Estratégia Concursos

# Aula 00

*Passo Estratégico de Conhecimentos*

*Esp p/ Senado Federal*

*(Analista-Informática) Cebraspe 2021*

Autor:

**Thiago Rodrigues Cavalcanti**

30 de Janeiro de 2021

# GESTÃO E GOVERNANÇA DE TI: GESTÃO DE SEGURANÇA DA INFORMAÇÃO. NORMAS NBR ISO/IEC 27001 E 27002. GESTÃO DE RISCOS E CONTINUIDADE DE NEGÓCIO. NORMAS NBR ISO/IEC 15999 E 27005

**Sumário**



## ANÁLISE ESTATÍSTICA

A análise estatística estará disponível a partir da próxima aula.

# ROTEIRO DE REVISÃO E PONTOS DO ASSUNTO QUE MERECEM DESTAQUE

*A ideia desta seção é apresentar um roteiro para que você realize uma revisão completa do assunto e, ao mesmo tempo, destacar aspectos do conteúdo que merecem atenção.*

Para revisar e ficar bem preparado no assunto, você precisa, basicamente, seguir os passos a seguir:

Os conceitos de segurança da informação estão diretamente relacionados com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

De acordo com a norma ISO 17799:2005, "segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".

A informação é um ativo que deve ser protegido e cuidado por meio de regras e procedimentos das políticas de segurança, do mesmo modo que protegemos nossos recursos financeiros e patrimoniais. Entretanto, "muitas vezes é difícil obter o apoio da própria alta administração da organização para realizar os investimentos necessários em segurança da informação. Os custos elevados das soluções contribuem para esse cenário, mas o desconhecimento da importância do tema é provavelmente ainda o maior problema". (CAMPOS, 2007)[1]

O Decreto Nº 3.505 de 13 de junho de 2000 instituído pelo presidente da República Federativa do Brasil, define segurança da informação como:

> *Art. 2. Para efeitos da Política de Segurança da Informação, ficam estabelecidas as seguintes conceituações:*
>
> *II – Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.*

Dessa forma, a segurança da informação é imprescindível para qualquer organização tanto do ponto de vista estratégico, quanto do tático e operacional.

Antes de falar sobre as políticas de segurança, precisamos entender que na segurança da informação existem quatro princípios básicos, definidos na norma ABNT NBR ISO/IEC 27002:2005, que fundamentam a proteção dos dados. A partir do quadro abaixo vamos citar e definir cada um destes princípios.

---

[1] CAMPOS, A. Sistema de segurança da informação: controlando os riscos. Florianópolis: Visual Books, 2ª ed, 2007.

# Princípios da Segurança da Informação


O dicionário Aurélio nos dá, entre os dezesseis significados de princípio, dois que se encaixam bem dentro deste contexto: 1 - Frase ou raciocínio que é base de uma arte, de uma ciência ou de uma teoria; 2 - Regras ou conhecimentos fundamentais e mais gerais. Ou seja, um princípio é uma definição sobre algo que se almeja.

| Princípio | | Definição |
|---|---|---|
| **D** isponibilidade | - | Princípio que garante que a informação estará sempre disponíveis. |
| **I** ntegridade | - | Princípio que garante que as informações serão guardadas ou enviadas em sua forma original, sem sofrer alterações. |
| **C** onfidencialidade | - | Princípio que garante o sigilo da informação com a capacidade de controlar o acesso, assegurando que elas só serão acessadas por pessoas autorizadas. Ou seja, é a garantia que as informações só serão acessadas através de uma senha. |
| **A** utenticidade | - | Princípio que permite verificar a identidade de uma pessoa em um sistema, garantindo a veracidade das informações. |

Note que foi formado o mnemônico **DICA** para facilitar a memorização e associação das definições.

É importante notar que nos princípios sempre está presente a partícula "...idade". Por exemplo: caso a banca cite o princípio da autenticação, estará incorreto. O correto é "Princípio da Autentic**idade**".

Algumas bancas indicam o Não Repúdio como parte dos princípios de segurança da informação, porém ele só é efetivamente usado junto com o princípio da Autenticidade que garante que as informações são verídicas e por este motivo não podem ser refutadas.

| | | |
|---|---|---|
| **N ão Repúdio** (Irrefutabilidade) | - | **Incapacidade de negação da autoria de uma informação.** (Este princípio está ligado diretamente ao princípio da Autenticidade) |

# Princípios

## Disponibilidade

O operacional de uma organização depende diretamente desse princípio, pois ele está relacionado ao tempo e à acessibilidade que se tem dos dados e sistemas, ou seja, se eles podem ser consultados a qualquer momento pelos colaboradores.

Praticamente todos os processos de trabalho de uma organização dependem da chegada ou busca de uma informação. Quando a informação está indisponível, os processos que dependem dela ficam impedidos de serem executados.

## Integridade

Esse princípio é absolutamente crítico do ponto de vista operacional, pois valida todo o processo de comunicação em uma organização. Conforme vimos na tabela acima, é importante que os dados circulem ou sejam armazenados do mesmo modo como foram criados, sem que haja interferência externa para corrompê-los ou comprometê-los.

Toda organização se comunica interna e externamente o tempo todo, transmitindo números, resultados, projeções, estratégias, regras, procedimentos e dados em todas as direções; e a comunicação efetiva só acontece quando o emissor e o receptor da informação a interpretam da mesma maneira.

Informação sem integridade demanda verificação, correção e retrabalho, que causa desperdício de energia, traduzido em perda de recursos, seja tempo, pessoal ou financeiro.

## Confidencialidade

A norma ISO/IEC 17799 define confidencialidade como “garantir que a informação seja acessível apenas àqueles autorizados a ter acesso”. Com isso, chegamos à conclusão que a confidencialidade tem a ver com a privacidade dos dados de uma organização. Esse conceito se relaciona às ações tomadas para assegurar que informações confidenciais e críticas não sejam roubadas dos sistemas organizacionais por meio de cyber ataques, espionagem, entre outras práticas.

Para que a confidencialidade seja reforçada, as organizações adotam medidas preventivas, como por exemplo a definição dos níveis de acesso as informações. Isso garante que apenas pessoas autorizadas terão acesso a dados sensíveis para a organização. Os níveis também precisam ser limitados conforme as áreas a que se relacionam (marketing, vendas, financeiro, administração, etc.).

Além de níveis de acesso para as pessoas, os dados são classificados de acordo com o potencial de impacto, caso sejam acessados por pessoas indevidas. Dessa forma as organizações criam modelos de contingencia que abrangem todas as possibilidades.

## Autenticidade

Esse princípio identifica e registra as ações de envio ou edição de uma informação, realizadas pelo usuário. Toda ação é documentada, garantido a autenticidade da informação proveniente de uma fonte confiável. Acima

citei que esse princípio torna a informação irrefutável, ou seja, a pessoa que cria, edita ou exclui um dado, não pode negar a sua ação.

## Métodos Relacionados aos Princípios

### Disponibilidade

Um exemplo de disponibilidade é o site para inscrição em um concurso. Dependendo do concurso pode acontecer de o site ficar ”fora do ar”, ferindo o princípio e causando uma indisponibilidade. Isso normalmente ocorre quando os recursos acessados estão ultrapassando o limite fornecido pelo servidor.

### Integridade

Em um arquivo é utilizada uma função *hash*, que mapeia os dados de comprimento variável para dados de comprimento fixo, criando, a partir dos valores retornados, um código *hash* ou *checksum*. Os algoritmos da função *hash* mais utilizados são MD5 e SHA-1. Os códigos gerados são únicos para cada arquivo, possuem tamanho entre 20 e 256 caracteres e a partir do código gerado não é possível retornar ao arquivo, ou seja, é um processo de via única.

### Confidencialidade

O uso de criptografia garante o sigilo quando a informação é confidencial. Existem dois métodos de criptografia: chaves simétricas e chaves assimétricas (com ou sem certificado digital). Além desses métodos, pode ser implantada a autenticação de dois fatores, a verificação biométrica e o uso de token.

### Autenticidade

O reconhecimento de firma em um cartório é um exemplo de um método de autenticidade. Em informática o uso de certificado digital é o que garante a autenticidade.


**Chave Simétrica** está relacionada diretamente a uma senha única.

**Chave Assimétrica** está relacionada a duas chaves diferentes que são correspondentes – chave pública e chave privada. A chave pública, como o próprio no diz, qualquer pessoa possui acesso. A chave privada apenas o próprio dono tem acesso. Quando um arquivo é criptografado com a chave pública, apenas o proprietário da chave privada poderá ter acesso a informação.

# Política de Segurança da Informação

Entendendo os princípios que servem como base para a segurança da informação, vamos agora estudar como esses princípios podem ser aplicados, através das políticas de segurança.

A política de segurança da informação (PSI) é o conjunto de ações, técnicas e boas práticas relacionadas ao uso seguro de dados. Ou seja, trata-se de um documento ou manual que determina as ações mais importantes para garantir a segurança da informação.

A formalização de uma PSI tem por objetivo preservar a integridade dos dados, garantir sua disponibilidade para as pessoas e sistemas certos, além de estabelecer a confidencialidade das informações, principalmente das mais críticas para o negócio.

Ela promove a homogeneização de ações, de modo que todas as pessoas envolvidas no processo saibam o que fazer e o que evitar. Além de possuir procedimentos para administrar corretamente emergências, como um plano de contingência para prevenir danos maiores nos dados.

A família ISO 27000, possui 45 normas que indicam boas práticas, tanto genérica quanto especificas para a gestão da segurança da informação. Essas práticas servem como guia para elaborar a PSI.

A NBR ISO/IEC 27001:2005 é uma norma de códigos de práticas para a gestão de segurança da informação, onde podem ser encontradas as melhores práticas para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.

Ela estabelece diretrizes e princípios gerais para se iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Essa norma possui uma seção introdutória sobre o processo de avaliação e tratamento de riscos e está dividida em onze seções específicas, que são: política de segurança da informação; organização da segurança da informação; gestão de ativos; segurança em recursos humanos; segurança física e do ambiente; gestão das operações e comunicações; controle de acesso; aquisição, desenvolvimento e manutenção de sistemas de informação; gestão de incidentes de segurança da informação; gestão da continuidade do negócio, e conformidade. Essas seções totalizam trinta e nove categorias principais de segurança, e cada categoria contém um objetivo de controle e um ou mais controles que podem ser aplicados, bem como algumas diretrizes e informações adicionais para a sua implementação.

De acordo com a NBR ISO/IEC 27002:2005, as PSI têm como objetivo “fornecer uma orientação e apoio da direção para prover a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes”.

**TOME NOTA!**

Segundo a ISO/IEC 27002:2005, a informação é um conjunto de dados que representa um ponto de vista, um dado processado é o que gera uma informação. Um dado não tem valor antes de ser processado, a partir do seu processamento, ele passa a ser considerado uma informação, que pode gerar conhecimento. Portanto, pode-se entender que informação é o conhecimento produzido como resultado do processamento de dados.

**A informação é encarada, atualmente, como um dos recursos mais importantes de uma organização, contribuindo decisivamente para a uma maior ou menor competitividade. De fato, com o aumento da concorrência de mercado, tornou-se vital melhorar a capacidade de decisão em todos os níveis. Como resultado deste significante aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades.**

## Itens da Política de Segurança

Para elaborar uma política de segurança, é necessário estabelecer alguns pontos indispensáveis:

- **Responsáveis**

Deve ser estabelecido que são os responsáveis não apenas pelo monitoramento, mas também pela elaboração, divulgação e revisão das políticas de segurança.

- **Tipos de Informações**

As informações devem ser classificadas de forma parecida com os documentos físicos: pública, interna, confidencial e secreta. Com base na classificação dos dados é que serão definidos os níveis de acesso de cada colaborador às informações, como os aplicativos de negócios serão implementados e qual o impacto que um incidente com aqueles dados pode gerar para a reputação da empresa. Mais adiante veremos as Políticas de classificação da informação.

- **Níveis de acesso**

A definição dos níveis de acesso deve considerar três pontos principais: Quem acessa? Como acessa? Quando acessa? A resposta para essas perguntas separa o nível / perfil de acesso de cada uma das pessoas.

Com os pontos citados acima, podemos concluir que a política de segurança deve considerar não apenas os ataques, mas todos os elementos que dizem respeito aquilo que é essencial quando o objetivo é combater situações adversas. A disponibilidade da infraestrutura da organização também deve ser considerada (HUR, 1999 apud NAKAMURA e DE GEUS, 2000)[2]:

- Vigilância: significa que todos da organização são responsáveis por garantir e fiscalizar a segurança de informação;
- Atitude: significa a postura e a conduta quanto à segurança. Todos os envolvidos devem ter a consciência que a política de segurança não tem efeitos se ela não for adotada de forma certa. É necessário treinamento e conscientização dos funcionários quanto à importância de se seguir a política de segurança estabelecida;

[2] NAKAMURA, E. T.; DE GEUS, P. L. Um modelo de segurança de redes para ambientes cooperativos. Instituto de Computação – Universidade Estadual de Campinas. Campinas, SP. 2000.

- Estratégia: significa ser criativo na elaboração da política de segurança além de ser adaptativa às mudanças no ambiente. A estratégia leva em conta também a produtividade dos usuários. Uma boa política não deve interferir negativamente no andamento dos negócios da organização;
- Tecnologia: a solução tecnológica deve ser flexível e adaptativa para suprir as necessidades da organização. Qualquer tecnologia desatualizada pode causar uma falsa sensação de segurança.

Em 2008 o Tribunal de Contas da União afirmou que o conteúdo da Política de Segurança da Informação aplicável à Administração Pública Federal direta ou indireta varia de acordo com a organização. Entretanto, alguns elementos são comuns nessas políticas:

- Definição de segurança de informações e de sua importância como mecanismo que possibilita o compartilhamento de informações;
- Declaração do comprometimento da alta administração com a Política de Segurança da Informação, apoiando suas metas e princípios;
- Objetivos de segurança da organização;
- Definição de responsabilidades gerais na gestão de segurança de informações;
- Orientações sobre análise e gerência de riscos;
- Princípios de conformidade dos sistemas computacionais com a Política de Segurança da Informação;
- Padrões mínimos de qualidade que esses sistemas devem possuir;
- Políticas de controle de acesso a recursos e sistemas computacionais;
- Classificação das informações (de uso irrestrito, interno, confidencial e secretas);
- Procedimentos de prevenção e detecção de vírus;
- Princípios legais que devem ser observados quanto à tecnologia da informação (direitos de propriedade de produção intelectual, direitos sobre software, normas legais correlatas aos sistemas desenvolvidos, cláusulas contratuais);
- Princípios de supervisão constante das tentativas de violação da segurança de informações;
- Consequências de violações de normas estabelecidas na política de segurança;
- Princípios de gestão da continuidade do negócio;
- Plano de treinamento em segurança de informações.

## Política de Classificação da Informação

A norma ISO/IEC 27001 descreve como a classificação da informação deve ser realizada. O processo é definido em quatro etapas onde (1) a informação deveria ser inserida em um Inventário de Ativos (controle A.8.1.1 da ISO 27001), (2) ela deveria ser classificada (A.8.2.1), (3) então ela deveria ser rotulada (A.8.2.2), e finalmente (4) ela deveria ser manuseada de forma segura (A.8.2.3).


## Inventário de ativos (Registro de ativo)

O inventário de ativos é feito para que seja possível saber quais informações classificadas você tem em sua posse, e quem é responsável por elas. A informação classificada pode estar em diferentes formatos e tipos de mídia, como por exemplo:

- documentos eletrônicos
- sistemas de informação / bases de dados
- documentos em papel
- mídias de armazenamento
- e-mail

## Classificação da informação

Segundo a ISO 27002:2013, "convém que a classificação e os controles de proteção, associados para a informação, leve em consideração as necessidades do negócio para compartilhar ou restringir a informação bem como os requisitos legais. Convém que outros ativos além dos ativos de informação também sejam classificados de acordo com a classificação da informação armazenada, processada, manuseada ou protegida pelo ativo".

Seguindo a orientação acima, entendemos que a classificação da informação deverá seguir os níveis de complexidade exigido pelo negócio. Porém existe um padrão com três níveis de confidencialidade e um nível público:

1) Confidencial (o mais alto nível de confidencialidade) - o impacto aos objetivos estratégicos e as consequências do acesso não autorizado à esta informação são severos e, possivelmente, irreversíveis.
2) Restrita (médio nível de confidencialidade) - impacto menor, mas consequências relevantes.
3) Uso interno (o mais baixo nível de confidencialidade) - constrangimento é maior que o impacto e suas consequências.
4) Pública (todos podem ver a informação) - o acesso é permitido a qualquer pessoa, sem impacto ou consequências ao negócio.

Em muitos casos, o proprietário do ativo é o responsável por classificar a informação – e isto é usualmente feito com base nos resultados da análise/avaliação de riscos: quanto maior o valor da informação (quanto maiores as consequências de uma quebra da confidencialidade), maior deverá ser o nível de classificação. É importante lembrar que deve haver alguma coerência entre a relevância e a classificação da informação.

### Rotulagem da informação

A partir do momento que a informação está classificada, é necessário rotulá-la apropriadamente. Por exemplo, é possível definir as regras para documentos em papel de tal forma que o nível de confidencialidade seja indicado no canto superior direito de cada página do documento, e que a classificação também seja indicada na capa ou no envelope que transporta tal documento, assim como na pasta onde o documento é armazenado. A rotulagem da informação geralmente é responsabilidade do proprietário da informação.

### Manuseio de ativos

O manuseio de ativos é usualmente a parte mais complexa do processo de classificação. A ISO 27001 permite a organização definir suas próprias regras, e elas são geralmente definidas na política de classificação da informação, ou nos procedimentos de classificação.

Assim, como você pode ver, o processo de classificação pode ser complexo, mas ele não tem que ser incompreensível. A ISO 27001 dá liberdade para o responsável pela classificação criar as próprias regras e definir como as informações serão classificadas.

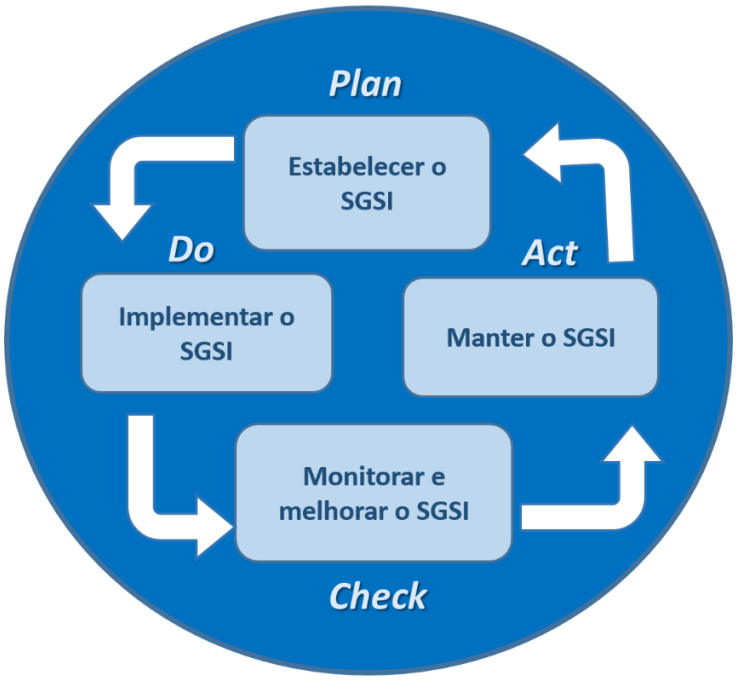
Além das normas citadas até aqui, o TCU possui um trabalho publicado para auxiliar as instituições da Administração Pública Federal a realizarem boas práticas em segurança da informação. Esse documento serve de base não apenas para as instituições federais, mas para qualquer organização. Você pode acessa-lo deste *link*.

## Sistema de Gestão de Segurança da Informação (SGSI)

O SGSI é um sistema (não necessariamente automatizado) que inclui toda a abordagem organizacional usada para proteger a informação. Ele inclui estratégias, planos, políticas, medidas, controles, e diversos

instrumentos usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

A norma ISO 27001 adota o modelo PDCA (Plan-Do-Check-Act) para descrever a estrutura de um SGSI. A imagem ao lado, junto com descrição de cada uma das etapas provavelmente irá ajudá-lo a ganhar um pouco mais de intimidade com o conceito.




**Estabelecer o SGSI** - é o ponto de partida do SGSI, a etapa que dá vida ao sistema. Suas atividades devem estabelecer políticas, objetivos, processos e procedimentos para a gestão de segurança da informação. São os instrumentos estratégicos fundamentais para que a organização possa integrar suas à segurança da informação às políticas e objetivos globais da organização. Abaixo temos os requisitos da norma ISO 27001 para esta etapa:

- Definição do escopo do SGSI (a quais processos organizacionais, departamentos e partes interessadas se aplica).
- 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).

**Implementar o SGSI**

Consiste em implementar e operar a política de segurança, os controles / medidas de segurança, processos e procedimentos. Os requisitos da norma 27001 para esta etapa são:

- Formular um plano de tratamento de riscos que identifique a ação de gestão apropriada, recursos, responsabilidades e prioridades para a #Gestão de Riscos.
- Implementar o plano de tratamento de riscos para alcançar os objetivos de controle identificados, que inclua considerações de financiamentos e atribuição de papéis e responsabilidades.
- Implementar os controles selecionados.
- Definir como medir a eficácia dos controles ou grupos de controles selecionados, e especificar como estas medidas devem ser usadas para avaliar a eficácia dos controles de modo a produzir resultados comparáveis e reproduzíveis.
- Implementar programas de conscientização e treinamento.
- Gerenciar as operações do SGSI.
- Gerenciar os recursos para o SGSI.

- Implementar procedimentos e outros controles capazes de permitir a pronta detecção de eventos de segurança da informação e resposta a incidentes de segurança da informação.

**Monitorar e analisar criticamente o SGSI**

Esse ponto reúne as práticas necessárias para avaliar a eficiência e eficácia do SGSI, apontando os resultados para uma análise crítica. A política de segurança é usada para comparar e desempenho alcançado com as diretrizes definidas. Os requisitos da norma 27001 para esta etapa são:

- Executar procedimentos de monitoração e análise crítica
- Realizar análises críticas regulares da eficácia do SGSI (incluindo o atendimento da política e dos objetivos do SGSI, e a análise crítica de controles de segurança), levando em consideração os resultados de auditorias de segurança da informação, incidentes de segurança da informação, resultados da eficácia das medições, sugestões e realimentação de todas as partes interessadas.
- Medir a eficácia dos controles para verificar que os requisitos de segurança da informação foram atendidos.
- Analisar criticamente as análises/avaliações de riscos a intervalos planejados e analisar criticamente os riscos residuais e os níveis de riscos aceitáveis identificados.
- Conduzir auditorias internas do SGSI a intervalos planejados.
- Realizar uma análise crítica do SGSI pela direção em bases regulares para assegurar que o escopo permanece adequado e que são identificadas melhorias nos processos do SGSI.
- Atualizar os planos de segurança da informação para levar em consideração os resultados das atividades de monitoramento e análise crítica.
- Registrar ações e eventos que possam ter um impacto na eficácia ou no desempenho do SGSI.

## Manter e melhorar continuamente o SGSI

Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI. Os requisitos da norma ISO 27001 para esta etapa são:

- Implementar as melhorias identificadas no SGSI.
- Executar as ações preventivas e corretivas apropriadas.
- Aplicar as lições aprendidas de experiências de segurança da informação de outras organizações e aquelas da própria organização.
- Comunicar as ações e melhorias a todas as partes interessadas com um nível de detalhe apropriado às circunstâncias e, se relevante, obter a concordância sobre como proceder.
- Assegurar -se de que as melhorias atinjam os objetivos pretendidos.

As normas de Gestão da Segurança da Informação se fundamentam em 10 premissas básicas aplicadas em qualquer tipo de organização, sendo elas:

- Política de Segurança da Informação

- Segurança Organizacional

- Classificação e controle dos ativos de informação

- Segurança em pessoas

- Segurança Física e Ambiental

- Gerenciamento das operações e comunicações

- Controle de Acesso

- Desenvolvimento de Sistemas e Manutenção

- Gestão da continuidade do negócio e a Conformidade.

## Normas ISO para Segurança da Informação

A ISO (*International Organization for Standardization*) é uma entidade de padronização e normatização, e foi criada em Genebra, na Suíça, em 1947 e tem como objetivo principal aprovar normas internacionais em todos os campos técnicos, como normas técnicas, classificações de países, normas de procedimentos e processos, e etc. No Brasil, a ISO é representada pela ABNT (Associação Brasileira de Normas Técnicas).

As normas técnicas têm como nomenclatura numerações, por exemplo, ISO 9001 → norma de padronização para um determinado serviço ou produto (uma das mais famosas). Em Segurança da Informação temos duas normas: ISO 27001 e ISO 27002, que serão o foco dessa parte da nossa aula.

### ISO 27001

É a norma internacional que define os Requisitos para Sistemas de Gestão de Segurança da Informação. Ela ajuda a organização a adotar um sistema de gestão da segurança da Informação que permita mitigar os riscos de segurança atribuídos a seus ativos e adequar as necessidades a área de negócio. A versão mais recente desta norma foi publicada em 2013, e seu título completo agora é ISO/IEC 27001:2013. A primeira versão desta norma foi publicada em 2005, e foi desenvolvida com base na Norma Britânica BS 7799-2.

O foco da ISO 27001 é proteger a confidencialidade, integridade e disponibilidade da informação de uma organização (princípios de Segurança da Informação que destacamos no início da parte teórica). Isto é feito identificando-se quais potenciais problemas podem ocorrer com a informação, e então definindo quais necessidades devem ser atendidas para prevenir tais problemas de ocorrerem.

Desta forma, a principal filosofia da ISO 27001 é baseada na gestão de riscos: descobrir onde os riscos estão, e então trata-los sistematicamente (implementação de salvaguardas).

As salvaguardas (ou controles) que são implementadas em geral estão na forma de políticas, procedimentos e implementações técnicas. Contudo, em muitos casos as organizações já possuem todo o hardware e software instalado, mas estão utilizando-os de forma insegura – desta forma, a maioria das implementações da ISO 27001 serão sobre definir as regras organizacionais que são necessárias de modo a prevenir brechas de segurança.

Uma vez que tal implementação irá requerer a gestão de múltiplas políticas, procedimentos, pessoas, ativos, etc., a ISO 27001 descreve como encaixar todos estes elementos de forma coerente no sistema de gestão de segurança da informação (SGSI).

Desta forma, gerir a segurança da informação não trata apenas de segurança em TI (exemplo: firewall, antivírus, etc.) mas também sobre gerenciar processos, proteção legal, recursos humanos, proteção física, etc.


A ISO / IEC 27001 é dividia em 11 seções e Anexo A, onde as seções de 0 a 3 são introdutórias (e não são obrigatórias para a implementação), enquanto as seções de 4 a 10 são obrigatórias – significando que todos os seus requisitos devem ser implementados em uma organização se ela quer estar em conformidade com a norma. Controles do Anexo A devem ser implementados apenas se declarados como aplicáveis na Declaração de Aplicabilidade. Vamos pontuar cada uma das seções.

- **Seção 0: Introdução** – explica o propósito da ISO 27001 e sua compatibilidade com outras normas de gestão.
- **Seção 1: Escopo** – explica que esta norma é aplicável a qualquer tipo de organização.
- **Seção 2: Referência normativa** – refere-se a ISO / IEC 27000 como uma norma onde termos e definições são dadas.
- **Seção 3: Termos e definições** – novamente, refere-se a ISO / IEC 27000.

- **Seção 4: Contexto da organização** – esta seção é parte da etapa de planejamento (Plan) do ciclo PDCA e define requisitos para o entendimento de assuntos externos e internos, partes interessadas e seus requisitos, e a definição do escopo do SGSI.
- **Seção 5: Liderança** – esta seção é parte da etapa de planejamento (Plan) do ciclo PDCA e define as responsabilidades da Alta Direção, estabelecendo papéis e responsabilidades, e o conteúdo da política de segurança da informação de alto nível.
- **Seção 6: Planejamento** – esta seção é parte da etapa de planejamento (Plan) do ciclo PDCA e define requisitos para a avaliação de risco, tratamento de risco, Declaração de Aplicabilidade, plano de tratamento de risco, e define os objetivos de segurança da informação.
- **Seção 7: Apoio** – esta seção é parte da etapa de planejamento (Plan) do ciclo PDCA e define requisitos de disponibilidade de recursos, competências, conscientização, comunicação e controle de documentos e registros.
- **Seção 8: Operação** – esta seção é parte da etapa execução (Do) do ciclo PDCA e define a implementação da avaliação e tratamento de risco, assim como controles e outros processos necessários para atingir os objetivos de segurança da informação.
- **Seção 9: Avaliação do desempenho** – esta seção é parte da etapa verificação (Check) do ciclo PDCA e define requisitos para o monitoramento, medição, análise, avaliação, auditoria interna e análise crítica pela Direção.
- **Seção 10: Melhoria** – esta seção é parte da etapa de atuação (Act) do ciclo PDCA e define requisitos para não conformidades, ações corretivas e melhoria contínua.
- **Anexo A** – este anexo disponibiliza um catálogo de 114 controles (salvaguardas) distribuídos em 14 seções (seções de A.5 até A.18).

Para implementar a ISO 27001 em uma organização, é necessário seguir estas 16 etapas:

1) Obter apoio da Alta Direção
2) Utilizar metodologia de gerenciamento de projeto
3) Definir o escopo do SGSI
4) Escrever a política de segurança da informação de alto nível
5) Definir a metodologia de avaliação de risco
6) Realizar a avaliação de risco de o tratamento de risco
7) Escrever a Declaração de Aplicabilidade
8) Escrever o Plano de tratamento de risco
9) Definir como medir a eficácia de seus controles e do seu SGSI
10) Implementar todos os controles e procedimentos aplicáveis
11) Implementar programas de treinamento e conscientização
12) Realizar todas as operações diárias prescritas pela documentação do seu SGSI
13) Monitorar e medir seu SGSI
14) Realizar auditoria interna
15) Realizar análise crítica pela direção
16) Implementar ações corretivas

Por fim, é necessário que todas as ações sejam documentadas. A ISO 27001 requer que a seguinte documentação seja escrita:

- Escopo do SGSI (cláusula 4.3)
- Política de segurança da informação e objetivos (cláusulas 5.2 e 6.2)
- Metodologia de avaliação de risco e de tratamento de risco (cláusula 6.1.2)

- Declaração de aplicabilidade (cláusula 6.1.3 d)
- Plano de tratamento de risco (cláusulas 6.1.3 e e 6.2)
- Relatório de avaliação de risco (cláusula 8.2)
- Definição de papéis e responsabilidades de segurança (cláusulas A.7.1.2 e A.13.2.4)
- Inventário de ativos (cláusula A.8.1.1)
- Uso aceitável dos ativos (cláusula A.8.1.3)
- Política de controle de acesso (cláusula A.9.1.1)
- Procedimentos operacionais para a gestão de TI (cláusula A.12.1.1)
- Princípios para projetar sistemas seguros (cláusula A.14.2.5)
- Política de segurança para fornecedores (cláusula A.15.1.1)
- Procedimento para gestão de incidente (cláusula A.16.1.5)
- Procedimentos de continuidade do negócio (cláusula A.17.1.2)
- Requisitos estatutários, regulatórios e contratuais (cláusula A.18.1.1)

Estes são os registros obrigatórios:

- Registros de treinamento, habilidades, experiência e qualificações (cláusula 7.2)
- Resultados de monitoramento e medição (cláusula 9.1)
- Programa de auditoria interna (cláusula 9.2)
- Resultados de auditorias internas (cláusula 9.2)
- Resultados de análises críticas pela direção (cláusula 9.3)
- Resultados de ações corretivas (cláusula 10.1)
- Registros (logs) de atividades de usuários, de exceções e de eventos de segurança (cláusula A.12.4.1 e A.12.4.3)

## ISO 27002

A ISO/IEC 27002 é a norma internacional que estabelece código de melhores práticas para apoiar a implantação do Sistema de Gestão de Segurança da Informação (SGSI) nas organizações.

Através do fornecimento de um guia completo de implementação, ela descreve como os controles podem ser estabelecidos. Estes controles, por sua vez, devem ser escolhidos com base em uma avaliação de riscos dos ativos mais importantes da organização. Ao contrário do que muitos gestores pensam, a ISO 27002 pode ser utilizada para apoiar a implantação do SGSI em qualquer tipo de organização, pública ou privada, de pequeno ou grande porte, com ou sem fins lucrativos; e não apenas em empresas de tecnologia.

O foco da norma 27002 é determinar princípios gerais para implantar o SGSI e iniciar, manter e aprimorar a segurança da informação. Nesse contexto, também estão incluídos: seleção, implementação e gestão dos controles segundo os ambientes de risco encontrados na empresa.

Porém, essa não é uma norma de gestão, ou seja, seu objetivo não é indicar como determinado sistema deve ser administrado. Essa responsabilidade é da 27001, que ajuda a construir a base da segurança da informação. A 27002 é um complemento, porque permite implementar os controles para isso.

Da mesma forma da ISO 27001, a ISO 27002 também traz benefícios. Os principais são:

- conscientização da importância da segurança da informação;
- controle adequado de ativos e informações sensíveis;
- abordagem correta para implantar políticas de controles;
- identificação de riscos e possibilidade de corrigir os pontos fracos;
- diminuição do risco de responsabilidade ao implementar o SGSI e/ou delimitação de políticas e processos;
- conquista de diferencial competitivo, o que atrai mais clientes;
- organização melhor estruturada de processos e mecanismos, os quais serão bem gerenciados e desenhados;
- redução de custos devido à prevenção de incidentes na área de segurança da informação;
- conformidade com a legislação e outros regulamentos.

Os principais itens que compões a ISO 27002 são:

**Seção 5 – Política de Segurança da Informação**

Deve ser criado um documento sobre a política de segurança da informação da empresa, que deve conter os conceitos de segurança da informação, uma estrutura para estabelecer os objetivos e as formas de controle, o comprometimento da direção com a política, entre tantos outros fatores.

**Seção 6 – Organização da Segurança da Informação**

Para implementar a Segurança da Informação em uma empresa, é necessário estabelecer uma estrutura para gerencia-la da maneira adequada. Para isso, as atividades de segurança da informação devem ser coordenadas por representantes da organização, que devem ter responsabilidades bem definidas e proteger as informações de caráter sigiloso.

**Seção 7 – Gestão de ativos**

Ativo, segundo a norma, é qualquer coisa que tenha valor para a organização e que precisa ser protegido. Mas para isso, os ativos devem ser identificados e classificados, de tal forma que um inventário possa ser estruturado e posteriormente mantido. Além disso, eles devem seguir regras documentadas, que definem qual o tipo de uso é permitido fazer com esses ativos.

**Seção 8 – Segurança em recursos humanos**

Antes de realizar a contratação de um funcionário – ou mesmo de fornecedores – é importante que ele seja devidamente analisado, principalmente se for lidar com informações de caráter sigiloso. A intenção desta seção é mitigar o risco de roubo, fraude ou mau uso dos recursos. E quando o funcionário estiver trabalhando na empresa, ele deverá estar ciente das ameaças relativas à segurança da informação, bem como de suas responsabilidades e obrigações.

**Seção 9 – Segurança física e do ambiente**

Os equipamentos e instalações de processamento de informação críticas ou sensíveis devem ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

**Seção 10 – Segurança das operações e comunicações**

É importante que estejam definidos os procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações. Isso inclui o gerenciamento de serviços terceirizados, o planejamento dos recursos dos sistemas para minimizar o risco de falhas, a criação de procedimentos para a geração de cópias de segurança e sua recuperação e a administração segura de redes de comunicações.

**Seção 11 – Controle de acesso**

O acesso à informação, assim como aos recursos de processamento das informações e aos processos de negócios, deve ser controlado com base nos requisitos de negócio e na segurança da informação. Deve ser assegurado o acesso de usuário autorizado e prevenido o acesso não autorizado a sistemas de informação, a fim de evitar danos a documentos e recursos de processamento da informação que estejam ao alcance de qualquer um.

**Seção 12 – Aquisição, desenvolvimento e manutenção de sistemas**

Os requisitos de segurança de sistemas de informação devem ser identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos visando a manutenção de sua confidencialidade, autenticidade ou integridade por meios criptográficos.

**Seção 13 – Gestão de incidentes de segurança da informação**

Procedimentos formais de registro e escalonamento devem ser estabelecidos, e os funcionários, fornecedores e terceiros devem estar conscientes sobre os procedimentos para notificação dos eventos de segurança da informação, para assegurar que eles sejam comunicados o mais rápido possível e corrigidos em tempo hábil.

**Seção 14 – Gestão da continuidade do negócio**

Planos de continuidade do negócio devem ser desenvolvidos e implementados, visando impedir a interrupção das atividades do negócio e assegurar que as operações essenciais sejam rapidamente recuperadas.

**Seção 15 – Conformidade**

É importante evitar a violação de qualquer lei criminal ou civil, garantindo estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação. Caso necessário, a empresa pode contratar uma consultoria especializada, para que verifique sua conformidade e aderência a requisitos legais e regulamentares.

A norma ISO 27002 possui 11 seções, 39 categorias e 133 controles. Abaixo temos uma tabela com a relação entre as seções e as categorias.

| Seção | Categoria |
|---|---|
| **1. Política de Segurança da Informação** | • Política de segurança da informação |
| **2. Organizando a Segurança da Informação** | • Infraestrutura da segurança da informação<br>• Partes externas |

| | |
|---|---|
| **3. Gestão de Ativos** | • Responsabilidade pelos ativos<br>• Classificação das informações |
| **4. Segurança em Recursos Humanos** | • Antes da contratação<br>• Durante a contratação<br>• Encerramento ou mudança da contratação |
| **5. Segurança Física e do Ambiente** | • Áreas seguras<br>• Segurança dos equipamentos |
| **6. Gerenciamento das Operações e Comunicações** | • Procedimentos e responsabilidades operacionais<br>• Gerenciamento de serviços terceirizados<br>• Planejamento e aceitação dos sistemas<br>• Proteção contra códigos maliciosos e códigos móveis<br>• Cópias de segurança<br>• Gerenciamento da segurança em redes<br>• Manuseio de mídias<br>• Troca de informações<br>• Serviços de comércio eletrônico<br>• Monitoramento |
| **7. Controle de Acesso** | • Requisitos de negócios para controle de acesso<br>• Gerenciamento de acesso de usuário<br>• Responsabilidades dos usuários<br>• Controle de acesso à rede<br>• Controle de acesso ao sistema operacional<br>• Controle de acesso à aplicação e à informação<br>• Computação móvel e trabalho remoto |
| **8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação** | • Requisitos de segurança de sistemas de informação<br>• Processamento correto nas aplicações<br>• Controles criptográficos<br>• Segurança dos arquivos do sistema<br>• Segurança em processos de desenvolvimento e suporte<br>• Gestão de vulnerabilidades técnicas |
| **9. Gestão de Incidentes de Segurança da Informação** | • Notificação de fragilidades e eventos de segurança da informação<br>• Gestão de incidentes de segurança da informação e melhorias |
| **10.Gestão da Continuidade do Negócio** | • Aspectos da gestão da continuidade do negócio, relativos à segurança da informação |
| **11. Conformidade** | • Conformidade com requisitos legais |

| | |
|---|---|
| | • Conformidade com normas e políticas de segurança da informação e conformidade técnica<br>• Considerações quanto à auditoria de sistemas de informação |

## Auditoria, Vunerabilidade e Conformidade

Existem algumas definições que permeiam o conceito de auditoria. Entretanto, vamos nos basear na NBR ISO 19011[3] que define auditoria como um processo sistemático, documentado e independente para obter evidências de auditoria e avaliá-las objetivamente de modo a determinar a extensão na qual os critérios de auditoria são atendidos.

As evidências de auditoria: são registros, apresentação de fatos ou outras informações, pertinentes aos critérios de auditoria. A auditoria pode ser quantitativa ou qualitativa. Já os critérios de auditoria: consistem em um conjunto de políticas, procedimentos ou requisitos. Os critérios de auditoria são usados como uma referência contra a qual a evidência da auditoria é comparada.

A NBR ISO 19011 apresenta alguns princípios, relacionados aos auditores, possibilitando que sejam fornecidas conclusões de auditoria relevantes e suficientes e permitindo que auditores trabalhem de forma independente e cheguem a conclusões semelhantes em situações semelhantes.

**Conduta ética**: consiste na alma do profissional, confiança, integridade, confidencialidade e discrição. A ética consiste em uma característica inerente às ações do ser humano, tornando-se um componente fundamental à sociedade.

**Obrigação**: existe a obrigação de reportar com veracidade e exatidão todas as informações pertinentes à auditoria, relacionadas com as constatações e as conclusões da auditoria e seus respectivos relatórios.

**Consciência profissional**: os auditores devem ter a preocupação de realizar as tarefas da forma mais profissional, de acordo com a importância e a confiança depositada em uma auditoria.

**Independência**: é a base para a imparcialidade e objetividade das conclusões de uma auditoria, porque os auditores são independentes em relação ao que será auditado, assim como não se ligam aos interesses e às tendências apresentadas.

**Evidência**: a evidência de auditoria pode ser verificada, pois ela é realizada com base em amostras de informações que se encontram disponíveis.

### Tipos de Auditoria

[3] NBR ISO 19011. Diretrizes para auditorias de sistema de gestão da qualidade, NBR. 2002.

Os autores Neto e Solonca (2007)[4] apresentam um quadro com os tipos de auditoria, separando-os em 3 classes abrangentes: forma de abordagem; órgão fiscalizador e área envolvida.

## QUANTO A FORMA DE ABORDAGEM

**Auditoria Horizontal** – Auditoria com tema específico, realizada em várias entidades ou serviços, paralelamente.

**Auditoria Orientada** – Foca em uma atividade específica qualquer ou atividades com fortes indícios de fraudes ou erros.

## QUANTO AO ÓRGÃO FISCALIZADOR:

**Auditoria Interna** – Auditoria realizada por um departamento interno, responsável pela verificação e avaliação dos sistemas e procedimentos internos de uma entidade. Um de seus objetivos é reduzir a probabilidade de fraudes, erros, práticas ineficientes ou ineficazes. Esse serviço deve ser independente e prestar contas diretamente à classe executiva da corporação.

**Auditoria Externa** – Auditoria realizada por uma empresa externa e independente da entidade que está sendo fiscalizada, com o objetivo de emitir um parecer sobre a gestão de recursos da entidade, sua situação financeira, a legalidade e regularidade de suas operações.

**Auditoria Articulada** – Trabalho conjunto de auditorias internas e externas, devido à superposição de responsabilidades dos órgãos fiscalizadores, caracterizado pelo uso comum de recursos e comunicação recíproca dos resultados.

## QUANTO A ÁREA ENVOLVIDA:

**Auditoria de programas de governo** – Acompanhamento, exame e avaliação da execução de programas e projetos governamentais. Auditoria do planejamento estratégico – verifica se os principais objetivos da entidade são atingidos e se as políticas e estratégias são respeitadas.

**Auditoria Administrativa** – Engloba o plano da organização, seus procedimentos, diretrizes e documentos de suporte à tomada de decisão.

**Auditoria Contábil** – É relativa à fidedignidade das contas da instituição. Essa auditoria, consequentemente, tem como finalidade fornecer alguma garantia de que as operações e o acesso aos ativos se efetuem de acordo com as devidas autorizações.

**Auditoria Financeira** – Conhecida também como auditoria das contas. Consiste na análise das contas, da situação financeira, da legalidade e regularidade das operações e aspectos contábeis, financeiros, orçamentários e patrimoniais, verificando se todas as operações foram corretamente autorizadas, liquidadas, ordenadas, pagas e registradas. Auditoria de legalidade – conhecida como auditoria de conformidade. Consiste

[4] NETO, Abílio Bueno; SOLONCA, Davi. Auditoria de sistemas informatizados. Palhoça: UnisulVirtual, 2007.

na análise da legalidade e regularidade das atividades, funções, operações ou gestão de recursos, verificando se estão em conformidade com a legislação em vigor.

**Auditoria Operacional** – Incide em todos os níveis de gestão, nas fases de programação, execução e supervisão, sob a ótica da economia, eficiência e eficácia. Analisa também a execução das decisões tomadas e aprecia até que ponto os resultados pretendidos foram atingidos.

**Auditoria da Tecnologia da Informação** – Tipo de auditoria essencialmente operacional, por meio da qual os auditores analisam os sistemas de informática, o ambiente computacional, a segurança de informações e o controle interno da entidade fiscalizada, identificando seus pontos fortes e deficiências.

## Termos Utilizados em Auditoria

Vamos nos basear nos termos apresentados por DIAS (2000)[5] no livro Segurança e auditoria da tecnologia da informação.

- Campo: está relacionado ao objeto a ser fiscalizado, período e tipo da auditoria.
- Âmbito: define o grau de alcance e a profundidade dos trabalhos.
- Área de verificação: dá limites aos temas da auditoria, em função da organização a ser fiscalizada e do tipo da auditoria.
- Controle: é a fiscalização exercida sobre as atividades das pessoas, departamentos, produtos, e outros, de forma que as atividades executadas ou produtos estejam dentro das normas preestabelecidas.

**Três tipos de controle são exercidos:**
Preventivo – previne erros e invasões. (Exemplo: identificação e autenticação de usuários do sistema a partir da utilização de senhas);
Detector – detecta erros, tentativas de invasões, etc. (arquivos logs, realização de controle de acesso de usuários);
Corretivo – reduz o impacto causado por falhas ou erros, fazendo a correção necessária (política de segurança, plano de contingência).

- Objetivos de controle: são as finalidades de controle a serem atingidas, ou aspectos negativos a serem evitados em cada transação, atividade ou função fiscalizada.
- Procedimentos de auditoria: é o conjunto de verificações e investigações que permitem obter e analisar as informações necessárias ao parecer do auditor.
- Achados de auditoria: são fatos a serem considerados como importantes para o auditor.
- Papéis de trabalho: são registros que evidenciam atos e fatos observados pelo auditor.
- Recomendações de auditoria: realizadas na fase de relatório, são as medidas corretivas que podem ou devem ser executadas para corrigir as falhas detectadas.

[5] DIAS, Cláudia. Segurança e auditoria da tecnologia da informação. Rio de Janeiro: Excel Books, 2000.

# APOSTA ESTRATÉGICA

*A ideia desta seção é apresentar os pontos do conteúdo que mais possuem chances de serem cobrados em prova, considerando o histórico de questões da banca em provas de nível semelhante à nossa, bem como as inovações no conteúdo, na legislação e nos entendimentos doutrinários e jurisprudenciais*[6].


A norma ISO 27002 possui 11 seções, 39 categorias e 133 controles. Abaixo temos uma tabela com a relação entre as seções e as categorias.

| Seção | Categoria |
|---|---|
| **1. Política de Segurança da Informação** | • Política de segurança da informação |
| **2. Organizando a Segurança da Informação** | • Infraestrutura da segurança da informação<br>• Partes externas |
| **3. Gestão de Ativos** | • Responsabilidade pelos ativos<br>• Classificação das informações |
| **4. Segurança em Recursos Humanos** | • Antes da contratação<br>• Durante a contratação<br>• Encerramento ou mudança da contratação |
| **5. Segurança Física e do Ambiente** | • Áreas seguras<br>• Segurança dos equipamentos |
| **6. Gerenciamento das Operações e Comunicações** | • Procedimentos e responsabilidades operacionais<br>• Gerenciamento de serviços terceirizados<br>• Planejamento e aceitação dos sistemas<br>• Proteção contra códigos maliciosos e códigos móveis<br>• Cópias de segurança<br>• Gerenciamento da segurança em redes<br>• Manuseio de mídias |

[6] Vale deixar claro que nem sempre será possível realizar uma aposta estratégica para um determinado assunto, considerando que às vezes não é viável identificar os pontos mais prováveis de serem cobrados a partir de critérios objetivos ou minimamente razoáveis.

| | |
|---|---|
| | • Troca de informações<br>• Serviços de comércio eletrônico<br>• Monitoramento |
| **7. Controle de Acesso** | • Requisitos de negócios para controle de acesso<br>• Gerenciamento de acesso de usuário<br>• Responsabilidades dos usuários<br>• Controle de acesso à rede<br>• Controle de acesso ao sistema operacional<br>• Controle de acesso à aplicação e à informação<br>• Computação móvel e trabalho remoto |
| **8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação** | • Requisitos de segurança de sistemas de informação<br>• Processamento correto nas aplicações<br>• Controles criptográficos<br>• Segurança dos arquivos do sistema<br>• Segurança em processos de desenvolvimento e suporte<br>• Gestão de vulnerabilidades técnicas |
| **9. Gestão de Incidentes de Segurança da Informação** | • Notificação de fragilidades e eventos de segurança da informação<br>• Gestão de incidentes de segurança da informação e melhorias |
| **10.Gestão da Continuidade do Negócio** | • Aspectos da gestão da continuidade do negócio, relativos à segurança da informação |
| **11. Conformidade** | • Conformidade com requisitos legais<br>• Conformidade com normas e políticas de segurança da informação e conformidade técnica<br>• Considerações quanto à auditoria de sistemas de informação |

## Itens da Política de Segurança

Para elaborar uma política de segurança, é necessário estabelecer alguns pontos indispensáveis:

- **Responsáveis**

Deve ser estabelecido que são os responsáveis não apenas pelo monitoramento, mas também pela elaboração, divulgação e revisão das políticas de segurança.

- **Tipos de Informações**

As informações devem ser classificadas de forma parecida com os documentos físicos: pública, interna, confidencial e secreta. Com base na classificação dos dados é que serão definidos os níveis de acesso de cada colaborador às informações, como os aplicativos de negócios serão implementados e qual o impacto que um incidente com aqueles dados pode gerar para a reputação da empresa. Mais adiante veremos as Políticas de classificação da informação.

- **Níveis de acesso**

A definição dos níveis de acesso deve considerar três pontos principais: Quem acessa? Como acessa? Quando acessa? A resposta para essas perguntas separa o nível / perfil de acesso de cada uma das pessoas.

Com os pontos citados acima, podemos concluir que a política de segurança deve considerar não apenas os ataques, mas todos os elementos que dizem respeito aquilo que é essencial quando o objetivo é combater situações adversas. A disponibilidade da infraestrutura da organização também deve ser considerada (HUR, 1999 apud NAKAMURA e DE GEUS, 2000)[7]:

- Vigilância: significa que todos da organização são responsáveis por garantir e fiscalizar a segurança de informação;
- Atitude: significa a postura e a conduta quanto à segurança. Todos os envolvidos devem ter a consciência que a política de segurança não tem efeitos se ela não for adotada de forma certa. É necessário treinamento e conscientização dos funcionários quanto à importância de se seguir a política de segurança estabelecida;
- Estratégia: significa ser criativo na elaboração da política de segurança além de ser adaptativa às mudanças no ambiente. A estratégia leva em conta também a produtividade dos usuários. Uma boa política não deve interferir negativamente no andamento dos negócios da organização;
- Tecnologia: a solução tecnológica deve ser flexível e adaptativa para suprir as necessidades da organização. Qualquer tecnologia desatualizada pode causar uma falsa sensação de segurança.

Em 2008 o Tribunal de Contas da União afirmou que o conteúdo da Política de Segurança da Informação aplicável à Administração Pública Federal direta ou indireta varia de acordo com a organização. Entretanto, alguns elementos são comuns nessas políticas:

- Definição de segurança de informações e de sua importância como mecanismo que possibilita o compartilhamento de informações;
- Declaração do comprometimento da alta administração com a Política de Segurança da Informação, apoiando suas metas e princípios;
- Objetivos de segurança da organização;
- Definição de responsabilidades gerais na gestão de segurança de informações;
- Orientações sobre análise e gerência de riscos;
- Princípios de conformidade dos sistemas computacionais com a Política de Segurança da Informação;
- Padrões mínimos de qualidade que esses sistemas devem possuir;
- Políticas de controle de acesso a recursos e sistemas computacionais;

[7] NAKAMURA, E. T.; DE GEUS, P. L. Um modelo de segurança de redes para ambientes cooperativos. Instituto de Computação – Universidade Estadual de Campinas. Campinas, SP. 2000.

- Classificação das informações (de uso irrestrito, interno, confidencial e secretas);
- Procedimentos de prevenção e detecção de vírus;
- Princípios legais que devem ser observados quanto à tecnologia da informação (direitos de propriedade de produção intelectual, direitos sobre software, normas legais correlatas aos sistemas desenvolvidos, cláusulas contratuais);
- Princípios de supervisão constante das tentativas de violação da segurança de informações;
- Consequências de violações de normas estabelecidas na política de segurança;
- Princípios de gestão da continuidade do negócio;
- Plano de treinamento em segurança de informações.

Imprima o capítulo Aposta Estratégica separadamente e dedique um tempo para absolver tudo o que está destacado nessas duas páginas. Caso tenha alguma dúvida, volte ao Roteiro de Revisão e Pontos do Assunto que Merecem Destaque. Se ainda assim restar alguma dúvida, não hesite em me perguntar no fórum.

# QUESTÕES ESTRATÉGICAS

*Nesta seção, apresentamos e comentamos uma amostra de questões objetivas selecionadas estrategicamente: são questões com nível de dificuldade semelhante ao que você deve esperar para a sua prova e que, em conjunto, abordam os principais pontos do assunto.*

*A ideia, aqui, não é que você fixe o conteúdo por meio de uma bateria extensa de questões, mas que você faça uma boa revisão global do assunto a partir de, relativamente, poucas questões.*


**1. CEBRASPE (CESPE) - Analista Judiciário (STM)/Apoio Especializado/Análise de Sistemas/2018**

Julgue o item seguinte, relativo a mecanismos de segurança em um ambiente computacional.

A análise de riscos define os direitos e as responsabilidades de cada usuário em relação à segurança dos recursos computacionais que utiliza e às penalidades às quais cada um deles está sujeito.

**Comentários**

De acordo com a cartilha Cert.br é a Política de Segurança que define os direitos e as responsabilidades de cada um em relação à segurança dos recursos computacionais que utiliza e as penalidades às quais está sujeito, caso não a cumpra.

**Gabarito: errado.**

**2. CEBRASPE (CESPE) - Analista Judiciário (STJ)/Apoio Especializado/Suporte em Tecnologia da Informação/2015**

Julgue o item seguinte, acerca de política de segurança da informação e sistemas de gestão de segurança da informação.

A política de segurança da informação de uma organização é um documento único que concentra todo o direcionamento relacionado à proteção dos ativos de informação, incluindo recomendações técnicas e definição de mecanismos para proteção de tais ativos.

**Comentários**

De acordo com a Norma ISO 27002:2013, " Políticas de segurança da informação **PODEM** ser emitidas em um único documento, "política de segurança da informação" ou como um conjunto de documentos individuais, relacionados." Ou seja, pode ser um documento único, não é uma obrigação.

Portanto, assertiva incorreta.

**Gabarito: errado.**

---

**3. CEBRASPE (CESPE) - Analista Judiciário (STJ)/Apoio Especializado/Suporte em Tecnologia da Informação/2015**

Com relação à gestão de continuidade de negócio e ao gerenciamento de incidentes de segurança da informação, julgue o item subsequente.

No processo de gestão de incidentes de segurança da informação, as atividades relacionadas com a detecção de incidentes são responsáveis pela coleta de informações relacionadas a ocorrências de segurança da informação.

**Comentários**

A atividade de detecção e comunicação envolve a detecção (normalmente com a ajuda de ferramentas de automação), coleta de informações associadas e relatórios sobre ocorrências de segurança da informação, vulnerabilidades de segurança que não foram antes exploradas, assim como os incidentes propriamente ditos, sejam eles provocados de forma intencional ou não intencional. De maneira simplificada os objetivos desta atividade são detectar ocorrências, vulnerabilidades e os próprios incidentes.

Portanto, assertiva correta.

**Gabarito: certo.**

---

**4. CEBRASPE (CESPE) - Analista Judiciário (TJDFT)/Apoio Especializado/Análise de Sistemas/2015**

Julgue o próximo item, relativo a políticas de segurança da informação.

Os objetivos do controle de segurança da informação devem ser estabelecidos com base em gerenciamento de riscos.

**Comentários**

A segurança da informação tem o objetivo de preservar ou proteger informações de possíveis ameaças, na intuição de garantir a continuidade e minimizar os danos, sendo monitorado pelo processo de gerenciamento de riscos, onde esse processo tem por função organizar seu processamento, armazenagem e transmissão de informações.

**Gabarito: certo.**

---

**5. CEBRASPE (CESPE) - Analista Judiciário (TJDFT)/Apoio Especializado/Análise de Sistemas/2015**

Julgue o próximo item, relativo a políticas de segurança da informação.

O documento que descreve a política de segurança da informação de uma organização deve ser classificado de forma a permitir o acesso a diretores e a colaboradores estratégicos — como gerentes intermediários. Os colaboradores das áreas operacionais devem receber orientações, mas o acesso ao documento deve ser coibido.

**Comentários**

Segundo a Norma ISO/IEC 27002, " Convém que todos os funcionários, fornecedores e terceiros sejam alertados sobre sua responsabilidade de notificar qualquer evento de segurança da informação o mais rapidamente possível. Convém que eles também estejam cientes do procedimento para notificar os eventos de segurança da informação e do ponto de contato designado para este fim." Dessa forma, além de avisos e palestras de conscientização, o documento que descreve a política de segurança da informação de uma empresa deve estar disponível para todos os funcionários, inclusive para terceirizados e prestadores de serviço.

**Gabarito: errado.**

---

**6. CEBRASPE (CESPE) - Analista Judiciário (TJDFT)/Apoio Especializado/Análise de Sistemas/2015**

Julgue o próximo item, relativo a políticas de segurança da informação.

Para que se implemente a política de segurança da informação, a alta direção deve emitir uma declaração de comprometimento com essa política.

**Comentários**

De acordo com a Norma ISO/IEC 17799 sobre a política de segurança da informação:

Objetivo: Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Convém que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização.

**Gabarito: certo.**

---

**7. CEBRASPE (CESPE) - Analista Judiciário (TJ SE)/Administrativa/Segurança da Informação/2014**

Acerca dos procedimentos de segurança da informação, julgue o seguinte item.

Os procedimentos de segurança da informação são componentes táticos da política de segurança da informação.

**Comentários**

A norma ABNT NBR ISO/IEC 27001 estabelece que a segurança da informação esteja implementada e operada de acordo com as políticas e procedimentos da organização. Dessa forma, os procedimentos de segurança da informação não são componentes táticos da política de segurança da informação, são operacionais.

**Gabarito: errado.**

---

**8. CEBRASPE (CESPE) - Analista Judiciário (TJ SE)/Administrativa/Segurança da Informação/2014**

Considerando o que dispõe a NBR ISO/IEC 27001, julgue o próximo item.

Essa norma aborda o processo que estabelece, implementa, opera, monitora, analisa criticamente, mantém e melhora o sistema gestão de segurança da informação de uma organização.

**Comentários**

A NBR ISO/IEC 27001 recomenta o seguinte:

"Esta Norma foi preparada para prover requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI). A adoção de um SGSI é uma decisão estratégica para uma organização. "

Desse modo, em acordo com o exposto, visualiza-se que está correta essa questão ao afirmar que a NBR ISO/IEC 27001 aborda o processo que estabelece, implementa, opera, monitora, analisa criticamente, mantém e melhora o sistema gestão de segurança da informação de uma organização.

**Gabarito: certo.**

---

**9. CEBRASPE (CESPE) - Analista Judiciário (TJ SE)/Administrativa/Segurança da Informação/2014**

No que se refere às políticas de segurança da informação, julgue o item subsequente, de acordo com a NBR ISO/IEC 27002.

Para que haja confiabilidade, o documento de política de segurança da informação deve permanecer inalterado ao longo do tempo.

**Comentários**

A norma NBR ISO/IEC 27002 estabelece o seguinte:

*"A informação tem um ciclo de vida natural, desde a sua criação e origem, armazenagem, processamento, uso e transmissão, até a sua eventual destruição ou obsolecência. O valor e os riscos aos ativos podem variar durante o tempo de vida da informação (por exemplo, revelação não autorizada ou roubo de balanços financeiros de uma companhia, é muito menos importante depois que elas são formalmente publicadas), porém a segurança da informação permanece importante em algumas etapas de todos os estágios.*

*Sistemas de informação têm ciclos de vida nos quais eles são concebidos, especificados, projetados, desenvolvidos, testados, implementados, usados, mantidos e, eventualmente, retirados do serviço e descartados. Convém que a segurança da informação seja considerada em cada estágio. Desenvolvimentos de sistemas novos e mudanças nos sistemas existentes são oportunidades para as organizações atualizarem e melhorarem os controles de segurança, levando em conta os incidentes reais e os riscos de segurança da informação, projetados e atuais."*

Assim, ante o exposto, fica claro que o documento de política de segurança da informação deve acompanhar o ciclo de vida natural da informação, bem como os ciclos de vida dos Sistemas de Informação.

**Gabarito: errado.**

---

**10. CEBRASPE (CESPE) - Analista Judiciário (TJ SE)/Administrativa/Segurança da Informação/2014**

No que se refere às políticas de segurança da informação, julgue o item subsequente, de acordo com a NBR ISO/IEC 27002.

O documento de política de segurança da informação de uma empresa deve definir as políticas dessa área, com base nos objetivos do negócio, na legislação e na regulamentação pertinente.

**Comentários**

A norma NBR ISO/IEC 27002 preconiza o seguinte:

"Políticas de segurança da informação podem ser emitidas em um único documento, "política de segurança da informação" ou como um conjunto de documentos individuais, relacionados."

Essa norma também afirma que a orientação da direção para segurança da informação deve prover uma orientação e apoio da direção para a segurança da informação, de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Dessa forma, em acordo com o exposto, visualizamos que realmente o documento de política de segurança da informação de uma empresa deve definir as políticas dessa área, com base nos objetivos do negócio, na legislação e na regulamentação pertinente.

**Gabarito: certo.**

---

**11. CEBRASPE (CESPE) - Analista Judiciário (TJ SE)/Administrativa/Segurança da Informação/2014**

Ainda acerca de política de segurança da informação, julgue o item a seguir, com base na NBR ISO/IEC 27002.

A situação de ações preventivas é uma saída da análise crítica da política de segurança da informação.

**Comentários**

A NBR ISO/IEC 27002 traz o seguinte sobre a Análise crítica das políticas para segurança da informação:

"Controle

Convém que as políticas para a segurança da informação sejam analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

Diretrizes para implementação

Convém que cada política de segurança da informação tenha um gestor que tenha aprovado a responsabilidade pelo desenvolvimento, análise crítica e avaliação das políticas de segurança da informação.

Convém que a análise crítica inclua a avaliação de oportunidades para melhoria da política de segurança da informação da organização e tenha um enfoque para gerenciar a segurança da informação em resposta às mudanças ao ambiente organizacional, às circunstâncias do negócio, às condições legais, ou ao ambiente de tecnologia.

Convém que a análise crítica das políticas de segurança da informação leve em consideração os resultados da análise crítica pela direção.

Convém que seja obtida a aprovação da direção para a política revisada."

**Gabarito: errado.**

---

**12. CEBRASPE (CESPE) - Analista Judiciário (TJ SE)/Administrativa/Segurança da Informação/2014**

Ainda acerca de política de segurança da informação, julgue o item a seguir, com base na NBR ISO/IEC 27002.

O documento de política de segurança da informação deverá conter a definição das responsabilidades gerais da gestão de segurança da informação. As responsabilidades específicas, como a gestão de incidentes de segurança da informação, devem ser contempladas em manuais de procedimentos.

**Comentários**

De acordo com NBR ISO/IEC 27002, em seu capítulo 5 onde trata da Política de segurança da informação, na seção 5.1.1, sobre o documento da política de segurança da informação:

5.1.1 Documento da política de segurança da informação

Convém que o documento da política contenha declarações relativas a:

[...]

e) definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança da informação;

[...]

Portanto, o documento da política de segurança da informação fine sim as responsabilidades específicas.

**Gabarito: errado.**

# QUESTIONÁRIO DE REVISÃO E APERFEIÇOAMENTO

*A ideia do questionário é elevar o nível da sua compreensão no assunto e, ao mesmo tempo, proporcionar uma outra forma de revisão de pontos importantes do conteúdo, a partir de perguntas que exigem respostas subjetivas.*

*São questões um pouco mais desafiadoras, porque a redação de seu enunciado não ajuda na sua resolução, como ocorre nas clássicas questões objetivas.*

*O objetivo é que você realize uma autoexplicação mental de alguns pontos do conteúdo, para consolidar melhor o que aprendeu ;)*

*Além disso, as questões objetivas, em regra, abordam pontos isolados de um dado assunto. Assim, ao resolver várias questões objetivas, o candidato acaba memorizando pontos isolados do conteúdo, mas muitas vezes acaba não entendendo como esses pontos se conectam.*

*Assim, no questionário, buscaremos trazer também situações que ajudem você a conectar melhor os diversos pontos do conteúdo, na medida do possível.*

*É importante frisar que não estamos adentrando em um nível de profundidade maior que o exigido na sua prova, mas apenas permitindo que você compreenda melhor o assunto de modo a facilitar a resolução de questões objetivas típicas de concursos, ok?*

*Nosso compromisso é proporcionar a você uma revisão de alto nível!*

*Vamos ao nosso questionário:*

## Perguntas

1. **Qual a definição de cada princípio da segurança da informação? Cite exemplos relacionados a cada princípio.**

## Perguntas com respostas

1) **Qual a definição de cada princípio da segurança da informação? Cite exemplos relacionados a cada princípio.**

Disponibilidade - Princípio que garante que a informação estará sempre disponível.

Integridade - Princípio que garante que as informações serão guardadas ou enviadas em sua forma original, sem sofrer alterações.

Confidencialidade - Princípio que garante o sigilo da informação com a capacidade de controlar o acesso, assegurando que elas só serão acessadas por pessoas autorizadas. Ou seja, é a garantia que as informações só serão acessadas através de uma senha.

Autenticidade - Princípio que permite verificar a identidade de uma pessoa em um sistema, garantindo a veracidade das informações.

> Existe um material desenvolvido pelo Comitê Gestor da Internet no Brasil - CGI.br, que aborda os principais pontos cobrados em concursos. Esse material está disponível em: *https://cartilha.cert.br/* e serve como base para o seu estudo sobre Segurança da Informação. Não é um material extenso e os textos são bastante didáticos para facilitar a compreensão.

...

Forte abraço e bons estudos.

**"Hoje, o 'Eu não sei', se tornou o 'Eu ainda não sei'"**

(Bill Gates)

# Thiago Cavalcanti

**Face**: www.facebook.com/profthiagocavalcanti
**Insta**: www.instagram.com/prof.thiago.cavalcanti
**YouTube**: youtube.com/profthiagocavalcanti

# ESSA LEI TODO MUNDO CONHECE:
# PIRATARIA É CRIME.

**Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.**

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.

**Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.**