# Segurança de Informação

# Para além de boas intenções

**Embora a Segurança de Dados e Informação seja um dos temas mais frequentemente discutidos nos tempos que correm, continua infelizmente a ser muitas vezes negligenciado. Aliás, o número de empresas que afirma ter perdido dados importantes, ou até confidenciais, devido a ameaças de segurança, está a aumentar. Num mundo em constante mudança, também ao nível das ameaças, a proteção da informação requer-se embebida nas atividades e operações das organizações, a todo o momento.**

Apesar do conhecimento das consequências que a perda de dados pode ter no normal funcionamento de uma organização, é frequentemente transposta a ténue linha que pode conduzir ao acidente.

**Segurança é, antes de mais, uma questão comportamental**

Numa sociedade cada vez mais globalizada, onde a produção de informação digital atinge recordes a cada dia que passa, a segurança de dados não significa apenas a utilização de um qualquer mecanismo de backup ou um simples antivírus. Nos dias de hoje, os tradicionais planos de segurança *per si* são manifestamente insuficientes, sobretudo se tivermos em conta que a questão de fundo é transversal a utilizadores e decisores, pois é essencialmente comportamental.

**Muitas organizações não têm planeado investimentos em segurança a curto prazo, nem Políticas e Normas para a Segurança da Informação**

Sintomático desta atitude, é a conclusão que se pode extrair de inquéritos publicados por diversos estudos efetuados quer pelos principais fabricantes de tecnologia, como por consultoras e organismos públicos, conclui-se que a maioria das organizações, principalmente as PMEs, não leva a segurança muito a sério, não tendo planeado qualquer investimento a curto prazo, nem dispondo de Políticas e Normas para a Segurança da Informação.

Mas quando estamos afinal perante uma perda de dados? Convencionalmente, poder-se-á definir uma perda de dados como uma situação em que o acesso aos dados armazenados digitalmente, seja qual for o suporte, é impedido de uma forma permanente. As causas para esta situação são as mais díspares e passam por avarias eletrónicas ou mecânicas, erros humanos, formatação dos dispositivos de armazenamento, incêndios, desastres naturais, pirataria e *hacking* ou o agora tão falados *Phishing* e *Rasonwares.*

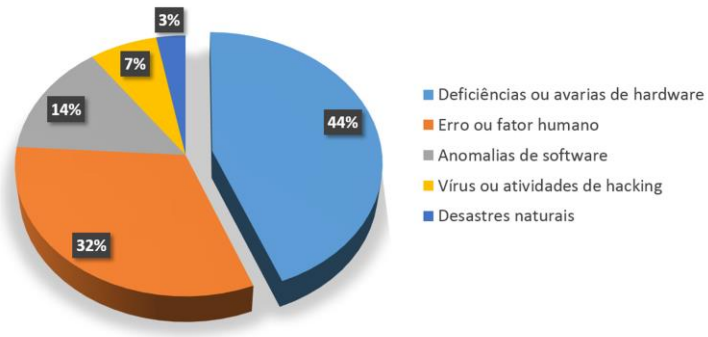
**Erros ou falhas de hardware e erro humano são as principais causas da perda de dados**

De acordo com alguns dos estudos que têm vindo a ser publicados, aproximadamente metade das perdas de dados devem-se a erros de hardware. No caso de particulares, resultam essencialmente de falhas nos discos rígidos e memórias flash, sendo que ao nível empresarial, é necessário ainda que incluir problemas com os sistemas RAID ou ações desenvolvidas por técnicos não qualificados. Ao erro humano é atribuído o segundo lugar do ranking das principais causas de perda de informação e, curiosamente, os tão temidos vírus não representam uma percentagem superior a 7%.

**Pense!**
**Com a alteração da ordem mundial em termos geopolíticos e geoestratégicos, onde vai querer ter os seus dados?**

**As ameaças vindas do interior da organização superam ataques externos**

Ainda relacionado com a perda de informação, está a proliferação de equipamentos portáteis, que embora redefinam o conceito de mobilidade e tenham um contributo decisivo na produtividade, são também responsáveis pelo aumento da vulnerabilidade face a acidentes ou roubos. Outro dos elementos interessantes que se tem trazido para a discussão da segurança de dados está ligado ao facto de, nos dias de hoje, as ameaças provenientes do interior da própria organização surgirem num patamar superior ao dos ataques com origem externa.




A colaboração online entre os funcionários de uma empresa, bem como as ações que possam desenvolver como gestão de contas bancárias, interação em redes sociais, falta de capacidade crítica sob os emails que lhe são endereçados, não só se pode traduzir numa má prática generalizada, como ser o suficiente para tornar um sistema vulnerável, elevar significativamente o risco e até manchar a imagem corporativa de uma organização.

**A análise dos riscos é essencial para quantificar o nível de exposição**

A análise dos riscos de segurança, ou tão-somente do risco é, pois, essencial na avaliação dos custos diretos e indiretos aos quais a organização é exposta, bem como ao nível a que se pode aceitar expor o negócio. Uma das metodologias com que se pode avaliar o risco traduz-se pela equação:

$$\text{Risco} = \frac{\text{Ameaça} * \text{Vulnerabilidade}}{\text{"Contra} - \text{medidas"}}$$

A *Ameaça* afigura o tipo de ação com potencial para danificar ou causar grande impacto, sendo que a *Vulnerabilidade* representa o nível de exposição à ameaça num âmbito em particular. Já as *Contra-medidas*, ou também denominadas medidas defensivas, caracteriza o conjunto de ações desenvolvidas no sentido de prevenir a *Ameaça*.

O conceito de *Contra-medidas* não passa exclusivamente por um conjunto de medidas de carácter técnico. Passa também pela formação, pelo compromisso dos utilizadores e pela precisão com que as regras estão definidas e são divulgadas no seio das Empresas e Organizações.

**Sensibilização e formação dos utilizadores deverá ser uma prioridade**

É no seguimento desta ideia, que a segurança informática de uma empresa e, em particular dos seus dados, resultam obrigatoriamente de um conhecimento claro por parte dos colaboradores das normas em vigor e das obrigações de cada um.

Este conhecimento não deve, no entanto, passar exclusivamente pela publicação de documentos com procedimentos ou avisos. Será, pois, necessário dar passos determinados na implementação de uma política que facilite a transmissão de conhecimento e a chegada de informação às pessoas: onde claramente o binómio sensibilização e formação seja enfrentado como uma prioridade.

Indiferentemente da orientação a seguir, existe um conjunto de pontos que deverão fazer parte de um plano. São eles:

- Disponibilização de dispositivos de segurança físicos e lógicos, adaptados às necessidades de cada empresa e ao uso dos seus colaboradores;
- Regras e Políticas de Segurança da rede, com destaque para as que podem expor a organização a ameaças externas, como a utilização do e-mail ou Internet;
- Formação de colaboradores e consciencialização para comportamentos a evitar;
- Plano de recuperação após incidente;
- Estratégias de salvaguarda, corretamente planificadas;
- Procedimentos para uma correta gestão de atualizações;
- Documentação atualizada sobre os sistemas (sejam de hardware ou software) e quais as interações entre cada um e eventuais dependências.

## Pense! A sua informação está segura?
## Onde tem os seus dados? Como acede? Com quem partilha?

Numa PME ocorrem em média entre 1 a 2 perdas de dados por ano. Para estas empresas tratam-se de perdas significativas que podem levar à falência. Estimam-se perdas em média na ordem dos 10K€/dia. Muitas das empresas vão à falência em 1 a 2 anos após uma perda maior de dados. Estas perdas têm ainda um impacto significativo na reputação. Estudos apontam que cerca de 54% dos Clientes de PME mudaram de fornecedores porque os anteriores não tinham sistemas fiáveis. Mais de 30% das empresas que faz backups regulares não faz cópia dos e-mails.

De um ponto de vista técnico, e tendo em atenção as várias soluções não tradicionais, uma das abordagens passa pela DLP (*Data Lost Prevention*), que tem demonstrado um grau de eficiência e proteção elevados. A tecnologia DLP é utilizada para proteger informações sensíveis, tais como: dados financeiros, informação médica, detalhes de contas bancárias ou informação de caráter privado. Os dados são bloqueados sempre que não seja autorizada a sua difusão ou onde não estejam a ser cumpridas regras para a sua transmissão, como por exemplo, o recurso a encriptação. Embora a DLP conte ainda com algumas lacunas, nomeadamente a incapacidade em filtrar imagens, é uma tecnologia que eleva a fasquia na prevenção da perca de dados, ou da propriedade intelectual de um Indivíduo ou da sua Organização.

Em suma, o importante a reter é a necessidade inequívoca de uma aposta em segurança dos dispositivos informáticos, nas redes de dados, assim como na formação dos recursos humanos. Para além de demonstrar clarividência, é uma aposta na robustez da organização e sobretudo no que é *core* ao seu funcionamento: os Dados e a Informação.

Contratar um serviço gerido de TI (*IT Managed Services*) profissional continuado para cuidar das TIC e dos dados é a primeira e melhor decisão para garantir a continuidade do negócio. Paga-se por si próprio em menos de 6 meses. Vale mais ter algum custo, definido e controlado, do que sujeitar-se ao imponderável. Deve salvaguardar os dados todos fora do escritório, incluindo e-mail, não apenas uma parte. A decisão pela implementação de boas práticas (normas e procedimentos) percetíveis para o exterior (Clientes e fornecedores) trará notoriedade e confiança.

## Os 10 Mandamentos da Segurança de Informação

1. Implemente todos os mecanismos de proteção da informação do seu computador, recorrendo ao uso de passwords: passwords de arranque, de rede e de *screen saver*;
2. As passwords são pessoais. Garanta que as mantém secretas e que faz uma alteração regular das mesmas;
3. Efetue backups regularmente, pois é a única forma de proteger a sua informação;
4. Quando viaja, nunca perca de vista os seus dispositivos - laptop, tablet e mobile phone. Transporte-os de forma discreta;
5. Não publicite o seu endereço de e-mail na internet;
6. Não aceda a sites com conteúdos algo duvidosos e que solicitem o seu registo;
7. Não abra e-mails desconhecidos e/ou suspeitos. Mesmo que abra e-mails suspeitos não clique em links nem abra ficheiros em anexo;
8. Assegure-se de que todos os upgrades de software são efetuados de acordo com as recomendações e prazos definidos;
9. Tenha atenção ao conteúdo das conversas ao telemóvel em locais públicos;
10. Proteja a informação, classificando-a como Secreta, Confidencial ou Particular.