



**IBERAMBAR**

## **Política do Sistema Integrado de Gestao**

Iberambar, Lda.

31/10/2023



#### **Declaración de confidencialidad y protección de datos LOPD**

La presente documentación es propiedad de Iberambar, Lda., tiene carácter confidencial y no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquiera otro. Asimismo, tampoco podrá ser objeto de préstamo, alquiler o cualquier forma de cesión de uso sin el permiso previo y escrito de Iberambar, Lda., titular del Copyright. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será perseguido conforme a la ley.

Cualquier dato, inclusive de carácter personal, entregado y/u obtenido por las partes como consecuencia de la provisión/recepción del Servicio, única y exclusivamente podrá ser utilizado o aplicado para dicho fin, no pudiendo ser entregado o cedido a terceros bajo ningún título (salvo el tratamiento o acceso por aquellos terceros relacionados con la recepción/provisión del Servicio o aquellos casos en los que legalmente la parte viniera obligada, sirviendo en dicho caso esta cláusula como consentimiento expreso a tales efectos), ni siquiera a los meros efectos de su conservación. Las partes deberán adoptar las medidas de índole técnico y organizativas necesarias para garantizar la seguridad de los datos y evitar su alteración, pérdida tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos suministrados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

En caso de que como consecuencia de la provisión del Servicio el proveedor de este accediera a datos de carácter personal del Cliente (o de sus clientes o empleados, de los que el Cliente ahora manifiesta haber obtenido el previo consentimiento), cumplirá con las obligaciones que establece la vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales es una ley orgánica aprobada por las Cortes Generales de España que tiene por objeto adaptar el Derecho interno español al Reglamento General de Protección de Datos. Los datos de carácter personal facilitados y todos los derivados de la relación contractual, se encuentran incluidos en un fichero automatizado propiedad de Iberambar, Lda., debidamente inscrito en la Comissão Nacional de Protecção de Dados, para las finalidades de envío de información de interés y/o del mantenimiento de la relación contractual y/o de gestión con Iberambar. Puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición de utilización de sus datos personales de acuerdo con la Ley Orgánica 3/2018, enviándonos un correo electrónico a [protecaodados@iberambar.pt](mailto:protecaodados@iberambar.pt), o por correo ordinario dirigido a Rua Rui Teles Palhinha, 3 Leíao 2745-015 Porto Salvo.

## Datos de control

REFERENCIA	Política do SIG	FECHA	31/10/2023
------------	-----------------	-------	------------

## Información del documento

NOMBRE DEL DOCUMENTO	Política do Sistema Integrado de Gestao
AUTOR/ES	Dpto. SGI / Direção

## Revisión del documento

VERSIÓN	FECHA	REVISADO POR	DESCRIPCIÓN	NOMBRE DEL FICHERO
1	10/03/2021	Dpto. SGI	Política do SIG	Política do Sistema Integrado de Gestao.docx
2	03/07/2023	Dpto. SGI	Atualizacao geral	Política do Sistema Integrado de Gestao.docx
3	31/10/2023	Dpto. SGI	Inclusao do código e canal comunicacao ética	Política do Sistema Integrado de Gestao.docx

## Aprobación del documento

VERSIÓN	FECHA	APROBADO POR	DESCRIPCIÓN	NOMBRE DEL FICHERO
1	10/03/2021	Direção	Política do SIG	Política do Sistema Integrado de Gestao.docx
2	03/07/2023	Direção	Atualizacao geral	Política do Sistema Integrado de Gestao.docx
3	31/10/2023	Direção	Inclusao do código e canal comunicacao ética	Política do Sistema Integrado de Gestao.docx





A Direção da **IBERAMBAR Lda.**, assume liderar e impulsiona a **Excelência** na Gestão através de seu compromisso com a **Melhora Contínua, Qualidade, a Proteção da Segurança e Saúde dos trabalhadores**, e **Inovação** nos Processos e Serviços, o cumprimento dos **Níveis de Serviço** e a proteção da **Segurança da Informação**, tem como objetivo fundamental para o sucesso da Organização.

Os princípios da Excelência fazem parte dos **valores** éticos e profissionais da Companhia e dos compromissos que **Iberambar Lda.**, tem adquirido com seus clientes, empregados, empresas fornecedoras, entidades colaboradoras e a sociedade, na hora de satisfazer suas necessidades e gerar **valor e riqueza** a todas as **partes interessadas** ao longo do tempo.

Para isso tem estabelecido as medidas necessárias para a implantação, manutenção, revisão, e melhoria contínua de um Sistema de Gestão Integrado baseado nos requisitos, das normas internacionais mais prestigiosas: Qualidade **ISO 9001**, , Gestão de Serviços **ISO/IEC 20000-1** e Segurança da Informação **ISO/IEC 27001**, para seus serviços de **“DESENHO, INSTALAÇÃO E/OU MANUTENÇÃO DE SISTEMAS INTEGRADOS e REDES DE COMUNICAÇÃO. GERENCIAMENTO E MANUTENÇÃO DE SISTEMAS INTEGRADOS DE SEGURANÇA. GERENCIAMENTO E MANUTENÇÃO DE SISTEMAS DE TI. SERVIÇOS PROFISSIONAIS. CENTRO DE SERVIÇO. GESTÃO DE INFRA-ESTRUTURAS.”**

A Direção de **Iberambar Lda.**, estabelece as seguintes directrizes:

1. Satisfazem-se os **Requisitos Legais, Regulamentares, Normativos** e outros que a Organização subscreva, aplicáveis aos serviços prestados.
2. Determinam-se **Objetivos e Metas** gerais e departamentais baseados em dados reais e mensuráveis, de forma que se possa provar o seu sucesso, sendo revistos periodicamente para sua contínua adequação.
3. Utilizam-se **Técnicas de Rastreamento e Medidas** dos processos, baseadas no estabelecimento de Indicadores que permitam melhorar sua eficácia e detetar os custos de Não Qualidade e **Não Prevenção da Poluição Ambiental e da Saúde e Segurança Ocupacional.**
4. Mantém-se uma **Infraestrutura** (instalações, veículos, equipes de trabalho, sistemas de TI...) conforme às necessidades da Empresa e dos processos, com um plano de manutenção preventiva definido e adequado para a substituição da infraestrutura obsoleta. Neste sentido estabelece-se um compromisso de inovação e melhoria contínua da qualidade, protecção do meio ambiente , proporcionar condições de trabalho seguras e saudáveis para a prevenção de lesões relacionadas ao trabalho e a deterioração da saúde e da segurança da informação, através do Sistema de Gestão Integrado.
5. Procura-se continuamente a **satisfação dos Clientes**, atendendo tanto às queixas e reclamações, como às sugestões dos mesmos. Periodicamente, avalia-se o seu grau de satisfação, para assim poder responder adequadamente a suas necessidades e expectativas, otimizando os processos e recursos que permitam o desenvolvimento de serviços com os mais altos níveis de qualidade e com os melhores resultados possíveis. Realizam-se reuniões periódicas com os Clientes aos que a Organização presta seus **Serviços de TI**, com o fim de identificar as suas necessidades, levar a cabo um rastreamento do nível de satisfação em relação aos serviços prestados, e identificar qualquer mudança ou petição de melhora dos mesmos.
6. Implica-se a **todo o Pessoal** Ihe fazendo consciente da importância de seu trabalho quanto ao cumprimento dos requisitos da qualidade sempre com comportamento de trabalho seguro, e dos níveis de serviço lembrados com os clientes, velando a sua vez pela proteção da segurança da informação e melhorar o seu comportamento no meio ambiental.

Todo o pessoal da empresa tem a responsabilidade de gerir a **prevenção dos riscos ocupacionais**, incluindo clientes e contratados, no compromisso ativo de melhorar as condições de trabalho o pessoal.

7. Estabelece-se um **Plano de Formação** contínua para todo o **Pessoal** de maneira que se assegure a sua completa capacitação para o desempenho de seu posto de trabalho e permita dispor de pessoal tecnicamente competente e devidamente instruído, para levar a cabo as tarefas encomendadas com a garantia de qualidade, segurança e de nível de serviço exigidas. Periodicamente, avalia-se a eficácia das ações formativas bem como o grau de satisfação do pessoal, para poder determinar e gerir o ambiente de trabalho e as necessidades formativas.
8. Mantém-se um contacto permanente com os **Fornecedores de Produtos e Prestadores de Serviços Externos** orientado a conseguir o controlo adequado sobre o produto comprado e o serviço fornecido externamente, mantendo o compromisso de adequar-se e respeitar os princípios e os acordos de nível de serviço estabelecidos. Leva-se a cabo um rastreamento e monitorização dos níveis de serviço estabelecidos com os empresas fornecedoras e subcontratados na prestação de **Serviços de TI**, com o fim de identificar e corrigir qualquer tipo de desvio que possa afetar os serviços oferecidos aos clientes.
9. Estabelece-se ações para abordar riscos e oportunidades, promovendo o **pensamento baseado em riscos**, contemplando as necessidades / expectativas das partes interessadas bem como o contexto da organização.
10. Mantém-se uma adequada **gestão de Orçamentos dos Serviços de TI**, onde se considera tanto os custos diretos como os indiretos bem como os custos iniciais e os derivados da manutenção periódica dos ativos a cada serviço. Estes orçamentos contrastam-se com os resultados da contabilidade associada, com o fim de levar um adequado rastreamento dos custos reais e dispor da informação necessária para corrigir e melhorar o controlo dos custos dos serviços TI.
11. Estabelecem-se e documentam os níveis de serviço lembrados com a cada **Cliente** para **melhorar continuamente** as características dos **Serviços de TI**, neles se especificam os níveis a cumprir para a cada uma das características do serviço. Todo o pessoal a vai porque os serviços prestados cumpram com ditos acordos de nível de serviço.
12. Monitoram-se adequadamente os **Serviços de TI** com o fim de proporcionar aos **Clientes** cada serviço, toda a informação necessária para levar a cabo o rastreamento das características relevantes dos mesmos.
13. Implica-se a **todo o Pessoal** a participar na identificação dos requerimentos de Disponibilidade e **Continuidade** dos **Serviços de TI**. Realiza-se uma adequada implementação dos ditos requerimentos, planeamento de provas e monitorização da disponibilidade dos serviços TI e da infraestrutura que os suporta, para verificar que estes requisitos se cumprem e melhoram progressivamente. Periodicamente, realizam-se provas de continuidade das que se desprendem planos de ação para corrigir os desvios que pudessem se produzir.
14. Vela-se para que os **Serviços de TI** prestados satisfaçam os pedidos de serviços de futuros clientes, pelo que se leva a cabo análise, e medidas para assegurar que tanto as necessidades atuais como futuras são adequadamente satisfeitas, garantindo que os pedidos dos clientes são atendidos do modo mais eficiente possível.
15. Gere-se adequadamente os **Incidentes** relacionados com os **Serviços de TI** fornecidos, com o fim de restabelecer com a máxima celeridade possível os níveis normais de operação dos serviços e minimizar os impactos adversos de ditos incidentes na organização, assegurando que se mantêm os níveis de qualidade e disponibilidade pactuados nos acordos de nível de serviço com o cliente.
16. Analisam-se adequadamente os **Problemas** identificados, tanto a raiz das atividades preventivas como do escalar a partir de um Incidente, até identificar a causa subjacente do erro. Estabelecem-se as ações corretivas necessárias para reparar ou minimizar os seus efeitos.
17. Leva-se a cabo um adequado rastreamento dos **Elementos de Configuração**, versões e suas características. Assim mesmo se verifica periodicamente que os registos de

configuração se mantêm atualizados, e se corrigem os desajustes produzidos. Garante-se que só após passar por um processo de planeamento, desenho, desenvolvimento, configuração e testes, de forma a restabelecer em produção o serviço final.

18. Revisam-se e validam de maneira formal todas as **Mudanças** que se produzem em relação a qualquer especto dos **Serviços de TI** previstos pela organização.
19. Declara-se a **Política Externa de Segurança da Informação**: O propósito desta Política é proteger os ativos de informação que suportam todos os serviços prestados pela **Iberambar Lda.**, pelo que a Direção dispõe das seguintes diretrizes para garantir o cumprimento dos requisitos de segurança de informação:
  - Estabelecem-se as medidas necessárias para proteger a informação de **Iberambar Lda.** contra perdas de **disponibilidade, confidencialidade, integridade, autenticidade e rastreabilidade.**
  - Estabelece-se uma metodologia de avaliação e tratamento do Risco adequada para o Sistema de Gestão de Segurança da informação, os requerimentos do negócio, os serviços, as mudanças, as ameaças e o meio exterior (requerimentos legais, obrigações contratuais...), que contemple, ademais, os controles necessários para mitigar os Riscos identificados, os critérios de aceitação do risco e os níveis de risco aceitável.
  - Garante-se que as atividades empresariais, operações, serviços e processos, tanto atuais como futuros de **Iberambar Lda.**, cumprem com os **requisitos e as obrigações legais, regulamentares e contratuais**, em matéria de Segurança da Informação.
  - Realiza-se uma **monitorização** constante das **medidas de segurança** implantadas na Empresa, assegurando o cumprimento eficiente das mesmas.
  - Gere-se adequadamente os recursos necessários para a manutenção da segurança da informação, garantindo a gestão eficiente dos mesmos, o seu acesso e o correto funcionamento da infraestrutura TI de **Iberambar Lda.**
  - Garante-se a correta **Gestão dos Incidentes de segurança da informação**, assegurando que as vulnerabilidades e os eventos de segurança, são detetados, comunicados e tratados, de maneira que seja possível empreender as ações oportunas.
  - Comunica-se ao pessoal da Organização a importância do cumprimento das atividades relacionadas com a segurança da informação, seu compromisso com a **Política Interna de Segurança da Informação**, e a sua contribuição ao lucro dos objetivos bem como suas responsabilidades em matéria de segurança.
20. Prevenem-se condutas ilegais incentivando o cumprimento das obrigações legais e evitando condutas que possam prejudicar o património, a imagen ou a reputação de **Iberambar, Lda.** O **Código de Ética e Conduta** do Grupo Ambar contém os princípios e regras que devem reger a atuação de todas as empresas do Grupo e de todo o seu pessoal, de forma a garantir um comportamento ético e responsável no desenvolvimento da sua atividade.
21. Qualquer membro dos grupos de interesse (clientes, funcionários, fornecedores, colaboradores e sociedade) que entenda ou tenha tido conhecimento da existencia de condutas irregulares ou de qualquer descumprimento ou violação de regulamentos internos e externos sobre assuntos que afetam a **Iberambar, Lda**, pode informar sobre esta ação através do **Canal de Comunicação Ética** disponível.

Esta Política junta com as Diretrizes estabelecidas, de encontrar implantar, manter, rever a comunicação de todas as pessoas que trabalham na Organização ou em nome dela, bem como de disponibilizar todas as partes interessadas. A Direção assume o compromisso de liderar este processo e atribuir os recursos necessários para cumprir com as premissas dantes citadas, de forma que se consiga melhorar continuamente a eficácia do sistema, face a obter a total satisfação dos grupos de interesse e conseguir os objetivos fixados.

Este Política do Sistema de Gestão Integrado tem sido aprovada pela **Direção de IBERAMBAR Lda.**, e é revista de maneira periódica.



Santander a 31 de octubre de 2023

La Dirección  
