Estratégia Concursos

Aula 00

SEFAZ-MG (Auditor Fiscal - Tecnologia da Informação) Passo de Segurança da Informação

Autor:
Thiago Rodrigues Cavalcanti

09 de Fevereiro de 2023

1. Gestão de segurança da informação. 2. Gestão de continuidade do negócio. 3. Gestão de Identidade e Acesso. 4. Gestão de Riscos de Segurança da Informação

Sumário

ANÁLISE ESTATÍSTICA

Inicialmente, convém destacar os percentuais de incidência de todos os assuntos previstos no nosso curso – quanto maior o percentual de cobrança de um dado assunto, maior sua importância:

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*

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

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.

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.

Não 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.

ESCLARECENDO

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”.

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;
- 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;

[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.

- 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.

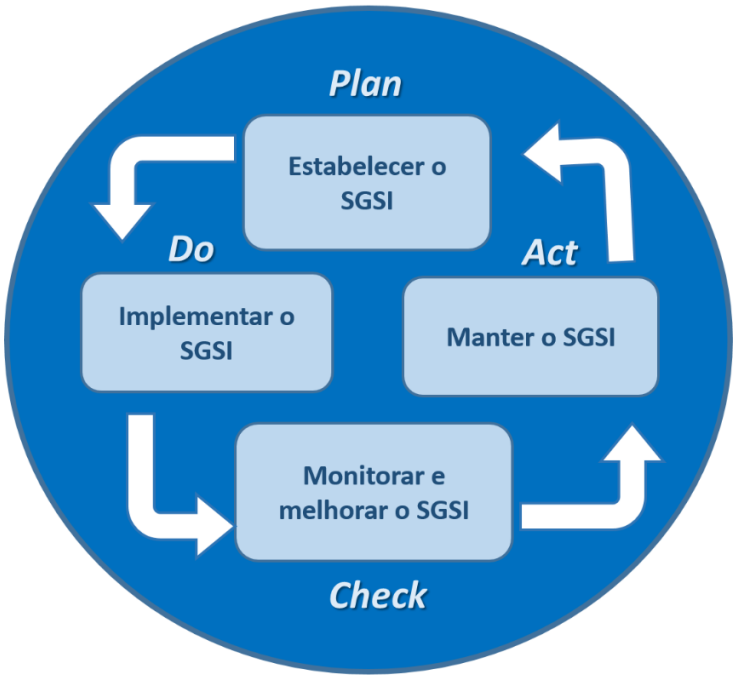
Assim, como você pode ver, o processo de classificação pode ser complexo, mas ele não tem que ser incompreensível. A ISO 27001 dá liberdade para o responsável pela classificação criar as próprias regras e definir como as informações serão classificadas.

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.

ISO 27001 - Requisitos para Sistemas de Gestão de Segurança da Informação

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 - Melhores práticas para implantação do Sistema de Gestão de Segurança da Informação

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.

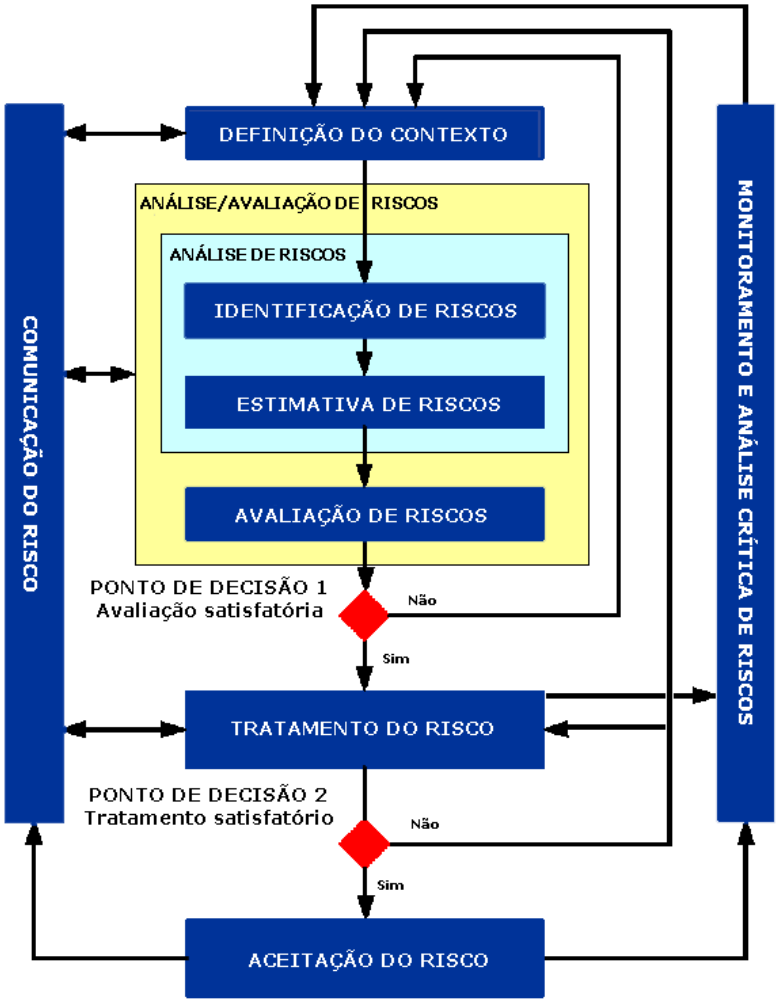
Seção	Categoria
1. Política de Segurança da Informação	• Política de segurança da informação
2. Organizando a Segurança da Informação	• Infraestrutura da segurança da informação • Partes externas
3. Gestão de Ativos	• Responsabilidade pelos ativos • Classificação das informações
4. Segurança em Recursos Humanos	• Antes da contratação • Durante a contratação • Encerramento ou mudança da contratação
5. Segurança Física e do Ambiente	• Áreas seguras • Segurança dos equipamentos
6. Gerenciamento das Operações e Comunicações	• Procedimentos e responsabilidades operacionais • Gerenciamento de serviços terceirizados • Planejamento e aceitação dos sistemas • Proteção contra códigos maliciosos e códigos móveis • Cópias de segurança • Gerenciamento da segurança em redes • Manuseio de mídias • Troca de informações • Serviços de comércio eletrônico • Monitoramento
7. Controle de Acesso	• Requisitos de negócios para controle de acesso • Gerenciamento de acesso de usuário • Responsabilidades dos usuários • Controle de acesso à rede • Controle de acesso ao sistema operacional • Controle de acesso à aplicação e à informação • Computação móvel e trabalho remoto

8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	• Requisitos de segurança de sistemas de informação • Processamento correto nas aplicações • Controles criptográficos • Segurança dos arquivos do sistema • Segurança em processos de desenvolvimento e suporte • Gestão de vulnerabilidades técnicas
9. Gestão de Incidentes de Segurança da Informação	• Notificação de fragilidades e eventos de segurança da informação • 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 • Considerações quanto à auditoria de sistemas de informação

ISO 27005 - Gestão de Riscos de Segurança da Informação (GRSI)

A norma ISO 27005 trata da **Gestão de Riscos de Segurança da Informação (GRSI).**

Para já termos uma noção, a própria norma nos traz uma visão geral de do processo de gestão de riscos de SI.



FIM DA PRIMEIRA OU DAS DEMAIS INTERAÇÕES

O processo de gestão de riscos de SI consiste, seguindo o fluxo da imagem acima:

1. Definição do contexto;
2. Processo de avaliação dos riscos;
3. Tratamento do risco;
4. Aceitação do risco;
5. Comunicação e consulta do risco;
6. Monitoramento e análise crítica de riscos;

Destaca-se que tal processo pode ser iterativo para o processo de avaliação de riscos e/ou para as atividades e tratamento do risco. Obviamente, como todo processo iterativo, busca-se aprimorar as rotinas e processos a que se propõe na iteração.

Um outro ponto que merece a nossa atenção é em relação à comunicação. Durante o processo de GRSI, é importante que os riscos e a forma com que são tratados sejam comunicados ao pessoal das áreas operacionais e gestores apropriados.

Tais informações são fundamentais para uma série de ações, principalmente aqueles relacionados à gestão de incidentes e problemas, gerando possíveis reduções a riscos associados a estes e seus respectivos impactos e prejuízos.

A conscientização dos gestores e pessoal no que diz respeito aos riscos, à natureza dos controles aplicados para mitiga-los e as áreas definidas como de interesse pela organização, auxilia a lidar com os incidentes e eventos não previstos da maneira mais efetiva.

Convém que os resultados detalhados de cada atividade do processo de gestão de riscos de segurança da informação, assim como as decisões sobre o processo de avaliação de riscos e sobre o tratamento de riscos sejam documentados.

Um outro ponto que merece nossa atenção é em relação ao alinhamento do processo do SGSI e do processo de GRSI, ambos vinculados ao ciclo do PDCA.

Desse modo, a norma define da seguinte forma:

Processos do SGSI	Processos do GRSI
Planejar	Definição do Contexto Processo de Avaliação dos Riscos Definição do Plano de Tratamento dos Riscos Aceitação do Risco
Executar	Implementação do Plano de Tratamento do Risco
Verificar	Monitoramento contínuo e análise crítica de riscos
Agir	Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação

Definição do contexto

Considerações gerais

ENTRADA - Todas as informações sobre a organização são relevantes para a definição do contexto da gestão de risco de Segurança da Informação.

AÇÃO - Convém que o contexto externo e interno para a gestão de riscos de Segurança da Informação seja estabelecido: o que envolve a definição dos critérios básicos necessários para a gestão de riscos de segurança da informação, a definição do escopo e dos limites e o estabelecimento de uma organização apropriada para operar a gestão de riscos de segurança da informação.

Nesse sentido, a norma nos traz uma relação de possíveis propósitos que podem ser considerados a aplicação da GRSI, quais sejam:

A. Suporte a um SGSI;
B. Conformidade Legal e evidência da devida diligência ("*due diligence*");
C. Preparação de um Plano de Continuidade de Negócios;
D. Preparação de um Plano de Resposta a Incidentes;
E. Descrição dos requisitos de segurança da informação para um produto, um serviço ou um mecanismo.

Lembrando sempre que essas relações de 5 itens da norma são sempre um prato cheio para questões de múltipla escolha. Portanto, memorizem esses propósitos. São um tanto intuitivos.

Critérios básicos

Abordagem da gestão de riscos

Dependendo do escopo e dos objetivos da gestão de riscos, diferentes métodos podem ser aplicados. O método também pode ser diferente para cada iteração do processo.

A norma traz ainda que um método de gestão apropriado seja selecionado ou ainda desenvolvido. Em termos de eficácia, ela deve considerar critérios básicos como:

Critérios de avaliação de riscos
Critérios de impacto
Critérios de aceitação do risco

Processo de avaliação de riscos de segurança da informação

Descrição geral do processo de avaliação de riscos de segurança da informação

ENTRADA - Critérios básicos, o escopo e os limites, e a organização do processo de gestão de riscos de segurança da informação que se está definido.

AÇÃO - Convém que os riscos sejam identificados, quantificados ou descritos qualitativamente, priorizados em função dos critérios de avaliação de riscos e dos objetivos relevantes da organização.

Desse modo, a norma define que o processo de AVALIAÇÃO DOS RISCOS consiste nas seguintes atividades:

> Identificação de riscos
>
> Análise de riscos
>
> Avaliação de riscos

Falaremos um pouco mais delas nas próximas seções.

O processo de avaliação de riscos é executado frequentemente em duas (ou mais) iterações. Primeiramente, faz-se uma avaliação de alto nível para identificas os riscos potencialmente altos, os quais merecem uma avaliação mais aprofundada.

A segunda iteração pode considerar com mais profundidade esses riscos potencialmente altos revelados na primeira iteração. Se ela não fornece informações suficientes para avaliar o risco, então análises adicionais detalhadas são executadas, provavelmente em parte do escopo total e possivelmente usando um outro método.

Identificação de riscos

A norma trata de maneira bem objetiva os aspectos relacionados à Identificação dos ativos.

Aqui a nossa primeira observação no que tange à identificação dos riscos.

Ela é dividida em 5 identificações:

> a) Identificação dos Ativos;
> b) Identificação das Ameaças;
> c) Identificação dos Controles existentes;
> d) Identificação das vulnerabilidades;
> e) Identificação das consequências;

Como toda boa lista da teoria e 5 itens, não preciso mencionar a importância de termos na ponta da língua esses 5 itens, certo?

AA - CVC

Ativos – **A**meaças – **C**ontroles existentes – **V**ulnerabilidades – **C**onsequências

Para ajudar na memorização, lembrem-se dos alcoólicos anônimos viajam pela CVC!

Vamos conhecer as ENTRADAS e AÇÕES de cada um dos processos de identificação.

a) Identificação dos Ativos:

ENTRADA - Escopo e limites para o processo de avaliação de riscos a ser executado; lista de componentes com responsáveis, localidade, função, etc.

AÇÃO - Convém que os ativos dentro do escopo estabelecido sejam identificados (referência à ISO 270001).

SAÍDA - Uma lista de ativos com riscos a serem gerenciados e uma lista dos processos de negócio relacionados aos ativos e suas relevâncias.

b) Identificação de Ameaças:

ENTRADA - Informações sobre ameaças obtidas a partir da análise crítica de incidentes, dos responsáveis pelos ativos, de usuários e de outras fontes, incluindo catálogos externos de ameaças.

AÇÃO - Convém que as ameaças e suas fontes sejam identificadas.

Uma ameaça tem o potencial de comprometer ativos (como informações, processos e sistemas) e, por isso, também as organizações. Ameaças podem ser de origem natural ou humana e podem ser acidentais ou intencionais. Ambas devem ser identificadas.

A ameaça pode surgir tanto de dentro como de fora da organização.

Algumas ameaças podem afetar mais de um ativo. Nesses casos, elas podem provocar impactos diferentes dependendo de quais ativos são afetados.

SAÍDA - Uma lista de ameaças com a identificação do tipo e da fonte das ameaças.

c) Identificação dos Controles Existentes:

ENTRADA - Documentação dos controles, planos de implementação do tratamento dos riscos.

AÇÃO - Convém que os controles existentes e os planejados sejam identificados.

SAÍDA - Uma lista de todos os controles existentes e planejadas, sua implementação e status de utilização.

d) Identificação das Vulnerabilidades:

ENTRADA - Uma lista de ameaças conhecidas, listas de ativos e controles existentes.

AÇÃO - Convém que as vulnerabilidades que podem ser exploradas por ameaças para comprometer os ativos ou a organização sejam identificadas.

SAÍDA - Uma lista de vulnerabilidades associadas aos ativos, ameaças e controles; uma lista de vulnerabilidades que não se refere a nenhuma ameaça identificada para análise.

e) Identificação das Consequências

ENTRADA - Uma lista de ativos, uma lista de processos do negócio e uma lista de ameaças e vulnerabilidades, quando aplicável, relacionadas aos ativos e sua relevância.

AÇÃO - Convém que as consequências que a perda de confidencialidade, de integridade e de disponibilidade podem ter sobre os ativos sejam identificadas.

Convém que as organizações identifiquem as consequências operacionais de cenários de incidentes em função de (não se limitando a):

1. Investigação e tempo de reparo;
2. Tempo (de trabalho) perdido;
3. Oportunidade perdida;
4. Saúde e Segurança;
5. Custo financeiro das competências específicas necessárias para reparar o prejuízo;
6. Imagem, reputação e valor de mercado.

SAÍDA - Uma lista de cenários de incidentes com suas consequências associadas aos ativos e processos de negócio.

No Anexo B da norma, tem-se exemplos de Identificação, e essa parte, por ter um cunho mais prático, despenca em prova.

A Norma define em seus exemplos, apenas dois tipos de Ativos:

1. PRIMÁRIOS

2. SUPORTE E INFRAESTRUTURA.

Os ativos **PRIMÁRIOS** contemplam:

1. Processos e Atividades de Negócio;
2. Informação;

Os Ativos de **SUPORTE E INFRAESTRUTURA** contemplam:

1. Hardware;
2. Software;
3. Rede;
4. Recursos Humanos;
5. Instalações Físicas;
6. Estrutura da Organização.

Desse modo, para facilitar a memorização, ao lembrarmos dos primários, poderemos, por eliminação, deduzir os de Suporte e Infraestrutura. Muito cuidado com os RECURSOS HUMANOS e ESTRUTURA DA ORGANIZAÇÃO, que, em uma primeira análise, não guardam relação direta com a terminologia de Suporte e Infraestrutura.

Análise de riscos

A análise de Riscos é a segunda etapa no processo de AVALIAÇÃO DOS RISCOS.

a) Metodologias de Análise de Riscos

A análise de riscos pode ser realizada com diferentes graus de detalhamento, dependendo a criticidade dos ativos, da extensão das vulnerabilidades conhecidas e dos incidentes anteriores envolvendo a organização.

Uma metodologia para análise de risco pode ser qualitativa ou quantitativa, ou ainda a combinação das duas, dependendo das circunstâncias.

Na prática, a análise qualitativa é frequentemente utilizada em primeiro lugar para obter uma indicação geral do nível de risco e para revelar os grandes riscos. Isso ocorre, como veremos mais à frente, porque normalmente esse processo é menos complexo e menos oneroso quando comparado com as análises quantitativas.

Em relação às metodologias de análise de Riscos, a norma nos traz dois tipos básicos de metodologias, saber:

1. Análise Qualitativa (Menos Complexa):
    a. Tratará aspectos subjetivos na análise.
    b. Considera a magnitude das consequências potenciais (ex. pequena, média e grande);
    c. Considera a probabilidade dessas consequências ocorrerem;
    d. Possui como vantagem a facilidade de compreensão;
    e. Como desvantagem, podemos elencar o próprio fator subjetivo de classificação, que não é uma regra mais precisa e exata;
    f. Convém que esta análise sempre utilize informações e dados factuais quando disponíveis;
2. Análise Quantitativa (Mais Complexa):
    a. Possui uma escala mais precisa e de valores numéricos, tanto para as consequências como para as probabilidades, buscando dados de diversas fontes;
    b. A qualidade da análise depende da exatidão e da integralidade dos valores numéricos e da validade dos modelos utilizados;
    c. Utiliza dados históricos dos incidentes, sendo esta uma vantagem no relacionamento direto aos objetivos de segurança da informação;
    d. Como desvantagem, é que sempre haverá ausência de dados históricos para novos riscos ou fragilidades. Além disso, quando os dados factuais e auditáveis não estão disponíveis.

b) Avaliação das Consequências

ENTRADA - Uma lista de cenários de incidentes identificados como relevantes, incluindo a identificação de ameaças, vulnerabilidades, ativos afetados e consequências para os ativos e processos de negócio.

AÇÃO - Convém que o impacto sobre o negócio da organização, que pode ser causado por incidentes (possíveis ou reais) relacionados à segurança da informação, seja avaliado levando-se em conta as consequências de uma violação da segurança da informação, como por exemplo: a perda da confidencialidade, da integridade ou da disponibilidade dos ativos.

SAÍDA - Uma lista de consequências avaliadas referentes a um cenário de incidente, relacionadas aos ativos e critérios de impacto.

c) Avaliação da Probabilidade dos Incidentes

ENTRADA - Uma lista de cenários de incidentes identificados como relevantes, incluindo a identificação de ameaças, ativos afetados, vulnerabilidades exploradas e consequências para os ativos e processos do negócio. Além disso, listas com todos os controles existentes e planejados, sua eficácia, implementação e status de utilização.

AÇÃO - Convém que a probabilidade dos cenários de incidentes seja avaliada.

SAÍDA - Probabilidade dos cenários de incidentes.

d) Determinação do Nível de Risco

ENTRADA - Uma lista de cenários de incidentes com suas consequências associadas aos ativos, processos de negócio e suas probabilidades (no método quantitativo e qualitativo).

AÇÃO - Convém que o nível de risco seja estimado para todos os cenários de incidentes considerados relevantes.

SAÍDA - Uma lista de riscos com nível de valores designados.

Avaliação de riscos

Por fim, realiza-se a avaliação de riscos propriamente dita.

Tratamento do risco de segurança da informação

Descrição geral do processo de tratamento do risco

ENTRADA - Uma lista de riscos priorizada, de acordo com os critérios de avaliação de riscos, em relação aos cenários de incidentes que podem levar a esses riscos.

AÇÃO - Convém que controles para MODIFICAR, RETER, EVITAR ou COMPARTILHAR os riscos sejam selecionados e o plano de tratamento do risco seja definido.

Logo de cara vamos destacar as opções de tratamento de riscos. Isso despenca em prova. Então alguns gostam do famoso MNEMONICO MORA COM.

MOdificação do Risco

Retenção do Risco

Ação de evitar o Risco

COMpartilhamento do Risco

Um outro ponto de atenção diz respeito ao fato de que **as quatro opções para o tratamento do risco NÃO são mutuamente exclusivas**.

Às vezes, a organização pode beneficiar-se substancialmente de uma combinação de opções, tais como a redução da probabilidade do risco, a redução de suas consequências e o compartilhamento ou retenção dos riscos residuais.

SAÍDA - O plano de tratamento do risco e os riscos residuais, sujeitos à decisão de aceitação por parte dos gestores da organização.

Modificação do risco

AÇÃO - Convém que o nível de risco seja gerenciado através da inclusão, exclusão, ou alteração de controles, para que o risco residual possa ser reavaliado e então considerado aceitável.

Em geral, os controles podem fornecer um ou mais dos seguintes tipos de proteção: correção, eliminação, prevenção, minimização do impacto, dissuasão, detecção, recuperação, monitoramento e conscientização.

Durante a seleção de controles, é importante pesar o custo de aquisição, implementação, administração, operação, monitoramento e manutenção dos controles em relação ao valor dos ativos sendo protegidos.

Convém que o retorno do investimento, na forma da modificação do risco e da possibilidade de se explorar em novas oportunidades de negócio em função da existência de certos controles, também seja considerado.

Adicionalmente, convém considerar as competências especializadas que possam ser necessárias para definir e implementar novos controles ou modificar os existentes.

Retenção do risco

AÇÃO - Convém que as decisões sobre a retenção do risco, sem outras ações adicionais, sejam tomadas tendo como base a avaliação de riscos.

Se o nível de risco atender aos critérios para a aceitação do risco, não há necessidade de se implementarem controles adicionais e pode haver a retenção do risco.

Ação de evitar o risco

AÇÃO - Convém que a atividade ou condição que dá origem a um determinado risco seja evitada.

Tal ação considera riscos que são elevados e quando os custos de implementação de outras opções de tratamento do risco excederem os benefícios. Desse modo, pode-se decidir que o risco seja evitado completamente.

Um exemplo clássico dessa ação diz respeito a uma instalação física sujeita a alagamento por enchentes. Construir andares muito altos ou barreiras físicas para mitigar o risco podem ser ações muito caras. Dessa forma, uma AÇÃO DE EVITAR O RISCO seria mover a instalação para um outro lugar que não haja esse risco.

Compartilhamento do risco

AÇÃO - Convém que um determinado risco seja compartilhado com outra entidade que possa gerenciá-lo de forma mais eficaz, dependendo da avaliação de riscos.

A decisão de compartilhamento envolve entidades externas de maior expertise para tratar o risco. Tal compartilhamento pode criar novos riscos ou modificar riscos existentes e identificados. Caso isso aconteça, pode ser que um novo tratamento do risco seja necessário.

Aqui temos o exemplo clássico de seguro para tratar as consequências de um risco. Além disso, uma outra alternativa, é utilizar empresas subcontratadas para monitorar e controlas determinados riscos, como uma empresa de vigilância por exemplo.

Aceitação do risco de segurança da informação

ENTRADA - O plano de tratamento do risco e o processo de avaliação do risco residual sujeito à decisão dos gestores da organização relativa à aceitação do risco.

AÇÃO - Convém que a decisão de aceitar os riscos seja feita e formalmente registrada, juntamente com a responsabilidade pela decisão.

SAÍDA - Uma lista de riscos aceitos, incluindo uma justificativa para aqueles que não satisfaçam os critérios normais para aceitação do risco.

Comunicação e consulta do risco de segurança da informação

ENTRADA - Todas as informações sobre os riscos obtidas através das atividades de gestão de riscos.

AÇÂO - Convém que as informações sobre os riscos sejam trocadas e/ou compartilhadas entre o tomados de decisão e as outras partes interessadas.

SAÍDA - Entendimento contínuo do processo de gestão de riscos de segurança da informação da organização e dos resultados obtidos.

Monitoramento e análise crítica de riscos de segurança da informação

Monitoramento e análise crítica dos fatores de risco

ENTRADA - Todas as informações sobre os riscos obtidas através das atividades de gestão de riscos.

AÇÃO - Convém que os riscos e seus fatores (isto é, valores dos ativos, impactos, ameaças, vulnerabilidades, probabilidades de ocorrência) seja monitorado e analisado criticamente, a fim de identificar, o mais rapidamente possível, eventuais mudanças no contexto da organização e de manter uma visão.

SAÍDA - Alinhamento contínuo da gestão de riscos com os objetivos de negócios da organização e com os critérios para a aceitação do risco.

Monitoramento, análise crítica e melhoria do processo de gestão de riscos

ENTRADA - Todas as informações sobre os riscos obtidas através das atividades de gestão de riscos.

AÇÃO - Convém que o processo de gestão de riscos de segurança da informação seja continuamente monitorado, analisado criticamente e melhorado, quando necessário e apropriado.

SAÍDA - Garantia permanente de relevância do processo de gestão de riscos de segurança da informação para os objetivos de negócios da organização ou a atualização do processo.

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[3].

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 • Partes externas
3. Gestão de Ativos	• Responsabilidade pelos ativos • Classificação das informações
4. Segurança em Recursos Humanos	• Antes da contratação • Durante a contratação • Encerramento ou mudança da contratação
5. Segurança Física e do Ambiente	• Áreas seguras • Segurança dos equipamentos
6. Gerenciamento das Operações e Comunicações	• Procedimentos e responsabilidades operacionais • Gerenciamento de serviços terceirizados • Planejamento e aceitação dos sistemas • Proteção contra códigos maliciosos e códigos móveis • Cópias de segurança • Gerenciamento da segurança em redes • Manuseio de mídias • Troca de informações • Serviços de comércio eletrônico

[3] 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.

	• Monitoramento
7. Controle de Acesso	• Requisitos de negócios para controle de acesso • Gerenciamento de acesso de usuário • Responsabilidades dos usuários • Controle de acesso à rede • Controle de acesso ao sistema operacional • Controle de acesso à aplicação e à informação • Computação móvel e trabalho remoto
8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	• Requisitos de segurança de sistemas de informação • Processamento correto nas aplicações • Controles criptográficos • Segurança dos arquivos do sistema • Segurança em processos de desenvolvimento e suporte • Gestão de vulnerabilidades técnicas
9. Gestão de Incidentes de Segurança da Informação	• Notificação de fragilidades e eventos de segurança da informação • 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 • 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)[4]:

- 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;

---

[4] 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.

- 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.

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. **FGV - Auditor Federal de Finanças e Controle (CGU)/Tecnologia da Informação/"Sem Especialidade"/2022**

Um Sistema de Gestão de Segurança da Informação (SGSI) é um conjunto de controles que uma organização implementa para proteger os seus próprios ativos de informação e também para proteger outros ativos pelos quais é responsável.

A norma ABNT NBR ISO/IEC 27001:2019 fornece os requisitos necessários para um SGSI. Rafael foi contratado para implementar o SGSI em um órgão público. Ele elencou os controles necessários para garantir a adequação à norma.

Para isso, Rafael teve que elaborar:

A) políticas de segurança da informação;

B) avaliação de desempenho;

C) política de controle de acesso;

D) definição de funções e responsabilidades de segurança;

E) declaração de aplicabilidade.

Comentários

A chave para responder essa questão está no final do enunciado.

"Ele elencou os controles necessários para garantir a adequação à norma."

Portanto, o que ele fez foi uma **declaração de aplicabilidade** dos controles com a Norma para que eles sejam devidamente implementados.

Gabarito: alternativa E.

---

2. FGV - Perito Criminal (PC AM)/4ª Classe/Processamento de Dados/2022

Para uma correta implementação de um sistema de gestão da segurança da informação em uma organização, é importante criar um documento que descreva tanto os controles que são pertinentes ao SGSI da organização, quanto aqueles controles que não são pertinentes e não serão usados, fazendo assim a ligação entre a avaliação de riscos e o tratamento da segurança da informação.

O nome desse documento é

A) política de segurança da informação, definida na norma NBR ISO/IEC 27002.

B) relatório de levantamento de riscos, definido na norma NBR ISO/IEC 27001.

C) política de controle de acesso, definida na norma NBR ISO/IEC 27002.

D) procedimento para gestão de incidentes definido na norma NBR ISO/IEC 27001.

E) declaração de aplicabilidade, definida na norma NBR ISO/IEC 27001.

Comentários

Outra questão versando sobre o mesmo documento.

O documento que descreve tanto os controles que são pertinentes ao SGSI da organização, quanto aqueles controles que não são pertinentes e não serão usados, fazendo a ligação entre a avaliação de riscos e o tratamento da segurança da informação é uma **declaração de aplicabilidade**.

Gabarito: alternativa E.

---

3. FGV - Analista Judiciário (TJDFT)/Apoio Especializado/Análise de Sistemas/2022

Durante uma auditoria externa contratada pelo Tribunal de Justiça ao departamento de segurança da informação, foram avaliados os sistemas existentes seguindo a Norma ABNT NBR ISO/IEC 27001. Durante a avaliação, houve a necessidade de prover um sistema de gerenciamento de senhas interativo e com qualidade.

Para criar o seu sistema, o departamento de segurança deve fazer uso do objetivo de controle:

A) requisitos do negócio para controle de acesso;

B) controle de acesso ao sistema e à aplicação;

C) responsabilidade pelos ativos;

D) segurança em recursos humanos;

E) gerenciamento de acesso do usuário.

Comentários

O "controle de acesso ao sistema e à aplicação" irá nos ajudar a responder essa questão.

> *A.9.4 Controle de acesso ao sistema e à aplicação*
>
> *Objetivo: Prevenir o acesso não autorizado aos sistemas e aplicações.*
>
> *A.9.4.1 Restrição de acesso à informação*
>
> *Controle*
>
> *O acesso à informação e as funções dos sistemas de aplicações devem ser restrito de acordo com a política de controle de acesso.*
>
> *A.9.4.2 Procedimentos seguros de entrada no sistema (log on)*
>
> *Controle*

> *Onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações devem ser controlados por um procedimento seguro de entrada no sistema (log-on).*
>
> *A.9.4.3 Sistema de gerenciamento de senha*
>
> *Controle*
>
> *Sistemas para gerenciamento de senhas devem ser interativos e devem assegurar senhas de qualidade.*

Portanto, a alternativa correta é a letra B.

Gabarito: alternativa B.

---

4. FGV - Especialista em Saúde (SEMSA Manaus)/Analista de Suporte de Tecnologia da Informação/2022

A opção que a norma ISO/IEC 27001 lista como uma tarefa que cabe à alta direção, dentro de um Sistema de Gestão de Segurança da Informação (SGSI), é

A) criar e atualizar informação documentada.

B) identificar os riscos de segurança da organização.

C) estabelecer uma política de segurança da informação que seja apropriada ao propósito da organização.

D) definir os critérios e o escopo das auditorias internas.

E) estabelecer os objetivos de segurança da informação para as funções e níveis relevantes.

Comentários

> *A Alta Direção deve estabelecer uma política de segurança da informação que:*
>
> *a) seja apropriada ao propósito da organização;*
>
> *b) inclua os objetivos de segurança da informação (ver 6.2) ou forneça a estrutura para estabelecer os objetivos de segurança da informação;*
>
> *c) inclua um comprometimento para satisfazer os requisitos aplicáveis, relacionados com segurança da informação;*
>
> *e d) inclua um comprometimento para a melhoria contínua do sistema de gestão da segurança da informação.*

Portanto, uma das tarefas da Alta Direção é estabelecer uma política de segurança da informação que seja apropriada ao propósito da organização. Alternativa correta, letra C.

Gabarito: alternativa C.

---

5. FGV - Analista Especializado (IMBEL)/Analista de Sistemas/2021/"Provas Reaplicadas" (e mais 1 concurso)

A Associação Brasileira de Normas Técnicas, ABNT, é responsável pela elaboração das Normas Brasileiras como, por exemplo, a ABNT NBR ISO/IEC 27001:2013, sobre aspectos da Segurança da Informação.

Dado que a sigla ISO deriva de International Organization for Standardization, assinale a correta natureza das normas NBR ISO.

A) São normas brasileiras que passam a ser adotadas pela ISO.

B) São normas definidas em conjunto com a ISO.

C) São traduções de normas da ISO que passam a ser adotadas pela ABNT.

D) São normas da ISO adaptadas pela ABNT às práticas brasileiras.

E) São normas brasileiras compiladas a partir da combinação de outras normas da ISO.

Comentários

A banca insiste que você precisa conhecer até o prefácio da Normas cobradas em prova.

A natureza das Normas NBR ISO são apenas traduções para o português, de forma que sejam preservados os entendimentos originais da Norma Internacional.

> *Este Projeto de Revisão foi elaborado pela Comissão de Estudo de Técnicas de Segurança (CE-21:027.00) do Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21)*
>
> *Previsto para ser equivalente à ISO/IEC 27001:2013*
>
> *A Associação Brasileira de Normas Técnicas (ABNT) é o Foro Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais (ABNT/CEE), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, delas fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros).*

Portanto, alternativa correta, letra C.

Gabarito: alternativa C.

6. FGV - Técnico Superior Especializado (DPE RJ)/Tecnologia da Informação/2019

De acordo com a norma ABNT NBR ISO/IEC 27001:2013, uma organização deve programar auditorias internas a fim de verificar a aderência da conformidade do sistema de gestão da segurança da informação aos seus requisitos e à legislação vigente.

Sobre a realização da auditoria interna, é correto afirmar que:

A) os critérios de verificação devem ser sempre os mesmos, independentemente do escopo ou do processo da organização a ser auditado;

B) os auditores não devem conhecer e considerar os resultados das auditorias anteriores para não influenciarem o trabalho de verificação;

C) os auditores devem ser do próprio setor auditado a fim de possibilitar o aproveitamento de seu conhecimento acerca das atividades desenvolvidas;

D) os resultados das auditorias devem ser de conhecimento da direção responsável pelo setor auditado;

E) os relatórios das auditorias podem ser descartados na ausência de inconformidades.

Comentários

A auditoria interna surge como tópico relevante dentro do processo de implementação, estando classificada no tópico relativo a avaliação de desempenho. Essa auditoria vai verificar as conformidades com a legislação aplicável, além da conformidade com os próprios processos internos, relativo a cada uma das organizações.

A auditoria tem o objetivo de recomendar e sugerir mudanças, bem como avaliar o desempenho da implementação do SGSI. Dessa maneira, deve dar conhecimento a direção para as devidas tratativas.

Gabarito: alternativa D.

...

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.