**Universidade Autónoma de Lisboa**

**Gestão da Segurança**

**de Informação**

**Disciplina:** Gestão de Sistemas e Redes

**Curso:** Engenharia Informática

**Discentes:**

Arialdo

Artur

Zubair

Miguel

**Docente:**

Hector

2022/2023

**Índice**

1. Introdução
2. Segurança da Informação
   1. Características da Informação
      1. Confidencialidade
      2. Integridade
      3. Disponibilidade
   2. Análise de risco
   3. Classificação da Informação
3. Plano de Segurança
   1. Conteúdos
   2. Política de Segurança
4. Processo de levantamento de requisitos SecReq
5. Sistemas de Gestão de Segurança da Informação
   1. Conceitos básicos
   2. Requisitos
   3. Importância
   4. Vantanges
6. Conclusão
7. Bibliografia

Segurança da Informação

2.1. Características da Informação

As características da informação são importantes pois são elas que conferem um determinado valor a essa mesma informação. Caso a informação altere alguma das suas características, por qualquer que seja o motivo, o valor da informação é consequentemente alterado também - o que normalmente resulta numa diminuição de valor. Mesmo que os profissionais de segurança da informação e os utilizadores possuam o mesmo entendimento dessas características, cada um destes grupos dá diferentes prioridades a cada uma delas.

Quando se procura garantir a segurança da informação, as principais características que atualmente orientam a análise, planeamento e a implementação da segurança são, segundo os padrões internacionais ISO/IEC 17799:2005, a tríade CIA (*Confidentiality, Integrity, Availability*) - Confidencialidade, Integridade e Disponibilidade

2.1.1. Confidencialidade

Confidencialidade da informação refere-se à qualidade da prevenção de acesso não autorizado à informação. A confidencialidade da informação deve assegurar que apenas os utilizadores ou sistemas que possuem direitos de acesso a um determinado conjunto de informação é que o poderão fazer - este acesso é muitas vezes referido por acesso autorizado, sendo permitido a entidades credenciadas para o efeito.

A proteção da confidencialidade deve garantir que qualquer indivíduo ou sistema sem acesso à informação, não a possa ganhar. Quando esse acesso acontece, estamos perante uma falha do sistema de segurança e pode ser afirmado que houve um comprometimento ou uma falha de confidencialidade. Um exemplo de quebra de confidencialidade são as mediáticas fugas de informação do segredo de justiça.

2.1.2. Integridade

Integridade da informação refere-se à qualidade da informação e se esta se encontra completa e não corrompida. A ameaça à integridade da informação existe em todas as situações em que esteja exposta à modificação não autorizada, corrupção, danificação ou qualquer outra forma de disrupção do seu estado de autenticidade. Pode também ocorrer quando a informação está a ser transmitida ou armazenada.

2.1.3. Disponibilidade

Disponibilidade da informação refere-se à acessibilidade da informação para os utilizadores e sistemas autorizados, sem obstruções ou interferências e no formato requerido. A disponibilidade da informação assegura que o acesso à informação, para utilizadores que foram devidamente verificados como tendo as credenciais adequadas, é concedido sempre que requerido, a qualquer momento e em qualquer lugar - disponibilidade total.

2.2. Análise de Risco

Tendo em conta que não é possível garantir total proteção da informação perante todas as ameaças (conhecidas e não conhecidas), é então imperativo conduzir uma análise de risco da segurança da informação de forma a determinar as vulnerabilidades, ameaças e contramedidas necessárias para serem aplicadas de forma a mitigar o impacto destes riscos para um nível razoável.

Desta forma, a análise de risco é um processo de identificação de ativos, os riscos para esses mesmos ativos, e os procedimentos para mitigar os riscos para esses ativos. As organizações ou os indivíduos necessitam de entender quais os riscos que existem no seu ambiente de ativos de informação e como esses riscos podem ser reduzidos ou mesmo eliminados. A gestão do risco é o processo de implementar e manter as contramedidas que reduzem os efeitos do risco para um nível razoável.

É da análise de risco que a informação que é necessária para a gestão tomar decisões acertada relativas à segurança da informação de uma organização, é obtida. Essa obtenção por esta via, deve-se ao facto da análise de risco identificar os controlos de segurança no local, calcular as suas vulnerabilidades e avaliar o efeito das ameaças, em cada área ou situação de vulnerabilidade. A gestão do risco deve ser um processo em curso, proativo, de modo a estabelecer e manter um nível aceitável de segurança, o processo de gestão de risco monitoriza o risco nas atividade quotidianas e segue os resultados da análise de risco de segurança.

A condução de uma análise de risco segue os seguintes passos:

1. Identificar e estimar o valor dos ativos:

Os primeiros passos na avaliação de risco são identificar e atribuir um valor aos ativos que necessitam ser protegidos. Exemplos de ativos nestas condições podem ser software, hardware, recursos humanos e fontes de informação. A informação poderia ser um ficheiro de clientes ou um processo de produção que seja sensível para a organização, ou ainda, como no caso da justiça, informação sobre um processo em segredo de justiça

1. Identificar ameaças associadas aos ativos:

As ameaças são eventos ou condições que podem ainda não ter ocorrido mas que podem potencialmente ocorrer e que a sua presença provoca um aumento de risco. Depois de identificar os ativos que necessitam de proteção, a ameaça a estes ativos deve ser identificada e examinada para determinar as suas consequências ou impactos. Por exemplo, um ataque por vírus, uma quebra de segurança por um hacker, entre uma enorme multiplicidade de possibilidades

1. Identificar as vulnerabilidades:

As vulnerabilidades são situações ou condições que aumentam a ameaça, o que, por sua vez, aumenta o risco. Assim, as vulnerabilidades que aumentam o risco, devem ser identificadas

1. Determinar as contramedidas necessárias:

Processo de eliminar, ou mitigar a ameaça e assim anular o risco. Determinar as contramedidas para reduzir a ameaça leva a ações como a instalação de firewalls, em redes de computador, na esperança de gerir o risco associado com os acessos indevidos. Um ativo possui uma certa quantidade de risco que lhe é inerente e está associada com a ameaça- A vulnerabilidade apenas torna o risco maior e as contramedidas servem para diminuir o risco. O risco residual é o que é deixado existir, depois das contramedidas serem aplicadas - o risco em boa verdade nunca é totalmente nulo.

Plano de Segurança

Tem como objetivo descrever o processo que a empresa vai seguir para assegurar que as suas medidas de segurança sejam compridas. O plano pode e deve ser visto e revisto pela organização e atualizado conforme as necessidades da mesma assim como com os resultados da gestão de risco.

3.1. Conteúdos

Conteúdos do plano de Segurança deveram sempre conter uma descrição do estado atual relativamente á segurança na organização assim como os planos para melhorias caso sejam necessários. O plano de segurança pode ser definido por especialistas dentro da própria organização ou “outsourced” para consultores externos. Um plano ideal considera os seguintes sete aspetos:

1.Política de segurança;

2.Situação Atual;

3.Requisitos;

4.Controlos Recomendados;

5.” Acountability”;

6.Calendario;

7.Rotina de revisão;

3.1.1 Política de Segurança

A política de segurança é um conjunto de regras e “guide lines” que descrevem como uma organização pretende proteger a sua informação sensível e os seus sistemas de acesso alheio. A política de segurança deve definir o “scope” do plano de segurança as posições e responsabilidades do pessoal e as medidas que serão tomadas para proteger a organização.

Uma Política de Segurança deve conter:

1. **Propósito**: O propósito da política de segurança deve estar claramente descrito de maneira a proteger a confidencialidade, integridade e disponibilidade da informação e dos sistemas da organização.
2. **Âmbito:** O âmbito da política de segurança deve definir que informação e sistemas estão sobre proteção como por exemplo toda a informação eletrónica, redes e sistemas de computadores.
3. **Roles e Responsabilidades:** A política de segurança deve definir as roles e responsabilidades do staff, incluindo quem é responsável por implementar e enforcar a política, assim como quem é responsável por gerir e proteger os sistemas de informação da organização.
4. **Controlo de Acesso:** A política de segurança deve clarificar as medidas que serão tomadas para gerir o controlo de acesso á informação da organização e aos seus sistemas como por exemplo autenticação do usuário, políticas para palavras-passe e listas de controlo de acesso.
5. **Classificação da Informação:** A política de segurança deve definir os diferentes níveis de sensibilidade para a informação da organização como: publica, interna, confidencial ou restrita. E deve também delinear o controlo apropriado para cada nível.
6. **Segurança de Rede:** A política de segurança deve definir as medidas que serão tomadas para proteger as redes da organização como firewall, sistemas para deteção de intrusos e VPNs.
7. **Resposta a Incidentes:** A política de segurança deve conter os procedimentos a seguir no caso de um incidente ou violação de segurança, incluindo como reportar o incidente, como conter o dano e como recuperar de tal acontecimento.
8. **Conformidade:** A política de segurança deve delinear a conformidade da organização com as leis e regulações relevantes a onde pratica as suas atividades.
9. **Rever e Atualizar:** A política de segurança deve descrever o processo para a revisão e atualização da sua própria política de segurança para garantir que esta continua relevante.

3.1.2 Situação Atual

Uma organização deve compreender qual o tipo e mais especificamente quais as vulnerabilidades a que estão expostas. Este conhecimento pode se adquirido através de uma análise de risco ao sistema e ao seu ambiente quer por uma equipa “in house” ou através de contratação de serviços externos.

Após esta análise os resultados permitem á organização descrever o atual estado da mesma no que toca á sua situação de segurança, ou seja, quais os ativos que devem ser protegidos e a quais ameaças e vulnerabilidades estão expostos.

3.1.3 Requisitos (cp)

Os requisites são as restrições relacionadas com os objetivos de segurança. Os  
requisitos de segurança constituem o núcleo da segurança na elaboração de  
qualquer plano de segurança. Ao contrário dos típicos requisitos de sistema ou  
requisitos funcionais, os requisitos de segurança podem ser potencialmente  
reutilizados, num domínio ou contexto semelhante, especialmente se  
especificados como instâncias de modelos reutilizáveis.

Os requisitos de segurança são desenvolvidos para especificar as políticas de  
segurança do sistema e ambas políticas como requisitos devem mapear os riscos  
de segurança já identificados, as ameaças e as vulnerabilidades. Os requisitos  
devem também suportar a implementação de um plano de segurança.

3.1.4 Controlos Recomendados

Após terem sido identificadas as vulnerabilidades nos tópicos anteriores, neste passo o objetivo é mapear os controlos recomendados (descrevem a maneira como a infraestrutura da organização e os seus sistemas podem ser desenvolvidos para corresponder aos requisitos de segurança previamente especificados) com as mesmas.

3.1.5 Acountability (cp)

“Acountability” refere-se á responsabilidade dos indivíduos ou grupos dentro da organização para garantir que a política de segurança é seguida e que os ativos estão protegidos. Pode-se incorporar “acountablity” a um plano de segurança garantindo os seguintes passos:

1. **Atribuir responsabilidades e roles especificas para segurança:** Cada colaborador ou grupo de colaboradores deve ter roles claramente definidas assim como responsabilidades correspondentes a segurança da informação. Isto pode incluir tarefas como manter as palavras-passe seguras, reportar acidentes de segurança e seguir protocolos de segurança relevantes.
2. **Implementar Controlos de Acesso:** Controlos de acesso são mecanismos que restringem o acesso a certos recursos ou sistemas apenas para indivíduos autorizados. Ao restringir o acesso apenas a certos indivíduos ajuda a manter responsabilidade pelas ações feitas a estes sistemas.
3. **Implementar Monitorização e reporte de Segurança:** Monitoramento regular e reporte de acidentes e atividades de segurança podem ajudar a identificar e lidar com potenciais vulnerabilidades de segurança. Isto pode ser feito através do uso de ferramentas de segurança como monitoramento de logs e protocolos de resposta a acidentes.
4. **Estabelecer consequências por incumprimento:** É importante ter consequências claras implementadas para indivíduos ou grupos que falhem com o seguimento das políticas de segurança. Isto pode incluir ação disciplinar , rescisão ou até consequências legais em casos severos ou incumprimento intencional.

Nesta parte deve ser especificado quais as pessoas que são responsáveis por  
implementar os requisitos de segurança. Esta documentação suporta quem tem  
a tarefa de coordenar as responsabilidades individuais em conjunto com os  
especialistas em segurança. Ao mesmo tempo, o plano torna explícito quem é  
(ou pode ser) responsável, se existem requisites que não possam ser cumpridos  
e vulnerabilidades a que não foi dada resposta.

Existem muitos e diversos papéis na organização a considerar, tais como a  
conceção, o desenvolvimento, a utilização e a manutenção do sistema. Tal leva a  
diferentes perfis de recursos humanos envolvidos diretamente no sistema, tais  
como utilizadores finais, gestores de projeto, gestores, administradores de bases  
de dados, administrativos, entre muitos outros. Quando a dimensão da  
organização é relevante (por exemplo mais de 30 colaboradores), deve existir  
uma equipa de planeamento de segurança que realiza uma análise de segurança e  
recomenda um programa de segurança.

3.1.6 Calendário

Para que toda a organização esteja na mesma página e para que a gestão da empresa consiga melhor acompanhar o progresso da implementação do plano o uso de um bem implementado calendário é crucial. O calendário deve ter em conta possíveis atrasos ou dificuldades que as equipas possa vir a encontrar enquanto o implementam o plano e deve conter deadlines que não fujam muito á realidade (nem muito sufocantes nem demasiado folgados) e dando sempre prioridade á implementação do controlo de riscos com maior importância.

3.1.7 Rotina de revisão

Após a realização do plano e sua implementação a fase de revisão torna-se a mais importante em conjunto com a revisão dos requisitos de segurança, pois manter o plano atualizado é crucial para manter o sistema o mais seguro possível. Fatores como a evolução da tecnologia, aparecimento de novas vulnerabilidades e novos tipos de ataques assim com alterações a nível dos requisitos do cliente ou do sistema jurídico forçam que este passo do plano de segurança nunca esteja concluído.

Sistemas de Gestão de Segurança da Informação

**5.1. Conceitos Básicos**

A Segurança da Informação busca garantir a Confidencialidade, a Integridade, a Disponibilidade e a Autenticidade.

* **Confidencialidade** – garantir que a informação seja acessada somente pelos responsáveis diretos, impedindo que seja divulgado para um usuário, entidade ou processo não autorizado.
* **Integridade** – garantir que a informação não seja alterada ou excluída sem a devida autorização.
* **Disponibilidade** – garantir que o acesso aos sistemas, dados e serviços seja realizado somente por usuários ou entidades autorizadas.
* **Autenticidade** – garantir a identidade de quem está enviando a informação.

A Segurança da Informação não diz respeito somente aos sistemas de informação, mas a todo o processo que envolva a pessoas, comunicação, equipamentos de hardware e qualquer outra atividade relacionada ao uso de Tecnologia da Informação pela empresa.

5.2. Requisitos

Os requisitos de segurança são desenvolvidos para especificar as políticas de segurança do sistema e ambas políticas como requisitos devem mapear os riscos de segurança já identificados, as ameaças e as vulnerabilidades. Os requisitos devem também suportar a implementação de um plano de segurança.

Os mecanismos de segurança (tais como identificação de utilizadores, senhas de acesso «passwords», criptografia, firewalls e software antivírus) são então pensados para satisfazer os requisitos de segurança- Alguns destes conceitos, influenciam a engenharia associada com os requisitos de segurança (isto é, políticas, riscos, ameaças e ativos), enquanto outros (isto é, mecanismos de segurança, vulnerabilidades e ataques) são influenciados pelos requisitos de segurança.

A figura 3, apresenta os relacionamentos entre alguns dos conceito mais relevantes, descritos no âmbito da segurança da informação. Com base na figura, é possível considerar que a base são os ativos. Os ativos podem ser um ou mais e de três tipos diferentes: humanos (pessoas); propriedade (coisas) e serviços (operações). Nos ativos que se constituem por coisas, designadas coletivamente como propriedade, podem ser de quatro tipos diferentes: dados, hardware, software e infraestruturas.

A existência de mecanismos de segurança, por sua vez, permitem reduzir as vulnerabilidades e suportam os requisitos de segurança. São os requisitos de segurança que especificam as políticas de segurança, que por sua vez, estabelecem os objetivos de segurança

– a Figura 3 resume todas estas relações, de um modo gráfico, mostrando também os termos em língua Inglesa.

Diagram

Description automatically generated

5.3. Importância

A **Segurança da Informação**, a cada dia, passou a ter grande importância para as empresas que utilizam Tecnologia da Informação nos seus processos diários de tomada de decisão.

Segurança da Informação é muito mais que ter um *software* antivírus instalado ou utilizar um *firewall* que impeça o ataque de agentes indevidos a sua rede corporativa. Segurança da Informação está relacionada a proteção de dados, a segurança física, a segurança ambiental, o alinhamento da Tecnologia da Informação com os objetivos e a missão da empresa, dentre outras funções essenciais para a continuidade dos negócios.

A informação é o bem mais precioso para uma empresa/indivíduo, sendo a principal fonte para as tomadas de decisão. Qualquer conteúdo que seja gerado pela empresa por meio de suas operações diárias, seja pelas transações de compra e venda, os registros de atividades dos funcionários ou qualquer outro conteúdo que necessite ser armazenamento.

Nos dias atuais, a informação passou a ser gerada na maioria das transações por meios digitais. Dessa forma, a segurança da informação existe para determinar o que pode ser afetado caso ocorram problemas relacionados a perda de acesso, o roubo de dados, a indisponibilidade de serviços, dentre outros eventos que podem interferir o funcionamento correto das atividades da empresa.

5.4. Vantagens

Benefícios que a segurança da informação promove

* identificação e solução de possíveis ameaças;
* proteção de dados referentes aos colaboradores;
* preservação e consolidação de parcerias com outras empresas;
* garantia do sigilo de informações internas;
* proteção das informações pessoais de clientes e fornecedores;
* destaque no mercado como uma instituição segura e confiável.