LAUREATE BRASIL

# AUDITORIA DE SISTEMAS

## UNIDADE 3 – POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

**Autor:**
Leandro Santos da Cruz
**Revisor:**
Jaime Gross Garcia

INTRODUÇÃO 01
3.1 POLÍTICA DE SEGURANÇA E ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO 02
3.2 DIREITOS E DEVERES DOS USUÁRIOS 05
3.3 SEGURANÇA ORGANIZACIONAL 09
3.4 MELHORES PRÁTICAS E PROCESSOS FAVORÁVEIS À SEGURANÇA DA INFORMAÇÃO DE SISTEMAS 12
SÍNTESE 16
REFERÊNCIAS BIBLIOGRÁFICAS 17

## Introdução

Caro(a) estudante,

Para proteger sistemas de informação dos altos níveis de ameaças cibernéticas que vêm crescendo atualmente, as organizações passaram a ter por obrigação inserir controles de segurança eficazes. Podemos afirmar que a política de segurança da informação é fundamental para controlar, organizar e garantir a eficiência da segurança, mas também a organização da informação em um ambiente organizacional.

A política de segurança da informação é, na sua essência, um manual de orientação e ajuda a traçar os limites da gestão da segurança da informação. Além do mais, indica o compromisso da gestão como apoio à segurança da informação e define o papel que se deve desempenhar para alcançar e apoiar a visão e a missão da organização. O fator humano é fundamental para sua gestão e controle. Assim, os usuários devem ser conscientizados e treinados para entender os procedimentos necessários para manter a segurança no ambiente organizacional.

Considerando esses fatos, nesta unidade, conheceremos os conceitos básicos de políticas de segurança e

organização da informação e melhores práticas de auxílio à segurança da informação, detalhando seus processos e métodos de implementação e manutenção nas organizações.

Bons estudos!

## 3.1 Política de segurança e organização da segurança da informação

Existem diversos tipos de controles e medidas que podem e precisam ser implementados em uma organização para garantir o funcionamento eficaz da segurança e gestão da informação. A maioria desses controles e medidas alternam-se entre regulamentos contratuais e soluções técnicas para conscientização das ameaças, riscos e vulnerabilidades. Seguramente, o controle mais importante atualmente é a política de segurança da informação.

De maneira simplificada, a política de segurança da informação é, na verdade, um conjunto hierárquico de documentos organizados, que cobrem todos os aspectos da segurança da informação no mais alto nível de gerenciamento. A segurança da informação possui quatro princípios básicos: disponibilidade, integridade, confidencialidade e autenticidade.


Figura 1 – A tríade em Segurança da Informação: atributos importantes.
Fonte: Elaborado pelo autor, 2020.

Segundo o princípio da disponibilidade, a informação deve estar sempre disponível. Já segundo a integridade, a informação só pode ser alterada por pessoas autorizadas, ou seja, é a garantia do controle das alterações. Segundo o princípio da confidencialidade, a informação deve ser acessada apenas por usuários liberados, segundo um bom controle de acesso documentado na política. Por fim o princípio da autenticidade garante a genuinidade de autoria da informação, contudo, este princípio não traz a garantia da veracidade do conteúdo dos dados.

E o não repúdio, o que quer dizer? A partir do momento que a informação se torna eletrônica, ela pode facilmente ser alterada ou modificada. Para evitar esse tipo de modificação é necessário um tipo de sistema no

qual as partes confiem nos dados que são compartilhados e utilizados nas transações diárias. Essa exigência para a confiança é conhecida como não repúdio.

Podemos destacar que o não repúdio pode vir a ser de muita importância no e-commerce, pois pode ser utilizado como forma de prevenção para que as partes integrantes de uma transação venham a contestar ou negar uma transação qualquer após sua realização. Em linhas gerais, um dos objetivos de um sistema de não repúdio é provar quem foi o autor de determinada ação e manter as evidências para utilizá-las em possíveis disputas ou auditorias.

A política de segurança da informação é desenvolvida para explicar e demonstrar a importância e valorização da cultura de segurança da informação e seus conceitos, do básico ao avançado, para todos os usuários que utilizam os recursos de informação de uma organização. Deve acrescentar os objetivos dos negócios da organização e refletir a vontade da alta gestão de operar a organização de maneira controlada e segura com seus ativos de tecnologia da informação.

Higgins (1999) argumenta que a “política de segurança da informação é o início do gerenciamento de segurança”. Podemos também adicionar o alerta de que o plano estratégico de sistemas de informação é um pré-requisito crítico para a formulação de políticas, uma vez que define o contexto de negócios no qual a segurança da informação será gerenciada e, com isso, os objetivos e as prioridades da gestão de segurança.

De forma simplificada, os princípios de segurança da informação descrevem as medidas gerais relacionadas à segurança da informação dentro de uma organização. Esses princípios buscam de forma lúdica demonstrar aos usuários qual é o comportamento adequado e inadequado em relação aos diversos tópicos e conceitos de segurança da informação.

De acordo com Hintzbergen et al (2018) uma política de segurança da informação deve ser escrita em conformidade com os requisitos do negócio e respeitando as leis e regulamentos relevantes.

Geralmente documentos como, por exemplo, políticas, possuem uma estrutura hierárquica. Muitos destes documentos são elaborados com base em alguma política corporativa de alto nível, obedecendo sempre ao padrão da política geral da organização, como afirma Hintzbergen et al. (2018).

### A evolução da Segurança da Informação

| | |
|---|---|
| **DÉCADA DE 1920** | **Criptografia**: Os alemães a aperfeiçoaram, chamando-a de “Enigma G”, ou “A máquina M”, que tinha o intuito de codificar e decodificar mensagens. |
| **DÉCADA DE 1960** | **Internet**: É criada a Arpanet, com a finalidade de interligar centros de computação militares e acadêmicos; pode ser considerada a mãe da internet. |

| | |
|---|---|
| **DÉCADA DE 1980** | **Computadores Pessoais**: Começa a onda de popularização dos computadores pessoais e aparece o primeiro programa com características de vírus que se tem notícia, o Elk Cloner, que foi criado por um garoto de 15 anos. |
| **DÉCADA DE 1990** | **Antivirus**: Surgem os primeiros antivírus. O Windows 95 é lançado com a promessa de um sistema seguro. |
| **DÉCADA DE 2010** | **Big data, mídias sociais, BYOD, cloud computing, Internet das Coisas**: A TI vive momentos de instabilidade com o crescimento de tecnologias emergentes e a conscientização dos usuários. |

A política de Segurança da Informação inclui uma ampla série de parâmetros de segurança, contudo, nem todas as partes da política necessitam da atenção de todos os usuários. Por exemplo, os funcionários da limpeza não precisam conhecer arduamente a seção da política relacionada à segurança de sistemas ERP. Portanto, recomenda-se que a política de segurança seja dividida em várias partes, conforme descrito a seguir.

A partir de uma análise de cargos bem elaborada e da política de segurança da informação ser aprovada pela alta gestão, podem ser elaborados os seguintes tipos de documentos base:

- **Regulamentos**. Um regulamento é um detalhamento de uma política. Seu não cumprimento pode gerar medidas disciplinares aos usuários;
- **Diretrizes**. Estas auxiliam na orientação de atividades especificas, descrevendo de forma lúdica quais aspectos e medidas devem ser seguidos;
- **Procedimentos**. É a descrição em detalhes de cada orientação descrita em uma política, instruções de trabalho, formulários, ou até mesmo orientação de como realizar determinada atividade específica.

A norma ABNT NBR ISO/IEC 27001 é a norma internacional de gestão de segurança da informação. Ela descreve a estrutura de um Sistema de Gestão de Segurança da Informação SGSI. A norma especifica os requisitos para estabelecer, implementar, manter e melhorar, de forma contínua, um sistema de gestão da segurança da informação dentro do contexto da organização. A norma também inclui requisitos para a avaliação e tratamento de riscos de Segurança da Informação voltados para as necessidades da organização (ABNT, 2013).

Um SGSI é descrito pela norma ABNT NBR ISO/IEC 27001 como um sistema com base em uma abordagem de risco do negócio, para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a Segurança da Informação.

Existem outras normas especificas para situações de risco em um ambiente organizacional para controle da Segurança da Informação, como a norma ABNT NBR ISO/IEC 27002, que utiliza como código de prática os controles de segurança da informação, focados em um SGSI. Já a ABNT NBR ISO/IEC 27005, aborda as questões de análise e gerenciamento de riscos de Segurança da Informação.

Os requisitos de estabelecimento de um SGSI de acordo com a Norma ABNT NBR ISO/IEC 27001 são:

- Definição do escopo do SGSI (os quais processos organizacionais, departamentos e partes interessadas se aplicam);
- A Política do SGSI (que inclui objetivo, diretrizes, alinhamento ao negócio, critérios de avaliação de riscos, dentre outros aspectos);
- Abordagem de gestão (a metodologia da organização utilizada para identificação, análise, avaliação e tratamento de riscos);
- Objetivos de controle e controles selecionados (a empresa deve declarar quais medidas foram selecionadas para tratar a segurança da informação);
- Declaração de aplicabilidade (com os objetivos de controle selecionados).

Agora que sintetizamos o que é uma política de Segurança da Informação, podemos concluir que a política de Segurança é uma ferramenta dinâmica e em constante processo de revisão. Ela muda de forma consideravelmente contínua, conforme as informações e outros recursos que a organização utiliza.

## VOCÊ QUER LER?

A ABNT NBR ISO/IEC 27005 foi desenvolvida para auxiliar a gestão de riscos da Segurança da Informação. A sua mais recente versão foi lançada em 2018. Assim como a ISO/IEC 9001, esta norma funciona como suporte à principal norma do seu grupo, no caso, a ABNT NBR ISO/IEC 27001. A ABNT NBR ISO/IEC 27005 auxilia a organização em técnicas de melhoria contínua, implementação e monitoramento do sistema de gestão. Para quem busca mais informações sobre a gestão e controle de riscos de Segurança da Informação, vale a leitura.

## 3.2 Direitos e deveres dos usuários

Os usuários possuem um papel importantíssimo no desempenho da Segurança da Informação dentro das organizações, por seu comportamento e sua consciência de segurança, que podem causar tanto grandes prejuízos como total segurança para a organização, caso adotem de forma segura as políticas da empresa.

Assim, a função dos usuários é uma das partes mais importantes para o gerenciamento da Segurança da Informação. Não ter conhecimento de seu escopo de trabalho de forma detalhada ou até mesmo não possuir conhecimento nos sistemas e recursos de TI coloca em risco a Segurança da Informação e o desconhecimento de técnicas de proteção é afetado de forma grandiosa.

A melhor arma para combater a engenharia social é a informação. Se os colaboradores de uma empresa não estiverem bem treinados e bem informados a respeito dos golpes envolvendo engenharia social, de nada adiantará os demais investimentos em meios tecnológicos voltados para segurança. O engenheiro social é alguém que usa a fraude, a influência e a persuasão contra as empresas em geral, visando suas informações (MITNICK, 2003).

Uma política de segurança da informação bem documentada e aprovada pela alta gestão leva aos usuários a responsabilidade de possuir um papel ativo no trabalho de Segurança da Informação, o que contribui para evitar possíveis incidentes indesejados, vulnerabilidade de sistemas e ataques, proteger os ativos da organização e entender como reagir da forma correta baseada na política de Segurança da Informação a Incidentes.

A percepção de um usuário a respeito da segurança da informação pode ser desenvolvida por fatores organizacionais, tecnológicos e individuais conectados. Podemos afirmar, assim, que as normas sociais e as interações no local de trabalho influenciam a compreensão individual relacionada à segurança da informação.

A qualidade de uma política de Segurança da Informação pode ser um fator preponderante para influenciar negativamente ou positivamente na consciência, motivação e comportamento dos usuários em relação à Segurança da Informação. Com isso, podemos afirmar que o papel dos usuários na Segurança da Informação é importantíssimo, contudo, é necessário um treinamento prévio com estes usuários em relação às políticas implantadas dentro da organização.

Geralmente os usuários são o elo mais fraco da cadeia de riscos, porque, em alguns casos, ele é o único obstáculo para prevenção de riscos e vulnerabilidades, evitando ou concretizando ataques como os de engenharia social. Por isso, um de seus deveres é contribuir com ações de boas práticas de Segurança da Informação, como, por exemplo, o uso cauteloso de e-mails.

Com diversos tipos de deveres e direitos que os usuários possuem, deixar de cumprir com essas orientações da política de Segurança da Informação ou com os procedimentos e diretrizes internas do departamento de tecnologia, apenas por negligência, pode causar enormes prejuízos financeiros, de imagem e físicos à organização.

Uma forma eficaz para diminuir esses tipos de ações são as campanhas de conscientização junto aos colaboradores. Essas campanhas podem ajudar a elucidar a atenção, redobrar os cuidados e manter sempre alerta o sinal para as ameaças que podem afetar os sistemas da organização. Pode-se citar como exemplo de ameaças e-mails, sites que podem provocar a proliferação de *malwares*, *trojans*, entre outras ameaças à rede.

É importante que antigos conceitos de trabalho, práticas e formas de pensar e atuar sejam revistas e até reinventadas, para que todos estejam cientes dos riscos e sobre como proteger as informações organizacionais.

A forma adequada para preservar a Segurança da Informação, nesses casos, é criar um tipo de contrato de confidencialidade com todos os colaboradores que utilizam e acessam informações secretas das organizações.

## VOCÊ SABIA?

Em empresas multinacionais que atuam em todo o globo e em outras empresas que adotaram o regime atual de home office durante a pandemia do novo Coronavírus, as equipes não estão mais localizadas no mesmo espaço. A diminuição na interação pessoal combinada com uma infinidade de ferramentas usadas para comunicação (e-mail, Zoom, Skype, Meeting, LinkedIn, entre outros) desenvolveu novos métodos de ataques de engenharia social.

Podemos concluir que os usuários são o elo principal no que se refere à gestão e controle da Segurança da Informação. É necessário ter o apoio constante dos funcionários, mas, para isso, a organização necessita prover recursos para que cada funcionário obtenha conhecimento de seus direitos e deveres junto a Segurança das Informações organizacionais.

**Principais ataques de engenharia social**

### *BAITING*

Um dispositivo infectado com malware, como um pen-drive ou um CD, com o propósito de despertar a curiosidade do indivíduo, para que insira o dispositivo em uma máquina a fim de checar seu conteúdo.

### *PHISHING*

Os usuários geralmente são coagidos a instalar um malware em seus dispositivos ou a compartilhar informações pessoais, financeiras ou de negócio.

### *PRETEXTING*

Falsas circunstâncias são geradas para coagir a vítima a oferecer acesso a informações e sistemas críticos.

## *QUID PRO QUO*

Um atacante requer informações privadas de alguém em troca de algo. “Oferece algo à vítima em troca de informações sensíveis”.

# Teste seus conhecimentos

## Identificação de tipos de ameaças à segurança da informação.

As ameaças intencionais são provocadas por invasões, fraudes e roubo de informações. As ameaças involuntárias são causadas por erros de desconhecimento no uso do ativo, onde aparecem erros inconscientes de funcionários que não foram devidamente treinados, infecções por vírus ou até mesmo os acessos indevidos. As ameaças exploram os pontos fracos, afetando assim a segurança da informação.

Considerando essas informações, assinale a alternativa que descreve o tipo de ataque que utiliza métodos de ilusão ou exploração da confiança das pessoas para obter acesso a informações importantes e sigilosas em organizações e sistemas.

**a** *Ransomware*.

**b** Engenharia Social.

**c** Ataque de Persuasão.

**d** *Backdoor*.

**e** DDoS.

Gabarito na página 19.
Atividade não pontuada

## 3.3 Segurança organizacional

Atualmente, as organizações dependem cada vez mais de sistemas computacionais, que armazenam informações importantes, mas acabam se tornando uma fonte de muitos riscos a organização. Consequentemente, aumentou a importância do gerenciamento de riscos à informação dentro das organizações.

A combinação de tecnologias sociais, como computação em nuvem, tecnologia de análise de dados e dispositivos móveis foram desenvolvidas para promover a permanente conectividade, gerando mobilidade e informação em tempo real. Nesse sentido, as metodologias de gestão da Segurança da Informação foram ganhando uma nova dinâmica de alinhamento de forma constante, proporcionando bloqueios de novos métodos de ataques à segurança nas bases de dados das organizações.

Todos esses fatores implicam e impactam de forma direta na cultura organizacional, que necessita de uma adequação em relação à transformação digital atual, modernizando os seus processos internos, sem descuidar da segurança. Para que isso ocorra, conceitos, práticas e formas de pensar arcaicas necessitam serem revistas e até reinventadas, uma vez que a falta de conformidade com as políticas de Segurança da Informação organizacional é um problema generalizado que cada vez mais acarreta custos diretos e qualitativos muito elevados.

Diversos artigos de segurança corporativa apontam que a segurança é principalmente uma questão de gerenciamento, em vez de tecnologia, porque a tecnologia é uma parte da segurança, mas sem uma mudança profunda na cultura de segurança da organização, a compra de produtos de segurança será pouco efetiva (POSTHUMUS, 2004).

Quando a tecnologia possui um impacto significativo nas atividades da organização, podemos afirmar que o departamento de TI é estratégico e direcionado para o negócio de origem. Neste caso, é necessário possuir um claro direcionamento do que esperar dos objetivos e ações da Segurança da Informação. De acordo com o COBIT 5 da ISACA (2012), a governança projeta o atendimento às atuais necessidades dos dirigentes de negócio alinhado aos atuais pensamentos de gestão e governança em TI. Ela, entretanto, é de responsabilidade de toda organização e não só da TI.

**Diagrama 2 – Fatores motivadores da Governança em TI**


Fonte: FERNANDES; ABREU, 2014. (Adaptado).

Segundo Fontes (2008), a governança é a gestão da gestão, sendo necessário que exista o básico da gestão da Segurança da Informação. Muitas organizações não possuem essa gestão básica e adotam a governança de tecnologia da informação. Para a gestão de segurança existir, Fontes (2008) propõe que alguns requisitos sejam implementados. O primeiro deles é a existência de uma pessoa responsável pelo processo de segurança da informação, não sendo essa pessoa responsável pela segurança, mas pelo processo de segurança, o que terá como consequência a implementação de uma boa política de Segurança da Informação.

A governança de TI está ligada diretamente à gestão da tecnologia da informação. O Quadro a seguir apresenta a diferença existente entre os cois conceitos.

**Quadro 1 – Diferença entre gestão e governança de TI**

| GOVERNANÇA DE TI | GESTÃO DE TI |
|---|---|
| Direciona os processos de TI | Mantém o desempenho de serviços |
| Monitora o cumprimento das regras estabelecidas | Promove a transformação digital |
| | Mantém a satisfação dos usuários e clientes dos serviços |
| | Faz gestão de equipes |

Fonte: CORREA, 2018.

A Segurança da Informação das organizações tornou-se um elemento crítico na prevenção de danos causados por ameaças, como intrusões ou vazamentos de dados não intencionais, assim, existem diversos desafios para as organizações manterem as informações seguras. Werlinger, Hawkey e Beznosov (2009) apresentam três dimensões que influenciam a Segurança da Informação – fatores humanos, fatores organizacionais ou fatores tecnológicos. Exemplos de fatores de base humana que se tornam desafios para as organizações são a falta de treinamento ou experiência, ou problemas de segurança de comunicação como citado anteriormente.

## VOCÊ SABIA?

A governança de TI é uma base sólida para manter a segurança organizacional atualmente. A partir disso, a utilização de *frameworks* tornou-se um método muito utilizado. Os *frameworks* nada mais fazem que orientar os líderes para obter boas estratégias e aperfeiçoar recursos, evitar falhas e reduzir riscos. Ficou curioso e quer saber um pouco mais sobre o tema? Então pesquise sobre *frameworks* de governança de TI.

Os desafios relacionados a fatores organizacionais são, por exemplo, estimativa incorreta de risco, falta de orçamento, distribuição incorreta de responsabilidades de TI ou controle de acesso fraco a dados confidenciais. Já exemplos de desafios tecnológicos são a complexidade dos sistemas, as vulnerabilidades dos sistemas ou aplicativos, mobilidade e acesso distribuído ou falta de ferramentas de segurança eficazes (WERLINGER; HAWKEY; BEZNOSOV 2009).

**A evolução da tecnologia da informação nas organizações**

| | |
|---|---|
| **DÉCADA DE 1960** | **Processamento de dados**: A partir de 1960 os computadores começaram a ser importantes para as organizações, mas na época eram muito limitados em relação às aplicações e incompatíveis entre eles. |
| **DÉCADA DE 1970** | **A Era dos sistemas de informações**: Durante o ano de 1970 as evoluções tecnológicas começaram a abrir novas opções para a transformação de dados em informações e ao melhoramento e adequação dos sistemas de acordo com as necessidades de cada empresa. |
| **DÉCADA DE 1980** | **A Era da inovação e vantagem competitiva**: A partir de ano de 1980, diversas mudanças tecnológicas, principalmente em tecnologias de escritório e microcomputadores, e o termo “Tecnologia da Informação” passou a ser utilizado com mais frequência. |

**DÉCADA DE 1990**

**Integração e reestruturação do negócio**: Essa integração tecnológica facilitou a troca e o acesso às informações de forma otimizada melhorando o funcionamento das organizações.

Todos esses desafios podem ser controlados quando decisões corretas são tomadas, o que pode eliminá-los ou atenuar os efeitos dessas ameaças. Hunker e Probst (2011) identificam diversas abordagens para enfrentar as ameaças internas dentro da organização, analisando os fatores técnicos, sociotécnicos, sociológicos e psicológicos. Os autores também abordam vários desafios, como controles de acesso, políticas de segurança da empresa e motivação dos atores internos da organização. Portanto, é relevante entender como esses padrões são aplicados ao contexto móvel, uma vez que a família ISO 27000 e, principalmente, a ABNT NBR ISO/IEC 27001 têm sido cada vez mais consideradas um padrão internacional para lidar com Segurança da Informação nas organizações Disterer (2013).

## 3.4 Melhores práticas e processos favoráveis à segurança da informação de sistemas

As boas práticas de segurança podem ser do básico ao avançado, a depender do método escolhido pela gestão de tecnologia da organização. Algumas são tradicionais e conhecidas por boa parte das pessoas e outras somente pelos especialistas da área. A proteção e a segurança das informações organizacionais atualmente representam um desafio de gerenciamento, devido a ameaças e ataques sofisticados à segurança.

A importância das boas práticas de gestão na proteção das fontes de informações organizacionais é primordial quando se fala em proteção dos dados, dessa maneira, os padrões internacionais de segurança como as normas da série ISO 27000 foram desenvolvidas para auxiliar as organizações a implementar uma gestão atuante de segurança da informação. Contudo, ainda restam lacunas em relação aos métodos de gestão e elementos cruciais da Segurança da Informação, especialmente, as pessoas, os processos e as tecnologias que fazem parte do ciclo de Segurança da Informação.

Uma organização em conformidade com a política de Segurança da Informação é muito importante para prevenção a ataques que atualmente estão cada vez mais complexos. Podemos destacar alguns itens que podem auxiliar na proteção da organização contra os ataques cibernéticos: a aplicação das diretrizes da política de Segurança da Informação, estabelecer uma estrutura de Segurança da Informação baseada em padrões já citados, como a ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 ou até mesmo a ABNT NBR ISO/IEC 27005, que trata da gestão de riscos, além do COBIT e ITIL, que são ferramentas essenciais para a gestão e governança de tecnologia da informação.

Mas o que é ITIL? Esse *framework* tem sido muito utilizado entre pessoas que trabalham na área de TI. ITIL é uma sigla em inglês. Seu significado é *Information Technology Infrastructure Library.* Sua tradução seria: Biblioteca de Infraestrutura de Tecnologia da Informação**.**

Clinch (2009) define o *framework* ITIL como uma estrutura de orientação de melhores práticas em Gerenciamento de Serviços de Tecnologia da Informação (ITSM). Ele descreve processos, funções e estruturas que suportam a maioria das áreas de Gerenciamento de Serviços de TI, principalmente do ponto de vista do Provedor de Serviços. Ainda segundo Clinch (2009) o ITIL pode ser adaptado e aplicado para se adequar às circunstâncias de um determinado provedor, cliente ou implementação, dependendo de vários fatores como tamanho, cultura, sistemas de gestão existentes, estrutura organizacional e a natureza do negócio. Clinch (2009) conclui que o ITIL não é prescritivo e, devido ao ajuste de implementação necessário, não há rigidez de aplicação que indique que os testes de conformidade são apropriados.

Já COBIT significa *Control Objectives for Information and related Technology,* em português "Objetivos de controle para informação e tecnologia relacionada". Na prática, significa uma estrutura capaz de fornecer governança de TI. Esse *framework* foi desenvolvido pela ISACA (*Information Systems Audit and Control Association*) e possui como principal objetivo agregar valor para a empresa, melhorando seus processos.

O COBIT basicamente trabalha com a necessidade de gerenciamento e controle da informação na TI. Ele é um padrão confiável que cada vez mais está sendo utilizado por um grande número de organizações em todo o globo. Embora exista uma variedade de estruturas, padrões e documentos relacionados ao controle de TI, o foco principal do COBIT é alinhar o uso de TI com o cumprimento das metas de cada organização. A ferramenta é extremamente popular, o que pode ser explicado por seu passo a passo para a gestão ser gratuito. Pagam-se apenas auditorias externas.

**Diferenças entre os padrões de gestão de tecnologia da informação**

| COBIT | ITIL |
|---|---|
| COBIT é um *framework* de boas práticas criado pela ISACA para a governança de tecnologia de informação de forma estratégica nas organizações. | É um conjunto de boas práticas detalhadas para o gerenciamento de serviços de TI que se concentra no alinhamento de serviços de TI, focada principalmente na parte operacional. |

Aumentando os métodos de controle e implementando boas práticas, a Segurança da Informação é melhorada, já que existem menores riscos de comprometimento das informações da organização.

Sabemos que mesmo com os esforços citados acima para se manter em conformidade o ambiente organizacional, podem haver prejuízos por problemas internos e até mesmo incidentes por ataques e vulnerabilidades no sistema e por falhas nos procedimentos e diretrizes.

Fazendo uma breve demonstração sobre algumas boas práticas de Segurança da Informação que podem ser aplicadas facilmente, podemos iniciar com a detecção de vulnerabilidades de *hardware* e *software*. Como já vimos, a evolução tecnológica continua constante e os *hardwares* e *softwares* acompanham de forma

significativa essa evolução, o que gera necessidade periódica de substituição destes ativos. Essa necessidade de substituição precisa levar em consideração no momento da aquisição aspectos técnicos e de qualidade para a organização manter seu padrão de gestão em segurança.

Os *hardwares*, por se tratarem de ativos físicos, sempre podem estar sujeitos a defeitos, seja de instalação, fabricação ou até mesmo por forma incorreta de utilização. Queima de componentes e má conservação também são fatores que podem afetar os ativos de *hardware*. Já os *softwares*, podem estar sujeitos a configurações inadequadas, falhas operacionais, configurações de segurança inadequadas e má gestão de controle de acesso, como logins e senhas.

Como forma de detecção de vulnerabilidades de *hardware* e *software*, é fundamental que todos os colaboradores possuam treinamento e atualização de conhecimentos sobre os recursos de TI da organização, já que o desconhecimento técnico do uso de uma ferramenta pode gerar vulnerabilidades de *hardware* e *software*.

O backup pode ser um mecanismo essencial para garantir a disponibilidade das informações em uma organização, caso os locais onde a informação esteja armazenada sejam danificados ou atacados. Sabemos que a partir do backup fica possível recuperar, de forma rápida, dados e informações que possam vir a ser danificadas ou perdidas de forma acidental ou proposital por parte de atacantes.

## VOCÊ SABIA?

Você sabe o que ocorreu com algumas empresas que funcionavam no World Trade Center na ocasião do trágico atentado de 11 de setembro de 2001? Boa parte destas empresas possuía uma gestão de segurança que pensava a proteção dos dados com backup dos DataCenters. Contudo, a maioria das empresas tinham seus backups na torre ao lado da qual trabalhava, ou seja, como o atentado atingiu as duas torres, os backups, que possuíam basicamente a vida das empresas, desapareceram.

Destacamos também como uma das boas práticas de segurança da informação a eficiência no controle de acesso às informações, seja controle físico, lógico ou mesmo a junção dos dois. Os mecanismos físicos podem ser um data center ou uma sala de infraestrutura de TI com acesso restrito, com câmeras de segurança ou outro tipo de restrição de acesso, como o uso de travas nas portas, acionadas por senha ou biometria. Na biometria, o acesso às informações é liberado apenas para pessoas cadastradas e autorizadas, utilizando-se de características físicas, como impressão digital, voz ou padrões da íris do olho ou do rosto inteiro.

Podemos destacar também como uma das formas mais avançadas de boas práticas e de garantia da segurança da informação, a computação em nuvem. Mas como a tecnologia em nuvem é segura? Podemos explicar da seguinte forma: na nuvem um arquivo, quando salvo, é dividido em diversas partes e geralmente é armazenado em servidores diferentes espalhados pelo mundo. Garante-se a integridade e disponibilidade dos dados pois, mesmo se um dos servidores for atacado, a informação contida nele é apenas uma fração do arquivo, ou seja, a organização não terá perdas e suas informações ficam seguras. A estrutura de nuvem possui três categorias: nuvem pública, privada ou híbrida.

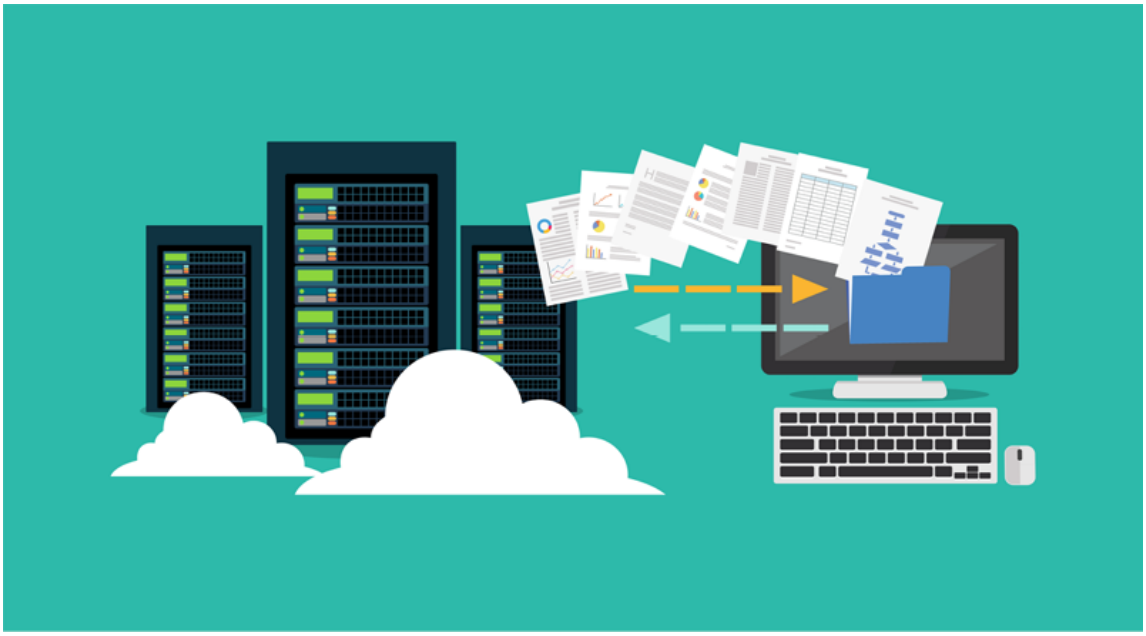

Figura 2 – Backup em nuvem. Fonte: Shutterstock. Acesso em: 12/01/2021.

De acordo com a Microsoft (2020), a nuvem híbrida é um tipo de computação em nuvem que combina uma infraestrutura local ou nuvem privada com uma nuvem pública. As nuvens híbridas permitem que os dados e aplicativos se movam entre os dois ambientes.

As nuvens públicas são a maneira mais comum de implantação da computação em nuvem. Os recursos de nuvem (como servidores e armazenamento) pertencem a um provedor de serviço de nuvem terceirizado, são operados por ele e entregues pela internet. Com uma nuvem pública, todo o *hardware*, *software* e outras infraestruturas de suporte são de propriedade do provedor de nuvem e gerenciadas por ele.

As nuvens privadas são recursos de computação em nuvem usados exclusivamente por uma única empresa ou organização. A nuvem privada pode estar localizada fisicamente no datacenter local da sua organização ou pode ser hospedada por um provedor de serviços terceirizado.

## Teste seus conhecimentos

## Métodos e práticas de segurança da informação nas organizações.

As estratégias aplicadas a partir da implantação dos conceitos que envolvem o planejamento estratégico baseados em diretrizes e normas auxiliam a gestão da organização a manter em equilíbrio a segurança da informação. Uma organização em conformidade com a política de segurança da informação é muito importante para prevenção a ataques cada vez mais complexos. O fator humano tem responsabilidade grande durante a aplicação das diretrizes da política de segurança da informação, estabelecendo uma estrutura de segurança da informação nas organizações.

Considerando esse contexto e os conteúdos estudados, analise as afirmativas a seguir.

I. Na proteção contra riscos “humanos”, do ponto de vista da segurança da informação, a causa mais provável de vazamento interno é o usuário que acessa regularmente os recursos e dados da rede corporativa.
II. Para uma eficiente detecção de vulnerabilidades de hardware e software é fundamental que todos os colaboradores possuam treinamento e atualização de conhecimentos sobre os recursos de TI da organização.
III. Somente a aplicação das normas de segurança como ISO 27001 e ISO 27002 é suficiente para manter o ambiente seguro e com a alta gestão segura com seus ativos de TI.
IV. A aplicação das normas de segurança como ISO 27001 e ISO 27002 somente é suficiente para manter o ambiente seguro caso seja implementada com a ISO 27005.

Está correto apenas o que se afirma em:

**a** I e II.

**b** II e III.

**c** III e IV.

**d** I e III.

**e** II e IV.

Gabarito na página 20.
Atividade não pontuada

## Síntese

Neste capitulo, foi possível compreender que para uma organização a Segurança da Informação nada mais é do que as políticas, processos e métodos que devem ser empregados para que as informações estejam seguras e controladas. Foi possível observar que através de uma política de Segurança da Informação, podemos obter bons resultados em relação à Segurança da Informação, contudo, ela precisa ser divulgada de forma clara e concisa para os usuários. Também pudemos ver que esses possuem direitos e deveres a serem aplicados. Foi possível observar que para esses deveres é necessário o apoio total da alta gestão da organização junto à Segurança da Informação. Pudemos também observar como e quando é necessária a aplicação de uma governança de TI ou Gestão de TI, e como elas ajudam a manter o ambiente seguro de ameaças e vulnerabilidades, além da contribuição final de boas práticas de segurança.

Podemos concluir que adotando uma política de Segurança da Informação, implementando regras de gestão baseadas nas normas internacionais disponíveis e aplicando conceitos básicos aqui citados como backup, computação em nuvem, um bom controle de acesso as informações podemos sim, praticar boas maneiras e métodos fáceis de Segurança da Informação, baseados em muito controle e gestão principalmente de pessoas, afinal elas são a base da segurança, para isso é importantíssimo treinamentos e recorrentes campanhas de conscientização junto aos colaboradores.

# SAIBA MAIS

**Título:** Uma contribuição para a Segurança da Informação: um estudo de casos múltiplos com organizações brasileiras
**Autor:** Napoleão Verardi Alegale, Edison Luiz Gonçalves Fontes, Bernardo Perr Galegale
Ano: 2017
**Comentário:** O artigo versa sobre os controles que auxiliem os gestores na elaboração de uma política de segurança.
**Onde encontrar:** <https://www.scielo.br/pdf/pci/v22n3/1981-5344-pci-22-03-00075.pdf>.

**Título:** Governança de Segurança da Informação - como criar oportunidades para o seu negócio
**Autor:** Sérgio da Silva Manoel
**Editora:** Braspot
**Ano:** 2014
**Comentário:** O livro aborda, de maneira didática, questões relacionadas à governança de segurança da informação, a partir das normas reguladoras.
**Onde encontrar:** Biblioteca Virtual Laureate

**Título:** Auditoria e Segurança de Sistemas com Professor Marcos Assis
**Autor(a):** Marcos Assis
**Ano:** 2020
**Comentário:** O vídeo aborda alguns conceitos dos controles internos para a gestão de risco em organizações.
**Onde encontrar?** <https://www.youtube.com/watch?v=yZgOtuHqbUs>.

## Referências bibliográficas


ABNT NBR ISO/IEC 27001:2013. Tecnologia da Informação – **Técnicas de segurança – Sistema de gestão de segurança da informação** – Requisitos – Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2013.

ABNT NBR ISO/IEC 27005:2011. Tecnologia da Informação – **Técnicas de segurança – Gestão de riscos de segurança da informação** – Requisitos – Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2013.

CLINCH, J. **ITIL V3 and Information Security**. International Best Practice, s.l, 2009. Disponível em: <https://www.internationalbestpractice.com/gempdf/ITILV3_and_Information_Security_White_Paper_May09.pdf>. Acesso em: 13 jan. 21.

DISTERER, G. ISO/IEC 27000, 27001 and 27002 for information security management. **Journal of Information Security**, v. 4, n. 1, pp. 92–100, 2013.

FERNANDES, A. A.; ABREU, V. F. **Implantando a Governança de TI**: da Estratégia à Gestão dos Processos e Serviços. São Paulo: Brasport, 2014.

FONTES, E. **Praticando a Segurança da Informação**. São Paulo: Brasport, 2008.

GALVÃO, M. C. **Fundamentos em segurança da informação**. São Paulo: Pearson, 2015.

HIGGINS, H. N. Corporate system security: towards an integrated management approach. **Information Management and Computer Security**, v. 5, n. 7, p. 217-222, 1999.

HINTZBERGEN, J. et al. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. São Paulo: Brasport, 2018.

HUNKER, J.; PROBST, C. W. Insiders and insider threats-an overview of definitions and mitigation techniques. **Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications**, v. 2, n. 1, pp. 4–27, 2011.

ISACA. **COBIT 5 for Information Security**. ISACA, 2012.

MITNICK, K. D.; SIMON, W. L. M.: **A arte de enganar.** Ataques de hackers: Controlando o fator humano na Segurança da Informação. São Paulo: Pearson Education do Brasil, 2003.

NBR ISO/IEC 27001:2013. Tecnologia da informação — **Técnicas de segurança — Sistemas de gestão da segurança da informação** — Requisitos – Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2013.

O QUE são nuvens públicas, privadas e híbridas? **Microsoft Azure**, *s.l,* 2020. Disponível em: <https://azure.microsoft.com/pt-br/overview/what-are-private-public-hybrid-clouds/#public-cloud>. Acesso em: 21 dez. 2020.

POSTHUMUS, S. (2004). A framework for the governance of information security. **Computers & Security**, s.l., v. 8, n. 23, p. 638-646, 2004.

SUHAIZA, S.; ZAWIYAH, M. Y. Public sector ict strategic planning: framework of monitoring and evaluating process. **Asia-Pacific J. Inf. Technol. Multimed.**, v. 6, n. 1, pp. 85–99, 2017.

WERLINGER, R.; HAWKEY; K.; BEZNOSOV, K., An integrated view of human, organizational, and technological challenges of it security management. **Information Management & Computer Security**, v. 17, n. 1, p. 4-19, 2009.

# Gabarito

## Identificação de tipos de ameaças à segurança da informação.

As ameaças intencionais são provocadas por invasões, fraudes e roubo de informações. As ameaças involuntárias são causadas por erros de desconhecimento no uso do ativo, onde aparecem erros inconscientes de funcionários que não foram devidamente treinados, infecções por vírus ou até mesmo os acessos indevidos. As ameaças exploram os pontos fracos, afetando assim a segurança da informação.

Considerando essas informações, assinale a alternativa que descreve o tipo de ataque que utiliza métodos de ilusão ou exploração da confiança das pessoas para obter acesso a informações importantes e sigilosas em organizações e sistemas.

**b** Engenharia Social.

A arte de manipular pessoas, enganando-as para que forneçam acesso a informações importantes e privadas em organizações e sistemas por meio da mentira ou exploração da confiança das pessoas denomina-se engenharia social. O explorador pode se passar outra pessoa, fingindo, por exemplo, ser um profissional de certa área.

# Gabarito

## Métodos e práticas de segurança da informação nas organizações.

As estratégias aplicadas a partir da implantação dos conceitos que envolvem o planejamento estratégico baseados em diretrizes e normas auxiliam a gestão da organização a manter em equilíbrio a segurança da informação. Uma organização em conformidade com a política de segurança da informação é muito importante para prevenção a ataques cada vez mais complexos. O fator humano tem responsabilidade grande durante a aplicação das diretrizes da política de segurança da informação, estabelecendo uma estrutura de segurança da informação nas organizações.

Considerando esse contexto e os conteúdos estudados, analise as afirmativas a seguir.

I. Na proteção contra riscos “humanos”, do ponto de vista da segurança da informação, a causa mais provável de vazamento interno é o usuário que acessa regularmente os recursos e dados da rede corporativa.
II. Para uma eficiente detecção de vulnerabilidades de hardware e software é fundamental que todos os colaboradores possuam treinamento e atualização de conhecimentos sobre os recursos de TI da organização.
III. Somente a aplicação das normas de segurança como ISO 27001 e ISO 27002 é suficiente para manter o ambiente seguro e com a alta gestão segura com seus ativos de TI.
IV. A aplicação das normas de segurança como ISO 27001 e ISO 27002 somente é suficiente para manter o ambiente seguro caso seja implementada com a ISO 27005.

Está correto apenas o que se afirma em:

**a** I e II.

O engenheiro social é alguém que usa a fraude, a influência e a persuasão contra as empresas, em geral visando suas informações. Uma política de segurança da informação bem documentada e aprovada pela alta gestão, traz para os usuários a responsabilidade de possuir um papel ativo no trabalho de segurança da informação, para isso precisa ser bem documentada e repassada a todos os colaboradores da organização.