados pessoais, necessita compartilhá-los com terceiros que fazem parte da cadeia de tratamento de dados e estejam legalmente autorizados para acessá-los, ex.: cumprimento de contrato, cumprimento de obrigação legal ou regulatória, execução de políticas públicas. Importante lembrar que os demais CO-CONTROLADORES ou OPERADORES devem estar adequados a LGPD.

**8° – INFORMAÇÕES CONFIDENCIAIS/ PRIVADAS**

Caso você tenha acesso às informações confidenciais em sua secretaria ou órgão, é obrigação legal e profissional que seja mantido segredo sobre elas. No tocante as informações privadas de colegas, familiares e outros titulares de dados sem relação direta ao trabalho desenvolvido, você não deve comentar ou divulgar, pois isso pode colocar em risco a segurança destas pessoas.

# Volta 4

## A QUEM RECORRER?

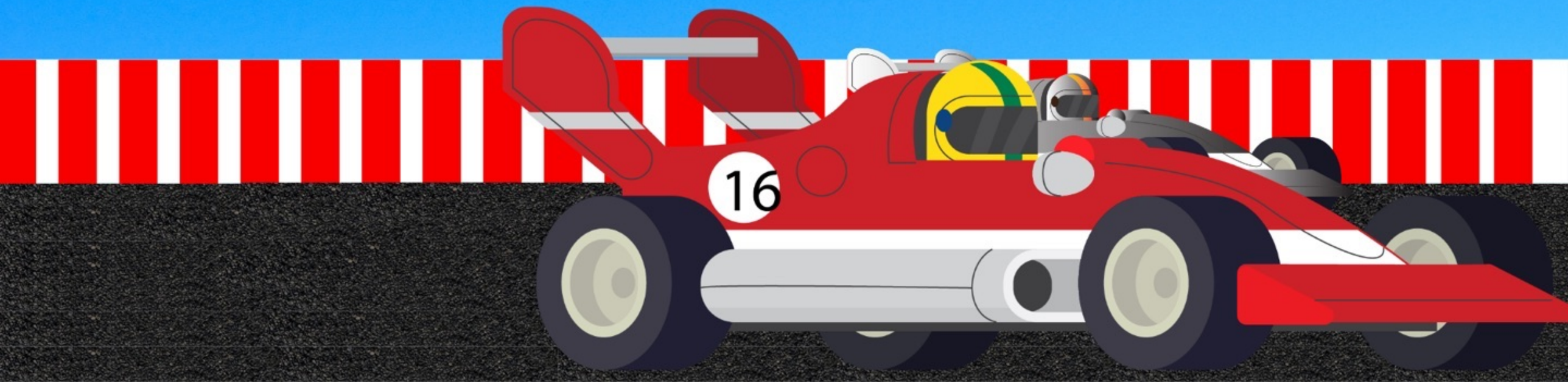


**7° – ENCARREGADO ou DPO (data protection officer)**
Este profissional pode ser uma pessoa física ou até uma pessoa jurídica com vasto conhecimento sobre a LGPD, POLÍTICAS DE PRIVACIDADE, POLÍTICAS DE SEGURANÇA. Além disso, o encarregado (DPO) é pessoa responsável por atuar como canal de comunicação entre a ANPD, TITULAR DE DADOS E CONTROLADOR.
Nossa gestão te oferece um encarregado (link para acesso), esta pessoa é referência também para ser contatada em casos de incidente de segurança com dados pessoais, sugestões de melhorias e orientações sobre proteção de dados.

**6° – EMAIL INVADIDO/SENHA CORROMPIDA**
Em caso de e-mail invadido, evite se logar durante a invasão e procure imediatamente ajuda ao setor de tecnologia.
Em caso de problemas com sua senha de acesso, procure imediatamente ajuda ao setor de tecnologia.

# Volta 5

## COMO ESTAMOS NOS ADEQUANDO?



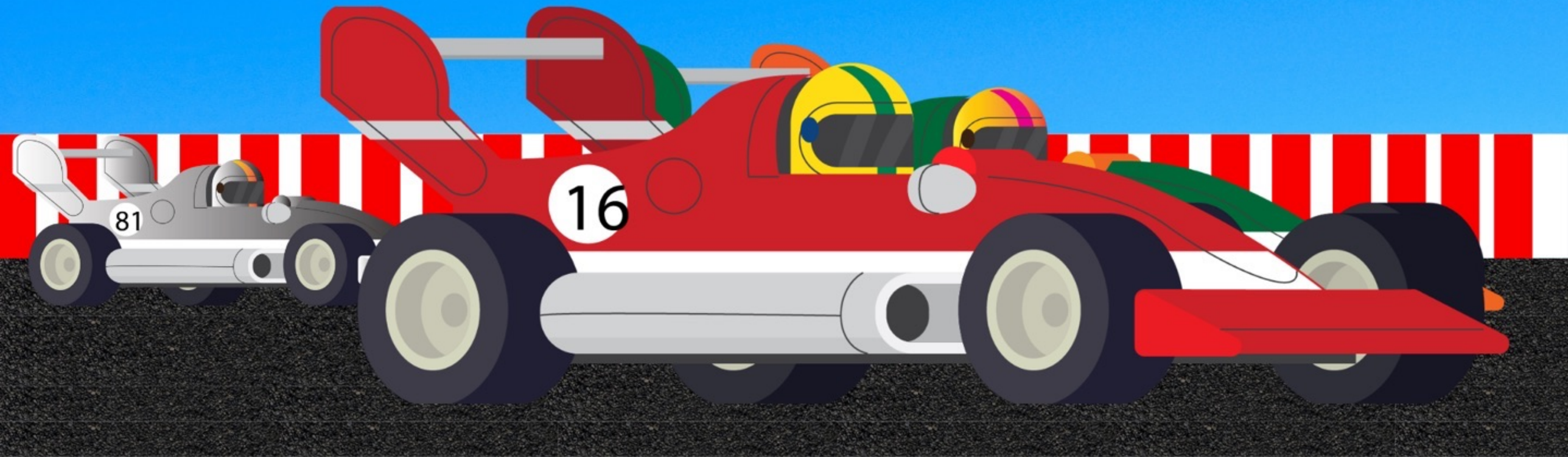
**5° – DECRETOS/PORTARIAS**
Além da designação do encarregado (DPO), foi designado um comitê de segurança e proteção de dados para dar o suporte necessário às demandas internas setoriais deste orgão público, por meio de decretos/portarias.

**4° - COMITÊ DE SEGURANÇA E PROTEÇÃO DE DADOS**
Esse grupo engloba um servidor de cada secretaria que fica responsável em fomentar as políticas e replicar as boas práticas, bem como auxiliar as medidas implementadas pelo encarregado e o setor de tecnologia em caso de crises de dados pessoais.

**3° – NOSSO SITE**
Fique atento ao nosso site, nele divulgamos os trabalhos sobre proteção de dados pessoais, legislação específica, materiais informativos que vão nos ajudar nesta jornada de aprendizado.

# Volta Final

## ATENÇÃO REDOBRADA.



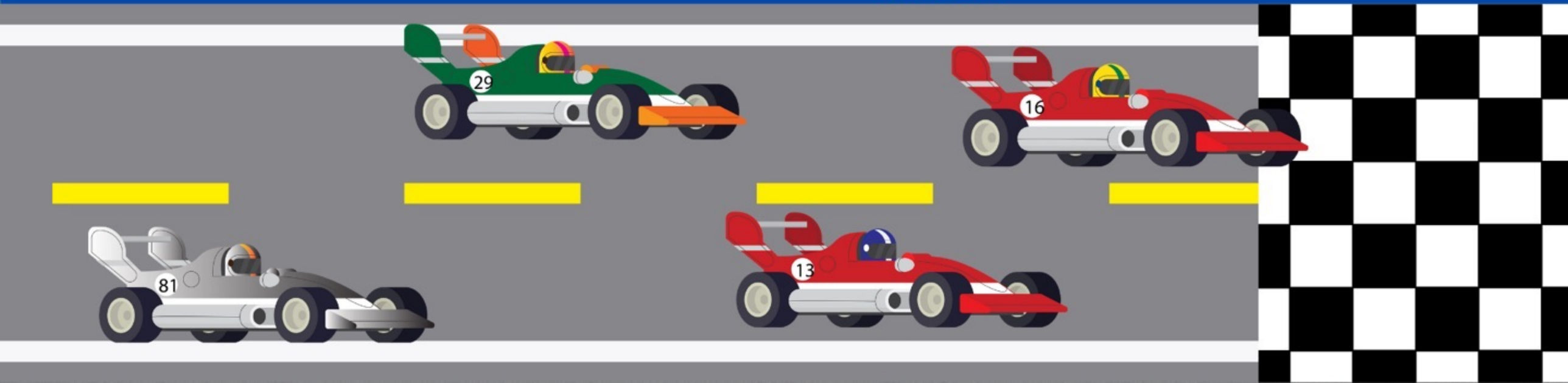
## 2°-AMEAÇAS

Tenha muito cuidado com seus acessos, pois, DIARIAMENTE, recebemos ameaças de invasão, capturas de senhas e sequestro de dados em nossos sistemas e WEBMAIL.

Nossa segurança também é sua!

## 1°- PROTEÇÃO DE DADOS PESSOAIS

A tarefa de proteger informações pessoais do cidadão é dever de todo servidor público, evite situações que podem comprometer a segurança de dados.




Parabéns, campeão!
Te vejo numa próxima
aventura.
Gestão Nota 10
16

máxima
tecnologia

**Desenvolvido por:**
**Máxima Tecnologia LTDA**
**Consultoria LGPD: Sandra V.M.Fernandes (83) 988560855**
**Certificação - Exin Foundation**

Versão 01/2022



**2022**