O guia essencial para conformidade com o RGPD

Elaborado pela

Índice

Introdução

Está na hora de adotar a privacidade desde a conceção

Em 25 de maio de 2018, entra em vigor o Regulamento Geral sobre a Proteção de Dados da UE (RGPD). O RGPD irá substituir todos os regulamentos nacionais relativos à proteção de dados, e todos os que têm negócios no mercado único terão de cumprir este regulamento. Isto abrange empresas que não estão estabelecidas na UE que lidem com clientes da UE.

Nos termos do RGPD, qualquer violação dos dados pessoais deve ser comunicada no período de 72 horas. O não cumprimento desta medida – ou em caso de negligência – poderá resultar em multas que ascendem a 20 milhões de euros ou a 4% da faturação global, o valor que for mais elevado. Felizmente, as medidas necessárias para proteger os dados da empresa como um todo servirão também para manter os dados do cliente mais seguros. A mesma abordagem de segurança de várias camadas em terminais que recomendamos na HP ajudará a garantir a conformidade com o RGPD.

Neste guia eletrónico, analisamos os componentes-chave do RGPD que os profissionais de TI precisam de conhecer e destacamos como um programa de segurança de terminais, orientado para dispositivos, pode ajudar a garantir a conformidade.

O RGPD na UE

Os pontos-chave para as TI

Existem dois pontos essenciais no RGPD: proteger os direitos dos dados dos indivíduos na UE e proteger a privacidade dos dados dos indivíduos na UE. Ambos têm implicações em termos tecnológicos.

Para saber mais informações, leia o texto completo. Mas para os decisores de TI, estes são os pontos que deve conhecer:

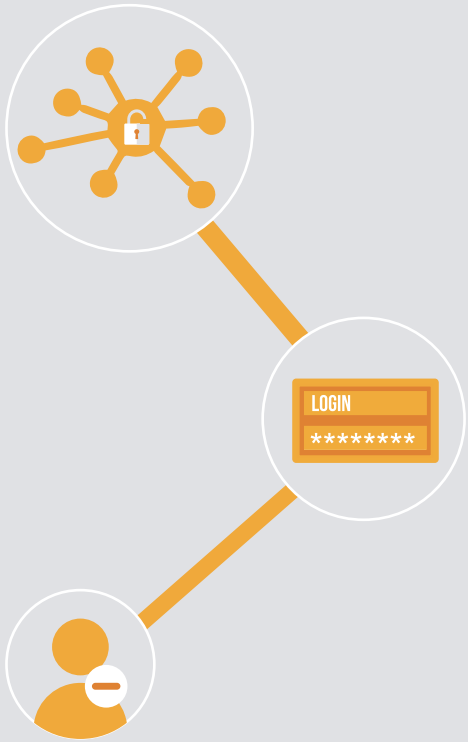
1. **As falhas devem ser comunicadas no período de 72 horas**
   Caso ocorra uma violação de dados, esta deve ser comunicada no período de 72 horas após tomar conhecimento. As sanções pelo não cumprimento desta medida são avultadas (consulte a secção "Quais são as sanções em caso de não cumprimento?" na página 5).

2. **O direito à eliminação de dados**
   Todos os indivíduos na UE têm o direito de solicitar a eliminação dos respetivos dados. Mediante pedido, deverá eliminar os respetivos dados, incluindo todas as cópias.

3. **O direito à portabilidade de dados**
   Os residentes na UE têm o direito de controlar os seus próprios dados. Mediante pedido, deverá fornecer os seus dados num formato acessível, caso seja permitida a transferência desses dados a terceiros.

4. **Transferências internacionais**
   A transferência de dados pessoais para outra jurisdição de dados (ou seja, fora da UE) só pode ser feita mediante consentimento explícito, e apenas a reguladores considerados como "adequados", ou com salvaguardas adicionais postas em prática.[1]

5. **Privacidade desde a conceção**
   As organizações devem adotar uma abordagem de privacidade desde a conceção que integre, por defeito, a segurança dos dados nos produtos, processos e serviços.[2,3]



A quem se aplica o RGPD?

O RGPD aplica-se a qualquer empresa que recolha e/ou processe dados pessoais de residentes na UE. Isto abrange organizações sediadas fora da UE, mas que desenvolvam atividade dentro da UE.

[1]https://iapp.org/news/a/top-10-operational impacts-of-the-gdpr-part-4-cross-border-data-transfers/ [2]Artigo "The EU General Data Protection Regulation" elaborado pela Allen & Overy (2016)
[3]http://www.computerweekly.com/news/450296306/10-key-facts-businesses-need-to-note-about-the-GDPR

O RGPD na UE

O que são considerados "dados pessoais"?

De acordo com o RGPD, "dados pessoais" abrangem "todos os dados que possam ser usados para identificar um indivíduo."

Isto inclui informações genéticas, mentais, culturais, económicas ou sociais, para além das informações normalmente consideradas como sendo informações de identificação.

Isto poderá levar a que as organizações que anteriormente não estavam abrangidas pelo âmbito da legislação de proteção de dados fiquem sob a alçada do RGPD.

Quais são as sanções em caso de não cumprimento?

A multa máxima é de 20 milhões de euros ou 4% da faturação global, o valor que for mais elevado. Esta multa aplica-se aos delitos mais graves de acordo com o regulamento, tais como a não comunicação de uma falha de segurança no período de 72 horas após ter tido conhecimento.

Aos delitos menos graves aplicam-se multas de 10 milhões de euros ou 2% da faturação global. Escusado será dizer que os custos resultantes do não cumprimento são avultados.

Lista de verificação de procedimentos do RGPD

Na sua estrutura de Governança de Dados, deverá dispor de procedimentos explícitos para:

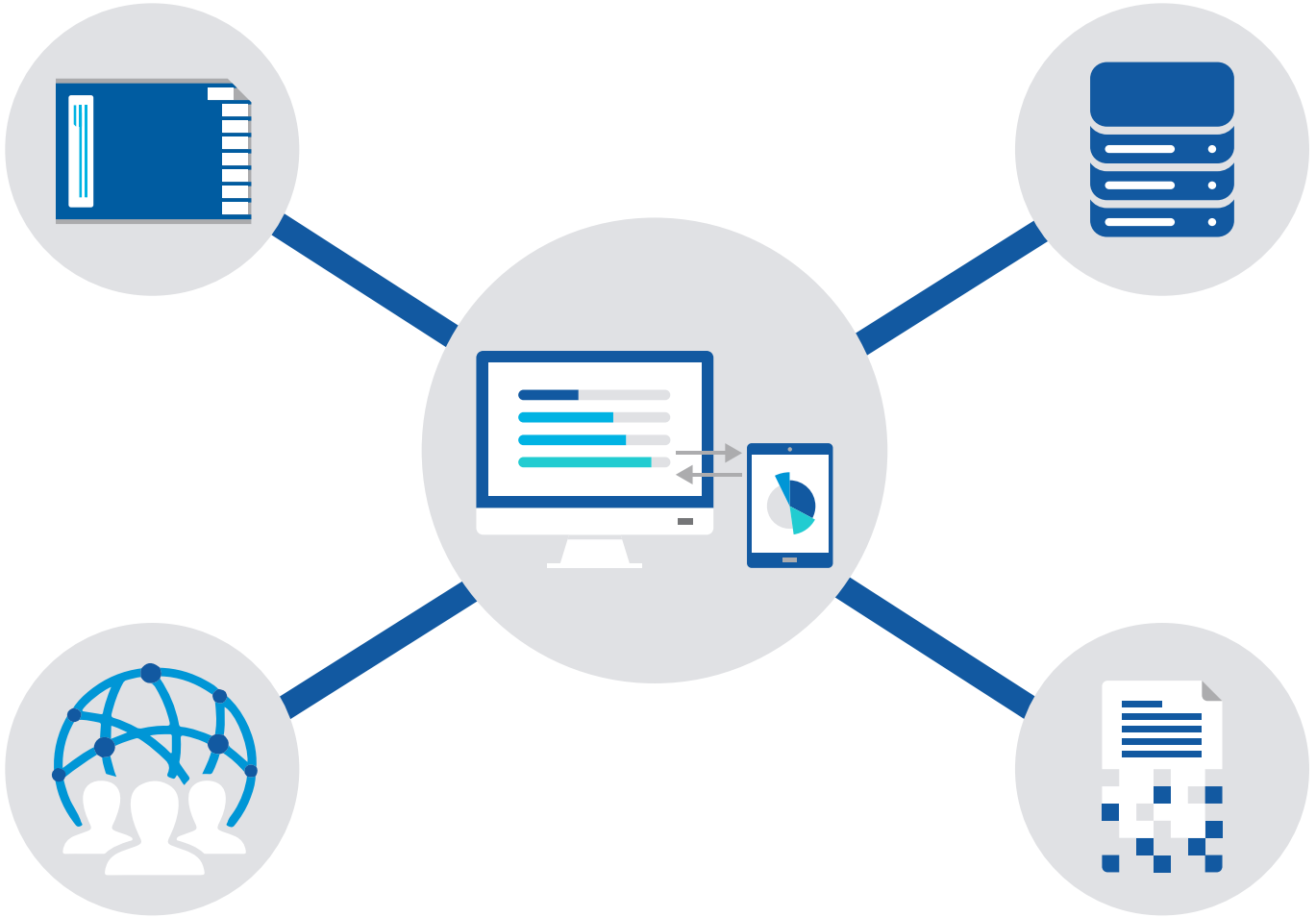
- Informar os indivíduos de como os seus dados serão recolhidos, armazenados e processados.
- Obter o consentimento explícito do indivíduo para o fazer.
- Fornecer as informações do indivíduo num formato que lhe seja acessível.
- Eliminar todos os dados pessoais do indivíduo, incluindo cópias.
- Transferir dados para outro controlador ou processador de dados.
- Transferir dados fora da UE – incluindo dentro da organização.

Os desafios técnicos da conformidade

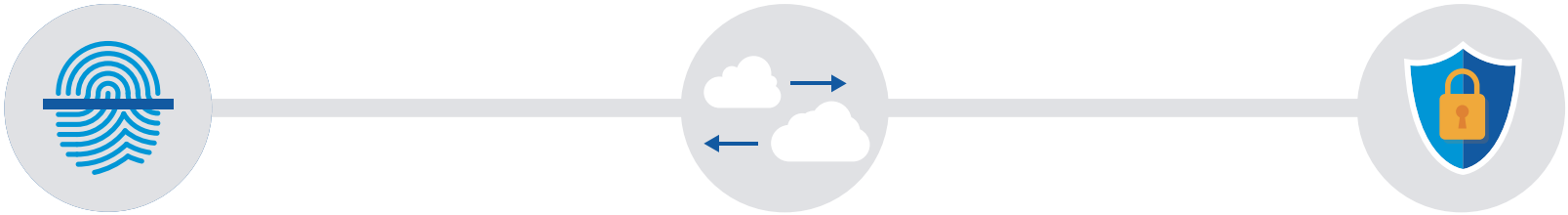
Os maiores desafios do RGPD são de natureza técnica.

Permitir uma portabilidade de dados segura, proteger os dados do indivíduo e o seu direito a ser esquecido, tudo isto requer um mapa abrangente de localização dos dados e acesso ao nível do dispositivo.

À medida que a ameaça do cibercrime aumenta de ano para ano, manter uma segurança absoluta é um desafio constante.



Os desafios técnicos da conformidade



Monitorizar os dispositivos

Cumprir a portabilidade de dados e o direito a ser esquecido requer um registo detalhado de todos os dados pessoais detidos pela organização.

Tem de ter conhecimento de:

- Todos os dispositivos que detêm dados pessoais.
- Todos os dispositivos que têm acesso a dados pessoais.

Esta é a única forma de garantir que consegue recuperar e/ou eliminar os dados pessoais detidos pela empresa.

Monitorizar as nuvens

A empresa europeia média utiliza 608 aplicações, um número estimado em 90% não registado em estatísticas. Muitas vezes, os funcionários utilizam aplicações de nuvem comerciais sem o conhecimento do departamento de TI.[4]

Para cumprir o RGPD, a utilização da nuvem deve estar confinada a serviços que estejam:

- Dentro da UE, e por isso, de acordo com o RGPD e em conformidade.
- De acordo com a jurisdição do regulador de proteção de dados considerado "adequado" pela UE.

Tudo o resto poderá constituir violação da regra de transferência internacional. E deve saber quais os serviços de nuvem que os funcionários utilizam, caso o direito de ser esquecido seja invocado.

Manter os dados protegidos

A ameaça do cibercrime está a crescer. As redes desprotegidas e os dispositivos pessoais também estão a crescer.

As falhas são praticamente inevitáveis. A UE sabe disso. Mas, para evitar uma multa avultada, deve:

- Implementar uma ferramenta SIEM (Systems Incident Event Monitoring) para comunicar uma falha no período de 72 horas.
- Implementar uma segurança de várias camadas em terminais para demonstrar a devida diligência na prevenção de uma falha.

Os utilizadores devem ter conhecimento das respetivas responsabilidades em não utilizar dispositivos e redes não autorizados.

[4]https://www.cloudindustryforum.org/content/cloud-and-eu-gdpr-six-steps-compliance

A ameaça do cibercrime

O cibercrime é uma ameaça real, presente e em crescimento

82%

das organizações depararam-se com uma falha/ameaça nos últimos 12 meses.[5]

80%

dos profissionais de TI afirmam que a ameaça do cibercrime vai aumentar nos próximos 3 anos.[6]

78%

das empresas comunicaram um aumento no número de ataques de malware nos últimos 5 anos.[7]

60%

dos líderes de TI afirmam que o cibercrime está a superar as defesas. [8]

81%

das empresas classificam a negligência interna como a maior ameaça à cibersegurança. [9]

81%

dos líderes de TI afirmam que os dispositivos móveis nas suas redes foram alvo de malware.[9]

72%

afirmam que a utilização de software de nuvem comercial por parte dos funcionários representa um risco. [9]

69%

afirmam que a política BYOD (bring your own device) representa um risco à segurança.

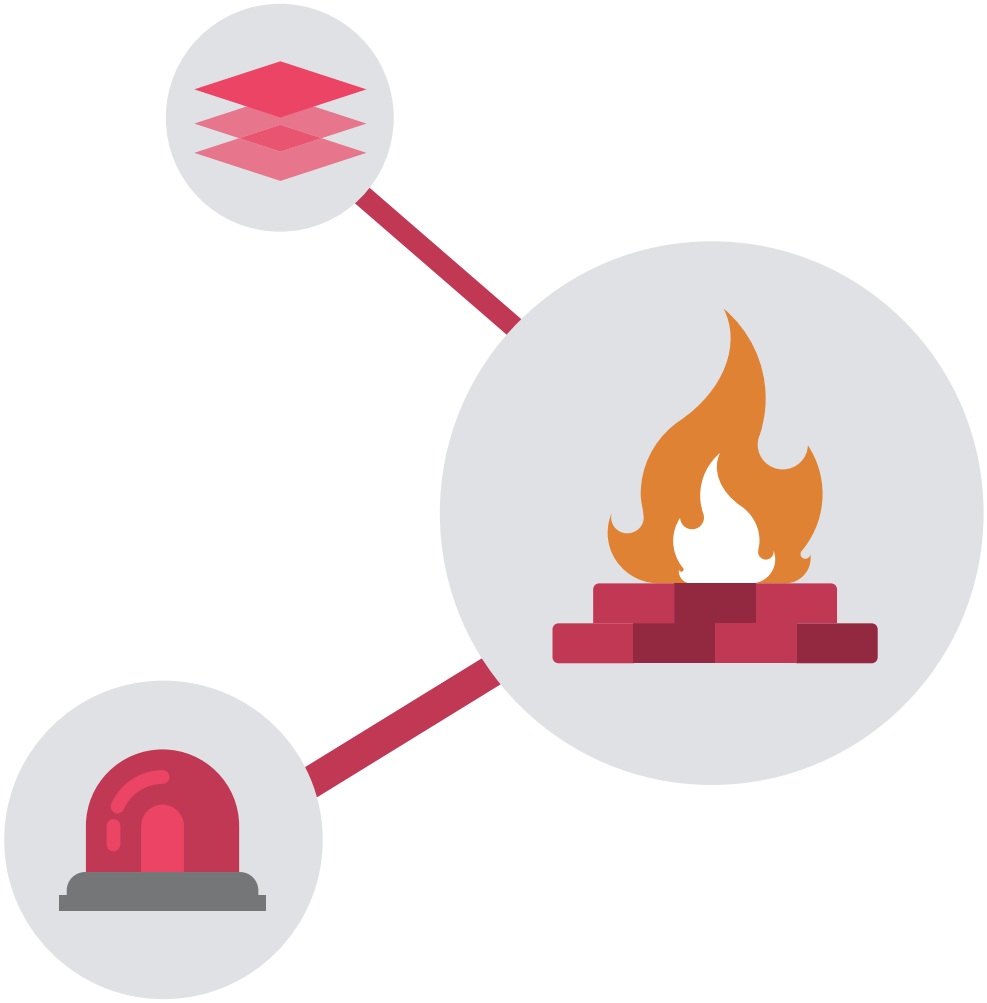
[5]Estudo "HPI Printer Security" elaborado pela Spiceworks (2016) [6]Relatório "HP Printer Security" (2015) [7]Relatório "State of the Endpoint" elaborado pela Ponemon (2016) [8]Estudo "CISO Assessment" elaborado pela IBM (2014) [9]Relatório "State of the Endpoint" elaborado pela Ponemon (2016)

A implementação da segurança de terminais

A abordagem de várias camadas da HP à segurança de terminais

A abordagem de prevenção e proteção da cibersegurança – firewall e antivírus – já não é suficiente. Nunca foi. Num estudo realizado pela Damballa, um software antivírus demorou cerca de 6 meses a identificar e eliminar 100% dos ficheiros maliciosos existentes.[10]

A HP afirma que a cibersegurança deve ter várias camadas, operar ao nível da rede, do dispositivo e do utilizador, com diversas defesas em cada um deles. Detetar e responder deve ser mais importante do que proteger e defender. E os terminais são o ponto de partida: tanto o dispositivo, como o utilizador.



Ações Critical Security Controls (CSC)

O Center for Internet Security (CIS) definiu 20 ações Critical Security Controls (CSC) reconhecidos em termos internacionais, desenvolveu-os e validou-os ao recorrer a especialistas em segurança de TI em todo o mundo. Estes são considerados importantes ações de "ciber-higiene" para todas as organizações.

Apenas referimos os principais CSC para conformidade com o RGPD, visto serem diretrizes úteis; o texto completo está disponível online. Descarregue-o gratuitamente na biblioteca CIS.

[10]https://www.damballa.com/time-to-fix-malware-strategies-2/

Segurança da rede

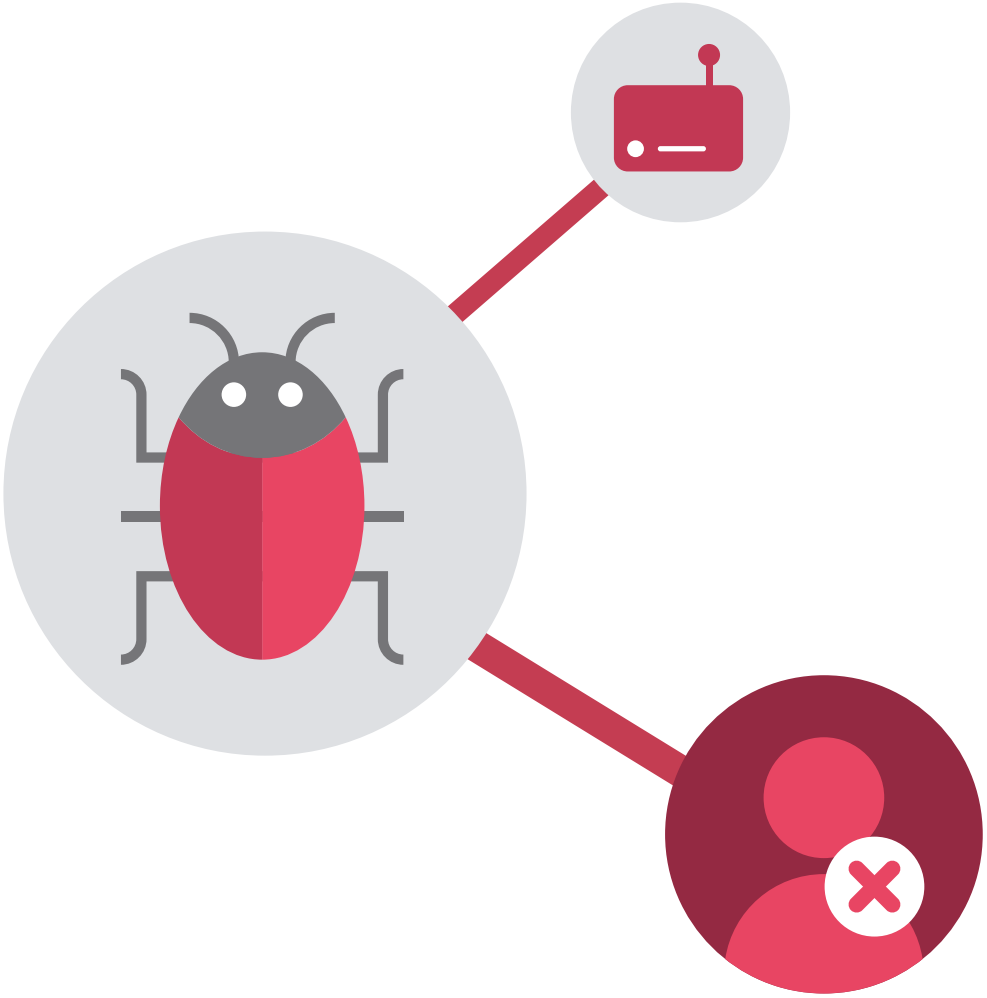
Os grandes ataques tendem a explorar apenas um ponto de entrada para obter acesso a toda a rede. Assim sendo, a segurança ao nível da rede deve ter como base a prevenção desse acesso indevido.

- **Controlo de privilégios administrativos (CSC 5)**
  Restringir a capacidade de alterar as definições da rede e as palavras-passe ao menor número de pessoas possível.
- **Controlo do acesso com base no princípio "necessidade de ter conhecimento" (CSC 14)**
  Controlar o acesso a informações confidenciais sobre o utilizador, o dispositivo e a localização. Avaliar o risco de segurança em relação à sensibilidade dos dados.
- **Limitação e controlo das portas, protocolos e serviços da rede (CSC 9)**
  Desligar quaisquer pontos de acesso desnecessários – virtuais e físicos –, incluindo o FTP, Telnet e serviços de impressão.
- **Manutenção, monitorização e análise de registos de auditorias (CSC 6)**
  Rever regularmente os registos de auditorias para analisar o comportamento do sistema e detetar atividades suspeitas.
- **Avaliação e remediação contínua da vulnerabilidade (CSC 4)**
  Avaliar continuamente a vulnerabilidade do ambiente e adotar medidas para corrigir os resultados, minimizando a oportunidade de ocorrência de falhas.

O objetivo é ter uma rede subdividida de acordo com a sensibilidade das informações. Os pedidos de acesso são avaliados conforme os riscos de segurança. Os dispositivos, utilizadores e pedidos desconhecidos de redes não seguras são bloqueados para a maioria das informações sensíveis. A política BeyondCorp da Google é um bom modelo.[11]

[11] https://research.google.com/pubs/pub43231.html

Segurança da rede



Todos os dispositivos são uma potencial vulnerabilidade, sejam eles profissionais ou pessoais. Deve conhecer cada smartphone, tablet, computador portátil ou computador que acede aos dados da empresa.

- **Inventário de dispositivos autorizados e não autorizados (CSC 1)**
  Realizar auditoria a todos os dispositivos que podem aceder aos dados.
- **Inventário de software autorizado e não autorizado (CSC 2)**
  Realizar auditoria a todas as aplicações utilizadas na rede – para aceder diretamente a dados ou não.
- **Defesas contra malware (CSC 8)**
  Garantir que todos os dispositivos estão atualizados em termos de antivírus e deteção de malware. Garantir análises e atualizações regulares.

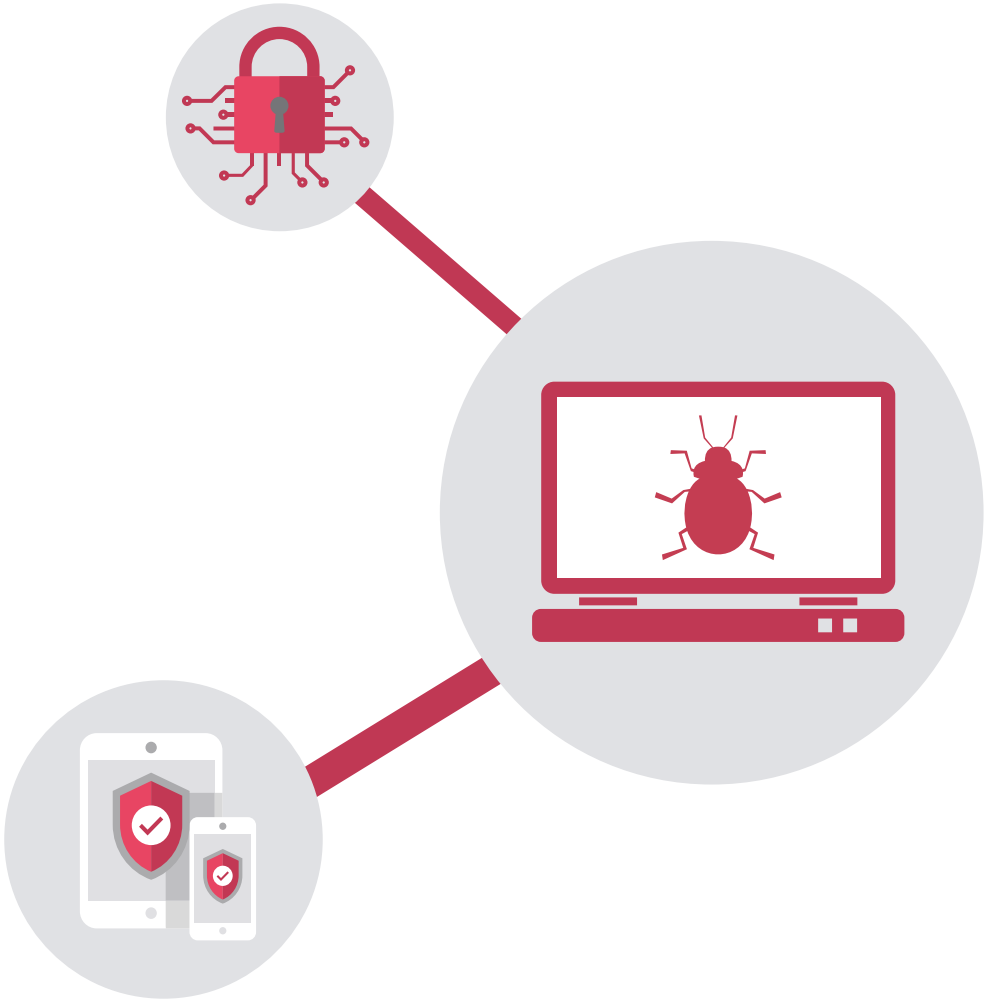
Segurança dos dispositivos

Para além disso, os departamentos de TI devem considerar as seguintes verificações adicionais:

- **Autenticação multifator**
  Garantir que todos os dispositivos de trabalho são seguros. De uma forma ideal, utilizar autenticação biométrica juntamente com palavras-passe (consulte a secção "Dispositivos com privacidade desde a conceção" na página 14).
- **Acesso remoto**
  Garantir um acesso remoto ao dispositivo para recuperar ou eliminar dados pessoais, colocar em quarentena e terminar processos, e desligar e bloquear o dispositivo em caso de perda ou roubo (consultar a secção "Detetar e responder" na página 14).
- **Informar todos os funcionários acerca de protocolos e procedimentos de segurança**
  Garantir que todos os funcionários têm conhecimento das suas responsabilidades relativamente à cibersegurança, incluindo comunicar atividades suspeitas.
- **Realizar sessões de formação ativas sobre cibersegurança**
  Organizar workshops, seminários e simulacros de phishing – garantir que todos sabem como evitar erros básicos e como manter a conformidade com o RGPD.
- **Minimizar a utilização de dispositivos/aplicações pessoais**
  Desincentivar a utilização de dispositivos e aplicações pessoais para fins profissionais. Uma política de CYOD (choose your own device) abrangente e flexível deve ajudar.

Implementar uma estrutura de segurança como esta deve ajudá-lo a manter o controlo sobre os dispositivos da empresa, ajudá-lo a proteger os dados e facilitar a portabilidade dos dados e o direito a ser esquecido.

Para saber mais informações sobre a abordagem da HP à segurança de várias camadas, leia o nosso livro branco empresarial "Security Begins at the Endpoint" (A segurança começa nos terminais).



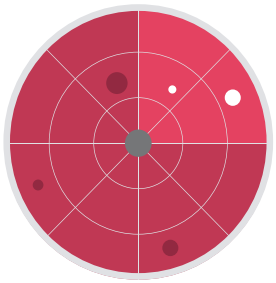
Por que motivo devem todos os funcionários estar atentos ao cibercrime

58% das ciberameaças vêm de funcionários, antigos funcionários e parceiros de confiança.[12] Manter os dispositivos seguros significa manter os seus utilizadores seguros.

- O Democratic National Committee (DNC) dos E.U.A. foi atacado, em 2016, quando John Podesta clicou numa hiperligação de phishing erradamente identificado como legítimo por um assistente.[13]
- Fotografias de celebridades nuas inundaram a Internet, em 2014, após Ryan Collins, de 36 anos, ter acedido às iClouds de Jennifer Lawrence e de outros com e-mails de phishing básicos fingindo representar a Apple.[14]
- 68 milhões de palavras-passe da Dropbox foram divulgadas em 2012 devido a um funcionário que usava a mesma palavra-passe para sistemas internos e para aceder ao seu LinkedIn.[15]
- O Presidente Donald Trump continua a usar um smartphone normal Samsung Galaxy. Os especialistas não questionam se já terá sofrido ataques de hackers, mas sim quantos serviços de espionagem já o fizeram.[16]

[12]http://www.clearswift.com/sites/default/files/images/blog/enemy-within.pdf [13]https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds [14]http://www.forbes.com/sites/thomasbrewster/2016/03/16/icloud-hacking-jennifer-lawrence-fappening-apple-nude-photo-leaks/#45fed5d77b88 [15]https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach [16]https://www.theguardian.com/commentisfree/2017/feb/19/if-trump-hates-leaks-needs-to-give-up-phone

Detetar e responder

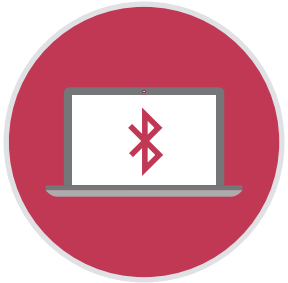


Detetar e responder é uma estrutura de cibersegurança que reconhece que a prevenção total é praticamente impossível.

O que interessa é ter consciência da falha (detetar) e adotar medidas imediatas (responder).

Estão disponíveis produtos de software que transformam qualquer dispositivo num sensor em tempo real, e permitem ao administrador responder, por exemplo, desligando os dispositivos, colocando ficheiros em quarentena e eliminando dados.

Dispositivos com privacidade desde a conceção



Os dispositivos da HP integram a privacidade desde a conceção.

As funcionalidades de segurança incluem o primeiro BIOS com capacidade de autorrecuperação, bloqueio automático por Bluetooth – que bloqueia o dispositivo quando o utilizador se afasta deste – e ecrãs de privacidade incorporados.

Estas funcionalidades não garantem, por si só, a conformidade com o RGPD, mas certamente ajudarão.

A preparação para o RGPD

Os passos práticos que deve executar agora

O RGPD entra em vigor a 25 de maio de 2018. Ainda há tempo para se preparar, mas como deve saber, há muito a fazer.

O primeiro passo é **realizar uma auditoria à sua situação atual em termos de dados**. Avalie onde os seus dados estão armazenados, onde são copiados e quem tem acesso aos mesmos. Caso utilize soluções de nuvem, saiba onde estão localizados os servidores e se estão em conformidade com o RGPD. O mesmo se aplica a qualquer SaaS (software como serviço) ou organizações parceiras com as quais trabalhe e partilhe os seus dados. Isto permitir-lhe-á ter uma ideia clara daquilo que precisa de ser alterado para estar em conformidade.

Crie a sua política de dados. Inclua procedimentos detalhados e protocolos sobre onde os dados estão armazenados, quem tem acesso a esses dados e quem faz cópias fora da empresa, ou além fronteiras no caso de uma multinacional. Inclua procedimentos para recuperar e eliminar dados pessoais. Comunique estes procedimentos a todos os funcionários da empresa. Realize sessões de formação. Destaque a sua importância.

Crie a sua política de segurança. Crie uma nova estrutura de cibersegurança que funcione numa base de deteção e resposta no terminal. Reorganize a sua política de dispositivos, se necessário. Invista em novas tecnologias, se necessário. Apenas 36% dos líderes de TI sentem que dispõem de um orçamento suficiente para garantir a segurança de terminais.[17] As sanções do RGPD podem ser a chamada de atenção para ter todos os executivos interessados no assunto.

[17]Relatório "State of the Endpoint" elaborado pela Ponemon (2016)

A preparação para o RGPD

Lista de verificação do RGPD

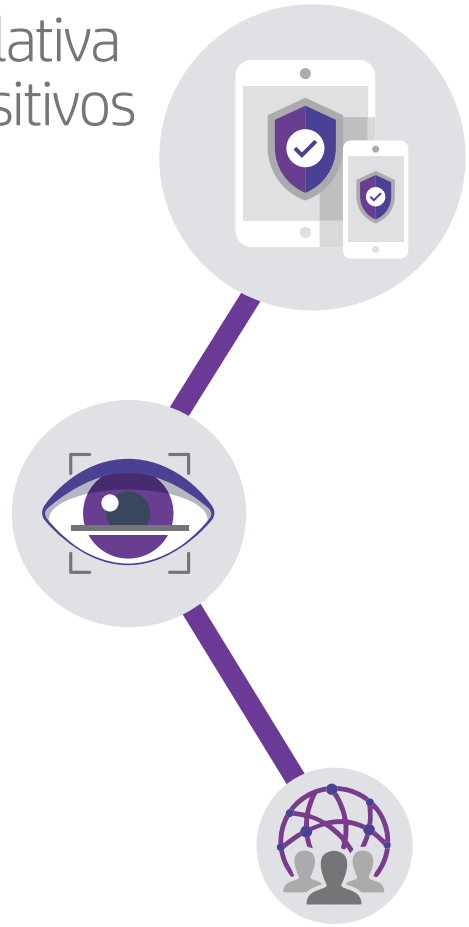
Os 5 pontos-chave para estar em conformidade com o RGPD

1. Nomeie alguém para ser responsável pelos dados, um Diretor de Proteção de Dados (DPO ou Data Protection Officer), se necessário.
2. Realize uma auditoria completa aos dados, incluindo a conformidade de nuvens e fornecedores de SaaS relativamente ao RGPD.
3. Crie uma nova estrutura de governança de dados, incluindo procedimentos para portabilidade de dados e direito a ser esquecido.
4. Crie uma nova estrutura de cibersegurança, implementando uma segurança de várias camadas nos terminais.
5. Comunique as políticas e protocolos a todos os funcionários da empresa.

Lista de verificação relativa à segurança de dispositivos

Os 6 passos-chave para manter os terminais seguros

1. Realize uma auditoria a todos os dispositivos autorizados e não autorizados que tenham acesso a dados pessoais.
2. Invista em novos dispositivos – e mais seguros –, se necessário.
3. Implemente o acesso remoto e direitos de eliminação de dados em dispositivos.
4. Implemente uma política de análise regular e atualização de software de segurança.
5. Implemente software de deteção e resposta em tempo real.
6. Dê formação sobre cibersegurança aos seus funcionários.



Calendário de segurança dos terminais

Um calendário básico para implementação da segurança nos terminais de acordo com o RGPD

2017

Maio

Nomear um gestor de projetos responsável pela implementação de segurança de terminais

Junho

Realizar auditorias às políticas de segurança, práticas e dispositivos atuais

Julho

Considerar os requisitos de dispositivos e políticas para segurança de terminais (CYOD/BYOD, etc.)

Agosto

Considerar soluções de software para deteção e resposta de segurança

Setembro

Criar um sistema de acesso multidisciplinar para dados da empresa

Outubro

Criar uma nuvem pública/privada para permitir um acesso a dados fora do local adequado

Novembro

Criar um programa de formação de utilizadores, incluindo ensaios de phishing

Dezembro

Comunicar as novas políticas de segurança à restante empresa

2018

Janeiro

Implementar uma nova arquitetura de dados na nuvem pública/privada

Fevereiro

Implementar uma nova política de dispositivos

Março

Implementar uma solução de software de deteção e resposta

Abril

Realizar formação em segurança para utilizadores, incluindo políticas relacionadas com o RGPD

Maio

O RGPD entra em vigor

Resumo

O RGPD está quase a chegar

Se tiver sorte, a sua organização já coloca em prática a maior parte dos regulamentos – estes são, em grande parte, uma mera formalização daquilo que constitui as melhores práticas.

E, se tem vindo a desenvolver atividade em diversos países da UE, é provável que já se tenha deparado com algumas destas medidas mais extremas.

As medidas de segurança que recomendamos que adote de forma a cumprir o RGPD são medidas que ajudam a prevenir falhas, que podem ser incrivelmente dispendiosas para uma organização. De acordo com os mais recentes dados estatísticos, o governo britânico estimou que as empresas no Reino Unido perdem 21 mil milhões de libras num único ano, um número que deverá aumentar ainda mais.[18]

Para além disso, muitas das medidas necessárias para garantir uma segurança verdadeiramente robusta ajudarão a cumprir outros aspetos do RGPD. Restringir o acesso de dados a determinados utilizadores, dispositivos e redes não só minimiza o risco para os dados, como torna mais fácil localizar os dados pessoais – e, desta forma, cumprir a portabilidade de dados e o direito a ser esquecido; já para não falar das transferências internacionais.

Este guia eletrónico é apenas o começo. A segurança tem sido sempre uma prioridade para a HP. A privacidade desde a conceção tem sido a nossa política durante muitos anos. Agora que é necessária, em vez de desejada, estamos numa boa posição de o ajudar a adotar a mesma abordagem.

Para saber mais informações sobre a HP e sobre como os nossos produtos podem ajudá-lo a cumprir o RGPD, consulte **a nossa página "Privacidade desde a conceção".**

[18]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the cost-of-cyber-crime-full-report.pdf