WINCODE | SOFTWARE | CONTABILIDADE | INTERNET

Manual de WRGPD

WRGPD
WINCODE - PROTEÇÃO DE DADOS

Santa *Maria da Feira*

VERSÃO 2018v1.1

Regulamento Geral Proteção de Dados

Como pode a WINCODE ser um seu aliado no cumprimento do RPGD?
A Wincode desenvolveu uma oferta integrada (RGPD) que é diferenciadora porque endereça de forma multidisciplinar as diferentes vertentes do Regulamento, nomeadamente, a **vertente legal**, a **organização de processos**, **a segurança das plataformas tecnológicas e a gestão da conformidade.**

A nossa abordagem assentou em três dimensões:

- **Avaliação:** identificar níveis de conformidade, avaliar o risco e definir um plano de atividades e ajuste aos sistemas e programas;
- **Implementação:** atualização dos programas Wincode, tendo por objetivo o cumprimento do RGPD de forma automática e incluída nos tratamentos já existentes;
- **Controlo:** Controlar e gerir a conformidade, baseado numa "framework de compliance" desenvolvida pela WINCODE, num sistema tipo **DAAS** – "DPO as a service".

Introdução:

A responsabilidade proativa, estabelecida no Artigo 25 do Regulamento Geral de Proteção de Dados (RGPD), obriga as partes responsáveis e os responsáveis pelo processamento a cumprir os princípios relativos ao processamento de dados pessoais e a demonstrar tal conformidade.

Estes princípios são os princípios de disponibilidade, integridade, confidencialidade e resiliência permanente dos sistemas e programas de gestão.

Na WINCODE preparamos os programas e plataformas para processar os dados pessoais de forma a garantir a segurança adequada dos mesmos, incluindo a proteção contra a gestão não autorizada ou ilegal e contra perda, destruição, roubo ou danos acidentais, através da aplicação de técnicas adequadas ou medidas organizativas, tais como pseudonimização e minimização de dados, a fim de cumprir os requisitos do RGPD e proteger os direitos das pessoas envolvidas.

Da mesma forma, aplicamos medidas técnicas e os procedimentos apropriados para garantir que, por padrão, somente os dados pessoais necessários para cada um dos propósitos específicos da administração são processados. Aplicamos essas medidas em todos os nossos produtos e serviços para manter os altos níveis de segurança exigidos pelo RGPD e pelos nossos próprios clientes.

Algumas dessas medidas são:

- Procedimentos para controlo e acesso à informação por funcionários.
- Firewall de perímetro e isolamento lógico, todas as plataformas possuem segurança.
- O acesso aos programas é restrito e carece de configuração pormenorizada dos utilizadores dos programas.
- Identificação e autenticação: todos os computadores possuem uma senha para aceder aos sistemas de informação. Serão implementadas políticas para alterar a senha que garante a segurança do acesso aos sistemas.
- Cópias de segurança: as cópias de backup são automáticas e encriptadas.
- Documentos: acesso aos documentos e anexos apenas através dos programas Wincode com palavra de acesso para abertura e consulta destes.
- Comunicações e suporte com a utilização de VPN.
- Antivírus instalado em todos os sistemas da empresa.

Como as novas regulamentações não estabelecem uma indicação precisa das medidas de segurança técnicas e organizacionais a aplicar, essas medidas foram preparadas por nós, levando em conta o artigo 32.1 do RGPD que afirma que:

Levando em conta o estado da tecnologia, os custos de aplicação, a natureza, o objetivo, o contexto e os propósitos da gestão, bem como os riscos variados de probabilidade e severidade dos direitos e liberdades das pessoas físicas, o controlador e o processador aplicará medidas técnicas e processos **adequados** para garantir um nível de segurança condizente com o risco, que, no nosso caso, inclui, entre outros:

a) a pseudonimização e encriptação de dados pessoais quando necessário;

b) a capacidade de garantir a confidencialidade, integridade, disponibilidade e resiliência permanente dos sistemas e serviços de gestão;

c) a capacidade de restaurar rapidamente a disponibilidade e o acesso a dados pessoais em caso de incidente físico ou técnico;

d) registo dos processos de verificação, avaliação e avaliação regular da eficácia das medidas técnicas e organizacionais para garantir a segurança da gestão.

e) obrigações de confidencialidade: todos os funcionários devem compreender a importância da confidencialidade em relação aos dados aos quais têm acesso, mesmo após o término do contrato de trabalho, mesmo assim, nos programas, apenas podem aceder aos dados que precisam para a execução das suas funções.

f) registo de atividades de gestão: o responsável pela gestão (DPO), terá um programa para registo das atividades de gestão realizadas.

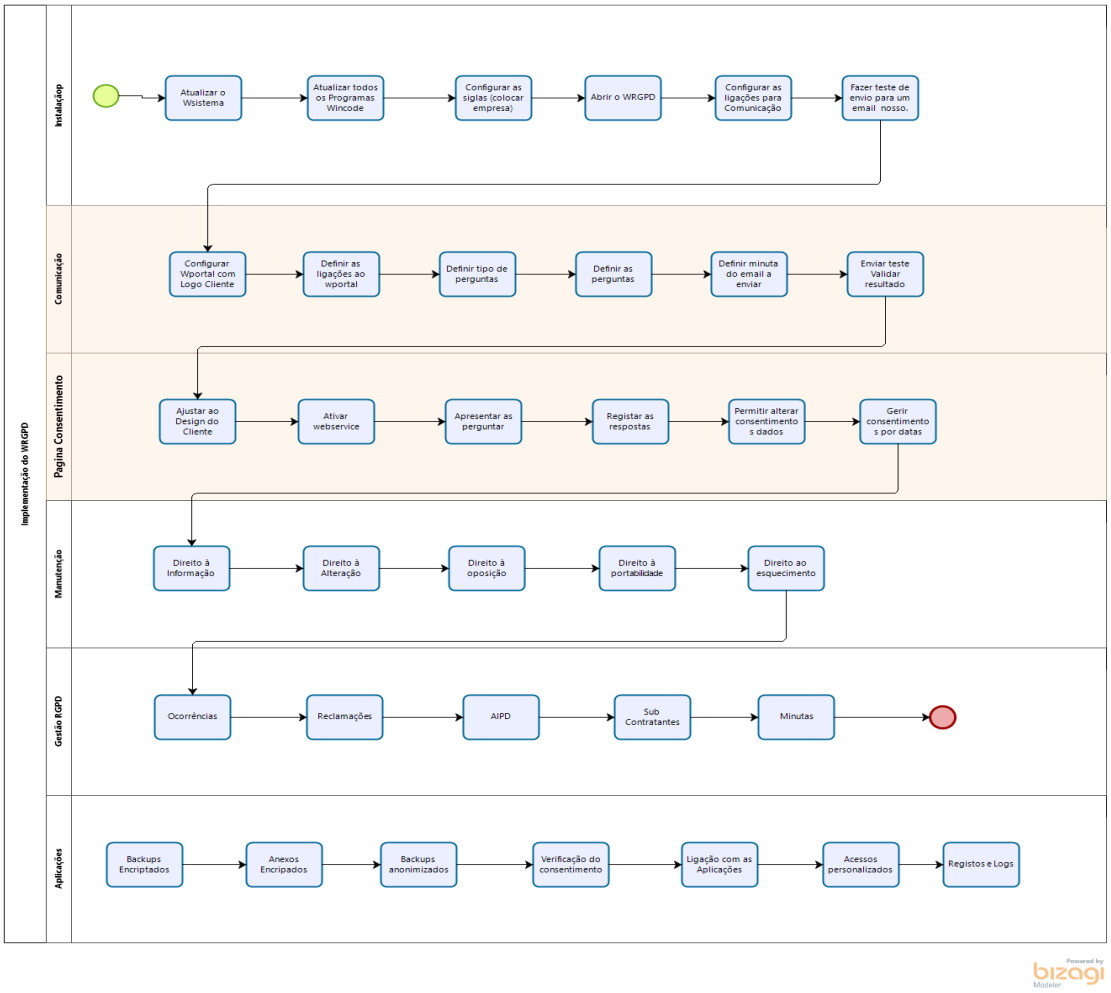
g) avaliação de impacto de privacidade (PIA) o programa permite ao responsável pela gestão, registar e gerir a realização uma PIA, caso forem obrigados a fazê-lo de acordo com as disposições do artigo 35 do RGPD, bem como para as consultas realizadas às entidades verificadoras, quando apropriado.

h) direito à informação: o responsável pela gestão do RGPD, tem no programa a forma de gerir essas solicitações e registar as interações com os titulares dos dados.

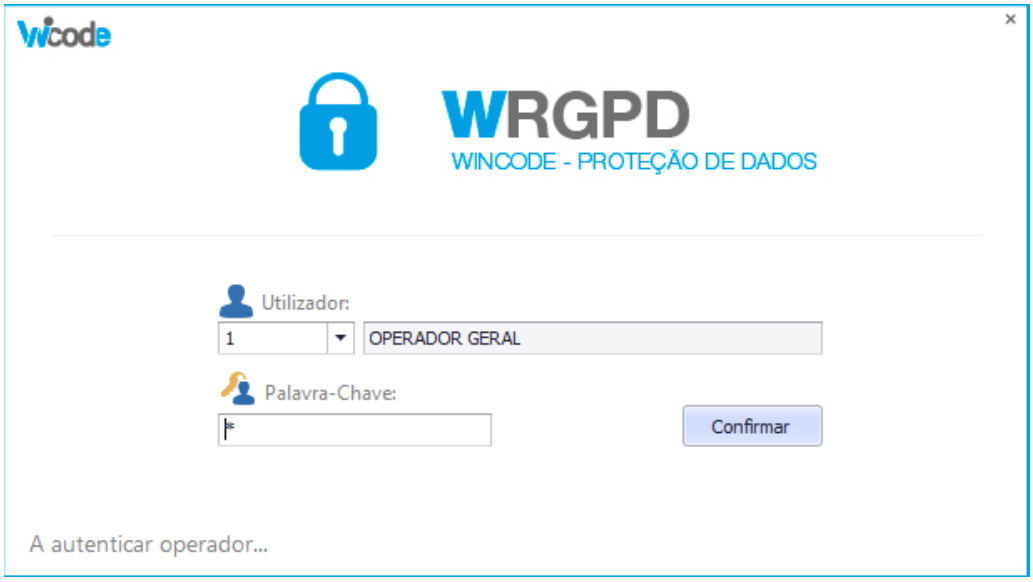
Os **programas Wincode** incluem agora algumas inovações, para cumprimento do regulamento:

- O acesso aos dados pessoais está protegido por configuração de **acessos individuais**.
- Gerir e dar resposta aos **direitos dos titulares** (eliminação, Informação, Retificação, oposição, portabilidade, etc.).
- Gestão da comunicação com os titulares para **obter os consentimentos** e gestão desses.
- Gestão do comprovativo dos consentimentos expressos do titular dos dados.
- Rotinas manuais e automáticas para registar, provar e **evidenciar** que todos os requisitos legais são cumpridos.
- Gerir as politicas de auditoria, verificação e ajustes de conformidade (**AIPD**)
- Gestão dos contratos com os funcionários que lidam com dados protegidos, para a confirmação que entendem o RGPD e se comprometem a aplica-lo.
- Gestão dos contratos com os **subcontratantes** que devem já terem sido revistos, (CC, Informática, ROC, Advogado, etc.)
- Gestão e **rastreabilidade** dos procedimentos e dos tratamentos efetuados sobre os dados dos titulares.
- **Interligação** com todos os programas Wincode, no intuito da conformidade “by design”.

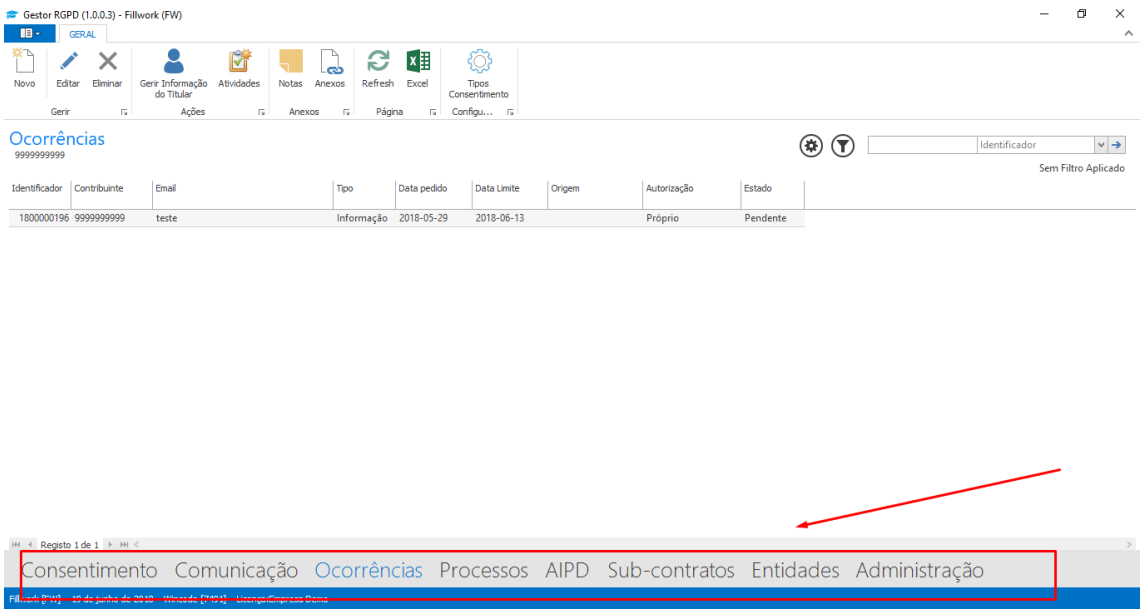
Diagrama com os procedimentos de instalação das funcionalidades do WRGPD.



Quadro de entrada e autenticação dos operadores que têm acesso à gestão do WRGPD



Quadro principal e menu da plataforma WRGPD, para o DPO, com todas as funcionalidades.



O Programa WRGPD, funciona como uma plataforma de gestão da conformidade com o RGPD e interligação com os programas Wincode, estabelecendo uma transversatilidade de todos os registos geridos e sujeitos ao regulamento.
Considerando que a segurança fisica e os acessos aos equipamentos está assegurada, contando também que a rede e os backups da informação está também em conformidade, vamos neste manual focar a atenção nos programas Wincode e à gestão das obrigatoridades que o regulamento obriga, iremos abordar:

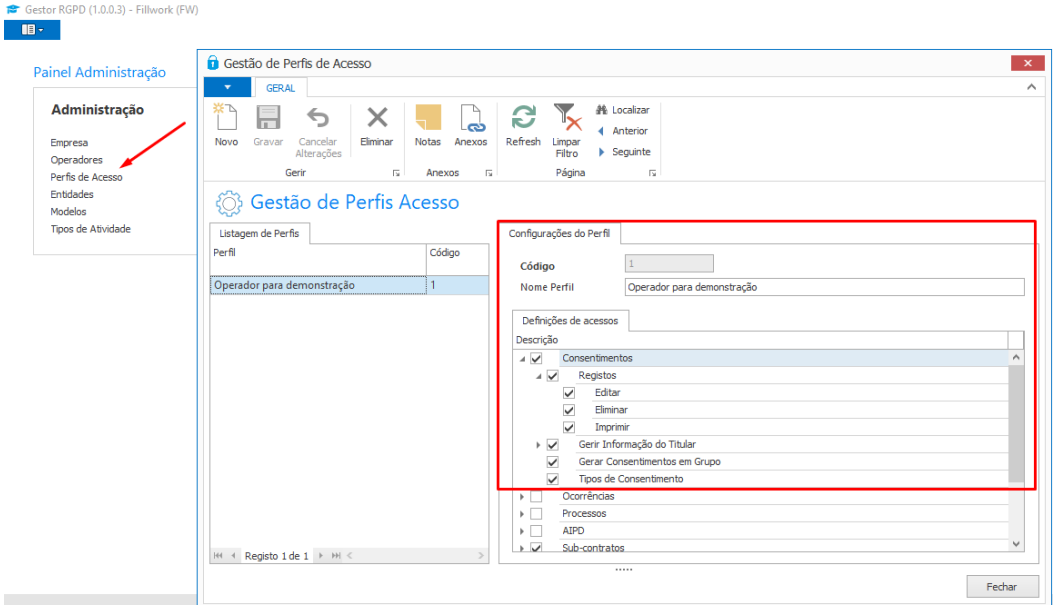
RESUMO DAS DINÂMICAS INCLUIDAS NESTA PLATAFORMA

Acessos dos Utilizadores | Documentos e Anexos | Anonimização dos Dados | Direitos dos Titulares

Consentimento | Comunicação | Logs e Rastreio das Alterações | Plataforma do DPO

Acessos dos Utilizadores

A gestão de acessos e perfis dos utilizadores foram revistos em todos os programas, esta alteração irá permitir definir com precisão as opçoes e os dados que cada operador poderá aceder. Será criado um utilizador para entrada nos programas, que terá de ser pessoal e intransmissivel e com palavra passe segura, deverá identificar inequivocamente o operador.



Cada programa tem agora, no seu menu de administração uma opção para definir quais os operadores que acedem ao programa e ainda quais as opções que o mesmo tem acesso (**perfil**).

Os programas Wincode que foram alterados e renovados para a conformidade com o RGPD, são:

WGAdmin | WEnsino | GAdmn3 | WHumanos | WContab | WCantina

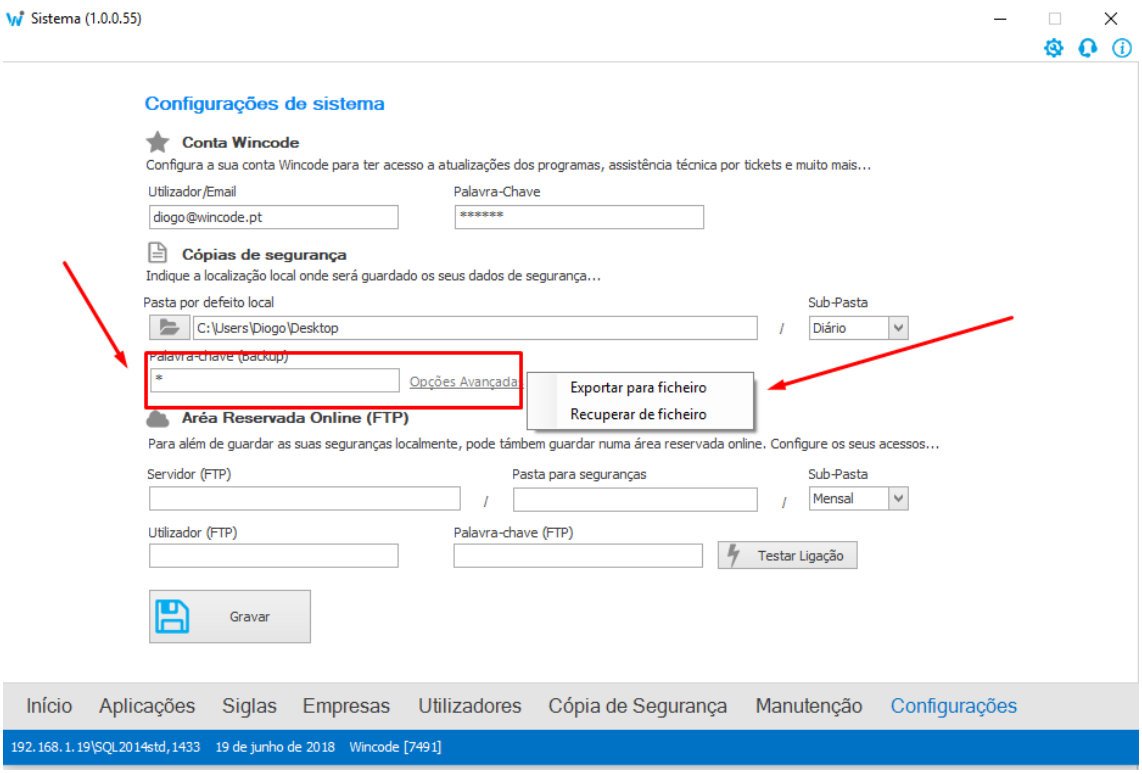
Todos estes programas foram renovados, na gestão dos **acessos**, na gestão dos **anexos**, nos **backups**, na gestão dos **logs** e das alterações, todos estão agora **interligados** com a plataforma do WRGPD, para gestão dessa vertente transversalmente. Teremos situações em que um mesmo titular, com dados em terceiros no WContab, também está como funcionário no WHumanos, por exemplo.

Documentos e Anexos

A funcionalidade de anexar documentos aos registos das aplicações, está agora melhorada e protege os documentos anexados aos programas, assim:

Ao selecionar e associar um documento em formato digital ao programa, por exemplo um PDF, um DOC ou um XLS, o programa irá **comprimir** esse documento, gerando um ficheiro ".zip" protegido com uma **palavra passe** segura. Esse documento ficará acessivel apenas pelo programa, não sendo possivel abrir sem a respetiva passe, que apenas o programa conhece.

Esta funcionalidade é transversal a todos os programas e será transparente para o utilizador, o sistema atua em relação à gravação e leitura, sem intervenção necessária do utilizador.

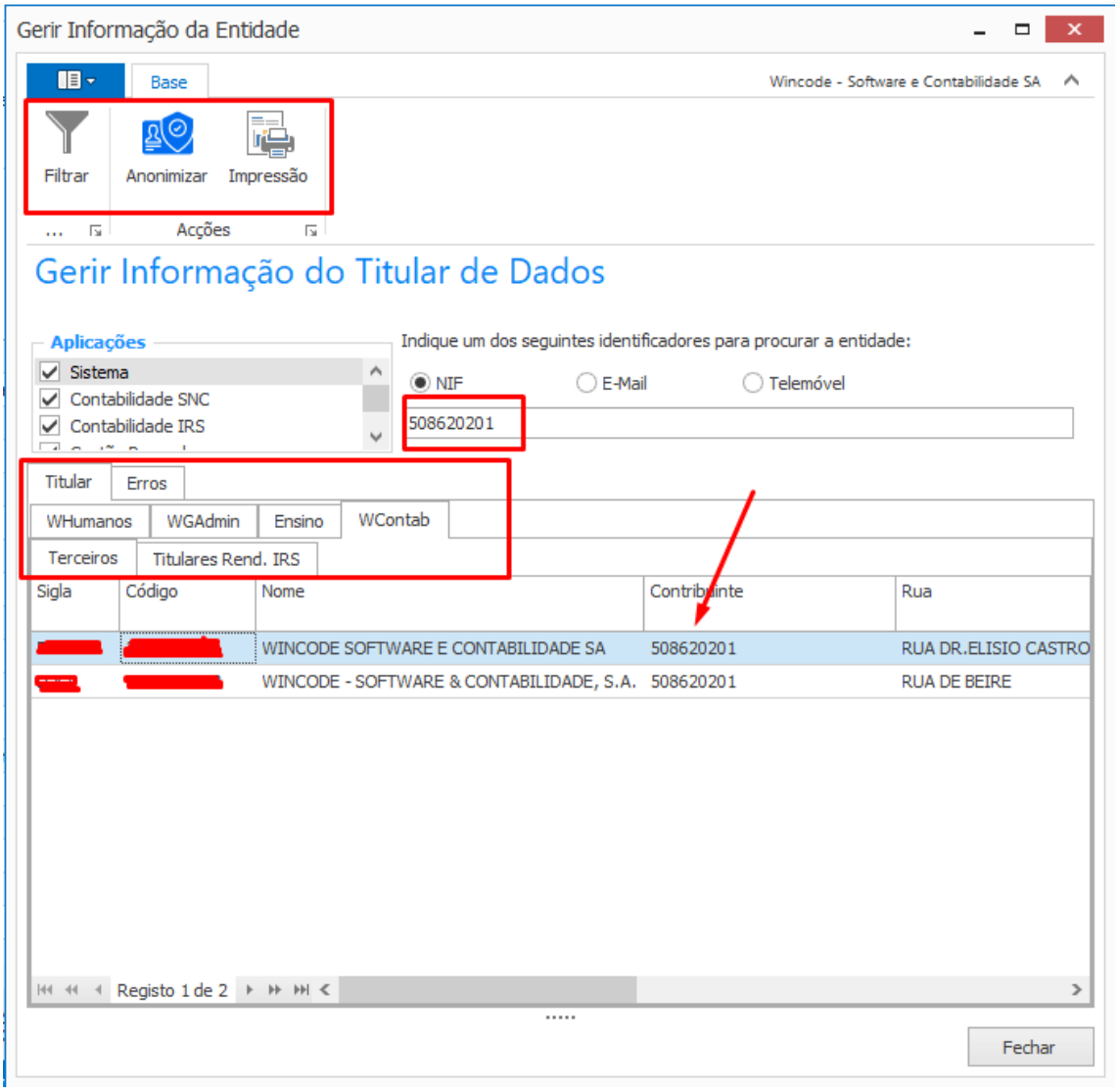


Neste quadro da configuração do sistema, é indicada a palavra para a proteção dos anexos e das seguranças, deve-se por segurança exportar essa palavra pass para um local fora do sistema, por exemplo um pen drive e guardar em sitio seguro.

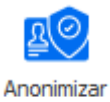
Os backups do sistema Wincode, também são comprimidos para formato ".zip" e protegidos com esta palavra passe.

Anonimização dos Dados

A proteção dos dados pode passar pela **pseudonomização** dos dados do titular, com esta funcionalidade o utilizador poderá tornar os dados do titular **anónimos**, sem comprometer a consistência da base de dados ou deteorar as estatisticas e análises às quantidades de registos ou ainda aos somatórios por critérios do utilizador.

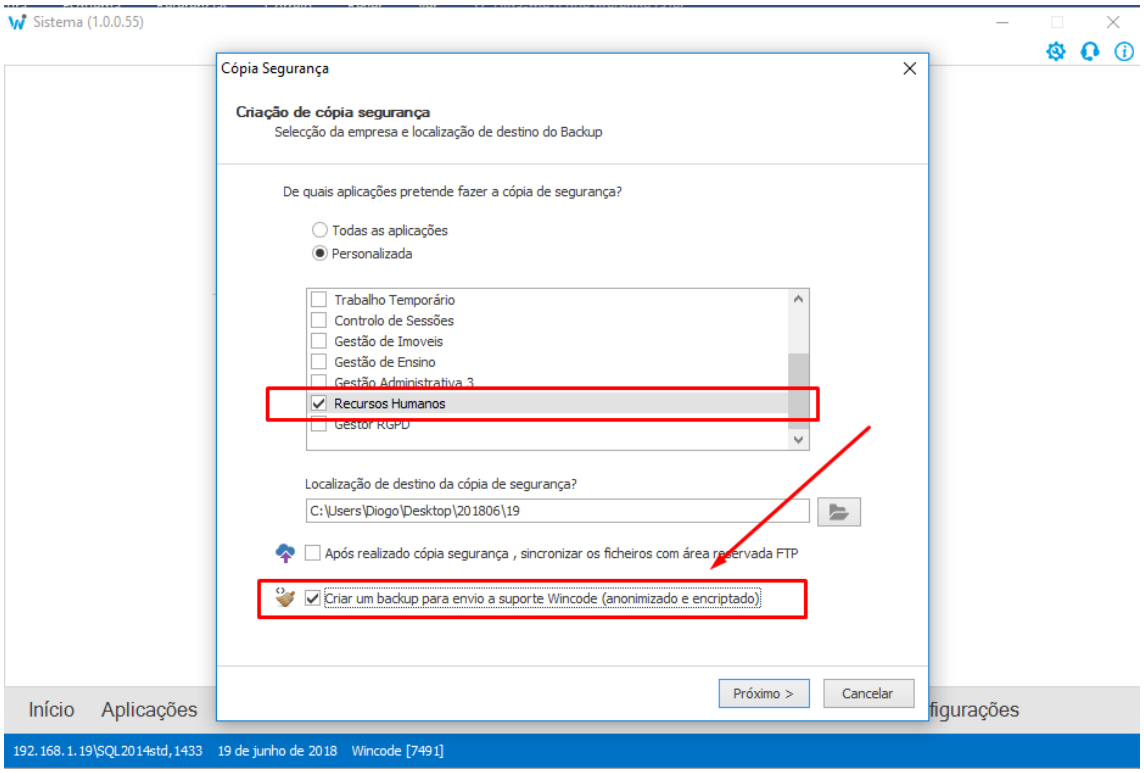


Na gestão do WRGPD pode ser consultada a informação que detemos sobre um determinado NIF, email ou telemóvel, o programa irá apresentar **todos os dados** que detemos dessa entidade, procura nas bases de dados dos **vários programas**, **ano atual** e também nos **anos anteriores**.
Neste exemplo procuramos pelo contribuinte "508620201" que é de uma pessoal coletiva que não está abrangida pelo regulamento, mas no caso de pessoal singular será idêntico.
Nesta opção o utilizador poderá selecionar para ver em conjunto os dados dos vários programas, "WHumanos", "WGadmin", "WContab" e "WEnsino", todos os dados serão apresentados.



A opção de "Anonimizar", vai marcar com "****" os campos de nome, morada, telefone, etc. dos registos consultados, tornando-os irreconheciveis, esta opção não tem retrocesso, **não pode desfazer**, deve ser utilizada com o devido cuidado.
A informação fica na mesma na base de dados, mas não será reconhecida.

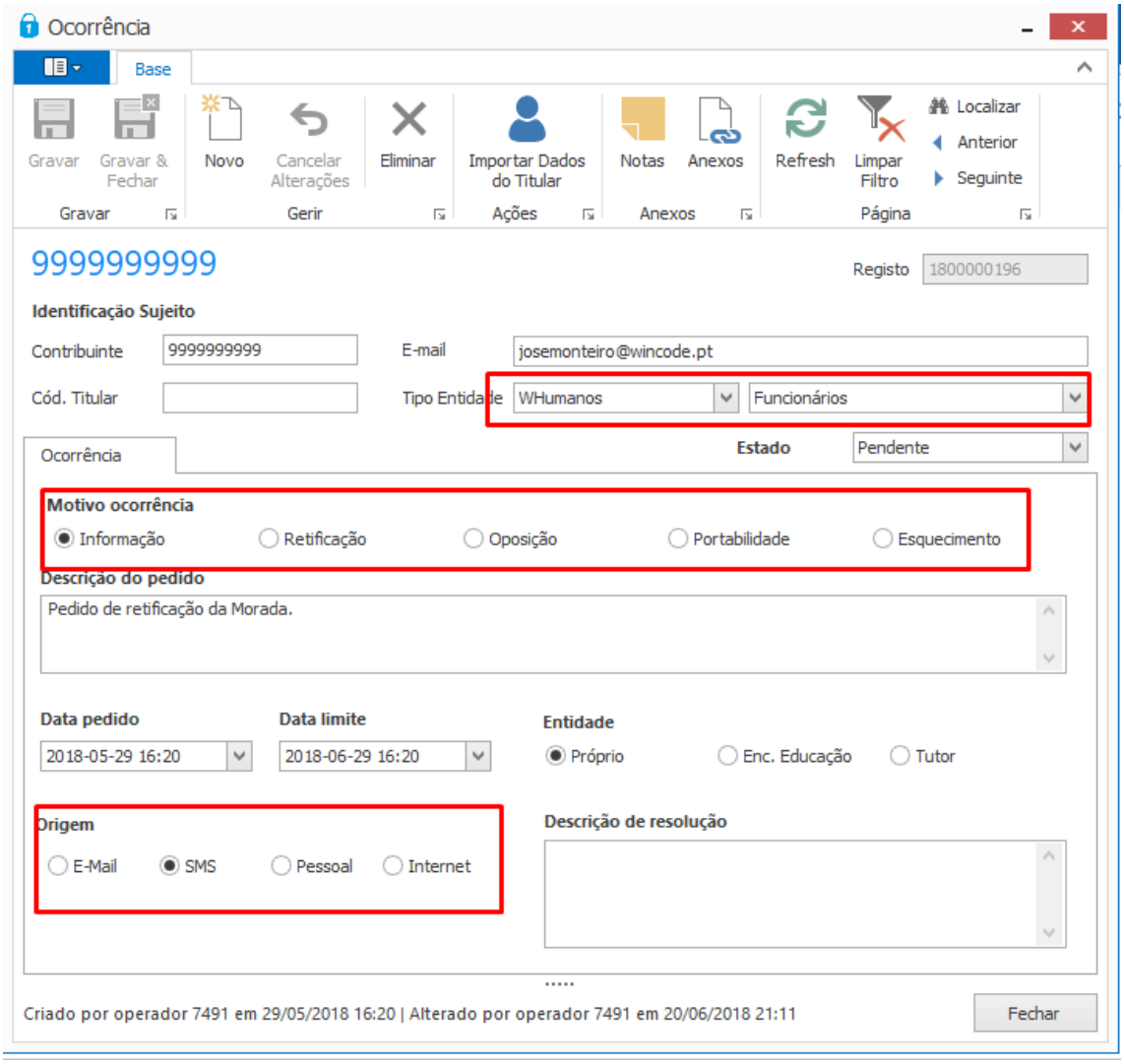
A pseudononimização pode também ser utilizada para o envio de uma base de dados para a assistência Wincode. Para que os técnicos da Wincode não tenham acesso aos dados das tabelas dos nossos clientes, quando estes nos enviam um backup para análise no nosso departamento de suporte ou de software, esse **backup é anonimizado**, e desta forma os dados que são transmitidos são totalmente **irreconhecíveis**, mas válidos para se testar alguma falha nas funcionalidades do programa e correção de erros.



Na execução da cópia de segurança para enviar para a Wincode o operador deverá selecionar a opção de **backup anonimizado**, conforme se apresenta na imagem.
Neste exemplo, será gerada uma cópia da base de dados de WHumanos, para ser enviada com completa segurança no envio e na proteção da informaçao a ser tratada.

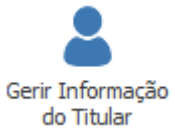
Direitos dos Titulares

Algumas das alterações mais importantes do regulamento tem a ver com os **direitos que o titular** dos dados tem sobre os mesmos, as empresas não são donas dos dados que lhes foram cedidos, "são apenas fieis depositários de dados".
Os titulares dos dados têm o direito de consultar, alterar, opor-se ao tratamento, direito ao esquecimento e à portabilidade, sobre os dados que temos dele.

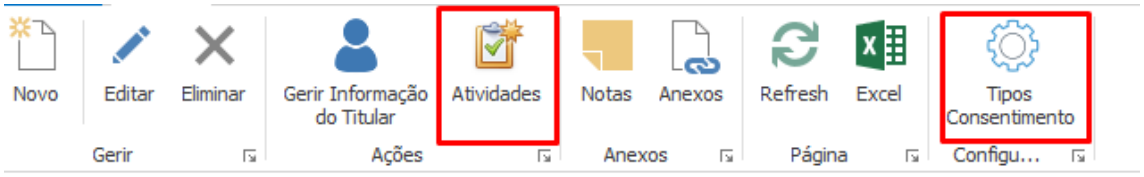


Neste quadro do WRGPD o DPO pode registar os pedidos dos titulares, ou então delegar esses trabalhos a um outro operador. Aqui será possivel gerir o prazo limite para dar resposta, informações dobre a origem do pedido, a sua ligação a algum dos programas Wincode, neste exemplo, temos a indicação da ligação à tabela de funcionarios do programa WHumanos.

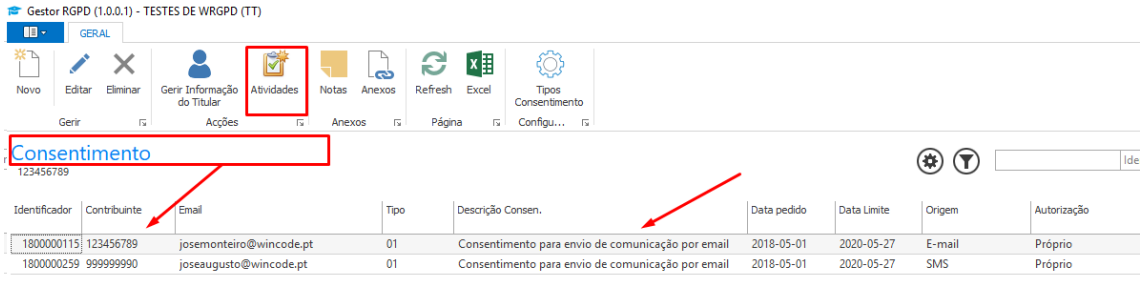
Os pedidos registados neste quadro devem ter sempre resposta e uma ação, o titular deverá acompanhar o que foi feito com esses dados. O pedido de **informação** deve dar origem a uma impressão ou envio sobre os dados que detemos desse titular.



Se for necessário o DPO ou quem este delegue, pode utilizar esta funcionalidade, **"Gerir Informação do Titular",** para aceder a todos os dados que estão nas nossas tabelas, e se for o caso, enviar esse resultado ao titular, ou então se o pedido era para "esquecer", poder anonimizar esses dados.
Este quadro deverá conter todas as interações com os titulares, nomeadamente na gestão dos seus direitos, registando ainda as atividades com estes ou então a ligação aos consentimentos.



Consentimento



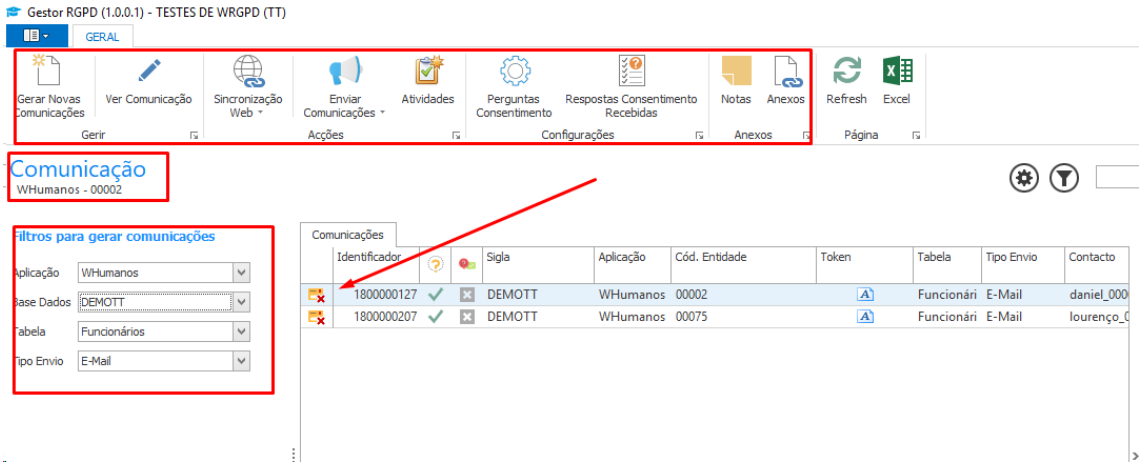
O **consentimento** será talvez a situação em que o programa WRGPD **mais poderá ajudar**, é talvez a parte mais dificil de gerir, é necessário que os programas Wincode que ligam com estes contribuintes, possam respeitar as autorizações e consentimentos que o titular dos dados forneceu, ou em caso negativo, respeitar essa vontade e não reter informação, elimina-la ou não enviar informação para este por email, SMS ou outro.

O principal trabalho é manter atualizados os registos de consentimento, para que os vários programas Wincode, WHumanos, WContab, WEnsino ou WGamin, possam consultar para nas ações e situações que carecem de consentimento, estes possam validar nesta tabela.

Para que todo o sistema possa funcionar, esta tabela terá que ter uma atualização automática e gerida em grupo, para que dessa forma, ela possa estar disponivel para consulta.

Sempre que o programa Whumanos for enviar, por exemplo, um email para um candidato com uma nova oferta de emprego na sua categoria ou area profissional, terá obrigatoriamente validar na tabela de consentimentos se temos autorização para esse envio.
Todos os programas Wincode terão de respeitar estas regra e efetuar estas validações.

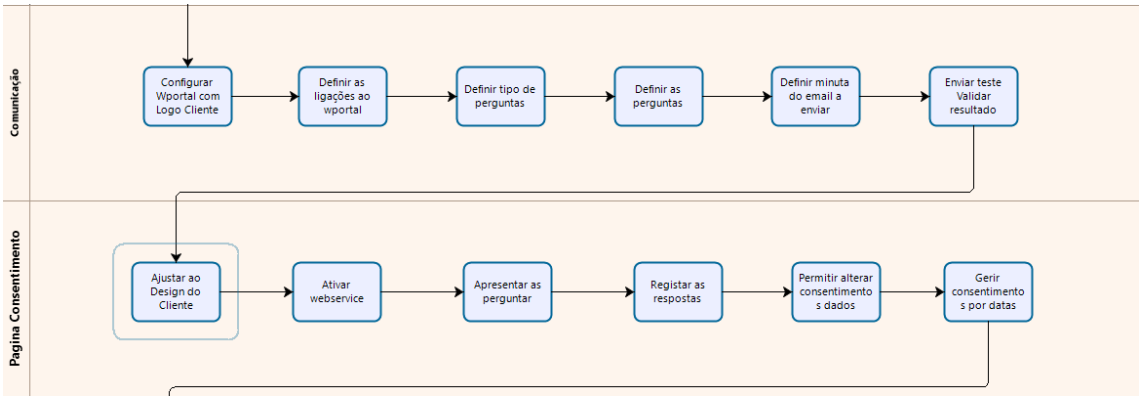
Comunicação



A **comunicação** tem um papel relevante na **obtenção do consentimento** dos titulares dos dados e as respetivas autorizações para o tratamento de dados pessoais.
Executa várias funções que permitem a gestão destas dinâmicas de forma simples e prática:

- Cria-se nas tabelas uma pergunta que se pretende que o titular dos dados, responda.
- Cria-se um modelo/minuta de um email ou SMS com a mensagem a enviar ao titular.
- Seleciona-se o programa e a tabela que contém os registos dos titulares a quem precisamos solicitar o consentimento.
- Geramos uma nova comunicação, e será enviado a cada titular um email com o texto que se definiu, junto com essa mensagem é enviado um link que contém um "token" ou identificador que vai identificar o titular.
- Em simultaneo é gerado um registo na página de internet que fica a aguardar a resposta que o titular queira dar.
- Quando o titular dos dados, responde à pergunta que está na página de internet, o programa recebe automaticamente essa resposta e regista-a para consulta por todos os programas.
- Quando o titular dos dados, segue novamente o link e altera a resposta, esta alteração é comunicada ao programa e provoca a alteração do consentimento se for o caso.

Diagrama que apresenta a sequencia de execução da comunição e registo das resposta.



Logs e Rastreio das Alterações

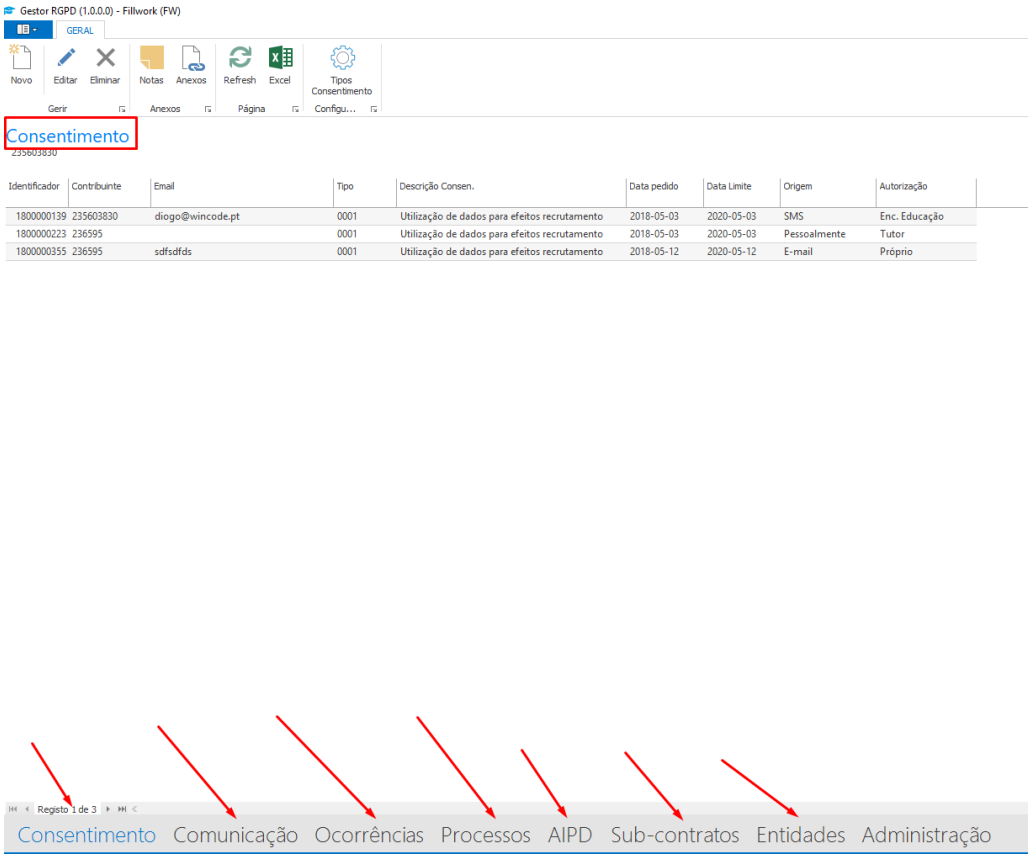
Nas configurações do WRGPD é possivel definir se vamos registar um log de todas as alterações efetuadas nas tabelas. Independente dessa configuração, a **gravação** da data/hora de criação e o operador que criou, assim como a data/hora da ultima alteração e também quem alterou, é **sempre efetuada**.
O regulamento indica que deverá haver um rastreio das alterações efetuadas aos registos protegidos por este documento. Nas empresas com menos de 250 trabalhadores (nº 5 do artigo 30º, do regulamento) esta obrigação não é obrigatória.
De toda a forma, as dinâmicas da plataforma WRGPD e dos programas Wincode que tratam dados protegidos, são rigorosos na gravação de quem alterou e quando.

Plataforma do DPO

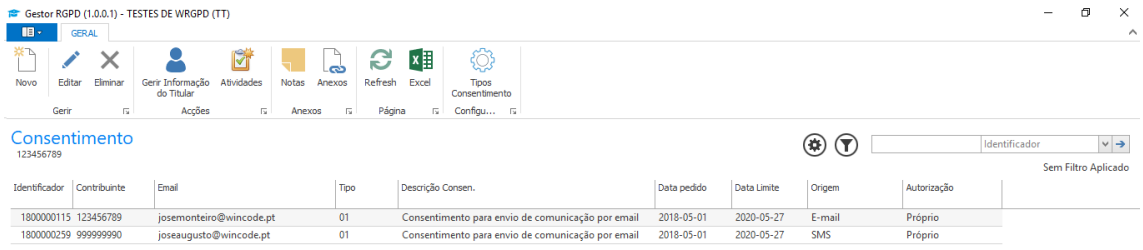
O WRGPD é no essencial a **ferramenta do DPO**, será com este software o DPO poderá gerir todas a atividades inerentes ao regulamento, quer sejam referentes a **direitos do titular**, **registo de ocorrências** sobre o tratamento de dados, **reclamações** ou alertas e **comunicações** de inconformidades com o regulamento por parte dos titulares ou pelas as instituições de fiscalização, Pode ainda registar e gerir o resultado de analises de impacto com a proteção de dados.
O programa prevê ainda a gestão dos contratos com subcontratantes e ainda com os proprios colaboradores.

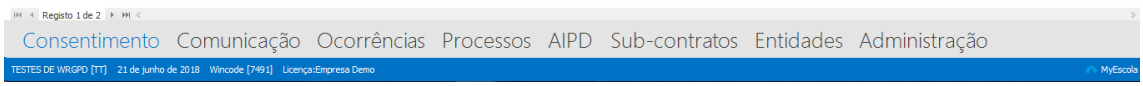
De seguida apresenta-se os quadro de algumas das funcionalidades disponibilizadas pela plataforma:

Quadro do menu principal com os acessos a todas as opções do módulo.

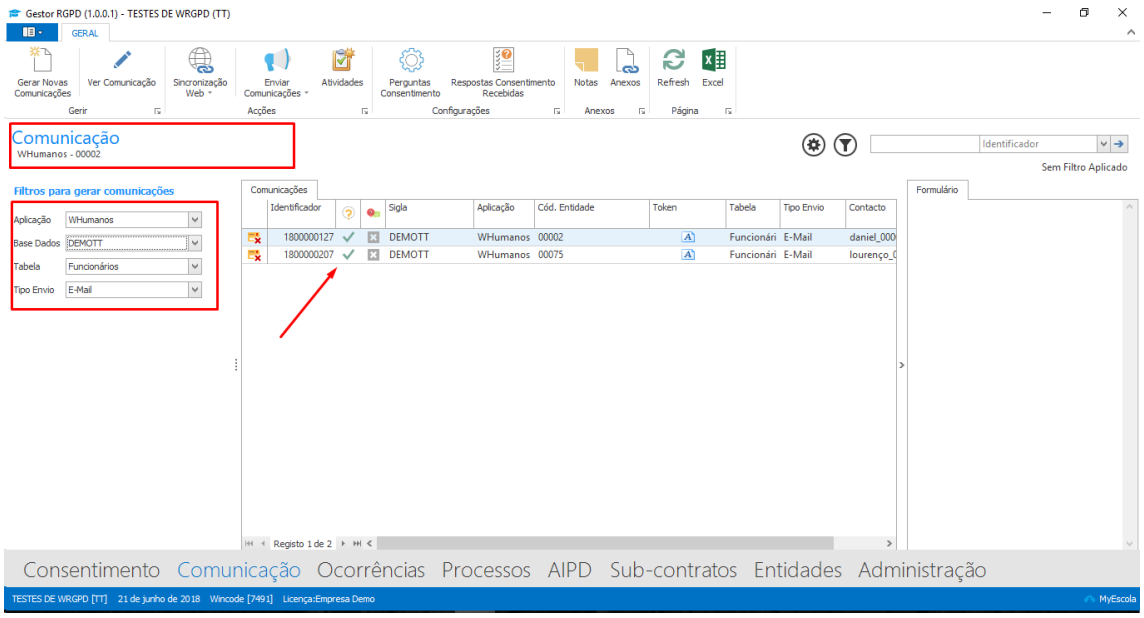


Quadro da gestão do consentimento, apresentação da informação sobre todos os consentimentos registados no programa, autorizações de tratamento, prazos, etc.

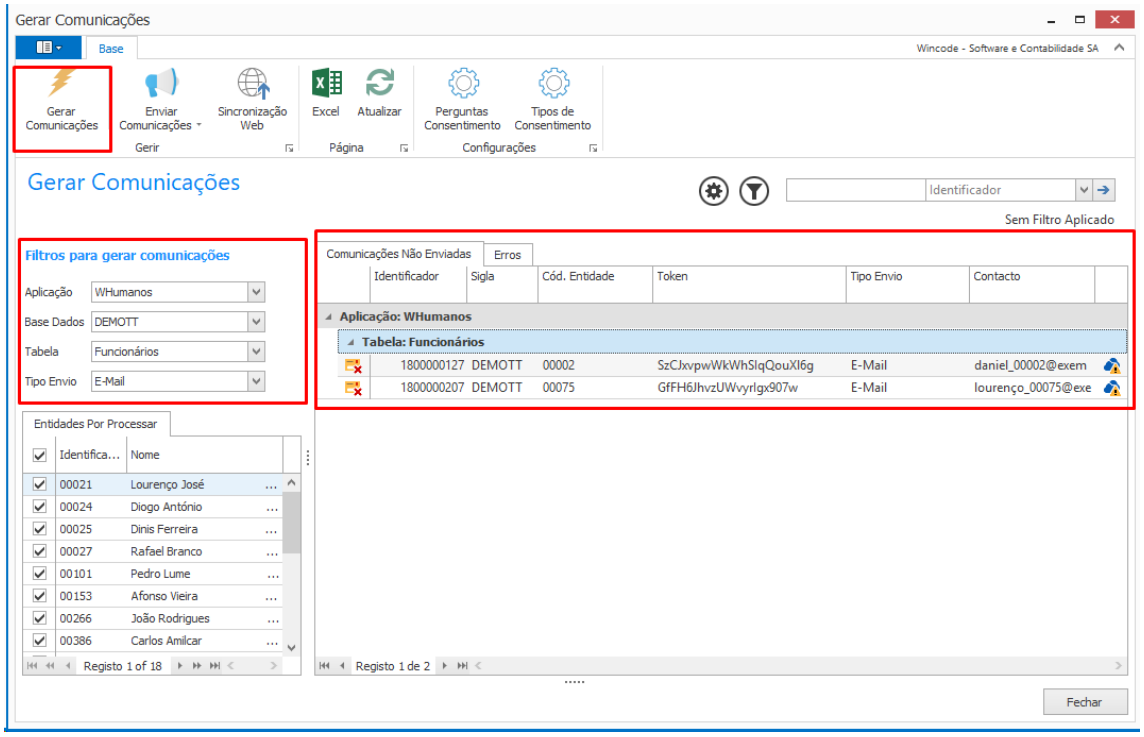




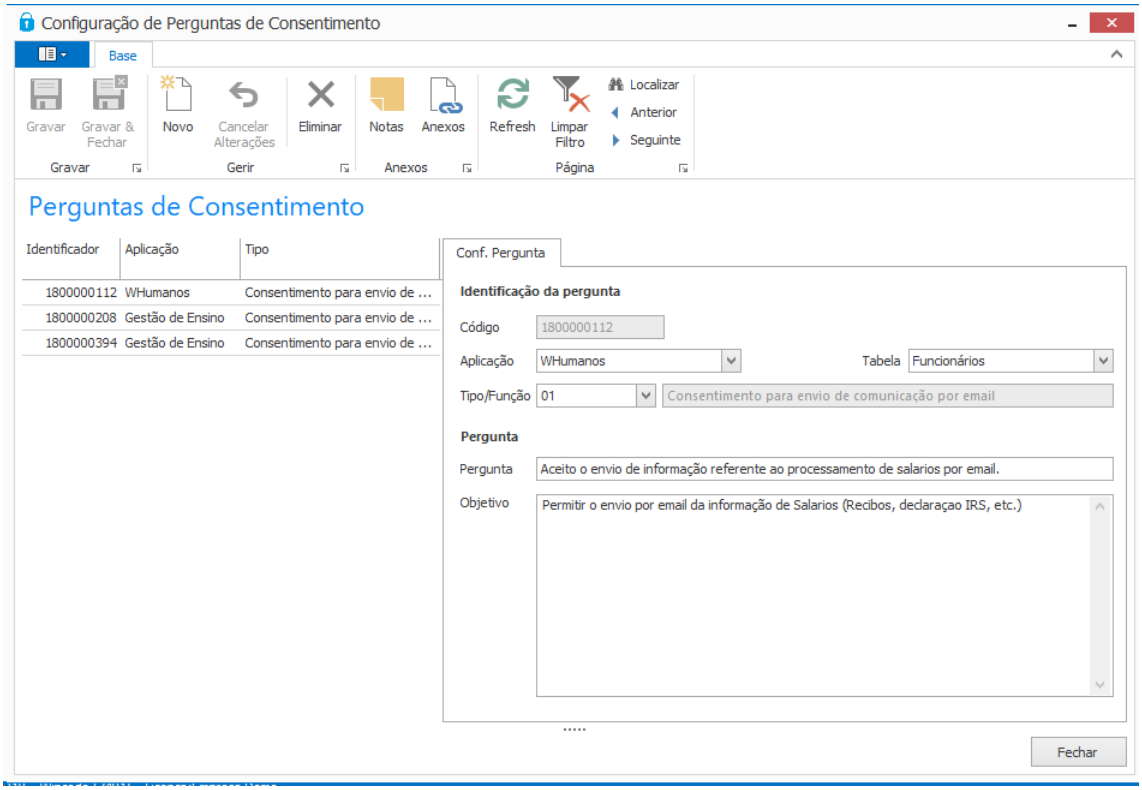
Comunicação com os titulares dos dados, envio de mensagens parta obtenção do consentimento, gestão das respostas e do estado da comunicação.



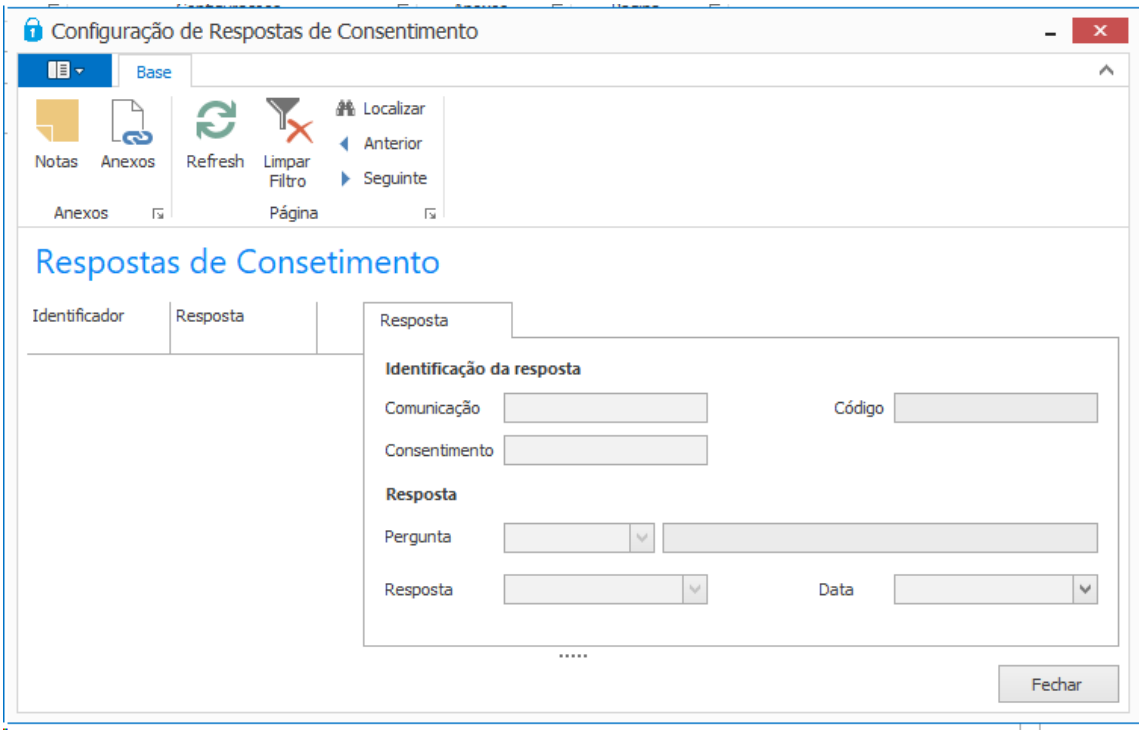
Geração de uma nova comunicação, enviar aos titulares dos dados, baseado nas tabelas de um dos programas.



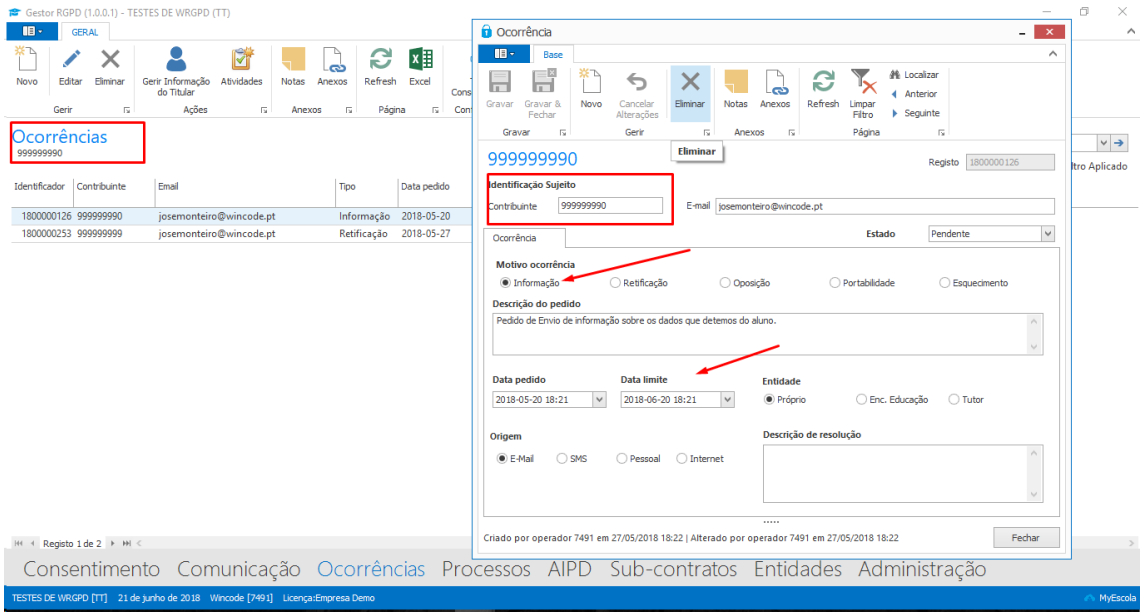
Configuração e criação das perguntas a utilizar na mensagem a enviar aos titulares dos dados.



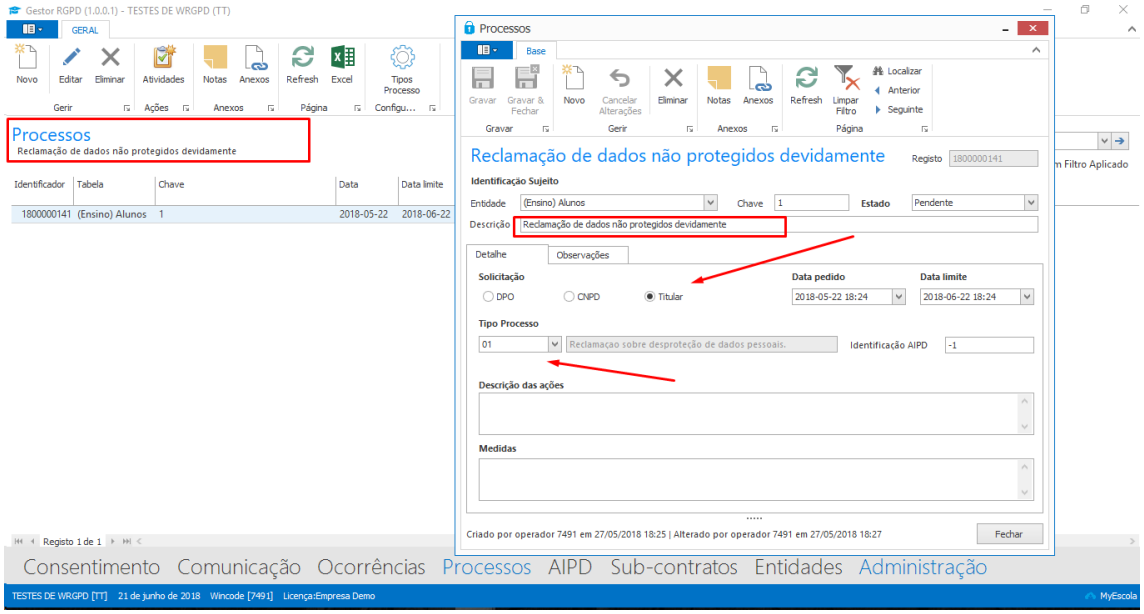
Consulta das respostas obtidas com a comunicação.



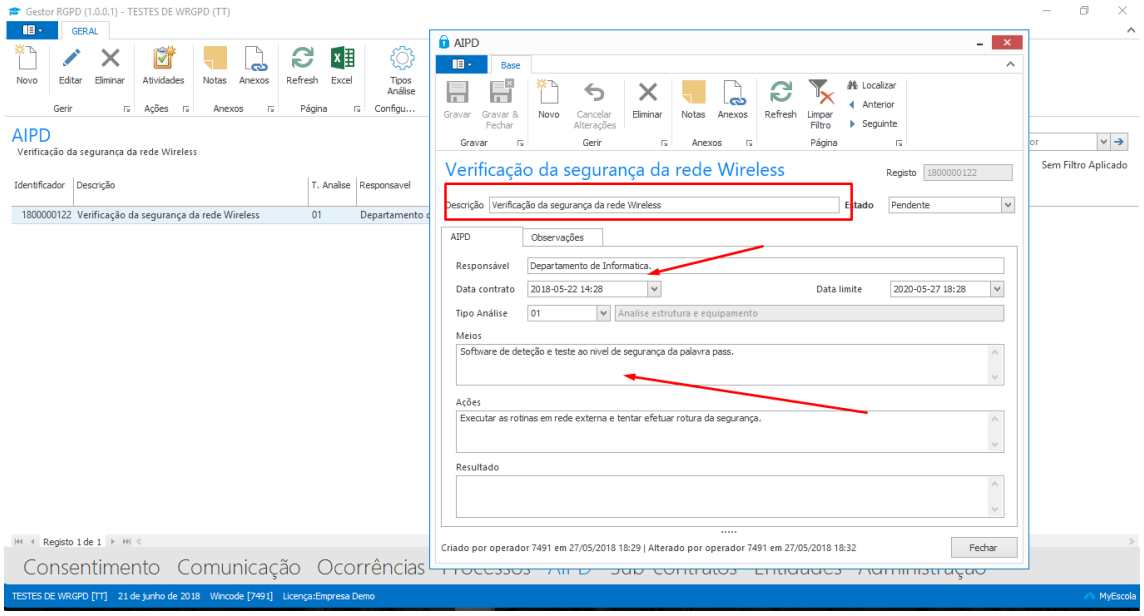
Gestão das ocorrências sobre o tratamento dos dados e solicitações efetuadas pelos titulares dos dados.



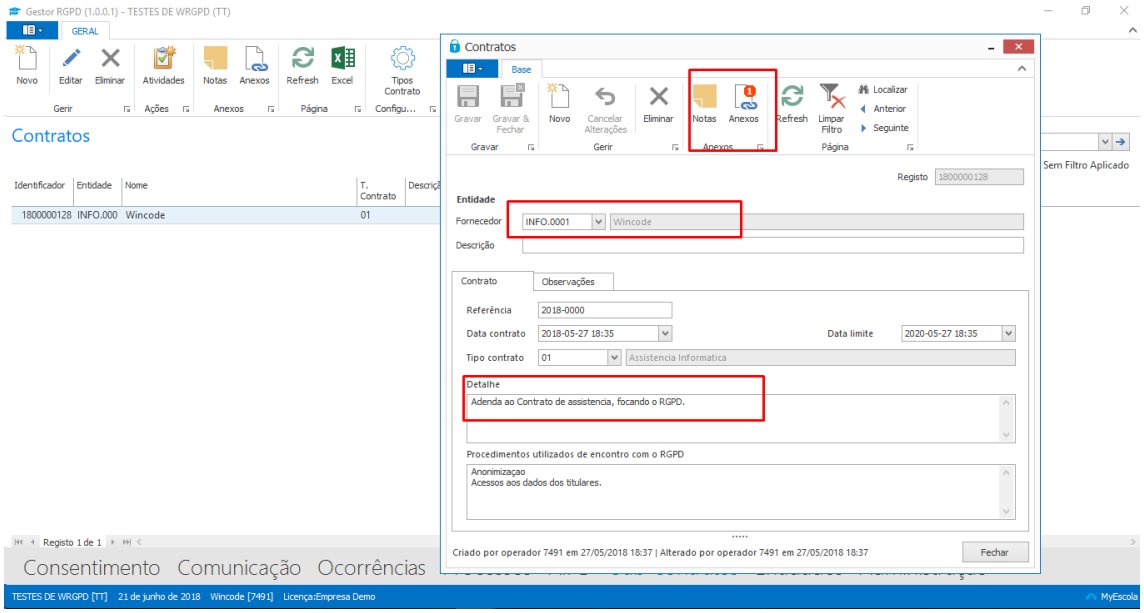
Reclamações dos titulares dos dados sobre anomalias ou inconformidades sobre o tratamento dos dados, por exemplo: utilização não autorizada.



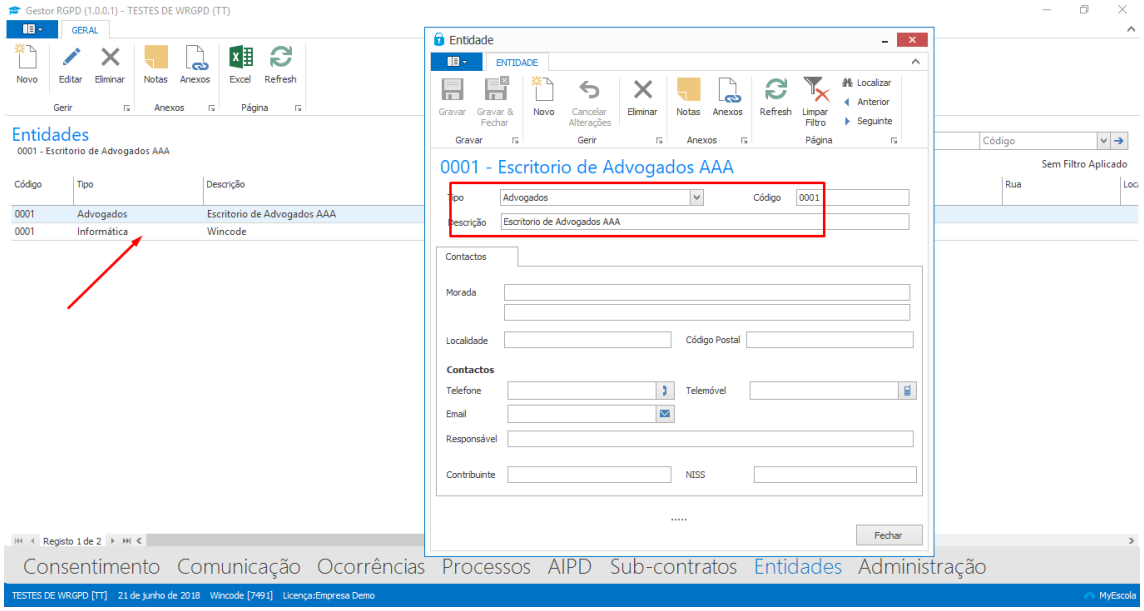
Registo de ações despoletas pelo DPO ou outros para verificação previa do impacto sobre a proteção de dados de um tratamento novo ou tratamento de rotina para verificação da conformidade com o regulamento.

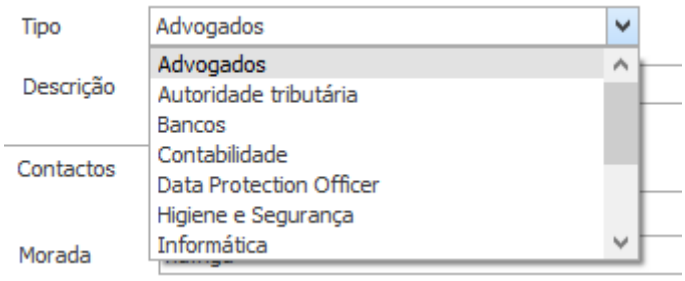


Registo dos contratos com os fornecedores de serviços que intercetam com a proteção de dados.

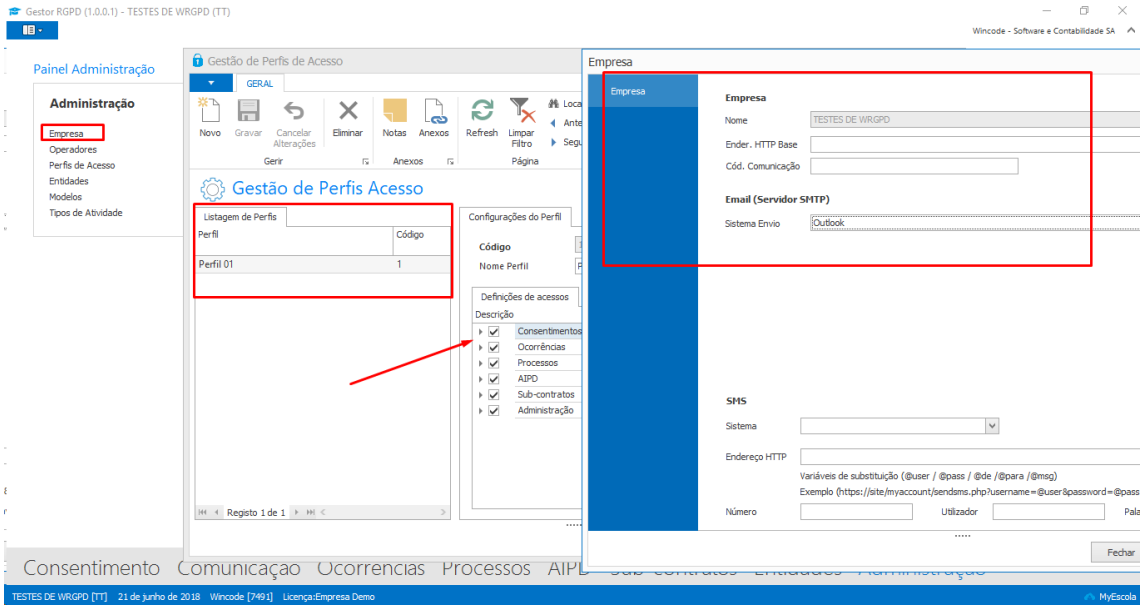


Criação de Novas entidades com ligação à empresa e que eventualmente terão acesso a dados protegidos pelo regulamento.





Configuração do portal onde serão apresentadas as mensagens das comunicações.



FIM