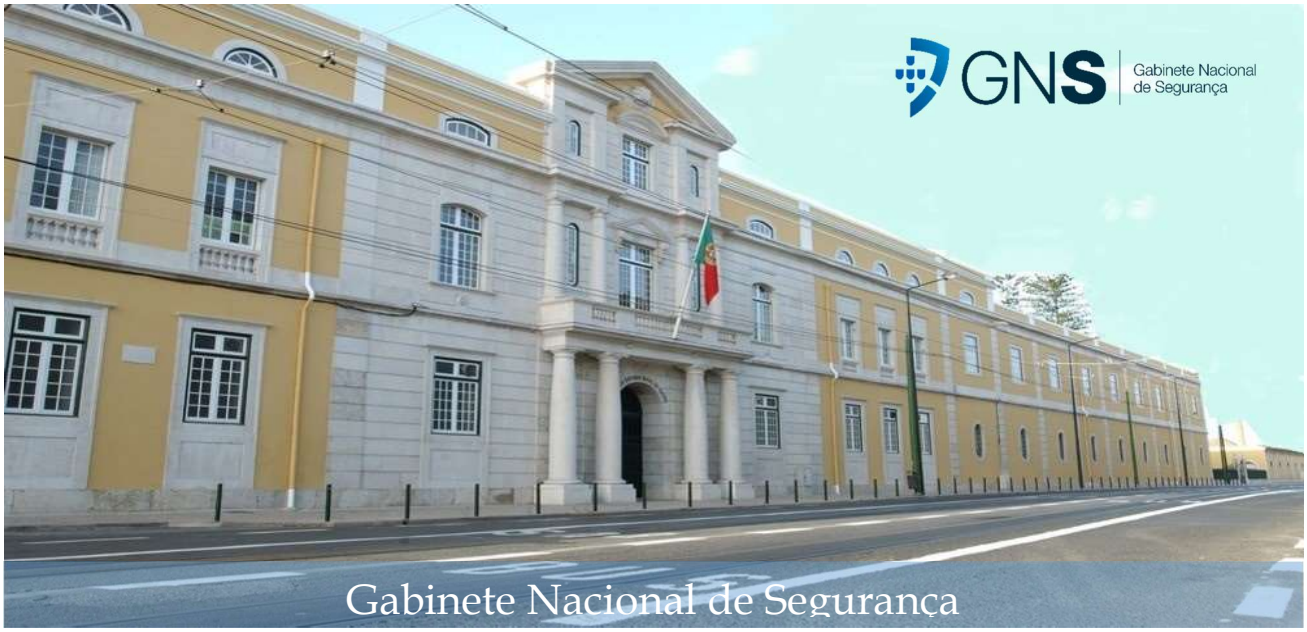
PRESIDÊNCIA DO CONSELHO DE MINISTROS

Gabinete Nacional de Segurança



RGPD e a Segurança das Redes e Sistemas de Informação

Manual de Boas Práticas

Parte II

Contributos para políticas e procedimentos

V1.0 16ABR18

Nota da Direção

No próximo dia 25 de maio entrará em vigor o novo Regulamento Geral de Proteção de Dados (RGPD), aplicável a todas as organizações, recaindo sobre estas a responsabilidade de o interpretar e fazer cumprir. Trata-se de um normativo que se baseia na autorregulação, cabendo por isso aos destinatários garantir a todo o tempo que se encontram em conformidade com as respetivas regras, sob pena de penalizações que todos pretendem evitar.

Para auxiliar quem, como nós, se encontra perante este desafio, o Gabinete Nacional de Segurança reuniu um conjunto de conceitos, informações e metodologias, com base nas melhores práticas adotadas na União Europeia e NATO relativas à segurança da informação, as quais, numa lógica transversal, foram vertidas num "Manual de Boas Práticas". Uma vez que a segurança dos dados pessoais inclui, mas não se limita, à implementação de medidas tecnológicas, este Manual deve ser entendido como um complemento aos requisitos técnicos mínimos que visam garantir uma arquitetura de segurança das redes e sistemas de informação que constam da Resolução de Conselho de Ministros nº. 41/2018.

Para maior facilidade de consulta, este Manual divide-se em três partes:

Parte I – Deveres e responsabilidades das organizações

Parte II – Contributos para políticas e procedimentos

Parte III – Segurança física

De realçar, no entanto, que este conjunto de documentos não deve ser considerado um normativo de aplicação obrigatória, nem mesmo um guia com carácter doutrinário, mas sim um algo que visa apenas partilhar as boas práticas que se julga adequado cada um utilizar, de acordo com a avaliação de risco que fizer da sua própria realidade e do estado de maturidade da sua organização no que respeita à salvaguarda da informação sensível, na qual se podem incluir os dados pessoais.

.

O Diretor-geral

António José Gameiro Marques

Assinado de forma digital por António José Gameiro Marques
Dados: 2018.04.18 18:29:27 +01'00'

António Gameiro Marques

CAlm

Índice

1. Políticas e procedimentos operacionais

A operação segura e correta das redes e sistemas de informação obriga à definição de políticas e procedimentos operacionais:

- As políticas de segurança devem ser escritas de forma clara, para que sejam facilmente compreendidas por todos os utilizadores do sistema;
- Todos os utilizadores devem estar familiarizados com as políticas de segurança;
- As políticas de segurança devem estar disponíveis e acessíveis a todos os utilizadores para rápida consulta;
- As políticas de segurança devem ser revistas periodicamente ou sempre que se justifique;
- Devem ser atribuídas responsabilidades coletivas e individuais, dentro da organização, no que concerne à segurança dos dados;
- Cada utilizador deve ser individualmente responsável por respeitar as políticas e medidas de segurança implementadas;
- Todas as atividades realizadas no sistema devem estar sujeitas a monitorização e auditorias;
- Deve estar instituída uma política de segregação de funções, de modo a reduzir a probabilidade de erro humano no tratamento de dados pessoais;
- Deve ser definida uma política rigorosa, indicando o grau de tolerância ou até mesmo a proibição absoluta, quanto:
  - À utilização de dispositivos móveis;
  - Aos acessos aos dados pessoais sob o controlo da organização a partir de dipositivos pessoais (*Bring Your Own Device* -BYOD);
  - À utilização de dispositivos da organização fora das instalações da mesma, incluindo para fins pessoais;
  - À utilização do correio eletrónico da organização;
- Ninguém deve ignorar os recursos de segurança do sistema, modificar qualquer programa ou aceder às áreas para as quais não tenham sido especificamente autorizados, ou tentar qualquer uma destas ações;
- O uso e o acesso não autorizados a equipamentos informáticos, programas e dados, e/ou a sua modificação, deve constituir uma infração de segurança que pode resultar em responsabilidade legal;
- A organização deve definir procedimentos internos, e quando aplicável ao nível da subcontratação, que visem lidar com os casos de violação de segurança dos dados pessoais;
- Os procedimentos internos acima referidos devem contemplar, no mínimo, medidas para deteção, identificação, investigação das circunstâncias, medidas mitigadoras, circuito da

informação entre responsáveis e subcontratante, responsabilidades e, ainda, a notificação às autoridades competentes dentro dos prazos legais (72 horas), bem como a notificação aos titulares dos dados nos casos em que possa resultar num elevado risco para os próprios;

- Deve, ainda, ser definida uma política de gestão de risco para corroborar as decisões sobre as medidas mais ajustadas para eliminar ou, no mínimo, reduzir eventuais riscos.

2. Proteção dos dados e dos recursos de tratamento

Para proteger os dados e os recursos de tratamento contra código malicioso (*malware*), devem ser implementados controlos de deteção e prevenção:

- Deve ser instalado *software* antivírus e *software anti-spam* em todas as estações de trabalho e servidores que compõem a rede e sistema de informação;
- O *software* antivírus e o software *anti-spam* devem ser sempre devidamente licenciados e mantidos atualizados;
- A atualização do antivírus e do *anti-spam* deve ser, preferencialmente, automática;
- Deve-se verificar regularmente a presença de código malicioso em:
  - Dados, sistema operativo instalado, pacotes de *software* e aplicações;
  - Dispositivos de armazenamento removíveis;
  - *E-mails* e anexos recebidos de fontes externas e internas;
- Devem ser instaladas equipamentos de proteção perimétrica (B*oundary Protection Devices*- BPD) quando existam ligações a outras redes;
- Recomendando-se igualmente a utilização de BPD quando se tratem de ligações entre sistemas com dados pessoais considerados muito críticos;
- As portas USB das estações de trabalho que não sejam necessárias devem ser bloqueadas;
- As portas USB que sejam necessárias devem ter políticas implementadas para impedir o acesso e abertura de ficheiros que possam executar programas potencialmente nocivos.

Deve-se sensibilizar os utilizadores para importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança, sempre que for detetado código malicioso.

Os utilizadores também devem ter cuidados para evitar a introdução de código malicioso, pelo que devem adotar as seguintes ações preventivas:

- Comunicar de imediato qualquer alerta apresentado pelo sistema antivírus;
- Evitar utilizar dispositivos de armazenamento removíveis;
- Se observar um comportamento suspeito do sistema, o utilizador deve parar imediatamente qualquer processamento em curso, desconectar o sistema potencialmente infetado da rede e notificar o responsável pela segurança.

3. Gestão do Ciclo de Vida dos utilizadores

Devem existir politicas e procedimentos para atribuição de privilégios de acesso e utilização do sistema, de modo a garantir que o acesso aos recursos de tratamento dos dados pessoais é efetuado apenas por utilizadores devidamente autorizados.

3.1 Criação de contas de utilizador

Devem ser estabelecidos procedimentos para a criação de contas de utilizador do sistema (procedimento de registo):

- O acesso ao sistema só pode ser concedido a quem tiver concluído, com sucesso, o procedimento de registo;
- Os pedidos de criação ou modificação de uma conta de utilizador, quando não exista um sistema de gestão de identidades e acesso (*Identity and Access Management* - IAM) devem ser efetuados através de formulários próprios, devidamente preenchidos e assinados;
- Devem existir igualmente regras específicas para contas de utilizadores genéricos (por exemplo, *webservices)*;
- Quando a aprovação é concedida, deve ser gerada automaticamente uma nova conta individual para o utilizador e uma palavra-passe inicial (a qual deve também obedecer às regras definidas para as palavra-passe) que lhe irão permitir aceder às funções do sistema para as quais foi autorizado;
- Não devem ser permitidas contas compartilhadas.

Deve ser criada e mantida atualizada uma lista de todas as pessoas autorizadas a usar o sistema e a extensão da respetiva autorização, isto é, a indicação dos respetivos privilégios de acesso.

Deverá ser disponibilizada ao encarregado da proteção dos dados a lista atualizada de utilizadores, para fins de controlo interno e verificação de conformidade (*self-auditing* e *self-monitoring*).

3.2 Definição de perfis de utilizador

O acesso às funções do sistema deve ser refletido em privilégios de acesso (perfis) diferenciados, em razão da necessidade de conhecer e da segregação de funções, respeitando sempre o princípio do menor privilégio (isto é, cada utilizador deve possuir somente os privilégios necessários para realizar a sua função na organização).

Os perfis devem ser devidamente especificados e explicados ao utilizador.

3.3 Credenciais de autenticação (palavra-passe)

As credenciais de autenticação de cada utilizador devem ser únicas e intransmissíveis.

No caso de autenticação ser efetuada por *userID*/palavra-passe:

- No primeiro acesso ao sistema, deverá ser solicitado ao utilizador a alteração da palavra-passe inicial, cabendo-lhe a escolha da sua própria palavra-passe a qual deve ser única, fácil de lembrar (mas difícil de adivinhar), não repetida e apenas conhecida e memorizada pelo próprio;
- A palavra-passe deve ter no mínimo 9 caracteres e ser complexa, significando que 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 (~! @ # $ % ^ & * () _ + | `- = \ {} []:"; '<>?,. /);
- Em alternativa, a palavra-passe poderá ser constituída por frases ou excertos de texto longo, sem caracter de "espaço";
- A palavra-passe deve ser alterada, no máximo, a cada 180 dias para perfis de utilizador e 90 dias para perfis de administradores de sistemas e bases de dados, ou quando for comprometida ou se suspeite que venha a ser comprometida;
- O sistema deve ser configurado para alertar os utilizadores de que devem alterar as respetivas palavras-passe, com uma antecedência adequada (máxima de 30 dias);
- A reutilização de palavras-passe anteriores deverá ser evitada, recomendando-se que não seja igual às últimas 4 palavras-passe.

3.4 Bloqueio de contas dos utilizadores

As contas dos utilizadores deverão ser automaticamente bloqueadas após 3 tentativas de autenticação mal sucedidas e bloqueadas manualmente se se suspeitar que a conta está a ser usada incorretamente.

O encarregado da proteção de dados deve ser alertado para as situações de bloqueio acima referidas através, por exemplo, de relatórios periódicos, de modo a poder detetar eventuais problemas ou desvios em relação à doutrina estabelecida.

As contas que deixam de ser necessárias devem ser bloqueadas, tornadas inativas ou eliminadas.

Devem ser definidas regras específicas para os casos de ausência prolongada de utilizadores (por exemplo, licenças, férias, baixas prolongadas, mudança de funções, entre outros), bem como procedimentos de reporte e de atualização destas situações.

3.5 Estações de trabalho

O bloqueio automático do ecrã da estação de trabalho deve ser ativado, preferencialmente, após 5 minutos de inatividade, podendo ser desbloqueado apenas com credenciais de acesso.

No final de cada ciclo de trabalho do utilizador, a respetiva sessão deve ser encerrada.

Deve ser previsto o encerramento automático da sessão de trabalho do utilizador em caso de inatividade por tempo superior a 3 horas, bem como o encerramento automático da estação de trabalho em caso de inatividade superior a 5 horas (excecionam-se necessidades de sessões ativas para efeitos de manutenção e administração de sistemas).

4. Registos de atividade

4.1 Registo e monitorização de atividade

Devem-se criar, atualizar e analisar periodicamente os registos de atividade (*logs*):

- Os registos devem conter detalhes suficientes sobre as atividades dos utilizadores do sistema que permitam a reconstrução do histórico de eventos (quem, onde, quando e ação efetuada sobre o dado pessoal);
- Os registos devem abranger qualquer atividade de criação, leitura, alteração, pesquisa, consulta, transmissão de dados a terceiros ou eliminação de dados pessoais, incluindo o registo temporal da ação e o respetivo resultado;
- Os registos de atividade devem ser guardados por um período mínimo de 12 meses.

4.2 Proteção dos registos de atividade

Devem-se estabelecer diretrizes para a proteção dos registos de atividade contra acessos não autorizados e modificações não autorizadas:

- Devem-se definir políticas que visem a criação, manutenção, integridade, disponibilidade e segurança dos registos de atividade dos utilizadores;
- A gravação, os *backups* e a manutenção dos registos de atividade devem ser obrigatórios e incluir todos os tipos de eventos (eventos bem-sucedidos e falhados);
- Os acessos aos registos de atividade dos utilizadores devem ser limitados a pessoas devidamente autorizadas e para os fins legalmente previstos, nomeadamente auditorias.

5. Controlo dos sistemas em produção

Nos sistemas em produção as atualizações de *software* devem ser controladas:

- As configurações dos sistemas em produção devem estar em conformidade com as regras de segurança para poderem ser aprovados;
- Devem ser implementados de forma expedita as atualizações de segurança disponibilizadas pelo fabricante, de modo a mitigar as vulnerabilidades do sistema em produção;
- As alterações ao sistema em produção devem ser comunicadas ao encarregado da proteção de dados por meio de, por exemplo, relatórios periódicos.

6. Instalação de novo *hardware* e *software*

Devem ser impostas restrições quanto à instalação de novo *hardware* e *software*, através da definição e implementação de regras e critérios:

- A configuração local de *hardware* e *software* do sistema não deve ser alterada sem autorização prévia;
- Devem ser definidos procedimentos internos para serem seguidos sempre que se requeiram alterações à configuração do sistema e que permitam o controlo dessas alterações;
- Apenas devem ser instalados componentes de *hardware* e *software* autorizados;
- Somente os componentes de *hardware* e os dispositivos periféricos autorizados podem ser ligados ao sistema;
- Alterações à configuração local de *hardware* e *software* do sistema devem ser comunicadas ao encarregado da proteção de dados.

7. Cópias de segurança

Devem ser efetuadas cópias de segurança (*backups*) periódicas dos dados e do *software* para proteger contra perdas e danos, bem como para garantir, quando necessário, uma rápida e correta recuperação do sistema:

- Deve ser definida uma política de salvaguarda da informação e do sistema que garanta a sua confidencialidade, integridade e disponibilidade e, ainda, a correta reposição dessa salvaguarda no sistema;
- Essa política deve, no mínimo, referir a periodicidade dos *backups*, a sua localização (a qual deverá ser diferente daquela onde se encontra o sistema em produtivo), o tipo (incremental, completo ou diferencial), o tempo de conservação, o acesso e a forma como devem ser armazenados.

8. Cifragem

Nas situações em que é necessário recorrer aos mecanismos de cifragem, como por exemplo, na transmissão de dados pessoais sensíveis:

- Devem ser tomadas todas as medidas necessárias para evitar que o material de cifra se torne acessível a pessoas não autorizadas;
- Devem ser definidos e implementados procedimentos de controlo para a segurança do sistema de cifra:
  - Deve ser dada por escrito uma autorização específica ao pessoal autorizado a aceder ao material de cifra;
  - Os procedimentos básicos para o uso de equipamentos de cifra devem estar detalhados nos respetivos manuais de operação;
  - O pessoal com acesso ao equipamento de cifra deve estar familiarizado com os respetivos procedimentos de tratamento e manuseamento;
  - Além disso, o pessoal deve ser proficiente na operação de equipamentos de cifra sob sua responsabilidade;
- Os utilizadores fornecidos com equipamentos de cifra devem seguir as instruções de segurança emitidas especificamente para esse dispositivo;
- Deve existir um suporte mínimo à gestão do ciclo de vida de chaves de cifra preparado para as criar, revogar e substituir.

9. Computação em nuvem (*Cloud*)

Caso se opte por recorrer aos serviços de computação em nuvem, para além de determinarem os requisitos técnicos (por exemplo, ser flexível e escalável), as organizações devem também preocupar-se com os requisitos de segurança:

- No caso das redes e sistemas de informação que utilizem os serviços de computação em nuvem públicos ou híbridos, devem ser avaliados o regime de responsabilidade e os níveis de serviço – *Service Level Agreement* (SLA) – particularmente no que respeita: a) à disponibilidade do sistema; b) à segurança dos dados; e c) à reposição de serviço;
- As políticas de segurança definidas devem ter em conta que a segurança na computação em nuvem também compreende a segurança da infraestrutura de rede, a segurança das aplicações em nuvem, a segurança das instalações físicas onde se encontram os dados e a possibilidade de realização de auditorias (periódicas e esporádicas) ao provedor de serviço;
- Os centros de dados devem ficar alojados em instalações com as condições de segurança adequadas à proteção dos dados pessoais e serviços contratados;
- Sempre que possível, devem ser escolhidos prestadores de serviço acreditados em referenciais internacionais de segurança e que demonstrem a conformidade com o RGPD;
- Deve-se, também, constituir requisito obrigatório o prestador de serviço possuir servidores físicos dentro do território nacional e/ou da União Europeia;
- Nos casos aplicáveis, deve-se optar por nuvens privadas da administração pública ou controladas por entidades públicas, em detrimento das nuvens públicas;
- O responsável pelo tratamento deve favorecer a aplicação de tecnologias *Privacy Enhancing Technologies* (PET);
- Deve-se reforçar a segurança dos dados mais sensíveis através de controlos de acesso mais rígidos, do uso de técnicas de cifragem e optando por um sistema de gestão de identidades e acessos (*Identity and Access Management*);
- As medidas tecnológicas adotadas devem assegurar que dados específicos não são enviados (e recebidos) para a (e da) nuvem se não estiverem cifrados.

Para garantir a segurança dos dados na computação em nuvem, devem ser adotadas medidas adicionais que visem:

- Impedir o acesso de pessoas não autorizadas às instalações utilizadas para o tratamento desses dados;
- Impedir que os suportes de dados possam ser lidos, copiados, alterados ou retirados por pessoas não autorizadas;
- Impedir a introdução não autorizada, a consulta, a alteração ou a eliminação não autorizada dos dados pessoais;

- Impedir que os sistemas de tratamentos automatizados de dados possam ser utilizados por pessoas não autorizadas;
- Garantir que as pessoas autorizadas só possam ter acesso aos dados abrangidos pela autorização;
- Garantir a verificação das entidades a quem possam ser transmitidos os dados pessoais através das infraestruturas de transmissão de dados;
- Garantir que a qualquer momento é possível saber a atividade efetuada sobre os dados pessoais, incluindo o quando e por quem;
- Impedir que na transmissão de dados pessoais, bem como no transporte do seu suporte, os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada;
- Assegurar que somente o pessoal autorizado possa ter acesso aos dados pessoais e apenas para fins legalmente autorizados;
- Assegurar a proteção dos dados pessoais transmitidos, armazenados ou de outro modo tratados contra a destruição, perda, alteração, divulgação ou acessos não autorizados.

10. Suportes de dados

10.1 Proteção dos suportes de dados

Os suportes de dados devem ser protegidos contra acessos não autorizados, utilização indevida ou violação da respetiva integridade:

- A organização deve disponibilizar os seus próprios suportes de dados eletrónicos;
- Devem ser autorizados apenas os suportes de dados da organização, devendo ser proibida a utilização de suportes de dados pessoais;
- A utilização dos suportes de dados removíveis deve ser gerida em todas as suas fases, incluindo a aquisição, distribuição, utilização e destruição;
- Devem ser definidos procedimentos de destruição de emergência para serem executados em circunstâncias excecionais;
- Antes da eliminação ou reutilização de equipamentos que contenham suportes de dados, deve-se verificar se todos os dados foram efetivamente removidos ou eliminados;
- No caso dos suportes de dados em papel, a impressão e/ou cópias de documentos contendo dados pessoais devem ser limitadas ao estritamente necessário;
- A reprodução dos documentos deve ser efetuada com recurso a um sistema de impressão segura (por exemplo, máquinas fotocopiadoras com autenticação do utilizador);
- Todos os utilizadores devem garantir que nenhuma impressão e/ou cópia fica esquecida na impressora/fotocopiadora.

10.2 Eliminação dos suportes de dados

Os suportes de dados devem ser eliminados de forma segura, quando deixarem de ser necessários, através da utilização de procedimentos formais:

- Devem ser definidos procedimentos formais para destruição dos suportes de dados, de forma a garantir que os dados são completamente eliminados;
- Devem ser eliminados todos os dados armazenados nos equipamentos em fim de vida;
- Os equipamentos em fim de vida devem ser desmagnetizados e/ou fisicamente destruídos;
- Os documentos em papel devem ser destruídos com recurso a máquinas trituradoras próprias;
- No caso de dados pessoais críticos, a destruição dos suportes de dados (eletrónicos e em papel) deve ser testemunhada presencialmente pelo encarregado da proteção de dados;

- Aquando da destruição de suportes de dados contendo dados pessoais críticos, devem ser elaborados certificados de destruição, recomendando-se a sua conservação por um período mínimo de 5 anos.

11. Instalação e proteção dos equipamentos

Os equipamentos devem ser instalados e protegidos de modo a reduzir os riscos de ameaças, os perigos ambientais e as oportunidades para acesso não autorizado.

11.1 Interrupções no fornecimento de energia elétrica

Os equipamentos devem ser protegidos contra eventuais interrupções no fornecimento de energia elétrica:

- Assegurar o fornecimento de energia elétrica adequada a todos os componentes críticos do sistema;
- Deve ser dimensionada e implementada a redundância energética para fornecer energia elétrica aos componentes críticos, com base nos respetivos requisitos de disponibilidade.

11.2 Cablagem elétrica e de telecomunicações

A cablagem elétrica e de telecomunicações, que transporta dados ou que suporta os serviços de informação, deve ser protegida contra interceção, interferência ou dano:

- Para manter a integridade dos serviços, eventuais alterações à cablagem elétrica e de telecomunicações devem ser efetuadas apenas por pessoal autorizado;
- Quaisquer alterações à arquitetura da cablagem e dos equipamentos devem ser previamente autorizadas;
- As comunicações entre componentes externos e o sistema devem ser cifradas e autenticadas ou, no caso de uma aplicação não suportar comunicações cifradas nativamente, deve ser criado um túnel (*Virtual Private Network* -VPN).

12. Manutenção

Deverão existir cuidados acrescidos na manutenção dos equipamentos e/ou sistema, particularmente nos casos em que manutenção é assegurada por terceiros:

- O processo de escolha da empresa subcontratada para o efeito deve incluir critérios de idoneidade;
- Salvo situações urgentes, as ações de manutenção devem ser programadas;
- As ações de manutenção devem ser realizadas preferencialmente nas instalações do responsável pelo tratamento e previamente autorizadas;
- As ações de manutenção que representem alta criticidade não deverão ser efetuadas por uma só pessoa;
- Deve ser exigido um registo escrito e detalhado de todas as ações de manutenção efetuadas;
- Devem ser eliminados todos os dados armazenados nos equipamentos antes de estes serem enviados para a manutenção;
- Quando existam, os discos rígidos dos equipamentos periféricos devem ser previamente removidos;
- O contrato de manutenção deve prever a penalização da empresa subcontratada nos casos de apropriação indevida, perda ou alteração dos dados.

13. Subcontratação de serviços

Cuidados a ter nos casos de subcontratação de serviços:

- Nos casos em que é necessário subcontratar serviços deve ser celebrado um contrato entre a entidade responsável pelo tratamento e a entidade subcontratada onde constem cláusulas contratuais com orientações explícitas quanto à segurança dos dados pessoais, designadamente:
  - Descrição exaustiva das responsabilidades e funções a desempenhar por cada uma das partes;
  - Não permitir o acesso remoto aos sistemas, salvo casos excecionalmente urgentes e nunca sem uma autorização prévia devidamente documentada;
  - As intervenções nas redes e sistemas de informação devem ser realizadas,preferencialmente, nas instalações do responsável por razões de segurança e controlo;
  - As intervenções devem ser programadas a previamente autorizadas pela entidade responsável pelo tratamento;
  - Deve existir um registo escrito com a descrição detalhada de todas as intervenções;
  - Credenciação de segurança do pessoal sob o controlo das entidades subcontratadas, quando aplicável;
  - Segregação dos ambientes de desenvolvimento e de produção através da atribuição de diferentes privilégios de acessos;
  - Planeamento e condução de auditorias às entidades subcontratadas;
- A entidade subcontratada deve ser devidamente informada sobre as suas responsabilidades na proteção dos dados pessoais, devendo indicar formalmente, aquando da assinatura do contrato, que compreende e aceita as suas responsabilidades neste o domínio.

14. Planos de emergência e de continuidade de negócio

Deve ser elaborado um plano de emergência e de continuidade de negócio, que inclua o plano de contingência, *backups* e os procedimentos de recuperação em caso de desastre (plano de recuperação de desastre), bem como a atribuição de responsabilidades:

- Estes planos destinam-se a todas as instalações disponíveis e incluem a manutenção de *backups* de dados, programas essenciais do sistema e a identificação de meios alternativos para manter a continuidade do negócio;
- As redundâncias existentes, bem como os meios utilizados na recuperação, devem possibilitar o mesmo nível de segurança dos dados que os sistemas produtivos;
- Nestes planos devem estar devidamente explicitados os procedimentos a seguir;
- Os procedimentos de evacuação em caso de sinistro devem acautelar a salvaguarda dos dados pessoais, incluindo os contidos nos equipamentos portáteis;
- No caso de uma evacuação de emergência, os equipamentos informáticos devem ser protegidos por bloqueio ou mesmo desligados, desde que tal ação não coloque ninguém em perigo;
- Os procedimentos de emergência devem ser do conhecimento de todos os colaboradores e testados, no mínimo, uma vez por ano;
- A ativação do plano de recuperação desastre deve ser entendida como uma medida interna provisória até o sistema recuperar a capacidade total, devendo ser respeitados os procedimentos nele estabelecidos.