

# Código de Conduta

**GAVIS**

# Índice

|       |                                                                                  |    |
|-------|----------------------------------------------------------------------------------|----|
| 1.    | A Gavis precisa de um código de conduta porquê?.....                             | 3  |
| 2.    | A quem se aplica?.....                                                           | 4  |
| 3.    | Princípios Fundamentais .....                                                    | 5  |
| 3.1.  | Saúde e segurança no trabalho .....                                              | 5  |
| 3.2.  | Prevenção do assédio, respeito e igualdade de oportunidades .....                | 5  |
| 3.3.  | Gestão e controlo de ativos .....                                                | 6  |
| 3.4.  | Gestão de informação, confidencialidade e proteção de dados.....                 | 7  |
| 3.5.  | Proteção do meio ambiente e transição energética .....                           | 7  |
| 3.6.  | Direitos Humanos .....                                                           | 8  |
| 3.7.  | Controlo, governança e conformidade nas nossas atividades.....                   | 8  |
| 3.8.  | Luta contra o suborno e a corrupção .....                                        | 9  |
| 3.9.  | Luta contra o branqueamento de capitais e o financiamento do terrorismo .....    | 9  |
| 3.10. | Conflitos de interesses .....                                                    | 10 |
| 3.11. | Relações com governo, administrações públicas e sindicatos.....                  | 10 |
| 3.12. | Relações com parceiros de negócio, fornecedores, clientes e outros grupos.....   | 10 |
| 3.13. | Meios de comunicação e transparência informativa .....                           | 11 |
| 4.    | O que fazemos em caso de indícios de incumprimento ou possível má conduta? ..... | 12 |
| 5.    | Atualização, Aceitação e Aprovação .....                                         | 13 |
|       | Anexo I – Código de Conduta para prevenção e combate ao assédio no trabalho..... | 14 |
|       | Introdução.....                                                                  | 16 |
| 1.    | Princípios gerais de conduta .....                                               | 17 |
|       | Anexo II – A Segurança da Informação.....                                        | 20 |
|       | Introdução.....                                                                  | 22 |
| 1.    | Princípios gerais de segurança da informação.....                                | 23 |
| 2.    | As passwords e o acesso à informação.....                                        | 24 |
| 3.    | Posto de trabalho e salas de reuniões .....                                      | 25 |
| 4.    | O Correio eletrónico e NetEtiqueta.....                                          | 26 |
| 4.1.  | Boas práticas de utilização do e-mail .....                                      | 26 |
| 4.2.  | NetEtiqueta .....                                                                | 26 |
| 5.    | Phishing, virus e ransomware .....                                               | 27 |
| 6.    | A Internet e a Comunicação.....                                                  | 28 |

|     |                                                      |    |
|-----|------------------------------------------------------|----|
| 7.  | Dispositivos móveis .....                            | 30 |
| 8.  | Parceiros Externos .....                             | 31 |
| 9.  | GDPR .....                                           | 33 |
| 10. | Destruição de dados e impressões.....                | 35 |
| 11. | Segurança de pagamentos eletrónicos .....            | 36 |
| 12. | Dez Mandamentos de Segurança .....                   | 37 |
|     | Anexo III – Declaração de Privacidade de Dados ..... | 38 |

# 1. A Gavis precisa de um código de conduta porquê?

Como empresa familiar com uma tradição de 50 anos de atividade, orgulhamo-nos de estar posicionados como uma referência do setor nas marcas que representamos. Como tal, temos uma forte responsabilidade social - para com os nossos colaboradores, clientes, fornecedores e público em geral - que queremos cumprir. Esta responsabilidade inclui o cumprimento das leis aplicáveis, respeitando os valores éticos fundamentais e está baseada nas nossas ações em torno de 13 princípios fundamentais.

Este não é apenas um dever da administração, mas sim de todos os colaboradores da empresa. Todos devem conhecer as suas responsabilidades e agir diariamente em conformidade.



## 2. A quem se aplica?

O Código de Conduta norteia as nossas ações, aplicando-se a todas as pessoas dentro da empresa: titulares de órgãos sociais, Diretores, todos os Colaboradores, Consultores e Colaboradores externos, apoiando-os a lidar com os desafios do seu dia a dia.

É responsabilidade da administração garantir que os princípios do Código sejam comunicados e compreendidos por todos. Isso significa que todos respeitam e cumprem as regras em vigor na Empresa, a qualquer momento e em qualquer local, com respeito, confiança e solidariedade.



## 3. Princípios Fundamentais

### 3.1. Saúde e segurança no trabalho

Todas as nossas operações, instalações e equipamentos estão de acordo com as disposições legais aplicáveis. A segurança no local de trabalho serve para prevenir acidentes de trabalho, doenças e riscos para a saúde relacionados com o trabalho, de acordo com as seguintes normas:

- Assegurar que os colaboradores são devidamente informados, capacitados e sensibilizados em matéria de segurança;
- Manter os nossos locais de trabalho sem álcool nem drogas. O consumo de álcool e o uso, posse ou distribuição de substâncias ilegais é proibido, podendo ser realizada prova em caso de suspeição;
- Participar de forma ativa em todas as atividades de formação que sejam exigíveis;
- Cuidar da segurança e saúde das pessoas com que se relaciona em todas as atividades que desenvolva e demonstrar a diligência suficiente quando trata de aspetos de segurança e saúde, incorporando os equipamentos de proteção individual exigidos;
- Reconhecer, antecipar e avaliar os riscos relativos à segurança e saúde no trabalho antes de tomar qualquer decisão e adotar as medidas necessárias para evitá-los.

### 3.2. Prevenção do assédio, respeito e igualdade de oportunidades

Respeitamos os respetivos requisitos legais nacionais sobre os direitos laborais, juntamente com todas as suas provisões, e apoiamos a sua aplicação na nossa organização.

Por esta razão cumprimos com os fundamentos dos direitos de proteção dos Colaboradores, cujos princípios são expressos nas convenções internacionais das Nações Unidas (ONU), nomeadamente:

- Trabalhar ainda mais pela igualdade de oportunidades, fomentando a diversidade sem discriminar ninguém na hora de contratar, promover ou remunerar os nossos colaboradores;
- Condenar qualquer forma de assédio ou abuso físico, sexual, psicológico ou verbal entre os colaboradores, assim como qualquer conduta que gere um ambiente de trabalho intimidatório, ofensivo, humilhante ou hostil;
- Fomentar o emprego digno, respeitando o direito das pessoas de não serem vítimas de trabalho forçado, e rejeitar qualquer forma de exploração laboral na nossa empresa ou nos nossos parceiros, fornecedores, clientes;
- Tratar as pessoas com quem nos relacionamos com respeito, dignidade e profissionalismo, sem ameaças, humilhação ou discriminação usando palavras, ou ações sugestivas, ou depreciativas, adaptando o seu comportamento às culturas locais.

Em caso de eventual situação de assédio, deve averiguar o ocorrido, tendo sempre presente o interesse de todas as partes em agir com a discrição necessária para proteger a dignidade e a privacidade de cada um;

- A não divulgação de qualquer informação a outras partes não envolvidas no incidente;
- As queixas devem ser investigadas e tratadas com celeridade;
- Todas as partes envolvidas devem ser ouvidas de forma imparcial e beneficiar de um tratamento equitativo;
- As queixas devem ser sustentadas com base em informações detalhadas;
- Não serão toleradas acusações falsas e os seus autores poderão ser alvo de processos disciplinares;
- Caso seja provada a ocorrência de assédio, serão tomadas medidas adequadas contra o(s) que o tenha(m) levado a cabo, as quais poderão compreender sanções disciplinares aí se incluindo o despedimento.

### 3.3. Gestão e controlo de ativos

Os ativos da Empresa são compostos por todos os recursos materiais e as propriedades intangíveis como a imagem, a reputação, a informação, as ideias patenteadas e não patenteadas, as instalações ou os programas e sistemas informáticos, entre outros.

Comprometemo-nos a colocar à disposição dos nossos colaboradores, os recursos e os meios necessários e adequados para o desenvolvimento da sua atividade profissional. Estes recursos devem ser usados de forma diligente e responsável, sem benefícios pessoais, protegendo-os e assegurando a sua conservação.

Realizar um uso responsável da marca GAVIS e não fazer uso dela em comunicações privadas ou não relacionadas com a atualidade real da Empresa.

O exercício da atividade deve ser eficiente, com o uso dos recursos disponíveis, evitando desperdícios e minimizando os custos.

Não participar, influenciar ou permitir situações ou ações que estejam ligadas ao roubo, furto, utilização incorreta, fraude, destruição, empréstimo, venda ou disposição de ativos de forma não autorizada.

Ser cuidadoso e não partilhar o seu cartão de acesso às instalações, nem as palavras-passe de acesso aos sistemas.

Os titulares de órgãos sociais e os colaboradores não devem usar informação privilegiada da empresa que com ela estejam em relação de domínio, em proveito próprio ou de terceiros, independentemente da expressão que tal vantagem assuma.

Remete-se para a leitura do Anexo I.

### 3.4. Gestão de informação, confidencialidade e proteção de dados

Adotamos os meios e ferramentas de segurança pertinentes e legalmente adequados para proteger a informação frente a qualquer risco interno ou externo de acesso não consentido.

As tecnologias da informação e sistemas de informação da Gavis (incluindo computadores, portáteis, hardware e software, tais como e-mail, internet, etc.) continuam a todo o momento a ser propriedade da empresa e devem ser usados apenas para fins de trabalho. O uso da tecnologia e sistemas de informação da Gavis deve ser para fins comerciais legítimos, de acordo com a política individual da empresa. Os sistemas não podem ser utilizados de forma ilegal, ofensiva, perturbadora ou prejudicial a outras pessoas. A aquisição de um software ilegalmente copiado nunca poderá ser feita ou utilizada, pois isso poderia expor o colaborador e a empresa a uma ação judicial.

A informação que não seja necessária será eliminada atendendo aos requerimentos do regulamento vigente sobre proteção de dados. A informação da Gavis e de terceiros que figure como classificada sem as autorizações pertinentes, não deve ser divulgada.

Para proteger a vida privada dos colaboradores, dos clientes e fornecedores, aderimos aos requisitos legais aplicáveis em relação ao tratamento de dados pessoais. Para fazer isso tomamos precauções técnicas de segurança para proteger a informação de acesso não autorizado.

Garantimos a proteção e o uso apropriado dos dados de carácter pessoal, tanto dos colaboradores como os dos nossos grupos de interesse, cumprindo com o regulamento que lhe seja aplicado.

A partir de 25 de maio de 2018 passou a ser aplicável o Regulamento Geral sobre a Proteção de Dados Pessoais - Regulamento n° 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que estabelece as regras relativas à proteção, tratamento e livre circulação dos dados pessoais das pessoas singulares e que se aplica diretamente a todas as entidades que procedam ao tratamento desses dados, em qualquer Estado membro da União Europeia, nomeadamente Portugal e que a Gavis utiliza.

Remete-se para a leitura do Anexo II e III.

### 3.5. Proteção do meio ambiente e transição energética

A sustentabilidade é uma parte importante da filosofia da nossa empresa. Por esta razão comprometemo-nos com o objetivo do zelo pela proteção ambiental sustentável, tanto para a geração atual como para as gerações futuras. Com isso em mente, a proteção ambiental abrangente é um objetivo igualmente importante para salvaguardarmos o futuro da empresa e a força de trabalho como a elevada qualidade dos nossos produtos e a nossa saúde e segurança no trabalho.

Vemos a necessidade de evitar riscos para o meio ambiente e conservar recursos como uma questão de honra.

Mitigar as emissões de CO2 associadas às atividades da empresa, seja nas suas instalações produtivas ou na sua carteira de produtos, alinhando-se com a sua ambição de redução de impacto climático e de transição energética.

Utilizar os recursos de maneira eficiente assegurando que o valor dos produtos e os materiais se mantenham na economia durante o maior tempo possível, reduzindo ao mínimo a criação de resíduos e otimizando a gestão dos mesmos, apoiando a economia circular.

Utilizar os recursos de maneira eficiente, reduzindo ao mínimo a criação de resíduos. A redução do desperdício, a reutilização de recursos, a reciclagem, bem como a eliminação segura e ecológica de resíduos, produtos químicos e águas residuais.

Estar em alerta ao que está a ocorrer ao seu redor e comunicar qualquer acidente, incidente ou preocupação com relação ao meio ambiente.

### 3.6. Direitos Humanos

O nosso compromisso é firme e sólido com todos os direitos humanos, particularmente com aqueles ligados à atividade empresarial, à infância e juventude, o direito de livre associação sindical ou o respeito para com as pessoas, igualdade de oportunidades e não discriminação.

Respeitamos e cumprimos os direitos reconhecidos internacionalmente, em todos os momentos. Com isso em mente, observamos sem restrições os respetivos regulamentos nacionais e os regulamentos das Nações Unidas sobre os direitos da criança e a eliminação do trabalho forçado. Em particular, comprometemo-nos a defender a Convenção sobre a idade da admissão ao emprego (Convenção 138 da Organização Internacional do Trabalho (OIT) e a Convenção sobre a Proibição e ação imediata para a eliminação das Piores Formas de Trabalho Infantil (Convenção 182, OIT).

### 3.7. Controlo, governança e conformidade nas nossas atividades

Órgãos sociais e colaboradores, devem respeitar o cumprimento das normas legais e regulamentares em vigor.

Contamos com os mecanismos e controlos adequados alinhados com a regulação para que o registro e contabilidade das transações sejam precisos e claros. A conformidade fiscal é assim uma parte importante da filosofia da nossa empresa.

A Gavis considera que os impostos e demais obrigações fiscais são uma parte importante da sua responsabilidade social. Encorajamos processos de negócio éticos e transparentes. Todos os impostos e taxas são pagos e as declarações fiscais são preenchidas de acordo com a lei vigente.

### 3.8. Luta contra o suborno e a corrupção

Proibimos os subornos, o tratamento preferencial ou vantagens injustas e outros atos de corrupção, como a aceitação ou entrega de presentes mediante pagamentos em dinheiro, ou qualquer outra forma de ação ilícita ou desonesta.

A corrupção é um crime grave e pode ter consequências criminais preocupantes.

Para descartar qualquer suspeita de crime, documentamos claramente todos os nossos acordos com clientes e fornecedores, incluindo qualquer subsequente modificação e aditamento. Nós selecionamos os fornecedores exclusivamente numa base competitiva e com base em critérios objetivos tais como custos totais do produto, qualidade, desempenho, a estabilidade económica do fornecedor

Contribuições sob a forma de presentes, de convites ou de qualquer outro tipo são comuns em todo o mundo de negócios e são, geralmente, permitidos numa extensão razoável. Com isso em mente, ao aceitar e dar presentes e outras contribuições ou recompensas, somos especialmente cautelosos para garantir que nunca influenciem qualquer tomada de decisão.

Assim aderimos às seguintes regras; ofertas efetuadas por terceiros a titulares dos Órgãos Sociais ou a Colaboradores, independentemente da sua natureza, só podem ter valor até Eu 50 (cinquenta euros), incluindo presentes de Natal e deverão sempre ser comunicadas aos nossos superiores ou o responsável pelo compliance, que decidirá sobre a oportunidade da sua aceitação ou recusa.

### 3.9. Luta contra o branqueamento de capitais e o financiamento do terrorismo

Operamos em conformidade com o regulamento, por isso evitaremos sempre qualquer colaboração com pessoas e/ ou entidades que possam ter como finalidade atividades ilícitas, o branqueamento de capitais ou o financiamento do terrorismo.

Colaboramos com as autoridades fiscais para detetar e prevenir práticas fiscais fraudulentas que possam ser utilizadas nos mercados onde estamos presentes. Não realizamos negócios com clientes e fornecedores envolvidos em atividades comerciais que usam fundos de fontes ilegítimas ou se suspeitas fundadamente que assim o façam.

Não realizamos nem recebemos transferências de fundos inusuais procedentes de, ou dirigidas para países com leis de sigilo bancário, escasso controlo contra o branqueamento de capitais, paraísos fiscais ou países onde o índice de corrupção é elevado.

### 3.10. Conflitos de interesses

Depende de nós tomar decisões baseadas exclusivamente em critérios objetivos e garantir que interesses pessoais, que possam entrar em conflito com os da empresa, não nos influenciam. Considerando que, mesmo a sugestão de um conflito de interesses pode ter resultados negativos para a empresa, sempre tomamos cuidado especial para os evitar.

Pode haver um conflito de interesses, por exemplo, se um membro da administração, colaborador ou parente próximo de um colaborador (parceiros, filhos, pais) tem interesses num concorrente, cliente, fornecedor ou prestador de serviços da Gavis.

Se nos for dado a conhecer um conflito de interesses, devemos informar os nossos superiores ou o responsável pelo compliance para proteger o bem-estar da empresa.

### 3.11. Relações com governo, administrações públicas e sindicatos

Promovemos, como base do nosso trabalho diário, um diálogo franco e honesto entre legisladores, reguladores e empresas.

Declaramos a neutralidade política da nossa Empresa, mas podemos e devemos manifestar publicamente sobre quaisquer assuntos que afetem os nossos interesses ou dos nossos colaboradores, clientes, fornecedores e acionistas.

Proibimos as doações ou qualquer tipo de ajuda económica ou em espécie a partidos políticos, entidades públicas e sindicatos.

### 3.12. Relações com parceiros de negócio, fornecedores, clientes e outros grupos

Promovemos a transparência e honestidade nas relações com terceiros, pelo que devemos ser prudentes nos serviços e capacidades sem fazer promessas que não possamos cumprir.

A concorrência justa e gratuita é protegida por leis da concorrência. Comprometemo-nos a cumprir os regulamentos da concorrência leal em conformidade com as disposições legais e, em particular, as disposições da lei da concorrência.

Exigimos que os nossos fornecedores, contratados, subcontratados e parceiros comerciais cumpram as leis e regulamentos aplicáveis e ajam em conformidade com os padrões de ética, integridade e cumprimento contidos neste código, as políticas de segurança e meio ambiente e o respeito aos direitos humanos, garantindo uma relação sustentável a longo prazo.

Atendemos os pedidos dos nossos clientes sem ceder nunca a um pedido que acarrete uma atuação ilegal ou contrária aos nossos padrões éticos.

Cooperamos e apoiamos as instituições sociais, culturais e outras na forma e medidas consideradas adequadas a cada caso.

### 3.13. Meios de comunicação e transparência informativa

As comunicações para o exterior apenas serão realizadas por pessoas autorizadas e de acordo com as pautas fixadas pela Direção e de acordo com os padrões das marcas representadas.

Estabelecemos sempre uma comunicação profissional, precisa e verdadeira, cumprindo a regulamentação e os princípios básicos de transparência e objetividade.

Não realizamos publicidade enganosa nem transmitimos informações que possam induzir em erro ou que possam prejudicar a reputação da nossa atividade ou das marcas que representamos.

## 4. O que fazemos em caso de indícios de incumprimento ou possível má conduta?

A responsabilidade que temos como colaboradores da Gavis promove que denunciemos qualquer suspeita ou incumprimento real da regulação vigente e do nosso regulamento interno. Ao fazê-lo, ajudamos a identificar e eliminar condutas desapropriadas e queixas, protegendo-nos a nós mesmos e à empresa dos danos e prejuízos que possam derivar.

É importante para nós evitar qualquer dano à empresa e, portanto, contribuir para o seu permanente sucesso. Com tal em mente, informaremos os nossos superiores ou a organização sobre quaisquer violações ou situações que violam este código de conduta.

Podemos comunicar qualquer indício de incumprimento do Código de Ética e Conduta, através de um dos seguintes canais habilitados: através da comunicação ao supervisor hierárquico para que o responsável da área informada encaminhe, imediatamente, a informação recebida para o responsável pelo Compliance ou para o email: [denuncie@gavis.pt](mailto:denuncie@gavis.pt)

Como empresa, não toleraremos nenhuma forma de represália dirigida contra quem, de boa-fé, exponha uma denúncia ou contra quem colabore numa investigação. A violação desta proibição será sancionada como um incumprimento, assim como as denúncias que se realizem de “má-fé”. Por isso, garantimos a confidencialidade dos dados da pessoa denunciante tal como determina a regulação de dados pessoais e a relacionada com a gestão de canais de denúncia.

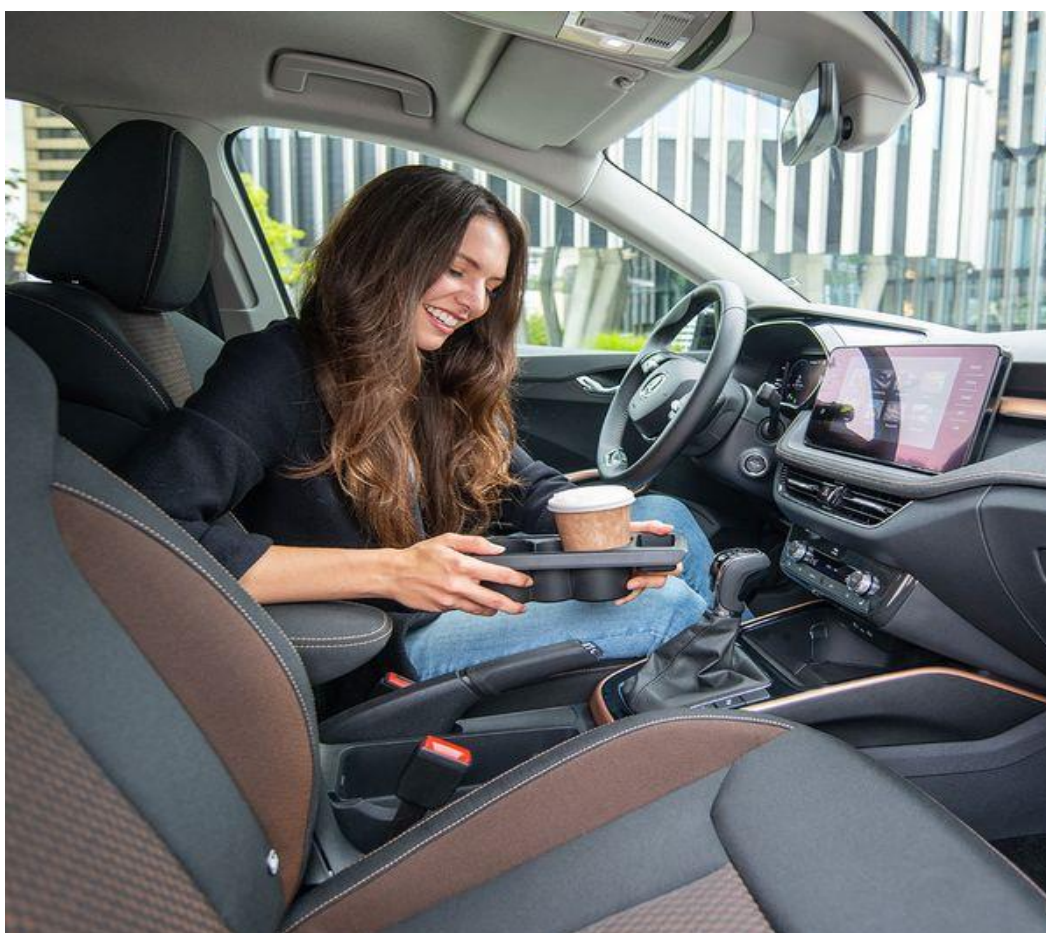
## 5. Atualização, Aceitação e Aprovação

O conteúdo deste Código teve a colaboração dos mais elevados representantes da empresa. Este Código foi aprovado pelo Conselho de Administração na sua reunião de 16 de janeiro de 2023 e produz efeitos a partir do momento da sua aprovação.

O presente Código é divulgado através do sítio institucional [www.gavis.pt](http://www.gavis.pt), promovendo-se dessa forma o livre acesso à sua consulta por todas as partes interessadas.

O conteúdo do presente documento será atualizado e revisto periodicamente, de acordo com o mesmo procedimento utilizado na sua criação, e adaptado às alterações da sociedade em geral e da Gavis em particular.

Contamos com a sua colaboração para cumprir e fazer cumprir todas as normas e princípios recolhidos neste código.



## Anexo I – Código de Conduta para prevenção e combate ao assédio no trabalho

# Código de Conduta para Prevenção e Combate ao Assédio no Trabalho

**GAVIS**

# Introdução

O presente Código de Conduta visa, por um lado, aumentar a consciência e a compreensão de todos os recursos humanos da Gavis S.A. e facultar um quadro orientador de ação que permita, por um lado, identificar, prevenir e gerir problemas de assédio no trabalho, e por outro lado, dar resposta à alínea k) do nº1 do artigo 127º do Código do Trabalho.



# 1. Princípios gerais de conduta

Os colaboradores da GAVIS, internamente ou em representação externa, devem pautar a sua atuação de acordo com os princípios e valores éticos associados à Empresa, adotando comportamentos baseados na responsabilidade, no rigor e no respeito estrito pela dignidade e direitos das pessoas.

A GAVIS incentiva o respeito e a cooperação entre todos os colaboradores, num ambiente de trabalho respeitoso e digno, pelo que não são toleradas ou admissíveis quaisquer práticas de assédio.

O que é o assédio no local de trabalho e quais as suas modalidades?

De acordo com o artigo 29º do Código do Trabalho:

“Entende-se por assédio o comportamento indesejado, nomeadamente o baseado em fator de discriminação, praticado aquando do acesso ao emprego ou no próprio emprego, trabalho ou formação profissional, com o objetivo ou o efeito de perturbar ou constranger a pessoa, afetar a sua dignidade, ou de lhe criar um ambiente intimidativo, hostil, degradante, humilhante ou desestabilizador.

Constitui assédio sexual o comportamento indesejado de carácter sexual, sob forma verbal, não verbal ou física, com o objetivo ou o efeito referido no número anterior”

Como identificar uma potencial situação de assédio?

O assédio constitui uma expressão de comportamentos inaceitáveis por parte de um ou mais indivíduos e podem assumir diversas formas, algumas das quais mais facilmente identificáveis do que outras.

O assédio ocorre quando um ou mais trabalhadores ou quadros dirigentes são repetida e deliberadamente intimidados, ameaçados e/ou humilhados em circunstâncias relacionadas com o trabalho.

O assédio pode ser levado a cabo por um ou mais quadros dirigentes ou trabalhadores, com o propósito ou efeito de violar a dignidade de um quadro dirigente ou trabalhador, afetando a sua saúde e/ou criando um ambiente de trabalho hostil.

O assédio no local de trabalho inclui, mas não está limitado aos seguintes vetores:

- Comportamento que seja degradante, ofensivo, insultuoso, intimidante, embaraçoso ou humilhante;
- Segmentar um indivíduo com tratamento diferenciado de uma natureza irritante;

- Impedimento do desempenho / sabotagem do trabalho;
- Espalhar rumores, incluindo blogs negativos, ou cyberbullying;
- Toques sexuais inapropriados, avanços, sugestões ou pedidos;
- Exibição ou circulação de imagens ou materiais ofensivos em formato eletrónico ou impresso que são conhecidos ou que devem ser reconhecidos como ofensivos.

Por outro lado, o assédio no local de trabalho não representa nem pretende impedir que os empregadores disciplinem ou procedam à gestão dos seus trabalhadores.

Assim, o assédio no local de trabalho não inclui, nomeadamente:

- Gestão de desempenho;
- Pressão decorrente do exercício das funções;
- Exercício de autoridade e do poder disciplinar;
- Requisitos ou decisões operacionais;
- Um desentendimento ou mal-entendido;
- Mudança relacionada ao trabalho (v.g.: mudança de localização, de colegas de trabalho ou trabalho ocupacional);
- Um único comentário ou ação, a menos que tenha efeitos graves, prejudiciais e duradouros;
- Rudeza, a menos que seja extrema e repetitiva;
- Elogios ocasionais;

#### Procedimento em caso de alegação de assédio

Em caso de eventual situação de assédio, que não se tolera, o procedimento a desenvolver internamente baseia-se nos seguintes princípios:

- O interesse de todas as partes em agir com a discrição necessária para proteger a dignidade e a privacidade de cada um;
- A não divulgação de qualquer informação a outras partes não envolvidas no incidente;
- As queixas devem ser investigadas e tratadas com celeridade;
- Todas as partes envolvidas devem ser ouvidas de forma imparcial e beneficiar de um tratamento equitativo;
- As queixas devem ser sustentadas com base em informações detalhadas;
- Caso seja provada a ocorrência de assédio, serão tomadas medidas adequadas contra o(s) que o tenha(m) levado a cabo, as quais poderão compreender sanções disciplinares aí incluído o despedimento;

- Os autores de acusações falsas poderão ser alvo de processos disciplinares.

Em caso de eventual situação de assédio, pode haver uma abordagem informal ou um procedimento formal.

#### Abordagem preliminar

Em alguns casos, pode ser possível corrigir situações sem se percorrer todo o formalismo inerente ao procedimento disciplinar.

Por vezes, as pessoas não sabem que o seu comportamento não é adequado, bem-vindo ou rejeitável, e uma abordagem direta, frontal e imediata, que também inclua os intervenientes, pode conduzir a um entendimento sobre o ocorrido e quanto à cessação do comportamento.

Nestes casos, os intervenientes, se assim o entenderem, podem enveredar por esta abordagem, comunicando e solicitando o apoio da sua chefia direta, ou outro elemento da sua estrutura hierárquica ou, ainda, outro colaborador da organização.

#### Procedimento formal

Em caso de alegação de assédio, o que representa a apresentação, por escrito, de todo o circunstancialismo de que se tenha conhecimento e que envolva a situação, é aberto um procedimento disciplinar que, sem prejuízo das regras constantes no Código do Trabalho, obedecerá ao seguinte:

- O trabalhador deve apresentar e formalizar por escrito a sua queixa, de forma o mais detalhada possível, junto de GAVIS, seja através de e-mail seja através de contacto pessoal, cabendo à GAVIS receber todas as queixas de assédio no trabalho;
- b) A GAVIS realiza a investigação das queixas que receber, tendo que ter ao seu dispor meios necessários, acesso às informações e documentação que possam estar relacionados com o caso, sendo que todos os recursos humanos estão obrigados a cooperar;
- A GAVIS elabora um relatório com conclusões, que inclui os factos e seu enquadramento jurídico, indicando, se possível, circunstâncias agravantes ou atenuantes, e propondo a GAVIS (quem detiver poder disciplinar) a tomada da decisão final;
- A GAVIS, com o acordo do Administrador Dr. Fernando Lopes de Oliveira Loureiro Martins, pode recomendar a adoção de medidas de carácter preventivo.

## Anexo II – A Segurança da Informação

# A Segurança da Informação

**GAVIS**

# Introdução

## O que é a segurança da informação?

É um processo organizado e estruturado que permite preservar a confidencialidade, integridade e a disponibilidade da informação.

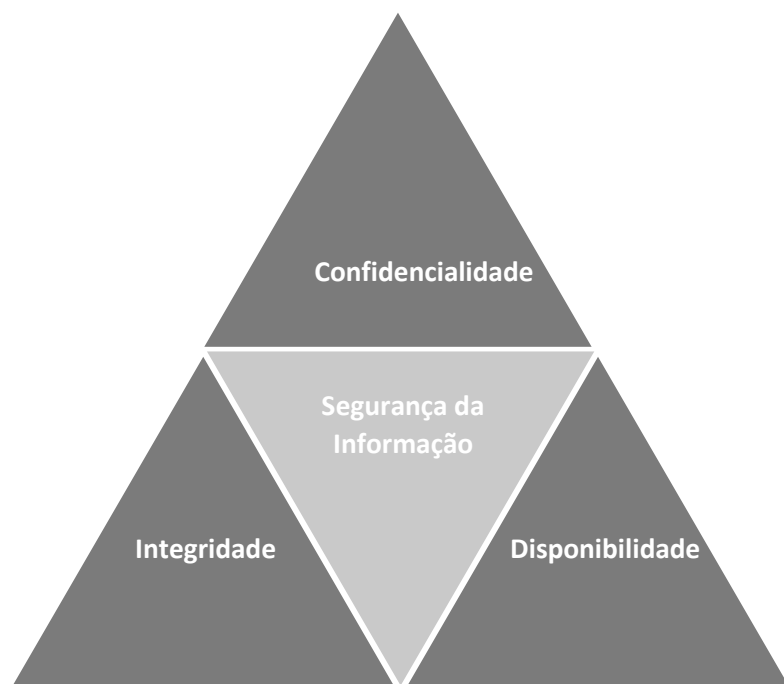
**Confidencialidade** é... assegurar que a informação é acessível somente por pessoas devidamente autorizadas. O acesso à informação é restrito a utilizadores legítimos.

**Integridade** é... garantir a veracidade e complementaridade da informação, bem como os seus métodos de processamento. O conteúdo da informação não pode ser modificado de forma inesperada.

**Disponibilidade** é... assegurar o acesso à informação e bens associados por quem devidamente autorizado. A informação deve estar acessível sempre que necessário.

## Quem é o responsável pela segurança da informação?

Todos nós somos responsáveis pela segurança da informação e todos temos a responsabilidade de proteger os nossos dados e os que nos são confiados.



# 1. Princípios gerais de segurança da informação

A proteção eficaz e adequada da informação e dos sistemas de informação contra quebras de confidencialidade, de integridade e de disponibilidade garante a continuidade da produção da organização, a confiança junto dos utentes e parceiros, bem como a imagem junto do público, faz parte imprescindível da política da organização.

- Estamos cientes da elevada importância da segurança da informação para a nossa organização e tratamo-la de forma adequada;
- Implementamos procedimentos sistemáticos que visam a redução dos riscos;
- Inculcamos a responsabilidade pela segurança da informação;
- Estabelecemos medidas adequadas à nossa organização para garantir a segurança da informação. Verificamos regularmente o respetivo cumprimento e a eficácia;
- Protegemos a informação própria e a que nos é confiada, impedindo a sua divulgação e alteração legal;
- Reagimos de imediato e adequadamente à situação em caso de violação da segurança;
- Garantimos a disponibilidade dos sistemas de informação com base nas exigências dos processos de negócio;
- Implementamos procedimentos adequados à não interrupção da atividade;
- As regras de segurança da informação são afixadas e comunicadas aos colaboradores, fornecedores e parceiros.

## 2. As passwords e o acesso à informação

As organizações estão dotadas de políticas, processos standards e guias de orientação. O principal objetivo é garantir a segurança dos dados confidenciais e dados pessoais.

**Algumas dicas de segurança:**

- Mantenha as suas passwords confidenciais;
- Memorize as suas passwords. As passwords não devem ser escritas em papéis ou locais visíveis;
- Mude as suas passwords regularmente, mesmo nos sistemas que não obriguem a fazê-lo;
- Guarde as suas passwords em softwares encriptados (ex. KeePass Safe) e respeite a política de passwords;
- Não grave as suas passwords de forma automática nos sistemas;
- Não utilize as mesmas passwords para os sistemas da organização e sistemas pessoais;
- Utilize passwords seguras, mas fáceis de memorizar.

| As <i>passwords</i> mais utilizadas são: |                    |
|------------------------------------------|--------------------|
| 1ª 123456                                | 4ª Abcd1234        |
| 2ª Password                              | 5ª Data nascimento |
| 3ª qwerty                                |                    |

### Como criar *passwords* seguras:

Construa uma frase.  
Carro do Ano 2023!

A *password*: CarANO2023!

### 3. Posto de trabalho e salas de reuniões

O posto de trabalho é uma “ferramenta” cuidadosamente pensada para que os colaboradores da nossa organização possam trabalhar de forma organizada, confortável e adequada às suas funções. O seu posto de trabalho é constituído por documentos e ferramentas que fazem parte de uma rede complexa, constituída por milhares de computadores e outros equipamentos. Implementamos medidas e procedimentos que protegem o seu posto de trabalho, a informação do negócio e os seus dados pessoais.

Todos os colaboradores fazem parte da cadeia de segurança, por isso, **para que a nossa informação esteja protegida a sua colaboração é fundamental.**

#### **Posto de trabalho**

O seu posto de trabalho deve estar sempre arrumado e cumprir o princípio “clean desk”.

Durante as reuniões, com temas confidenciais ou sensíveis, deve verificar se a sala está corretamente fechada e protegida para que a informação seja partilhada de forma confidencial.

#### **O PC**

Quando não está a utilizar o seu computador, **■ + L** bloqueie a sua sessão.

O seu PC apenas tem software autorizado e devidamente licenciado.

Evite o armazenamento de dados em pastas locais, todos os documentos de trabalho devem estar armazenados nas pastas da rede.

#### **Documentos**

Os documentos, impressões, agendas e blocos de apontamentos com dados confidenciais devem ser tratados de forma a garantir que terceiros não possam ter conhecimento do seu conteúdo.

Sempre que se afaste do seu posto de trabalho coloque os documentos dentro de armários ou gavetas devidamente trancadas.

As impressões devem ser recolhidas da impressora o mais rápido possível.

Quando imprime documentos confidenciais deve acompanhar presencialmente a saída das folhas e garantir que foram todas recolhidas da impressora.

## 4. O Correio eletrónico e NetEtiqueta

O correio eletrónico (e-mail) é uma ferramenta de trabalho que deve ser utilizada de forma profissional e cuidada. A utilização imprudente ou inadequada pode dar origem a ataques aos nossos sistemas e à nossa informação.

### 4.1. Boas práticas de utilização do e-mail

1. Utilize o e-mail de forma segura, produtiva, profissional e educada;
2. Não reenvie e-mails com brincadeiras ou correntes da fortuna e felicidade nem reaja por impulso ao conteúdo;
3. Verifique sempre os endereços dos destinatários;
4. Não abra e-mails e ficheiros de origem desconhecida, elimine-os imediatamente;
5. Nunca envie informação pessoal que lhe seja solicitada por e-mail, tal como: n.º do cartão de crédito, username, password, nomes. Nenhuma empresa lhe pedirá este tipo de informação por e-mail;
6. Não siga as ligações (links) de e-mails suspeitos. Escreva o endereço diretamente no browser;
7. Informações críticas ou dados pessoais só podem ser enviados em formato encriptado. As passwords devem ser enviadas por outro meio de comunicação.

### 4.2. NetEtiqueta

1. Evite escrever mensagens em MAIÚSCULAS com cores e a bold;
2. Tente ser claro e objetivo, produza textos simples com cuidado gramatical e ortográfico;
3. Tente ser educado e simpático, agradeça e cumprimente;
4. Pode usar smileys :-), é uma forma simples de dar a entender os seus sentimentos;
5. Não reaja de forma emotiva porque normalmente escrevemos e-mails ou partilhamos o que não queremos;
6. Antes de publicar alguma informação verifique se o conteúdo:
  - Tem interesse;
  - Tem qualidade, é atual e respeita a missão da organização;
  - Tem o formato correto e está a ser publicado no dia, hora e local correto.

## 5. Phishing, virus e ransomware

O **Phishing** é uma das principais preocupações ao nível da segurança da informação.

Trata-se de um crime informático baseado no envio de um e-mail fraudulento com objetivo de obter dados pessoais ou confidenciais. É um e-mail falso, normalmente emitido em nome de uma entidade credível tal como um Banco, Facebook, Twitter, Microsoft, Vodafone, etc. mas que na realidade só pretende recolher dados ou infetar os sistemas.

### **Vírus**

Os vírus são programas maliciosos (malware); que se espalham a outros computadores com o objetivo de permitir acessos ou danificar dados e serviços. O utilizador com publicidade (scareware) que é um falso alerta de vírus ou problemas informáticos que levam o utilizador a fazer o que lhe pedem, como por exemplo instalar um programa.

O **Ransomware** é uma estratégia de resgate suportada por um software de encriptação que bloqueia o acesso aos ficheiros ou aos computadores, até que se pague o resgate. Este software encripta os dados com uma chave secreta.

### **“O seu dinheiro ou os seus dados?”**

Para recuperarmos os dados é necessário pagar um resgate.



## 6. A Internet e a Comunicação

Vivemos no mundo da informação e a comunicação é a chave do sucesso pessoal e empresarial. Por este motivo é fundamental garantirmos que comunicamos de forma adequada, nos meios adequados e apenas transmitimos a informação necessária.

No mundo da internet existem regras e códigos de conduta com o objetivo de melhorar a segurança da informação.

### Internet

- Certifique-se que o site é seguro fazendo duplo clique sobre o cadeado ou aceda pelo endereço (URL) que deve começar por "https://" e não por "http://";
- Certifique-se que o seu browser e o antivírus estão atualizados e utilize uma firewall pessoal;
- Consulte os extratos das suas contas bancárias e de serviços com regularidade. Se encontrar algum movimento estranho, contacte imediatamente o prestador de serviço ou banco;
- Não é permitido aceder a sites com conteúdos ilegais ou inadequados;
- Atualize as suas passwords a cada 90 dias. Sempre que possível utilize passwords diferentes para sites seguros e sites não seguros;
- Não é permitido utilizar serviços públicos de e-mail, de transferência de ficheiros e ou serviços cloud para troca de dados da organização;
- Não é permitido divulgar informação ou dados nas redes sociais;
- Não é permitido jogar ou fazer apostas online com recursos da nossa organização (REDE, PCs, etc.).

### Comunicação

- Quando fala ao telefone tenha cuidado para não divulgar informação confidencial;
- Evite falar de assuntos de trabalho em locais e transportes públicos, proteja-se contra os ouvintes;
- Evite ler informações críticas ou confidenciais em locais e transportes públicos;
- Evite abrir envelopes com dados confidenciais em espaços públicos;
- Não utilize redes sociais ou ferramentas (APPS) públicas para comunicar com parceiros e fornecedores (ex: WhatsApp ou Wunderlist), estas não são seguras;
- Não divulgue a extensão telefónica, e-mail e telemóvel de um colega sem que este o permita;

- Não coloque informações da organização em sites públicos (ex. Dropbox);
- Não registre o seu endereço de e-mail de trabalho em redes sociais;
- Não é permitido enviar dados da organização para e-mails pessoais (Ex. Gmail, Hotmail, etc.);
- Pense nas consequências antes de publicar qualquer informação, uma informação embaraçosa pode comprometer a sua imagem e a da sua organização.



## 7. Dispositivos móveis

Os equipamentos móveis são uma potencial fonte de perda de informação crítica de negócio e pessoal. Por este motivo, devem ser tratados com especial atenção e devem estar sempre protegidos.

Olhe para os seus dispositivos móveis (telemóvel, portátil, PEN, token, pasta de documentos) e verifique se estão aplicadas algumas das seguintes regras de segurança.

- Todos os dispositivos portáteis estão protegidos com password;
- Os dispositivos portáteis devem ter os dados encriptados sempre que seja tecnicamente possível;
- O software deve estar atualizado. Sempre que possível ligue o seu equipamento à rede da organização para receber as devidas atualizações (pelo menos a cada 15 dias);
- O equipamento deve ter instalado um antivírus e uma firewall;
- Devem ser feitas cópias de segurança dos dados. Os dados da organização devem ser colocados nas pastas da rede;
- Em locais públicos e transportes públicos os equipamentos devem estar sob vigilância;
- O trabalho com equipamentos móveis em locais públicos deve garantir que os dados do ecrã estão protegidos contra pessoas não autorizadas;
- Os equipamentos móveis não devem ser deixados nos veículos automóveis;
- O computador portátil deve estar sempre com o cadeado de segurança para evitar roubos;
- É proibido desbloquear equipamentos com recurso a ferramentas ou sistemas operativos não autorizados (ex. Jailbreak ou Root);
- *Home-office* - os documentos que são levados para trabalhar em casa devem estar protegidos contra acesso indevido.

## 8. Parceiros Externos

Existe uma ordem cronológica natural de relacionamento com os parceiros externos, esta ordem passa pelas seguintes fases:

1. Antes do contrato;
2. Durante o período de relação de negócio;
3. E terminada a relação de negócio.

Para todas estas fases estão definidas regras e boas práticas que garantem a proteção dos dados, e das infraestruturas da nossa organização e dos nossos parceiros. Estas regras aplicam-se a todos os parceiros externos.

### **Antes do contrato:**

- Os parceiros e as empresas subcontratadas assinam um NDA - Acordo de Confidencialidade;
- Os parceiros que processam ou armazenam dados da nossa organização recebem um briefing de segurança da informação;
- São definidos os dados a serem trocados e os canais seguros para a troca;
- São definidos os interlocutores do parceiro e os nossos, e acordado entre ambos a forma de comunicar incidentes de segurança;
- Se forem trocados dados críticos (pessoais ou de negócio) os interlocutores devem garantir que foram tomadas as medidas de proteção técnicas e funcionais adequadas;
- O prestador de serviço apresenta um plano de segurança claro e atualizado;
- É assinado um contrato-tipo disponibilizado pelo Departamento Jurídico.

### **Durante a relação de negócio:**

- São atribuídos acessos locais ou remotos aos parceiros de acordo com princípio do “Mínimo acesso permitido”;
- Os sistemas dos parceiros externos apenas podem ser instalados na nossa infraestrutura se existirem comprovadas razões técnicas ou económicas;
- Não é permitido instalar o nosso software em equipamentos de parceiros;
- Os nossos sistemas apenas podem ser colocados nas instalações dos parceiros após aprovação formal do CISO;

- Em todos os contratos deve ser assegurado o direito de auditoria aos parceiros e fornecedores, estas auditorias pode ser realizadas por nós ou por um parceiro escolhido pelas partes e acontecem no âmbito da prestação de serviço.

**Terminada e relação de negócio:**

- O interlocutor da organização informa todos as entidades envolvidas;
- Todos os privilégios são imediatamente eliminados;
- Todos os equipamentos são desligados e recolhidos.

## 9. GDPR

O novo Regulamento Geral sobre a Proteção de Dados, constante do Regulamento (UE) 2016/679, foi publicado no Jornal Oficial da União Europeia no dia 4 de maio de 2016. Este regulamento revoga toda a legislação publicada antes da era digital.

Este normativo comunitário, designado na língua inglesa por General Data Protection Regulation (GDPR), é aplicável a partir do dia 25 de maio de 2018. O período transitório de dois anos tem como principal objetivo permitir que as organizações se adaptem às novas regras, tais como:

- Novos direitos e obrigações, ex. direito ao esquecimento e a portabilidade dos dados, etc;
- Coimas elevadas em caso de incumprimento, até 20 milhões de euros ou 4% do volume anual de negócios do grupo;
- Incluir a privacidade desde a conceção como princípio orientador (Privacy by default)-,
- A confiança nas TIC, impõe garantir que as tecnologias não afetam os direitos fundamentais das pessoas à privacidade e à proteção dos dados pessoais (Privacy by Design),
- Princípio de responsabilidade na recolha e proteção dos dados, Accountability e Opposition to Profiling-,
- Define a criação de uma nova função DPO - Data Private Officer que na língua portuguesa se designa por Encarregado de Proteção de Dados;

### **É importante saber:**

- O que são dados pessoais - são todas as informações relativas a uma pessoa identificada ou identificável (nome, morada, património, vencimento, datas, números de cartões, n.º de telefone, IP, vídeos, imagem, raça, dados biométricos, folhas de presença, avaliações, curriculum vitae, etc);
- Não deve reunir dados pessoais em papel ou em formato eletrónico sem informar o DPO;
- Cuidado ao enviar dados pessoais, estes devem estar sempre encriptados ou protegidos;

- Cuidado ao destruir ou eliminar dados pessoais, estes devem ser definitivamente apagados ou eliminados de forma a não serem recuperados por terceiros;
- Cuidado com os dados pessoais que troca com os seus parceiros e em especial com parceiros fora da EU;
- Documentos com dados médicos, e dados de menores são muitos sensíveis pelo que deve ter um cuidado redobrado na sua utilização;
- Se perder ou lhe roubarem dados pessoais informe de imediato o seu DPO;
- O DPO tem a obrigação de comunicar as autoridades todas as “fugas” ou perdas de dados pessoais.



## 10. Destruição de dados e impressões

Informação é um ativo com valor para o negócio.

A informação pode existir sob várias formas, como por exemplo: em suportes de papel (folhetos, jornais, cartolinas, posters, etc.) ou suportes eletrónicos designados por media (CDs, disquetes, tapes, microfilme, discos rígidos, PEN USB, cartões de memória, etc.).

A destruição de informação confidencial deve ser realizada de acordo com regras de segurança e procedimentos adequados. Apenas empresas certificadas podem fazer a destruição da nossa informação. Existe contrato com empresas certificadas para a destruição de informação.

Estas empresas garantem a recolha e o transporte dos documentos e equipamentos, em condições de rigorosa segurança, através da utilização exclusiva de viaturas próprias com caixa blindada, cumprindo os requisitos previstos na Lei da Proteção de Dados Pessoais e os requisitos associados ao acondicionamento e transporte de resíduos.

1. No processo de destruição a empresa produz um relatório detalhado com a descrição dos dispositivos, quantidade e código de barras.
2. A documentação e certificados de destruição ficarão à guarda do CISO.
3. A destruição de grandes volumes de papel é feita a pedido.
4. A destruição de pequenos volumes (documentos de trabalho e flip charts com informação confidencial) é realizada pelo próprio colaborador nos destruidores de papel disponibilizados pela empresa.
5. A eliminação das impressões deve ocorrer no escritório. No escritório de casa, a eliminação de impressões só é permitida se os documentos forem cortados por uma trituradora de corte em pedaços com o máximo de 8 mm.
6. Os equipamentos eletrónicos media só podem ser destruídos ou ter os dados apagados pelas TIC.

# 11. Segurança de pagamentos eletrónicos

Empresas certificadas, como por exemplo as que têm certificação PCI DSS são mais seguras nos pagamentos eletrónicos. Isto quer dizer que cumprem as regras de segurança e executam procedimentos que garantem a transação segura de pagamentos eletrónicos.

Para impedir situações de manipulação e fraude recomendamos atenção a:

1. Observe com atenção o estado do Terminal de Pagamento Automático (ATM), se identificar um teclado diferente mais elevado ou com a ranhura de leitura de cartões alterada, escolha outro ATM;
2. Compre apenas em websites seguros e de confiança;
3. Os websites devem ter mecanismos de segurança, tais como: recurso a certificados SSL, tecnologia SET, entre outros;
4. Utilize apenas cartões de crédito pré-pagos e carregados com o valor necessário para a compra;
5. Evite fazer compras em websites fora da União Europeia, pois poderá ter problemas em caso de necessidade de reclamar;
6. Cuidado com as compras feitas em redes WI-FI públicas, muitas destas redes não são seguras e podem estar a guardar os dados dos seus cartões.

Sempre que possível utilize o contactless, é a melhor forma de proteger o seu PIN.

## 12. Dez Mandamentos de Segurança

1. Não introduzirás PENS alheias no PC de trabalho.
2. Não deixarás o teu PC desbloqueado, mesmo entre amigos ou colegas.
3. Não esquecerás os backups e apostarás nas redundâncias.
4. Não esquecerás o antivírus.
5. Não cobiçarás phishing alheio.
6. Assumirás o papel de melhor linha de defesa contra os ciberataques.
7. Não desejarás trabalhar fora de ambientes de redes seguras.
8. Não partilharás passwords e códigos de acesso.
9. Amarás as medidas de segurança sobre todas as coisas.
10. Não procrastinarás as atualizações, mesmo aos domingos e feriados.

## Anexo III – Declaração de Privacidade de Dados

## DECLARAÇÃO DE PRIVACIDADE DE DADOS

A seguinte declaração de privacidade de dados é voluntária e pode ser retirada a qualquer momento. Só serão incorridos custos, com taxas padrão, para questões de comunicação. A nossa empresa leva a proteção dos dados do cliente com toda a seriedade. Queremos que os nossos clientes se sintam confortáveis com o nosso processo de proteção de dados. A proteção da privacidade individual em relação ao registo e tratamento de dados pessoais é a nossa principal preocupação, à qual prestamos profunda atenção nos nossos processos de negócio. Independentemente da conclusão de um potencial contrato (contrato de compra, de serviço, de arrendamento, de crédito, etc.) e a aquisição legal de dados pessoais para a liquidação do contrato a ele associado, concordo que os dados pessoais que indico, em particular o meu nome, morada, telefone, telemóvel, fax, e-mail, ocupação e hobbies relacionados com o meu veículo podem ser recolhidos, gravados, tratados e utilizados por: **GAVIS - SOCIEDADE DE REPRESENTAÇÕES DE AUTOMÓVEIS, S.A.** exclusivamente para os seus próprios fins, em particular para atendimento e serviços ao cliente e informações do cliente adaptadas às minhas necessidades pessoais.

## EXPLICAÇÕES DA PRIVACIDADE DE DADOS

### Geral:

Por regulamentações legais entende-se que, por exemplo, certos prazos são exigidos para disponibilização de dados pessoais às autoridades fiscais ou outras autoridades como a polícia, autoridade dos transportes, etc., podendo exigir o registo dos seus dados pessoais independentemente da declaração de privacidade de dados aqui realizada. Além disso, os dados pessoais só serão gravados por nós desde que haja um interesse legítimo e viável da nossa parte, como por exemplo a cópia de um cartão de cidadão no caso de um test drive, registando a morada com a finalidade de manter contatos ou algo semelhante.

### Dados Pessoais e Passatempos:

Os seus dados que recolhemos relativos a hobbies utilizamos com o objetivo de um acompanhamento personalizado de informação (por exemplo, "Interessado em desportos de inverno" pode desencadear informações sobre equipamentos de inverno, ou "Adepto de Surf" pode

levar ao envio de informações sobre barras de tejadilho). Se não concorda, pedimos que nos notifique.

## PROPÓSITOS PARA A RECOLHA, GRAVAÇÃO, TRATAMENTO E UTILIZAÇÃO DE DADOS:

### Publicidade:

Publicidade em geral dos nossos produtos e serviços. Entrando em contato consigo por escrito, e-mail ou telefone, por exemplo, para que receba convites para eventos, informações sobre melhorias técnicas relacionadas com o seu veículo, notificações da próxima e-check ou inspeção técnica, informações sobre o seu próprio aperfeiçoamento, por exemplo "como trocar um pneu" ou "como proceder em caso de avaria".

### Informação Pessoal do Cliente:

Entrando em contato consigo, por exemplo, para campanhas de “recall” (recordatórias) que afetam o seu veículo, a expiração de um contrato de leasing ou contrato de financiamento ou uma opção na compra de um veículo novo para o seu veículo atual.

### Inquéritos de Satisfação:

Após a execução de um serviço por parte da nossa empresa, entraremos em contato consigo por escrito, e-mail ou telefone, solicitando o seu grau de satisfação em relação aos serviços prestados por nós. Isso também poderá ser feito por uma empresa em nosso nome.

