UNIVERSIDADE da MADEIRA

Faculdade de Ciências Exatas e da Engenharia

Mestrado em Engenharia Informática

Análise de Risco

Segurança em Sistemas de Comunicação/Redes

2022/2023

Resumo

A segurança em bases de dados é um assunto de extrema importância, uma vez que as informações armazenadas podem ser sensíveis ou críticas para as empresas ou organizações. Nesse sentido, os profissionais de segurança devem dedicar-se à implementação de medidas para proteger as bases de dados contra ameaças externas e internas. A segurança em bases de dados é uma tarefa contínua, pois as ameaças e vulnerabilidades estão sempre evoluindo. Portanto, é essencial estar sempre atualizado e estar atento às últimas tendências e práticas recomendadas para garantir a segurança dos dados confidenciais. Este trabalho tem como principal objetivo falar da Análise de Risco em bases de dados, bem como dos métodos de segurança que existem para proteger as mesmas, a avaliação do risco para determinados problemas e das políticas de segurança e ferramentas que podem ser utilizadas.

Índice

Lista de Figuras

Lista de Tabelas

1. Introdução

1.1. O que é a Análise de Risco?

A Análise de Riscos é um passo fundamental na Segurança de Sistemas de Comunicação/Redes. Este passo envolve identificar, avaliar e mitigar as potenciais ameaças e os pontos de vulnerabilidade numa rede de computadores.

O Risco pode ser definido como a probabilidade de um evento indesejável ocorrer e as possíveis perdas ou danos associados a esse evento. O risco é uma parte inevitável que se encontra associada a qualquer atividade que se possa realizar, por isso, deve-se realizar uma análise de riscos, de modo a reduzir a sua probabilidade de ocorrência, bem como minimizar o seu impacto. No contexto da cibersegurança, o risco é definido como a possibilidade de um ataque cibernético afetar a disponibilidade, integridade ou confidencialidade de dados, sistemas ou redes.

1.2. Metodologias de análise de risco

A identificação, avaliação e priorização dos riscos, são etapas que fazem parte da abordagem da análise de riscos na segurança da informação. Esta análise pode ser realizada de duas formas: a **análise quantitativa** e a **análise qualitativa**.

A **análise quantitativa** envolve a utilização de modelos e fórmulas matemáticas e estatísticas para avaliar o risco. Este método utiliza dados quantitativos, como a probabilidade de ocorrência de um ataque e o impacto potencial desse ataque, para avaliar o risco. Por outro lado, a **análise qualitativa** envolve a utilização de julgamentos subjetivos e experiência para avaliar o risco, ou seja, baseia-se em percepções, opiniões e avaliações subjetivas dos profissionais envolvidos na análise do risco. Rege-se muito no conhecimento empírico e na experiência de outros trabalhos que os profissionais já enfrentaram.

Para além da análise quantitativa e qualitativa, a metodologia de análise de risco na segurança de sistemas de comunicação, pode englobar as seguintes técnicas:

- **Identificação dos componentes e ameaças**: A primeira etapa é identificar os componentes das redes, suscetíveis a ataque, como o *hardware*, *software*, dados de utilizadores, e as potenciais ameaças ou ataques como é o caso de *malwares*, *phishing*, ataques de força bruta e ataques *DoS* (*Denial of Service*).
- **Avaliação de riscos**: Uma vez que os componentes e possíveis ameaças da rede estão identificados, é importante avaliar o risco associado a cada ameaça em relação a cada componente do sistema. Esta etapa, pode pressupor a criação de um modelo de ameaça para identificar como é que os atacantes podem tentar penetrar a rede e quais são as maiores vulnerabilidades do sistema de comunicação.

- **Avaliação de vulnerabilidades**: Esta etapa foca-se na identificação dos pontos fracos na segurança da informação, incluindo vulnerabilidades em sistemas, aplicações e processos de negócios.
- **Avaliação do impacto**: Sempre que falamos de risco, devemos ter em conta o impacto que certos eventos podem causar num determinado sistema. Daí ser de extrema importância avaliar o potencial impacto que uma violação de segurança na rede pode gerar, incluindo possíveis danos financeiros, perda de dados de clientes, bem como a interrupção do serviço e danos associados à reputação da marca ou empresa.
- **Mitigação dos riscos**: Com base nas informações obtidas nas etapas anteriores, é importante implementar medidas de mitigação de risco adequadas, de modo a se reduzir o risco geral da rede. A aplicação de *patches* de segurança, a configuração de *firewalls*, a criação de políticas de segurança para os utilizadores e a realização de ações de formação para consciencializar os utilizadores para os perigos associados à utilização e navegação na rede, são algumas medidas que podem ser adotadas com o intuito de mitigar riscos nos sistemas de comunicação.

- **Monitorização contínua**: Finalmente, é de extrema importância realizar uma monitorização contínua na rede para detetar possíveis ameaças e vulnerabilidades que possam vir a aparecer de modo a implementar as medidas necessárias para mitigar os riscos. Esta etapa pode envolver a implementação de ferramentas de monitorização de rede e a realização de testes de penetração, regularmente, para garantir a segurança da rede.

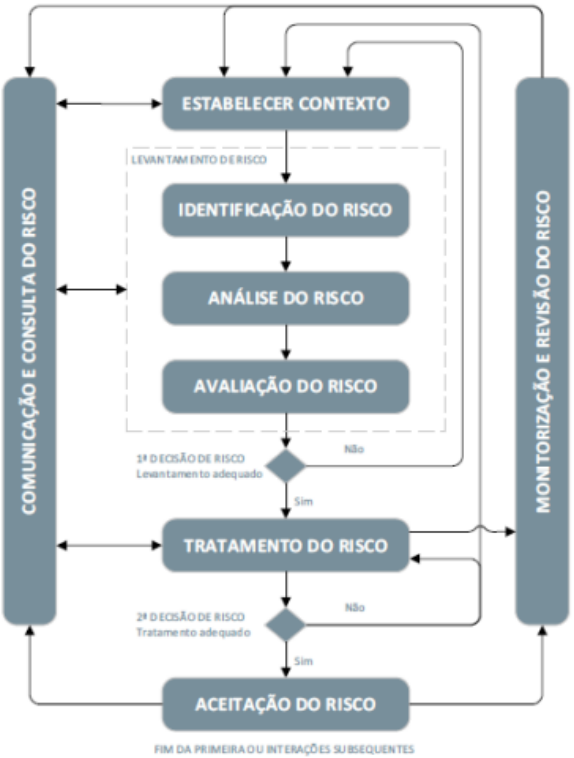

Figura 1: Fluxograma dos processos da Avaliação de Risco

1.3. Análise de Risco em Bases de Dados Empresariais

Como tema principal deste trabalho, decidimos nos focar na Análise de riscos em Bases de Dados Empresariais. Quando falamos em segurança em bases de dados, referimo-nos à proteção daquilo que é mais importante para as empresas no ponto de vista dos clientes, os dados. Os dados são recursos que os clientes, confiam às empresas e que têm um grande valor e por isso são muitas vezes o alvo de muitos ciberataques que acontecem num sistema. Muitos hackers, realizam ataques às bases de dados de empresas de modo a conseguirem obter os dados dos seus clientes para os venderem a outras empresas, de modo que estas depois realizem, por exemplo, campanhas de propagação de anúncios personalizadas.

É importante reconhecer que existem vários tipos de riscos de segurança. A segurança de bases de dados precisa de se proteger contra erros humanos, privilégios excessivos de funcionários, ataques internos, hackers, *malwares* ou até mesmo de danos físicos em servidores de bases de dados. Para se proteger destes perigos e atingir um maior grau de segurança, as organizações/empresas devem adotar múltiplas técnicas de proteção de dados.

Ao longo deste trabalho serão mencionados os diferentes tipos de segurança em Bases de dados, explicado o porquê da importância da segurança nas bases de dados, as melhores práticas de segurança a adotar e soluções e ferramentas a ter em conta de modo a se mitigar os riscos.

2. Porque é que a segurança em Bases de Dados Empresariais é importante

As bases de dados são o grande foco de muitos ciberataques porque armazenam informações valiosas, confidenciais e sensíveis, incluindo dados bancários ou registos de clientes. É importante evitar estes ataques e proteger o **roubo de dados**, que os hackers muitas vezes tentam aceder para utilizar as informações para roubar identidades e fazer compras não autorizadas, por exemplo.

Empresas com problemas de segurança nas bases de dados que comprometem a informação dos clientes podem prejudicar a reputação da organização, resultando num declínio nas vendas e no abandono dos clientes, dando **prejuízo ao negócio e manchando a reputação da empresa**. Estes problemas também podem levar à perda de receitas para uma determinada organização, pois havendo uma fuga de dados, pode resultar numa interrupção das operações comerciais e da geração de receitas, até que os desafios de segurança da base de dados sejam resolvidos.

Muitas vezes, as empresas vêm os custos associados à segurança dos seus dados, como desnecessário e um desperdício. Porém as **violações de dados podem custar milhões de euros para corrigir**, incluindo sanções legais para recuperar dados e restaurar sistemas. As empresas também podem ter de pagar a hackers que exigem um pagamento para restaurar os seus ficheiros e dados bloqueados.

3. Tipos de Segurança em Bases de Dados

A nível da **segurança da rede**, uma das medidas de proteção mais utilizadas são os ***firewalls***. Os *firewalls* são vistos como a primeira linha de defesa contra os ataques maliciosos. Este mecanismo de defesa tem como função restringir o tráfego e pode ser configurado pelas empresas para refletir a sua política de segurança de dados. Ao utilizarmos uma firewall, estamos a aumentar a segurança a nível do sistema operativo, fornecendo um ponto de estrangulamento, onde as medidas de segurança podem estar focadas.

Quanto à **gestão do acesso aos dados**, é necessário também adotar medidas preventivas contra ameaças exteriores. Uma das formas mais comuns de garantir segurança no acesso aos recursos, é através da implementação de um serviço de autenticação. A **autenticação** consiste no processo de verificação da identidade de um utilizador antes de lhe ser concedido o acesso aos recursos. Este processo normalmente é feito por meio de passwords, autenticação de dois fatores ou biometria, que é um método de verificação de identidade baseado nas características físicas ou comportamentais dos utilizadores (por exemplo: impressões digitais ou o reconhecimento facial). Outra medida importante para salvaguardar a segurança dos dados, é definir políticas de **autorização**. Desta forma, é possível definir direitos de acesso específicos a cada utilizador, não dando, por exemplo, demasiados privilégios a utilizadores mais recentes numa dada empresa. Por fim, outra medida de segurança no acesso aos dados que pode ser implementada é o **controlo de acesso físico**, isto é, permitir apenas o acesso físico às instalações onde se encontram as bases de dados, a pessoas devidamente autorizadas. Esta medida de segurança, incide mais sobre a camada física, porém é de igual importância.

Como **proteção contra ameaças,** deve-se realizar frequentemente **auditorias**, de modo a se rastrear as atividades nas bases de dados, ajudando assim a manter a conformidade das normas de segurança. Também permite analisar e investigar atividades históricas para identificar potenciais ameaças ou suspeitas de abuso e violações de segurança.

Já no campo da **proteção de informaçõe**s e daquilo que é mais preciso numa empresa, a **encriptação dos dados** é essencial, de modo a se proteger os dados confidenciais, convertendo-os num formato alternativo para que apenas as partes interessadas consigam decifrá-los de volta à sua forma original e aceder-lhes. Embora a encriptação não proteja os dados de serem acedidos por estranhos, esta aumenta a segurança, limitando a perda de dados quando estes mecanismos de controlo de acesso são violados. Mesmo que um hacker obtenha os dados, este terá de despender um grande esforço para desencriptar e aceder aos dados. Outra medida que deve-se utilizar de modo a proteger os dados é realizar **cópias de segurança dos dados e da base de dados**. É fulcral realizar cópias dos dados e do estado da base de dados em ficheiros e guardá-los em lugares seguros, onde só

possam ser acedidos por meio de autorizações, caso se verifique uma falha de segurança.

4. Avaliação do Risco

A avaliação do risco, como já foi referido, é um passo importante a ter em conta. As empresas atualmente tendem a aceitar cada vez mais projetos, onde a complexidade é cada vez maior e a margem de erro menor.

Como responsável pela gestão de risco, é necessário estar em constante alerta para a ocorrência de eventos adversos durante o desenvolvimento de um projeto. Nem todos os tipos de risco, que podem ocorrer têm de ser tratados, devemos dar prioridade aqueles que constituem maior ameaça ao bom funcionamento do projeto, pois podem ter consequências a nível financeiro e de tempo maior. Para facilitar na decisão de quais são os riscos com maior probabilidade de ocorrência, podemos utilizar a Tabela de Impacto do Risco/Probabilidade, que nos fornece uma *framework* que ajuda na tomada de decisão de quais os riscos que devemos ter em atenção.

4.1. Como utilizar a ferramenta

A tabela do Impacto do Risco/Probabilidade é baseada num princípio, que nos diz que o risco tem duas dimensões primárias:

1. **Probabilidade** – O risco está associado a um evento que pode acontecer. A probabilidade desse mesmo risco ocorrer pode variar entre uma percentagem de 0 até 100. (Nota: Não pode ser exatamente 100% ou 0%, porque se não seria uma certeza e não um risco.)
2. **Impacto**– O risco pela sua natureza, tem um impacto negativo. Porém, o tamanho do impacto pode variar em termos de custos e no impacto que este pode causar na vida humana, saúde e bem-estar ou outro fator crítico.

A tabela permite-nos avaliar o risco, tendo em conta estas duas dimensões. A probabilidade de um risco ocorrer está representada no eixo horizontal e o impacto do risco no eixo vertical, como podemos ver pela **figura 2**, representada em baixo.

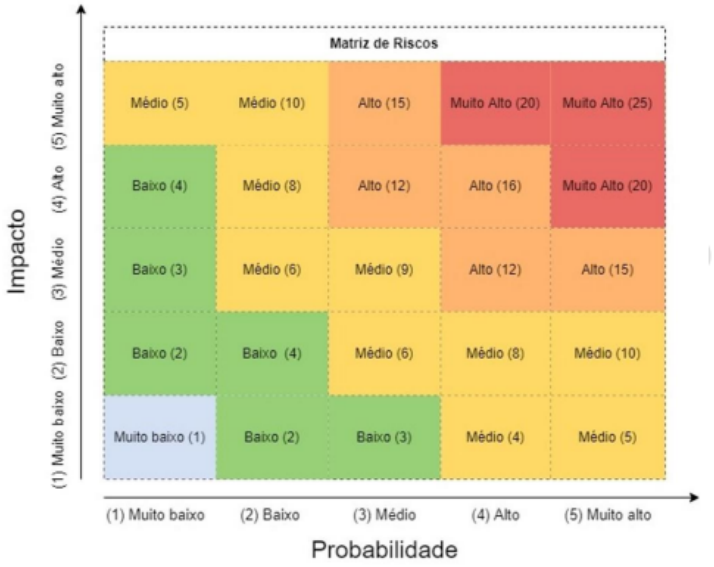

Figura 2: Matriz de Riscos

Os cantos da tabela têm as seguintes caraterísticas:

- **Baixo Impacto/Baixa probabilidade –** Riscos no canto inferior esquerdo são de baixo nível e podem por vezes ser ignorados.
- **Baixo impacto/Alta probabilidade** – Riscos no canto superior esquerdo são de importância moderada – se acontecer, o risco deve ser aceite. No entanto, quando possível, os riscos devem ser reduzidos, ou seja, reduzir a probabilidade de eles ocorrerem.
- **Alto impacto/Baixa probabilidade** – Riscos no canto inferior direito são de importância alta, caso ocorram, mas são de baixa probabilidade de ocorrer. Para estes casos, devem ser adotadas medidas de mitigação para reduzir o seu impacto. Planos de contingências, por vezes, são necessários.
- **Alto impacto/Alta probabilidade** – Riscos no canto superior direito são de extrema importância. Estes são os riscos de probabilidade mais alta e devem ser tratados cuidadosamente, com planos e medidas de mitigação.

4.2. Tratamento dos Dados

Depois de considerar a tabela acima, a exposição a um determinado risco é dada pelo produto do impacto pela probabilidade. Um limite de pontuação deve ser estabelecido pela equipa de análise de risco, onde pontuações mais altas seriam eliminadas, mitigadas ou transferidas para outras entidades, como por exemplo seguradoras. Por outro lado, pontuações mais baixas podem ser ignoradas ou até aceites.

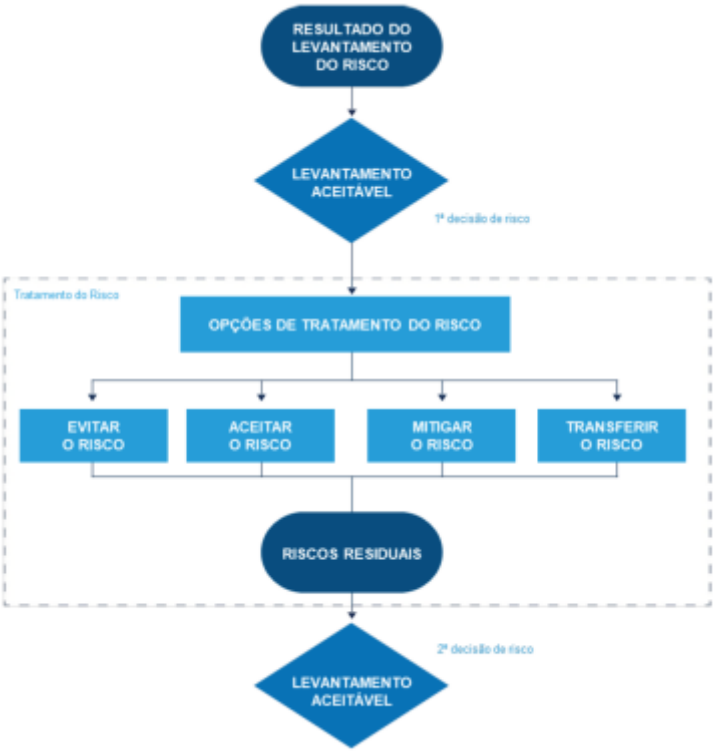

Figura 3: Fluxograma do Tratamento de Risco

5. Ameaças e Vulnerabilidades

Uma ameaça e uma vulnerabilidade não são a mesma coisa. Uma ameaça é uma pessoa ou evento que tem como objetivo impactar um recurso valioso e crítico de uma maneira negativa. Uma vulnerabilidade é a qualidade do tal recurso ou o seu ambiente que permite à ameaça ser viabilizada.

As ameaças e vulnerabilidades para o ativo em questão neste estudo (Bases de Dados Empresariais) será categorizado em Técnicas e Não-Técnicas.

Não-Técnicas:

1. Física: Roubo, adulteração, espionagem, vandalismo, acesso local;
2. Ambiental: Desastres naturais, perda de energia, incêndio;
3. Ameaça interna: Funcionários, prestador de serviços, ou colaboradores;
4. Engenharia social, email e técnicas de fraude utilizando media social.

Técnicas:

1. *Hacking*: Acesso indevido e não autorizado a um dispositivo ou à rede na qual está conectada a Base de Dados, contaminação por *malware*;
2. *Cracking*: Engenharia reversa de software, palavras-chave ou criptografia;
3. Uso indevido: Funcionários ou terceiros a tirar vantagem de recursos fiáveis como por exemplo abuso administrativo, violação de políticas internas e uso de ativos/recursos não-aprovados;

4. Violação de dados: Transmissão física ou eletrônica não autorizada dentro da organização para um destino externo sem permissão;
5. Ataques de disponibilidade: Ciberataques estruturados a fins de extorsão ou danos materiais a ativos.

Um plano de contingência e mitigação de riscos deve ser desenvolvido usando a matriz de riscos (**Figura 2**) como base, associada com todas as ameaças a serem analisadas. Os controlos para redução de cada risco devem considerar uma gama de fatores, tais como:

- Políticas organizacionais;
- Custo-benefício;
- Impacto operacional;
- Viabilidade;
- Leis e regulamentos a nível local e internacional;
- Eficácia geral dos controlos recomendados;
- Segurança e confiabilidade, entre outros.

5.1. Documentação da Avaliação de Risco

Um dos passos finais para desenvolver uma clara e efetiva Avaliação de Risco é documentar todos os resultados envolvidos nas fases anteriores num relatório conciso de forma a apoiar as equipas executivas a tomar decisões apropriadas relacionadas ao orçamento, políticas e procedimentos. Para cada ameaça, o relatório descreve as correspondentes vulnerabilidades, os ativos em risco, o impacto global na organização e infraestrutura, a probabilidade de ocorrência e os controlos de redução recomendados. Este relatório deve estar disponível para todas as partes interessadas como gerentes e executivos de todos os departamentos, *CISO* (*Chief of Information Security Officer*), equipas de TI e pessoas chave envolvidas com a organização.

Ameaça	Vulnerabilidade	Impacto	Probabilidade	Risco	Controlos de redução
Acesso físico não-autorizado Médio	Fechadura da sala de servidores Alto	Alteração de dados Alto	Palavras-chave de login fortes Baixo	Possível perda ou adulteração dos dados Alto	Sistema modernos de Fechadura eletrônica (RFID/NFC)
Perda de energia Médio	Sistemas UPS disponíveis por apenas 8 horas Médio	Indisponibilidade do Base de Dados Crítico	Rede Elétrica Resiliente Baixo	Possível perda ou adulteração dos dados Alto	Solução em tempo real de backup em Cloud ou atualização do sistema UPS
Ataques maliciosos internos Alto	IPS e Firewall estão bem configurados Baixo	Base de dados comprometida (adulterada ou indisponível) Crítico	Ataques não são comuns Médio	Possível litígio devido à violação de dados e custo de indisponibilidade Alto	Equipas de Segurança de Informação dedicadas a monitorizar e usar um sistema de alerta automatizado
Engenharia Social Baixo	Funcionários devidamente educados Médio	Roubo de identidade e acesso à rede interna Alto	Autenticação multifactor Baixo	Inicialização de um ataque malicioso ou espionagem Alto	Educação e treino em Segurança e consciencialização
SQL Injection Alto	Bugs não detetáveis na aplicação Frontend Baixo	Acesso não-autorizado à Base de Dados Crítico	Médio	Violação de dados Alto	Criptografia dos dados
Auditoria fraca e conformidade MuitoBaixo	Segurança de dados em conformidade com uma entidade respeitável Baixo	Interrupção dos negócios até a conformidade ser restabelecida Alto	Baixo	Coimas e investigações de órgãos Reguladores Alto	Registo e arquivo de incidentes e monitorização de políticas

Tabela 1: Análise de Riscos Qualitativa

5.2. Frameworks

Há muitas *Frameworks* notoriamente conhecidas que podem ser usadas tanto para a criação de uma Avaliação de Risco quanto para uma elaboração de políticas de segurança. Como por exemplo:

- *ISO 27000* - Padrões de segurança gerais internacionais;
- *NIST 800* - Resiliência da infraestrutura crítica;
- *eIDAS* - Identidades Digitais;
- *PSD2* - Instrumentos de pagamento;
- *HIPAA* - Sector de Saúde.

Todas têm em comum características e ferramentas relacionadas à implementação de medidas de proteção de dados de forma técnica e organizacional, associadas com obrigações legais a serem seguidas, assim como modelos de relatório como guias. Como as leis e diretrizes acerca da Privacidade podem sempre ser alteradas, o uso de uma *framework* reconhecida traria uma maior segurança jurídica, ajudando assim novos contractos e aquisições.

A organização não necessita de escolher uma *framework* em detrimento de outra, mas sim utilizar uma ou a combinação de várias para se adequar à realidade da instituição como um guia geral. Em alternativa, uma empresa pode escolher criar a sua própria *framework* sempre observando as legislações vigentes a nível Nacional e de outros países nos quais a empresa mantém relações comerciais.

6. Políticas de Segurança

6.1. RGPD – Responsabilidades e penalidades

O Regulamento Geral da Proteção de Dados na União Europeia, também conhecido como RGPD, é o principal documento legal de proteção na União Europeia, aplicável a todos os Estados Membros, rejeitando a atual Diretiva de Proteção dos Dados 95/46/EC. Atualmente, as empresas na União Europeia têm de lidar com 28 leis diferentes de proteção dos dados. Esta fragmentação grande, constitui um grande entrave administrativo, que impede muitas empresas, especialmente pequenas e médias empresas, de aceder a novos mercados.

Uma das principais obrigações para todas as empresas, incluindo o *SMEs*, responsáveis pelo processamento e controlo dos dados na RGPD, é a segurança dos dados pessoais. Em particular, de acordo com a RGPD, a segurança abrange:

- confidencialidade, integridade e disponibilidade, bem como a resiliência dos sistemas e serviços que processam os dados pessoais;
- a capacidade de restaurar a disponibilidade e acesso aos dados em tempo útil, em caso de incidente;

- um processo para testar e avaliar a eficácia das medidas, técnicas que garantem a segurança no processamento dos dados;

Dados pessoais podem ser definidos como qualquer informação ou contacto pessoal, dados financeiros, profissionais, criminais ou registos de saúde, académicos.

As Políticas de segurança especializadas para uma base de dados empresarial devem levar em conta a proteção da informação sensível, quer seja armazenada, em transmissão ou em uso. As melhores práticas da indústria devem ser adotadas, como controlos de confiabilidade e integridade durante a transmissão. Uma vez armazenada esta informação e acedida, há uma preocupação em não permitir o acesso indevido por outros processos ou outros componentes virtualizados em memória.

Além disso, para evitar a perda, destruição ou danificação dos dados, é importante garantir a segurança do servidor e da base de dados, bem como a segurança da rede e das comunicações. Várias medidas podem ser tomadas a esse respeito, como por exemplo, o uso de antivírus, de programas de deteção de *malwares* e limitadores de acesso à rede nos controladores. A monitorização do tráfego que entra e sai do sistema TI, também é importante (por exemplo: através do uso de *firewalls* e sistemas de deteção IDS e prevenção de IPS intrusos).

Chamada de atenção importante para o facto de alguns setores, além de seguir boa parte das normas e diretrizes do RGPD, são obrigados a seguir as regulações específicas do setor e leis locais. Como por exemplo o setor público, saúde, infraestrutura crítica, segurança Nacional, sistema judiciário e prisional.

O não cumprimento e conformidade ao RGPD, assim como a não notificação em caso de violação de dados às autoridades competentes, pode resultar na detenção dos responsáveis, multas até $20M ou 4% da receita anual global da organização.

O RGPD especifica que no caso de violação de dados, a empresa ou controlador (*DPO - Data Processing Officer*) deve comunicar, se possível, no mais tardar 72 horas após tomar conhecimento da violação, às autoridades competentes. No caso de Portugal, a autoridade responsável é a Comissão Nacional de Proteção de Dados (CNPD) e deve ser informada, sobre os detalhes do incidente através do preenchimento de um formulário disponível online.

A CNPD recomenda que a empresa, assim que constate a violação, torne público a natureza da violação, quais os grupos ou indivíduos afetados, os tipos de dados expostos, as possíveis consequências e medidas a serem tomadas para evitar ou mitigar efeitos adversos que o incidente pode provocar. Um ponto de contacto com a empresa, incluindo responsáveis pela segurança da informação, deve ser aberto e mantido para eventuais dúvidas do público.

Outras políticas administrativas de segurança também devem ser implementadas como: *least privilege*, onde o utilizador somente tem acesso aos recursos que necessita para efectuar a sua função ou tarefa. Pode-se ainda em conjunto, usar

biometria e autenticação multifactor para o reforço na segurança. Funcionários e prestadores de serviço devem perder acesso a qualquer recurso da empresa imediatamente assim que forem afastados da mesma, seja por término de contracto ou demissão voluntária.

6.2. Comunicação e Revisão

A fase "Comunicação do Risco" (**Figura 1**) é uma atividade que tem como objetivo alcançar o consenso sobre como gerir os riscos de segurança da informação e cibersegurança, através da troca e/ou partilha das informações sobre os riscos entre os responsáveis e as outras partes interessadas. Esta comunicação é importante pois os tratamentos igualmente eficazes podem ser mais aceitáveis para algumas partes do que para outras, considerando-se os interesses e objetivos comuns e particulares.

A organização deverá estabelecer um plano de comunicação e consulta do risco para assegurar o compromisso dos responsáveis, internos ou externos, pelos riscos, de acordo com a estrutura do plano de comunicação criado. O plano de comunicação e consulta do risco deve assegurar que todos os *outputs* das práticas da gestão do risco, incluindo decisões de modificação dos mesmos, são comunicados via canais já definidos.

Juntamente com a fase anterior, a "Monitorização e Revisão do Risco" (**Figura 1**) visa verificar a eficácia dos controlos implementados e obter informações adicionais para melhoria do processo. Todos os resultados das fases anteriores devem ser registados para o aperfeiçoamento contínuo e a análise de desempenho dos procedimentos, métodos e ferramentas utilizados.

Novas informações a serem consideradas podem ser consultadas por:

- Pareceres de especialistas de segurança da informação e segurança física;
- Informações dos departamentos legais;
- Informação veiculada através de meios de comunicação;
- Informação comunicada por instituições públicas e/ou outras com relevo para a segurança da organização nacional;
- Catálogo de ameaças comuns de entidades respeitáveis.

Abaixo é possível consultar uma tabela com o resumo dos princípios e regras seguidas pelo RGPD.

Regras e Princípios	RGPD
Minimização de Dados	● Sistemas e serviços devem minimizar a recolha de dados e uso de dados pessoais
Limitação de armazenagem de Dados	● Limitação em retenção de Dados ● Pseudonimização ● Criptografia ● Controlo de Acesso ● Segurança de Servidores e Base de Dados ● Segurança de Redes e comunicações ● Eliminação automática periódica de Dados
Confidencialidade de Dados	● Políticas de Segurança ● Registos de atividades de processamento de Dados ● Segurança física
Análise de riscos e medidas de segurança	● Análise de risco ● Análise de Impacto de proteção de dados ● Implementação de medidas técnicas e organizacionais
Design de proteção de Dados como padrão	● Adoção de requerimentos e procedimentos específicos de segurança desde os estágios iniciais de desenvolvimento ● Procedimentos para integração de proteção de Dados dentro das atividades de processamento ● Tecnologias específicas capazes de promover privacidade e proteção de Dados (*PET - Privacy-Enhancing Technologies*)
Avaliações regulares para se aferir a eficácia das medidas de segurança adotadas	● Registos de medidas de segurança técnicas e organizacionais adotadas ● Testes de vulnerabilidade e *Pentest (Ethical Hacking)*
Notificações, comunicações obrigatórias, e medidas de mitigação no caso de violação dos dados	● Procedimentos apropriados para se estabelecer imediatamente se houver violação e dispersão de dados ● Plano de contingência e resposta a incidentes ● Análise de fluxo de Dados e *logs*
Continuidade de negócios, recuperação de desastres e resiliência	● Plano e medidas tecnológicas para continuidade de negócios ● Procedimentos para recuperação de Dados ● Opção por uma abordagem ciber-resiliente efetiva

	• Plano de recuperação após desastre • Técnicas de *Backup*
Processo de Certificação	• Certificação voluntária entregue por entidades reconhecidas e respeitáveis (Artigo 43 do RGPD) ou por Autoridades supervisionárias competentes

7. Soluções e Ferramentas de Segurança

Existem diversos softwares de segurança em bases de dados disponíveis no mercado que oferecem uma ampla gama de recursos para proteger as informações armazenadas. Como exemplos de softwares temos a *Oracle Database Security*, o *IBM Guardium,* o *Microsoft SQL Server Security*, o *Symantec Data Loss Prevention* e o *McAfee Database Security*, que oferecem recursos de criptografia, controlo de acessos, monitorização de atividades e mecanismos de auditorias e deteção de ameaças para a proteção de bases de dados de várias plataformas, incluindo Oracle, SQL Server e IBM DB2.

Cada software tem as suas vantagens e desvantagens, por isso é importante fazer uma análise detalhada dos recursos de segurança oferecidos por cada um deles e avaliar qual o melhor face às necessidades específicas de uma organização. Além disso, é importante lembrar que os softwares de segurança de bases de dados devem ser usados em conjunto com outras medidas de segurança, como políticas de segurança, formação a utilizadores e monitorização constante, para garantir uma proteção eficaz contra ameaças e vulnerabilidades.

8. Conclusão

Concluindo, os riscos são eventos que podem acontecer em qualquer fase de um projeto e, como tal, é necessário adotar medidas preventivas contínuas de modo a minimizar o seu impacto. Daí a importância dos processos de avaliação de risco de modo a ser possível averiguar e tomar a decisão de quais as melhores medidas a aplicar para mitigar o risco. Existem vários tipos de soluções que se deve adotar de modo a proteger os nossos dados, principalmente quando se trata de um meio empresarial, onde são guardados dados muito preciosos de clientes. Por vezes, as organizações descartam estas tarefas de avaliação e análise do risco, "poupando" assim gastos relacionados com a segurança, mas na verdade os custos associados à recuperação de um sistema, caso este sofra um ataque ao nível da segurança, serão maiores do que aqueles que seriam necessários para proteger os sistemas. Estes acontecimentos vêm cada vez mais realçar a importância da consciencialização das organizações para os perigos e medidas que se devem adotar no campo da segurança, seguindo as políticas de segurança existentes para

as diferentes áreas de negócio. As políticas de segurança dentro de uma empresa devem estar bem constituídas e devem conseguir comunicar com todos os departamentos da organização, de modo que caso aconteça algum problema, este seja comunicado rapidamente às entidades competentes minimizando assim o impacto.

9. Bibliografia

- https://www.linkedin.com/pulse/an%C3%A1lise-de-risco-em-seguran%C3%A7a-da-informa%C3%A7%C3%A3o-e-dario-caraponale/?trk=pulse-article&originalSubdomain=pt
- https://www.di.ubi.pt/~hugomcp/bd2/SegAdmDW.pdf
- https://www.oracle.com/security/database-security/advanced-security/
- https://www.ibm.com/guardium
- https://learn.microsoft.com/en-us/sql/sql-server/?view=sql-server-ver15
- https://blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/
- ENISA - Handbook on Security of Personal Data Processing, 2017, www.enisa.europa.eu
- The common EU approach to personal data and cybersecurity regulation, Mantelero, A., Vaciago, G., Esposito, M., Monte, N. - International Journal of Law and Information Technology, Volume 28, Issue 4, Pages 297-328, https://doi.org/10.1093/ijlit/eaaa021
- Guia para gestão de Riscos em matérias de Segurança da Informação e Cibersegurança, Centro Nacional de Cibersegurança PORTUGAL (CNCS), V 1.0, https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos.pdf
- https://privacyref.com/blog/choosing-a-privacy-framework/
- Portugal Data Protecting Overview, https://www.dataguidance.com/notes/portugal-data-protection-overview
- Cocco, M., et al, Portuguese Implementation of the GDPR, Practical Law Practice Note w-0267267, https://www.vda.pt/xms/files/05_Publicacoes/2020/Livros_e_Artigos/Portuguese_Implementation_of_the_GDPR_MPC_IAB_MLG.pdf