Declaração de Postura de Cibersegurança e Inteligência Artificial

Como protejo a informação dos clientes e conduzo os trabalhos de consultoria

Propósito e âmbito

Luis Ferreira, fundador e proprietário da **LuisFerreira Consulting OÜ**, no âmbito da sua prestação de serviços, apresenta os princípios e a postura sobre cibersegurança e inteligência artificial adotados na condução dos contratos de consultoria sénior junto dos seus clientes, nomeadamente conselhos de administração, CEOs, CFOs, CIOs e CISOs.

Destina-se a clientes atuais e potenciais, parceiros e a qualquer terceiro com interesse legítimo em compreender as salvaguardas aplicadas à informação trocada durante os contratos. Complementa, mas não substitui, a Política de Privacidade publicada neste sítio, que rege o tratamento de dados pessoais no âmbito do Regulamento Geral sobre a Proteção de Dados (RGPD — Regulamento (UE) 2016/679, *GDPR*).

Princípios orientadores

A segurança da informação e a utilização ética da tecnologia são fundamento da confiança depositada no trabalho de consultoria sénior independente. Seis princípios orientam todos os contratos:

- **Confidencialidade** — a informação do cliente é partilhada apenas com quem dela tenha legítima necessidade no âmbito do contrato.
- **Integridade** — a informação é protegida contra modificação não autorizada, perda ou corrupção ao longo do seu ciclo de vida.
- **Disponibilidade** — os entregáveis do contrato e a informação de suporte mantêm-se acessíveis quando o cliente deles necessita.
- **Privilégio mínimo e minimização** — o acesso a sistemas e a dados do cliente é solicitado apenas na medida estritamente necessária, pelo tempo estritamente necessário.
- **Privacidade e segurança desde a conceção** — as recomendações e arquiteturas propostas aos clientes incorporam considerações de privacidade e segurança desde o início, e não como complemento posterior.
- **Proteção técnica** — todos os dados recolhidos durante a execução do contrato são catalogados e armazenados em suportes encriptados, com acesso protegido por autenticação multifator. Quando se trate de dados pessoais, estes são adicionalmente anonimizados sempre que praticável.

Referenciais e credenciais

A postura profissional descrita neste documento alicerça-se em referenciais internacionais reconhecidos e em quatro décadas de experiência executiva em tecnologias de informação, *governance*, risco e *compliance*.

- **ISO/IEC 27001** — utilizada como referencial de orientação para as práticas de gestão da segurança da informação. *Não se reivindica certificação.*
- **NIST Cybersecurity Framework (CSF) 2.0** — estrutura as funções de identificação, proteção, deteção, resposta e recuperação aplicadas ao próprio ambiente de consultoria.
- **Regulamento Geral sobre a Proteção de Dados (GDPR)** — rege o tratamento de dados pessoais e está refletido na Política de Privacidade acima referenciada.
- **Regulamento da Inteligência Artificial da União Europeia (Regulamento (UE) 2024/1689)** — observado no papel de *deployer* de sistemas de inteligência artificial, com as correspondentes obrigações de transparência e supervisão.

O consultor Luis Ferreira é **membro da ISACA** (Information Systems Audit and Control Association) e exerceu funções de CIO e CISO num grande grupo empresarial português antes de fundar a LuisFerreira Consulting OÜ.

Classificação e tratamento da informação

A informação dos clientes é tratada como confidencial por omissão e classificada de acordo com a sua sensibilidade. Os seguintes compromissos aplicam-se durante o contrato e após o seu termo:

- A informação do cliente é tratada apenas para os fins acordados na carta de mandato ou em instrumento contratual equivalente.
- As obrigações de confidencialidade subsistem após a conclusão do contrato e são formalizadas em acordos de não divulgação sempre que solicitado.
- Dados pessoais sensíveis, dados regulados (financeiros, de saúde) e informação classificada como restrita pelo cliente são objeto de tratamento reforçado, incluindo pseudonimização ou anonimização prévia a qualquer trabalho analítico, sempre que praticável.
- A informação do cliente é segregada da informação pessoal e da informação de outros clientes.

Aplica-se internamente um esquema simples de classificação, que distingue informação confidencial de cliente, informação sensível ou regulada (sujeita a tratamento reforçado) e informação não sensível, com controlos proporcionais à sensibilidade de cada categoria. O detalhe operacional do esquema pode ser partilhado com clientes em contexto de diligência sobre fornecedores.

Medidas técnicas e organizativas

Sem revelar o detalhe operacional que constituiria, ele próprio, um risco de segurança, encontram-se implementadas as seguintes categorias de controlos:

- **Controlo de acessos e autenticação** em todos os sistemas utilizados na atividade de consultoria, incluindo autenticação multifator.
- **Cifra (encriptação)** dos dados em repouso e em trânsito nos dispositivos e armazenamento utilizados para informação de clientes.
- **Proteção de *endpoints* e gestão de atualizações** em todas as estações e servidores sob controlo direto.
- **Wi-Fi público** — os acessos a sistemas ou a dados de clientes em redes Wi-Fi públicas ou abertas são sempre realizados através de *VPN*.
- **Antivírus e antimalware** — todos os equipamentos têm software de proteção ativo, com subscrição válida e atualizações automáticas permanentes.
- **Cópias de segurança e recuperação** com redundância e verificação periódica.
- **Canais de comunicação seguros** para troca de informação confidencial com clientes.
- **Segurança física** dos dispositivos e documentos, incluindo práticas de segurança em viagem quando os contratos decorrem nas instalações do cliente.
- **Diligência sobre fornecedores** relativamente a serviços de terceiros utilizados na prestação dos serviços, com preferência por fornecedores que ofereçam garantias contratuais de proteção de dados.
- **Aprendizagem contínua** em segurança e ameaças emergentes, incluindo desenvolvimento profissional formal e participação ativa na comunidade de segurança.
- **Política de alojamento e processamento de dados em *cloud*** — subcontratação apenas de serviços *cloud* prestados por fornecedores *hyperscaler* (nomeadamente Google Cloud, AWS e Microsoft Azure), assegurando, sempre que tecnicamente e contratualmente possível, que o alojamento e o processamento de dados ocorrem em *data centers* localizados na União Europeia, em conformidade com os requisitos de segurança e proteção de dados aplicáveis.

Mantém-se internamente um inventário detalhado das medidas técnicas, que pode ser discutido, sob acordo de confidencialidade adequado, com clientes que conduzam processos de diligência sobre fornecedores.

Utilização de inteligência artificial no trabalho de consultoria

Recorre-se a ferramentas de inteligência artificial de forma seletiva, para apoio a tarefas de pesquisa, análise, redação e desenvolvimento de código nos contratos de consultoria. A sua utilização rege-se pelos compromissos seguintes, concebidos para assegurar que a adoção de IA não compromete a confidencialidade e a qualidade a que os clientes têm direito.

- **Subscrições pagas, de nível profissional** são as únicas utilizadas para serviços de IA. Não se recorre a ferramentas gratuitas ou não verificadas no tratamento de informação de clientes, em alinhamento com a política, acima detalhada, de alojamento e processamento em *data centers* na União Europeia.
- **Garantias de não treino** — apenas se utilizam serviços que excluem contratualmente a utilização do conteúdo submetido para treino de modelos no tratamento de informação de clientes.

- **Anonimização e minimização** — a informação do cliente submetida a sistemas de IA é anonimizada, pseudonimizada ou generalizada sempre que o objetivo analítico possa ser alcançado sem detalhe identificável. Identificadores sensíveis, configurações proprietárias e dados pessoais são removidos antes da submissão sempre que possível.
- **Supervisão humana** — todos os resultados produzidos com apoio de IA são revistos, validados e, quando apropriado, corrigidos antes de serem entregues aos clientes. A responsabilidade profissional pelos entregáveis permanece integralmente do consultor.
- **Transparência** — os clientes são informados quando ferramentas de IA são utilizadas de forma material na produção de entregáveis, e a IA nunca é apresentada como substituto do discernimento executivo sénior.
- **Proibição de automação opaca** — não se tomam decisões automatizadas com efeito sobre os interesses dos clientes sem revisão humana.
- **Alinhamento com o AI Act** — no papel de *deployer* de sistemas de IA, observam-se as obrigações aplicáveis de transparência, supervisão e manutenção de registos previstas no Regulamento (UE) 2024/1689.

Os clientes com restrições específicas sobre a utilização de IA nos seus contratos (por exemplo, sectores regulados com proibições explícitas) são convidados a comunicar essas restrições por escrito; tais restrições são formalmente incorporadas no contrato e respeitadas sem exceção.

Tratamento de incidentes e notificação ao cliente

Caso ocorra um incidente de segurança que afete informação do cliente:

- O cliente é notificado **sem demora indevida** e, em qualquer caso, no prazo de **72 horas** após o conhecimento do incidente, em alinhamento com o padrão do artigo 33.º do GDPR.
- A notificação inclui a natureza do incidente, as categorias de informação afetadas, as medidas tomadas para o conter e as ações recomendadas, quando aplicável.
- É prestada cooperação integral ao cliente e, quando relevante, às autoridades competentes (CNPD, autoridade nacional de cibersegurança) na investigação e remediação do incidente.
- As lições aprendidas são documentadas e incorporadas nos controlos acima descritos.

Responsabilidade e contacto

Numa prática de consultoria sénior unipessoal, a função de responsável pela cibersegurança e pela governação da inteligência artificial cabe ao fundador e gerente, **Luis Ferreira**. Esta responsabilidade não é delegada.

Para qualquer assunto relacionado com esta declaração — incluindo processos de diligência sobre fornecedores, notificações de incidentes ou requisitos contratuais específicos de segurança — solicita-se contacto através de:

- **Endereço eletrónico:** luis@luisferreira.pt
- **Entidade:** LuisFerreira Consulting OÜ — Sepapaja tn 6, 15551 Tallinn, Estónia (n.º de registo 17408024).

Revisão e controlo de versões

Esta declaração é revista, no mínimo, anualmente e sempre que ocorra alteração material no panorama tecnológico, regulamentar ou de ameaças que justifique atualização.

- **Versão:** 1.0
- **Data de entrada em vigor:** 10 de maio de 2026
- **Próxima revisão prevista:** 10 de maio de 2027
- **Responsável:** Luis Ferreira, Gerente, LuisFerreira Consulting OÜ.