

Boas Práticas na utilização dos Sistemas de Tecnologia de Informação e Comunicação e no Tratamento de Dados Pessoais

Regulamento Geral de Proteção de Dados (RGPD)

Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016 que revoga a Diretiva 95/46/CE



RGPD: Enquadramento e conceitos gerais.....	3
Gestão da informação.....	5
Atribuição de acessos.....	7
Utilização de equipamento informático ou de telecomunicações.....	9
Utilização de dispositivos de armazenamento externo (Pen drive ou disco externo).....	11
Utilização de correio eletrónico.....	12
Utilização e acesso à Internet.....	16
Controlo de dados de comunicações telefónicas e de dados de tráfego.....	17
Acesso remoto ao computador do trabalhador.....	18

O Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, designado por RGPD - Regulamento Geral de Proteção de Dados, veio introduzir um novo regime em matéria de proteção de dados pessoais, tendo revogado a Diretiva 95/46/CE e é aplicável a partir de **25 de maio de 2018**.

Para além do reforço da proteção jurídica dos direitos dos titulares dos dados, o RGPD preconiza **novas regras e procedimentos** do ponto de vista tecnológico e alteração de paradigma no tratamento dos dados pessoais.

Esta nova relação entre os Sistemas de Tecnologia de Informação e Comunicação e a Legislação sobre o Tratamento de Dados Pessoais, está espelhada no RGPD, da seguinte forma:

- na **proteção de dados** desde a conceção e por defeito (artigo 25.º do RGPD)
- nas medidas adequadas para garantir a **segurança do tratamento** (artigo 32.º do RGPD)
- na notificação de **violações de dados pessoais às autoridades de controlo** (artigo 33.º do RGPD)
- na comunicação de **violação de dados pessoais aos titulares dos dados** (artigo 34.º do RGPD)
- na avaliação de **impacto sobre a proteção de dados** (artigo 35.º e seguintes do RGPD)

Com o intuito de minimizar o impacto do incumprimento deste novo enquadramento legal, importa clarificar qual a operação ou conjunto de operações de tratamento de dados pessoais, que poderão estar presentes na utilização dos Sistemas de Tecnologia de Informação e Comunicação:

- Recolha
- Registo
- Organização
- Estruturação
- Recuperação
- Conservação
- Utilização
- Interconexão
- Consulta
- Alteração
- Divulgação
- Apagamento

O RGPD considera **CRIME**, se durante a operação ou conjunto de operações de tratamento de dados pessoais, se verificar uma ou mais das seguintes ações:

- Utilização de dados de forma incompatível com a finalidade
- Acesso indevido
- Desvio de dados
- Viciação ou destruição de dados
- Inserção de dados falsos
- Violação do dever de sigilo
- Desobediência

O tratamento de dados pessoais decorrentes do controlo da utilização das tecnologias de informação e comunicação no contexto laboral, o controlo do correio eletrónico e do acesso à Internet obedece ao justo equilíbrio entre a tutela da esfera jurídica do colaborador e o princípio da liberdade de organização dos meios de trabalho, com especial respeito do princípio da legalidade, devendo conciliar especialmente estes princípios com os direitos fundamentais da reserva da intimidade da vida privada e da proteção de dados pessoais.

Com o intuito de proteger os ativos de informação detidos e utilizados pela DGSS de todas as ameaças, internas ou externas, deliberadas ou acidentais, foi estabelecido um conjunto de boas práticas que devem ser observadas, visando igualmente defender os pilares básicos da **confidencialidade**, **integridade** e **disponibilidade** da informação.



Toda a informação institucional apenas deve ser disponibilizada a entidades autorizadas
(**confidencialidade**)



Toda a informação institucional e privada / pessoal, mantém-se íntegra quando é armazenada com as suas características originais, ou seja, sem alterações (**integridade**)

Toda a informação institucional deverá estar disponível sempre que os utilizadores autorizados, dela necessitem (**disponibilidade**)

Não deve ser realizada a troca de dados ou informação institucional entre computadores ou equipamentos informáticos da DGSS que tenham instalada a Estação Padrão e equipamentos pessoais do trabalhador, via Bluetooth ou conectividade de rede (via cabo, sem fio ou por dados móveis) ou com recurso a periféricos de armazenamento externo de dados (PEN Drive ou disco externo) ou ainda através de qualquer outro sistema de troca de dados ou informação.



O acesso às aplicações disponibilizadas na **Estação Padrão** pelo Instituto de Informática, I.P., é atribuído segundo as necessidades inerentes à categoria profissional e à área de atividade própria de cada uma das unidades orgânicas da DGSS e dos respetivos trabalhadores.

Para além das aplicações informáticas disponibilizadas na Estação Padrão, não é permitido o acesso a outras aplicações informáticas.

A informação disponibilizada em qualquer aplicação específica e que contenha informação pessoal de terceiros, não pode ser divulgada para outros fins diferentes do que aquele para que está habilitada e para o fim a que é realizada a consulta.



UTILIZAÇÃO DO EQUIPAMENTO INFORMÁTICO OU DE COMUNICAÇÕES

É expressamente proibido qualquer tipo de conectividade (por cabo ou sem fios) de qualquer computador ou equipamento informático pessoal do trabalhador, à rede da DGSS ou domínio do MTSSS.



Também é proibido a ligação de qualquer dispositivo periférico de comunicação móvel de dados (PEN de Banda Larga ou Router) aos computadores ou equipamentos informáticos da DGSS, que não sejam os dispensados pelo NTIC.

Não é permitido ao trabalhador deixar um computador desacompanhado e ligado à rede da DGSS ou domínio do MTSSS, com a palavra-passe ou palavra-chave introduzida (a Estação Padrão deve ficar sempre bloqueada quando há ausência do posto de trabalho por períodos curtos de tempo).



No fim do dia de trabalho, **entre 2ªfeira e 5ªfeira**, inclusive, ou quando há ausências mais prolongadas deve ser sempre realizado o procedimento de encerrar o posto de trabalho (computador ou equipamento informático, impressoras locais, certificadoras, digitalizadores de secretária e monitor).

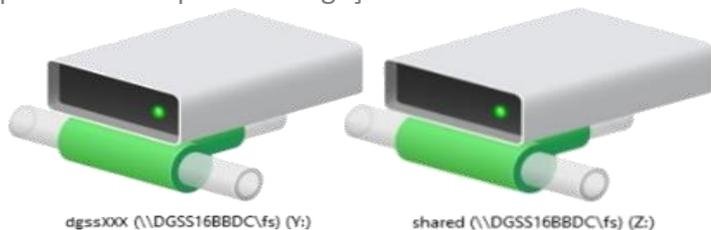
No fim do dia de trabalho, à **6ªfeira** ou noutro dia qualquer que seja o último da semana, deve ser realizado o procedimento de terminar sessão no computador, desligando sempre as impressoras locais, certificadoras, digitalizadores de secretária e monitor.

UTILIZAÇÃO DO EQUIPAMENTO INFORMÁTICO OU DE COMUNICAÇÕES

Para aplicação da regra de separação inequívoca de pastas institucionais (profissionais) e privadas / pessoais no sistema de informação da DGSS, os trabalhadores devem armazenar os ficheiros, nos seguintes locais:

DOCUMENTOS INSTITUCIONAIS

pastas ou subpastas na ligação à unidade = Y: ou Z:



Os ficheiros com **conteúdo de vídeo ou fotografias** que não sejam de caráter institucional não podem ser guardados em nenhuma pasta ou subpasta nas ligações às unidades = W:, Y: ou Z:



Em caso de **perda** ou **extravio** de equipamento institucional de comunicações (telemóvel) ou informático (portátil), o trabalhador deverá de imediato reportar às autoridades e o auto de notícia (documento de participação) recebido, deve ser disponibilizado ao NTIC o mais rapidamente possível (1º dia útil seguinte à ocorrência). Se a situação ocorrer em dias úteis e no horário de funcionamento da DGSS, deverá ser alertado de imediato o NTIC, de modo a realizar os procedimentos que protejam a informação contida no equipamento.

DOCUMENTOS PRIVADOS / PESSOAIS

pastas ou subpastas na ligação à unidade = L:



UTILIZAÇÃO DE DISPOSITIVOS DE ARMAZENAMENTO EXTERNO

(PEN DRIVE OU DISCO EXTERNO)

Qualquer dispositivo periférico de armazenamento externo de dados com conectividade USB (PEN Drive ou disco externo), só pode ser instalado ou configurado, pelo NTIC, em qualquer computador ou equipamento informático da DGSS que tenha instalada a Estação Padrão e que esteja ligado à rede da DGSS ou domínio do MTSSS, independentemente de pertencerem à DGSS ou aos próprios utilizadores.



HD



DVD



CD



Pendrive



Cartão SD



Memory Stick



HD Portátil



Disquete



Deve ser evitada a colocação de um periférico de armazenamento externo de dados com conectividade USB (PEN Drive ou disco externo) quando se liga o computador ou equipamento informático da DGSS, de forma a evitar a proliferação de possível *malware* ou outros veículos de infeção.

Os periféricos de armazenamento externo de dados (PEN Drive) pessoais do trabalhador, devem ser formatados em computadores ou equipamentos pessoais do trabalhador, antes de serem utilizados e ligados a computadores ou equipamentos informáticos da DGSS que tenham instalada a Estação Padrão e que estejam ligados à rede da DGSS ou domínio do MTSSS.

A DGSS disponibiliza o uso de um sistema de correio eletrónico aos seus trabalhadores para o desempenho das suas funções.

É, porém, permitido o uso pessoal e ocasional do correio eletrónico, sendo as mensagens pessoais tratadas como “pessoais”.

Os **procedimentos** a adotar deverão ser os seguintes:



- No envio de correio pessoal, deverá ser retirada a assinatura institucional;
- Não deve ser alterada a informação da assinatura oficial / institucional do correio eletrónico adotada pela DGSS quando o trabalhador responde institucionalmente, excecionando-se o envio de correio eletrónico pessoal ou com destinatário não institucional.
- Os utilizadores do correio eletrónico devem criar uma pasta pessoal independente para arquivo de informação pessoal, que deve ter uma designação intuitiva do seu carácter privado / pessoal, de modo a permitir a sua rápida identificação.
- Também pode ser disponibilizado ao utilizador, o acesso à caixa de correio institucional da respetiva Unidade Orgânica a que pertence, sendo o acesso atribuído segundo as necessidades inerentes à sua área de atividade e mediante solicitação expressa da chefia dessa Unidade.

Outlook® Web App

Domínio\nome de utilizador:

Palavra-passe:

 [iniciar sessão](#)

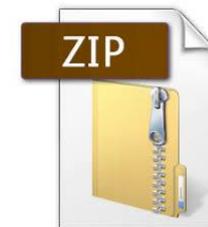
A DGSS permite ao trabalhador o acesso ao seu correio eletrónico institucional via Web, num computador ou equipamento informático sem a Estação Padrão e fora da rede do MTSSS, desde que a conectividade de rede (via cabo, sem fio ou por dados móveis) seja realizada de forma segura, as suas credenciais de acesso (nome de utilizador e palavra-passe ou palavra-chave) sejam válidas e que nunca sejam guardadas no equipamento utilizado, bem como, em termos de utilização, o tempo seja o mínimo necessário para a obtenção da informação pretendida.

Nenhum trabalhador pode utilizar o sistema de correio eletrónico de forma que essa utilização possa ser interpretada como ofensiva por qualquer outra pessoa, organismo ou instituição, ou de qualquer outra forma que possa ser considerada prejudicial para a imagem da própria DGSS.

Não é permitido o envio ou receção de anexos (documentos ou ficheiros) com **conteúdo de vídeo**, exceto em casos excecionais, devidamente ponderados.



Ao anexar ficheiros ao correio eletrónico de saída, deve ser utilizado o programa **compressor de ficheiros** instalado na Estação Padrão.



Na utilização do correio eletrónico, deve ser tomada especial atenção a:



FONTES DESCONHECIDAS

- não abrir correio eletrónico desconhecido;
- não clicar em ligações e/ou atalhos (link's e URL's) que possam ser suspeitas;

INFORMAÇÃO SENSÍVEL

- não enviar em correio eletrónico, credenciais de acesso (nome de utilizador e palavra-passe ou palavra-chave) de nenhum sistema operativo ou aplicacional;

SPAM E CORREIO ELETRÓNICO NÃO SOLICITADO



- não dar seguimento a “correntes” e eliminar ou colocar na pasta de “correio eletrónico não solicitado”, todo o correio eletrónico que se enquadre nesta categoria;

**Dizemos NÃO
ao Spam**



FICHEIROS ANEXOS

- não podem ser abertos anexos de correio eletrónico que sejam executáveis (ficheiros *.exe, *.bat, *.cmd,...);
- não enviar ficheiros cujo tamanho máximo exceda os 10MB.

Nas situações de ausência programada (v.g., férias, licenças), o trabalhador deve adotar o mecanismo de “Respostas automáticas (Fora do escritório)”, com indicação de endereço alternativo dentro da DGSS e no domínio seg-social.pt.



Respostas Automáticas (Fora do Escritório)

Utilize respostas automáticas para notificar outros quando estiver fora do escritório, de férias, ou não estiver disponível para responder a mensagens de correio eletrónico.

O acesso pontual por terceiros (NTIC/Instituto de Informática, I.P.) ao correio eletrónico dos trabalhadores da DGSS, nos casos e circunstâncias em que tal seja permitido por decisão do âmbito disciplinar, policial ou judicial, ou por outro motivo justificado, é sempre realizada na presença do trabalhador visado e/ou de terceiro por ele indicado.



A DGSS disponibiliza o acesso à Internet aos respetivos trabalhadores no sentido de os ajudar no seu desempenho profissional, presumindo-se sempre que o seu uso é limitado às atividades e missão da DGSS.

No procedimento de manipulação e acesso a qualquer navegador de rede, navegador web, navegador da internet ou simplesmente navegador (browser) deve ser tomada especial atenção a:

TEMPO

Os navegadores devem permanecer abertos durante o menor período de tempo possível (*1);



CREDENCIAIS DE ACESSO

Quando o acesso à página de navegação solicitar credenciais de acesso (nome de utilizador e palavra-passe ou palavra-chave), deve ser efetuado, no início, o ligar (logon ou login) e, no fim, o desligar (logoff ou logout) do site ou sistema em que se encontra;



SITES SEGUROS

Sempre que possível, o acesso aos sites deve ser realizado através de ligação segura (HTTPS) ou que garanta a integridade dos certificados (que possuam um cadeado “fechado” na barra do endereço ou URL)



DOWNLOAD

Não é permitido efetuar download de software não autorizado / não institucional de e em qualquer navegador;



Recomenda-se que no navegador de rede, navegador web, navegador da internet ou simplesmente navegador (browser), o utilizador recuse a possibilidade de armazenamento das credenciais, dados e informação pessoal (*1), evitando a credenciação abusiva através de veículos de infeção automática ou manual.

(*1) Resolução do Conselho de Ministros n.º 41/2018, de 28/03, publicada em *Diário da República*, 1.ª série — N.º 62

CONTROLO DE DADOS DE COMUNICAÇÕES TELEFÓNICAS E DE DADOS DE TRÁFEGO

A DGSS providencia o acesso à utilização de telefones fixos ou móveis aos seus colaboradores, no sentido de os ajudar no seu desempenho profissional, presumindo-se sempre que o respetivo uso é limitado às atividades e missão da DGSS.



Nos termos da Deliberação n.º 1638/2013 da CNPD, de 16/07, a DGSS admite a utilização das comunicações telefónicas fixas ou móveis, no tempo e local de trabalho, para fins privados, bem como a proibição de acesso ao conteúdo das comunicações, a utilização de qualquer dispositivo de escuta, armazenamento, interceção e vigilância de comunicações.



ACESSO REMOTO AO COMPUTADOR DO TRABALHADOR

As ferramentas de controlo à distância no acesso remoto a computadores só podem ser utilizadas para assistência técnica (NTIC), a pedido ou com o conhecimento do trabalhador, e sempre que ocorra esse tipo de intervenção.

