Revista "O Molde"; CEFAMOL; N.127; pp.32.34; Outubro 2020
https://www.cefamol.pt/index.php?id=85&idn=324

DESAFIOS DA GESTÃO E SEGURANÇA DOS DADOS NAS EMPRESAS

Mário Antunes *
* Instituto Politécnico de Leiria (IPLeiria); Centro de Investigação em Informática e Comunicações (CIIC - IPLeiria)
Center for Research in Advanced Computing Systems (CRACS – INESC-TEC)

ENQUADRAMENTO

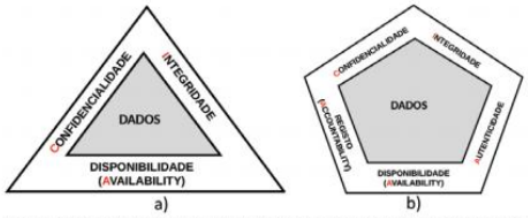
A gestão e a tomada de decisões nas empresas fazem-se com recurso a informação credível, relevante, íntegra e que esteja atempadamente disponível. A digitalização crescente das empresas, transversal aos vários sectores de atividade, originou o aumento exponencial do volume de dados produzidos e, consequentemente, da informação que daí se pode extrair. A globalização das empresas neste ambiente digital tem potenciado a competitividade dos negócios, mas também a necessidade de implementar mecanismos cada vez mais eficazes de segurança da informação, que evitem a exfiltração dos dados e o acesso indevido.

Os dados e a informação são ativos muito importantes para as empresas. Além dos dados referentes às atividades do negócio (por exemplo, faturação, indicadores de produção, clientes e fornecedores), são igualmente relevantes os que estão relacionados com os registos de atividade dos servidores (vulgarmente designados por *logs*), os documentos referentes à propriedade intelectual e industrial e os dados pessoais dos colaboradores e de outras entidades que se relacionam direta ou indiretamente com as empresas. A localização dos dados assenta atualmente em soluções descentralizadas, onde a cloud assume um papel de complementaridade aos servidores locais. Por estas razões torna-se importante quantificar com rigor o valor dos dados e definir estratégias concertadas para a sua proteção.

O VALOR DOS DADOS E OS PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

O valor dos dados e, consequentemente, da informação, é de difícil quantificação e envolve várias dimensões, como a área de atuação das empresas, a sua dimensão ou o volume de negócios. Em cada caso importa quantificar o valor que uma determinada informação terá nas tomadas de decisão por parte do gestor e, não menos importante, quanto poderá valer essa informação para as empresas concorrentes. Esta quantificação é particularmente importante, no sentido de definir e implementar estratégias realistas de gestão e proteção dos dados, assentes nos princípios básicos de segurança da informação.

A Figura 1a ilustra os três princípios básicos de segurança da informação, designadamente a confidencialidade, integridade e disponibilidade.



// F-1 . Princípios de segurança da Informação - Adaptado de Cryptography and Network Security: Principles and Practice (7th Edition); William Stallings; Editor: Pearson.

O princípio da confidencialidade garante que o acesso à informação é limitado apenas a quem tenha autorização prévia. A integridade consiste em garantir que a informação mantém as características iniciais após o acesso e manuseio pelos utilizadores. Por fim, o princípio da disponibilidade consiste em garantir que a informação está disponível para os utilizadores autorizados. A esta tríade são frequentemente adicionados mais dois princípios (Figura 1.b), designadamente a autenticidade e o registo *(accountability)*, que se referem respetivamente à garantia de incorruptibilidade dos dados desde a sua criação e à capacidade de registo e controlo da atividade dos utilizadores no acesso aos dados.

O CICLO DE VIDA DOS DADOS E AS ESTRATÉGIAS DE SEGURANÇA

Em cada momento, os dados poderão estar numa das fases do seu ciclo de vida, ilustrado na Figura 2. Para cada um desses estados é possível identificar ameaças e vulnerabilidades, bem como um conjunto de correspondentes medidas de proteção que poderão ser aplicadas.

// F-2 . ciclo de vida dos dados.

Os dados são **criados** através do sistema de informação (por exemplo, a inserção de um novo cliente na base de dados) ou pela recolha através de uma fonte específica (por exemplo, a leitura através de um sensor). É fundamental identificar a localização onde os dados são criados, que funções poderão ser realizadas (por exemplo, apenas leitura ou leitura e escrita) e quem lhes poderá aceder. A classificação correta dos conteúdos, de acordo com o nível de sensibilidade e o valor para a empresa, é fundamental, já que permitirá definir controlos de segurança fortes e eficazes e, consequentemente, mitigar situações de acesso indevido.

O **armazenamento** dos dados ocorre imediatamente após a fase de criação e pode ser realizado de múltiplas formas, como seja num disco do servidor ou num repositório na *cloud*. Nesta fase os dados deverão ser protegidos de acordo com a sua classificação, nomeadamente através da utilização de mecanismos de encriptação, de políticas de acesso e de estratégias de monitorização e de *backups*. O uso ineficiente de listas de controlo de acessos (ACL – Access Control List), a inexistência de mecanismos de *scanning* de vírus aos ficheiros ou a sua incorreta classificação de acordo com o grau de sensibilidade, poderão potenciar o ataque externo aos dados armazenados. Reforça-se o papel dos *backups*, não apenas na fase de armazenamento, mas também no arquivamento. Numa situação de exfiltração de dados, erro humano, ou ainda após um ciberataque, a existência de uma política de *backups (online e offsite)* bem delineada e que contemple todos os dados armazenados e/ou arquivados, tendo em conta o seu valor para a organização, minimizará os riscos de perda permanente e de *downtime* do sistema de informação e do negócio.

A **utilização** dos dados corresponde a todas as atividades relacionadas com a sua visualização, processamento e tratamento. Os dados podem igualmente ser **transferidos** ou partilhados, ficando assim disponíveis para outros utilizadores que poderão estar fisicamente distantes. A utilização dos dados acarreta alguns riscos, como o processamento em estações de trabalho inseguras e eventualmente de forma não encriptada. Quanto aos dados em trânsito, deverão negar-se acessos não autorizados através da rede, recorrendo entre outros mecanismos, a estratégias de monitorização constante dos ficheiros e dos serviços de rede, a sistemas de deteção e prevenção de intrusões e à instalação de *firewalls*.

Ao longo do tempo, a necessidade da utilização regular de alguns dados torna-se reduzida. Neste caso, há lugar ao **arquivamento** a longo prazo, normalmente em suporte magnético, tendo em conta que poderá haver imposições legais que impliquem a sua consulta num horizonte temporal alargado. A fase de arquivamento constitui desafios ao nível da necessidade de recuperação. Ou seja, quando os dados são arquivados a longo prazo, é necessário ter em conta que poderá haver necessidade de os repor, seja por questões de ordem jurídico-legal, por destruição acidental ou ainda pela necessidade de realizar uma análise digital forense. Em qualquer das situações é necessário assegurar que a empresa detém os meios tecnológicos adequados para efetuar essa recuperação, caso contrário os dados arquivados de pouco servirão. Por exemplo, quando se arquivam dados em suporte de banda magnética num horizonte temporal de dez anos, deverá haver a preocupação de assegurar que existirão equipamentos adequados para realizar uma eventual recuperação.

O ciclo de vida encerra-se com a fase de **destruição**, que pode consistir na destruição lógica dos apontadores para os ficheiros ou na destruição física do suporte em que os dados estão armazenados. Nesta fase deverão sempre respeitar-se os prazos estipulados para os dados arquivados a longo prazo. Na destruição física do suporte (por exemplo, discos ou *pen*), além do respeito pelas normas ambientais e de sustentabilidade, deverá haver o cuidado de evitar a possibilidade de recuperação posterior dos dados através de aplicações específicas para o efeito.

A definição de uma política de segurança da informação é fundamental para proteger os ativos da empresa. A mitigação do acesso ilegítimo e não autorizado aos dados contribui positivamente para a continuidade dos serviços das empresas e para a competitividade dos seus negócios. A auditoria e a validação de controlos de segurança ao longo do ciclo de vida dos dados, usando boas práticas internacionais (por exemplo, a norma ISO 27001:2013), terão um impacto positivo na gestão proativa do sistema de informação e da infraestrutura de rede e de servidores que suportam o negócio da empresa. A formação dos colaboradores em questões relacionadas com a cibersegurança deve igualmente ser encarada como um investimento, já que contribuirá para a proteção de um dos ativos muito valiosos das empresas: os dados.