Guia de Boas Práticas e Regras para sítios web SNS/MS

CIBERSEGURANÇA

REPÚBLICA PORTUGUESA
SAÚDE

40 ANOS
SNS
SERVIÇO NACIONAL DE SAÚDE 1979-2019

SPMS EPE
Serviços Partilhados do Ministério da Saúde

Cibersegurança
SNS

Índice

Glossário

Android
Sistema operativo móvel desenvolvido pela Google.

Anexos das mensagens
Arquivo qualquer (imagem, texto, vídeo, etc.) que é incorporado a uma mensagem de correio eletrónico.

Application Programming Interface (API)
Conjunto de comandos, funções, protocolos e objetos que os programadores podem usar para criar *software* ou interagir com um sistema externo.

Ataques
Tipo de atividade maliciosa que tenta coletar, perturbar, negar, degradar ou destruir recursos de sistema de informação ou a informação em si.

Ataques Man-In-The-Middle
Forma de ataque em que os dados trocados entre duas partes são de alguma forma intercetados, registados e possivelmente alterados pelo atacante sem que as vítimas se apercebam.

Autenticação da mensagem
Processo de validar o código de autenticação de uma mensagem, para obter a garantia de que um dado remetente emitiu essa mensagem para o destinatário previsto e de que a mesma não sofreu alterações durante a transmissão.

Autenticação do remetente
Verificação ou validação da identidade de uma pessoa ou da identificação de qualquer outra entidade através de um sistema de segurança.

Autenticidade
Num contexto informacional, propriedade de uma informação cuja origem e integridade são garantidas.

Biometria
Informações detalhadas sobre o corpo de alguém, como os padrões de cor em seus olhos, que podem ser usados para provar quem é essa pessoa.

Browser
Aplicação que serve para aceder a sítios *WEB*.

Chave criptográfica
Cadeia de *bits* que comanda as operações de um algoritmo criptográfico. O secretismo destas chaves garante, normalmente, a segurança da transformação (cifragem/decifragem), especialmente quando o algoritmo de transformação é, como desejável, público.

Cifra
Algoritmo de complexidade variável que permite a transformação de um texto claro num texto ilegível,

Cookies
Pacote de informação enviado de um servidor Web para um programa de navegação, e depois reenviado sempre que este aceda ao servidor.

Correio eletrónico
Qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha.

Criptografia
Aplicação de algoritmos matemáticos que cifram a informação, entre uma origem e um destino, para garantir atributos de segurança: autenticação, confidencialidade, integridade e não repúdio.

Domínios
Grupo de computadores e dispositivos de uma rede, em particular da *Internet*, que são administrados como uma unidade, com regras e procedimentos comuns, e que partilham um nome comum (nome do domínio).

Double Factor Authentication
Uso de fatores associados a conceitos básicos de autenticação: algo que eu sei, algo que eu tenho (cartão matriz, cartão de acesso ou token enviado para o telemóvel) e algo que eu sou. A dupla autenticação usa dois destes fatores.

Formato PDF
Formato de arquivo projetado para apresentar documentos de maneira consistente em vários dispositivos e plataformas.

HASH
Função que converte um valor noutro. Dados de *hash* são uma prática comum em ciência da computação e são usados para várias finalidades diferentes. Exemplos incluem criptografia, compressão, *etc*.

Hiperligações
Referência de algum ponto de um hipertexto para um ponto do mesmo ou de outro documento; uma tal referência é normalmente especificada de uma forma diferenciada do resto do hipertexto (por exemplo, usando palavras sublinhadas).

Internet
Rede de área alargada que é uma confederação de redes de computadores das universidades e de centros de pesquisa, do Governo, do comércio e da indústria, com base no protocolo TCP/IP. Proporciona acesso a sítios *Web*, correio eletrónico, bases de dados, fóruns de discussão, etc.

iOS
Sistema operativo móvel desenvolvido pela *Apple*.

Palavra-passe
Sequência de caracteres ou palavras que um sujeito apresenta a um sistema, como informação de autenticação.

Phishing
Envio aos internautas de mensagens de correio eletrónico, com a aparência de terem origem em organizações financeiras credíveis, mas com ligações para falsos sítios *Web* que replicam os originais, e nos quais são feitos pedidos de atualização de dados privados dos clientes.

Plain text
Termo que representa apenas caracteres de material legível, mas não a sua representação gráfica e nem outros objetos.

Plugins
Programa de computador usado para adicionar funções a outros programas maiores, provendo alguma funcionalidade especial ou muito específica. Geralmente pequeno e leve, é usado somente sob demanda.

Protocolo HTTPS
Versão segura do protocolo HTTP. Foi criada pela Netscape Communications Corporation para fornecer autenticação e comunicação cifrada, e é usada no comércio eletrónico.

QR-Code
Código de barras bidimensional que pode ser facilmente digitalizado usando a maioria dos *smartphones* equipados com câmara. Esse código é convertido em texto (interativo), um endereço URI, um número de telefone, uma localização georreferenciada, um e-mail, um contato ou um SMS.

SHA256

Secure hash algorithm. SHA-256 e SHA-512 são funções *hash* inovadoras computadas com palavras de 32 e 64 *bytes*, respetivamente.

Smartcard

Cartão de circuitos integrados, normalmente com a dimensão de um cartão de crédito, provido de um microprocessador e de memória, capaz de armazenar e atualizar informação sobre o utilizador, permitindo-lhe, por exemplo, efetuar transações de natureza financeira.

Token

Geralmente utilizado como um fator de segurança adicional em transações financeiras realizadas em canais remotos/*Internet*.

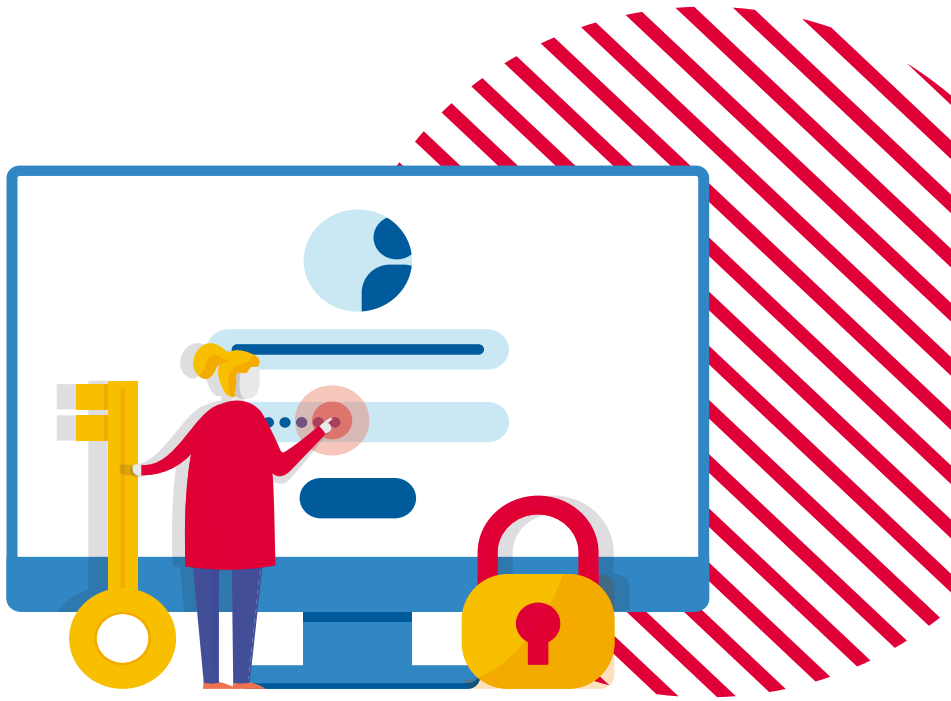
Spam

Lixo eletrónico ou envio de mensagens irrelevantes para um grupo de notícias ou quadro de avisos.

tinyURL

Serviço *web* que transforma links longos em links curtos, que permitem um redireccionamento de páginas.

Introdução



O paradigma de comunicação em Portugal está a mudar o setor da saúde, com o trabalho desenvolvido pelas suas empresas públicas, através da introdução de um modelo de relação próximo, acessível e simples a qualquer cidadão.

A elaboração deste Guia de Boas Práticas pretende apresentar recomendações teóricas para a manutenção e segurança dos mais variados *websites* e *newsletters* de todas as instituições do Serviço Nacional de Saúde e Ministério da Saúde. Além disso, é um guia de orientação para todas as equipas que tenham interesse em melhorar a qualidade dos seus websites, sendo que este se encontra em permanente evolução.

No entanto, para que isso seja realmente efetivado, é necessário que sejam cumpridas diferentes normas e regras.

A segurança de redes e sistemas de informação tem uma importância inegável na atualidade, existindo para isso a Cibersegurança. Este termo diz respeito a um conjunto de meios e tecnologias que visam proteger, de danos e intrusão ilícita, programas, computadores, redes e dados.

Mais do que os utilizadores particulares e as empresas privadas, cabe às instituições governamentais terem um especial cuidado na defesa dos seus meios digitais, assim como de todos os utilizadores desses mesmo meios.

Pela gravidade que os ciberataques e o roubo de dados podem ter junto de empresas e pessoas, este guia de boas práticas deve ser ter e consideração com vista a prevenir qualquer vulnerabilidade.

Arquitetura de segurança das redes e sistemas de informação

Requisitos Técnicos

Atendendo à constante dinâmica e evolução das ameaças às redes e aos sistemas de informação, devem ser mantidas evidências de um elevado padrão de segurança ao longo de todo o ciclo de vida do site, nomeadamente:

- Formação periódica aos utilizadores diretamente envolvidos, visando aspetos de segurança no manuseamento e administração da solução e respetivas componentes;
- Realização, em intervalos regulares, de auditorias de segurança à solução;
- Obtenção dos riscos associados à disponibilização e exploração da solução através da realização, em intervalos regulares, da respetiva análise de risco;
- Existência de contratos de manutenção ativos que garantam o acesso a atualizações que permitam corrigir de forma atempada as potencias falhas de segurança detetadas;
- Definição e execução de uma política de atualização da solução e seus componentes, com eventuais prioridades distintas face à criticidade da correção envolvida.

Independentemente da tecnologia ou linguagem utilizada para criação ou manutenção do *website*, devem ser seguidas regras básicas, nomeadamente:

- Não fazer referência a endereços de correio eletrónico (principalmente se forem endereços pessoais) substituindo pelo recurso a formulários de preenchimento;
- Evitar solicitar o *upload* de ficheiros. Caso seja necessário deve ser restrito e definido o seu formato e dimensão;
- Evitar o recurso a *Plugins*.

1 Regras para Instalação de sítios WEB seguros (HTTPS)

Hoje em dia é fundamental que todos os dados sensíveis, transacionados entre um cliente (ex. *browser*) e um servidor, sejam cifrados de modo a que estes não possam ser entendidos por terceiros. No caso dos sítios WEB, a opção mais acertada são os certificados SSL.

Os certificados TLS/SSL são responsáveis por verificar a autenticidade da comunicação entre duas máquinas, servindo como base para estabelecer uma comunicação criptografada. Para ser identificado como válido, um certificado deve (pelo menos) ser emitido/assinado por uma entidade certificadora fidedigna, ter uma data de validade e estar associado a um nome de domínio. Para além da validade de um certificado, é também importante a sua configuração, já que a força da sua segurança depende de definições como o seu algoritmo de assinatura, chave pública e chave privada.

O SSL é um requisito obrigatório em sítios WEB que implementem funcionalidades de autenticação ou introdução de dados sensíveis. Caso o seu *website* não tenha configurado nenhum certificado SSL, de uma entidade credível, este não oferece nenhuma garantia ao utilizador que é seguro, podendo ser até clonado e usado para esquemas de *phishing*. Além disso, os sítios WEB sem SSL estão vulneráveis a ataques *Man-In-The-Middle,* podendo os atacantes obter os dados pessoais dos utilizadores.

2 Regras para Instalação de sítios WEB seguros (HTTPS)

No âmbito do desenvolvimento das aplicações cliente (Android, IOS, WEB), devem ser seguidas as boas práticas de desenvolvimento seguro, tais como:

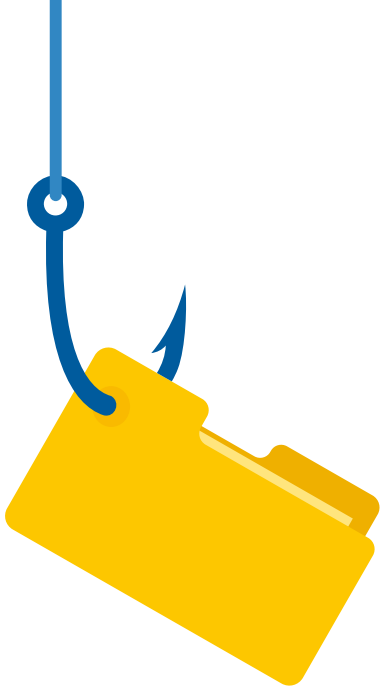
- Seguir as boas práticas de desenvolvimento, como por exemplo as definidas no *Open Web Application Security Project (OWASP)*, no que respeita ao desenvolvimento de código seguro e de submissão desse código a testes de segurança;
- Utilizar sessões seguras com protocolo de Segurança;
- Usar *Transport Layer Security (TLS)*, na sua versão mais recente;
- Não guardar informação pessoal no *browser*, memória ou disco, para além do tempo da sessão, e apenas na medida do necessário;
- Utilizar certificados através de *Application Programming Interface (API)*, não sendo desta forma necessário o uso de palavras-passe;
- Não utilizar credenciais em *plain text*, quer no código quer em ficheiros de configuração;

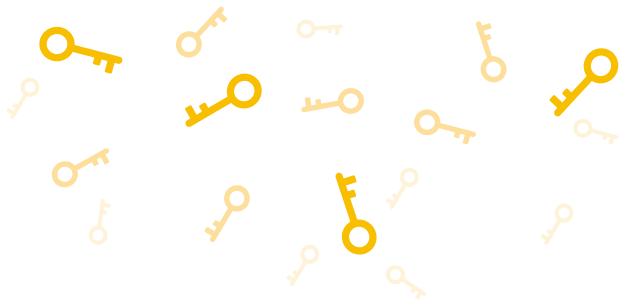
- Evitar palavras-passe embebidas no código;
- Codificar as credenciais que necessitem de ser armazenadas em ficheiros de configuração (HASH - mínimo SHA 256).

3 Regras para controlo de acessos seguros

Deve ser garantida a capacidade para autenticar e autorizar todos os utilizados e dispositivos, incluindo o controlo de acesso a sistemas e aplicações, nomeadamente:

- O processo de autenticação deve ser sempre iniciado e mantido em sessão segura.
- Recomenda-se: 1) o uso de TLS, na sua versão mais recente; ou 2) o uso de palavra-passe, preferencialmente em combinação com outro fator (*Double Factor Authentication* -2FA), como por exemplo:
  - Palavra-passe + SMS *Token*;
  - Palavra-passe + *Smartcard*;
  - Palavra-passe + Biometria;
  - Palavra-passe + padrão gráfico;
  - Palavra-passe + Cartão de coordenadas;
  - Palavra -passe + código aleatório temporário (menos de 5 minutos de validade) enviado na forma de QR-*Code*.





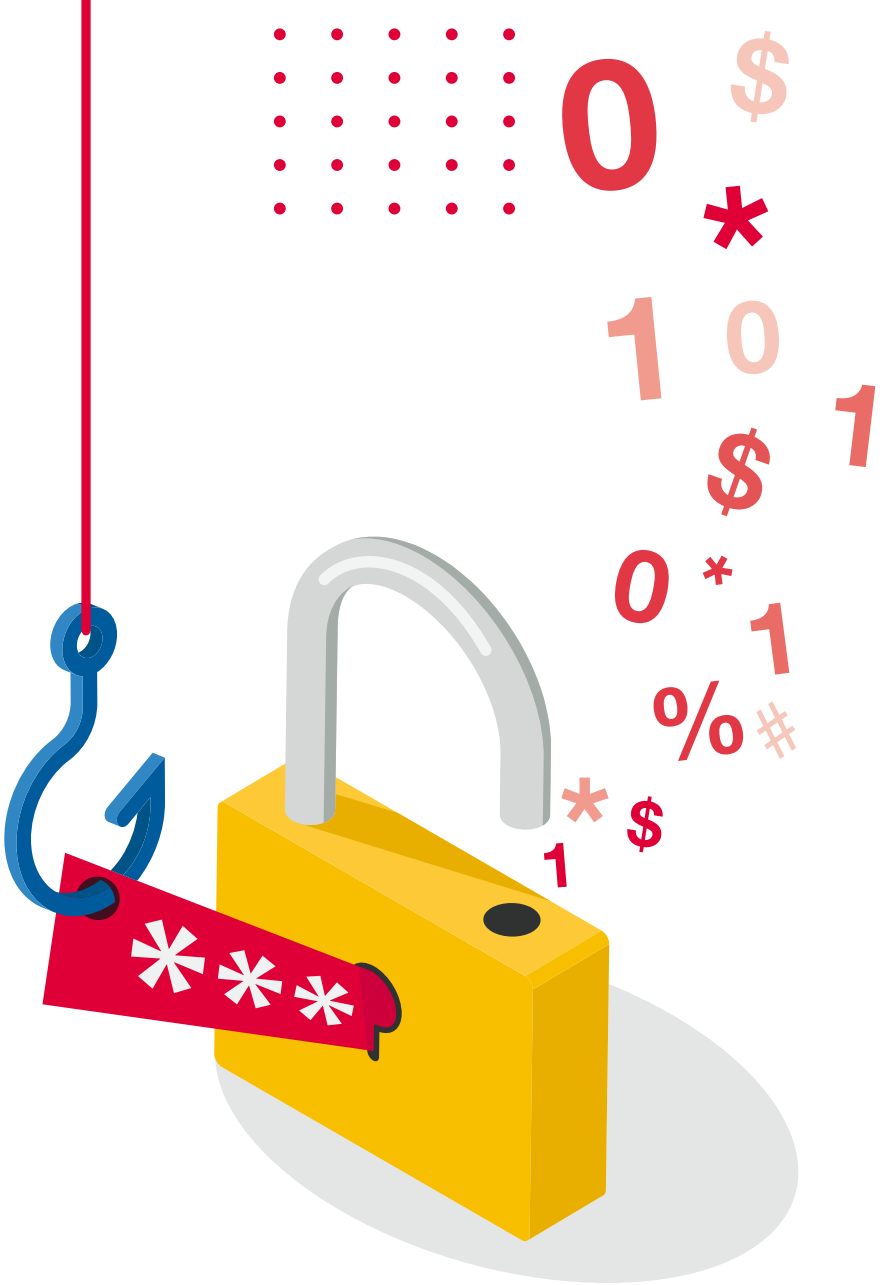
- Dados pessoais de sessão excluídos das variáveis *Uniform Resource Locator* (URL) ou de outras variáveis visíveis ao utilizador.

  Credenciais de início de sessão transmitidos através do seu HASH, mínimo Secure *Hash Algorithm* -256 (SHA -256), ou utilização de cifra ou codificação para a transmissão de dados pessoais (nome do utilizador e palavra-passe em HASH, e restantes dados cifrados).

  Sempre que aplicável, a palavra-passe deve ter no mínimo 9 caracteres (13 caracteres para utilizadores com acesso privilegiado) e ser complexa. 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);
  - caracteres especiais
    (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : " ; ' < > ? , . /);
  - Poderá, em alternativa, ser constituída por frases ou excertos de texto longo conhecidos pelo utilizador, sem caracter de «espaço».

A atribuição das credenciais de acesso deve ser controlada através de um processo formal de gestão do respetivo ciclo de vida, garantindo a sua revisão em intervalos regulares. Os direitos de acesso privilegiados devem ser atribuídos de forma restrita e controlada.



Newsletters

A *newsletter* ou boletim informativo permite uma comunicação mais completa e focada, sendo atualmente vista como uma das mais importantes ferramentas de *marketing*. No entanto, a nossa utilização da *newsletter* tem um caracter informativo, um meio de fazer chegar informações importantes sobre atualizações e serviços aos utentes do SNS/Ministério da Saúde.

O seu objetivo é trazer informações relevantes ao público que se interessa por assuntos relacionados com a instituição. É importante recordar que a *newsletter* não chega a pessoas aleatórias, mas sim a pessoas que optaram por receber esse conteúdo.

1 Regras de utilização de hiperligações em mensagens de correio eletrónico

Devem ser seguidas as seguintes diretrizes de utilização de hiperligações em mensagens de correio eletrónico para permitir ao destinatário avaliar adequadamente a segurança dos mesmos:

- Deve ser garantido que os domínios utilizados estão claramente visíveis e identificados.
- Deve ser evitado o uso de hiperligações reduzidas (TinyURL).
- Deve ser evitado qualquer tipo de camuflagem do domínio (do tipo “Clica aqui”).

2 Regras para envio de mensagens de correio eletrónico em massa

Devem ser seguidas as seguintes diretrizes de envio de mensagens de correio eletrónico em massa para impedir que as mensagens sejam bloqueadas por filtros de *spam*:

- Deve ser fornecida identificação suficiente para evitar o bloqueio, incluindo endereço com o domínio da entidade no campo "FROM" (ex.: nome@spms.min-saude.pt). Pode ser incluída a morada física e número de telefone, claramente identificados.

- Autenticar mensagens de fornecedores externos de comunicação de *marketing*. Ou seja, se enviar estas mensagens em massa através de um fornecedor de *marketing* externo (por exemplo, *MailChimp*) usando um endereço da sua instituição, use DKIM para garantir a autenticação e legitimidade da sua mensagem.

- Evitar o uso de conteúdo com *spam*, tais como:
  - TUDO EM MAISCULAS;
  - Palavras "*spammy*" (por exemplo, "dinheiro grátis") na linha de assunto;
  - Pontuação excessiva;
  - Mensagens que contenham anexos de documentos – É preferível usar uma hiperligação a uma página com conteúdo adicional;
  - Se for mesmo necessário um anexo, use um ficheiro no formato PDF em vez de um documento do Word, PowerPoint ou outros tipos de arquivos;
  - Mensagens com hiperligações para uma página da *web* que requer autenticação são frequentemente sinalizadas como possíveis tentativas de *phishing*.

3 Possibilitar a autenticação do remetente

A entidade recetora das mensagens de correio eletrónico deve ter a possibilidade de validar a identidade do remetente. Tal torna-se possível se o remetente da mensagem implementar as seguintes tecnologias:

- *Sender Policy Framework* (SPF)
- *DomainKeys Identified Mail* (DKIM)

O objetivo da autenticação do domínio de envio é proteger contra remetentes (tanto aleatórios quanto agentes maliciosos) de falsificar o domínio de outra entidade e iniciar mensagens com conteúdo falso, e contra os agentes maliciosos de modificar o conteúdo das mensagens em trânsito.

Sender Policy Framework (SPF) é a maneira padronizada para um domínio de envio identificar remetentes de correio autorizados para um determinado domínio.

Domain Keys Identified Mail (DKIM) é o mecanismo para confirmar os servidores de envio e eliminar a vulnerabilidade do *man-in-the-middle* modificar o conteúdo, usando para esse efeito assinaturas digitais geradas a partir do servidor de envio de mensagens de correio eletrónico.

4 Orientações para o destinatário

A segurança das mensagens de correio eletrónico deve ser invisível para o utilizador final, tanto quanto possível. Os utilizadores devem ter a opção de reportar qualquer indício de intenção maliciosa, se necessário, mas não precisam tomar decisões técnicas complexas.

Não deve ser dificultada a segurança dos utilizadores, pois eles podem encontrar soluções menos seguras.

- Forneça orientação para que os utilizadores:
  - Possam continuar a trabalhar com o mínimo de interrupção;
  - Entendam e possam agir em caso de mensagens de erro ou de retorno;
  - Saibam quem contatar se algo correr mal.
- Devem ser incluídas na própria mensagem algumas notas de sensibilização de segurança para o destinatário, tais como:
  - Verifique sempre o remetente das mensagens eletrónicas que recebe;
  - Não abra anexos das mensagens sem garantir a autenticidade do remetente;
  - Não clique em hiperligações incluídas no conteúdo de mensagem que rececionou, sem identificar claramente o endereço associado ao link (URL).

Política de *Cookies*

Pela sua importância para uma melhor experiência na utilização do nosso *website*, são indispensáveis, mas por terem um funcionamento intrusivo, que instala e absorve informação, devem ser autorizados pelo utilizador.

A política de *cookies* existe para mediar e assegurar a confiança que o utilizador deposita na SPMS enquanto navega no *website*.

1 O que são *cookies*?

Cookies são pequenos arquivos de texto armazenados no seu navegador quando visita um *website*. A maioria dos sítios WEB utiliza-os para melhorar a experiência do respetivo utilizador e o seu desempenho.

2 Como a SPMS usa *cookies*?

A SPMS usa *cookies* para registar detalhes sobre cada uma das suas sessões atuais, preferências de idioma, e para recolher estatísticas de forma a otimizar o funcionamento do *website* e fornecer conteúdo adaptado aos seus interesses. Alguns recursos do *website* podem não funcionar corretamente se não ativar o uso de *cookies*.

3 Que tipos de *cookies* a SPMS usa?

- *Cookies* funcionais (estritamente necessários);
  Usados para armazenar cada configuração de sessão, nomeadamente as suas preferências de idioma.

- *Cookies* analíticos
  Usados para medir o desempenho da velocidade do *website* e para recolher informações relacionadas com quais páginas do *website* têm mais ou menos visualizações, de forma a ajudar a melhorar o conteúdo para todos os utilizadores em geral.

- *Cookies* de segmentação
  São cookies que registam a visita do utilizador ao nosso website, as páginas visitadas e as ligações seguidas.

Em particular, os sítios WEB da SPMS utilizam o *Google Analytics*, que utiliza *cookies* de forma a permitir a SPMS analisar como utiliza os sítios WEB da SPMS.

A informação gerada pelos cookies sobre a utilização dos sítios WEB (incluindo o endereço IP) poderá ser transmitida à Google e armazenada por esta, sendo que a Google irá usar a informação em causa para avaliar a utilização dos sítios WEB pelo utilizador, criar relatórios sobre o tráfego de cada página dos sítios WEB para os operadores dos sítios WEB e para prestar outros serviços relacionados com o tráfego dos sítios WEB e utilização da *Internet*. A Google também poderá transmitir esta informação a terceiros em cumprimento de uma obrigação legal que lhe seja aplicável, ou no caso em que esses terceiros tratam a informação por conta do Google. A Google não irá associar o seu endereço de IP com quaisquer outros dados na posse da Google. Pode desativar estes *cookies* selecionando as preferências apropriadas no seu navegador *(browser)*.

4 Como pode gerir os seus *cookies*?

Pode gerir os seus *cookies* através das suas preferências de *cookies* ou através das funcionalidades do seu navegador. No entanto, a desativação de cookies pode impedir que alguns serviços funcionem corretamente, afetando, parcial ou totalmente, a navegação nos sítios WEB da SPMS.

Pode optar por não ativar cada uma das categorias de *cookies* (exceto os estritamente necessários) acedendo às suas preferências de *cookies* do seu navegador *(browser)*:

- Firefox: Gerir Cookies no Firefox
- Chrome: Gerir Cookies no Google Chrome
- Internet explorer: Gerir Cookies no Internet Explorer
- Tudo sobre Cookies: www.aboutcookies.org

Política de Privacidade

Exemplo de política de privacidade

https://www.sns24.gov.pt/politicas-de-privacidade/

Legislação

Resolução do Conselho de Ministros n.º 41/2018

Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD)

"Lei dos *cookies*" - Lei 46/2012

DIRETIVA (UE) 2016/1148 DO PARLAMENTO EUROPEU E DO CONSELHO de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (NIS)

Referências

- Associação para a Promoção e Desenvolvimento da Sociedade de Informação.
- Centro Nacional de Cibersegurança Portugal (CNCS)

Guia de Boas Práticas e Regras para sítios WEB SNS/MS

CIBERSEGURANÇA

REPÚBLICA PORTUGUESA
SAÚDE

40 ANOS SNS SERVIÇO NACIONAL DE SAÚDE 1979-2019

SPMS EPE
Serviços Partilhados do Ministério da Saúde

Cibersegurança SNS