GUIA DE APLICAÇÃO

O RGPD PARA AS EMPRESAS DE CONTABILIDADE E OS CONTABILISTAS CERTIFICADOS

MAIO 2018

ORDEM DOS CONTABILISTAS CERTIFICADOS

Introdução

O Regulamento Geral de Proteção de Dados (RGPD) é a lei de privacidade que defende os residentes europeus dos comportamentos menos apropriados por parte de empresas no que diz respeito aos seus dados pessoais.

Desta feita, todas as empresas e profissionais que lidem com dados pessoais deverão aplicar regras e comportamentos que estejam em conformidade com a nova lei.

Este manual é direcionado aos Contabilistas e PME de Contabilidade.

Para um bom seguimento do mesmo é necessário ter conhecimentos de base do RGPD, tais como descritos no "Guia Prático de RGPD" que este acompanha.

Neste guia não são abordados temas jurídicos. Apenas são relatados os princípios básicos do RGPD, os direitos dos titulares dos dados, os conceitos básicos de aplicação (baseados e mapeados precisamente nos Princípios e nos Direitos) e finalmente um exemplo de aplicação numa empresa fictícia que pretende representar a grande maioria das PME de Contabilidade.

Princípios básicos do RGPD

Os dados pessoais são toda a informação relativa à identificação ou que possam levar à identificação do seu titular de forma direta ou indireta.

Exemplos de dados pessoais:

- Nome
- Número de identificação
  - BI, NIF, carta de condução, Passaporte.
- Endereços de identificação e localização
  - Físicos como por exemplo a morada
  - Eletrónicos: endereço de *email*, página web, página de Facebook, etc...
- Biométricos
  - Altura, peso, conotações físicas diversas
  - Genética
- Saúde
  - Síndromas, doenças
  - Desempenho físico ou mental
  - Dados de diagnósticos como pressão arterial ou ECG

- Económicos
- Culturais
- Sociais
- Políticos

Para compreender o RGPD é necessário conhecer os princípios básicos sobre os quais está construído:

- Legalidade, justiça e transparência
  - Os dados pessoais devem ser processados de forma legal, justa e transparente em relação à pessoa em causa
- Limitação de propósito
  - Os dados pessoais devem ser recolhidos para fins específicos, explícitos e legítimos e não devem ser processados de forma incompatível com esses fins.
- Minimização de dados
  - Os dados pessoais devem ser adequados, relevantes e limitados ao necessário em relação aos fins para os quais são processados.
- Precisão
  - Os dados pessoais devem ser precisos e, sempre que possível, mantidos atualizados
- Limitação de armazenamento
  - Os dados pessoais devem ser mantidos num formato que permita a identificação dos titulares de dados por não mais do que o necessário para as finalidades para as quais os dados pessoais são processados.
- Integridade e confidencialidade
  - Os dados pessoais devem ser processados de uma maneira que garanta a segurança apropriada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, usando medidas técnicas ou organizacionais apropriadas.
- Imputabilidade
  - O controlador deve ser responsável e demonstrar a conformidade com o RGPD.

Direitos do titular dos dados

Quem é o "Titular dos dados"? Qualquer pessoa particular aos quais os dados fazem referência. Somos todos nós enquanto residentes europeus.

Com o RGPD o "titular dos dados" adquire os seguintes direitos:

- O direito a ser informado sobre a forma como os seus dados são utilizados
- O direito de acesso aos seus dados sem qualquer custo ou demora
- O direito à retificação dos seus dados em caso de incorreção
- O direito a ser esquecido / apagado
- O direito à restrição de processamento dos seus dados para qualquer outro fim que não o referido aquando da sua obtenção
- O direito à portabilidade dos dados, ou seja, a obrigação por parte da empresa de fornecer os dados na totalidade num formato digital de fácil acesso (como Zip ou CSV)
- O direito à objeção da utilização dos dados para qualquer outro fim que não o referido aquando da sua obtenção.
- Direitos relacionados com o processamento automático dos dados, ou seja, o direito a uma intervenção humana no processamento.

Estes direitos podem ser garantidos de forma automática ou através do *Data Protection Officer*.

Estes direitos não se aplicam apenas a dados digitais bem como aos dados em formato físico.

Conceitos básicos de aplicação

Para uma boa aplicação do RGPD deverá pensar nestes princípios e direitos como mandamentos.

Quando tiver de introduzir dados no seu sistema, alterar esses dados, efetuar uma qualquer operação de envio ou transmissão, etc... deverá pensar sempre se a ação que está prestes a executar está a quebrar algum destes princípios ou dificultar a aplicação dos direitos.

Para que os princípios sejam de facto aplicados de forma natural e os direitos concedidos de forma ágil e atempada deverá embarcar no processo de aplicação prática do RGPD.

Podemos considerar o início da aplicação do RGPD como o "Ano Zero" no que diz respeito à conformidade. Os métodos anteriores à aplicação do RGPD são sujeitos a ações corretivas e reativas, mas a partir do momento em que se aplicam os métodos e as diretivas estamos sujeitos aos procedimentos e devemos cumpri-los.

De forma simplificada, é necessário:

- Verificar se os requisitos de segurança mínimos estão a ser cumpridos na empresa tanto em termos passivos (segurança de rede) como ativos (comportamentos dos trabalhadores), digitais ou físicos.
- Verificar se as ferramentas informáticas permitem a aplicação do RGPD.
- Criar procedimentos que ajudem os trabalhadores da empresa a cumprir com os princípios e com a aplicação dos direitos.
- Criar procedimentos que contemplem incidentes e como atuar em caso de fugas de informação ou não conformidades.
- Consciencializar e formar as pessoas para que cumpram com todos procedimentos.

Este processo pode tornar-se complexo à medida que vai avançando, mas a sua aplicação básica tem por base quatro passos essenciais:

- **Levantamento**: identificação dos dados pessoais que são processados na empresa.
- **Proteção**: estabelecimento de controlos de segurança e rastreabilidade.
- **Controlo**: gestão de como os dados são adquiridos, acedidos e processados.
- **Relatório**: ações requisitadas pelos titulares dos dados e documentação.

Dependendo do volume dos dados processados, uma empresa poderá necessitar de ter um *Data Protection Officer*. Não existe um número específico na lei que defina de forma clara a necessidade de ter um DPO. Porém, podemos inferir que, caso uma empresa processe um volume significativo de dados ao ponto de por em risco centenas de titulares de dados, muito provavelmente será obrigado a nomear um DPO para garantir que os processos são postos em prática e que a reatividade em caso de solicitação da ativação dos direitos por parte dos titulares é cumprida atempadamente e da forma mais eficaz.

Cabe também ao DPO iniciar a jornada de aplicação do RGPD seguindo os quatro passos essenciais mencionados acima.

O DPO pode ser uma pessoa com vínculo laboral à empresa ou externo, mas deverá ter sempre um vínculo contratual. No contrato deverá constar qual o limite de responsabilização do DPO, tendo sempre em conta que o responsável máximo para a aplicação do RGPD serão os gerentes da empresa. O DPO será sempre responsável pela estratégia de aplicação, mas a aplicação em si, as decisões em caso de incidente e eventuais não conformidades ou violações serão imputadas ao sujeito responsável pelo processamento e, em ultima instância, como referido acima, à gerência da empresa.

Levantamento

Quando se inicia o processo de levantamento é necessário envolver todas as pessoas (ou pelo menos uma amostra significativa) que lidam com dados pessoais no seu dia a dia.

Regra geral os dados passam pelo seguinte ciclo de vida:

- **Aquisição dos dados**: quando os dados passam a constar no nosso sistema.
- **Processamento e utilização**: quando os dados são acedidos, utilizados ou alterados para o negócio.
- **Remoção ou arquivo**: quando os dados chegam ao final da sua vida útil e serão arquivados ou removidos.

Estes dados residem nos nossos sistemas em forma física ou digital.

Devemos detetar:

- Durante a aquisição
  - Que dados são adquiridos
  - Para que localização são adquiridos
    - Exemplo: Excel, base de dados, CRM, ERP, etc...
- Durante o processamento
  - Que ações são efetuadas sobre os dados:
    - Exemplo: processamento de salários, exportação para ficheiros diversos, cópia, envios, por que métodos, etc...
  - Se todos os dados constam no processamento ou apenas alguns
- No final do ciclo de vida
  - Se efetivamente os dados estão a ser eliminados de forma eficaz e de todas as localizações.

Os objetivos do levantamento passam por:

- Conhecer o ecossistema dos dados e saber onde residem
  - Assegurar que estamos a centralizar os dados para que a gestão dos mesmo seja o mais simplificada. É má prática adquirir os dados e copiá-los para diversos sistemas (base de dados, *excel*, CRM, todos ao mesmo tempo). Em caso de retificação por exemplo o processo não é ágil e podemos estar a provocar incongruências internas nos dados.
- Verificar que as ferramentas informáticas utilizadas estão em conformidade
- Verificar a aplicação dos princípios e dos direitos durante o ciclo de vida dos dados
  - Por exemplo: verificar se estamos a recolher demasiados dados ou dados inúteis. Assegurar que a forma e os locais onde os dados estão a ser guardados permitem garantir os direitos de forma atempada e ágil.

» Assegurar que aquando da aquisição o Titular dos Dados está a ser informado sobre o destino e processamento dos seus dados e que temos prova do seu consentimento

» Otimização em geral

- Devemos pensar no passo seguinte da aplicação que é a **Proteção**. Os dados devem ser otimizados para que seja possível protege-los de forma apropriada.

Como referido acima, estamos traçar o "Ano Zero", logo:

» Os dados que existentes devem ser otimizados para que se possa cumprir com o RGPD

- Migrando bases de dados se necessário
- Centralizando os dados o mais possível
- Removendo os dados obsoletos
- Atualizando as aplicações

» Os dados adquiridos no futuro

- Criando procedimentos e regras internas para que os dados possam ser colocados nos locais corretos e da forma apropriada.

Proteção

Após o levantamento e otimização, devemos então iniciar a fase de proteção.

Nesta fase iremos verificar se os dados se encontram protegidos da forma apropriada e se de facto as ferramentas informáticas que possuímos possibilitam o grau de proteção necessário segundo a aplicação do RGPD na nossa empresa.

Na maioria dos casos as PME de Contabilidade possuem uma rede interna.

A proteção de uma rede e dos seus recursos deve ser sempre considerada de forma modular e em camadas

De fora para dentro podemos considerar:

» A proteção do perímetro da rede:

- Proteção contra ataques utilizando *firewalls* ou outros métodos de prevenção de acesso não autorizado no perímetro (acesso à internet) da rede

» A proteção dos dispositivos

- Através de *firewalls*, anti-virus ou outro *software* de prevenção de acesso ou segurança, mas instalado diretamente no dispositivo

» Proteção dos recursos partilhados pelo dispositivo

- Controlo de acessos por via de autorização baseada na autenticação

» Proteção das aplicações

- Normalmente atingido de forma programática pela própria aplicação disponibilizada pelo servidor

Para aceder aos recursos de rede, os utilizadores dos PC devem usar um nome de utilizador e uma *password*.

Este conceito de "autenticação" e de "identidade do utilizador" é a pedra angular da proteção dos dados. Toda a rastreabilidade do acesso aos dados assentam sobre a autenticação e a identidade. É com base neste conceito que devemos criar ou afinar os procedimentos de proteção de dados.

Imaginemos então que os dados estão guardados numa base de dados num servidor *Windows*. Devemos garantir que apenas os utilizadores que efetivamente necessitam de acesso aos dados podem aceder a esta base de dados.

Caso a base de dados esteja guardada num ficheiro partilhado numa pasta, podemos utilizar as funcionalidades do *Windows Server* para garantir que apenas os utilizadores autorizados terão acesso. Assim apenas os utilizadores poderão de facto executar a base de dados. Ainda assim podemos aplicar outra camada de proteção, por exemplo, se se tratar de uma base de dados em Access, aplicando uma *password*. Neste caso, mesmo que um utilizador consiga executar a base de dados, apenas terá acesso à mesma se conhecer a *password*.

Relativamente à rastreabilidade, os servidores Windows permitem ativar o sistema de "logging" sobre ficheiros e assim guardar informações sobre os acessos de escrita ou leitura a uma pasta ou a um ficheiro específico.

Caso tenhamos um software de CRM ou ERP, dado que normalmente estes possuem um sistema de autenticação que assenta no *user* e *password* utilizado aquando do *logon* no PC, ou então um sistema autónomo. Em ambos os casos este tipo de *software* tem, geralmente, um sistema de *logging*, não apenas nos acessos à base, bem como de acesso aos dados, podendo registar, quem acedeu a que dados e que ações efetuou sobre os mesmos.

Veremos mais adiante, na aplicação prática, formas mais comuns de proteção dos dados.

É necessário também ter em atenção que a proteção também passa pelos comportamentos dos utilizadores. Podemos aplicar todos os mecanismos de proteção possíveis que tivermos à disposição, mas se os utilizadores partilharem as senhas de acesso e proporcionarem acessos não autorizados, como por exemplo abrindo anexos maliciosos por *email*, toda a proteção cai por terra.

A proteção assenta também na prevenção.

Controlo

Nesta fase pretende-se criar efetivamente procedimentos que, assentando nos dois pontos anteriores, permitam cumprir com os princípios e direitos.

É nesta fase que iremos criar *workflows* que permitem a formação dos utilizadores e eventualmente a automatização dos processos.

Por exemplo:

- Procedimento de aquisição de um novo cliente
  - O cliente assina o contrato de prestação de serviço onde deverá constar:
    - Quais os dados que serão recolhidos
    - Qual o propósito da recolha dos dados
    - Por quanto tempo os dados serão guardados
  - O pedido explícito de consentimento para os processamentos mencionados
  - Um ou mais endereços de *email* considerados fidedignos pelo cliente
  - Caso o processamento dos salários dos trabalhadores faça parte do serviço também pode constar o procedimento de envio dos recibos, mencionando
    - Que serão transmitidos apenas ao endereço de *email* especificado no contrato salvo exceções expressamente pedidas pelo cliente
    - Que serão encriptados e protegidos por *password* e que esta não será transmitida por mail.
- Procedimento de alteração de dados
  - De que forma o cliente pode pedir a alteração dos dados
  - Aquando da entrada do pedido como alterar os dados e utilizando que métodos e ferramentas
  - Como, e o que, deve ser comunicado ao cliente depois da alteração
- Como proceder em caso de pedido de ativação de outro direito

Relatório

Nesta fase criamos métodos de relação para que durante todas as fases da aplicação do GDPR existam métodos efetivos de rastreabilidade.

Devemos, por exemplo, ter relatórios para registar incidentes e não conformidades detetados, tal como ataques, divulgação involuntária de dados, etc...

Estes relatórios são normalmente criados e preenchidos pelo DPO.

EXEMPLO DE APLICAÇÃO PRÁTICA

Sistemas, Procedimentos e fluxos de dados influenciados pelo RGDP

Em qualquer empresa existem procedimentos que geram fluxos de dados. Poderíamos dizer que todos os fluxos de dados que contivessem dados pessoais devem ser manuseados debaixo do prisma do RGPD. Contudo, para compreender mais a fundo a mentalidade exata e o objetivo do RGPD podemos dizer que todos os fluxos de dados que, direta ou indiretamente, tenham a capacidade de revelar informação pessoal sobre os visados nos mesmos devem manuseados por forma a minimizar o risco de uma divulgação indevida.

Tendo em conta esta premissa podemos considerar, a título de exemplo, os seguintes sistemas, procedimentos e fluxos existente geralmente numa PME de Contabilidade ou executados no dia-a-dia por um Contabilista.

Sistemas informáticos envolvidos

Podemos começar com a descrição dos cuidados que é necessário ter com os sistemas informáticos, no que diz respeito ao RGPD.

Há dois princípios essenciais para todo e qualquer sistema, em termos de segurança:

- Controlo de acessos
- Rastreabilidade

Estes dois princípios devem ser aplicados aos seguintes sistemas, porém, para cada um deles é necessário ter em atenção outros fatores, como descrito abaixo:

- Sistema de autenticação
- Base de dados de clientes
- *Software* de faturação
- *Software* de processamento de salários
- Servidores de partilha ficheiros
- Impressoras
- Terminais (PC Fixos, *Laptop, Tablets e Smartphones*)
- Sistema de acesso à internet
- Sistema de acesso externos

Sistema de autenticação e identidade

O sistema de rede normalmente tem como base um *Windows Domain*. Com este método, os utilizadores do sistema necessitam de ter um nome de utilizador e palavra passe para aceder aos recursos da rede.

Com o advento da *cloud* este tipo de sistema passou a existir na internet em vez de necessitar de servidores dedicados dentro da empresa.

No caso de existir um *Windows Domain*, todos os acessos aos recursos do sistema são geridos através do de um servidor central. Logo pode-se controlar o acesso aos ficheiros e recursos guardados no servidor.

Software de faturação, processamento de salários, e outros, normalmente possuem um sistema próprio de identidade, daí a necessidade de usar um *user* e *password* para aceder ao *Windows*, por exemplo, e outro para aceder ao PHC ou Primavera.

O importante é compreender que existem mecanismos que nos permitem aplicar a rastreabilidade de acessos tanto às aplicações como aos ficheiros, com base na identidade do utilizador, tanto ao nível do *Windows* como ao nível das aplicações.

Caso não exista qualquer sistema de acesso centralizado deverá ser feito um esforço adicional para aplicar o princípio da rastreabilidade.

Os utilizadores nunca deverão partilhar palavras passe e caso necessitem de partilhar dados deverão ser postos em prática métodos que permitam dar acessos a utilizadores diferentes do habitual, assim garantindo a rastreabilidade e *reporting*.

Se os utilizadores partilharem os seus nomes de utilizadores e palavras-passe este princípio perde-se completamente.

Base de dados de clientes

Deverá existir apenas uma base de dados para poder agilizar os pedidos dos clientes aquando de necessidade de retificação ou remoção. Por exemplo, se possuir e utilizar *software* de faturação deverá usar a base de dados deste, não sendo de todo aconselhado ter uma base de dados separada em Excel ou Access ou outros produtos ou serviços.

Deverá suportar controlo de acessos, de preferência granular. Deverá ser possível vedar o acesso à base de dados com base na identidade do utilizador. De preferência deverá ser possível vedar o acesso a dados de clientes aos trabalhadores que não necessitam do acesso aos mesmos. Este acesso deverá ser dado apenas em caso de necessidade.

Deverá ser mantida segura, centralmente, de preferência em *cloud* ou *server* e não deverá ser possível a cópia integral da mesma.

Ainda nesta temática é importante que o utilizador bloqueie sempre o seu computador antes de se afastar dele. Mesmo em pequenas empresas, pois é possível que, por acaso ou maliciosamente, alguém veja dados do seu ecrã enquanto não estiver no seu posto.

Exemplos

- Base de dados mantida em *Excel* (desaconselhado)
  - Não possibilita a granularidade dos acessos
  - Caso esteja guardada num servidor, o acesso pode ser vedado para leitura ou escrita.
  - Na maioria dos casos é possível efetuar uma cópia integral do file, caso o utilizador tenha acesso mesmo só de leitura
- Base de dados em *Access* (desaconselhado)
  - Possibilita em parte a granularidade dos acessos
  - Tal como *Excel*, caso seja guardada em servidor podemos vedar o acesso para leitura e escrita.
  - Como em *Excel*, é possível cópia integral
- Base de dados dedicada aplicacional em servidor ou *cloud* (aconselhado)
  - O acesso pode ser granular, dependendo do tipo de base de dados.
  - É centralizada mas o acesso é feito de forma aplicacional ou web logo o acesso é normalmente granular.
  - Pode estar integrada ou um sistema de faturação ou ser mesmo parte do sistema.
  - Normalmente não é possível uma cópia integral.

Software de faturação

Tal como referido acima este tipo de *software* necessita de cumprir com o controlo de acessos e rastreabilidade. É importante que cada utilizador tenha um *user* e *password* de acesso e não a partilhe com mais ninguém.

Em caso de necessidade de acesso por um utilizador não-habitual a dados de um cliente, estes acessos deverão ser dados na aplicação para garantir a rastreabilidade. Idealmente a própria ação de alteração de acessos devia ser documentada.

Software de processamento de salários

Tal como na alínea anterior, os utilizadores não devem partilhar os seus dados de acesso com mais ninguém, nem e caso urgente de acesso. A proteção da identidade é uma pedra angular de todos os processos informáticos envolvidos ou influenciados pelo RGPD e os utilizadores devem interiorizar este conceito para evitar pontos fracos no processamento dos dados pessoais.

O processamento salarial com todos os seus pormenores e dados confidenciais é certamente um dos momentos de mais risco no que diz respeito ao processamento de dados numa empresa de contabilidade.

Idealmente, para além de ter controlo de acessos, a base de dados de um *software* deste género devia ser encriptada para que, em caso de extravio (por exemplo: *hacking* ou mesmo roubo físico do servidor), não possa ser aberta.

Servidores de partilha de ficheiros

Em geral os servidores de ficheiros apoiam-se um *Windows Domain* e desta forma é possível controlar, vedar e rastrear os acessos aos ficheiros. Porém o rastreamento deve ser ativado. Os responsáveis pelas IT da empresa devem garantir que a rastreabilidade está ativada e funcionante.

Impressoras

Embora estejamos a falar essencialmente de dados digitais, é claro que muitos terão de ser impressos.

As boas práticas ao nível das impressoras normalmente são as normais de "segurança física". Mas há algumas ações que devem ser tidas em conta.

Um trabalhador nunca deve imprimir um documento com dados pessoais ou confidenciais, sem ter a certeza de que estes não serão vistos ou consultados por outro trabalhador que não deverá ter acesso aos mesmos.

No caso de ter impressoras de secretária a preocupação não é muito grande. Contudo se tiver impressoras centralizadas, os trabalhadores deverão estar cientes das melhores práticas.

Muitas impressoras centralizadas possibilitam *confidential printing*. Ao imprimir o documento, podemos introduzir um PIN. Neste caso para que o documento seja impresso é necessário ir até à impressora e introduzir este PIN.

Assim não corremos certamente o risco que os documentos que imprimimos sejam vistos por quem não tem autorização para o fazer.

Terminais

Quer que sejam *Windows*, *Linux* ou *Apple*, os terminais deverão estar preparados para que o acesso aos mesmos só possa ser efetuado através de *username* e password.

No caso de *desktop computers* e *laptops* os cuidados a ter são:

- Manter as *passwords* seguras e nunca em *post-its* no ecrã
- Ativar o software *Bitlocker* para que o disco rígido do computador seja completamente encriptado. Aquando do arranque o disco será desencriptado através de um código. A encriptação em *Windows* é feita através do *Bitlocker* que está acessível nativamente em *Windows* 7, 8.1 e 10. Assim, em caso de extravio, roubo ou desaparecimento do PC, mesmo removendo o disco rígido não é possível aceder ao mesmo sem a chave de acesso.
- Os terminais devem ter anti-vírus atualizados, bem como *firewalls* locais ativas e efetivas.
- O acesso aos PC alheios deve ser feito apenas utilizando um utilizador e *password* do utilizador que deseja aceder ao mesmo, para garantir uma completa rastreabilidade.

No caso de dispositivos móveis como *tablets* e *smartphones*

- Encriptar o dispositivo utilizando as opções do *smartphone*
- Utilizar um PIN de, no mínimo 6 dígitos para acesso

Sistemas de acesso à internet

Os acessos à internet devem ser vedados e rastreados com base na necessidade dos utilizadores.

Os utilizadores não devem ter acesso a *sites* não fidedignos. Isto consegue-se utilizando um servidor de *Proxy* interno e/ou *firewall* para segregar a rede interna da internet e mitigar ataques.

Sistema de acesso externo

Para que os trabalhadores tenham acesso a recursos internos da rede, normalmente usa-se uma VPN (*Virtual Private Network*).

É importante que os utilizadores, mais uma vez, tenham a plena consciência do que necessitam de fazer para que a VPN seja completamente segura.

Nunca aceder à VPN a partir de redes suspeitas para que os dados de acesso não sejam capturados e eventualmente reutilizados.

Em termos de segurança é necessário garantir que o *software* de VPN utilizado não sujeita a rede a ataques externos. Uma *firewall* no perímetro da rede como falado no tópico anterior é certamente de extrema importância.

Exemplos de procedimentos e fluxos de dados

A tabela abaixo demonstra exemplos de procedimentos e fluxos de negócio afetados pelo RGPD.

Para cada um iremos desenvolver os cuidados ter, incluindo os sistemas envolvidos por parte de quem acede e processa os dados.

Procedimento	Fluxo de dados
1. Aquisição de novo cliente	Cliente -> Contabilista
2. Alteração de dados do cliente	Cliente -> Contabilista ou Interno
3. Envio de *newsletter* para clientes	Contabilista -> Clientes
4. Processamentos salariais	Interno Cliente -> Contabilista
5. Acesso a Portal das Finanças e Segurança Social de cliente para envio de declarações e similares	Interno
6. Lançamento de documentos, fechos anuais e *reporting*	Interno
7. Comunicações com os clientes (normais ou confidenciais)	Contabilista <-> Cliente
8. Transporte de documentos desde e para o cliente (fisicamente em formato impresso ou digital tipo PEN)	Contabilista <-> Cliente
9. Impressão de documentos	Interno
10. Passagem de pastas para outro contabilista (entrega de documentação ao cliente) dever de lealdade	Código deontológico

Vamos agora olhar para os exemplos de procedimentos acima e descrevê-los em mais pormenor, delineando os passos necessários para que seja cumprida a conformidade.

1.Processo de aquisição de novo cliente

RESUMO

Ao adquirir um novo cliente entramos na fase em que devemos introduzir os dados do mesmo no sistema. Cada empresa terá uma metodologia diferente para este processo, porém em geral os passos são os que se seguem:

- Envio do contrato para assinatura
- Introdução dos dados do cliente na base de dados
- Introdução do *email* na lista de *newsletter*
- Transmissão de dados a subcontratantes
- Atribuição de permissões e responsabilidades a trabalhadores internos

DESCRIÇÃO DETALHADA

ENVIO DO CONTRATO DE PRESTAÇÃO DE SERVIÇOS AO CLIENTE

Este contrato tem de estar de acordo com o RGPD **(ver manual)** e deverá incluir todas as informações relevantes sobre o processamento que irá fazer sobre os dados do cliente bem como, no caso de processamento salarial, os dados dos trabalhadores do cliente.

É necessário que o cliente dê o seu consentimento para ações como:

- Inscrição em *newsletters*
- Transmissão dos dados a sub-contratantes
- Acesso aos dados por parte de terceiros e para que processamento

O contrato poderá ter também a informação sobre os direitos do cliente e convém também que contenha uma secção onde o cliente confirma os meios oficiais de contacto como o seu *email* fidedigno. Desta forma toda a informação deverá sempre ser enviada para esse *email* ou *emails* contratualizados e a responsabilidade da segurança do mesmo será sempre e só do cliente.

Veremos mais adiante, no caso em que o cliente necessite de receber dados pessoais e/ou confidenciais noutra caixa do correio, o cliente terá de fazer o pedido por escrito e será considerado uma exceção.

Tendo em conta que o contrato em si também contém dados pessoais e confidenciais deverá ser armazenado em local seguro e de acesso controlado. Normalmente será guardado na pasta do cliente, sendo que o acesso deve se vedado a estranhos e, se possível, o acesso deve ser proporcionado apenas a quem de facto necessitar de aceder. Em cenário ideal também deveria ser feito o registo do acesso à documentação, porém sabemos que não é prático. Eventualmente podemos apenas fazer o registo de acesso por parte do substituto do colaborador que processa o cliente, aquando das férias deste último. Assim garantimos a rastreabilidade dos acessos.

INTRODUÇÃO DOS DADOS NA BASE DE DADOS DE CLIENTES

Com base no contrato é necessário introduzir os dados na base de dados de clientes. A base tecnológica da base de dados pode variar muito. Poderá ser um *software* de faturação, ou mesmo uma base de dados dedicada aos clientes. Poderá ser ainda uma folha de *Excel*, ficheiro de *Access* ou outras como já referido acima.

Qualquer um destes métodos são validos, porém, deverão cumprir com alguns requisitos mínimos, como descrito acima. Não esquecer que a rastreabilidade e controlo de acessos são dois fatores importantíssimos para a conformidade.

Os dados introduzidos deverão ser apenas os relevantes para o seu processamento, cumprindo assim com o princípio da minimização.

Como também descrito acima, é necessário assegurar que a base de dados está segura e, caso seja possível, deve-se restringir-se o acesso aos dados do cliente apenas por parte do trabalhador ou trabalhadores que irão processar os dados desse cliente. Vamos desenvolver abaixo na "Atribuição de responsabilidades".

INSCRIÇÃO NA LISTA PARA ENVIO DE NEWSLETTER

Em geral os serviços de *newsletter* são mantidos *online*. A inscrição do cliente neste serviço deve ser feita apenas se o mesmo tiver consentido em contrato esta utilização.

Serviços como *Mailchimp* possuem todos os automatismos para cumprir com o RGPD. Caso o serviço que usa não tiver um *link* de *Unsubscribe* ou "Remover da lista" não estará a cumprir com o RGPD, logo aconselha-se a trocar de serviço.

Caso tenha um sistema de newsletter interno é **absolutamente imperativo** que tenha em atenção que, aquando do envio do mail, por exemplo, a partir da caixa de correio "geral" da empresa, os recipientes da mensagem vão em "BCC" e não em "CC" ou "Para". Quando o envio é feito em "CC" ou "Para" os endereços dos recipientes são mostrados e isto configura uma clara violação de conformidade do RGPD.

TRANSMISSÃO DE DADOS A SUBCONTRATANTES

Caso o cliente o consinta e seja absolutamente necessário para o bom funcionamento do processo de negócio, em alguns casos temos de passar os dados do cliente a um subcontratante. Em alguns casos, por exemplo, podemos colaborar com uma empresa de higiene e segurança no trabalho e proporcionar este serviço subcontratando-o a outra entidade.

Neste caso, e antes de mais, é necessário garantir que o subcontratante cumpre com os requisitos de RGPD. Uma declaração de conformidade será suficiente.

A transmissão dos dados de um único cliente poderá ser feita por via de *email* sendo que é um método suficientemente seguro desde que tomadas as precauções necessárias. Normalmente basta utilizar um endereço de destino fidedigno definido pelo subcontratante em contrato, pedir um recibo de entrega e de seguida apagar o *email* dos "Enviados" minimizando o risco de exposição. Neste caso o impacto em caso de extravio ou divulgação dos dados é mínimo. Após o envio, o cliente deve ser informado de que existiu esta transmissão de dados. Em geral o método utilizado é o *email*.

Se necessitarmos de transmitir um número elevado de dados de clientes, como por exemplo, toda a nossa base de dados, devemos tomar precauções redobradas. Neste caso é necessário enviar os dados em anexo ao *emai*l, num ficheiro encriptado com password. Na maioria dos casos será um ficheiro ripo ZIP ou RAR. O passo mais importante é garantir que a *password* será transmitida ao subcontratante por via alternativa ao e-mail para garantir que, em caso de acesso indevido à sua caixa de correio, quem tenta um qualquer acesso malicioso não pode abrir a base de dados por falta de autenticação. Também é necessário apagar o *mail* dos "Enviados" após o envio e instruir o subcontratante para que faça o mesmo com o mail recebido.

Em geral é aconselhável ligar o cliente diretamente a este subcontratante, eliminando, desta forma, a necessidade de passagem de dados em cascata.

ATRIBUIÇÃO DE PERMISSÕES E RESPONSABILIDADES A TRABALHADORES INTERNOS

Para que seja possível uma rastreabilidade melhorada e uma minimização do risco de exposição, é aconselhável que o acesso aos dados seja proporcionado apenas ao trabalhador que necessitar deste acesso.

Para além disso é aconselhável que o trabalhador tenha apenas o acesso necessário, sendo que, por exemplo, caso não necessite acesso de escrita sobre os dados, este não deve ser dado.

O ideal é verificar as funcionalidades da base de dados mapear as mesmas ao cumprimento do RGPD.

2. Alteração de dados do cliente

RESUMO

Quando for necessário alterar os dados do cliente, em regra geral, o procedimento será o seguinte.

- O cliente pede a alteração dos dados (direito à retificação) ou internamente verificamos que houve há dados errados.
- Os dados são alterados e o cliente é informado

DESCRIÇÃO DETALHADA

Como vimos acima o acesso aos dados do cliente por parte dos trabalhadores deve ser apenas o estritamente necessário. Aquando da necessidade de alteração dos dados do cliente, por pedido do mesmo ou por correção interna, o cliente deve ser informado.

O que se procura é ter transparência máxima no que diz respeito á intervenção sobre os dados do cliente.

Como o que devemos comunicar ao cliente é informação especifica sobre as alterações efetuadas, é imperativo que, tal como visto na rubrica anterior:

- A informação deve ser explícita, sobre que alteração foi efetuada
- A informação deve ser transmitida de forma segura. Um endereço fidedigno e contratualizado será suficiente.
- Deve remover-se a informação do "enviados" em caso de transmissão por *email* para garantir a minimização do risco de exposição.

A remoção dos mails da pasta "Enviados" deverá de facto tornar-se numa prática comum para garantir que não existem cópias da informação pessoal espalhadas e fora do controlo central.

Caso seja necessário fazer prova do envio dos *emails* é possível e aconselhável pedir um recibo de entrega e esse sim, já que não possui qualquer informação confidencial nem pessoal, pode ser guardado como uma prova de entrega.

3. Envio de newsletter para clientes

RESUMO

O envio de uma *newsletter* ou comunicação em massa é uma tarefa bastante simples. O processo de aquisição de dados para a mesma foi já descrito acima e deve, normalmente acontecer durante a aquisição do cliente.

Porém podemos ter na nossa base de dados de *newsletter* entidades ou pessoas que não são nossos clientes. Teste caso, normalmente recorre-se à inscrição via *website*. A inscrição tem um procedimento em que:

- O cliente introduz o seu *email* num campo do website
- O site, automaticamente envia *email* para o cliente em jeito de confirmação
- O cliente clica num *link* do mail para confirmar o seu *email*.
- O cliente é inscrito na base de dados.

O penúltimo passo é o mais importante assume o papel de "prova". Caso não haja confirmação, então significa que ou o cliente foi inscrito por alguém na *newsletter*, mas não tem intenção de facto de a receber, ou então o *email* está errado.

Não é permitida a inscrição do cliente na base de dados diretamente mesmo que o cliente o tenha confirmado por outro método. Outros métodos que não sejam os descritos acima, em geral, não fazem prova de consentimento.

DESCRIÇÃO DETALHADA

O envio da *newsletter* em si é bastante simples mas é necessário ter alguns cuidados:

- Não incluir informação pessoal ou confidencial.
- Não expor os endereços dos clientes uns aos outros.

Uma simples mensagem de felicitações por aniversário de um cliente enviada numa *newsletter*, caso não tenha sido consentida, configura uma violação da conformidade com RGPD porque expõe a data de nascimento da pessoa.

4. Processamento Salarial

RESUMO

O processamento salarial é o momento em que os nossos trabalhadores irão claramente lidar com os dados pessoais mais sensíveis e em maior número.

Existe uma metodologia generalizada para o processamento salarial, porém o fluxo de dados pode variar bastante. O que se pretende nesta secção é informar das melhores práticas para se estar dentro do cumprimento das normas RGPD.

Para facilitar a compreensão separamos o processamento salarial em quatro grandes tarefas:

- Admissão de trabalhadores
- O processamento salarial normal (incluindo baixas e ausências justificadas ou não)
- A emissão e envio de relatórios de resumo e de recibos de ordenado
- Os despedimentos

DESCRIÇÃO DETALHADA

ADMISSÃO DE TRABALHADORES

Durante a admissão de trabalhadores os dados são transferidos do cliente para o contabilista, normalmente por *email*. Em muitos casos as cópias dos documentos de identificação serão transferidos em anexo ao *email*.

Como vimos acima, as cópias destes documentos deverão ser eliminadas de todo e qualquer local onde não necessitem de estar, como por exemplo a caixa de correio.

Ao ser recebidas devem ser guardadas, por exemplo numa pasta segura, num *software* de gestão documental, ou em qualquer outro local que possibilite a rastreabilidade e o controlo de acesso.

Estes documentos devem ser guardados apenas em caso de necessidade comprovada.

O ónus da obtenção do consentimento junto do trabalhador, neste caso, cabe ao cliente.

O PROCESSAMENTO SALARIAL NORMAL

Durante o processamento salarial normal, o contabilista tem acesso a muitos dados pessoais e confidenciais que são do foro íntimo do seu titular.

O contabilista tem de conhecer muito bem o Código Deontológico e segui-lo à risca no que diz respeito à confidencialidade. Por cima do código terá de construir comportamentos e procedimentos que assegurem que durante o processamento a possibilidade de divulgação acidental dos dados pessoais seja minimizada.

Estes comportamentos são simples e podem ser mecanizados muito rapidamente. Fazem de facto parte de uma cultura de proteção de dados que deve ser incutida partindo do mais alto nível e fomentada todos os dias, inclusive entre colegas.

Alguns exemplos:

» Sempre que o colaborador se afastar do PC deverá bloqueá-lo **(Ver tutoriais)**

» Sempre que o colaborador tenha de se afastar da sua secretária deverá tomar as devidas precauções para que os documentos impressos não fiquem à vista.

» O colaborador que necessite de imprimir documentos com dados sensíveis deverá optar por fazê-lo numa impressora próxima dele ou então usar um código de impressão **(Ver tutoriais**).

» Sempre que alguém que não deve ter acesso aos dados se aproximar da sua secretária o colaborador deverá minimizar as janelas com dados sensíveis **(Ver tutoriais)**

» Todos os dados relativos a ausências, baixas, etc... devem ser guardados apenas num local e deve existir apenas uma cópia dos mesmos. Se estes dados forem recebidos por *email*, é uma boa prática descarregá-los para um local seguro (software ou pasta com controlo de acessos) e apagá-los da caixa de email.

Todos estes comportamentos deverão tornar-se naturais. São apenas um exemplo pois os procedimentos internos deverão ser analisados debaixo da lupa do RGPD.

Dado que estes variam de empresa para empresa poderá haver outros que elevam o risco de não conformidade.

Em alguns casos é necessário processar salários com pormenores como baixas, ausências justificadas ou não justificadas. Claramente aqui entramos no foro do mais íntimo que há para um trabalhador. É necessário ter especial atenção aos documentos médicos do trabalhador e as regras acima devem ser absolutamente seguidas à risca.

EMISSÃO, IMPRESSÃO OU ENVIO DE RELATÓRIOS E RECIBOS DE ORDENADO

Este é claramente um momento em que os dados dos trabalhadores dos nossos clientes podem potencialmente estar mais expostos a riscos de divulgação.

Mais uma vez, tal como na secção acima, a minimização do risco passa por uma interiorização de comportamentos.

» Emissão, impressão e envio de recibos de ordenado

- Durante a emissão é imperativo garantir que os recibos são guardados numa pasta com controlo de acessos para que possam ser eventualmente "zipados" e enviados ao cliente por *email*. Após o envio é necessário apagar o *email* dos "itens enviados". Uma excelente prática é também apaga-los da pasta já que a qualquer altura podem efetivamente ser reemitidos a partir do *software*. **(Ver tutorial)**
- Durante a impressão deve optar sempre por uma impressora à qual tenha acesso rápido para que os documentos não fiquem á merce de qualquer pessoa por muito tempo. Se tiver a oportunidade deve utilizar impressão com código.
- O envio deve ser feito usando um ficheiro com *password*, de preferência com-

plexa. Como referido acima, pode ser feito juntando os recibos num file ZIP e designando uma *password* para o mesmo. Há *software* que emite os recibos em PDF num documento único e de seguida pode-se definir uma *password* nesse documento. A *password* deve ser comunicada ao cliente à parte e nunca para o mesmo endereço de e-mail para onde enviamos o ficheiro. Pode ser enviada, por exemplo por SMS para o número definido como fidedigno no contrato de prestação de serviços. Após o envio o ficheiro deve ser apagado dos "enviados", como vimos anteriormente.

» Emissão, impressão e envio de relatórios

- Esta operação rege-se precisamente pelas mesmas regras descritas acima. Todo e qualquer relatório deve ser enviado, encriptado (ver tutorial) ou em caso de impressão, selado em embalagem inviolável.
- Tal como no envio dos recibos, será sempre boa prática eliminar o *mai*l dos enviados, ficando apenas com uma cópia do recibo de entrega. **(Ver tutorial)**

DESPEDIMENTO

O despedimento é claramente uma operação que pode envolver informação privada e até do foro judicial em caso de justa causa ou conflito laboral.

Neste caso tudo o que descrevemos acima, tal como em caso de baixa ou informação médica, deve ser seguido à risca e a cada transferência e operação devemos sempre zelar pela confidencialidade e proteção dos dados do trabalhador.

5.Acesso a portais usando as credenciais do cliente

RESUMO

Na profissão de contabilista temos de utilizar muitas vezes as credenciais dos nossos clientes para aceder aos diversos portais como de Finanças, Segurança Social, etc...

A entrega atempada das declarações depende absolutamente deste acesso.

Sendo assim há duas tarefas essenciais relativamente a este assunto:

» Manutenção das credenciais em local seguro

» Transmissão das credenciais pelo cliente

DESCRIÇÃO DETALHADA

As famigeradas folhas de Excel com as credenciais dos clientes podem efetivamente existir. Só

não estão em conformidade com o RGPD se não forem tomadas as devidas precauções.

- O ficheiro deve estar guardado num servidor, como por exemplo numa pasta partilhada, com controlo de acessos e rastreabilidade para que seja possível saber quem efetuou acessos.
- De preferência cada trabalhador deve apenas acesso de leitura a um ficheiro onde constam as credenciais dos clientes que eles gerem, não mais que isso.
- O ficheiro deve estar protegido por *password*.
- O ficheiro **nunca** deve ser transmitido por *email*.

Se seguirmos as normas acima, podemos considerar que estamos em conformidade, mas não minimizamos o risco já que um ou mais ficheiros de Excel não são claramente a opção mais segura.

Algum *software* de gestão ou mesmo de faturação possui nas suas fichas de clientes uma zona onde se pode guardar as credenciais de acesso dos clientes. Este será claramente um método preferencial pois não é possível extrair em massa todas as credenciais, tal como pode acontecer com uma simples cópia do ficheiro Excel.

6.Lançamento de documentos, fechos anuais e reporting

RESUMO

Durante o lançamento de documentos estes ficam expostos à vista de colaboradores que podem não ter a necessidade nem devem ter acesso aos mesmos.

Cabe ao colaborador evitar que outros vejam pormenores do trabalho que está a ser efetuado.

Esta é uma situação muito similar ao processamento de salários.

Os mesmos princípios se aplicam aos fechos anuais e ao *reporting*.

DESCRIÇÃO DETALHADA

Algumas boas práticas:

- Não deixar documentos em cima da secretária
- Minimizar as janelas sempre que um colaborador que não deve ter acesso se aproxima **(Ver tutorial)**
- Se for necessário imprimir os documentos utilizar uma impressora próxima ou com código de impressão
- Todo e qualquer esclarecimento de dúvidas com o cliente que seja feito por *email*, deve ser avaliado e, caso não haja necessidade de arquivo, deve ser eliminado da caixa

do correio ou arquivado.

» O envio de *reports* deve ser feito utilizando um ficheiro com *password*, o *mail* eliminado do enviados e o *report* deve ser arquivado em local seguro ou mesmo eliminado caso haja a possibilidade de gera-lo novamente por *software*.

7. Comunicações com o cliente (normais ou confidenciais)

RESUMO

A comunicação com um cliente pode ser feita utilizando diversos métodos:

» *Chat* (*Whatsapp*, Facebook, Google, Skype, SMS)

» Voz (telefone ou presencial)

» *Email*

Em todos os casos devemos seguir algumas regras básicas para garantir a proteção dos dados.

DESCRIÇÃO DETALHADA

CHAT

É desaconselhada a utilização de *chats* de redes sociais como Facebook ou Instagram. Não são claramente serviços vocacionados para o negócio e nunca sabemos quem pode estar a ver as mensagens do outro lado pois baseiam-se sobre credenciais de acesso. Chats como o Whatsapp ou SMS podem ser considerados seguros pois baseiam-se não apenas em credenciais de acesso bem como o número de telefone para o acesso. Isto garante um maior grau de privacidade e garantia de conformidade. Porém, é desaconselhado a utilização destes canais de conversação para transferir dados pessoais, confidenciais ou sensíveis.

O mesmo vale para o Skype. Embora seja um serviço seguro e empresarial não podemos garantir a identidade de quem está do outro lado.

VOZ

As reuniões com os nossos clientes devem ser mantidas em espaços confidenciais, tanto telefónicas como presenciais. As informações transmitidas devem ser ouvidas apenas por quem necessita delas para executar o seu trabalho.

EMAIL

Nas secções acima demos muitos exemplos de transmissão dos dados por *email*.

A regras de base são:

» Usar sempre um *email* fidedigno, contratualizado e garantido pelo cliente para receber e transmitir a informação.

» Nunca transmitir dados sensíveis sem que estes sejam encriptados. A encriptação pode estar ao nível do *email* ou mesmo ao nível do ficheiro transferido. De preferência o ficheiro transferido deverá estar sempre encriptado.

» A *password* para abrir o ficheiro deve ser comunicada por método alternativo e diferente do mail para onde se enviou o file.

» Apagar sempre dos "itens enviados" os ficheiros sensíveis mesmo que estes estejam encriptados.

» Caso o cliente nos envie dados sensíveis não encriptados devemos sempre chamar a atenção para este facto para que o cliente tenha esteja ciente e informado do nosso compromisso para com a segurança dos dados.

8.Transporte de documentos e transferência via internet

SUMÁRIO

Na atividade de contabilidade, o transporte de documentos é algo de normal entre o cliente e o contabilista.

Os documentos transportados podem ser físicos ou mesmo em formato digital mas em suporte físico como uma *pen*, disco USB, CD etc.

Também podemos incluir neste tipo de transporte a transferência via internet já que normalmente trata-se de um volume significativo de dados que não pode ser enviado por *email*.

DESCRIÇÃO DETALHADA

TRANSPORTE DE DOCUMENTOS FÍSICOS E IMPRESSOS

É uma boa prática que, quem transporta os documentos ou os dossiês, que em muitos casos podem chegar às dezenas, o faça tomando todas as medidas necessárias para que haja risco mínimo de extravio.

Por exemplo, quando estamos a transferir os documentos através de uma viatura devemos garantir que esta não está em risco de assalto ou roubo. Ou, caso seja possível, ao sair da viatura, levar os documentos sensíveis consigo.

Os dossiês, caixas ou envelopes devem estar selados para que o cliente tenha a garantia que não houve interferências durante o transporte.

TRANSPORTE DE DOCUMENTOS DIGITAIS EM FORMATO FÍSICO

Quando é necessário transferir documentos digitais em meio físico é extremamente importante encriptar os ficheiros antes de os copiar para o meio físico. (Ver tutorial)

Caso haja extravio da *pen*, do disco ou do CD quem tiver acesso ao meio físico não deverá poder ter acesso ao ou aos ficheiros.

Uma melhor prática será mesmo encriptar o disco na sua totalidade. O *Windows* tem de raiz o *Bitlocker* que permite precisamente este tipo de encriptação total.

O dispositivo só poderá ser lido usando uma *password* ou PIN específico**. (Ver tutorial)**

TRANSFERÊNCIA DE GRANDES VOLUMES DE INFORMAÇÃO VIA INTERNET

Como referido acima podemos incluir este tipo de transferência no conceito de transporte, embora o meio seja a internet.

Valem precisamente as mesmas práticas:

- Os ficheiros devem ser encriptados
- Deve ser utilizado um método que nos garante que estamos a transferir o ficheiro apenas para a pessoa entendida.
- Devemos garantir que após bom recebimento o ficheiro é apagado.

Serviços como *Wetransfer* não são aconselhados, pois o *link* para o ficheiro *online* pode ser partilhado com terceiros.

Porém, serviços como Onedrive, Gdrive permitem dar acesso apenas a quem entendermos, usando o seu *email*. Além disso os ficheiros podem ser apagados após confirmação da receção. **(Ver tutorial)**

9.Impressão de documentos

Como já referido acima, é necessário que o colaborador garanta que durante o processo de impressão de documentos não serão revelados ou divulgados dados pessoais.

Para isso é necessário garantir que a impressão, caso contenha dados confidenciais, é efetuada para uma impressora que possibilite a impressão apenas quando quem imprime esteja perto da mesma ou mesmo imprimir para uma impressora pessoal.

Algumas impressoras permitem impressão com código. Estas são as ideais para garantir a conformidade com RGPD.

10.Passagem de pastas ou transferência de cliente

Embora tenha sido um assunto muito muito abordado pelos contabilistas, de facto todas as

regras mencionadas acima aplicam-se na transferência de um cliente.

Neste caso o que é mais importante e anda de mãos dadas com o RGPD é claramente o Código Deontológico.

Vale a pena mencionar que, de facto, toda a passagem de documentação deve ser feita para o cliente e que em caso de transferência eletrónica é necessário garantir a segurança dos dados digitais com encriptação.

Exemplos de procedimentos inerentes ao RGPD (Aplicado ao exercício de contabilidade)

Tal como na tabela acima descrevemos abaixo os procedimentos inerentes à conformidade com RGPD.

Procedimento	Despoletado por	Ação
1.O titular pede acesso aos seus dados	Artigo 15 – Direito de acesso	Devemos informar o titular de forma transparente
2.O titular pede a retificação dos dados	Artigo 16 – Direito à retificação	Devemos retificar os dados, fazer prova da retificação e informar eventuais subcontratados
3.O titular pede para que todos os seus dados sejam removidos das bases de dados	Artigo 17 – Direito a ser esquecido	Na medida do possível e do legal devemos aceder ao pedido. Caso não seja possível devemos fazer um esforço para pseudonimizar os dados. Devemos de seguida informar o titular
4.O titular não quer que os seus dados sejam divulgados com terceiros	Artigo 18 – Direito à restrição de processamento	Durante a aquisição é necessário definir no contrato qual a utilização que será feita dos dados do cliente e informa-lo para evitar incidentes
5.O titular quer mudar de contabilista e quer que lhe sejam fornecidos todos os seus dados	Artigo 20 – Direito à portabilidade	Devemos extrair os dados do cliente dos nossos sistemas em formato legível e acessível como TXT, XML ou CSV e fornece-lo ao cliente. Não significa que o cliente seja apagado pois isso é outro direito.
6.O titular recebe *newsletters* regulares e quer deixar de receber.	Artigo 21 – Direito à objeção	De certa forma se sobrepõe ao artigo 18. Devemos remover imediatamente o cliente da lista da nossa *newsletter*.

Tutoriais

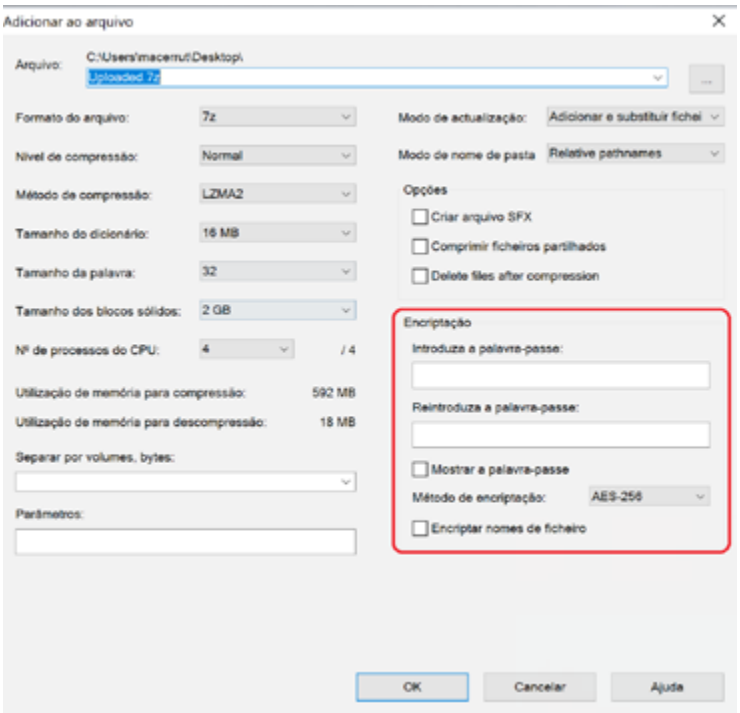
1. Como criar um ZIP com password

Para criar um file ZIP com *password* para transmissão segura devemos proceder da seguinte forma:

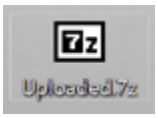
Utilizando o *software* "7zip". (https://www.7-zip.org/download.html)

» Clique sobre o ficheiro ou pasta com o botão direito do rato para que apareça o menu contextual. Seleccione "7zip" e de seguida "Adicionar ao arquivo".

» Na janela "Adicionar ao Arquivo", na secção "Encriptação" podemos adicionar uma *password*, bem como selecionar o método de encriptação e se queremos encriptar os nomes dos ficheiros também. Ao selecionar esta opção, os nomes dos ficheiros irão aparecer encriptados até à extração do ficheiro, como vamos ver em 1.1.



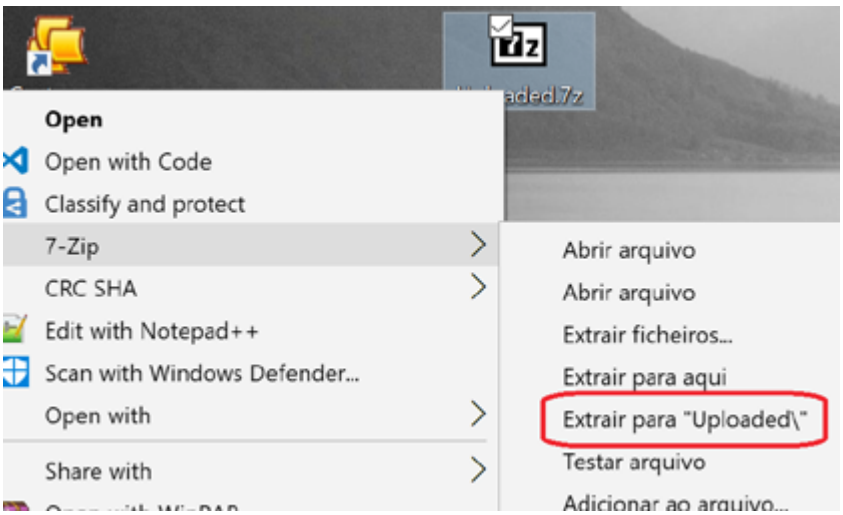
» Ao introduzir e confirmar a palavra-passe o ficheiro será encriptado. Neste caso selecionamos o formato "7z". Basta clicar "OK" e o ficheiro será criado e pode ser então enviado por *email* ou carregado para um sistema de transferência.



ABRIR UM FICHEIRO ENCRIPTADO

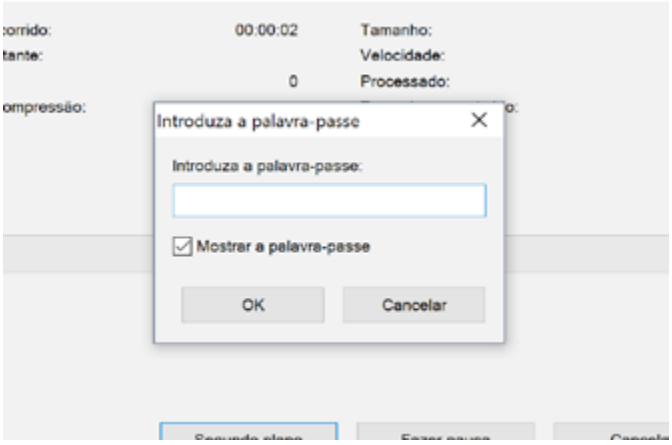
Sempre utilizando o *software* "7zip" vamos ver como abrir um ficheiro encriptado.

» Clique sobre o ficheiro "7z" ou "zip" com o botão direito do rato e arraste até "7-zip". Selecione "Extrair para..."



Esta ação irá extrair o file para a pasta com o mesmo nome do ficheiro. Caso não exista irá ser criada automaticamente.

» A este ponto será solicitada a palavra-passe



» Bastará introduzi-la para extrair os ficheiros.

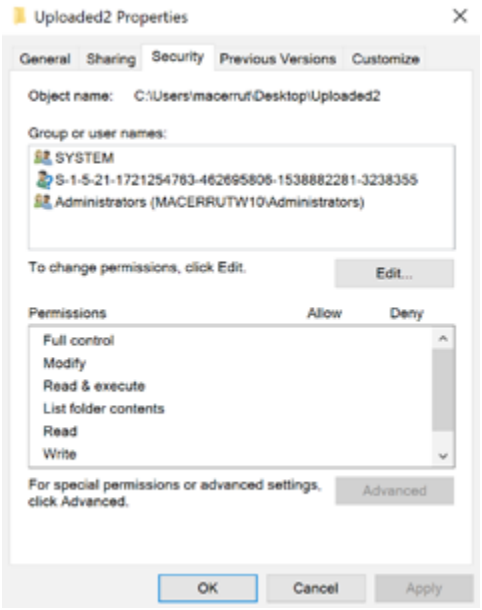
2. O que é uma pasta com controlo de acesso

Uma pasta ou um ficheiro com controlo de acessos significa que este permite aplicar permissões que regulam o acesso.

O acesso pode ser dado ou negado, a diversos níveis como leitura, escrita, execução, etc...

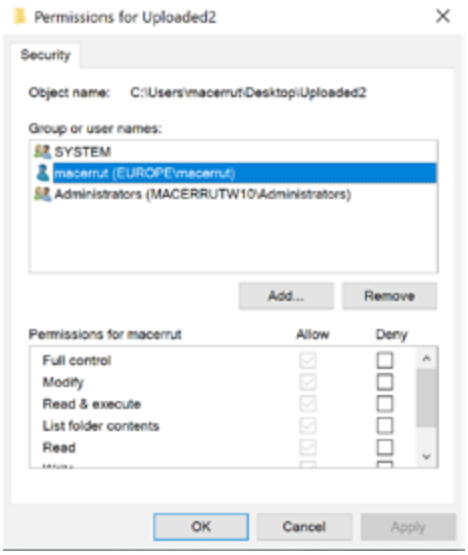
O *Windows* possibilita aplicar permissões a pastas tanto partilhadas como locais.

» Selecionando com o botão direito a pasta ou o ficheiro, clique em "Propriedades"



» No TAB *Security* podemos ver os utilizadores ou grupos com permissões aplicadas.

» Para editar as permissões clique sobre o botão "Editar"



» Aqui podemos selecionar o utilizador e editar as permissões de acesso ou então adicionar um utilizador e aplicar permissões.

Esta é uma tarefa que deverá ser normalmente executada em conjunto com os responsáveis de informática. Normalmente os ficheiros estarão centralizados e o controlo depende dos utilizadores e grupos criados na rede.

3. Como apagar um item dos "Enviados"

Pode parecer algo de simples, mas para apagar definitivamente um item dos "enviados" é absolutamente necessário garantir que não foi transferido para os "Itens eliminados".

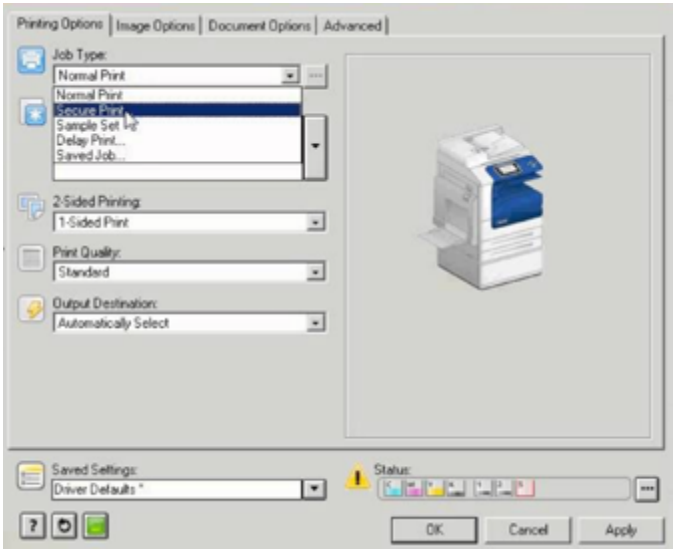
Para apagar definitivamente um item é necessário efetuar o seguinte:

- Apagar o *email*
- Ir aos Itens eliminados e apagá-lo novamente

Porém há uma técnica mais rápida. Se selecionarmos o *email*, de seguida pressionarmos a tecla "shift" + "del" o mail será apagado permanentemente sem passar pelo "Itens eliminados".

4. Exemplo de impressão com código

Algumas impressoras permitem, através to driver de impressão, selecionar uma opção de *Secure Printing*.



Ao selecionar esta opção, antes de imprimir, é solicitada a introdução de um código.

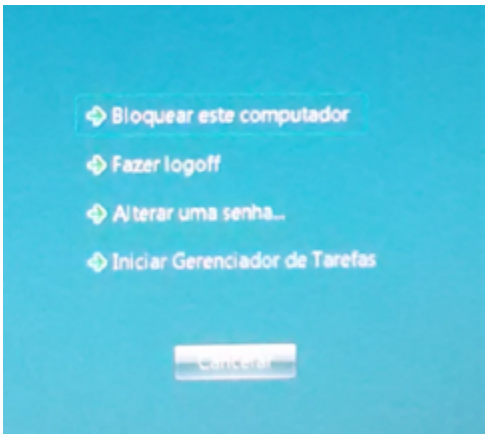
A impressora não irá iniciar a impressão imediatamente. Teremos sim que nos deslocar até junto da mesma, selecionar o documento a imprimir e digitar o código que definimos aquando da impressão.

Somente nessa altura a impressora irá imprimir.

5. Como bloquear o seu computador

O bloqueio do PC é extremamente importante para um bom cumprimento do RGPD. Sempre que um utilizador se afaste do PC necessita de o bloquear.

Para bloquear o computador basta pressionar as teclas "ctrl" + "alt" + "Del" e selecionar "Bloquear este PC" ou "Bloquear" dependendo da versão do *Windows*.



Após o bloqueio somente quem bloqueou o PC ou o administrador podem desbloqueá-lo. No caso de ser o administrador, a sessão será terminada, logo nem o administrador terá acesso aos dados do utilizador.

6. O que é uma password efetivamente segura

É um assunto muito debatido. Uma *password* segura, normalmente é considerada uma *password* com carateres diversos, como números e símbolos. Porém, matematicamente é mais difícil encontrar uma *password* mais longa do que uma mais curta, mesmo com carateres especiais e números.

Logo, sempre que criar uma *password*, opte por uma que seja mais longa.

Por exemplo:

A *password* "Esta é a minha password. Desde 1999" é matematicamente muito mais difícil de encontrar que "Edbrt99%%".

Algo que também é de extrema importância no que diz respeito a *passwords* é a frequência com a que devem ser alteradas. Não alterar uma *password* por longos períodos de tempo é dar oportunidade a um *hacker* de tentar encontrar essa password.

Em ambientes de segurança média aconselha-se a alteração a cada 60 dias e sem a possibilidade de utilizar as seis *passwords* anteriores.

Estas políticas deverão ser discutidas e aplicadas pelos departamentos de informática.

7. Como minimizar rapidamente todas as janelas

Para minimizar todas as janelas que possam conter informação confidencial ou sensível deve-se utilizar a combinação de teclas "windows" + "d".

"Windows" é a tecla com o símbolo do *Windows* que normalmente fica entre o CTRL e o ALT do lado esquerdo da barra de espaços.

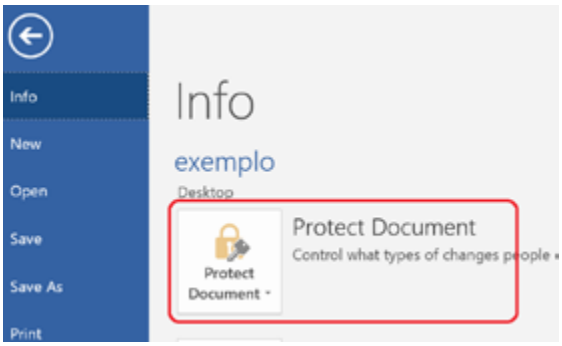
Isto funciona com todas as versões atuais suportadas do *Windows*.

8. Como por uma password num documento do Office

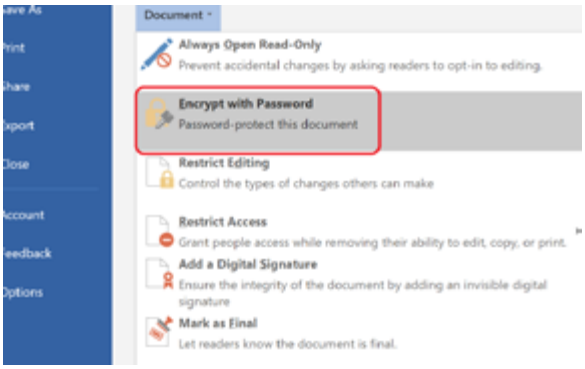
Os documentos do Office suportam a possibilidade de proteção utilizando uma *password*.

No Word, versão 2016, distribuída com o Office 365.

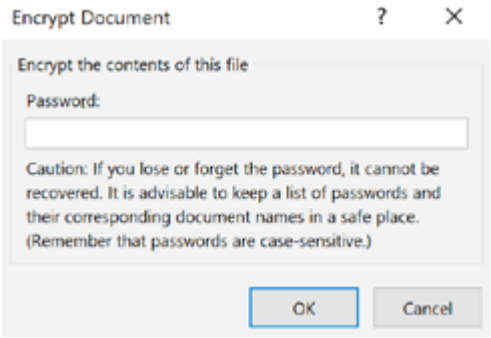
» Selecione "Ficheiro" e de seguida "Proteger Documento"



» Existem algumas opções de proteção, e como podemos ver algumas até são baseadas na identidade do utilizador, como a restrição de acesso ou edição.

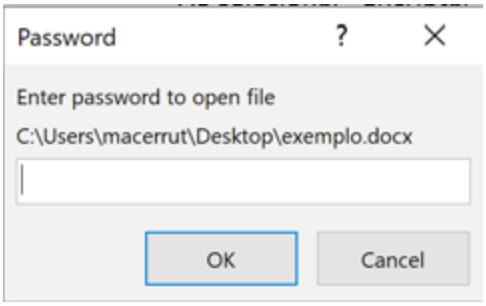


» Ao selecionar "Encriptar com password" é-nos solicitada a introdução de uma *password*



» Caso esta *password* seja perdida, não será possível aceder novamente ao ficheiro, logo é importante usar esta opção com cuidado.

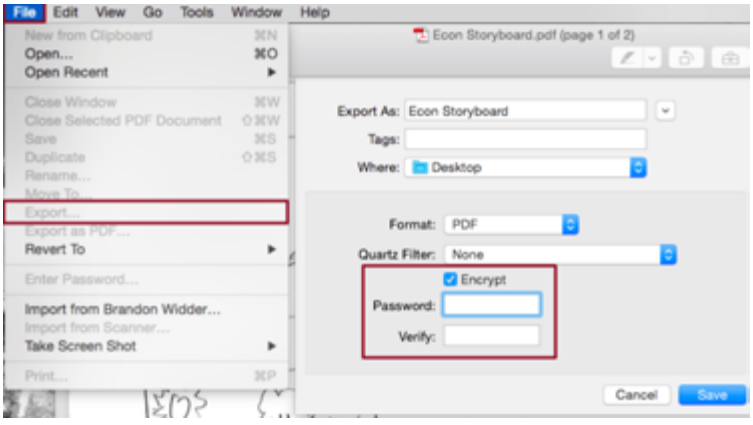
Para abrir o documento então, temos de teclar a *password*.



Para *Excel* o método é idêntico, assim como para *Powerpoint* e todas as outras ferramentas do *Office*.

9. Password num PDF

Tal como acima, e dependendo do *software* de PDF, é possível de facto proteger um PDF ao nível do ficheiro.



Usando *software* da Adobe é possível definir uma *password* no menu de exportação do ficheiro.

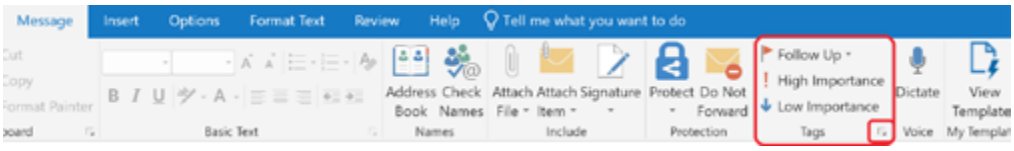
10. Pedir recibos de entrega por mail

Como descrito nos procedimentos, devemos apagar sempre os dados sensíveis da nossa caixa postal "enviados" para minimizar o risco de divulgação.

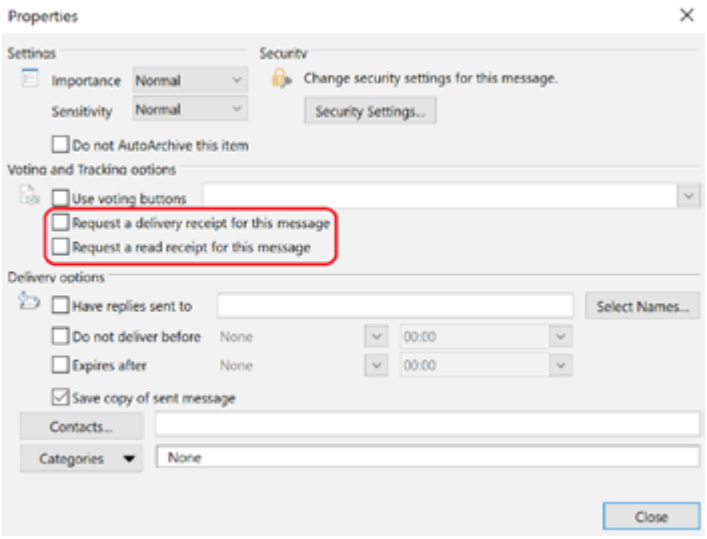
Mas no caso em que seja absolutamente necessário manter um histórico das comunicações de *email* é extremamente importante pedir recibos de entrega e de leitura.

Em Outlook 2016 pode fazer-se da seguinte forma:

» Num *email* novo, selecionar "*tags*"



» Nas propriedades pode selecionar "Pedir recibo de leitura" ou "Recibo de entrega"



11. Como encriptar totalmente um disco rígido

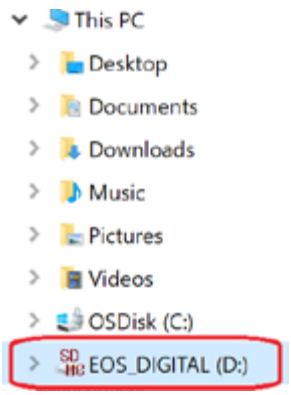
Um disco rígido amovível, fixo, uma *pen* USB ou mesmo cartões de memória podem ser encriptados.

Como vimos este método deve ser utilizado, em primeiro lugar, em portáteis ou computadores suscetíveis de extravio. Desta forma mesmo que alguém consiga abrir o PC e remover o disco para o colocar noutro PC não irá conseguir aceder aos dados, devido à encriptação.

Também devemos aplicá-lo a discos que contenham dados em transporte para a partir do nosso cliente.

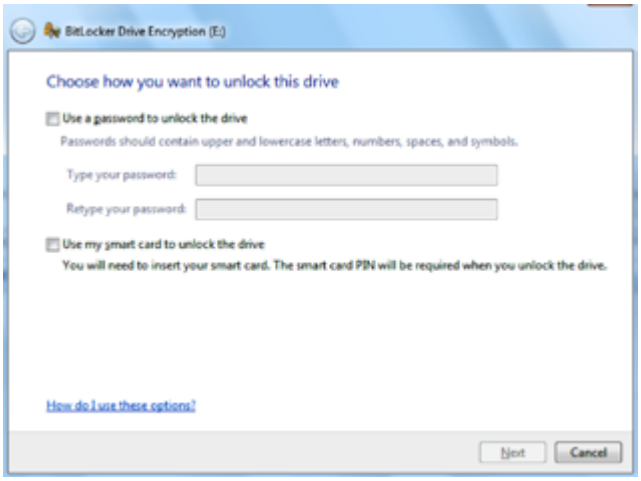
Para encriptar um disco podemos utilizar a ferramenta *bitlocker* do Windows.

» Selecionar no Windows Explorer o disco que queremos encriptar, com o botão direito do rato.

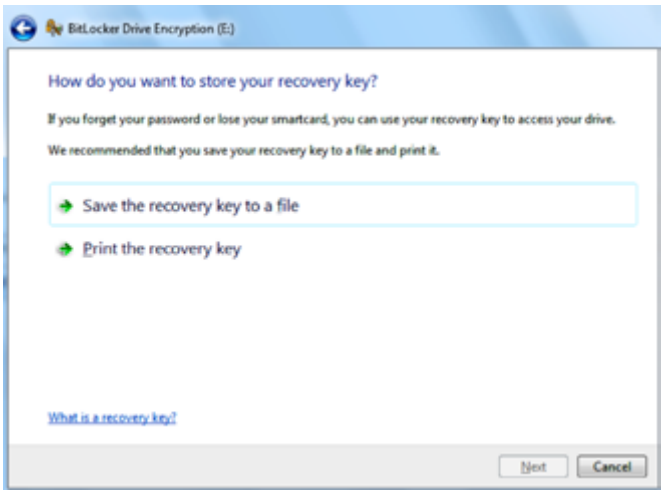


» Seleccionar "Ativar Bitlocker"

» Podemos então selecionar um de dois métodos: uma *password* ou um *smart card* para desencriptar os ficheiros.



» Podemos então teclar a *password* e de seguida, para garantir que não perdemos acesso aos dados, podemos imprimir ou guardar uma chave de recuperação



» A encriptação pode demorar algum tempo, dependendo do tamanho do disco

» Ao colocar o disco noutro PC, teremos então de inserir a *password* para que os ficheiros possam ser lidos.

www.occ.pt

Avenida Barbosa du Bocage, 45 | 1049-013 Lisboa
Tel. 217 999 700 Fax. 217 957 332
Email: geral@occ.pt