

Disciplina: Governança em Tecnologia da Informação

Aula 6: Governança de segurança

Apresentação

A segurança da informação tornou-se uma questão-chave, considerando o novo posicionamento da informação nas organizações. À medida que cresce o número de ataques e falhas, que podem impactar negativamente na reputação da organização, também é crescente o surgimento de normas, padrões e regulamentações no assunto.

As organizações que ainda não possuem maturidade em segurança da informação necessitam de um ponto de partida para o desenvolvimento de diretrizes específicas de segurança para a organização. Existem vários padrões e normas que podem suprir essa necessidade e um exemplo são as normas da família ISO 27000.

Nesta aula, abordaremos as normas ISO 27000, essencial na construção dos conceitos fundamentais e do vocabulário comum em segurança da Informação; ISO 27002, utilizada para a implementação de controles de segurança; e a ISO 27014, com um processo para orientar as organizações na governança da segurança da informação.

Bons estudos!

Objetivos

- Identificar os conceitos básicos, princípios e melhores práticas em segurança da informação;
- Descrever os conceitos e princípios de um sistema de gestão de segurança da informação;
- Realçar a importância da governança da segurança da informação.

Segurança da informação

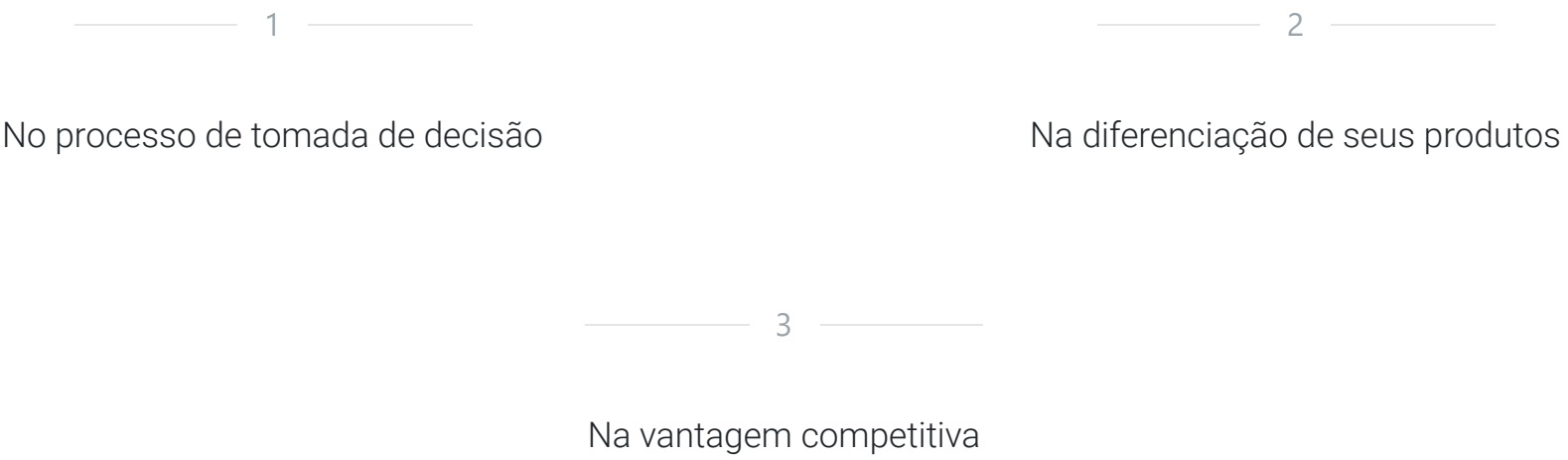
Com o avanço da internet e a adoção cada vez maior de tecnologia da informação para a implementação dos negócios das organizações, a segurança tornou-se uma questão-chave para que as empresas garantam a proteção das informações consideradas relevantes e críticas.

 Segurança da informação | Fonte: Pixabay

O valor da informação para as empresas é considerado, na atualidade, algo imensurável, já que apresenta valor estratégico e/ou financeiro para a organização.

Ao longo dos anos, e com o amadurecimento da tecnologia e das organizações, a informação ganhou valor, trouxe conhecimento para as organizações e, posteriormente, trouxe inteligência aos processos de negócio, conforme ilustra o esquema a seguir.

Esse amadurecimento tem auxiliado as organizações da seguinte forma:



Desse modo, a demanda gradual por armazenamento de conhecimento tem levado à necessidade de administração desses dados de forma confiável.

Uma ação maliciosa bem-sucedida pode ter um impacto direto na reputação da organização. Com o objetivo de mitigar os riscos, as organizações têm investido esforços e dinheiro na implementação de processos, métodos, ferramentas e recursos humanos qualificados em segurança da informação.

Ao mesmo tempo em que cresceu o número de ações maliciosas, surgiram também regulamentações, padrões e boas práticas no assunto, como algumas normas da família ISO 27000, específica de segurança da informação.

Com as normas da família ISO 27000, as organizações podem desenvolver e implementar uma estrutura para gerenciar a segurança de seus ativos de informação e também para a implementação de uma Sistema de Gestão de Segurança da Informação (SGSI).

Veja as normas da ISO 27000 e o que trata cada uma:

ISO 27000	Fornece um vocabulário comum em segurança da informação.
ISO 27001	Fornece as diretrizes para a implementação e manutenção de um sistema de gestão de segurança da informação (SGSI).
ISO 27002	Fornece um código de práticas para a implementação de controles de segurança da informação.
ISO 27014	Fornece um processo para a governança da segurança da informação.

Vamos conhecê-las com mais detalhe a seguir.

Norma ISO 27000

A norma ISO 27000 estabelece uma revisão sobre aspectos e importância da segurança da informação no contexto organizacional, evidencia ainda sobre o estabelecimento e a importância de implementação de um Sistema de Gestão de Segurança da Informação (SGSI) e apresenta um vocabulário comum sobre o assunto.

Vejamos os aspectos dessa norma.


Segurança da Informação

É baseada em três princípios fundamentais, conhecidos como a tríade CID ou, em inglês, AIC ou CIA:

Segundo a norma, a segurança da informação está garantida quando um ou os três princípios estão assegurados.

Em alguns casos, outras propriedades de segurança também podem ser envolvidas como a autenticidade, prestação de contas ou não repúdio e a confiabilidade.

Vamos conhecer cada princípio:

 Clique nos botões para ver as informações.

Confidencialidade

▼

As informações não serão disponibilizadas ou divulgadas a indivíduos, entidades ou processos. Significa garantir que apenas as pessoas que devem ter conhecimento a seu respeito poderão acessá-la.

Autenticidade

▼

Uma entidade é o que se afirma ser.

Disponibilidade

▼

Ser acessível e utilizável sob demanda por uma entidade autorizada. Uma informação disponível é aquela que pode ser acessada por aqueles que dela necessitam, no momento em que precisam.

Integridade

▼

Exatidão e integridade. Significa proteger as informações contra alterações em seu estado original.

Não repúdio

▼

Capacidade de provar a ocorrência de um evento ou ação reivindicada e suas entidades de origem.

Confiabilidade

▼


Comportamento e resultados pretendidos consistentes.

Incidente de segurança da informação

A norma apresenta também o conceito de **incidente de segurança da informação**, que representa um único ou uma série de **eventos indesejados** ou inesperados de segurança da informação que tenham **probabilidade** de comprometer operações comerciais e ameaçar a segurança da informação de uma organização.

O esquema a seguir ilustra a ocorrência desses eventos:

Vamos conhecer esses eventos com mais detalhe.

 Clique nos botões para ver as informações.

Vulnerabilidade



Fraqueza de um ativo ou controle, que pode ser explorada por uma ou mais ameaças.

Ativos



São aqueles que produzem, processam, transmitem ou armazenam informações em uma organização. Podem ser **físicos** (sala, arquivo, cofre), **tecnológicos** (servidor, e-mail, sistema) ou **humanos** (funcionário, porteiro, secretária).

Ameaça



Causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização. Pode ser **física** (incêndio, apagão, inundação), **tecnológica** (vírus, bug software, invasão web) e **humana** (sabotagem, fraude, erro humano).

Risco



Efeito ou incerteza sobre o atingimento de um objetivo. Indica a probabilidade de uma determinada ameaça se concretizar, combinada com os impactos que ela trará. Quanto maior a **probabilidade** de uma determinada ameaça ocorrer e o impacto que ela trará, maior será o risco associado a este incidente.

Norma ISO 27002

Apresenta um conjunto de melhores práticas a serem seguidas pelas organizações e pode ser o ponto de partida para a implementação da segurança da informação pelas organizações.

Ela apresenta os conceitos básicos sobre segurança da informação e como estabelecer os requisitos de segurança nas organizações. Esses requisitos são identificados por meio de:

Com os requisitos de segurança, os riscos identificados e as decisões para o tratamento dos riscos tomadas, as organizações devem selecionar e implementar os controles apropriados para que possam assegurar que os riscos sejam reduzidos a um nível aceitável.

O esquema a seguir ilustra esse processo:




Análise / avaliação
sistemática dos riscos



Tratamento
dos riscos



A norma ISO 27002 contém 14 seções:

 Gestão da continuidade do negócio.

Cada uma das 14 seções apresenta:



Um **objetivo de controle** declarando o que se espera ser alcançado.



Um ou mais controles que podem ser aplicados para se alcançar o objetivo do controle.

Saiba mais

Para conhecer cada seção da norma ISO 27002, leia o texto [“Seções da norma ISO 27002”](#) [<galeria/aula6/anexos/secoes_da_norma_ISO_27002.pdf>](#).

Na implementação desses controles de segurança, as organizações devem considerar o **ciclo de vida** da informação.

Esse ciclo de vida é composto e identificado pelos em que os ativos físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que mantêm a operação da empresa.

Observe o ciclo a seguir:

Atividade

1 - Complete a frase:

A Norma apresenta um conjunto de boas práticas e controles em segurança da informação que servem de guias para as organizações.


ISO 27001

A norma ISO 27001 tem como objetivo oferecer um modelo para que as organizações possam estabelecer, implementar, operar, monitorar e analisar criticamente um sistema de gestão de segurança da informação (SGSI).

Não adianta as organizações aplicarem uma série de dispositivos de segurança da informação sem uma estrutura que garanta sua permanente atualização, adequação e avaliação de efetividade. No estabelecimento de seu sistema de gestão (SGSI), a organização deve determinar o escopo e abrangência do sistema.


A norma ISO 27001 adota em seu processo de gestão o ciclo [PDCA¹](#) para estruturar todos os processos envolvidos em um SGSI.

Observe o ciclo PDCA a seguir:

 Fonte: Shutterstock.

O PDCA é uma ferramenta gerencial que possibilita a melhoria contínua de processos, bem como a solução de problemas por meio de um ciclo de revisões periódicas.

Vamos conhecer melhor cada etapa do ciclo:

 Clique nos botões para ver as informações.

Planejar



São estabelecidos os objetivos e processos necessários para garantir que as metas e objetivos planejados serão atingidos.

Executar



São executados os processos e as atividades planejados na etapa anterior e ainda coletados os dados para serem executados na etapa seguinte.

Verificar



São analisados os dados coletados na etapa anterior e comparados com as metas estabelecidas na etapa de planejamento, determinando possíveis desvios.

Agir



São analisados as causa dos desvios, se existirem, e implementadas as ações corretivas no processo. Podem ser realizadas ações de melhoria ou ainda ações preventivas como forma de mitigar problemas futuros.

Atividade

2 - Qual é a norma que trata dos requisitos para a implementação de um sistema de Gestão de segurança da informação?

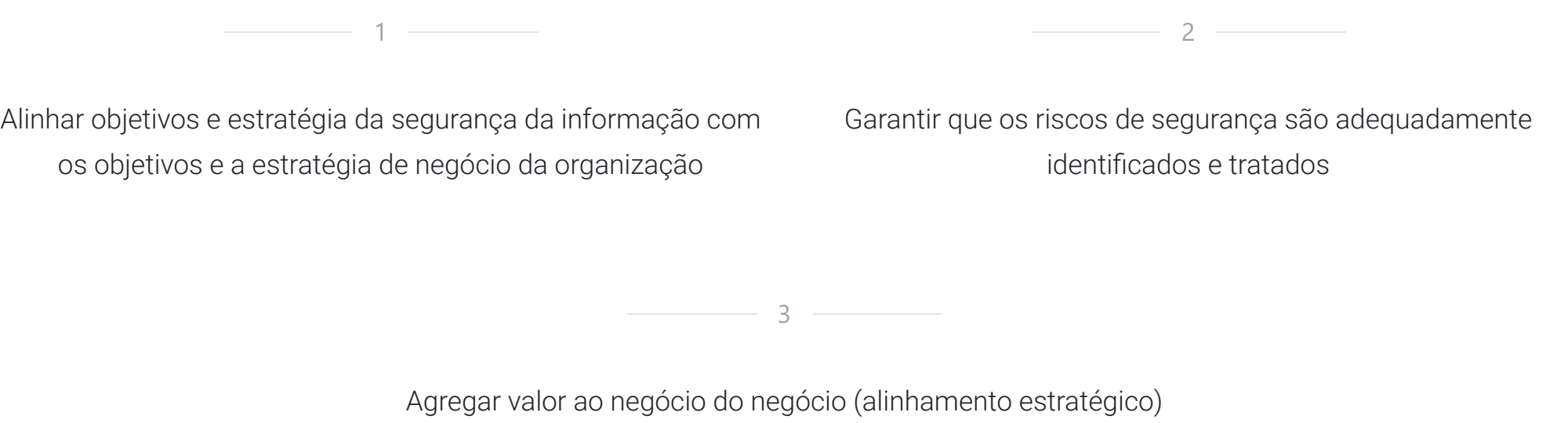
ISO 27014

Com a abrangência das ações de segurança nas organizações é essencial que exista um alinhamento dessas ações com os objetivos e estratégias de negócio da organização.

É essencial que a organização implemente a governança da segurança da informação e que esta seja alinhada com os objetivos e estratégias do negócio e em conformidade com leis, regulamentos e contratos.

 Segurança da informação | Fonte: Pixabay.

São **responsabilidades do corpo diretivo** as decisões e o desempenho da governança de segurança nas organizações. Ele deve garantir que a abordagem de segurança da informação da organização seja eficiente, eficaz, aceitável e alinhada com os objetivos e estratégias de negócios, considerando às expectativas das partes interessadas. São objetivos da governança da segurança da informação:



Assim como as demais governanças implementadas na organização, a governança de segurança apresenta seis princípios importantes para o sucesso de sua implementação:

Estabelecer a segurança da informação em toda a organização

▼

A segurança da informação deve ser tratada considerando o negócio da organização e aplicada a toda a organização de forma integrada.

Adotar uma abordagem baseada em riscos

▼

A governança da segurança da informação deve ser fundamentada em decisões baseadas nos riscos e integrada à abordagem de risco global da organização.

Estabelecer a direção de decisões de investimento

▼

Deve ser estabelecida uma estratégia de investimento em segurança da informação baseada em resultados de negócios alcançados com visões de curto e de longo prazos.

Assegurar conformidade com os requisitos internos e externos

▼

A governança de segurança deve garantir que as políticas e práticas de segurança da informação atendam à legislação e a regulamentações pertinentes obrigatórias, assim como aos requisitos de negócio ou contratuais e aos outros requisitos externos ou internos.

Promover um ambiente positivo de segurança

▼

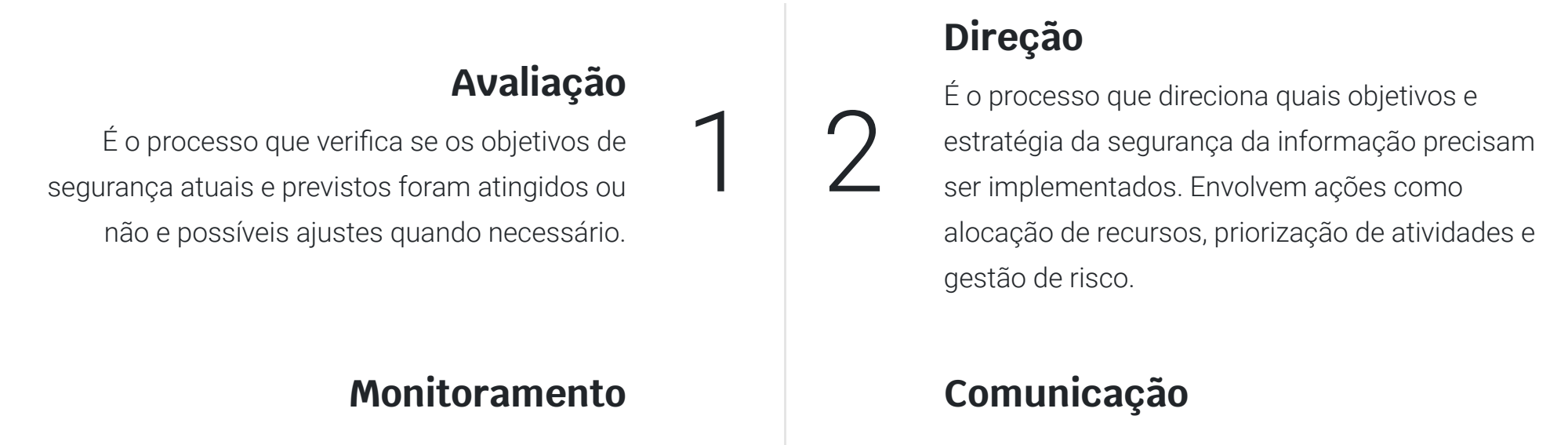
A governança de segurança da informação deve promover e apoiar a coordenação das atividades das partes interessadas para alcançar uma direção coerente para a segurança da informação, viabilizando a implantação de programas de educação, treinamento e conscientização em segurança.

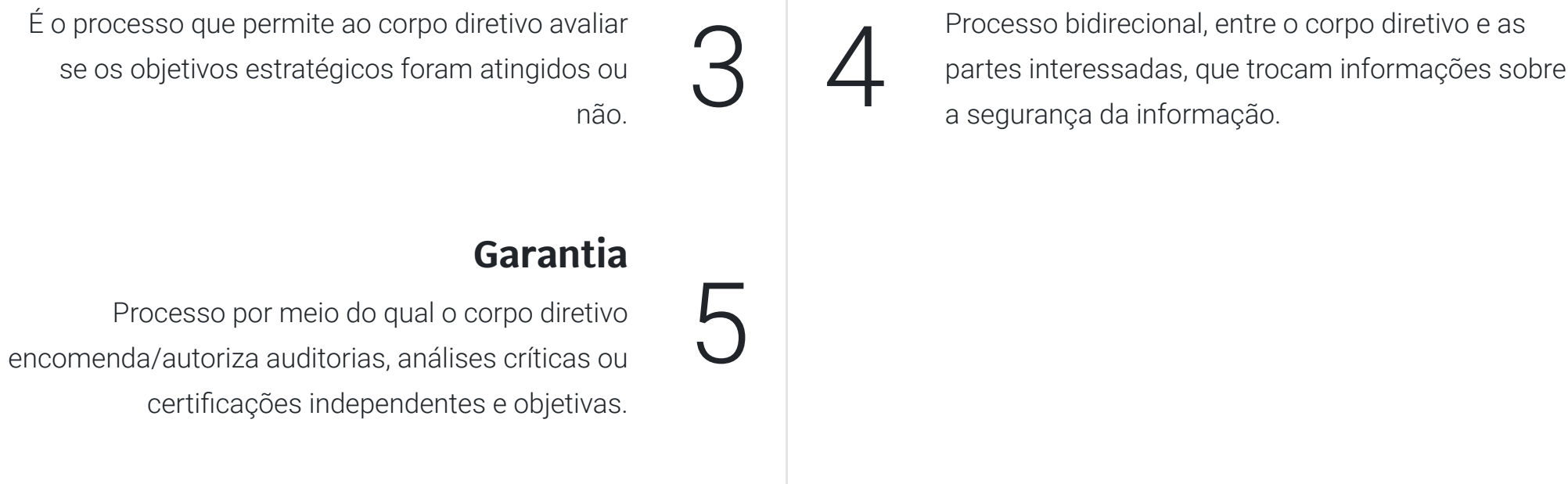
Analisar criticamente o desempenho em relação aos resultados de negócios

▼

A governança da segurança da informação deve garantir que seja adotada uma abordagem para proteger a informação de forma adequada aos interesses da organização e que o desempenho da segurança seja mantido nos níveis necessários para atender aos requisitos de negócio da organização atuais e futuros.

A norma ISO 27014 apresenta um modelo de processo de governança de segurança em que o corpo diretivo executa os seguintes processos de:





O corpo diretivo da organização executa os processos de avaliação, direção, monitoração e comunicação para governar a segurança da informação.

E por meio do processo de garantia poderá solicitar auditorias, análises críticas e certificações independentes, conforme ilustra o processo a seguir:

Vejamos agora quais são benefícios com a implementação da governança da segurança da informação:



Agilidade na tomada de decisão em relação aos riscos de segurança.



Eficiência e eficácia nos investimentos de segurança.



Conformidade com os requisitos externos (legais, regulamentares ou contratuais).



Transparência sobre as ações de segurança da informação.

Você sabe a diferença entre uma ameaça e um ataque?

Segundo a **RFC 2828**, Internet security glossary:

Ameaça



Potencial para violação da segurança quando há uma circunstância, capacidade, ação ou evento que pode quebrar a segurança e causar danos. Ou seja, uma ameaça é um possível perigo que pode explorar uma vulnerabilidade.

Ataque



Um ataque à segurança do sistema, derivado de uma ameaça inteligente, ou seja, um ato inteligente que é uma tentativa deliberada (especialmente no sentido de um método ou técnica) de burlar os serviços de segurança e violar a política de segurança de um sistema.

Exemplo

Em nosso país, o responsável por manter as Normas de Gestão de Segurança da Informação (ISO 27000) é a ABNT, representante da ISO no Brasil e responsável por normatizar essa questão. Todo o trabalho relacionado à elaboração e/ou adaptação das normas ISO na ABNT é realizado por meio de trabalho voluntário e está associado a um dos comitês da ABNT. Na área de informática, o comitê que trata de assuntos relacionados a área é o comitê CB-021.

[ABNT/CB-021 <http://www.abnt.org.br/>](http://www.abnt.org.br/) - Comitê Brasileiro de Computadores e Processamento de Dados Âmbito de atuação:



Normalização no campo de computadores e processamento de dados compreendendo automação bancária, comercial, industrial e do controle de acesso por bilhetes codificados; automação e informática na geração, transmissão e distribuição de dados; segurança em instalações de informática; técnicas criptográficas; gerenciamento em OSI; protocolo de serviços de níveis interiores e cabos e conectores para redes locais, no que concerne a terminologia, requisitos, métodos de ensaio e generalidades.

Atividade

3 - A governança da segurança da informação deve garantir que seja adotada uma abordagem para proteger a informação de forma adequada aos interesses da organização. Sabendo disso, responda à pergunta:

Qual a norma que apresenta um processo para a sua implementação?

PDCA ¹

Plan, Do, Check, Act.

Referências

ABNT NBR. ISO/IEC 2701. Tecnologia da Informação. Técnicas de Segurança. **Sistema de gestão de segurança da Informação**. Requisitos, ABNT, 2013.

_____. ISO/IEC 2702. Tecnologia da Informação. Técnicas de Segurança. **Código de práticas para controle de segurança**. ABNT, 2013.

_____. ISO/IEC 2714. Tecnologia da Informação. Técnicas de Segurança. **Governança de segurança da informação**. ABNT, 2013.

ISO/IEC 27000:2018, Information technology. Security techniques. **Information security management systems** — Overview and vocabular. 5.ed. Disponível em: www.iso.org <<https://www.iso.org/home.html>> Acesso em: 26 fev. 2019.

THE INTERNET SOCIETY. **RFC 2828**: Internet Security Glossary. IETF, 2000. Disponível em: <https://tools.ietf.org/html/rfc2828> <<https://tools.ietf.org/html/rfc2828>> Acesso em: 26 fev. 2019.

Próxima aula

- Conceitos básicos e princípios da Governança de dados e do DAMA-DMBOK;
- Princípios e conceito da Governança de Terceirização: eSCM-SP;
- Princípios e conceito da Governança de Terceirização: eSCM-CL.

Explore mais

Conheça os sites:

- [ABNT](http://www.abntcatalogo.com.br/) <<http://www.abntcatalogo.com.br/>>;
- [Cert.br](http://www.cert.br/) <<http://www.cert.br/>>;
- [NIST](http://csrc.nist.gov/) <<http://csrc.nist.gov/>>;
- [SecuriTeam](http://www.securiteam.com/) <<http://www.securiteam.com/>>;
- [SecurityFocus](http://www.securityfocus.com/) <<http://www.securityfocus.com/>>.

Conheça, ainda, a [cartilha do Cert.br](http://cartilha.cert.br/) <<http://cartilha.cert.br/>>.