SPMS EPE
Serviços Partilhados do Ministério da Saúde

A Segurança da Informação

- Informação ao Colaborador

REPÚBLICA PORTUGUESA
SAÚDE

SNS
SERVIÇO NACIONAL DE SAÚDE

SPMS EPE
Serviços Partilhados do Ministério da Saúde

Índice

REPÚBLICA PORTUGUESA
SAÚDE

SNS
SERVIÇO NACIONAL DE SAÚDE

O que é a segurança da informação?

É um processo organizado e estruturado que permite preservar a confidencialidade, integridade e a disponibilidade da informação

Tríade da Segurança da Informação

Confidencialidade: Garante que a informação não está disponível, acessível ou é divulgada a indivíduos ou entidades não autorizadas.

Integridade: Garante que a informação está correta e completa, assegurando a sua proteção contra corrupção ou alteração não autorizada.

Disponibilidade: Garante que a informação está acessível e pode ser utilizada sempre que solicitada por um indivíduo ou entidade autorizada.

Responsáveis e Princípios

Todos nós somos responsáveis pela segurança da informação e todos temos a responsabilidade de proteger os nossos dados e os que nos são confiados.

✓ Estarmos cientes da elevada importância da segurança da informação para a nossa organização e tratamo-la de forma adequada;

✓ Implementamos procedimentos sistemáticos que visam a redução dos riscos e não interrupção ou adulteração da informação;

✓ Incutimos a responsabilidade pela segurança da informação;

✓ Estabelecemos medidas adequadas à nossa organização para garantir a segurança da informação.

✓ Verificamos regularmente o respetivo cumprimento e a eficácia;

✓ Protegemos a informação própria e a que nos é confiada, impedindo a sua divulgação e alteração ilegal;

✓ Reagimos de imediato e adequadamente à situação em caso de violação da segurança.

02 | Gestão de acessos e passwords

I - Use Passwords Fortes e Únicas

- Use passwords que combinem letras maiúsculas e minúsculas, números e símbolos. Evite informações fáceis de adivinhar, como aniversários ou sequências.
- Evite reutilizar a mesma password em diferentes contas e sistemas.
- Use um gestor de passwords para armazenar as suas credenciais de maneira segura, evitando a necessidade de memorizá-las ou anotá-las em lugares inseguros.
- As passwords não devem ser divulgadas a quaisquer outras pessoas, incluindo colegas.
- Altere as suas passwords regularmente, especialmente para contas que acedem a dados sensíveis ou confidenciais.
- Não reutilize senhas antigas.

Passwords de utilizador em geral: deve ter no mínimo 8 caracteres e ser complexa. Neste caso, a sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres:

- letras minúsculas (a…z), letras maiúsculas (A…Z), números (0…9) e caracteres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : “ ; ‘ < > ? , . /);
- Passwords contas privilegiadas: Deve ter no mínimo 13 caracteres e ser complexa conforme regra acima.
- A implementação de regras como:
  - Não criar passwords que sejam facilmente associadas ao utilizador (e.g. nomes próprios, matrículas de veículos, datas de aniversário).
  - Não reutilização das últimas 10 passwords

02 | Gestão de acessos e passwords

II - Autenticação Multifator (MFA) e VPN

- Ativar o **MFA** dificulta o acesso para cibercriminosos, mesmo que descubram a sua password.
- Sempre que possível, prefira aplicações de autenticação (como Google Authenticator ou Microsoft Authenticator) em vez de SMS, pois eles são mais seguros.
- **Proteção de Dados Pessoais:** Redes públicas de Wi-Fi são alvos fáceis para cibercriminosos que podem intercetar suas informações. Uma **VPN** criptografa seus dados, tornando-os ilegíveis para qualquer pessoa que tente acede-los.
- **Privacidade:** Ao usar uma **VPN**, seu endereço IP e suas atividades de navegação são mascarados. Isso impede que provedores de internet, anunciantes e possíveis invasores rastreiem seus hábitos online.
- **Segurança Adicional:** Além de proteger seus dados, uma **VPN** também ajuda a evitar ataques de phishing e outras ameaças cibernéticas, proporcionando uma camada extra de segurança enquanto você navega.

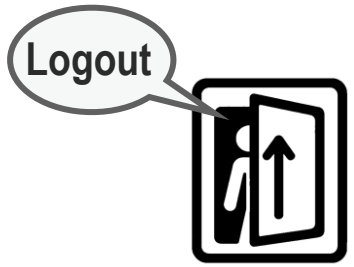
02 | Gestão de acessos e passwords

III – Garanta o Ciclo de Vida dos Acessos e Princípios da na Necessidade de saber e Segregação de Funções

- Conceda e requeira apenas o acesso mínimo necessário para o seu trabalho e funções.
- Se precisar de acesso adicional para uma tarefa específica, solicite apenas um acesso temporário.
- Desative ou reconfigure os acessos que já não são necessários.
- Realize uma revisão periódica dos acessos, verificando se ainda precisa ter acesso a determinados sistemas e removendo permissões desnecessárias.
- Certifique-se de que processos críticos são divididos em etapas executadas por pessoas diferentes.

IV - Cuidado com Sessões Abertas em Dispositivos Não Seguros

- Nunca faça login em sistemas corporativos a partir de computadores ou redes públicas, pois podem estar comprometidos com softwares maliciosos ou malware.

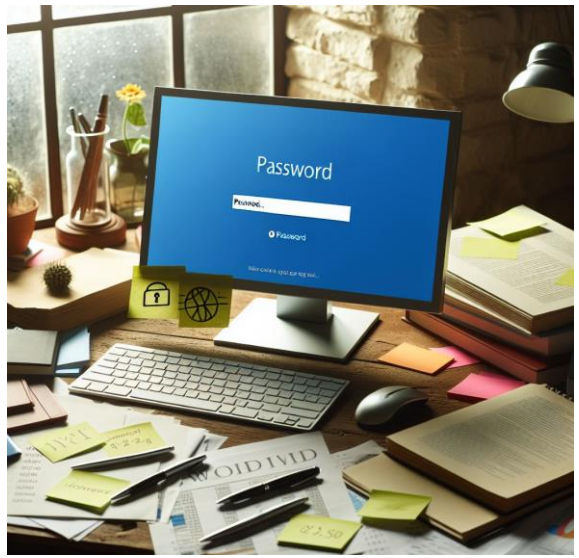


- Lembre-se de sempre fazer logout das suas contas ao finalizar o trabalho, especialmente em equipamentos partilhados ou não corporativos.

03 | Posto de trabalho e salas de reuniões

I - Use apenas equipamentos permitidos:

- Utilize os equipamentos disponibilizados pela organização, pois eles são configurados e protegidos para o ambiente corporativo.
- Evite conectar pendrives ou discos rígidos pessoais ou de outras pessoas no computador de trabalho, pois eles podem estar contaminados com malware.
- No caso de ser permitido BYOD (*Bring Your Own Device*) na sua organização, garanta o cumprimento das medidas de segurança.



II - Bloqueie o Computador ao Afastar-se e Mesa Limpa

- Use atalhos como Windows + L no Windows ou Command + Control + Q no Mac para bloquear o ecrã sempre que se afastar dele.
- O ecrã do computador deve ser sempre posicionado de maneira a evitar que terceiros possam ler informações do mesmo
- Ative o bloqueio automático de ecrã para que o computador se bloqueie sozinho após alguns minutos de inatividade, garantindo proteção mesmo que se esqueça.
- Guarde papeis e ficheiros com informação em gavetas e armários fechados à chave.
- Evite deixar documentos sem supervisão.

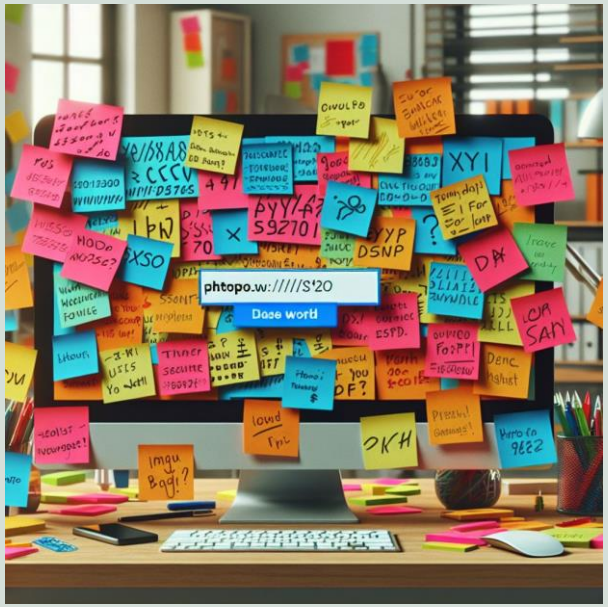
03 | Posto de trabalho e salas de reuniões

III - Mantenha o Dispositivo e Aplicações Atualizados

- Não ignore as mensagens de atualizações.
- Mantenha o sistema operativo, aplicações e browsers atualizados para proteger contra vulnerabilidades de segurança.
- A instalação de aplicações e programas deve ser feita por pessoal autorizado e através de fontes confiáveis.
- Apenas utilize software devidamente autorizado e devidamente licenciado.

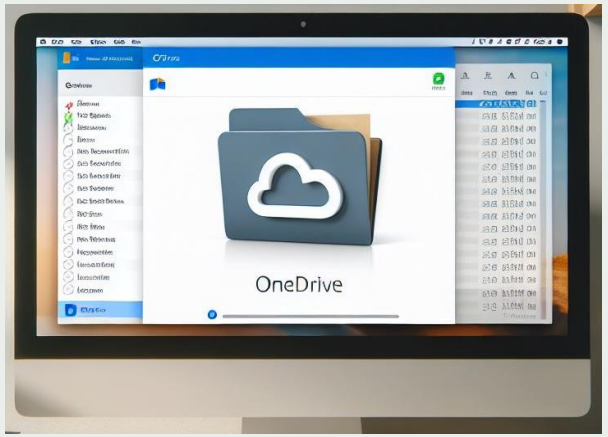
IV- Evite Post-its e Anotações Visíveis com Informações Confidenciais

- Não deixe senhas ou credenciais anotadas em post-its, papéis colados no monitor ou em documentos sem proteção.
- Qualquer anotação com dados sensíveis, como dados de acesso, deve ser armazenada em local seguro e nunca deixada exposta.



V - Evite Salvar Dados Confidenciais Localmente e Faça Backups:

- Sempre que possível, armazene a informação em arquivos seguros fornecidos pela organização, como unidades de rede ou soluções de armazenamento em nuvem (ex. Sharepoint ou OnDrive).
- Realize backup regular dos arquivos em locais seguros.
- Se precisar descartar arquivos sensíveis, certifique-se de que eles são apagados de forma segura e definitiva.



04 | O correio eletrónico e NetEtiqueta

I - Cuidado com E-mails e Mensagens Suspeitas

- Verifique sempre o remetente e desconfie de e-mails ou mensagens que pedem informações urgentes e confidenciais.
- Avalie com atenção os pedidos/plataformas de login ou de partilha de palavras-passe ou outros dados sensíveis.

- Se um e-mail tiver um link, passe o cursor sobre ele (sem clicar) para ver o endereço completo. Se parecer suspeito, não clique.
- Se receber um e-mail estranho de um “conhecido”, confirme com a pessoa por outro meio antes de responder.

II – Cautela no Envio de E-mails

- Verifique sempre o endereço dos destinatários a quem pretende enviar o email.
- Não encaminhe mensagens para endereços externos à organização, sem verificar a legitimidade e a segurança do destinatário.
- Não reencaminhe informação da organização para e-mails pessoais.

04 | O correio eletrónico e NetEtiqueta

SPMS EPE Serviços Partilhados do Ministério da Saúde

III – Reporte E-mails Suspeitos:

- Caso receba um e-mail suspeito ou mensagens estranhas, avise imediatamente a equipa de cibersegurança ou de informática de sua entidade.
- O reporte de incidentes de cibersegurança pelos utilizadores pode minimizar impactos na organização e prevenir riscos para outros utilizadores.
- É essencial o reporte em situações que tenha colocado o seu email ou password em sites ou campanhas fraudulentas.

CSIRT
Serviços Partilhados do Ministério da Saúde

csirt@spms.min-saude.pt

IV – Use o E-mail Profissional para Fins Corporativos

- Não associe a sua conta de e-mail profissional em sites ou redes sociais.
- Divulgar o seu e-mail profissional publicamente pode trazer riscos de segurança para entidade.
- O envio ou receção de informação relacionados com atividades da entidade deve ser efetuado por via de contas de email corporativas, e não através da utilização de emails pessoais.

REPÚBLICA PORTUGUESA SAÚDE

SNS SERVIÇO NACIONAL DE SAÚDE

04 | O correio eletrónico e NetEtiqueta

- Evite escrever mensagens em MAIÚSCULAS com cores e a bold ;
- Tente ser claro e objetivo, produza textos simples com cuidado gramatical e ortográfico;
- Tente ser educado e simpático, agradeça e cumprimente;
- Pode usar smileys :-) é uma forma simples de dar a entender os seus sentimentos;
- Não reaja de forma emotiva porque fazendo assim normalmente escrevemos e-mails ou partilhamos o que não queremos;
- Antes de publicar alguma informação verifique se o conteúdo:
  - Tem interesse e agrega valor ?
  - Tem qualidade e é atual respeitando a missão da organização?
  - Tem o formato correto e está a ser publicado no dia, hora e local correto?

05 | Phishing, vírus e ransomware

O **Phishing** é uma das principais preocupações ao nível da segurança da informação. Trata-se de um crime informático baseado no envio de um e-mail fraudulento com o objetivo de obter dados pessoais ou confidenciais.
Trata-se de um e-mail falso ou mensagem, normalmente emitido em nome de uma entidade credível tal como um Banco, Facebook, Twitter, Microsoft, Vodafone, a própria organização, etc., mas que na realidade só pretende recolher dados ou infetar os sistemas.

Os **vírus** são programas maliciosos - **malware** que se espalham a outros computadores com o objetivo de permitir acessos ou danificar dados e serviços.

Existem diferentes tipos de vírus: o **spyware** que regista a atividade do utilizador e envia para o atacante; o **adware** que ataca o utilizador com publicidade; o **scareware** que é um falso alerta de vírus ou problemas informáticos que levam o utilizador a fazer o que lhe pedem, por como exemplo instalar um programa; e o **ransomware**, um dos mais agressivos e de maior impacto.

O **Ransomware** é uma estratégia de resgate suportada por um software de encriptação que bloqueia o acesso aos ficheiros ou aos computadores, até que se pague o resgate.

Este software encripta os dados com uma chave secreta.

“O seu dinheiro ou os seus dados?”

Para recuperarmos os dados é necessário pagar um resgate.

05 | Phishing, vírus e ransomware

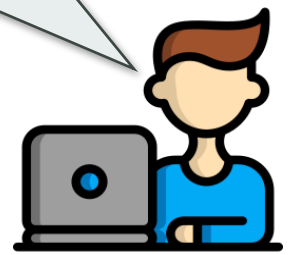
Os seis passos do Ransomware

1. O ransomware entra via e-mail ou download da internet
2. O utilizador abre o ficheiro e este executa-se
3. O software gera uma chave pública e uma privada
4. A chave privada é transferida para um servidor do atacante e é apagada do seu PC
5. O software começa a encriptar os seus dados com a chave publica;
6. Terminada a encriptação o software malicioso coloca uma mensagem no desktop com instruções para pagar o resgate com cryptomoeda.

NOTA: Se o seu computador detetar um vírus ou suspeitar de um comportamento anormal por favor siga os seguintes passos:

1. Desligue o Wi-Fi;
2. Remova o cabo de rede (ou retire o portátil da docking station);
3. Não desligue o equipamento;
4. Contacte imediatamente a equipa TIC e reporte o incidente.

UCS – Unidade de Cibersegurança
csirt@spms.min-saude.pt.



06 | A Internet e a Comunicação

Vivemos no mundo da informação e a comunicação é a chave do sucesso pessoal e empresarial. Por este motivo é fundamental garantirmos que comunicamos de forma adequada, nos meios adequados e apenas transmitimos a informação necessária.

No mundo da internet existem regras e códigos de conduta com o objetivo de melhorar a segurança da informação.

INTERNET

- ✓ Certifique-se que o site é seguro fazendo duplo clique sobre o cadeado ou aceda pelo endereço (URL) que deve começar por “https://” e não por “http://”;
- ✓ Certifique-se que o seu browser e o antivírus estão atualizados e utilize uma firewall pessoal;
- ✓ Consulte os extratos das suas contas bancárias e de serviços com regularidade. Se encontrar algum movimento estranho, contacte imediatamente o prestador de serviço ou banco;
- ✓ Não é permitido aceder a sites com conteúdos ilegais ou inadequados;
- ✓ Atualize as suas passwords/PIN a cada 90 dias.
- ✓ Utilize passwords diferentes para sites seguros e sites não seguros, para uso profissional e para uso pessoal;
- ✓ Não é permitido utilizar serviços públicos ou pessoais de e-mail, de transferência de ficheiros e ou serviços cloud para troca de dados da organização;
- ✓ Não é permitido divulgar informação ou dados corporativos nas redes sociais;
- ✓ Não é permitido jogar ou fazer apostas online com recursos da nossa organização (REDE, PCs, etc.).

COMUNICAÇÃO

- ✓ Quando fala ao telefone tenha cuidado para não divulgar informação confidencial;
- ✓ Evite falar de assuntos de trabalho em locais e transportes públicos, proteja-se contra os ouvintes;
- ✓ Evite ler informações críticas ou confidenciais em locais e transportes públicos;
- ✓ Evite abrir envelopes com dados confidenciais em espaços públicos;
- ✓ Não utilize redes sociais ou ferramentas (APPs) públicas para comunicar com parceiros e fornecedores.
- ✓ Não divulgue o e-mail e telemóvel de um colega sem que este o permita;
- ✓ Não coloque informações da organização em sites públicos (ex. Dropbox);
- ✓ Não registe o seu endereço de e-mail profissional em redes sociais ou sites de compras online;
- ✓ Não é permitido enviar dados da organização para e-mails pessoais (Ex. Gmail, Hotmail, etc.);
- ✓ Pense nas consequências antes de publicar qualquer informação, uma informação embaraçosa pode comprometer a sua imagem e a da sua organização.

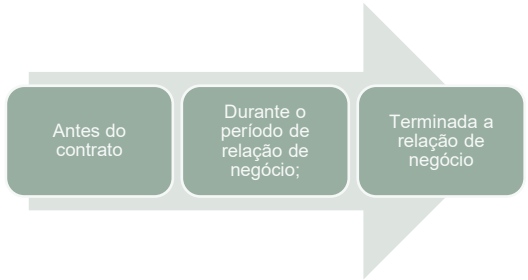
07 | Dispositivos móveis

Os equipamentos móveis são uma potencial fonte de perda de informação crítica de negócio e pessoal. Por este motivo, devem ser tratados com especial atenção e devem estar sempre protegidos. Olhe para os seus dispositivos móveis (telemóvel, portátil, PEN, token, pasta de documentos) e verifique se estão aplicadas algumas das seguintes regras de segurança.

- ✓ Todos os dispositivos portáteis estão protegidos com password;
- ✓ Os dispositivos portáteis devem ter os dados encriptados sempre que seja tecnicamente possível;
- ✓ O software deve estar atualizado. Sempre que possível ligue o seu equipamento à rede da organização para receber as devidas atualizações (pelo menos a cada 15 dias);
- ✓ O equipamento deve ter instalado um antivírus e uma firewall que devem estar atualizados;
- ✓ Devem ser feitas cópias de segurança dos dados ou utilizar os recursos disponibilizados pela Organizaçãpo como o OneDriver ou Sharepoint;
- ✓ Em locais públicos e transportes públicos os equipamentos devem estar sob vigilância constante;
- ✓ O trabalho com equipamentos móveis em locais públicos deve garantir que os dados do ecrã estão protegidos contra pessoas não autorizadas;
- ✓ Os equipamentos móveis não devem ser deixados nos veículos automóveis;
- ✓ O computador portátil deve estar sempre com o cadeado de segurança para evitar roubos;
- ✓ É proibido desbloquear equipamentos com recurso a ferramentas ou sistemas operativos não autorizados (ex. Jailbreak ou Root);
- ✓ Home-office - os documentos que são levados para trabalhar em casa devem estar protegidos contra acesso indevido.

08 | Parceiros externos

Existe uma ordem cronológica natural de relacionamento com os parceiros externos, esta ordem passa pelas seguintes fases:



Para todas estas fases estão definidas regras e boas práticas que garantem a proteção dos dados, e das infraestruturas da nossa organização e dos nossos parceiros. Estas regras aplicam-se a todos os parceiros externos.

Antes do contrato:

- ✓ Os parceiros e as empresas subcontratadas assinam um NDA - Acordo de Confidencialidade;
- ✓ Os parceiros que processam ou armazenam dados da nossa organização recebem um briefing de segurança da informação;
- ✓ São definidos os dados a serem trocados e os canais seguros para a troca;
- ✓ São definidos os interlocutores do parceiro e os nossos, e acordado entre ambos a forma de comunicar incidentes de segurança;
- ✓ Se forem trocados dados críticos (pessoais ou de negócio) os interlocutores devem garantir que foram tomadas as medidas de proteção técnicas e funcionais adequadas;
- ✓ O prestador de serviço apresenta um plano de segurança claro e atualizado;
- ✓ É assinado um contrato-tipo disponibilizado pelo Departamento Jurídico.

Durante a relação de negócio::

- ✓ São atribuídos acessos locais ou remotos aos parceiros de acordo com princípio do “Mínimo acesso permitido”;
- ✓ Os sistemas dos parceiros externos apenas podem ser instalados na nossa infraestrutura se existirem comprovadas razões técnicas ou económicas;
- ✓ Não é permitido instalar o nosso software em equipamentos de parceiros;
- ✓ Os nossos sistemas apenas podem ser colocados nas instalações dos parceiros após aprovação formal do CISO;
- ✓ Em todos os contratos deve ser assegurado o direito de auditoria aos parceiros e fornecedores, estas auditorias pode ser realizadas por nós ou por um parceiro escolhido pelas partes e acontecem no âmbito da prestação de serviço.

Terminada e relação de negócio:

- ✓ O interlocutor da organização informa todos as entidades envolvidas;
- ✓ Todos os privilégios são imediatamente eliminados;
- ✓ Todos os equipamentos são desligados e recolhidos.

09 | RGPD

O novo Regulamento Geral sobre a Proteção de Dados, constante do Regulamento (UE) 2016/679, foi publicado no Jornal Oficial da União Europeia no dia 4 de maio de 2016.

Este regulamento revoga toda a legislação publicada antes da era digital.

Este normativo comunitário, designado na língua inglesa por General Data Protection Regulation (GDPR), é aplicável a partir do dia 25 de maio de 2018.

Regras e Diretrizes:

- ✓ Novos direitos e obrigações, ex. direito ao esquecimento e a portabilidade dos dados, etc;
- ✓ Coimas elevadas em caso de incumprimento, até 20 milhões de euros ou 4% do volume anual de negócios do grupo;
- ✓ Incluir a privacidade desde a conceção como princípio orientador (*Privacy by default*);
- ✓ A confiança nas TIC, impõe garantir que as tecnologias não afetam os direitos fundamentais das pessoas à privacidade e à proteção dos dados pessoais (*Privacy by Design*)
- ✓ Princípio de responsabilidade na recolha e proteção dos dados, *Accountability e Opposition to Profiling*;
- ✓ Define a criação de uma nova função DPO - *Data Private Officer* que na língua portuguesa se designa por Encarregado de Proteção de Dados.

É importante saber:

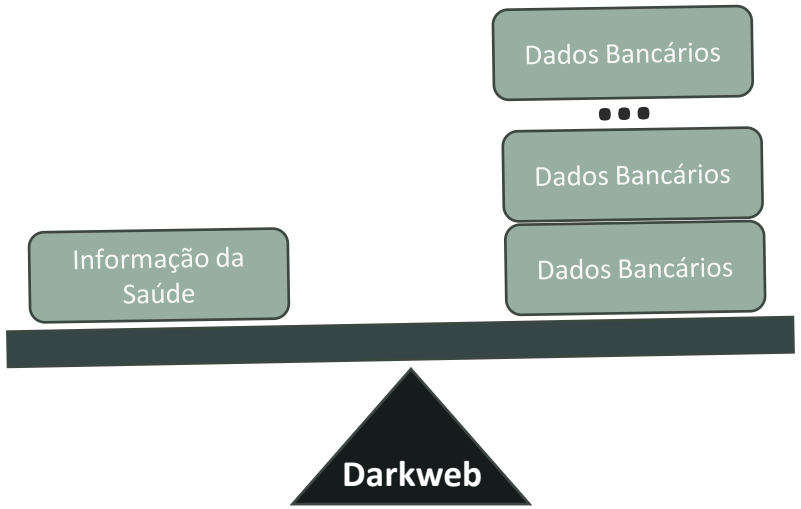
- ✓ O que são dados pessoais - são todas as informações relativas a uma pessoa identificada ou identificável (nome, morada, património, vencimento, datas, números de cartões, n.º de telefone, IP, vídeos, imagem, raça, dados biométricos, folhas de presença, avaliações, curriculum vitae, etc);
- ✓ Não deve reunir dados pessoais em papel ou em formato eletrónico sem informar o DPO;
- ✓ Cuidado ao enviar dados pessoais, estes devem estar sempre encriptados ou protegidos;
- ✓ Cuidado ao destruir ou eliminar dados pessoais, estes devem ser definitivamente apagados ou eliminados de forma a não serem recuperados por terceiros;
- ✓ Cuidado com os dados pessoais que troca com os seus parceiros e em especial com parceiros fora da EU; Documentos com dados médicos, e dados de menores são muitos sensíveis pelo que deve ter um cuidado redobrado na sua utilizaç ão;
- ✓ Se perder ou lhe roubarem dados pessoais informe de imediato o seu DPO;
- ✓ O DPO tem a obrigação de comunicar as autoridades todas as esfiltrações ou perdas de dados pessoais.

10 | Destruição de dados e impressões

Informação é um ativo com valor para o negócio. A informação pode existir sob várias formas, como por exemplo: em suportes de papel (folhetos, jornais, cartolinas, posters, etc.) ou suportes eletrónicos designados por media (CDs, disquetes, tapes, microfilme, discos rígidos, PEN USB, cartões de memória, etc.).

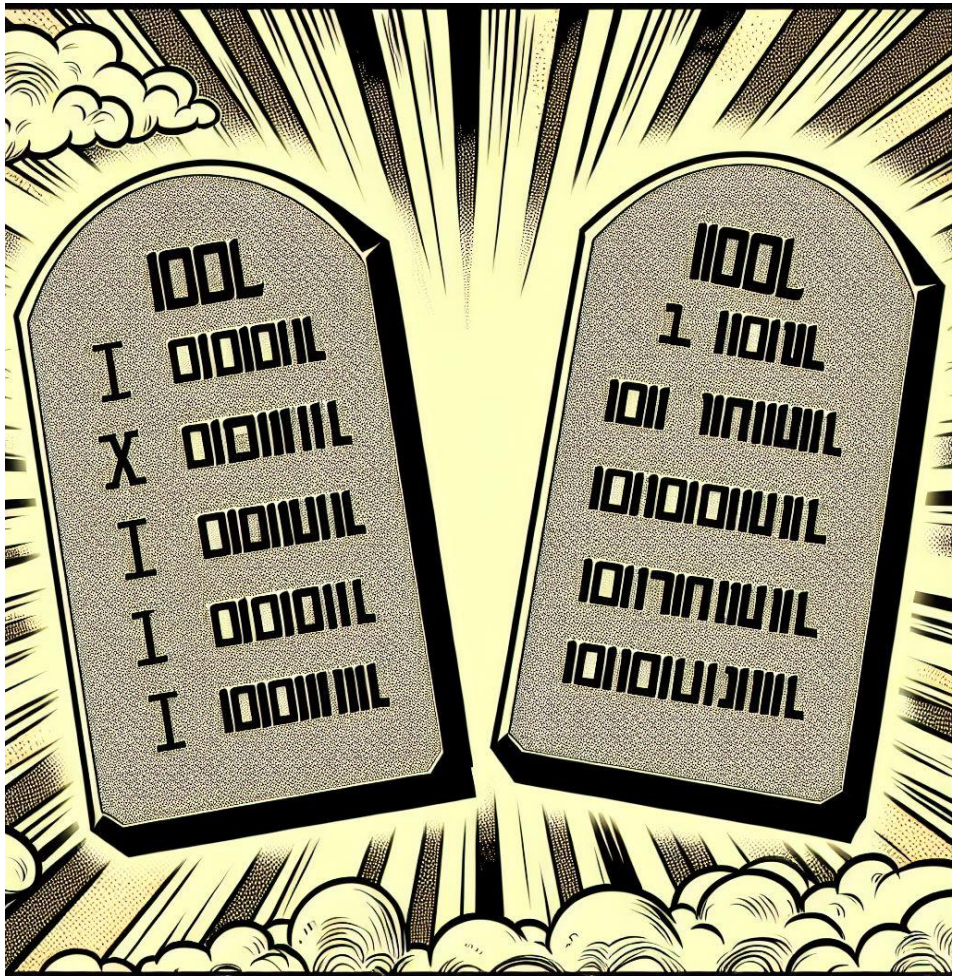
A destruição de informação confidencial deve ser realizada de acordo com regras de segurança e procedimentos adequados. Apenas empresas certificadas podem fazer a destruição da nossa informação.

Estas empresas garantem a recolha e o transporte dos documentos e equipamentos, em condições de rigorosa segurança, através da utilização exclusiva de viaturas próprias com caixa blindada, cumprindo os requisitos previstos na Lei da Proteção de Dados Pessoais e os requisitos associados ao acondicionamento e transporte de resíduos.



- No processo de destruição a empresa produz um relatório detalhado com a descrição dos dispositivos, quantidade e código de barras.
- A documentação e certificados de destruição ficarão à guarda do CISO.
- A destruição de grandes volumes de papel é feita a pedido.
- A destruição de pequenos volumes (documentos de trabalho e flip charts com informação confidencial) é realizada pelo próprio colaborador nos destruidores de papel disponibilizados pela empresa.
- A eliminação das impressões deve ocorrer no escritório. No escritório de casa, a eliminação de impressões só é permitida se os documentos forem cortados por uma trituradora de corte em pedaços com o máximo de 8 mm.
- Os equipamentos eletrónicos media só podem ser destruídos ou ter os dados apagados pelas TIC

11 | Dez Mandamentos de Segurança



1. Não introduzirás PENs alheias no PC de trabalho.
2. Não deixarás o teu PC desbloqueado, mesmo entre amigos ou colegas.
3. Não esquecerás os backups e apostarás nas redundâncias.
4. Não esquecerás de atualizar o antivírus.
5. Não cobiçarás phishing alheio.
6. Assumirás o papel de melhor linha de defesa contra os ciberataques.
7. Não desejarás trabalhar fora de ambientes e de redes seguras.
8. Não partilharás passwords e códigos de acesso.
9. Amarás as medidas de segurança sobre todas as coisas.
10. Não procrastinarás as atualizações, mesmo aos domingos e feriados.

SPMS EPE
Serviços Partilhados do Ministério da Saúde

REPÚBLICA PORTUGUESA
SAÚDE

SNS
SERVIÇO NACIONAL DE SAÚDE